AMI 환경에서의 안전한 디바이스 관리를 위한 그룹키 관리 메커니즘

Group Key Management Mechanism for Secure Device in AMI Environment

장유종*, 곽 진**

Yu-Jong Jang*, Jin Kwak**

요 약

스마트그리드 시스템 보안에 대한 관심이 증가하면서 스마트그리스 시스템 내부 통신보안에 대한 연구가 활발히 진행되고 있다. 이러한 연구중에서도 스마트그리드 키관리 시스템에 대한 연구가 활발히 진행되고 있으나 지금까지 제안된 키관리 시스템은 스마트그리드 환경 상에서의 가용성 및 사용되는 디바이스의 정보보안에 대하여 취약하다. 본 논문에서는 AMI 환경에서 공개키 암호알고리즘과 해쉬함수를 사용하여, 사용되는 키의 수를 줄이고 디바이스의 보안성을 향상시키는 스마트그리드 환경에 적합한 키관리 메커니즘을 제안한다.

Abstract

Many researches have proposed key management schemes for Smartgrid System. However, previous studies lack the proper considerations for availability and device security. In this paper, we build up cryptographic security improvement for robust Smartgrid Systems. In addition, we propose a public-key management and hash fuction architecture for robust Smartgrid Systems which supports reduces the number of key and Secure Device in AMI network erviroments.

Key words : Smartgrid, AMI, Group Key, Hash

I. 서 론

현대 사회에서는 산업의 발달 및 인구 증가로 인해 에너지에 대한 효율적 관리 요구가 증가하고 있다. 이에 대한 대비책으로 에너지 사용절감 및 관리에 관한 저탄소 녹색 성장 기술이 차세대 기술로 주목을 받고 있다. 특히 스마트그리드는 에너지를 절약하고 효율적으로 소비하여 환경오염 및 에너지 낭비를 최소화 시키는 대표적인 기술로 많은 연구가 진행되고 있다. 국내에서는 점차적으로 전력 환경을 지능화시켜 지능형 전력 서비스(Smart Electricity Service)를 확장해 나감으로써 세계 최초의 국가단위 스마트그리드 환경 구축을 추진중에 있다[1].

이러한 스마트그리드 서비스를 제공하기 위한 핵심 기반 시설인 AMI(Advanced Metering Infrastructure)의 통신 구조는 HAN(Home Are Network)의 디바이스

* 순천향대학교 정보보호학과 정보보호응용및보증연구실(ISAA Lab, Department of Information security Engineering, Soonchunhyang University)
** 순천향대학교 정보보호학과(Department of Information security Engineering, Soonchunhyang University)
· 제1저자 (First Author) : 장유종
· 투고일자 : 2012년 6월 15일
· 심사(수정)일자 : 2012년 6월 15일 (수정일자 : 2012년 8월 16일)
· 게재일자 : 2012년 8월 30일

-스마트미터간 지능형 장치와 WAN(Wide Area Network)환경에서 스마트미터-DCU-AMI서버간의 지능형 장치들로 구성된다. 이러한 AMI에서 사용되는 통신 구조는 기존 네트워크 환경과 동일하므로 기존에 가지는 보안위협들이 스마트그리드 환경에서도 동일한 보안위협으로 작용할 수 있다. 이러한 보안위협 중 하나로 디바이스와 디바이스의 정보를 관리하는 스마트미터간의 통신이 제3자에게 노출된다면 개인정보 노출 및 금전적인 피해를 일으킬 수 있다[2][3].

따라서 본 논문에서는 보다 효율적이고 안전한 스마트그리드 서비스를 위하여 AMI환경에서의 보안 취약점을 분석하고 스마트그리드의 통신 환경에 적용 가능한 그룹키 관리 기법을 제안한다. 먼저 2장에서는 스마트그리드 통신환경의 구조와 키관리 프로토콜을 분석한다. 다음으로 3장에서는 스마트그리드 통신환경에 적용 가능한 그룹키 관리 기법을 제안하고 4장에서는 제안하는 프로토콜의 안전성과 효율성을 분석한다. 마지막으로 5장에서 결론을 맺는다.

Ⅱ. 관련연구

2-1 AMI 통신 환경

AMI 통신 환경은 스마트그리드를 구성하는 중요한 인프라중 하나로 홈 네트워크의 디바이스-스마트미터-전력제어시스템까지의 통신 구조를 말한다. 이러한 AMI 통신 구조는 그림 1과 같이 구성된다. AMI의 통신 인프라는 기존 네트워크 환경인 이더넷과 같은 유·무선 통신 기술과 기존 전력 통신망으로 사용되는 PLC(PowerLine Communication)등과 같은 통신 기술을 사용하여 구성이 가능하다. 이러한 네트워크가 구성되는 스마트그리드의 소비자 영역부터 전력 제공자간의 통신망 구조를 살펴보면 가정네트워크인 HAN(Homw Area Network), 스마트그리드환경에서 전력이 전송되는 필드영역인 FAN(Field Area Network), 스마트그리드 서비스의 백홀 네트워크인 WAN(Wide Area Network)로 분류되며 그림 1과 같이 나타낼 수 있다[2].

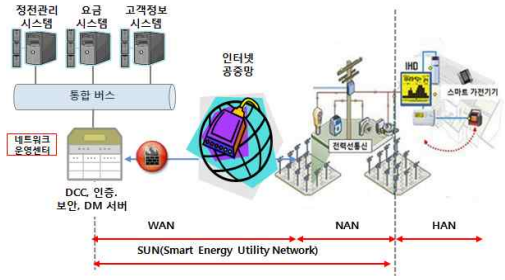

그림 1. AMI 통신 인프라 구조
Fig 1. AMI Communication Infrastructure

2-2 SCADA 시스템 키관리 기법

2-2-1 SKMA [4] (Secure Key-Management Architecture)

SKMA는 Dawson 등이 제안한 프로토콜로 스마트그리드 환경중 SCADA 시스템을 위한 키 관리 방식이다. SKMA는 대칭키 암호 알고리즘으로만 이루어져 공개키 암호 알고리즘을 사용하는 프로토콜에 비하여 계산 복잡성에 대한 효율성을 고려한 프로토콜이다. SKMA에서 사용되어지는 키 관리 기술은 다음과 같다.

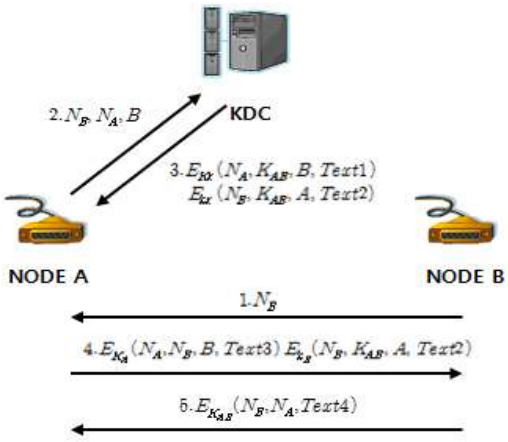

그림 2. SKMA 키 관리 방식
Fig 2. Key establishment protocol in SKMA

- Long term node-KDC key :
이 키는 node와 KDC사이에 공유되는 키로 통신을 위해 키를 설정할 때 사용
- Long term node-node key :

노드와 노드사이에 공유되는 키

- Session Key :

메시지를 암호화 하는데 사용되는 키

- Node-KDC Key :

이 키는 수동적으로 설치되며, node와 node사이의 키를 생성할 때 사용

Node-KDC Key는 시스템에 노드가 배포되기 전에 설치된다. 또한 새로운 노드가 추가될 때 node-node 키가 그림 2와 같은 과정을 통해서 교환된다. 데이터를 암호화하는데 사용되는 세션키는 3자간 키 확립 프로토콜로 얻은 node-node키와, 타임스탬프(세션의 유지기간에 기반을 둔)값을 해쉬하여 생성한다.

2-2-2 LKH 프로토콜 [5]

키 관리 구조 중 그룹키 관리 구조는 그룹의 구성원에 대하여 가입 및 탈퇴와 같은 변화가 생길때마다 키를 갱신해야한다. 이러한 과정을 효율적으로 처리하기 위하여 다양한 연구가 이루어지고 있다. 이중 가장 널리 사용되는 방법 중 하나가 LKH 기법이다. LKH 프로토콜은 각각의 노드가 배포되기전 노드에서부터 root가 있는 곳까지의 경로 상에 있는 키를 저장한다. 초기 배포가 끝난 후 새로운 노드가 추가된다면 키 업데이트를 통해 키를 분배 한다. 예를 들어 그림 3에서처럼 N1 노드가 추가되면 KDC는 기존의 키 K0,K11,K21을 업데이트 하여 새로운 키 K'0,K'11, K'21을 생성한다.

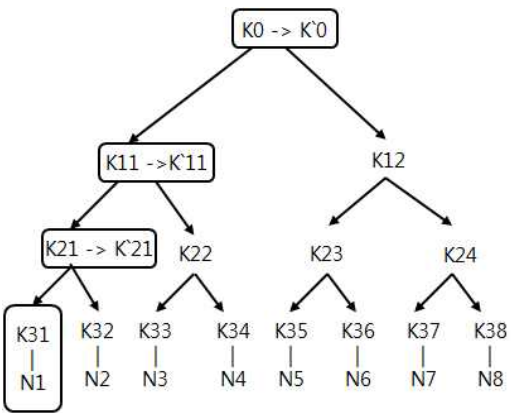

그림 3. LKH 새로운 노드의 가입
Fig 3. Key update in LKH

2-2-3 기존 프로토콜의 취약점 분석

기존에 연구되고 있는 스마트그리드 환경에서의 키 관리 시스템의 경우 송/배전시 사용되는 SCADA (Superisory Control And Data Acquisition) 시스템에서의 키 관리 기술이 일반적이다[7]. 따라서 AMI 시스템에서 사용되기에는 적합하지가 않다. 또한 다양한 취약점이 발생하게 된다.

- 디바이스의 접근제어 및 무결성 : 기존에 연구되고 있는 LKH, SKMA 같은 프로토콜에서는 스마트미터의 하위단인 디바이스에 관해서는 적용시킬 수 없다. 하지만 디바이스 정보 또한 매우 민감한 정보이며 이는 스마트그리드 통신환경에서 보호되어야할 정보이다. 또한 HAN 네트워크상에서 다양한 디바이스에 대하여 스마트미터에 접근을 제어해야 한다.

- 키 관리의 효율성 : LKH, SKMA 프로토콜을 AMI 환경에 적용을 시키면 AMI 환경에 전체적으로 적용되는 것이 아닌 스마트미터-RTU-서버 이렇게 3단계에서 적용을 시킬 수 있게 된다. 이렇게 된다면 디바이스-스마트미터에 대한 키관리가 한번더 이루어 져야 하기 때문에 프로토콜이 한번더 사용되어야 한다.

2-3 AMI 시스템 상에서의 키관리 보안요구사항

- 데이터 기밀성 : 스마트그리드 통신 환경에서는 과금이나 제어 메시지등과 같은 민감한 정보들이 네트워크를 통해 전송되므로 비 인가된 제 3자가 데이터의 내용을 알 수 없도록 암호화를 통해 송/수신 되는 정보를 보호해야 한다[8].

- 데이터 무결성 : 스마트그리드 환경에서 전송되는 미터 사용량, 요금 관련 정보, 제어 메시지 등이 불법적인 접근에 의해 위·변조 되지 않도록 보장해야 한다[8].

- 상호인증 : 스마트그리드 환경에서 공격자가 정상적인 사용자로 위장함으로써 사용자 측에서 원활한 서비스 제공을 받지 못하는 등의 위협이 발생할 수 있다. 이러한 위협에 대비하여 상호인증 제공되어야 한다[8].

- 디바이스의 무결성 보호 : 스마트미터에 연결되

어 소비전력을 전송하는 디바이스의 경우. 보안 고려하지 않고 사용되고 있는 디바이스들의 경우가 많다. 스마트그리드 서비스가 활성화 된다면 디바이스에 대한 무결성 검증이 보장되지 않는 경우. 공격자가 디바이스를 통하여 통신 네트워크를 오염시키거나 스마트그리드 서비스의 가용성을 손상시킬 수 있다. 따라서 디바이스에 대한 무결성 검증이 요구된다.

- 시스템 가용성 : 스마트그리드 환경에서는 안정적이고 지속적으로 실시간 양방향 통신을 제공하기 위해 디바이스, 시스템 및 네트워크의 가용성이 보장되어야한다.

Ⅲ. 제안하는 키관리 기법

본 장에서는 스마트그리드 환경에서 효율적으로 디바이스들을 관리하기 위해 필요한 그룹키 관리 기법을 제안한다. 제안하는 그룹키 관리 기법은 새로운 디바이스를 스마트미터에 등록하여 사용하는 프로토콜(그룹 B)과 스마트미터를 AMI Server에 등록 및 사용하는 프로토콜(그룹 A)을 두 개의 구룹으로 관리하는 키 관리 기법으로 구성된다.

기본구조는 LKH 키관리 구조를 따른다. 스마트미터에 등록 되어 있는 디바이스가 새롭게 등록되거나 삭제 된다면 해당하는 스마트미터의 그룹 키를 갱신하고 이렇게 갱신된 새로운 그룹키를 통해서 디바이스간 통신을 하고 AMI 서버-스마트미터의 그룹키는 유지된다.

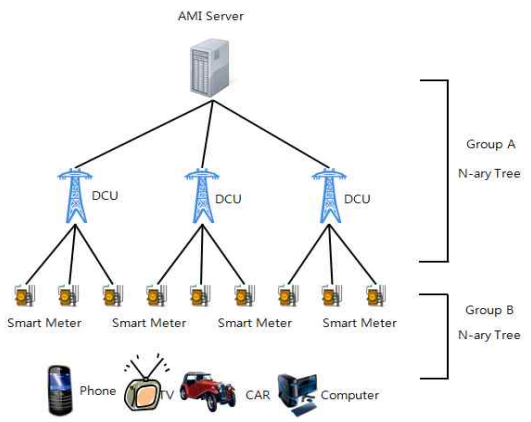

그림 4. 그룹 키 관리 구조
Fig 4. Group Key Management architecture

그룹키 키 관리 방안으로는 그림 5와 같이 스마트미터와 디바이스단 사이에서 그룹키 설정을 하고 설정된 그룹키를 사용하여 스마트미터-디바이스의 통신이 이루어진다. 또한 이렇게 설정된 그룹키 B를 기반으로 DCU에서 그룹키 A를 설정하여 공개키 암호를 통하여 스마트미터와 AMI 서버에 그룹키 A를 비밀통신으로 분배 후 그룹키 A를 통하여 스마트미터-AMI서버의 비밀통신이 이루어진다.

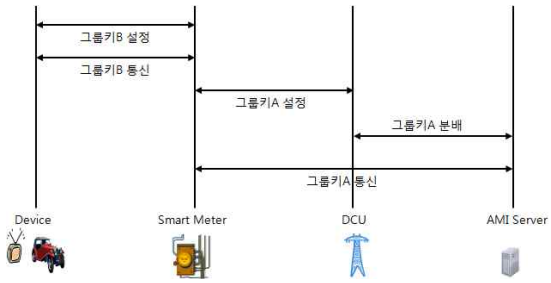

그림 5. 그룹 키 관리 방법
Fig 5. Group Key Management Methods

3-1 표기법

제안하는 그룹키 관리 기법에서 사용하는 표기와 의미는 표 1과 같다.

표 1. 표기법
Table 1. Notation

표기	의미
SM	스마트미터
$Device$	전력 소비 디바이스
$AMI\ Server$	AMI Server
$H(\cdot)$	해쉬함수
$\oplus$	XOR 연산
$E(\cdot)$	대칭
GA_n	그룹 A의 현재 키
GB_n	그룹 B의 현재 키
GA_{n+1}	갱신된 그룹 A의 그룹키
GB_{n+1}	갱신된 그룹 B의 그룹키

3-2 키 관리 방법

3-2-1 가입 프로토콜

가입 프로토콜은 새로운 디바이스를 스마트미터에 등록하는 과정과 새로운 전력사용자를 위한 스마트미터를 AMI 서버에 등록하는 것으로 구분되어 진행되게 된다.

3-2-1-1 디바이스 가입 프로토콜

디바이스 가입 프로토콜은 새로운 디바이스를 스마트미터에 등록하기 위한 프로토콜이며 절차는 다음과 같다.

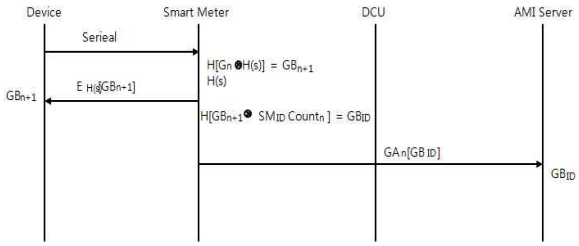

그림 6. 디바이스 - 스마트미터 간 가입 처리 과정
Fig 6. Device - Smartmeter join protocol

[단계 1] 디바이스 : 새로운 디바이스에 등록되어 있는 Serieal을 파악한 후 스마트미터에 입력 한다.

[단계 2] 스마트미터 : 스마트미터는 입력된 Serieal을 해쉬 한 값과 기존의 디바이스-스마트미터간 그룹키 G_n을 XOR 연산한 값을 해쉬 하여 새로운 그룹키 G_{n+1}을 생성한다.

[단계 3] 스마트미터 : 스마트미터는 새롭게 생성된 그룹키(G_{n+1})를 Serieal의 해쉬 값인 $h(S)$ 값을 키 값으로 암호화하여 디바이스에 전송한다.

[단계 4] 디바이스 : 전송받은 값을 Serieal을 해쉬하여 $H(S)$ 생성 복호하여 그룹키 G_{n+1}을 저장한다.

[단계 5] 스마트미터 : 새롭게 갱신된 그룹키 GB_{n+1}와 스마트미터의 ID의 카운터 값과 XOR연산, 해쉬하여 그룹키ID GB_{ID}를 생성한다.

[단계 6] 스마트미터 : 생성된 그룹키ID GB_{ID}를 그룹키 GA_n을 사용 하여 암호화 한 후 전송한다.

[단계 7] AMI 서버 : 전송된 그룹키 GB_{ID} 를 저장한다.

3-2-1-2 스마트미터 가입 프로토콜

스마트미터 가입 프로토콜은 AMI 환경에 스마트미터를 등록하기 위한 프로토콜이며 절차는 다음과 같다.

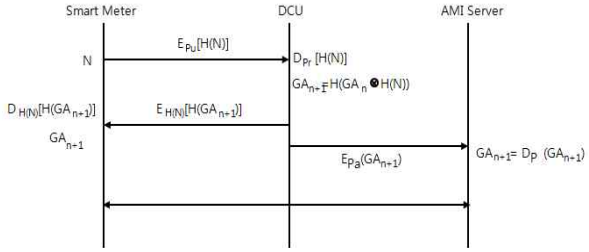

그림 7. 스마트미터 - AMI 서버 간 가입 처리 과정
Fig 7. Smartmeter - AMI Server join protocol

[단계 1] 스마트미터 : 새로운 스마트미터에서 Nonce 값을 생성 하여 DCU의 공개키 값으로 암호화 하여 DCU에게 전송한다.

[단계 2] DCU : 전송받은 스마트미터의 Nonce 값과 기존 그룹 A의 그룹키 GA_n를 XOR 연산한 후 해쉬하여 새로운 그룹키 GA_{n+1}을 생성한다.

[단계 3] DCU : 새롭게 생성된 그룹키 GA_{n+1}를 $H(N)$ 값으로 암호화 하여 스마트미터에 전송하고 DCU의 개인키로 GA_{n+1}를 암호화하여 AMI 서버에 전송한다.

[단계 4] 스마트미터 : 전송받은 값을 GA_{n+1}로 복호화하여 그룹A의 그룹키 GA_{n+1} 를 저장한다.
AMI 서버 : 전송받은 값을 DCU의 공개키로 복호화하여 그룹A의 그룹키 GA_{n+1} 를 저장한다.

3-2-2 탈퇴 프로토콜

3-2-2-1 디바이스 탈퇴 프로토콜

스마트그리드 서비스를 제공받던 디바이스를 교체하거나 고장과 같은 원인으로 더 이상 서비스를 사용

하지 않는 경우 다음의 탈퇴 프로토콜을 수행한다.

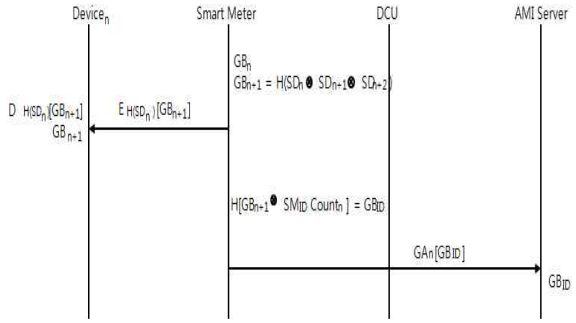

그림 8. 디바이스 탈퇴 처리 과정
Fig 8. Device leave protocol

[단계 1] 스마트미터 : 현재 사용중인 그룹키 G_n에서 탈퇴하는 디바이스의 비밀키 SD_n를 제외한 나머지 비밀키를 XOR 연산한 후 해쉬하여 G_{n+1}을 생성한다.

[단계 2] 스마트미터 : 탈퇴한 디바이스를 제외한 나머지 디바이스들에게 새로운 그룹키 G_{n+1}을 디바이스의 해당 비밀키 SD_n로 암호화하여 전송한다.

[단계 3] 디바이스 : 새로운 그룹키 G_{n+1}을 전송받은 디바이스는 복호하여 새로운 그룹키를 저장한다,

위의 단계 1-3을 통하여 디바이스가 탈퇴한 후 새로운 그룹키를 생성하게 된다. 이후 단계는 디바이스의 등록과정과 동일한 과정을 거친다.

[단계 4] 스마트미터 : 새롭게 갱신된 그룹키 GB_{n+1}와 스마트미터의 ID의 카운터 값과 XOR연산, 해쉬하여 그룹키ID GB_{ID}를 생성한다.

[단계 5] 스마트미터 : 생성된 그룹키ID GB_{ID}를 그룹키 GA_n을 사용 하여 암호화 한 후 전송한다.

[단계 6] AMI 서버 : 그룹키 GB_{ID} 를 저장한다.

3-2-2-1 스마트미터 탈퇴 프로토콜

스마트그리드 서비스를 제공받는 사용자의 스마트미터가 고장과 같은 원인으로 교체되거나 사용자가 서비스를 더 이상 제공 받지 않는 경우 다음의 탈퇴 프로토콜을 수행한다.

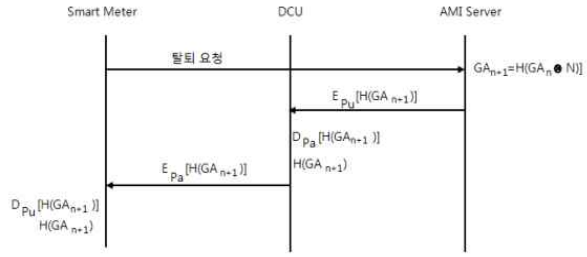

그림 9. 스마트미터 탈퇴 처리 과정
Fig 9. Smartmeter leave protocol

[단계 1] 스마트미터 : AMI 서버에 탈퇴 요청을 전송한다.

[단계 2] AMI Server : 탈퇴한 디바이스를 제외한 나머지 디바이스들에게 새로운 그룹키 G_{n+1}을 디바이스의 해당 비밀키 SD_n로 암호화하여 전송한다.

[단계 3] 디바이스 : 새로운 그룹키 G_{n+1}을 전송받은 디바이스는 복호화하여 새로운 그룹키를 저장한다,

Ⅳ. 안전성 및 효율성 분석

본장에서는 제안하는 스마트그리드 환경에 적합한 그룹키 관리 기법에 대해 그룹키 안전성 및 그룹키 효율성을 분석하고 기존의 기법들과의 비교 분석 및 결과를 제시한다.

4-1 안전성 분석

- 기밀성 : 제안하는 키 관리 기법은 스마트그리드 서버에 등록된 스마트미터와 스마트미터에 등록된 디바이스에 한해서만 H값을 통한 그룹키를 분배하기 때문에 스마트미터에 등록되지 않은 디바이스일 경우 해쉬체인을 통한 그룹키를 복호화 할 수 없다.

- 무결성 : 제안하는 키 관리 기법은 기존 SKMA, ASKMA 방식에서 분배된 키를 통하여 데이터 무결성을 지원하고 있는것처럼 그룹키 관리 기법을 이용한 키분배를 통해 데이터 무결성을 지원한다[4][6].

- 상호인증 : 제안하는 키 관리 기법은 기존 SKMA, ASKMA 방식에서 스마트미터가 AMI 서버에 접근할시 분배된 키를 통하여 상호인증이 이루어지는 거와 같이 제안하는 기법에서 또한 디바이스-스마트미터, 스마트미터-AMI서버간 상호인증을 지원한다.

- 디바이스의 무결성 보호 : 제안하는 키 관리 기법은 기존 스마트미터와 AMI 서버단까지 키를 관리하는 프로토콜과 다르게 디바이스와 스마트미터, 스마트미터와 AMI 서버단까지 키를 관리한다. 이를 통하여 스마트미터에 추가 되는 디바이스의 정보에 대한 무결성을 제공한다.

- 디바이스 인증 : 제안하는 키 관리 기법은 SKMA, ASKMA 기법에서는 관리 하지 않는 디바이스의 키를 관리함으로써

4-2 안전성 분석

- 브로드캐스팅 : 기존 프로토콜인 SKMA, ASKMA 방식은 SCADA 시스템 환경에 적합한 키 관리 모델로 메시지 브로드캐스팅과 같은 기능을 고려하지 않고 만들어져 메시지 브로드캐스팅을 제공하지 않는다. 본 논문에서 제안하는 키 관리 기법은 그룹키를 통하여 AMI서버에서 스마트미터까지 브로드캐스팅을 지원하고 스마트미터에서 디바이스까지 브로드캐스팅을 지원한다.

표 2. 안전성 및 효율성 비교 분석
Table 2. Security and Efficiency Comparisons Between Existing Method and Our Proposal

안 전 성	SKMA	ASKMA	제안 시스템
기밀성	X	X	O
무결성	O	O	O
상호인증	O	O	O
디바이스의 무결성 보호	X	X	O
디바이스 인증	X	X	O
효 율 성	SKMA	ASKMA	제안 시스템
브로드캐스팅	X	X	O

Ⅴ. 결 론

최근 들어 환경 위기와 자원 위기를 동시에 해결하고 지속적인 경제 발전을 이룩할 수 있는 주요 기술로 스마트그리드가 주목받고 있다.

그러나 통신 기술을 활용한 지능형 디바이스의 사용으로 데이터 송・수신시에 발생할 수 있는 데이터 노출, 데이터 도용 및 다양한 보안 위협들이 존재할 가능성이 있으며, 이는 국가 중요기반시설인 전력 시스템과 연계된 스마트그리드에서 사이버 테러와 같은 보안 사고를 야기할 수 있다. 따라서 이러한 보안 위협들에 대해 발견 즉시 대응하고, 효율적인 디바이스 관리를 위한 다양한 보안 메커니즘의 개발이 요구된다.

본 논문에서는 스마트그리드 통신 환경에서 고려해야 하는 통신 품질 및 보안 요구사항들을 분석하였고, 안전하고 효율적인 스마트그리드 통신 환경을 구축하는데 필요한 그룹키 관리 기법을 제안하였다. 제안하는 그룹키 관리 기법은 안전하게 생성된 그룹키를 사용함으로써 스마트그리드에서 발생할 수 있는 누전이나 정전과 같은 전력사고 시에 대한 빠른 인식과 함께 다수의 디바이스를 효율적으로 관리함으로써 스마트그리드의 안정적인 운영을 도울 수 있을 것이라 기대한다.

참 고 문 헌

[1] 이일우, 박완기, 박광로, 손승원, “ 스마트그리드 기술 동향”, *한국통신학회지(정보와통신),* 제 26권 제 9호, pp.24-33, 08. 2009.

[2] 이정준, “AMI 기술 동향”, *조명・전기설비,* 제 23권 제 6호, pp. 27-31,12. 2009

[3] 전용희, “스마트그리드의 취약성, 특성, 설계 원칙 및 보안 요구사항 분석.” *정보보호학회지,* 제 20권 제 3호, pp. 79-89, 2010년 6월

[4] R. D. Colin, C. Boyd, J. Manuel, and G. Nieto, "KMA-A key management architecture for SCADA systems," *in Proc. 4th Australasian Inf. Security Workshop*, Vol.54, pp. 138-192, 2006.

[5] Chung Kei Wong, Hohamed Gouda, Simon S. Lam, "Secure Group Communications Using Key Graphs" *In Proceedings of the ACM SIGCOMM `98 Conference on Applications, Technologies, Architecture, and Protocols for Computer Communication,* pp.68-79, 1998.

[6] D. Choi, H. Kim, D. Won, and S. Kim, "Advanced Key Management Architecture for Secure SCADA Communications", *IEEE Transaction on Power Delivery*, VOL24, No.3, pp. 1154-1163, 2009.

[7] C.L. Beaver. D.R. Gallup. W.D. NeuMann and M.D. Torgerson "Key Management for SCADA". *Technical Report. SAND 2001-3252.* Mar.

[8] NIST, "Smartgrid Cyber Security Strategy and Requirements", *Draft NISTIR 7628*, 02. 2010

장 유 종 (張庾琮)

2012년 2월 : 순천향대학교 정보보호학과(공학사)
2012년 3월~현재 : 순천향대학교 정보보호학과 석사과정
관심분야 : 스마트그리드 보안, 클라우드 컴퓨팅 보안 등

곽 진 (郭鎭)

1994년~2006년 : 성균관대학교 학사, 석사, 박사
2006년 4월 : 일본 큐슈대학교 시스템정보공학부 방문연구원
2006년 8월~2006년 11월 : 일본 큐슈 시스템정보기술연구소 특별연구원
2006~2007년 : 정보통신부 개인정보보호기획단 개인정보보호팀 통신사무관
2007~현재 : 순천향대학교 정보보호학과 교수
2007~2009년 : 정보통신연구진흥원 집필위원
2009~2009년 : 순천향대학교 공과대학 교학부장
2009~2010년 : 순천향대학교 정보보호학과 학과장
2010~2010년 : 교육과학기술부 국가기술수준평가 전문위원
현재 : 정보통신산업진흥원 기술평가위원, 사)국제정보능력평가원 쇼핑몰 플래너 자격 검정 출제 및 채점위원, 한국과학기술정보연구원 충남 과학기술 정보협의회 전문위원, 지식경제부 지식경제기술혁신평가단 평가위원, 순천향 BIT 창업보육센터 센터장, 순천향대학교 중소기업산학협력센터 센터장
관심분야 : 암호프로토콜, 응용시스템보안, 개인정보보호, 정보보호제품평가, 클라우드 컴퓨팅 보안, 스마트워크 등