제36회 한국정보처리학회 추계학술발표대회 논문집 제18권 제2호 (2011. 11)

AMI 시스템에서 안전한 정보 전송을 위한 인증 프로토콜

정수영, 고웅, 곽진
순천향대학교 정보보호학과

e-mail: syjung@sch.ac.kr, wgo@sch.ac.kr, jkwak@sch.ac.kr

The Authentication Protocol for secure data transfer in AMI system

Su-Young Jung, Woong Go, Jin Kwak
Department of Information Security Engineering, Soonchunhyang University.

요 약

21세기에 들어오면서 기존 전력망의 한계를 극복하기 위해 IT기술을 접목시켜 신재생에너지 활용과 효율적이고 안정적인 전력공급을 할 수 있다. 또한 스마트미터를 이용해 사용 전력량, 요금 등을 관리할 수 있다. 하지만 IT기술과 접목되어서 기존의 폐쇄망과는 달리 개방적으로 바뀌면서 외부의 공격에 쉽게 노출되어있다. 따라서 본 논문에서는 스마트미터와 이를 통해 수집되어진 정보를 취합하는 AMI Headend사이의 안전한 정보 전송을 위해 프로토콜을 제안한다.

1. 서론

21세기에 들어오면서 기존의 전력망으로는 효율적인 전력 공급에 대한 요구를 따라가지 못하고, 제한된 자원을 활용한 에너지 생산으로 인한 자원 고갈의 문제, 친환경적인 에너지인 태양열, 풍력 등의 신재생에너지의 전력 공급 불안정 등의 이유 때문에 전력망은 변화가 필요했다. 이런 문제를 해결하기 위한 대책으로 스마트 그리드가 만들어지게 되었다.

스마트 그리드는 IT기술과 접목된 스마트 기기를 이용하여 각 가정에서 실시간으로 전력 사용량 및 가격을 체크하여 전력 요금 절감에도 도움이 되고, 전력 사업자가 전력망을 모니터링 하여 전력이 많이 소비되는 피크 타임에는 전력 요금을 차등적으로 부과하거나, 전력 생산량을 증가시키는 등의 조치를 취해서 전력을 안정되고 공급을 할 수 있다. 또한 태양열, 풍력 등 신재생에너지로 생산한 전력은 안정적으로 항상 공급하기가 어렵기 때문에 전력 저장장치를 이용한 전력 저장 등의 방법으로 제어할 수 있다[1].

스마트 그리드를 도입하면 앞서 언급한 것처럼 많은 효과를 이끌어 낼 수 있지만 안전상의 이유로 폐쇄 망으로 구성했던 전력을 IT기술과 접목시켜 통신을 주고받으면서 IT환경에서 발생할 수 있던 취약점에 그대로 노출되게 되었다. 따라서 스마트 그리드를 구성하는데 있어서 통신망을 통한 외부 위협에 효과적으로 대응하는 것이 가장 중요한 문제이다.

본 논문에서는 스마트 그리드 AMI 시스템에서 각 가정의 전력 사용, 요금 등의 정보를 수집하는 스마트미터와 각 스마트미터에서 전송된 정보를 취합하여 전력 회사 배전망으로 재전송 역할을 하는 AMI Headend간의 정보를 전송하는 과정에서 안전하게 정보를 전송할 수 있도록 하기 위한 인증 프로토콜을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 스마트 그리드를 구성하는 주요 내용에 대해 기술하고, 3장에서는 프로토콜을 구성하는데 있어서 필요한 보안 요구사항을 분석한다. 4장에서는 스마트미터와 AMI Headend 사이의 통신에 있어서 발생할 수 있는 문제점을 분석하고, 5장에서는 문제점을 개선할 수 있는 프로토콜을 제안한다. 마지막으로 6장에서는 결론으로 끝을 맺는다.

2. 관련 연구

2.1 AMI 시스템

AMI(Advanced Metering Infrastructure)는 기존의 단방향 원격 검침(AMR : Automatic Meter Reading)보다 한 단계 기능이 향상된 개념으로 전력회사와 소비자가 양방향으로 통신하여 소비자에 대한 정보를 수집하고 소비자에게 전력사용 정보를 제공한다. 크게 4단계로 HAN(Home Area Network)에서 각 가정에 전력 사용 관련 기기, 댁내 및 댁외 사이의 통신에서 전력 사용량, 전력 요금 등을 기록하게 되는 스마트 미터, 전력사와 스마트미터 간의 연결을 할 수 있도록 해주는 통신 시스템, MDMS(Meter Data Management System)를 중심으로 구성된 상위 시스템으로 분류할 수 있다.

2.2 스마트미터

양방향 통신을 이용하여 집 내부에 있는 각각의 가전제품의 사용 전력량, 요금 등을 실시간으로 체크하여 전력사와 통신을 한다. 또한 이를 이용하여 전력 사용 패턴 분석 등을 통해 전력사는 안정적인 전력 공급을 위해 활용할 수 있어 정전 등을 예방할 수 있고 소비자는 전력 사용량을 효율적으로 할 수 있어 요금 절약이 가능하다.

2.3 AMI Headend

전력 회사 배전망의 경계에 있는 AMI Headend는 HAN안에 있는 각각의 기기로부터 전력 사용량을 스마트미터를 통해 전송하고 AMI Headend는 수집된 정보를 전송받아 취합하여 전력 운영망인 MDMS 등의 상위 시스템에 다시 재전송을 한다. 또한 정보에 대한 추가 기능 제공, 감시 등의 역할을 수행한다[2].

3. 보안 요구사항

· 기밀성 : 통신을 하는 과정에서 전달되는 정보는 정당한 사용자에게만 공유되어야 하며 제 3자가 전송 하는 정보에 대한 내용을 볼 수 없도록 해야 한다.

· 무결성 : 통신상에서 전달되는 정보는 과금정보, 전력 사용량 등의 정보가 포함되어 있으므로 중간에 위조 및 변조가 되지 않도록 보장되어야 한다.

· 가용성 : 스마트미터가 AMI Headend와 통신할 때 지속적으로 안정된 서비스를 제공받을 수 있어야 한다.

· 인가 : 스마트미터와 AMI Headend가 정보를 주고받을 때 정당하게 등록된 사용자만 정보를 주고받을 수 있어야 한다.

4. 문제점 분석

기존 전력망에 IT기술이 결합된 스마트 그리드의 AMI 시스템은 사용자 각 가정의 전력 사용량, 전력 사용 요금 등의 정보를 스마트미터에서 전송하여 AMI Headend에서 수집하게 된다. 스마트미터에서 전송되는 정보에는 사용자의 전력 사용량, 사용 요금, 소비 패턴 등의 정보가 내장되어있다. 이 정보가 중간자 공격, 위·변조 등으로 유출될 경우 실제 사용량 보다 적게 사용한 것으로 조작된 요금, 전력 사용 패턴 분석을 통해 외출 여부를 판단하여 댁내부 침입하는 2차적인 피해, 개인정보 유출 등의 문제점이 발생 할 수 있다[3].

5. 안전한 정보 전송을 위한 프로토콜 제안

스마트 그리드에서 각 가정에 배치되어 전력 사용에 대한 정보를 담고 있는 스마트미터와 AMI Headend는 서로 정보를 주고받기 때문에 AMI Headend는 한 번에 많은 양의 정보를 전송 받게 된다. 따라서 본 논문은 스마트미터와 AMI Headend의 정보 전송에 있어 기존방법보다 안전하면서 연산횟수와 연산량을 줄인 정보 전송을 위한 프로토콜을 제안한다.

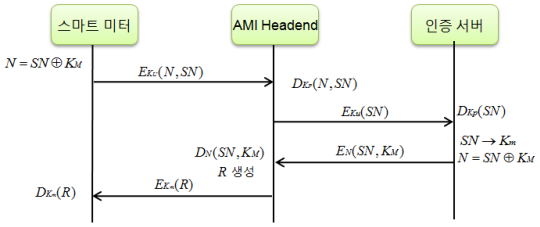
<표 1>은 제안된 인증 프로토콜에서 사용하는 시스템 파라미터이다.

<표 1> 시스템 파라미터

기호	의미
E	암호화
D	복호화
K_u	공개키
K_P	개인키
SN	스마트미터 고유 번호
K_M	스마트미터 대칭키
N	SN과 K_M을 XOR한 값
R	AMI Headend에 SN과 K_M을 저장하기 위한 난수(사용된 난수 값은 중복 불가)
I	스마트미터에 수집된 정보
T	타임스템프

5.1 등록 단계

등록 단계는 스마트미터의 SN과 대칭키를 AMI Headend로 전송하여 등록시키고 AMI Headend에서 생성된 R값은 스마트미터로 전송하여 등록이 완료된다. 인증서버에는 스마트미터 설치당시 각 스마트미터의 SN을 저장하고 이에 해당하는 대칭키를 발급한다. 미리 등록을 하여 매번 스마트미터가 AMI Headend에 접근하려 할 때마다 등록할 필요 없이 한 번의 등록으로 등록단계는 수행이 완료된다[4,5].



(그림 1) 등록 절차

1단계 : 스마트미터는 자신의 SN과 K_M을 XOR하여 N 값을 생성한다. 생성한 값과 SN을 AMI Headend의 공개키를 이용하여 암호화하여 AMI Headend에 전송한다.

2단계 : AMI Headend는 전송받은 암호화된 값을 개인키를 이용하여 복호화하고 SN은 공개키로 암호화하여 인증서버로 전송한 후 SN이 유효한 값인지 확인을 요청한다.

3단계 : 전송받은 암호화된 값을 개인키로 복호화하고 복

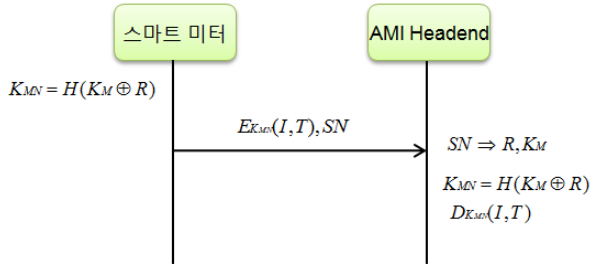
호화된 SN을 인증서버에 저장되어 있는 SN을 검색하여 유효한 값인지를 검증한 후 유효한 값이면 SN과 같이 저장되어 있는 스마트미터의 대칭키 K_M을 찾는다. K_M을 SN과 XOR 연산을 통해 N을 만들고, N을 이용하여 SN, K_M을 암호화한 후 AMI Headend에 전송한다.

4단계 : N을 이용해 암호화된 값을 2단계에서 복호화를 통해 얻은 N으로 복호화 후에 SN, K_M을 얻는다. 얻은 두 개의 값을 저장하고 이에 해당하는 R을 생성하여 같이 저장한다. 복호화를 통해 얻은 K_M을 이용하여 R을 암호화하여 스마트미터에 전송한다.

5단계 : 전송받은 암호화된 값을 갖고 있던 K_M을 이용하여 복호화 후 R을 저장 하고 등록절차를 종료한다.

5.2 정보 전송 단계

등록 단계를 거쳐 스마트미터에는 R이, AMI Headend에는 R에 해당하는 SN과 K_M이 저장되어 있다. 저장된 값을 연산하여 정보를 AMI Headend만 복호화 할 수 있는 키로 만들어 암호화하여 전송한 뒤 AMI Headend에서는 이를 복호화 후 안전하게 정보를 전송 받는다[6].



(그림 2) 정보 전송 단계

1단계 : 스마트미터에서 수집된 정보 I를 안전하게 보내기 위해 암호화를 위한 대칭키 K_{MN}은 K_M과 R을 XOR 연산 후 해쉬연산하여 만든다. 키 K_{MN}을 이용하여 I 값과 T 값을 암호화한 값과 SN을 AMI Headend에 전송한다.

2단계 : AMI Headend는 전송받은 SN을 검색하여 그에 해당하는 R와 K_M을 획득하여 두 값을 XOR하여 해쉬연산 후 그 값을 이용해 복호화한다.

3단계 : 복호화된 T와 비교하여 시간 차이가 일정 기준 시간 안에 포함되면 I를 MDMS 등으로 재전송하기 위한 준비를 한다.

6. 결론

스마트 그리드는 전력사는 전력량 파악을 통한 안정적인 전력 공급, 신재생에너지 활용 등을 가능하게하고 소비자는 사용 패턴 분석을 통한 전력요금 절약 등의 장점을 갖게 한다. 하지만 국가 기반시설로 안전이 중요시되는 전력망에 IT가 결합되면서 기존의 IT기술에서 발생할 수 있는 문제점이 그대로 발생할 수 있어 이에 대한 대책이 필요하다.

본 논문에서는 AMI 시스템에서 스마트미터와 AMI Headend 사이에 전력 사용정보, 전력 사용량, 개인정보 등의 정보 전송을 안전하게 하기 위한 프로토콜을 제안을 하였다. 또한 각 가정에 위치한 많은 스마트미터로부터 정보를 전송받는 환경을 고려하여 연산횟수를 최대한 줄이도록 설계하였으며, 등록 단계에서 인증 서버를 통해 검증하여 등록단계에서의 인증의 신뢰도를 높였다. 본 논문을 통해 AMI 시스템에서 스마트미터와 AMI Headend간의 안전한 정보 전송을 위한 연구 자료로 활용될 수 있다.

참고문헌

[1] 이정준, “AMI의 구조”, 한국통신학회지 제 27권 제 4호, pp. 17~22, 2010.4

[2] “클라우드 기반 스마트 그리드를 위한 보안기술 연구“, 한국인터넷진흥원, 2010.12

[3] Gary Locke and Patric D. Gallagher, “Guidelines for Smart Grid Cyber Security : Vol. 3, Supportive Analyses and References”, NISTIR 7628, The Smart Grid Interoperability Panel - Cyber Security Working Group, Aug. 2010.

[4] 심희원, 박준형, 노봉남, "스마트카드를 이용한 향상된 동적 ID기반 원격 사용자 인증 기술", 인터넷정보학회 논문지 제 10권 제 4호, pp. 223~230, 2009.8

[5] 전재우, 임선희, 이옥연, "스마트 그리드를 위한 Binary CDMA 기반의 AMI 무선 네트워크 구조 및 AKA 프로토콜", 한국정보보호학회논문지 제 20권 제 5호, pp.111~124, 2010.10

[6] 김홍기, 홍민, 이임영, “스마트 그리드환경에서 안전한 전력량 전송을 위한 AMI 인증기법”, 제 35회 한국정보처리학회 춘계학술대회 논문집 제18권 1호, pp.877~878, 2011.5