The Transactions of the Korean Institute of Electrical Engineers Vol. 61, No. 8, pp. 1186~1192, 2012
http://dx.doi.org/10.5370/KIEE.2012.61.8.1186

제주 스마트그리드 실증단지 수용가 환경에서 Zigbee 보안 체계 설계

A Design for a Zigbee Security System in the Customer Side Environment of Jeju Smart Grid Field Test

이 명 훈* · 손 성 용†
(Myung-Hoon Lee · Sung-Yong Son)

Abstract - In Jeju Smart Grid field test, Zigbee technology is being used as one of customer side solutions for AMI. Although Zigbee networks that provides effective connectivity and control among devices are advantages in ease of implementation and use, the data can be exposed to cyber attacks such as eavesdrop, unauthorized data dissemination and forgery. Currently authentication and confidentiality services are provided with the network and link keys generated based on public key pairs that are pre-installed in offline. However, the network is vulnerable once a hacker intrudes into a local network because operation and management policies for the generated keys are not well-established yet. In this paper, the vulnerability of the Zigbee security system in the customer side environment of Jeju Smart Grid field test is analyzed. Then, two-way authentication with the unique identifiers of devices and user-specific group management policies are proposed to resolve the vulnerability.

Key Words : Smart grid, Security, AMI, Public key, Zigbee

1. 서 론

스마트 그리드에서는 수용가의 전기 사용량 원격 검침 및 전력 사용 패턴 기반의 맞춤형 요금 제도 등 전력 소비자와 생산자의 서비스를 제공하기 위해 실시간 양방향 통신망을 필요로 한다. 제주 스마트그리드 실증단지에서는 실시간 양방향 통신망 구축을 위해 PLC(Power Line Cable), Zigbee, Wibro, WiFi 등 다양한 통신망을 사용하고 있으며, 특히 저전력, 저사양, 저용량으로 임베디드 통신 환경에 최적화 시킨 Zigbee 통신망 도입에 대한 연구가 활발히 추진되고 있다. 그러나, AMI에 Zigbee 통신 시스템 도입은 무선 통신구간에 대한 해커의 접근을 봉쇄할 수 없고, 미터기 데이터 도청을 기반으로 불법 데이터 유포나 데이터 재전송 공격을 시도하여 네트워크와 시스템의 성능을 저하시킬 수 있는 위험을 내포하고 있다. 또한 데이터를 위·변조하여 고객의 전기 요금을 변조하거나 수요반응 명령을 내려 가정의 전력 공급과 수요의 혼란을 야기시킬 수 있다.

UCAIUG에서는 AMI 통신 데이터 해킹에 대한 사전 대응을 위해 AMI-SEC 표준을 제시하였고, 인증, 기밀성, 무결성, 가용성 등 보안 서비스를 요구하였다[1]. 이를 반영하기 위해 Zigbee Alliance에서는 단말 인증, 기밀성, 무결성 등 단말 인증 및 키 분배 방안을 제시하였다[2]. 이러한 보안 요구사항을 만족시키기 위해 제주 실증단지의 Zigbee 통신 구간은 보안 서비스 제공을 위해 사전 공개키 탑재 방식의 PKKE(Public-Key Key Establishment) 알고리즘을 적용하였고, 인증 및 기밀성, 무결성 서비스를 제공하였다. 그러나, 공개키 기반의 인증 방안은 단말에 대한 인증부분이 결여되기 때문에 공개키 위조나 외부 공개키를 이용하여 내부 통신망 접근이 가능하다. 그리고, ESP(Energy Service Portal) 에서 키 운영·관리 방안이 마련되지 않았기 때문에 내부 통신망에 접근할 경우 모든 단말의 링크키를 획득하여 사이버 공격에 악용될 수 있다.

본 논문에서는 제주 실증단지 수용가에 적용된 Zigbee 통신망의 데이터 보호를 위해 Zigbee 보안 표준 및 실증단지 구축 현황, 취약점 등을 분석하였고, 이를 근거로 Zigbee 시스템을 탑재한 단말의 양방향 인증 방안과 그룹별 키 관리에 따른 링크키 운영·관리 방안을 제안한다. 2장에서는 Zigbee 시스템 보안 표준에 대하여 설명하고, 3장에서는 제주 실증단지에서 Zigbee 시스템 보안 솔루션에 대하여 제시하였다. 4장에서는 제주 실증단지 Zigbee 시스템 취약점에 대하여 분석하였고, 5장에서 취약점 해결을 위한 방안을 제안하였다. 6장에서는 제안 시스템에 대하여 고찰하였고, 7장으로 결론을 맺었다.

2. Zigbee System 보안

Zigbee Alliance는 스마트 그리드 환경에서 수용가 영역의 내부온도 측정이나 전력 사용량 등 지능형 응용 프로그램의 연결을 수월하게 처리하기 위하여 Zigbee SE(Smart Enery) 프로토콜을 표준으로 제안하였고, 무선통신 구간의 데이터 보호를 위해 인증, 기밀성, 무결성 등 보안 서비스

* 준 회 원 : 롯데정보통신
† 교신저자, 정회원 : 가천대 에너지IT학과 조교수
E-mail : xtra@gachon.ac.kr
접수일자 : 2012년 2월 21일
최종완료 : 2012년 6월 25일

제공 방안을 제시하였다[2].

2.1 Zibgee 시스템 구성

전력 소비자와 공급자의 데이터 통신 서비스를 제공하기 위해 도입되는 Zigbee 시스템은 그림 1과 같이 수용가 영역에 구축되어 데이터 통신 서비스를 제공하고, 수용가의 정보를 처리하기 위해 AMI 서버, ESP, 수용가 기기로 구분하였다. 첫 번째, AMI 서버는 수용가들의 전기 사용량 정보를 수집하고, 수집된 정보를 분석하여 전기 요금 고지서 발송 및 전기 수요가 급증할 경우 수요반응 서비스 등을 제공한다. 그리고, 실시간 전기 요금 또는 고객의 전기 사용 패턴들을 저장하여 고객을 위한 다양한 전력 요금제를 제공한다[3].

두 번째, ESP(Energy Service Portal)는 데이터 집중기, 스마트 미터기, 홈 서버 등 수용가 내부기기와 AMI 서버의 데이터 중계를 위해 유무선 신호 및 통신 프로토콜을 변경하는 게이트웨이 역할을 담당하고 있으며, 추가적으로 수용가 기기들에 대한 인증 및 키 운영 관리 업무 수행한다. 세 번째, 수용가 기기는 스마트 미터기, IHD(In Home Device), 관리 콘솔 등 댁내에 구축되는 시스템으로 가정의 전기 사용량을 상위로 전송하고, 전기 요금 정보나 수요 반응 요청을 상위로부터 전송받아 능동적인 또는 강제적으로 전력 관리 서비스를 제공한다.

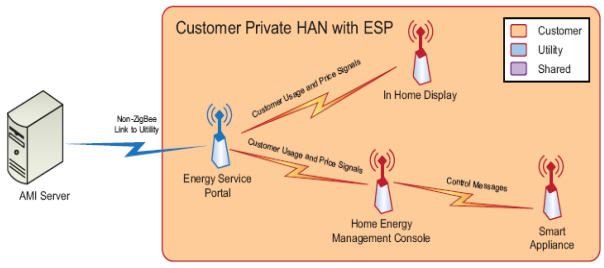

그림 1 수용가 시스템 구성
Fig. 1 Customer system configuration

2.2 Zibgee 보안 프로토콜 스택

Zigbee 보안 서비스 제공을 위한 스택 구성은 그림 2와 같이 키 관리를 위한 NWK(Network Layer)와 키교환 및 암호 알고리즘을 관리하는 APS(Application Support Sublayer)로 구분되며, 단말 인증 및 기밀성 제공을 위한 ECC, AES 등 보안 알고리즘과 마스터, 네트워크, 링크 키를 관리한다. 첫 번째, ECC는 보안 협약에 사용되며, 협약 과정에서 단말 인증을 통해 네트워크/링크 키를 안전하게 생성한다. AES는 데이터 기밀성 제공을 위해 사용되며, 생성된 네트워크/링크 키를 통해 데이터 암호화 서비스를 제공한다[4].두 번째, Zigbee 시스템의 마스터 키는 사전 탑재나 키 교환 알고리즘 등에 의해 분배되어 APL 계층에 저장되며, 단말 인증과 네트워크/링크 키 분배를 위해 사용된다. 네트워크 키는 NWK에 저장되며, ESP와 댁내의 무선 통신 구간의 데이터 보호한다. 링크키는 APS에 저장되며, ESP나 댁내의 Zigbee 통신 단말간 통신 데이터 보호를 위해 이용한다.

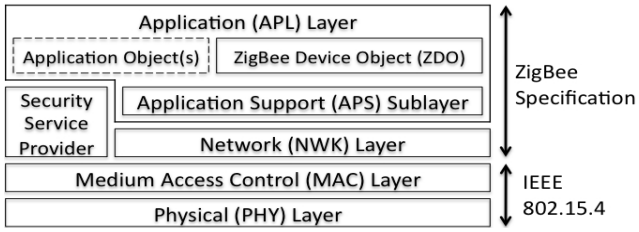

그림 2 Zigbee 스택 계층
Fig. 2 Layers of Zigbee stacks

2.3 인증 및 키 교환

Zigbee 통신 구간은 무선 데이터 전송에 따라 외부에서 도청이 수월하기 때문에 통신 데이터 보호를 위해 “기밀성, 무결성, 인증, 부인봉쇄, 권한부여, 가용성, 감사” 등과 같은 보안 서비스를 요구되었다. 다음은 Zigbee 시스템에서 보안 서비스 제공을 위한 기술이다.

- 인증 : ECC 인증서
- 기밀성 : AES-128, ECMQV Key 협약
- 무결성 : CCM*, Counters, ECDSA 전자 서명
- 부인봉쇄 : ECDSA 전자 서명
- 권한부여 : 링크 키, ECC 전자 서명
- 가용성 : 주파수 회피
- 감사 : Report Event Status

위와 같은 보안 서비스 제공을 위하여 Zigbee 시스템은 "ECC, AES, 난수 생성기“를 APS에 사전 탭재되고, 구축 환경에 따라 마스터키를 사전 설치하거나 또는 신뢰센터를 통해 분배받는다. 초기 단말이 등록될 경우 단말 인증 및 안전한 키 교환 서비스 제공을 위해 ECC 기반 알고리즘과 마스터 키, 난수 생성기를 이용하여 인증, 부인봉쇄, 권한부여 등 보안 서비스를 제공하기 위해 대칭키 기반의 SKKE(Symmetric-Key Key Establishment)나 공개키 기반의 PKKE(Public-Key Key Establishment), CBKE (Certificate-based Key Establishment) 등 보안 협약 과정을 수행한다. 보안 협약 결과 생성된 네트워크/링크 키를 이용하여 128bit AES 암호 알고리즘을 이용하여 기밀성과 무결성 서비스를 제공한다.

3. 제주 실증단지 Zigbee System

제주 실증단지에서는 고객의 전력 사용량에 대한 운영 관리를 위해 실시간 양방향 통신망을 구축하였으며, 자체적으로 사설 통신망의 구축은 "HAN->NAN->WAN"으로 구분하여 통신 환경 및 프로토콜을 구분하였다. 현재 Zigbee 시스템은 HAN 내부와 NAN 연계구간에 구축되었으며, 데이터 보호를 위해 Zigbee 통신기기 제조 단계에서 ECC, AES, 난수 생성기 등을 사전에 탑재하였고, 초기 제조 단계에서 공개키 쌍을 주입시킨 상태에서 구축하였다.

3.1 실증단지 시스템 구성도

제주 실증단지의 Zigbee 시스템은 그림 3과 같이 수용가 기기와 데이터 집중기 구간에 구축되었다. 기기의 데이터 전송을 위해 DLMS(Device Language Message Specification) 프로토콜을 도입하였다. 수용가 기기는 스마트 미터기와 IHD(In Home Device)가 있으며, 스마트 미터는 정해진 주기로 고객의 전기 사용량을 데이터 집중기에 전송하고, IHD는 전기 요금 정보를 AMI 서버에 요청하여 실시간으로 요금 정보를 제공하였다.

데이터 집중기 DCU(Data concentrate unit)는 수용가 기기들의 정보를 주기적으로 제공받아 수집하고, AMI 서버가 정보를 요청할 경우 TCP/IP 통신 방식으로 수집된 정보를 제공하였다. 또한, 수용가 기기와 AMI 서버의 통신을 중개하기 위해 게이트웨이 역할을 수행하며, 추가적으로 수용가 기기의 보안 협약의 주체로써 네트워크/링크 키 운영 및 관리를 위하여 DCU가 ESP역할을 담당하였다.

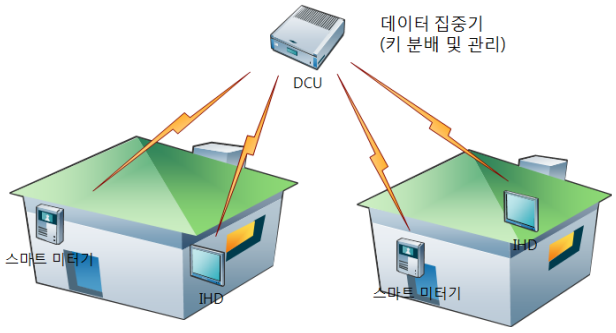

그림 3 제주 실증단지 Zlbgee 시스템 구성도
Fig. 3 Zlgbee system configuration in Jeju field test

3.2 시스템 인증 절차

제주 실증단지의 Zigbee 통신구간은 보안성 향상을 위하여 데이터 기밀성과 수용가 기기의 MAC 주소 인증을 통해 권한 부여 서비스를 제공하였다. 데이터 기밀성 제공은 수용가 기기가 Zigbee 통신망에 접근할 경우 제조 단계에서 주입된 공개키 쌍을 마스터키로 사용하여 그림 4와 같이 ECC 알고리즘 기반의 PKKE 보안 협약 과정을 진행하여 네트워크/링크 키를 생성하고, AES 알고리즘에 생성된 키를 이용하여 데이터 기밀성을 제공하였다. 다음은 보안 협약의 세부 동작 과정을 설명하였다[5,6,7].

1) 초기 통신자와 수신자는 임의의 랜덤값과 공개키 공유
   - $S_U|S_V|E_U|E_V$
2) 공유된 정보를 이용하여 네트워크/링크 키 생성
   - 공유된 값들을 이용하여 “Z” 값을 유도
   - kdf(Key Derivation Function)에 Z를 입력하여 MacKey와 KeyData를 추출
   - "MacData2"를 MacKey로 암호화하여 “MacTage2”를 생성
3) MacTage를 생성하여 키 검증을 위해 전송
   - 생성된 MacTag값을 이용하여 키 검증
   - 링크키는 키 협약 과정에서 Key_load=HMAC(0x02)lk 하여 링크키 탑재
   - 네트워크 키는 Key_trasport=HMAC(0x00)lk 하여 네트워크키 탑재

그러나, PKKE 방식을 이용한 보안 협약은 공개키 쌍을 기반으로 진행되기 때문에 단말에 대한 인증 서비스가 반영되지 않았기 때문에 제주 실증단지 수용가 기기의 인증을 위해 MAC 주소 기반의 인증 방식을 추가로 도입하였다. MAC 주소 인증은 통신망에 수용가 기기가 접속할 경우 AMI 서버에 등록이 되지 않았을 경우 데이터를 차단시키는 방법이다. 관리자에 의해 MAC 주소를 승인할 경우에 한해서 데이터 통신 서비스를 제공하였다. 그리고, 단말 인증 및 키 관리를 DCU에서 수행함에 따라 인증된 단말은 DCU에서 관리하고 있는 단말들의 접근 권한을 부여하고 있으며, 내부 단말들의 키를 DCU에서 제공받아 데이터 도청 및 위변조 공격이 가능하다.

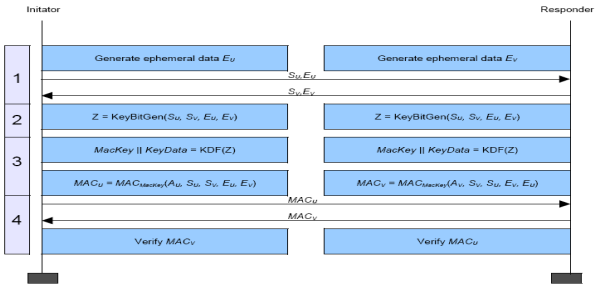

그림 4 PKKE 보안 협약 방식
Fig. 4 PKKE security agreement scheme

4. 제주 실증단지 Zigbee System 보안 취약점 분석

제주 실증단지 수용가 환경에서 Zigbee 시스템은 통신 데이터 보호를 위해 사전에 보안 모듈과 공개키 쌍을 탑재하였고, 이를 기반으로 안전한 보안 협약 및 데이터 암호화를 위한 키를 생성하였다. 그러나, 암호 키가 노출될 경우 해커는 내부망에 접근 가능하며, 데이터 집중기와 연계된 모든 수용가 기기들의 정보가 노출될 수 있다. 본 장에서는 단말 인증 및 키 운영·관리 방안에 대한 취약점을 분석하였다.

4.1 단말기의 인증

제주 실증단지의 Zigbee 시스템 인증은 제조 단계에서 삽입한 공개키 쌍과 미터기 모뎀의 MAC 주소를 기반으로 수행하고 있다. 공개키 쌍을 이용한 인증은 마스터키로 공개키 쌍을 활용하여 PKKE 보안 협약을 진행하고, ECC 기반 보안 협약으로 안전하게 생성된 네트워크/링크 키에 따라 네트워크 망의 접근권한을 부여받는다. 그러나, 현재 실증단지에 구축된 공개키 쌍 기반의 인증은 제조 단계에 탑재된 마스터키만을 이용하고 있기 때문에 단말에 대한 인증 방안은 마련되지 않았다.

따라서, 단말에 대한 인증 서비스를 제공하기 위해 MAC 주소 기반의 단말인증 방안을 추가하였다. 그러나, Zigbee에서 제공하는 기밀성은 데이터 보호를 목적으로 MAC 주소 상위에서 보안 서비스를 제공하기 때문에 MAC 주소는 평문으로 외부에 전송되며, 해커가 네트워크 망을 도청할 경우 MAC 주소는 그대로 노출되어 위조가 가능하다. 따라서, 외부 공격자의 접근을 사전 탐지 및 차단할 수 있는 단말 고유 식별자 기반의 접근제어 방안이 필요하다.

4.2 ESP 키 운영 및 관리

실증단지에 구축된 Zigbee 시스템은 단말의 데이터 보호를 위해 보안 모듈과 마스터 키를 사전에 탑재하여 구축하고, 단말 인증 및 데이터 암호화를 위한 키를 생성하기 위해 ESP와 보안 협약을 수행한다. ESP는 단말의 인증 과정을 통해 네트워크와 링크키를 분배하고, 분배된 키를 운영·관리하여 인증된 단말의 접근 및 제어 서비스를 제공한다. 그러나, ESP는 연계된 모든 단말들의 키를 통합 관리하고 있으며, ESP에 연계된 단말들 간의 통신에 대한 접근 제한 방안이 마련되지 않았다. 만약, 해커가 통신망에 접근하여 ESP 인증을 받을 경우 연계된 모든 단말에 대한 접근이 가능하고, 정보의 도청 및 위변조 공격을 시도하여 전력 정보의 혼란을 야기시킬 수 있다. 이러한 문제를 해결하기 위해 기기간의 특징에 따른 통신 서비스 운영 방안이 필요하다.

5. 시스템 제안

본 장에서는 제주 실증단지 Zigbee 시스템의 취약점인 단말 인증 및 키 운영·관리 체계를 강화하기 위하여 고유식별자 기반의 인증 및 그룹키 생성 방법을 제안하였다. 제안된 인증 방안은 PKKE 과정에 단말의 고유 ID 정보를 추가하여 인증을 시도하고, 고유 ID 정보를 기반으로 그룹키를 생성하는 방법을 사용한다. 고객에 따라 제공되는 고정 식별자를 근거로 양방향 인증 및 그룹 키 생성하여 실증단지의 취약점을 해결할 수 있다.

5.1 시스템 구조

제안된 시스템에서는 현재 제주실증단지의 구조를 그대로 유지하면서 AMI 서버와 DCU, 단말의 기능을 그림 5와 같이 구조를 수정하였다. AMI 서버는 기존의 MAC 주소 인증을 대신하여 단말의 고유 식별자 기반으로 인증 방법을 수정하고, 고유 식별자의 해쉬값을 이용하여 양방향 인증을 제공한다. DCU는 내부망 통신을 관리하기 위해 고유 식별자를 기반으로 고객별 그룹 키를 생성하고, 단말의 네트워크/링크키 생성시 그룹키와 맵핑하여 운영·관리한다. 마지막으로 단말은 기존 Zigbee 보안 모듈을 그대로 유지하며, 고객별로 고유식별자를 생성 및 안전하게 AMI 서버와 통신하기 위한 알고리즘을 제안한다. 고유식별자 전송 알고리즘은 PKKE 협약이 완료된 시점에서 협약된 키를 이용하여 안전하게 AMI 서버에 전송하여 단말의 양방향 인증을 수행한다.

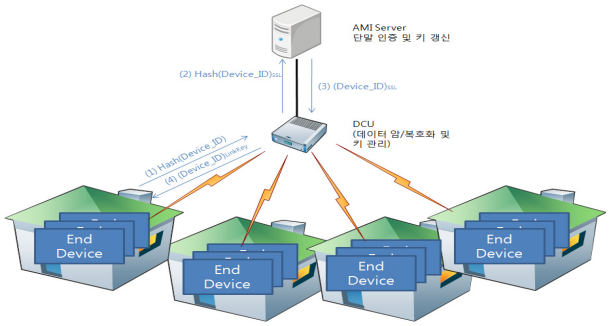

그림 5 제안된 시스템 구성도
Fig. 5 Proposed system configuration

5.2 양방향 단말 인증

제안된 시스템의 양방향 단말 인증은 기존 공개키 기반에 단말의 고유 식별자를 추가하여 안전하게 양방향 인증 방식을 제공한다. 키 분배를 위한 PKKE 과정에서 마스터키는 공개키 쌍 기반 ECC 알고리즘을 그대로 유지하고, 키 검증 과정에서 단말의 고유 식별자를 이용하여 인증서비스를 제공한다. 그림 6과 같이 제안 시스템은 기존 PKKE와 동일하게 보안협약을 진행되며, 검증단계에서 고유식별자를 추가하여 AMI 서버와 양방향 인증서비스를 제공한다. 다음은 제안한 협약과정에 대한 세부 동작 과정이다.

1) 1 단계
- 안전하게 네트워크/링크 키 생성을 위한 요소의 교환
  - 단말 'U'와 DCU 'V'는 키 키생성을 위해 공개키 'E'와 랜덤 값 'S'를 상호 공유
    U, V = "Su, Eu, Sv, Ev"

2) 2 단계
- 단말과 DCU는 내부연산으로 키 생성을 위해 Z 값을 생성
  - KeyBitGen에 단말과 DCU가 공유한 키 생성 요소들을 탑재하여 실행
  - 단말과 DCU는 동일한 값을 가진 256bit의 Z 값을 생성
    Z = KeyBitGen(Su, Eu, Sv, Ev)

3) 3 단계
- Z 값을 이용하여 MacKey와 KeyData를 생성
  - Z값을 kdf에 넣어 256bit의 키를 변환
  - 생성된 Key의 상위 128bit는 MacKey로 사용하고, 하위 128bit는 KeyData로 사용
  - MAC 값에서 송신자 A는 02_{16}을 탑재하고, 수신자 A는 03_{16}으로 값 생성
    KKeyData = kdf(Z, 256)
    MacKey = Leftmost 128 bits of KKeyData
    KeyData = Rightmost 128 bits of KKeyData
    MAC = MAC_{MacKey}(A, Su, Eu, Sv, Ev)

4) 4 단계
- 생성된 MAC 값 및 Device_ID를 전송하여 단말인증
  - 생성된 MAC 값을 교환하여 보안 협약이 제대로 이루어졌는지 검증

$MAC_U = MAC_{MacKey}(02_{16}, Su, Eu, Sv, Ev)$
$MAC_V = MAC_{MacKey}(03_{16}, Su, Eu, Sv, Ev)$

- Device_ID를 AMI 서버에 Device_ID를 해쉬한 값을 전송하여 인가 요청
- AMI는 인증후 Device_ID를 U에게 전송하고 V는 협약된 LinkKey로 Device_ID를 암호화하여 전송

$U = Hash(Device\_ID)$
$V = (Device\_ID)_{LinkKey}$

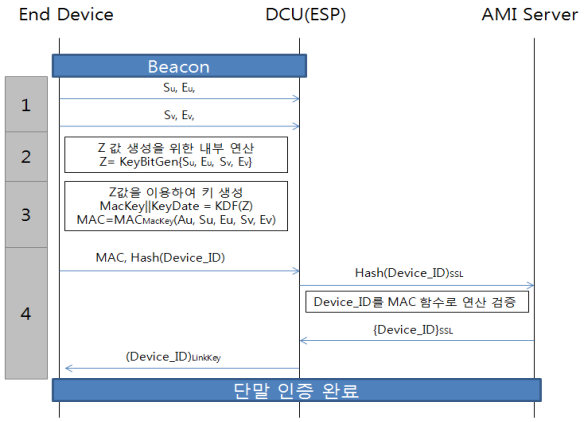

그림 6 제안된 시스템의 보안 협약
Fig. 6 Security agreement scheme of the proposed system

5.3 그룹키 생성

현재 ESP의 역할을 수행하는 DCU는 사전에 탑재된 공개키 쌍을 이용하여 단말의 인증서비스를 제공하고 있으며, 단말과 DCU의 통신 데이터 기밀성 제공을 위한 네트워크/링크 키 생성 및 운영, 관리 서비스를 제공한다. DCU에는 최대 50대의 단말이 연계가 가능하고, 데이터 기밀성 제공을 위해 인증된 모든 단말의 네트워크/링크 키를 저장하여 관리하고 있다. DCU의 내부 단말의 키 운영·관리에 따라 내부망에 인증된 단말기가 DCU에 접근하여 단말간의 통신을 요청할 경우 DCU는 쌍방의 링크 키를 단말에 전송하여 단대단 통신 서비스를 지원한다.

이러한 통신 구조는 공격자가 내부망에 접근할 경우 모든 단말의 링크키를 획득할 수 있으며, 데이터 도청에 따른 악의적인 공격이 가능하기 때문에 내부 단말들간의 접속을 제한하기 위한 방안이 필요하다. 그림 7과 같이 내부 단말들의 접근을 제안하기 위해 고객의 고유식별자를 기준으로 그룹을 생성하고, DCU는 그룹별로 단말간의 통신서비스를 제한하기 위해 다음과 같은 협약과정을 수행한다.

1) 1 단계
- 단말 양방향 인증 요청
  - 단말과 양방향 인증을 위해 고유식별자 정보를 AMI 서버에 전송
  - 단말은 PKKE 과정에서 Hash(Device_ID)를 전송

2) 2 단계
- 그룹별 키 생성 및 AMI 서버에 단말 인증 요청
  - PKKE 보안 검증을 선행하고, 정상시 Hash(Device_ID)를 기준으로 링크키를 저장
  - Hash(Device_ID)를 사전 협약된 SSL 알고리즘을 이용하여 AMI 서버에 전송

3) 3 단계
- 단말 인증
  - AMI 서버는 구축과정에 등록한 단말의 Device_ID를 Hash 알고리즘에 탑재하여 Hash(Device_ID) 값과 비교하여 단말 인증
  - 단말 인증이 정상적으로 수행될 경우 Device_ID를 DCU에 전송

4) 4 단계
- 단말 접근 승인
  - DCU는 Device_ID를 Hash 알고리즘에 탑재하여 수행하고, 정상적일 경우 단말의 접근권한 부여

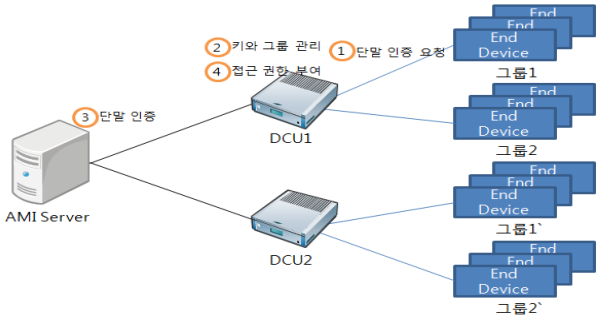

그림 7 그룹키 관리 체계
Fig. 7 Group key management scheme

5.4 키 교환 방식의 성능 분석

제안된 시스템에서는 단말이 스마트그리드 통신망에 최초로 접근을 시도할 경우 양방향 인증을 통한 키 생성 및 분배 방안을 사용하였다. 최초 단말이 등록될 경우 ECC 기반의 공개키 알고리즘을 이용하여 단말 인증 및 데이터 기밀성 제공을 위한 대칭키를 분배하고, 이후 데이터 통신은 대칭키 방식으로 데이터 기밀성을 제공하는 방식이다.

최초 단말 등록시 안전하게 양방향 인증 서비스와 키 교환에 걸리는 시간은 환경에 따라 다르지만 그림 8과 같이 키의 길이에 따라 공개키 생성 및 키 분배에 소요되는 시간이 제시되기도 하였다[8]. 초기 단말 부팅과정에서 소요되는 공개키 분배 시간은 중요 데이터를 전송하기 이전이기 때문에 데이터 가용성에 영향을 미치지 않는다.

초기 단말의 양방향 인증 및 대칭키를 교환한 이후 대칭키 알고리즘을 도입하여 데이터 기밀성을 제공한다. 현재 개발된 알고리즘에서 최고의 성능은 그림 9와 같이 초당 90,000의 데이터를 처리할 수 있는 AES가 가장 효과적이며, 현재 제주 실증단지에 적용중인 SEED와 TDES보다 두 배 이상의 처리 성능을 보이고 있기 때문에 기밀성 및 가용성을 안정적으로 제공할 수 있다[9]

$E : y^2 \equiv x^3 - 3x + b \pmod{p}$

P	공개키 생성 시간	키 분배 시간	총 시간
192	1797	1796	3593
224	2567	2519	5086
256	4273	4273	8546
384	15664	15493	31157
521	43742	43304	87046

그림 8 ECC 알고리즘 키교환 소요시간 예 [8]

Fig. 8 An example of key exchange time with ECC algorithm

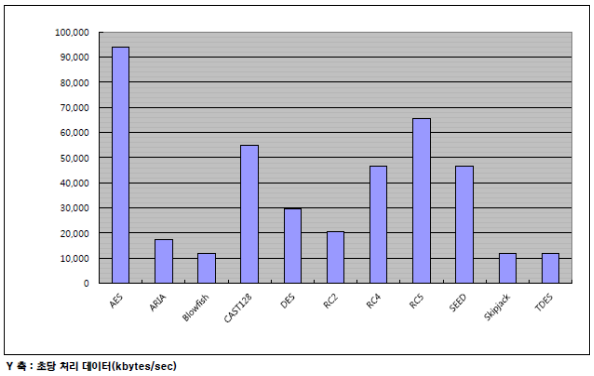

그림 9 대칭키 알고리즘 성능비교 [9]

Fig. 9 Performance comparison among symmetric key algorithms

6. 제안 시스템 고찰

제주 실증단지에 구축된 수용가의 Zigbee 시스템은 비용을 고려하여 임베디드 환경의 저사양, 저용량으로 개발되었고, 보안 모듈은 저사양에서도 동작을 할 수 있어야 하기 때문에 작은 키로도 보안강도가 높은 ECC 기반의 모듈을 탑재하였다. ECC 보안 모듈은 Zigbee SE 표준에 준하는 국내 제품이 미흡한 관계로 외산 제품을 탑재하여 실증하고 있으며, 일부 컨소시엄의 스마트 미터기 모뎀에 보안 모듈을 탑재하여 실증 테스트를 진행하고 있다.

제주 실증단지의 Zigbee 시스템은 사전에 탑재된 공개키 쌍을 이용하여 인증 및 보안 협약을 진행하기 때문에 단말에 대한 인증은 제공되지 않으며, ESP에서 관리하는 보안키는 내부망에 접근하는 단말의 경우 모두 공개되어 단말간의 통신을 제공한다는 단점이 있다. 그리고, 현재 실증중인 보안 모듈은 외산 제품을 구입하여 실증하기 때문에 소스가 공개되지 않아 통신 프로토콜 수정이 어렵고, 공개키 쌍 생성을 위한 라이센스 구입 문제가 존재한다.

현재 Zigbee 단말은 공개키 쌍과 MAC 주소를 기반으로 인증 서비스를 제공하고 있다. 그러나, 인증서는 단말 인증보다는 기밀성 제공을 위한 키 교환이 목적이기 때문에 ECC 기반 인증서 탑재한 단말은 네트워크 망에 접근이 가능하고, 외부 접근 가능성을 사전에 차단을 위해 MAC 주소 기반 인증 방안을 추가하였으나 평문으로 MAC 주소가 노출되기 때문에 변조에 따른 네트워크 망 접근이 가능하다. 따라서, 단말의 양방향 인증 서비스 제공을 위하여 고유식별자 기반의 인증 방안을 제안하였다.

고유 식별자 기반 양방향 인증 시스템은 단말의 설치과정에서 고객의 고유 식별자를 AMI 서버에 등록하고, 단말이 네트워크 망 접근을 요청할 시 고유 식별자를 이용해 접근 권한을 부여한다. 만약, 해커가 고유식별자 정보를 도청할 경우 고객의 위치를 확인할 수 있으며, 정보를 이용하여 고객의 생활 패턴을 분석 등의 위험에 사전 대응하기 위해 외부에 노출되어도 정보의 복호화가 어려운 단방향 해쉬 함수를 도입하였다.

현재 키 운영·관리를 위한 Zigbee 시스템은 제조 단계에서 탑재되는 공개키 쌍을 기반으로 안전하게 네트워크/링크 키 생성을 위한 PKKE를 수행한다. 그러나, 생성된 키에 대한 체계적인 운영·관리 방안이 마련되어 있지 않아 키 생성에 따른 통신망의 접근은 DCU와 연계된 모든 단말의 접근이 가능하며, 한번 생성된 키는 영구적으로 사용하게 된다. 이는 해커가 키를 획득할 경우 DCU와 연계된 모든 단말의 키를 제공받을 수 있으며, 도청 및 위변조 공격이 가능하다.

7. 결 론

제주 실증단지에서는 수용가 기기의 데이터를 상위 AMI 서버에 전송하기 위하여 무선 통신 회선인 Zigbee 시스템을 이용하여 데이터 집중기까지 전송하고, 데이터 집중기는 수용가 기기의 정보를 수집하여 AMI 서버에 전송하고 있다. Zigbee 무선 통신 구간은 주파수 영역에서 해커가 데이터 도청에 따른 패킷 재전송과 같은 네트워크 트래픽 증가 공격이 가능하기 때문에 인증, 무결성, 기밀성, 가용성 등 보안 서비스는 필수적이다. 그러나, 제주 실증단지에 구축된 일부 Zigbee 시스템은 기밀성, 무결성 제공을 목적으로 개발되었기 때문에 단말 인증 방안이 필요하며, 키 운영·관리 방안이 마련되지 않아 마스터 키나 링크키를 해킹할 경우 네트워크 망의 접근이 가능하고, DCU와 연계된 모든 단말의 정보를 수집할 수 있다.

본 논문에서는 제주 실증단지의 Zigbee 시스템 보안성 강화를 위하여 단말의 양방향 인증, 그룹 키 생성 및 운영·관리 방안을 제안하였다. 단말의 양방향 인증을 위해 사전에 단말의 고유 ID를 이용한 설정 방법을 제시하였고, 고유 ID 기반으로 그룹을 생성하여 키를 관리하는 방안을 제시하였다. 이를 통해 DCU와 연계된 단말들을 그룹으로 구분하여 타 그룹과의 통신은 근본적으로 차단하여 키 노출에 대한 해킹의 위협을 최소화하기 위한 방안을 제안하였다.

현재 제주 실증단지의 보안은 사이버 보안을 기반으로 데이터 보호를 위한 기밀성과 무결성 제공을 목적으로 보안 시스템이 적용되었다. 그러나, 스마트그리드가 확대 적용되어 스마트 미터기의 보급이 증가할수록 키 운영·관리에 대한 이슈는 부각될 것이다. 본 논문에서는 현재 적용 운영중인 제주 실증단지의 보안 현황을 분석하였고, 향후 스마트 미터기의 확대 적용에 따라 발생 가능한 키 운영 관리방안을 제안하였다.

본 연구에서 제주 실증단지를 위한 Zigbee 시스템 보안은 기존 구조를 그대로 유지하면서 외부 위협에 대한 피해를 최소화하기 위해 양방향 단말 인증 및 그룹 키 생성 및 운영·관리 방안을 제시하였으나, DCU의 단말의 인증 서비스 및 키 운영·관리에 따른 부하집중에 따라 수용가의 규모가

확대될 경우 트래픽 폭주에 따른 통신 오류가 발생할 가능성이 높다. 이를 해결하기 위해 DCU의 부하를 최소화할 수 있는 운영·관리 방안에 대한 추가적인 연구가 필요하다.

감사의 글

본 연구는 2011년도 지식경제부의 지원에 의하여 이루어진 연구로서, 관계부처에 감사 드립니다.

참 고 문 헌

[1] UCAIUG:AMI-SEC-ASAP, AMI System Security Requirements, Dec. 2008.
[2] Zigbee Alliance Document, "Zigbee Specification Pro/2007", 2007.
[3] No-Gil Myung, Young-Hyun Kim, Sang-Yeum Lee, "A study on AMI system of KEPCO," the journal of Korea information and communication society, vol. 35 No. 8, pp. 1251-1258, Aug. 2010.
[4] FIPS pub 197, "Advanced Encryption Stadard(AES)", NIST Springfield, Virginia, November 2001.
[5] IEEE Std 802.15.4, "Wireless Medium Access Control(MAC) and Physical Layer(PHY) Specifictions for Low-Rate Wireless Personal Area Networks (LR-WPANs)," 2003.
[6] ANSI X9.63-2001, "Public Key Cryptography for the Financial Services I
[7] FIPS pub 198, The Keyed-Hash Message Authentication Code(HMAC), NIST Springfield, Virginia, March 2002.
[8] 김태호, 김창훈, 권순학, 홍춘표, "타원곡선 키 교환 프로토콜 응용을 위한 마이크로소프트 COM 소프트웨어 모듈 구현", 한국통신학회 하계종합학술발표회, 2006.
[9] "암호 알고리즘 및 키길이 이용안내서", 한국인터넷진흥원, 2010.

저 자 소 개

이 명 훈

배재대학교 학사 (2001년)
배재대학교 석사 (2003년)
배재대학교 박사 (2006년)
퓨쳐시스템 MSS 사업부 과장 (2009~2011년)
롯데정보통신 (2011년 ~ 현재)

손 성 용 (孫 晟 榕)

Univ. of Michigan 박사 (2000년)
LG 소프트웨어 (1992~1995년)
포디홈네트 (2000~2004년)
아이크로스테크놀로지 (2004~2005년)
가천대학교 IT대학 에너지IT학과 조교수 (2006년 ~ 현재)