제36회 한국정보처리학회 추계학술발표대회 논문집 제18권 제2호 (2011.11)

스마트그리드환경에서 OTP기반의 AMI인증방식에 관한 연구*

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

A Study on OTP-based AMI Authentication Scheme in SmartGrid Environment

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

요 약

스마트그리드는 기존의 전력망 환경에 정보통신 기술을 접목하여 발전소와 사용자가 실시간으로 정보를 교환하며, 사용 과금 및 전력공급의 효율성을 증대시키는 기술이다. 스마트그리드는 전력관리소인 MDMS(Meter Data Management System)와 각 가정에 연결되어있는 스마트미터와의 통신을 통해 전력데이터를 수집하게 되는데, 각 가정의 디바이스들은 전력사용량을 사용한 만큼 스마트미터에게 정보를 전송하여 스마트미터에서는 그 정보를 MDMS에게 전송하는 방식을 사용하고 있다. 이는 네트워크를 활용하여 전송하고 있기 때문에 기존의 보안위협 및 스마트그리드환경에서의 추가적인 보안위협이 예상된다. 따라서 본 논문에서는 각 가정에서 측정한 전력데이터 값을 안전하게 전송하기 위해 디바이스를 OTP를 기반으로 안전하게 인증하는 기술에 대하여 제안하였다.

1. 서론

스마트그리드는 기존의 전력망 시스템에 정보통신기술을 접목하여 사용자와 발전소간 양방향 통신을 통해 실시간으로 전력 사용량을 교환하며, 전력 사용 및 공급의 효율성을 극대화 하는 기술이다.

스마트그리드에서는 전기로 작동되는 모든 기기들이 유·무선 네트워크로 연결되며, 서로간의 정보 교환을 통하여 유기적인 관계로 이루어진다. 현재 제공되는 전력 시스템은 전력사용예측이 불가능하기 때문에 일반적으로 10%이상의 예비전력을 보유하여 저장하고 있다. 그러나 스마트그리드 환경에서는 스마트미터(Smart Meter)를 통해 실시간으로 사용되는 에너지를 분석함으로써 에너지를 효율적으로 분배할 수 있다[1].

스마트그리드의 핵심 인프라로 원격 검침 시스템인 AMI(Advanced Metering Infrastructure)가 있다. 이는 에너지를 효율적으로 관리하기 위한 체계로써, 각 가정 내 설치되는 스마트미터와 각 가정의 디바이스, 그리고 전력량을 취합하는 MDMS(Meter Data Management System)로 구성된다. 소비자들은 AMI를 통해 실시간 에너지 사용량 정보를 기반으로 에너지를 관리함으로써 가정 및 기업의 에너지 비용을 절감할 수 있으며, 전체 에너지 사용량을 효율적으로 관리할 수 있다[2].

본 논문의 구성은 다음과 같다. 2장에서는 AMI구조 및 일회용 패스워드 생성방식에 대하여 분석한다. 3장에서는 관련연구를 기반으로 한 AMI 인증기법에서의 보안요구사항에 대하여 분석한다. 4장에서는 보안요구사항을 만족하는 제안방식을 기술하며, 5장에서는 보안요구사항에 의한 제안방식을 분석한다. 마지막으로 6장에서 결론을 맺는다.

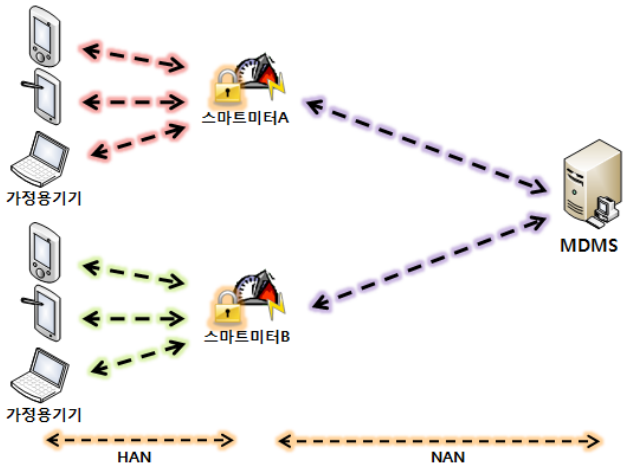
2. 관련연구

본 장에서는 AMI의 구조를 분석하고, 기존의 스마트기기와 서버 간 제공되고 있는 인증기술의 취약점을 분석한다.

2.1 AMI 구조

AMI는 최종 소비자와 전력회사 사이의 전력 서비스 정보화 인프라로서 스마트그리드 운용에 필수적인 스마트미터 기반의 핵심 인프라 시스템이다. 단순히 계량 값만을 읽어가는 기존의 AMR(Automated Meter Reading)과는 다르게 소비자의 수요 및 전력가격을 실시간으로 양방향 전송하는 역할을 담당한다. 이는 스마트미터를 중심으로 양방향 통신과 오픈 프로토콜(Open Protocol)에 기반해 원격 전력차단이 가능하고 선불형 계량의 인프라가 될 수 있으며 실시간 요금제, 피크 요금제, TOU(Time-of-Use)

"본 연구는 지식경제부 및 정보통신산업진흥원의 "대학 IT연구센터 육성·지원사업"의 연구결과로 수행되었음" (NIPA-2011-C1090-1001-0004)



(그림 1) AMI 구조

요금제 등 다양한 요금제의 적용도 가능하다. 수요반응 매커니즘에는 없어서는 안될 내용이며 더 나아가서는 홈오토메이션, 홈네트워킹과 연결되고, 결국 스마트그리드 기본 인프라가 되는 것이 AMI이다.

AMI의 구성요소는 (그림 1)과 같이 MDMS를 중심으로 한 전력사 내의 상위 시스템, 전력사와 수용가의 스마트 미터간의 연결시켜주는 통신 시스템, 스마트미터, 가정용 기기 등으로 구분된다[3].

2.2 S/Key 일회용 패스워드

RFC 1760 표준인 S/Key 인증방식에서는 해쉬 알고리즘인 SHA-1을 이용하여 일회용 패스워드를 생성한다. S/Key방식은 그림 1과 같이 사용자의 패스워드와 서버에서 생성한 난수 *Seed*를 XOR연산과 해쉬 연산을 이용하여 일회용 패스워드를 생성하고 있다. 또한 서버 데이터베이스에 해쉬 체인을 이용한 OTP 생성 값이 저장되어 있어, 추가적인 인증 요구 시 빠른 속도를 제공하고 있다.

그러나 S/Key 인증방식은 모든 값이 평문으로 전송되어 공격자에게 쉽게 노출된다는 단점을 가지고 있다. 또한 서버의 난수인 *Seed*값이 동일하게 유지되고 있기 때문에 *N*번의 로그인 횟수가 노출되면 공격자는 쉽게 다음 일회용 패스워드 값을 유추할 수 있다[4].

2.3 시간동기화 일회용 패스워드

본 방식은 시간 동기화방식을 이용한 일회용 패스워드 생성방법으로써, 그림 2와 같이 시간편차에 의한 인증이 실패할 가능성이 있는 기간을 표시하는 flag를 사용하여 flag의 값이 1일 경우 클라이언트의 시간 값을 이용하여 일회용 패스워드를 생성 후 서버에 전송하고 서버에서는 전송받은 flag가 1이라는 것을 확인 후 자신의 시간 값으로 일회용 패스워드를 계산하여 전송받은 값과 비교 후 인증한다.

본 방식의 경우 시간동기화 방식을 사용하고 있으며, 클라이언트에서 일회용 패스워드를 계산 후 서버로 전송하고 있어 전송시간 지연의 문제와 계산 지연 문제가 발생할 수 있으며, 중간에 flag의 값이 노출될 경우 정당한 사용자가 인증 받지 못하는 문제점이 발생할 수 있다[5].

3. 보안요구사항

스마트미터는 15분 간격으로 디바이스의 전력량을 전송받고 있다. 이에 적은 연산량과 통신횟수가 제공되어야 한다. 따라서 AMI 인증 및 데이터 전송기법에서의 보안요구사항은 다음과 같다.

- 기밀성 : 통신에 사용되는 데이터들은 사용자의 개인정보를 포함하고 있어, 정당한 통신객체들만이 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 디바이스의 확인을 위하여 서로간의 상호인증이 제공되어야 한다.
- 연산량 : 빠른 속도로 데이터를 암호화하고 복호화하기 위하여 연산 효율성이 높아야 한다.

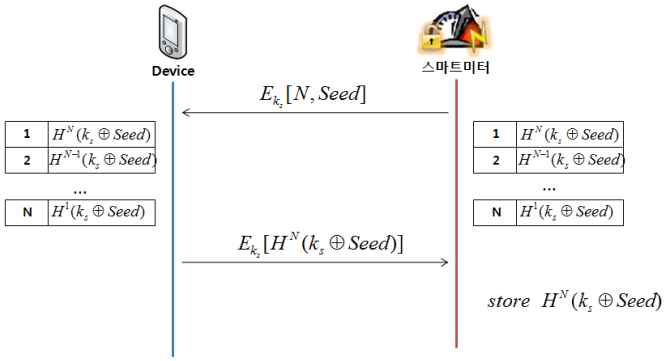
4. 제안방식

이 장에서는 3장의 보안요구사항을 만족하는 AMI 인증과 데이터 전송기법을 제안한다. 스마트그리드 환경에서는 스마트미터와 디바이스가 주기적인 시간에 통신을 수행하므로 다수의 디바이스에서 일괄적으로 데이터가 전송된다. 따라서 제안방식은 기존의 인증기법보다 적은 연산량과 통신횟수를 통해 안전하게 스마트미터를 인증하게 데이터를 전송하는 기법을 제안한다. 본 제안방식은 등록단계, 인증단계로 구분되며, 각 단계의 수행절차를 다음과 같다.

4.1 시스템 계수

본 제안방식에서는 다음과 같은 시스템계수를 사용하여 프로토콜을 설계한다.

- $*$: 각각의 개체 (*De* : Device, *SM* : 스마트미터)
- N : 전체 로그인 횟수
- ks : 디바이스와 스마트미터간 세션키
- $Seed$: 초기값
- C : 디바이스에서 측정한 카운터
- Ts : 타임스템프
- $E_*[\ ]$: $*$의 키로 암호화
- $H(\ )$: 일방향 해쉬함수



(그림 2) 등록단계

4.2 등록단계

등록단계에서는 [그림 2]와 같이 기존 S/Key방식과 동일한 방법으로 서버에 일회용 패스워드 테이블을 등록한다. 서버는 전체 로그인 횟수 N과 초기값 $Seed$를 클라이언트에게 전송해 주고, 클라이언트는 전송받은 $Seed$값과 사전에 공유되어있는 서버와의 세션키를 통하여 XOR연산 수행 후 해쉬 연산을 수행한다.

해쉬 연산 후 생성된 결과값을 세션키로 암호화하고 서버에게 전송하여 생성된 결과값을 통해 인증받게 된다. 등록단계의 수행은 다음과 같다.

Step1 : 스마트미터에서는 생성한 $Seed$값과 전체로그인 횟수 N을 세션키 ks를 통해 암호화하여 디바이스에게 전송해 준다.

$$De \rightarrow SM : E_{ks}[N \,||\, Seed]$$

Step2 : 디바이스와 스마트미터는 $Seed$값과 세션키 ks를 XOR연산하여 전체 로그인 횟수 N만큼 해쉬 연산 한 일회용 패스워드 테이블을 생성한다.

$$De : H^N(ks \oplus Seed) \cdots H(ks \oplus Seed)$$
$$SM : H^{N'}(ks \oplus Seed) \cdots H(ks \oplus Seed)$$

Step3 : 디바이스에서는 전체 로그인 횟수 N만큼 해쉬 연산한 $H^N(ks \oplus Seed)$을 세션키 ks로 암호화하여 스마트미터에게 전송하고, 스마트미터에서는 생성한 $H^{N'}(ks \oplus Seed)$값과 전송받은 값을 비교하여 일회용 패스워드 전체 테이블을 저장한다.

$$De : E_{ks}[H^N(ks \oplus Seed)]$$
$$SM : H^N(ks \oplus Seed) =? H^{N'}(ks \oplus Seed)$$
$$SM : OTP\_Table\ Store$$

4.3 인증단계

등록단계를 수행하면 디바이스와 스마트미터는 같은 일회용 패스워드를 보유하고 있다. 이후 인증단계에서는 [그림 4]와 같이 시간 값을 통해 P를 생성하고, P를 이용해 해쉬테이블에서 일회용 패스워드를 임의로 사용하여 디바이스를 인증한다. 인증 후 다른 $Seed$값을 활용하여 사용한 해쉬테이블 자리에 새로 생성한 OTP값을 삽입하여 해쉬테이블을 갱신한다.

새로 생성한 OTP값은 세션키로 암호화하여 서버에 전송하고, 서버에서는 이를 복호화 하여 해쉬테이블을 갱신한다. 인증단계는 다음과 같은 과정으로 진행된다.

Step1 : 디바이스는 시간 값을 측정하여 P의 값을 생성하고, 이를 통해 일회용 패스워드 값을 해쉬 테이블 내에서 추출한다.

$$De : P = T_s \bmod N$$

Step2 : 디바이스는 전체 로그인 횟수인 N과 $Step1$에서 계산한 P의 값을 통해 일회용 패스워드 테이블 내 OTP값을 사용한다.

$$De : OTP = H^{N-P}(ks \oplus Seed)$$

Step3 : 디바이스는 카운터 값과 타임스템프를 세션키로 암호화하여 OTP값과 함께 스마트미터에게 전송한다.

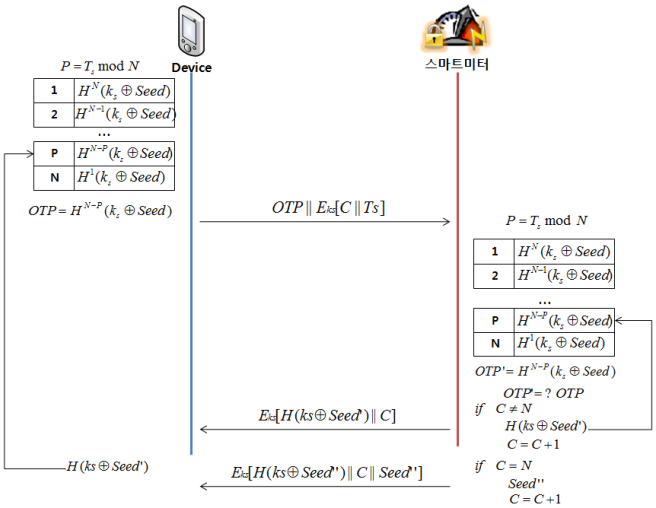
$$De \rightarrow SM : OTP \,||\, E_{ks}[C||Ts]$$

Step4 : 스마트미터에서도 P의 값을 생성하고 이 값을 통해 일회용 패스워드 테이블 내 OTP값을 사용하여 디바이스를 인증한다.

$$SM : P = T_s \bmod N$$
$$SM : OTP' = H^{N-P}(ks \oplus Seed)'$$
$$SM : OTP =? OTP'$$

Step5-1 : 스마트미터에서는 카운터값을 전체로그인 수와 비교하여 같지 않다면 $Seed'$을 이용하여 사용한 P의 자리에 새로 생성한 일회용 패스워드값을 삽입하고, 디바이스에게 사용한 일회용 패스워드 값과 증가한 카운터값을 전송한다.

$$SM : H(ks \oplus Seed')$$
$$SM \rightarrow De : E_{ks}[H(ks \oplus Seed')||C]$$



(그림 3) 인증단계

Step5-2 : 스마트미터에서는 카운터값을 전체로그인 수와 비교하여 둘의 값이 같다면 *Seed*값을 갱신하고 이를 통해 만든 OTP값과 카운터 값 새로 생성한 *Seed*값을 세션키로 암호화하여 디바이스에 전송해 준다.

$$SM : Seed''$$

$$SM \rightarrow De : E_{ks}[H(ks \oplus Seed'')||C]$$

Step6 : 디바이스에서는 전송받은 새로운 OTP값을 사용한 해쉬테이블에 삽입하여 후에 사용할 OTP값을 갱신한다.

$$De : H(ks \oplus Seed')$$

5. 제안방식분석

OTP기반의 디바이스와 스마트미터 간 인증방식의 보안요구사항에 대한 제안방식 분석은 다음 <표 Ⅴ-1>과 같다. 기존 인증방식 및 제안방식은 모두 기밀성, 무결성, 상호인증을 제공한다. 그러나 스마트그리드 환경에서 높은 연산량 및 통신횟수는 일괄적으로 데이터를 처리하는데 문제점이 있다. 이에 제안방식은 스마트그리드 환경에 적합하도록 스마트미터에서 수행하는 연산량을 감소시켜 빠른 속도로 인증이 가능하도록 고안하였다.

또한 초기 등록이후에는 등록과정이 수행되지 않기 때문에 2회의 통신만으로 스마트미터에게 전력량을 안전하게 전송할 수 있도록 매 세션 변경되는 일회용 패스워드를 생성하여 스마트미터에게 인증 받는다.

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

- 기밀성 : 대칭키 암호 알고리즘을 통해 스마트미터의 정보 일회용 패스워드를 암호화 후 전송하여 기밀성을 제공한다.
- 무결성 : 스마트미터가 디바이스에게 전송할 때 그 데이터에 대한 키를 알 수가 없기 때문에 위·변조가 불가능하다. 또한 변경을 시도하게 되더라도 해쉬 값을 통해 검증이 가능하다.
- 상호인증 : 생성한 OTP값이 해쉬테이블에 속해있지 않으면 디바이스를 인증할 수 없고, 스마트미터는 자신이 측정한 카운터 값과 디바이스의 카운터값을 일치하여야 하기 때문에 상호인증이 제공된다.
- 통신횟수 : 등록단계를 포함한 인증단계는 4번의 통신으로 인증을 수행한다. 등록단계는 한 번의 등록 후 다시 수행되지 않기 때문에 주기적인 데이터 전송 시 인증 단계만 수행된다.

<표 1> 제안방식 분석

구분	S/Key[4]	시간동기화[5]	제안방식
기밀성	제공	제공	제공
무결성	제공	제공	제공
상호인증	×	×	○
	제공안함	제공안함	세션키를 통한 상호인증 제공
임의성	×	×	○
	순차적사용	순차적사용	랜덤수기반
통신횟수	5	1	4

○:제공, 좋음 △:보통, ×:제공안함, 나쁨
E:대칭키연산, U:공개키연산, H:해쉬연산

6. 결론

기존의 폐쇄적인 단 방향 전력망에 외부와의 양방향 통신기술을 접목하여 실시간 양방향 정보교환 및 에너지 효율을 최적화하는 스마트그리드 기술의 개발이 활발하게 이루어지고 있다. 스마트그리드는 각 가정의 디바이스에서 사용한 전기를 스마트미터에서 측정하여 MDMS에게 전송하여 전력효율성을 극대화하고 있다. 이에 각 가정에서 사용한 전력량을 스마트미터는 정확하게 측정해야 할 필요가 있다. 그러나 보안위협의 증가로 인해 타 가정에서 사용하고 있는 디바이스의 접근이 가능해 짐에 따라 다양한 공격기술들이 등장하고 있다.

따라서 본 논문은 시간값을 이용하여 임의성을 강화시킨 일회용 패스워드 기술을 기반으로 각 가정의 디바이스를 스마트미터에서 인증하고 전력량을 측정하는 방식을 제안하였다. 향후 스마트미터에서 안전하게 MDMS로 전력량을 전송하는 연구가 진행되어야 할 것으로 사료된다.

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] Neil M. Haller, "The S/Key One-Time Password System", RFC 1760, 1995.02

[5] 강철오, 박중길, 홍순좌, 배병철, 박봉주, "시간을 이용한 효율적인 일회용 패스워드 및 시간 교정 알고리즘", 한국 통신학회 논문지, Vol.27, No.11C, 2002.4