스마트그리드환경에서 안전한 전력량 전송을 위한 AMI 인증기법

김홍기, 홍민+, 이임영
순천향대학교 컴퓨터소프트웨어공학과
e-mail:[hgkim31, mhong, imylee]@sch.ac.kr

AMI Authentication Scheme for Secure Electricity Transmission in SmartGrid Environment

Hong-Gi Kim, Min Hong, Im-Yeong Lee
Department of Computer Software Engineering, Soonchunhyang University

요 약

최근 기존의 단 방향 전력망 시스템에 IT기술을 접목한 스마트그리드 기술의 개발이 활발하게 이루어지고 있다. 스마트그리드의 핵심 인프라로 원격검침시스템인 AMI는 스마트미터에서 측정한 전력량을 상위 데이터 저장소인 MDMS에 전송한다. 스마트미터는 IT기술을 활용하여 전력데이터를 전송하고 있기 때문에 기존 보안위협을 포함한 추가적인 보안위협이 예상된다. 이는 소비자의 개인정보노출 및 산업시스템 마비 등의 손실이 발생할 가능성이 있다. 따라서 이러한 보안위협에 대응하기 위해 스마트그리드 환경에서 스마트미터와 MDMS간 상호인증과 데이터 전송방식에 관하여 제안하였다.

1. 서론

스마트그리드는 기존의 단 방향 전력망에 정보통신기술을 접목하여 전력 공급자와 소비자가 양방향으로 실시간 정보를 교환함으로써 에너지 효율을 최적화하는 지능형전력망을 지칭한다.

스마트그리드의 핵심 인프라로 전체 에너지 사용량을 효율적으로 관리하기 위한 원격 검침 시스템인 AMI(Advanced Metering Infrastructure)가 있다. 이는 에너지를 효율적으로 관리하기 위한 체계로써, 각 가정 내 설치되는 스마트미터와 전력량을 취합하는 MDMS(Meter Data Management System)로 구성된다[1,2].

이러한 AMI기술은 스마트기기 간 정보통신기술을 활용하여 전력데이터를 처리하고 있어, 기존 IT기술의 보안위협을 포함한 추가적인 보안위협이 예상된다. 스마트미터는 실시간 에너지소비량, 요금정보 및 각종 개인정보들을 포함하여 저장하기 때문에 개인의 프라이버시 문제 및 산업 시스템 마비 등의 손실이 발생할 가능성이 있다. 따라서 AMI서비스를 제공하기 위해 발생 가능한 보안위협에 대응하는 서비스가 마련되어야 한다[3]. 이에 본 연구는 스마트그리드 환경에서 스마트미터와 MDMS간 상호인증과 데이터 전송방식에 관하여 제안한다.

2. 보안요구사항

스마트그리드 환경에서 스마트미터와 MDMS간의 통신은 주기적인 시간에 일괄적으로 이루어진다. 이에 적은 연산량과 통신횟수가 제공되어야 한다. 이에 AMI 인증 및 데이터 전송기법에서의 보안요구사항은 다음과 같다.

- 기밀성 : 통신에 사용되는 데이터들은 사용자의 개인정보를 포함하고 있어, 정당한 객체들만이 공유되어야 하며 통신 중간에 노출되더라도 그 데이터의 값을 유추하지 못해야 한다.
- 무결성 : 통신상에서 제공되는 데이터들은 과금과 같은 금전 거래의 근거가 되므로 통신 중간에 위조 및 변조되지 않아야 한다.
- 상호인증 : 정당한 스마트미터와 MDMS의 확인을 위하여 서로간의 상호인증이 제공되어야 한다.
- 연산량 : 빠른 속도로 데이터를 암호화하고 복호화하기 위하여 연산 효율성이 높아야 한다.

3. 제안방식

이 장에서는 2장의 보안요구사항을 만족하는 AMI 인증과 데이터 전송기법을 제안한다. 스마트그리드 환경에서는 스마트미터와 MDMS가 주기적인 시간에 통신을 수행하므로 다수의 스마트미터에서 일괄적으로 데이터가 전송된다. 따라서 제안방식은 기존의 인증기법보다 적은 연산량과 통신횟수를 통해 안전하게 스마트미터를 인증하게 데이터를 전송하는 기법을 제안한다. 본 제안방식은 등록단계, 인증 및 데이터 전송단계로 구분되며, 각 단계의 수행절차를 다음과 같다.

3.1 시스템 계수

- $*$: 각각의 개체 (SM : 스마트미터, MD : MDMS)
- M : 전력량 데이터
- K_{*P} : $*$의 비밀키

+ 교신저자 : 홍민(mhong@sch.ac.kr)

- K_{*U} : *의 공개키
- *MAC_Addr* : 스마트미터의 MAC Address
- *MDMS_ID* : MDMS의 이름
- T : 전송 시간 값

3.2 등록단계

등록단계에서는 인증 받는 스마트미터의 MAC Address와 해쉬연산 된 개인키를 전송하여 저장한다. 저장완료 후 MDMS에서는 자신의 이름을 전송하여 등록을 완료한다.

등록단계는 스마트미터가 최초로 등록될 때 1회 수행하며, 이후 모든 인증 및 데이터 전송 시에 등록단계는 수행되지 않는다.

Step1 : 스마트미터는 자신의 MAC Address와 개인키를 통해 N_A를 생성하고 타임 스탬프를 포함하여 MDMS의 공개키를 사용하여 암호화한다. 암호화된 데이터를 MDMS에게 MAC Address를 추가하여 전송한다.

Step2 : MDMS에서는 전송받은 암호문을 MDMS의 개인키 K_{MDP}로 복호화하여 MAC Address를 확인하고, MAC Address와 N_A에 포함되어있는 해쉬 연산 된 스마트미터의 개인키 $H(K_A)$를 저장하여 후에 암호화키로 사용한다.

Step3 : MDMS는 스마트미터의 개인키를 저장 후 자신의 이름 *MDMS_ID*와 스마트미터에게 전송받은 시각 T를 포함하여 $H(K_A)$로 암호화후 스마트미터에게 전송한다.

Step4 : 스마트미터는 전송받은 암호화 값을 복호화하여 MDMS의 이름을 저장하고 등록단계를 마친다.

3.3 인증 및 데이터 전송단계

등록단계가 완료되면 스마트미터는 MDMS의 이름을 저장하고 있고, MDMS는 해쉬연산 된 스마트미터의 개인키와 MAC Address를 저장하고 있다. 이를 이용하여 데이터 전송단계에서는 스마트미터에서 측정한 전력량을 등록한 MDMS만 복호화 가능하도록 세션키를 생성하여 암호화하여 전송한다.

Step1 : 스마트미터는 측정된 전력량을 전송하기 위하여 사용될 키 K_{SA}를 등록단계에서 사용된 $H(K_A)$와 *MDMS*의 이름값, 타임 스템프를 해쉬연산하여 생성한다.

Step2 : 생성된 키 K_{SA}를 통해 측정된 전력량 M을 암호화하고 이를 MDMS가 복호화 할 수 있도록 타임스탬프를 포함하여 $H(K_A)$를 키로 사용하여 재 암호화한다. 재 암호화 후 생성된 값을 MAC Address를 포함하여 MDMS에게 전송한다.

Step3 : MDMS는 전송받은 MAC Address를 통해 $H(K_A)$를 검색하고, 복호화를 수행한다.

Step4 : 복호화 후 남아 있는 암호문을 K_{SA}를 생성하여 복호화하고 측정된 전력량을 저장한다.

5. 제안방식분석

본 제안방식은 안전하게 전력량 데이터를 전송하기 위하여 도출된 보안요구사항을 다음과 같이 만족한다.

- 기밀성 : 공개키 및 대칭키 암호 알고리즘을 통해 스마트미터의 정보 및 전력량을 암호화 후 전송하여 기밀성을 제공한다.
- 무결성 : 스마트미터가 MDMS에게 전송할 때 그 데이터에 대한 키를 알 수가 없기 때문에 위·변조가 불가능하다. 또한 변경을 시도하게 되더라도 해쉬 값을 통해 검증이 가능하다.
- 상호인증 : 스마트미터의 MAC Address와 $H(K_A)$를 통해 MDMS에게 인증 받고, MDMS는 자신의 이름을 전송하여 상호인증을 제공한다.
- 연산량 : 등록단계를 포함한 인증 및 데이터전송단계는 3번의 통신으로 4번의 해쉬연산과 3번의 암호화 과정을 통해 인증을 수행한다. 등록단계는 한 번의 등록 후 다시 수행되지 않기 때문에 주기적인 데이터 전송 시 인증 및 데이터전송단계만 수행된다. 이때 해쉬연산은 2번, 암호화 과정은 1번만 수행되기 때문에 감소된 연산량을 통해 인증과정을 수행할 수 있다.

6. 결론

본 논문에서는 스마트미터와 MDMS간 인증 및 데이터전송을 스마트미터의 MAC Address를 통해 수행한다. 제안방식은 기존의 스마트기기 인증기법보다 적은 통신횟수와 연산량을 통해 빠른 인증속도를 제공한다. 또한 매 세션 간 다른 세션키를 생성 후 전력데이터를 전송하여 이전에 세션키가 노출돼도 다음번의 전력데이터를 확인하지 못하는 안전성을 제공하고 있다. 향후 소비자가 전송한 전력데이터의 정당성을 확인하는 서명기술 및 최상위 MDMS만 전력량을 확인가능 한 기술 등이 연구되어야 할 것으로 사료된다[4,5].

참고문헌

[1] 남궁완, 조효진, 조관태, 이동훈, "스마트미터 보안 연구", 한국정보보호학회지 제 20권 제 5호, pp. 20~30, 2010.10

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

[3] 이정준, "AMI 기술 동향", 조명, 전기설비 학회지 제 23권 제 6호, pp. 27~31, 2009.12

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

[5] 이영구, 김정재, 김현철, 전문석, "PKI 기반 홈 네트워크 시스템 인증 및 접근제어 프로토콜에 관한 연구", 한국통신학회논문지 제35권 제4호, pp.592~598, 2010.4