한국항행학회 논문지 제16권 제6호 2012년 12월 (JKONI 16(6): 1014-1023, Dec. 2012)

스마트 그리드에서의 AMI 보안에 관한연구

A Study on Security of AMI(Advanced Metering Infrastructure) in SMARTGRID

김연수*, 김진철**, 고종빈***, 손태식***

Yeoun-Soo Kim*, Jin-Cheol Kim**, Jong-Bin Ko***, and Tae-Shik Shon****

요 약

최근 스마트그리드가 발달함에 따라 AMI망에서의 보안은 전력정보통신에 많은 변화를 주었다. 본 연구는 사이버 공격으로부터 AMI시스템과 제품사이에 연결되어있는 각각의 구성품을 안전하게 보호하고, 댁내와 사용자에게 발생할 수 있는 2차 피해를 막기 위해 설계되었다. AMI망에서의 보안문제를 해결하기위해 공개된 암호키를 기반으로 보안알고리즘을 구성하고 키를 생성하여, 새로운 AMI설비가 보호될 수 있도록 제안하였다.

Abstract

Recently with improvement of SMART Grid, AMI network security has been affecting the environment for Electric information and communication. The system and communication protection consists of steps taken to protect the AMI components and the communication links between system components from cyber intrusions. The addition of two way communications between SUN and HAN introduces additional risk for unauthorized access to the AMI system. In this paper, we propose new AMI device authentication infrastructure, key establishment and security algorithm based on public key encryption to solve AMI network security problems.

Key words : AMI, SMART Grid, security

I. 서 론

현재까지 전력망은 폐쇄형, 단독망으로 운영관리되어 크게 문제가 되지 않았지만 IT가 결합됨에 따라 정보통신 네트워크 기기에서 발생하고 있는 보안문제가 나타날 수 있는 우려가 높다. 고객의 프라이버시노출, 정보도용, 사용요금 조작은 물론, 전력시스템의 마비까지 기존 전력망에서 나타나지 않았던 새로운 위협의 가능성이 도사리고 있으나, 현재까지 이에 대한 연구는 이루어지지 않고 있으며, 매체의 단점을 극복하기 위해 전송 에러율을 낮추고 전송 속도를 높이는데 초점을 두고 다양한 시도를 해왔으며 소기의 성과를 거두고 있다. 그러나 이에 비해 검침데이터를 원격으로 안전하게 전송하는 방법에 대한

* 한전KDN(주), 아주대 박사과정 (KEPCO KDN, Division of Information and Computer Engineering College of Information Technology, Ajou University)
** 한전KDN(주), 전력 IT 연구원 (KEPCO KDN)
*** 아주대학교 정보통신대학 정보컴퓨터공학부 (Division of Information and Computer Engineering College of Information Technology, Ajou University)
· 제1저자 (First Author) : 김연수 (Yeoun-Soo Kim, Tel. +82-10-5239-3772, email:yskim@kdn.com)
· 투고일자 : 2012년 1월 28일
· 심사(수정)일자 : 2012년 1월 26일 (수정일자 : 2012년 2월 23일)
· 게재일자 : 2012년 12월 30일

연구는 초기 단계로서 국내외 표준마저 없는 실정이다. 그나마 현재 시범적으로 적용되고 있는 원격검침 시스템은 암/복호화 알고리즘으로 DES(Data Encryption Standard)를 사용하거나 톤맵 (Tone Map)으로 암호화 알고리즘을 대체하고 있는 실정이다. 그러나 IBM에 의해 최초로 개발된 DES 알고리즘은 이미 1990년 초반 선형공격(LC : Linear Cryptanalysis)이나 차분공격(DC : Differential Cryptanalysis)에 안전하지 않은 것으로 증명되었다. 더구나 1999년 DES Challenge III에서는 Electronic Frontier Foundation의 Deep Crack이 22시간 15분 만에 키 전수조사 공격을 성공시켰다. 이러한 이유로 2000년 미국 NIST에서 새로운 블록암호 알고리즘을 공모하여 AES (Advanced Encryption Standard)를 선정하였다[1].

추가로 Tone Map은 어떠한 암호학적 기반을 이용한 것이 아니라 채널 설정의 임의성에 기반 한 것으로 암호학적 안전성을 보장할 수 없다. 현재의 상황을 종합하면 원격검침을 위한 암호 및 네트워크 보안 기술의 우 다른 유 무선 통신 기술에 비해 그 중요성에 대한 인식이 부족하고 기술 개발이 미흡하다. 이러한 보안 부분에 있어서의 문제점은 좁게는 정확한 검침값 전달 실패에서 넓게 는 국가 전력 기간망의 위협으로까지 이어질 수 있다. 설치가 간편하고 접근이 용이한 전력망에서의 원격검침에 있어 암호 및 보안기술은 전력 공급자의 입장에서 뿐만 아니라 개별 고객의 입장에서도 매우 중요한 요소이므로 원격검침에 필요한 기기의 생산에서 설치까지의 안전성을 보장하고, 개별 검침기의 인증 및 검침값의 위/변조를 막을 수 있는 암호 및 보안 기술의 개발이 시급하다. 따라서 본 논문에서는 AMI 기반 스마트그리드 보안 기술에 대한 제안 및 시험을 진행하였다.

Ⅱ. 관련 연구 및 취약점 분석

2-1 관련연구 동향

최근에 미국, 유럽 등 여러 나라에서 원격검침을 하기 위해 스마트 미터링 방식을 도입하고 있고, 검침값을 안전하고 공정하고 정확하게 검침하기 위해 검침 방법, 검침값 전송을 위한 네트워크 방법, 검침값에 대한 암호화 방법 등 여러 분야에 걸쳐 연구를 진행하고 있다. 대부분의 경우 보안 요구사항을 도출하는 단계에서 연구를 진행하고 있으며 보안요구 사항을 만족하는 프로토콜 규격에 관한 연구는 초기 상태이다. 스마트 미터링은 일반적으로 지능형 검침기를 댁내에 설치하고 검침 값을 원격으로 판독한 후 사용자에게 결과를 통보하는 구조로서 전기와 함께 가스, 수도 등이 통합되어 검침되는 형태를 취한다.

미국은 2008년 12월 AMI(Advanced Metering Infrastructure)에 대한 보안 요구사항을 제시하고, AMI 시스템 보안 요구사항 명세서를 발표하였다. 미국의 표준기술연구소(NIST)는 2009년 9월 스마트그리드의 사이버 보안을 위한 표준 6가지를 포함하고 있는 정보처리 상호운용 표준 프레임 워크를 발표하고, 스마트 그리드 사이버 보안 전략 및 요구사항 1차 초안을 발표하였고, 그 후 2010년 2월 2차 초안을 발표하였다. 보안 요구사항은 크게 비밀성, 무결성, 가용성을 만족시키는 것을 목적으로 하며, 기기 인증, 공개키 인증서 사용, 키 분배 방식 등 구체적인 상황에 필요한 보안 요구사항들이 기술되어 있다. UCAIug(Utility Communication Association International User Group)의 Open Smart Grid Subcommittee에서는 AMI-SEC Task Force를 신설하여 AMI에 대한 사이버 보안 연구를 진행 중이다. AMI-SEC Task Force에서는 AMI 보안 위협 모델을 연구하고, AMI 보안 요구사항을 작성하여 배포하였다[2].

EU 또한 스마트 그리드 표준화의 하위 작업의 하나로 스마트 그리드 보안에 대한 표준화를 포함하고 있다. 특히 2006년부터 표준화 움직임이 나타나기 시작하여 5개 연구부문에 19개의 세부과제로 구성된 스마트 그리드 유럽기술 플랫폼(SmartGrids: European Technology Platform) 프로젝트를 들 수 있으며, 이와는 별도로 EU는 Open Meter 프로젝트를 진행하고 있다. 2009년 7월 보안요구사항 규격서가 완료된 상태

이다. 보안요구사항은 크게 접근제어, 데이터 비밀성, 데이터 무결성과 자원 가용성으로 분류한 후 요구사항의 필요성 및 관련된 암호기술을 제시하고 있다. IEC는 스마트 그리드를 위한 국제 표준에서 2010년 6월 IEC 스마트 그리드 표준화 로드맵을 제시하고, 스마트 그리드 및 스마트 미터링에 필요한 각 세부 항목별로 현재 존재하고 있는 표준과 스마트 그리드에 접목시켰을 때 벌어지는 차이점과 보안해야할 요구사항들을 제시하고 있다[3].

2-2 AMI보안 취약점분석

AMI(Advanced Metering Infrastructure)는 에너지부하자원의 효율적인 관리와 에너지 소비의 절감을 위하여 에너지 공급자와 사용자간 양방향 정보교환을 위한 인프라로서 에너지사용정보를 측정·수집·저장·분석 하고, 이를 활용하기 위한 총체적인 시스템을 의미한다. 또한 협의의 의미로는 유틸리티 사업자가 에너지사용자의 에너지사용정보를 취득하여 과금을 하기 위한 인프라를 의미한다.

AMI는 악성코드 감염에 따른 분산 서비스 거부공격(DDoS, Distributed Denial of Service), 개인정보 노출, 과금정보 위/변조 등의 보안 위협이 존재한다. 방대한 전력사용정보가 수집되는 과금 및 포털, MDMS 등 AMI내 주요 서버 대상으로는 분산 서비스 거부공격 발생이 가능하다. 스마트 기기 펌웨어 업그레이드, 스마트 기기 자체 취약점, 물리적 공격 등 HAN(House Area Network) 내 주요기기 해킹을 통한 분산 서비스 거부공격, 개인정보 노출, 과금정보 조작 등 다양한 2차 공격 발생이 가능하다. 또한 통신 취약점을 이용한 과금정보 폭탄, 과금 전가에 따른 피해, 잘못된 수요반응 정보로 인해서 전력 계통이 불안정하게 되어 대규모 정전까지 발생할 수 있다.

특히 AMI에서 주요 기기인 스마트 미터를 대상으로 해킹을 통한 오작동 유도 및 다양한 2차 공격 발생이 가능하다. 예를 들어, 스마트 미터의 F/W 업그레이드 시 해커에 의한 악성코드가 삽입되어 디지털 기기를 파괴하는 PDoS(Permanent DoS) 공격 발생이 가능하다. PDoS 공격은 내장형 소프트웨어로 백신 프로그램 등을 통해 탐지 및 치료, 공격자 추격이 매우 어렵다. 또한, 스마트 미터의 자체 취약점을 이용한 악성코드 감염을 유도할 수 있으며, 물리적 해체/교체를 통해 악성코드를 감염시킬 수도 있다[4].

2009년 7월30일 Black Hat 2009에서는 스마트 미터에서의 웜 감염 및 전파 시연이 있었다. 시뮬레이션 결과 24시간 동안 특정 스마트 미터 제품을 대상으로 15,000~22,000대의 원격제어 권한 획득이 가능하였고, 웜에 감염된 스마트 미터에 대한 제어가 가능함을 보임으로써 스마트그리드 사이버 공격이 현실 속에 존재함을 보였다.

2009년 3월 CNN에서는 스마트 미터를 통하여 전력네트워크에 침투할 수 있는 가능성을 제기 하였고, 2010년 3월 31일 AP통신에서는 전기 배선 조작을 통하여 타인의 전기 요금을 대폭 올리거나 타인의 전기 사용을 원격지에서 제어할 수 있는 스마트 미터 보안 위협에 대해서 발표했다[5].

2-3 키 관리 설계 고려사항

2-3-1 General Design Consideration

○ 암호기술의 선택 및 사용 : FIPS 승인 및 NIST 권고 암호모듈 사용

○ Entropy

- 스마트그리드 장비 배포 전 DRBG (Deterministic Random Bit generator) 기반 씨앗키 주입
- 장비에 기 제공된 키를 이용해 키 유도 KDF(Key Derivation Function) 가능

○ 암호 모듈 고도화 가능성

- 스마트그리드 장비는 평균적으로 20년마다 종종 교체가 요구되고, 이는 IT와 통신시스템의 발전보다 더 오래됨
- 장비의 교체는 다른 시스템 교체보다 값비싸고 시간소요가 많이됨

○ 난수 생성

- 스마트그리드 장비는 Entropy의 Source(잡음원)

제공에 제약적임

- 난수 생성을 위한 권위 있는 표준 : NIST SP 800-90, Recommendation for Random Number Generation Using DRBG (Deterministic Random Bit Generators)

○ Local Autonomy of Operation

- 다른 시스템과의 접속이 불안정하거나 불가할 때도 인증/인가 기능이 제공되어야 함
- 인증/인가를 위한 정보(검증정보)를 운영 도메인별 자체적으로 관리할 수 있도록 함

○ 가용성

- 키 또는 인증서 유효기간 만료로 인한 서비스 접속이 불가해서는 안됨

○ 알고리즘 & 키 길이

- NIST SP 800-57, Recommendation for Key Management 권고

○ Physical Security Enviroment

- 물리적 보안을위한 Crypto module을 이용
  예) TRSM, HSM, SAM cards

2-3-2 Key Management for Smart Grid - PKI

○ 적정한 인증서 폐지와 만료일

- 스마트그리드 기기에 대한 CRL 크기는 기하급수적 증가 위험이 존재
- 인증서 유효기간이 길수록 CRL의 크기는 증가
- 스마트그리드 장비의 배포 시 수년간(대략 10~15년) 사용을 고려하여 유효기간을 선정해야 함(장비의 교체가 자주 발생되면 안됨)
- 현 인증서가 만료되기 충분한 시일 전에 새로운 인증서로 교체되어야 함
- CRL은 기기의 네트워크 위치, 기기 유형, 발급년도 등 특정기준에 기반하여 CRL을 분할되어야 함

○ High Availability and Interoperability Issues of Certificates and CRLs

- 인증서 검증 시점에 검증서버에 접근하지 못할 경우 가용성에 치명적
- 디바이스에서 분할 CRL 캐시 관리 또는 OCSP stapling 기법 고려

○ 인증서 상태 관련 고려사항

- 제조사가 발급한 인증서에는 제조사 정보, 모델, 기기 일련번호를 담음
- 인증서에는 시스템에 사용되는 인가정보를 포함할 수 있음
  예) 전력회사 X에 의한 소유, 설치된 변전소 Y, 인가 받은 애플리케이션 Z 등
- 신원확인, 인가정보 검증 외 기기의 펌웨어 정보가 위/변조 되지 않았음을 검증할 수 있어야 함

2-3-3 Smart Grid Architecture

스마트 그리드를 위한 스마트 미터의 통합은 [그림1]과 같다.

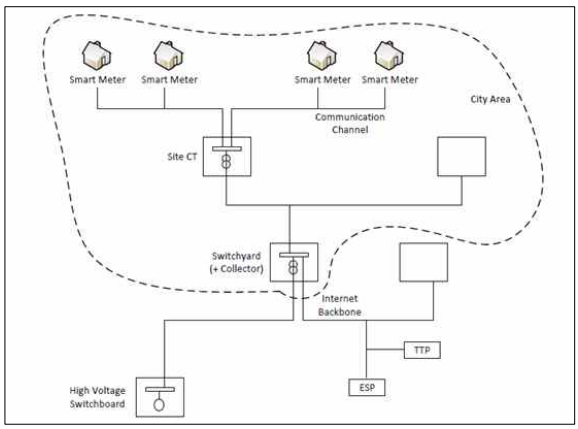


그림 1. 스마트그리드 구성도
Fig.1. Smart Grid Architecture

○ ESP(Energy Service Provider)

- 고객은 자유롭게 ESP를 선택

○ CT(Current transformer)

- 수십 또는 수백 세대를 공급
- 가정은 성형 토폴로지 네트워크의 사이트 CT에 연결

III. 제안 AMI 보안 시스템

3-1 보안인증체계 및 시스템구성도

3-1-1 시스템 구성도

보안인증체계는 그림과 같이 CA, RA 기능을 가진 PKI 인증센터와 인증서 중계모듈과 주입모듈이 있는 기기제조사, 그리고 보안인증모듈을 가지고 있는 서비스도메인으로 구성되어 있으며 [그림2]와 같다.

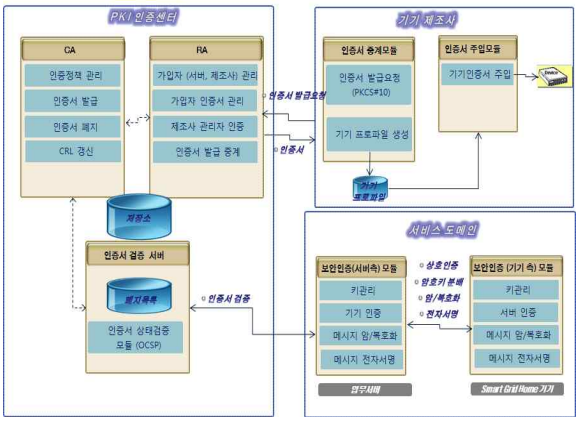


그림2. 시스템 구성도
Fig.2. System Architecture

3-1-2 각 구성요소별 모듈 구조도

① CA(인증서발급) 모듈

CA관리모듈은 관리서비스, CRL일괄갱신서비스, 인증서 일괄발급서비스를 수행하는 주요기능이 있으며, 각각의 기능을 살펴보면 다음과 같다.

○ 관리서비스 : CA관리자 또는 RA간 인터페이스를 통한 다음기능제공
- 인증서 정책관리 : 유형별 인증정책 & CRL 정책 등록기능
- 가입자 관리 : 가입자(제조사, 서버)등록 및 발급인가
- 인증서 폐지 : 인증서(제조사,서버,기기)폐지 및 실시간 CRL갱신

○ CRL일괄갱신 서비스 : 주기적으로 Invoke되어 모든 인증서에 대한 CRL의 갱신 기능을 제공하며, 폐지된 모든 인증서에 대한 CRL Update를 한다

○ 인증서 일괄발급 서비스 : 주기적으로 Invoke되어 기기인증서 요청 목록을 확인후 해당 인증서를 발급하며, PKCS#10 CertificateRequest에서 subject필드와 공개키를 추출하여 기기인증서를 발급하며 [그림3]은 CA모듈을 나타낸 것이다.

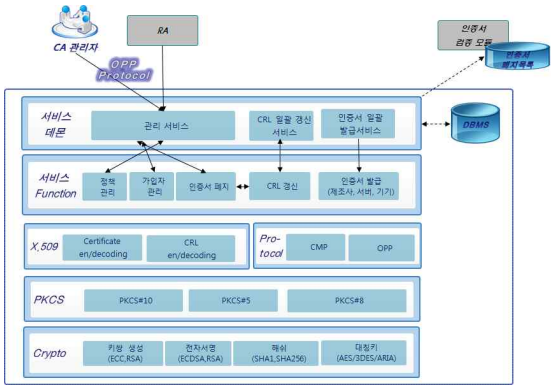


그림3. CA(인증서 발급) 모듈
Fig.3. CA Module

② RA(등록관리) 모듈

RA등록관리 모듈은 인증서 발급요청,인증서 획득, 가입자관리하는 주요기능이 있으며, 이들의 역할을 살펴보면 다음과 같다.

○ 인증서 발급요청 : 제조사 담당자가 중계모듈을 통해 생성된 PKCS#10 CertificateRequest 목록을 구성하여 인증서 발급요청 메시지를 업로드 하며, 요청메세지 검증 후 “인증서 요청목록” 저장소에 저장

○ 인증서 획득 : 제조사 담당자가 인증서를 조회 후 다운로드 한다

○ 가입자관리 : 제조사 & 업무서버의 등록/수정/삭제등 가입 관리와 제조사 & 업무서버의인증서 발급인가/폐지처리를 수행하며, [그림4]은 RA모듈을 나타낸 것이다.

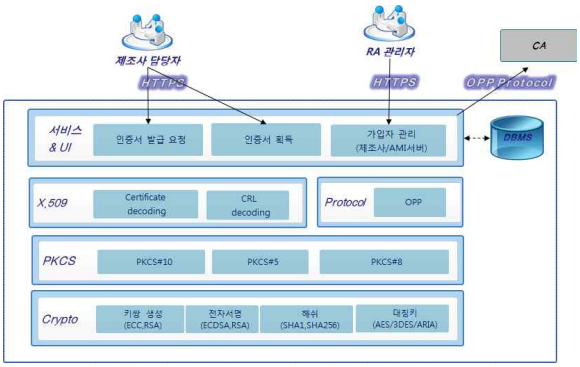


그림4. RA(등록관리) 모듈
Fig.4. RA Module

③ 중계 및 인증서 주입모듈

제조사담당자는 인증서 요청양식을 생성하고 기기 프로파일을 생성하는 중계모듈과 기기인증서를 주입하는 인증서 주입모듈이 있으며, [그림5]은 중계 및 인증서 주입모듈을 나타낸 것이다.

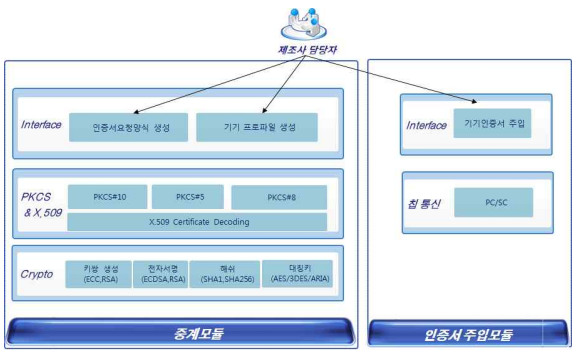


그림5. 중계 및 인증서 주입모듈
Fig.5. Relay and Certificate Injection Module

④ 보안인증 모듈(기기 측)

기기 측 보안인증모듈은 AMI 기기 firmware와 연동을 위한 API 형태로서 Cryto 칩과 연계하여 암호연산을 수행하기 위해 인증서 요청메세지와 인증응답을 생성하고 AMI 메시지를 암/복호화하며, AMI command를 인증하며, 아래 [그림6]은 보안인증 모듈(기기 측)을 나타낸 것이다.

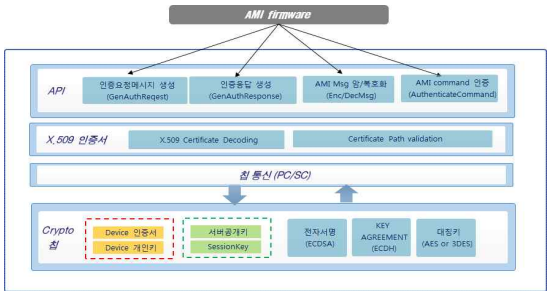


그림6. 보안인증 모듈(기기 측)
Fig.6. Security Certificate Module(Device)

⑤ 보안인증 모듈(업무서버 측)

업무서버 측 보안인증 모듈은 인증서요청서와 응답메세지를 검증하고,challenge를 생성하고 AMI Msg를 암/복호화 하며, Secure AMI Command를 생성하는 기능이 있으며, [그림7]은 보안인증 모듈(업무서버 측)을 나타낸 것이다.

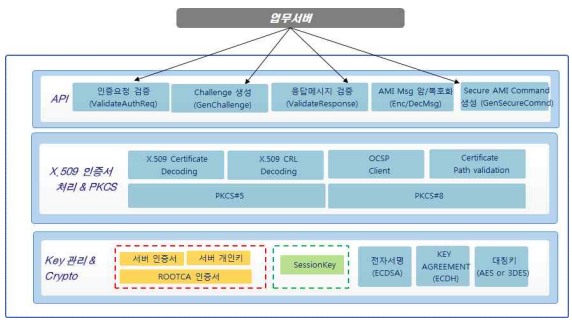


그림7. 보안인증 모듈(업무서버 측)
Fig.6. Security Certificate Module(Server)

3-2 제안모델 기기인증서 및 키교환 시나리오

3-2-1 기기인증서 발급/주입 시나리오

제조사는 기기프로파일 생성프로세스를 통하여 AMI기기의 인증서를 발급받고 인증서주입 프로세스를 통하여 주입모듈은 AMI기기에 인증서를 주입한다. 이때 제조사의 보안정책에 따라서 기기에서 기기의 개인키와 공개키를 생성하는 방법과 중계모듈에서 기기의 개인키와 공개키를 생성하는 방법이 가능하다 이에 대한 시나리오는 [그림8]과 같다.

그림8. AMI기기인증서발급/주입 시나리오

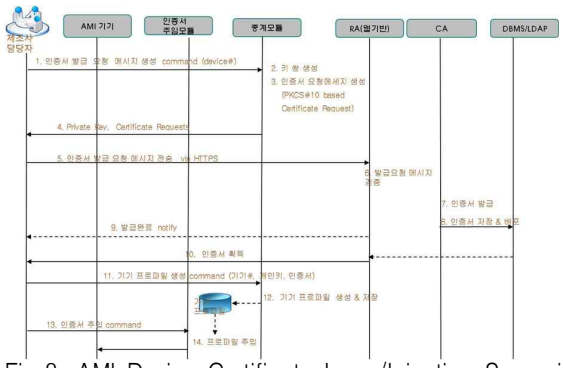


Fig.8. AMI Device Certificate Issue/Injection Scenario

3-2-2 키교환 시나리오

AMI기기는 위에서 언급한 인증서 발급 및 주입시나리오에 따라서 AMI기기에 인증서를 주입하고,[그림9]와 같이 주입된 인증서를 기반으로 AMI기기는 AMI서버에 기기인증을 요청하고, AMI서버는 인증서의 유효성을 검증하고 세션키를 생성하고 ECDH방식으로 세션키를 교환한다.

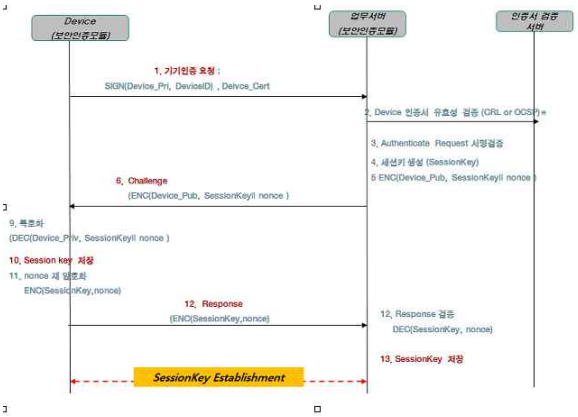


그림9. 키교환시나리오

Fig.9. Key Exchange Scenario

3-2-3 데이터교환 시나리오

기기 인증 절차에 의해서 DCU와 AMI 기기는 세션 키를 교환하고, [그림10]과 같이 LASP 데이터 암호화 절차에 의해서 LP 데이터, 이벤트 데이터, 전월 데이터 등의 데이터를 암호화하여 교환한다.

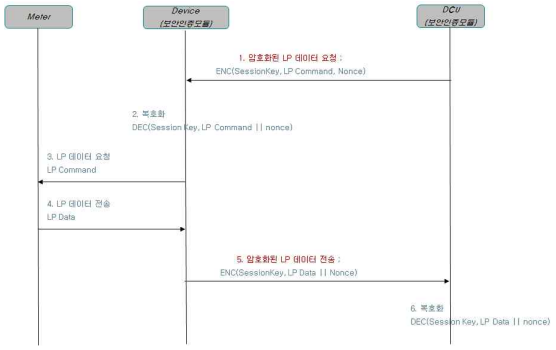


그림10. 데이터교환 시나리오

Fig.10. Data Exchange Scenario

3-3 시험환경 및 방법

3-3-1 시험환경

실제시험은 [그림11]과 같이 AMI지능형 집중기에서 무선모뎀이 장착된 스마트 미터까지의 데이터를 측정하여 비교분석하였으며, 제안한 알고리즘의 성능평가를 위한 실험항목은 다음과 같다. 첫째, 실험 시스템에 제안한 원격검침 프로파일을 적용한 결과를 수행하였으며. 둘째. 제안한 키교환 및 보안 알고리즘에 대해서 변화에 따른 성능 비교를 하였다.

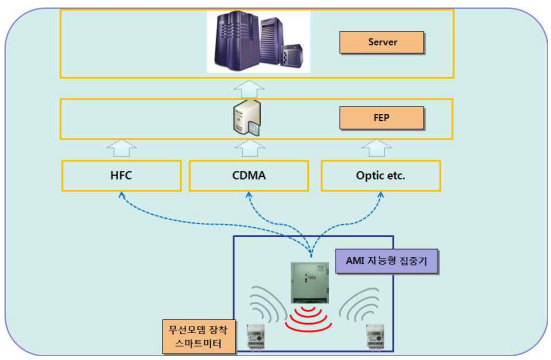


그림11. 시험구성도

Fig.11. Testing Architecture

3-3-2 시험방법

○ 네트워크 조인속도 비교를 위해 Packet analyzer를 이용하여 각각의 조인시간을 측정

○ 데이터 응답속도 비교

① PC와 코디네이터를 연결(시리얼)

② PC시리얼 어플에서 LP데이터, 이력데이터, 전원 데이터요청을 주기적(10초 간격)으로 전송

③ PC에서 코디네이터로 전송한 시간값 기록

④ 검침기에서 각 요청에 대해 응답된 값이 수신된 시간을 기록

⑤ 3번과 4번 값의 차이를 1000회 반복하여 평균값을 검출

3-4 시험결과

3-4-1 검침프로파일

검침프로 파일을 적용한 실험의 성능평가는 [표1]과 같다

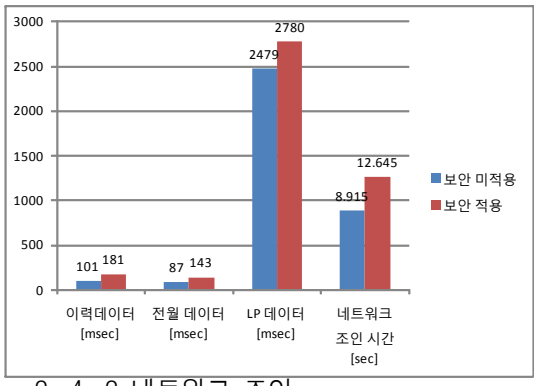
표1. 검침 프로파일 성능평가 결과
Table 1. Meter Profile Testing Result

시 험 항 목	에러율	시 험 항 목	에러율
계량기 ID 읽기	0%	검침일 설정	0%
계량기 날짜 설정	0%	전월 데이터 읽기	0%
계량기 시간 설정	0%	검침 데이터 읽기	0%
계량기 시간 읽기	0%	Load Profile 데이터 읽기	0%
검침일 읽기	0%		

3-4-2 보안적용/미적용 데이터 속도

각각의 검침데이터에 대해 보안 미적용시와 적용할 때 측정한 결과는 [표2]와 같다.

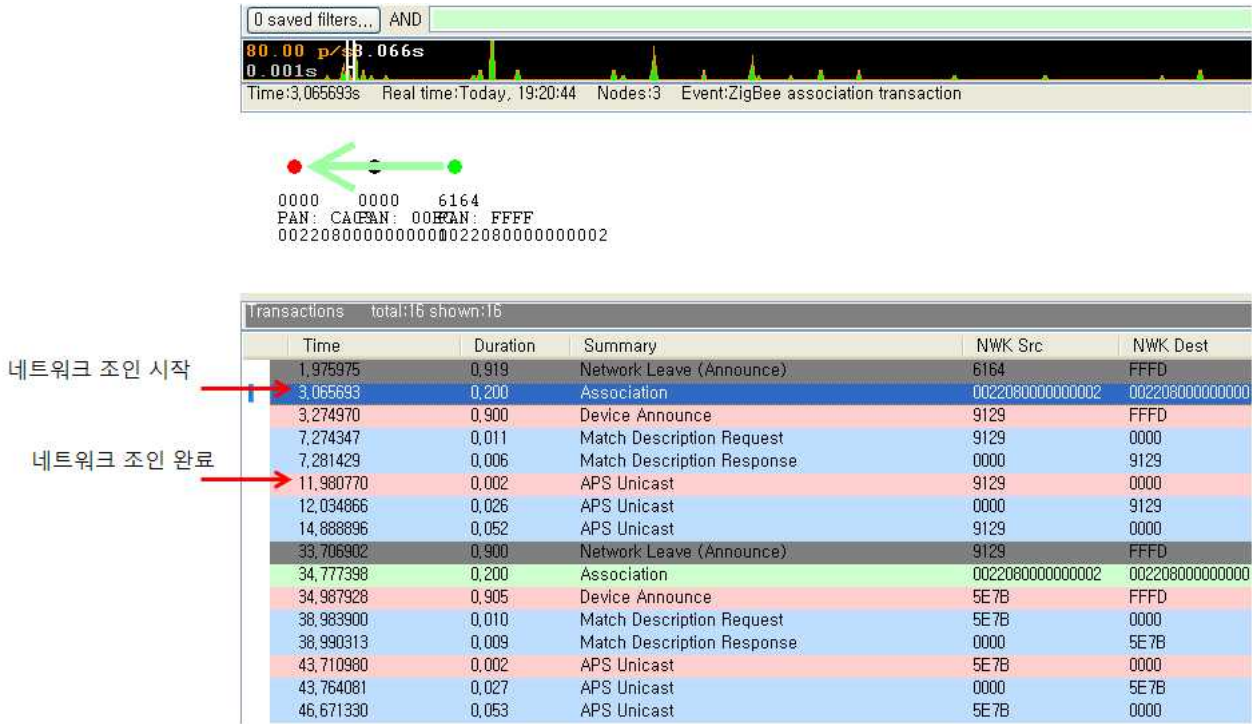
표2. 보안적용/미적용 속도비교
Table 2. Security Apply/Non apply Result



3-4-3 네트워크 조인

네트워크 조인 시 측정된 보안 미적용 시 걸린 시간은 8.915Sec이고, 보안 적용 시 걸린 시간은 12.645Sec 이며 [그림11]은 이에 대한 결과를 보여주고 있다.

① 보안미적용 조인데이터



② 보안적용 조인데이터

IV. 결 론

스마트그리드 기반의 AMI 시스템에서 통신의 신뢰성 향상과 안전한 통신을 위한 표준화 개발을 위한 원천기술로 사용될 수 있다. 좀 더 자세히 살펴보면 본 연구는 스마트그리드망을 기반으로 한 원격검침 및 부가사업이 본격화되어 이에 따른 보안문제 부재에 따른 호환성 문제를 해결하고 시스템의 안전성 보장을 위해 필수적인 암호학적 요구사항을 만족하는 키관리 방법, 검침값의 안전한 전송을 위한 키공유 방법, 검침값 전송 방법을 제공한다. 그러므로 IRM과 검침기기 및 기타설비가 공격자의 다양한 공격에 노출된 상황에서도 안전하게 데이타를 서버까지 전달되도록 보장한다.

AMI는 스마트그리드의 핵심 인프라로서 다양한 이해당사자가 참여하게 되어 전력망의 외부연계에 따른 새로운 사이버 공격 취약점 생성되고, AMI 기기는 낮은 연산 능력과 통신 대역폭, 적은 메모리 등의 한계로 기존 보안 기술의 적용이 어렵다.

본 논문에서는 AMI보안부문에 대한 국제표준 및 기술동향에 대한 분석을 하고, AMI 보안을 위한 PKI(Public Key Infrastructure) 기반의 기기 인증체계와 AMI기기간 상호 인증을 하고 키 교환을 통하여 데이터를 암호화하여 전송할 수 있는 보안 프로토콜을 제안 및 시험하여 그 적용 가능성을 검증하였다. 향후에는 보다 AMI 네트워크 환경에 적합한 스마트그리드 보안 기술에 대한 연구가 필요하다.

Reference

[1] “Smart Grid cyber Security Strategy and Requirements,” *NIST*, 2009.01.

[2] “AMI System Security Requirements V1.01,” *UCAIUG,* 2008.12.

[3] “State-of-the-art technologies & protocols Version:1.0,” *OPEN Meter,* 2009.06.

[4] Ralph Mackiewicz, "IEC61850 & ICCP-TASE.2 Technical Overview", *SISCO*

[5] Chartwell, "The Chartwell AMR Report 2003 8th Edition", October 2003.

김 연 수

2012.12 한전KDN 근무,
아주대학교 박사과정

김 진 철

2006 : 광운대학교 전자통신공학 (박사)
1996 ~ 현재: 한전KDN(주) 전력 IT연구원 차장

고 종 빈

2006.02 : 아주대학교 정보 및 컴퓨터 공학부 졸업
2008.02 : 아주대학교 컴퓨터 공학 석사
2008.02～현재 : 아주대학교 컴퓨터공학과 박사과정

손 태 식

2000.02 : 아주대학교 정보 및 컴퓨터 공학부 졸업
2002.02 : 아주대학교 컴퓨터 공학 석사
2005.08 : 고려대학교 정보보호대학원 박사
2004.02～2005.02 : University of Minnesota, Research Scholar
2005.08～2011.02 : 삼성전자 DMC 연구소 책임연구원
2011.02～현재 : 아주대학교 정보통신공학부 조교수