제36회 한국정보처리학회 추계학술발표대회 논문집 제18권 제2호(2011. 11)

스마트그리드 환경에서 스마트미터와 디바이스간 안전한 인증기술 연구

장유종, 고 웅, 곽 진
순천향대학교 정보보호학과
e-mail : yjjang@sch.ac.kr, wgo@sch.ac.kr, jkwak@sch.ac.kr

A Study on Authentication Scheme for Device and Smartmeter in Smart Grid Environment

You-Jong Jang, Woong-Go, Jin Kwak
Dept of Information Security Engineering, SoonchunhyangUniversity

요 약

스마트그리드는 기존의 전력망에 디지털 시스템을 결합함으로써, 전력망의 안정성을 높이는 동시에 신재생 에너지의 활용 및 전력 사용량 분산 등과 같이 전력망의 효율성을 끌어올리는 기술이다. 이 같은 기술은 전력공급원과 각 가정에 연결되어 있는 스마트미터와의 실시간 통신을 통해 전력 데이터를 수집하여 이루어진다. 이렇게 수집된 전력데이터들은 기존의 정보통신기술을 사용하여 전송하고 있다. 이러한 이유로 스마트그리드 환경은 기존의 정보통신기술의 취약점뿐만 아니라 스마트그리드 환경에만 적용되는 보안위협이 예상된다. 따라서 본 논문에서는 이러한 보안위협 중 하나로 전력공급원과 실시간 통신을 하는 스마트미터와 각 가정의 디바이스들 간의 인증기술에 대하여 제안한다.

1. 서론

현대 사회에서는 산업의 발달, 인구 증가로 더 많은 에너지 수요를 요구하고 있다. 또한 악화되어 가는 환경 문제로 에너지 사용절감 및 관리에 관한 연구를 하는 저탄소 녹색 성장 기술이 차세대 기술로 떠오르고 있다. 이러한 차세대 기술 중 스마트그리드는 에너지를 절약하고 효율적으로 소비하여 환경오염 및 에너지낭비를 최소화 시키는 대표적인 기술로 많은 연구가 진행되고 있는 중이다.

스마트그리드 환경에서는 스마트미터를 통한 실시간으로 사용되는 에너지를 분석 및 예측하여 에너지를 효율적으로 분배할 수 있다[1]. 따라서 본 논문은 스마트그리드환경에서 각 가정의 디바이스들과 스마트미터와의 안전한 인증기술에 대하여 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 스마트그리드와 스마트미터의 정의, 기존의 다양한 인증기술에 대해 분석하고, 3장에서는 분석된 인증기술들을 통하여 각 가정의 디바이스들과 스마트미터간의 안전한 인증기술을 제안한다. 4장에서는 보안 요구사항에 따른 제안방식을 분석하며, 마지막으로 5장에서는 결론을 맺는다.

2. 관련연구

2.1 스마트그리드

기존의 전력망은 일방향적으로 소비자에게 전력을 공급해주는 구조이다. 이러한 기존 전력망에서 스마트그리드는 IT기술을 융합하여 발전소와 송전·배전 시설, 전력 소비자를 양방향 통신이 가능하게 네트워크로 연결하여 수집된 전력정보를 통해 전력시스템을 효율적으로 운영하여 전력의 생산과 공급, 소비를 최적화하고, 에너지 효율을 최대화 할 수 있다. [1].

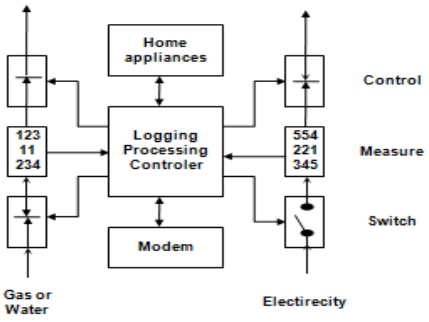
(그림 1) 스마트그리드 개요

2.2 스마트미터

전통적인 전력미터 시스템은 에너지의 사용량만을 측정하며, 한 달 또는 두 달에 한번 미터기에 기록된 전력량을 사람을 통하여 직접 체크한다. 그러나 스마트미터는 실시간 에너지측정 및 양방향 통신이 가능하도록 설계된 미터기이다. 스마트미터는 에너지공급업자 및 시스템 운영업자와 거대한 네트워크를 형성하며, 사용되는 에너지에 대하여 원격으로 요금이 청구된다. 또한 에너지공급업자는 유동적인 전력 요금 책정을 위해 스마트미터를 이용하여 실시간 또는 10분~1시간 간격으로 에너지 소비량을 수집하

여 기록한다. 스마트미터는 시간대별로 측정되는 전력 요금과 현재까지 사용한 에너지사용료에 대한 정보를 사용자에게 제공한다. 이러한 스마트미터는 플랫폼의 무결성을 위해 에너지 공급업자에 의해 플랫폼 상태가 관리되어야 한다. 따라서 에너지 공급업자는 스마트미터 내부의 기능적 문제가 생겼을 경우 펌웨어를 업데이트하거나, 갑작스러운 에너지공급중단 현상이 발생할 경우 저장되어 있는 임시 베터리로 전환시킬 수 있다. 이러한 스마트미터의 특징은 다음과 같이 요약할 수 있다.[2]

- 양방향 전력량 계량
- 메모리 무단접근 감지 기능
- 유효전력량(kWh), 무효전력량(kVrh) 계측
- 최대 수요전력 제한 기능
- 원격 관리 지원



(그림 2) 스마트미터 내부구조

2.3 스마트미터 보안 요구사항

스마트미터는 실시간 또는 일정한 간격으로 디바이스의 전력량을 전송받고 있기 때문에 빠른 속도로 인증을 수행하여야 한다. 이에 따라 인증기술에 대한 보안요구사항은 다음과 같다.[3]

- 기밀성 : 스마트미터를 통해 수집되는 데이터들은 매우 민감한 정보들을 포함하고 있다. 에너지 사용량을 악의적인 목적으로 사용하게 된다면 개인 프라이버시 노출과 같은 문제를 초래하게 된다. 이러한 데이터들은 통신 중간에 노출되더라도 데이터의 값을 유추하지 못해야 한다.

- 무결성 : 스마트미터를 통해 수집되는 데이터들은 에너지 사용량과 같은 과금정보를 포함하고 있다. 따라서 이러한 데이터들은 금전거래의 근거가 되므로 위조 및 변조되지 않아야 한다.

- 상호인증 : 스마트미터는 가정의 모든 가전기기와 연결되어 있다. 이러한 기기간의 인증이 제대로 이루어지지 않은채 통신을 하게 된다면 스마트미터 내부의 데이터 조작 잘못된 에너지 사용량 같은 문제가 초래할 수 있다.

- 경량화 : 스마트미터는 스마트그리드 환경에서 사용된다. 또한 실시간에 가깝게 각 디바이스들의 에너지 사용정보를 수집해야 하기 때문에 연산 속도가 빠르고 효율성이 높아야한다.

2.4 스마트미터 인증 프로토콜

이 절에서는 기존의 다양한 인증기술에서 스마트그리드 환경에서 스마트미터와 각 디바이스들 간에 적용할 수 있는 ID 기반 인증기술 및 PKI 기반 인증기술에 대하여 설명한다.

2.4.1 동적 ID기반 인증기술

본 방식은 원격사용자를 인증하기 위하여 동적 ID를 기반으로 연산량이 적은 XOR연산과 해쉬함수를 이용하여 인증을 수행하는 기술이다. 또한 시간 값을 사용하여 재사용 공격에 대응하고 있고, 기존의 검증 테이블을 이용하지 않으며 자유롭게 패스워드를 수정할 수 있는 특징을 가진다. 본 방식은 통신량이 등록단계 및 인증단계를 포함하여 3회로 적다는 장점이 있지만 비밀통신상에서 암호화 처리가 2회 있고, 해쉬연산 및 XOR 연산이 매우 많아 다수의 스마트미터에서 전송한 데이터를 서버에서 연산하여 처리하기 힘들다는 단점이 존재한다[4].

2.4.2 PKI 기반 디바이스 인증기술

PKI기반 디바이스 인증기술은 외부 클라이언트에서 홈네트워크를 컨트롤하기 위한 사용자 인증기술을 공개키 인증서를 이용하여 수행한다. 또한 인증서버에서 생성한 사설인증서를 이용하여 해당기기에 대한 권한을 브여함으로 허가받지 않은 사용자의 접근을 제어한다. 본 방식은 스푸핑 및 스니핑 공격, 재전송 공격 등에 안전성을 제공하고 있다. 그러나 통신 횟수가 많고 인증서 생성을 포함한 전송단계에서 연산량이 많아 스마트그리드환경에 적용하기 어렵다는 단점이 있다[5].

3. 향상된 스마트미터 인증 시스템

본 논문에서는 안전한 스마트그리드 서비스 환경을 구축하기 위하여 2장의 보안요구사항을 만족하는 스마트미터와 디바이스간 인증기술을 제안한다. 제안방식은 등록과정에서 공개키 암호 알고리즘을 사용하여 기존에 사용되고 있는 인증기술과는 다르게 비밀통신이나 사전키 공유 없이 스마트미터와 디바이스간 정보 교환이 가능하다. 또한 스마트그리드 환경 특징에 맞추어 경량화를 제공하기 위하여 실시간 통신이 이루어지는 인증 과정에서는 대칭키 암호 알고리즘을 사용하지 않고 XOR 연산과 해쉬함수 연산만을 통하여 디바이스를 인증하고 있어 경량화 된 인증기술을 제공하고 있다. 본 제안방식은 등록단계, 인증단계로 구분되며 각 단계의 수행절차는 다음과 같다.

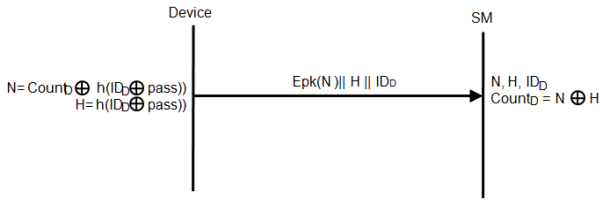
<표 1> 시스템 파라미터

기호	정의
*	각각의 개체(D : Device, SM : Smart Meter)
R_D	디바이스에서 생성한 랜덤 수
R_{SM}	스마트미터에서 생성한 랜덤 수
ID*	각각 개체의 디바이스의 ID
ID_{SM}	스마트미터의 ID
Count*	각각 개체의 카운터 값
T*	각각의 개체의 타임스탬프
SK	스마트미터에서 개인키
PK	스마트미터에서 공개키
h()	일방향 해쉬함수
H, S, N	보안 매개변수

3.1 등록단계

등록단계에서 디바이스에서는 초기 카운터 값과 디바이스의 아이디 및 디바이스 초기 설정시 입력하는 패스워드를 이용하여 N의 값을 생성한다. N의 값은 보안 매개변수로 이 후 타임스탬프 값과 함께 디바이스를 인증할 때 사용되게 된다.

스마트미터는 디바이스의 아이디와 카운터 값, 보안 매개변수 N값을 저장한다. ID 및 카운터 값은 N의 값을 확인 시 식별사로 사용한다. 등록단계는 다음과 같은 단계로 진행된다.



(그림 3) 등록 단계

Step1 : 디바이스에서는 초기 카운터 값을 설정, 저장하고 디바이스의 ID와 설정된 패스워드를 XOR 연산한다. XOR 연산된 값은 해쉬함수를 돌려 H값을 생성, 저장하고 카운터 값과 XOR 연산을 한다. H값은 이후 카운터 값을 연산하는 매개변수로 사용된다.

$$D : N = Count \oplus h(ID_D \oplus pass)$$
$$H = h(ID_D \oplus pass)$$
$$Count_D = Count$$

Step2 : 디바이스는 생성한 N의 값을 스마트미터의 공개키로 암호화 하고, 디바이스의 ID 값, 생성한 H 값을 연접하여 스마트미터에 전송한다.

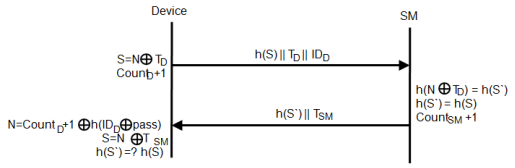
$$D \rightarrow SM : E_{PK}(N) \,||\, H \,||\, ID_D$$

Step3 : 스마트미터는 전송받은 데이터 중 개인키로 복호화하여 얻은 N값을 H값과 XOR 연산하여 카운터 값을 구하고 그 값을 스마트미터의 카운터 값으로 저장한다.

$$SM : D_{SK}(N)$$
$$Save : N,\ ID_D,\ H,\ Count_{SM}$$

3.2 인증단계

등록단계를 수행하고 나면 스마트미터에서는 디바이스의 아이디와 N의 값, 카운터 값을 저장하고 있다. 디바이스에서는 저장되어 있는 보안 매개변수 N을 통하여 보안 매개변수 S값을 생성하고, ID, 타임스탬프 값과 함께 전송한다. 이러한 방식은 디바이스와 스마트미터간 비밀정보를 노출 하지 않아 비밀성을 보장한다 또한 기존에 저장되어 있는 카운터 값 및 타임스탬프 값을 상호 비교하여 중간자 공격에 효과적인 대응을 할 수 있다. 또한 디바이스를 인증한 후 증가된 카운터 값을 통하여 스마트미터를 인증하는 상호 인증이 이루어진다. 이러한 인증 단계는 다음과 같은 단계로 진행된다.



(그림 4) 인증 단계

Step1 : 디바이스는 등록 단계시 저장한 N값과 타임스탬프 값을 XOR 연산하여 보안 매개변수 S값을 생성하고 저장되어 있는 카운터 값을 증가시킨다.

$$D : S = N \oplus T_D$$
$$Count_D+1$$

Step2 : 디바이스는 생성한 S값에서 해쉬 값을 추출하여 타임스탬프 값과 아이디를 연접하여 스마트미터에 전송한다.

$$D \rightarrow SM : h(S) \,||\, T_D \,||\, ID_D$$

Step3 : 스마트미터는 등록 단계에서 저장되어 있던 N값과 전송 받은 타임스탬프 값을 XOR 연산하여 해쉬 값을 추출하고 전송 받은 값 h(S)와 비교 하여 디바이스를 인증한다. 인증이 완료 되면 카운터 값을 증가 시킨다.

$$SM : h(N \oplus T_D) = h(S`) =? h(S)$$
$$count_{SM}+1$$

Step4 : 스마트미터는 증가시킨 카운터 값을 통하여 S`을 생성 하고 해쉬값을 추출하여 타임스탬프 값과 같이 디바이스에 전송한다.

$$SM : N` = Count_{SM}+1 \oplus h(ID \oplus pass)$$
$$S`=N` \oplus T_{SM}$$
$$SM \rightarrow D : h(S`) \parallel T_{SM}$$

Step5 : 디바이스에서는 전송 받은 h(S`)값과 저장되어 있는 증가된 카운터 값을 통하여 생성한 S값의 해쉬값을 비교 스마트미터를 인증을 한다.

$$D : N = Count_{D+1} \oplus h(ID_D \oplus pass)$$
$$S=N \oplus T_{SM}$$
$$D : h(S`) = h(S)$$

4. 제안방식 분석

본 장에서는 논문에서는 제안한 인증기술과 기존에 사용되는 인증기술들을 비교하여 스마트그리그 환경에 보다 적합한 인증기술에 대하여 분석한다. 기존 인증기술과 본 논문에서 제안한 인증 기술의 분석표는 <표 2>와 같다.

<표 2> 제안방식 분석

보안 요구사항	ID기반 인증 시스템	PKI기반 인증 시스템	제안 시스템
기밀성	제공	제공	제공
무결성	제공	제공	제공
상호인증	미제공	제공	제공
경량화	12H+2E	2H+3U	5H+1U
통신횟수	3	4	3

※ H : 해쉬함수, E : 대칭키 암호 알고리즘
U : 공개키 암호 알고리즘

ID기반 인증 방식은 동적 ID를 기반으로 경량화된 인증을 제공하고 있으나, 정보를 전송하는 통신과정 중 3번의 통신에서 2번의 통신이 비밀 통신으로 이루어지고 있다. 스마트그리드는 일반 통신상에서 이루어지기 때문에 이 인증 기술은 스마트그리드 환경에 부적합하다. 또한 스마트미터와 디바이스에 대한 상호 인증이 아닌 디바이스만 인증이 가능하여 보안성이 취약하다.

PKI기반 인증 방식은 공개키 암호 알고리즘을 사용하고 있어, 연산횟수는 대칭키 기반 인증기술보다는 작지만 연산량이 많고 통신 횟수가 ID 기반 인증기술보다 많아 경량성을 보장해야 하는 스마트그리드 환경에는 부적합하다.

제안방식의 경우 등록단계에서 공개키 암호 알고리즘을 사용하여 일반 통신상에서 사전 키 공유 없이도 비밀 통신이 가능하게 하였다. 이러한 공개키 암호 알고리즘은 등록단계에서만 사용되기 때문에 스마트미터와 디바이스간 실시간 상호인증에서는 해쉬함수와 XOR 연산만을 사용하여 인증이 이루어지기 때문에 안전성은 높이고 효율적인 경량화를 제공하고 있다. 또한 카운터 값과 타임스탬프 값을 통하여 재사용공격이나 중간자 공격에 대비하여 안전성을 높였다.

5. 결론

스마트그리드는 전력망의 효율성을 높일뿐만 아니라 안정성을 높이는 동시에, 그린 IT 기술을 이끌어나가는 선두주자이다. 현재 전력 시설망의 노후와 에너지 부족에 대비하기 위하여 많은 연구가 진행되고 있다. 스마트그리드는 각 가정의 디바이스에서 사용한 전기를 스마트미터에게 전송하여 취합한 전력량을 전력공급원에게 전송하는 방식으로 전력데이터를 측정하고 있다. 이러한 데이터가 노출 되거나 공격자에게 의하여 수정된다면 작게는 사용자의 개인정보가 노출되고 크게는 스마트그리그 시스템 전반에 피해를 줄 가능성이 있다. 본 논문에서는 이러한 공격에 대비한 프로토콜을 제안하였다. 연산성능이 제약된 스마트그리드의 환경에 맞추어서 등록과정에서만 공개키 암호를 사용하였다. 실시간으로 이루어져야 하는 통신과정에서는 XOR 연산과 해쉬함수 연산만을 사용함으로써 경량성을 만족하는 프로토콜을 설계하였다. 따라서 제안하는 프로토콜은 발전하는 스마트그리드 기술 중 스마트그리드 환경에서 스마트미터와 각 디바이스간의 인증을 할 수 있는 적합한 하나의 방법이 될 수 있다.

참고문헌

[1] 도윤미, 김선진, 허태욱, 박노성, 김현학, 홍승기, 서정해, 전종암, “스마트그리드 기술 동향 전력망과 정보통신의 융합기술,” 전자통신동향분석 제 24권 제 5호, 2009.10

[2] 남궁완, 조효진, 조관태, 이동훈, "스마트미터 보안 연구", 한국정보보호학회지 제 20권 제 5호, pp. 20~30, 2010,10

[3] 김홍기, 이임영, "스마트그리드환경에서 디바이스와 스마트미터간 ID기반 인증기술에 관한 연구" 한국정보보호학회논문지, 제 21권 제 1호, pp. 109~112. 2011. 6

[4] M.L. Das, A. Saxena, V.P. Gulati, "A Dynamic ID-based Remote User Authentication Scheme", Consumer Electronics, IEEE, 2004

[5] 이영구, 김정재, 김현철, 전문석, "PKI 기반 홈네트워크 시스템 인증 및 접근제어 프로토콜에 관한 연구", 한국통신학회 논문지 제 35권 제4호, pp. 592~598, 2010. 4