스마트 그리드 환경에서 프라이버시 보호를 위한 안전한 데이터 전송 프로토콜

고웅* · 곽진**

Secure Data Transaction Protocol for Privacy Protection in Smart Grid Environment

Woong Go* · Jin Kwak**

요 약

최근 저탄소 녹색성장이 세계적 관심사로 등장하면서 온실가스 배출을 최소화하기 위한 핵심으로 스마트 그리드라는 개념이 출현하게 되었다. 이와 같은 스마트 그리드는 전력 서비스의 효율성, 중요성, 신뢰성, 경제성, 지속성을 향상시키기 위해 모든 공급자와 소비자의 전력 생산, 공급, 소비 등을 기존 전력망과 정보통신기술을 접목하여 제공하는 시스템이다. 스마트 그리드를 통해 사용자는 자신의 집에서 사용하는 가전기기의 개별적 사용량 및 총 사용량을 실시간으로 알아볼 수 있으며, 전력 사용량이 최고에 달할 때에는 공급자가 특정 가전기기의 사용량을 제한하는 방식 등으로 효율적인 전력 공급을 수행할 수 있게 된다. 그러나 이와 같이 수집된 사용자의 정보가 노출될 경우, 전력 소비 양상, 생활 방식, 주거형태 등이 노출되는 심각한 프라이버시 문제가 발생하게 된다. 따라서 본 논문에서는 가정에서 전송되는 정보에서 어떠한 가전기기가 얼마만큼의 전력량을 사용했는지 알 수 없도록 보호하는 프로토콜을 제안한다. 본 제안 방식을 통해 전력회사라 하더라도 사용자의 패스워드 없이 어떠한 가전기기가 전력을 사용한지 알 수 없도록 한다.

ABSTRACT

Recently, it has been found that it is important to use a smart grid to reduce greenhouse-gas emissions worldwide. A smart grid is a digitally enabled electrical grid that gathers, distributes, and acts on information regarding the behavior of all participants (suppliers and consumers) to improve the efficiency, importance, reliability, economics, and sustainability of electricity services. The smart grid technology uses two-way communication, where users can monitor and limit the electricity consumption of their home appliances in real time. Likewise, power companies can monitor and limit the electricity consumption of home appliances for stabilization of the electricity supply. However, if information regarding the measured electricity consumption of a user is leaked, serious privacy issues may arise, as such information may be used as a source of data mining of the electricity consumption patterns or life cycles of home residents. In this paper, we propose a data transaction protocol for privacy protection in a smart grid. In addition, a power company cannot decrypt an encrypted home appliance ID without the user's password.

키워드

스마트 그리드, 스마트미터, 프라이버시 보호, 데이터 전송 프로토콜

Key word

Smart Grid, Smart Meter, Privacy Protection, Data Transaction Protocol

* 정회원 : 순천향대학교 (wgo@sch.ac.kr)
** 정회원 : 순천향대학교 (교신저자)

접수일자 : 2012. 06. 28
심사완료일자 : 2012. 07. 17

Open Access http://dx.doi.org/10.6109/jkiice.2012.16.8.1701

Ⅰ. 서 론

최근 산업과 IT 기술의 발전으로 인해 다양한 서비스가 제공되면서 지구온난화 등의 환경 파괴의 심각성이 크게 대두되고 있다. 이를 해결하기 위하여, 전 세계적으로 저탄소 녹색 성장을 목적으로 다양한 연구가 진행되고 있다. 저탄소 녹색 성장은 다양한 서비스를 위해 배출되는 이산화탄소의 양을 줄이고 환경 친화적이고 효율적인 자원의 사용을 목적으로 한다. 따라서 다양한 분야에 걸쳐 연구가 진행되고 있으며, 그 중에서도 전력 사용을 보다 효율적으로 관리하기 위한 연구로 스마트 그리드가 크게 주목받고 있다[1][2].

스마트 그리드는 전력 서비스의 효율성, 중요성, 신뢰성, 경제성, 지속성을 향상시키기 위해 모든 공급자와 소비자의 전력 생산, 공급, 소비 등을 기존 전력망과 정보통신기술을 접목하여 제공하는 시스템이다. 스마트 그리드의 핵심은 전력망에 정보통신기술을 합쳐 소비자와 전력 회사가 실시간으로 정보를 주고받는 것이다. 다시 말해, 사용자는 전력의 사용량을 실시간으로 확인할 수 있고, 전력 회사는 전력의 사용 패턴을 분석하여 시간에 따라 필요한 만큼만 전력을 생산하는 것이 가능해진다[3].

이와 같은 기술을 활용하기 위해서는 사용자 가정에서 사용되는 각 가전기기의 정보와 사용자의 정보 등이 필요하게 되며, 이를 정보통신기술을 통해 전력회사에 제공되게 된다. 그러나 정보통신기술을 적용함에 따라 기존 네트워크에서 존재하던 문제점들이 그대로 발생할 가능성이 증가하게 되었다 특히 전송되는 정보는 사용자의 생활 패턴 등의 프라이버시 정보가 포함되어 있으므로 안전성이 무엇보다 중요하다. 만약 악의적인 공격자가 사용자가 사용하는 가전기기 및 전력 소비량을 수집하여 분석한다면, 사용자의 생활 패턴, 주거형태 등을 분석해 낼 수 있다.

예를 들어, 사용자가 집에 있는 시간과 없는 시간을 파악하여 집에 불법적으로 침입한 후 물건을 훔쳐가는 등의 문제가 발생할 수 있다. 따라서 본 논문에서는 사용자의 프라이버시 보호를 위한 안전한 데이터 전송 프로토콜을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 스마트 그리드에 대하여 분석하고, 3장에서는 문제점을 도출한다. 그리고 4장에서는 안전한 데이터 전송 프로토콜을 제안하고, 5장에서 안전성 및 효율성을 분석한다. 마지막으로 6장을 결론으로 끝을 맺는다.

Ⅱ. 스마트 그리드

2.1. 스마트 그리드 개요

스마트 그리드는 전력망과 정보통신기술의 융합을 이용한 지능형 전력망으로 중전, 통신, 가전, 건설, 자동차, 에너지 등과 같은 유관 산업과의 시너지 기회를 제공할 수 있는 국가 단위의 녹색성장 플랫폼이라고 할 수 있다[1]. 이러한 스마트 그리드는 전 세계적으로 관심이 증가하고 있으며, 환경 구축을 위한 다양한 연구가 진행되고 있다.

기존의 전력망이 전력 공급자에 의한 일방적인 의사소통이 이루어졌다면, 스마트 그리드 환경에서는 정보통신 기술로 인해 전력 공급자와 소비자가 양방향으로 실시간 전력 정보를 교환할 수 있다. 따라서 전력 공급자와 소비자 사이에서 보다 효율적으로 전력 운영이 가능하다[4].

이와 같은 스마트 그리드는 전력 시스템과 제어 시스템 간의 상호연동을 위하여 AMI 통신 인프라를 구축하고 있으며, 이더넷 및 PCL 등과 같은 유선 통신 기술과 ZigBee, Wi-Fi 및 3GPP 등과 같은 무선 통신 기술을 사용하여 구성이 가능하다[5][6].

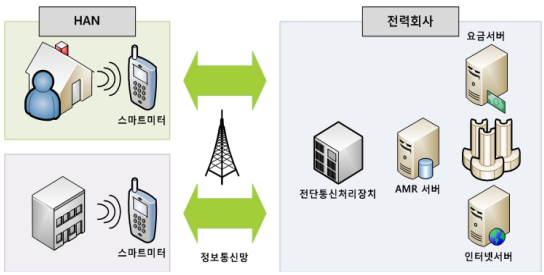

그림 1. 스마트 그리드 구조
Fig. 1 Smart Grid Structure

스마트 그리드 통신 네트워크는 몇 가지 서로 다른 서브시스템 네트워크로 구성되어 있다. 서브시스템

네트워크에는 SCADA(Supervisory Control and Data Acquisition), LMRS(Land Mobile Radio System), 무선, 마이크로웨이브, 광통신, 전용선 또는 교환선, RS-232/RS-485 시리얼 링크 네트워크, 유/무선 지역 네트워크와 같은 다양한 서로 다른 네트워크가 존재한다[7][8].

이와 같은 스마트 그리드 환경에 대한 관심이 증가하는 가운데 지난 2006년, IBM에서는 현재의 스마트 그리드와 거의 유사한 형태의 솔루션을 발표하고 공식적으로 출시한 사례도 있다[9].

2.2. 스마트 그리드 프라이버시

NIST의 CSWG(Cyber Security Working Group) 내 프라이버시 서브그룹에서는 프라이버시에 대해 개인정보 프라이버시, 개인 프라이버시, 개인행동 프라이버시, 개인 통신 프라이버시의 4가지로 구분하고 있다[10].

- 개인정보 프라이버시 : 특정 개인을 식별할 수 있는 개인정보에 대해 통제, 접근, 안전성 보장의 권리
- 개인 프라이버시 : 자기 신체의 무결성을 통제할 수 있는 권리
- 개인행동 프라이버시 : 특정 개인행동에 대한 사실을 기밀로 유지할 수 있는 권리
- 개인 통신 프라이버시 : 부당한 감시, 모니터링, 검열 없이 통신할 수 있는 권리

스마트 그리드 환경은 전력 소비자 유틸리티 사업자, 에너지 서비스 제공자 등의 이해 관계자들이 존재하는 복합구조로서, 실시간 전력사용량이 정보통신망을 통해 전송되어 수집, 저장, 유통, 공유 등이 가능하다.

이와 같은 정보는 사용자의 개인정보가 포함되므로 사용자의 습관 및 생활 방식 프로파일링이 가능하게 된다. 따라서 스마트 그리드에서 관리하는 사용자의 정보는 기존의 네트워크에서보다 더욱 민감하다고 할 수 있으며, 이를 통해 새로운 형태의 프라이버시 침해가 발생될 수 있다.

Ⅲ. 문제점 분석

3.1. 프라이버시 문제

스마트 그리드 환경에서 가장 많은 문제점으로 대두되고 있는 것은 사용자의 프라이버시 정보이다. 기존의 사용자의 신상정보와 전력사용량을 함께 수집하는 환경이므로, 두 가지 정보가 결합되어 특정 소비자의 생활 패턴 및 전력 소비 양상 등을 확인할 수 있게 된다.

이와 같은 정보는 단순 정보 노출뿐만 아니라 추가적인 피해를 발생시킬 수 있다. 특히, 사용자가 주로 전력을 사용하는 시간대를 확인하여 집이 비어있는지 확인한 후 직접 집에 침입하여 물품을 훔치는 등의 도난 사고가 발생할 수 있다. 또한, 사용되는 전력정보에 따라 사용자의 가정에 존재하는 가전기기의 종류 및 유형을 알 수 있게 된다. 다음 표는 전송되는 데이터에 따라 노출되는 프라이버시 정보를 나타낸다.

표 1. 프라이버시 정보
Table. 1 Privacy Information

데이터	노출 정보
에너지 사용정보	- 전력 사용 패턴 및 가전기기 사용 정보, 모니터링을 통한 가정 내 개인행동 및 활동 패턴, 행동 패턴 등의 사용자 프라이버시 정보 - 실시간 감시를 통해 가정 내 사람의 유무 확인
가전기기 정보	- 가정 내 사용되는 가전기기의 전력사용량을 통해 종류 및 유형 분류 가능

실제 MIT에서 개발한 NALM(Non-intrusive Appliance Load Monitor) 기술을 이용하여 실시간으로 전력사용량의 소비를 분석하고 이를 통해 가정 내 사용자의 전력 소비 패턴을 알 수 있으며, 가전기기의 종류 또한 분류할 수 있다[11][12]. 이 기술을 통해 특정 가정집의 전력 소비 패턴을 분석하면, 전력을 사용한 가전기기와 시간대를 알 수 있으며, 사람의 유무도 판단할 수 있다.

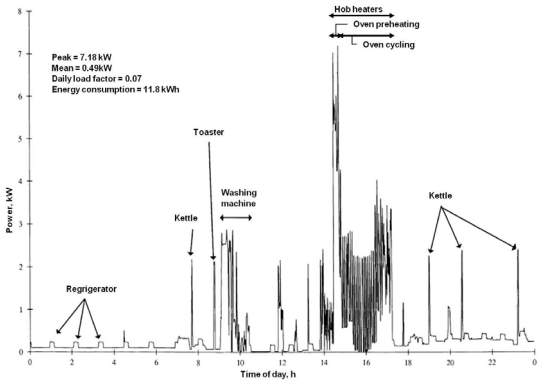

그림 2. 전력사용량 패턴 분석
Fig. 2 Analysis of Electricity Consumption Pattern

3.2. 불법적인 전력사용량 위변조

스마트 그리드 환경에서 가장 핵심이 되는 정보는 전력사용량이라 할 수 있다. 기존의 일방향성의 전력망에서도 전력사용량의 안전한 전송이 중요하였지만, 양방향 통신이 가능한 스마트 그리드 환경에서는 그 중요성이 더욱 높아졌다고 할 수 있다. 이는 단순히 전력회사가 전력사용량을 측정하는데 폐쇄망으로도 가능하여 외부의 침입에 대해서는 안전하였던 상황에 비해 개방적인 네트워크를 활용하는 스마트 그리드는 상대적으로 취약점이 많이 노출되어 있기 때문이다.

또한, 사용자가 전력사용량을 실시간으로 확인할 수 없으므로, 현재 전송되는 전력사용량을 알 수 없어 위변조가 쉽지 않다. 그러나 기존의 정보통신망과 동일한 네트워크 형태를 사용하는 스마트 그리드 환경에서는 사용자가 현재까지 사용한 전력사용량을 알기 쉬우므로 전력사용량을 불법적으로 변경하여 과금에 대한 이득을 취하려 할 수 있다. 마찬가지로 악의적인 공격자에 의해 사용자가 실제 사용한 전력사용량 보다 더 많이 전력사용량이 사용된 것처럼 변조되어 과금에 피해가 발생할 수 있다.

이와 같은 위변조는 기존 정보통신망을 그대로 이용함에 따라 문제점 또한 동일하게 발생할 수 있기 때문에 이를 이용하여 충분히 위변조가 가능하다.

Ⅳ. 제안 사항

본 논문에서는 스마트 그리드 환경에서 사용자의 생활 패턴이나 가전기기 및 전력사용량 등과 같은 가정 내 상황을 유추할 수 있는 프라이버시 정보를 보호하기 위한 데이터 전송 프로토콜을 제안한다.

이와 같은 사용자의 민감한 정보를 보호하기 위해서 사용자 ID, 가전기기 ID, 전력사용량을 암호화하여 전송한다. 또한, 전송되는 정보의 무결성을 검증하기 위한 해시값과 난수를 사용한다. 이를 통하여 악의적인 공격자가 전송되는 데이터를 도청하더라도 필요한 정보를 얻지 못하도록 구성한다.

제안하는 프로토콜은 등록단계, 전송 단계, 요청 단계의 3단계로 구성된다. 등록단계는 사용자와 전력회사간의 인증 정보를 등록하는 단계로써 네트워크를 이용하는 대부분의 서비스의 회원가입과 같은 단계를 의미한다.

전송단계는 사용자가 사용하는 가전기기의 전력사용량을 암호화하여 안전하게 전송하는 단계이다. 마지막으로 요청 단계는 가전기기별 전력사용량을 확인하거나 가정 내 모든 가전기기의 전력사용량을 확인하는 등에 필요한 요청을 수행하는 단계이다. 본 단계에서 전송되는 정보 역시 암호화되어 전송되며, 제3자 혹은 전력회사라 하더라도 가전기기의 종류 및 사용자의 정보를 알 수 없다.

다음 그림은 제안한 프로토콜의 기본 구조를 나타낸다.

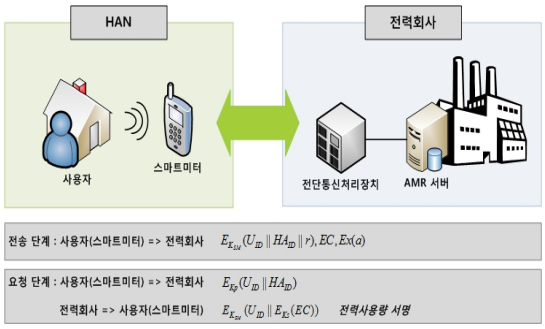

그림 3. 프로토콜 기본 구조
Fig. 3 Basic Structure of Proposed Protocol

4.1. 용어 정의

다음 표는 제안하는 프로토콜에서 사용되는 용어들의 표기법 및 정의를 기술한 것이다.

전력회사의 공개키(Kp)와 개인키(Ks)는 사용자의 신원을 위한 암호화와 정당한 전력회사가 전송한 전력 사용량이라는 것을 검증하기 위하여 사용된다. 또한, 프로토콜에서 사용되는 K_{SM}은 전력회사와 스마트미터 간에 사용되는 암복호화키로 최초 제작시에 사전에 삽입되는 키로, 상호간의 안전한 통신을 위하여 사용된다.

표 2. 용어 정의
Table. 2 Notation

표기법	정의
U_{ID}	사용자 ID
HA_{ID}	가전기기 ID
HA	가전기기 고유번호
EC	전력사용량
pw	사용자 비밀번호
r	난수값
$PRNG(\bullet)$	의사난수생성기
$H(\bullet)$	해시함수
$Ex(\bullet)$	XOR 연산
Kp	전력회사 공개키
Ks	전력회사 개인키
K_{SM}	암복호화키

4.2. 등록 단계

사용자와 전력회사 간의 양방향 통신이 수행되기 위해서는 먼저 사용자 인증 요소의 등록이 필요하다. 해당 정보는 접근하는 사용자가 정당한 사용자 인지 확인하고, 전송되는 정보의 무결성을 보장하기 위하여 사용된다. 이를 위해 사용되는 정보는 사용자의 ID(U_{ID})와 비밀번호(pw)이며 암호화된 상태로 전력회사에 전송된다. 이 후 전력회사는 신뢰할 수 있는 제 3 기관에게 사용자의 신원 확인을 의뢰하여 확인 후 정보를 등록한다. 본 단계는 기존의 네트워크를 이용하는 대부분의 서비스에서 제공하는 회원가입과 동일하다. 따라서 본 논문에서는 이에 대한 자세한 기술은 생략한다.

4.3. 전송 단계

전송단계에서는 사용자는 사용하는 가전기기 일련번호(HA)와 전력 사용량(EC)을 암호화하여 안전하게 전송된다. 이와 같은 보안성을 위하여 프로토콜에서는 사용자의 비밀번호(pw), 난수값(r), 해시함수($H(\bullet)$), XOR 연산($Ex(\bullet)$)을 사용한다. 사용자의 비밀번호는 사용되는 가전기기의 종류를 알아낼 수 없도록 하기 위해서 사용되며, 난수값과 해시함수는 송수신되는 데이터의 무결성을 검증하기 위해 사용된다. 그리고 XOR 연산은 전력사용량의 무결성을 검증하는 데 사용된다.

다음 그림은 전송 프로토콜을 나타낸다.

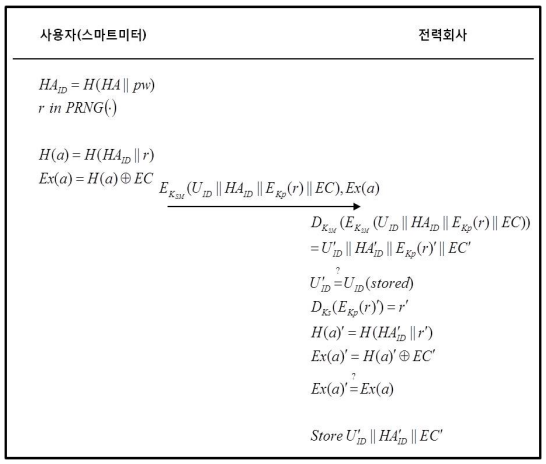

그림 4. 전송 단계 프로토콜
Fig. 4 Transaction Phase Protocol

사용자의 가정에서 전력사용량을 보내기 위해 가전기기 고유번호(HA)와 사용자의 비밀번호(pw)를 연접하여 해시값 HA_{ID}를 생성한다. HA_{ID}는 가전기기 ID로 전력회사에서 가전기기별 전력사용량을 확인하기 위한 정보로 활용된다. 그 후, 의사난수생성기로 난수값을 생성한다. 난수값은 가전기기 ID의 정보의 무결성을 검증하기 위하여 사용된다.

사용자(스마트미터)

$HA_{ID} = H(HA \| pw)$
$r \in PRNG(\bullet)$

생성된 난수값은 해시값과 함께 연접하여 해시값 $H(a)$를 생성한다. 이 해시값과 전력사용량을 XOR 연산하여 $Ex(a)$ 값을 생성한다. 이 값은 전력사용량의 무결성을 검증하기 위하여 사용된다.

사용자(스마트미터)

$H(a) = H(HA_{ID} \| r)$
$Ex(a) = H(a) \oplus EC$

마지막으로 등록단계에서 입력한 사용자 ID(U_{ID})와 가전기기 확인정보(HA_{ID}), 난수값(r), 전력사용량(EC)을 암복호화키(K_{SM})로 암호화하고, 전력사용량의 무결성 검증을 위한 값($Ex(a)$)을 함께 전력회사에 전송한다.

사용자(스마트미터) => 전력회사

$E_{K_{SM}}(U_{ID} \| HA_{ID} \| E_{Kp}(r) \| EC), Ex(a)$

전력회사는 전송받은 정보에서 암호문을 복호화 한다. 복호화된 정보 중 사용자 ID를 통해 최초 등록한 사용자 ID와 동일한지 확인한다. 그 후, 전력회사의 개인키를 이용하여 난수값을 복호화 한다.

전력회사

$D_{K_{SM}}(E_{K_{SM}}(U_{ID} \| HA_{ID} \| E_{Kp}(r) \| EC)$
$= U'_{ID} \| HA'_{ID} \| E_{Kp}(r)' \| EC'$
$U'_{ID} \stackrel{?}{=} U_{ID}(stored)$
$D_{Ks}(E_{Kp}(r)') = r'$

이 후, 복호한 가전기기 ID와 난수값을 해시하여 해시값 $H(a)'$을 생성하고, 해시값과 전력사용량을 XOR 연산하여 $Ex(a)'$을 생성한다. 이렇게 생성된 $Ex(a)'$을 전송받은 값과 비교하여 전력사용량의 무결성을 검증한다. 모든 검증이 완료되면, 전력회사는 사용자 ID(U_{ID}'), 가전기기 ID(HA_{ID}'), 전력사용량(EC')을 연접하여 저장한다.

전력회사

$H(a)' = H(HA'_{ID} \| r')$
$Ex(a)' = H(a)' \oplus EC'$
$Ex(a)' \oplus Ex(a)$

$Store\ U'_{ID} \| HA'_{ID} \| EC'$

4.3. 요청 단계

사용자가 자신이 원하는 특정 가전기기의 전력사용량을 알고자 할 때, 전력회사에게 이를 요청할 수 있다. 본 단계에서는 사용자가 전력사용량을 요청하기 위하여 사용자 ID(U_{ID})와 가전기기 ID(HA_{ID})를 이용한다.

해당 정보는 전력회사의 공개키(Kp)를 통해 암호화하여 전력회사에 전송되며, 전력회사는 사용자의 정보를 통해 전력사용량을 검색한다. 검색된 전력사용량은 전력회사의 개인키(Ks)로 서명되어 사용자에게 전송된다.

다음 그림은 요청 프로토콜을 나타낸다.

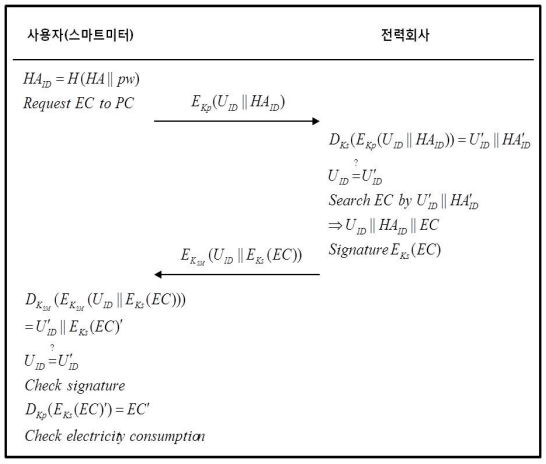

그림 5. 요청 단계 프로토콜
Fig. 5 Request Phase Protocol

먼저, 사용자는 원하는 가전기기 정보(HA)와 자신의 비밀번호(pw)를 이용하여 가전기기 ID(HA_{ID})를 생성한다.

사용자(스마트미터)

$$HA_{ID} = H(HA \| pw)$$

생성된 가전기기 ID를 사용자의 ID와 함께 전력회사의 공개키로 암호화하여 전송한다.

사용자(스마트미터) ⇒ 전력회사

$$E_{Kp}(U_{ID} \| HA_{ID})$$

전력회사는 전송받은 데이터로부터 개인키(Ks)를 이용하여 사용자 ID와 가전기기 ID를 복호화 한다. 복호화된 사용자 ID를 최초 등록된 사용자 ID와 비교하여 정당한 사용자로부터 전송된 정보인지 확인한다.

전력회사

$$D_{Ks}(E_{Kp}(U_{ID} \| HA_{ID})) = U'_{ID} \| HA'_{ID}$$
$$U_{ID} \stackrel{?}{=} U'_{ID}$$

비교 결과가 동일할 경우, 사용자 ID와 가전기기 ID를 통해 전력사용량을 검색한다. 이를 통해 검색된 전력사용량은 전력회사의 개인키로 서명한다. 서명을 통해 정당한 전력회사로부터 받은 정보라는 것을 확인하고, 불법적인 변경이 이루어지지 않았다는 것을 확인할 수 있다. 서명을 한 후에는 사용자 ID와 서명한 전력사용량을 암호화하여 전송한다.

전력회사

$$Search\ EC by\ U'_{ID} \| HA'_{ID}$$
$$\Rightarrow U_{ID} \| HA_{ID} \| EC$$
$$Signature\ E_{Ks}(EC)$$

전력회사 ⇒ 사용자(스마트미터)

$$E_{K_{SM}}(U_{ID} \| E_{Ks}(EC))$$

사용자는 전송받은 데이터를 통해 사용자 ID와 서명된 전력사용량을 복호화하고, 자신의 ID와 복호화한 ID를 비교한다. 이를 통해 자신이 요청한 정보라는 것을 확인하고 전력회사의 공개키로 전력사용량의 서명을 검증한다. 검증 결과가 동일하면, 최종적으로 사용자가 전력사용량을 확인한다.

사용자(스마트미터)

$$D_{K_{SM}}(E_{K_{SM}}(U_{ID} \| E_{Ks}(EC)))$$
$$= U'_{ID} \| E_{Ks}(EC)$$
$$U_{ID} \stackrel{?}{=} U'_{ID}$$
$$Verify\ signature$$
$$D_{Kp}(E_{Ks}(EC)') = EC'$$

V. 안전성 및 효율성 분석

3.1. 프라이버시 보호

현재 진행되고 있는 스마트 그리드 환경에서는 양방향 통신을 위하여 사용자의 정보와 전력사용량을 함께 전송하고 있다. 이와 같은 정보는 일정한 시간 간격으로 수집되어 저장되는데, 해당 정보를 통해 사용자의 생활 패턴, 행동 양식, 전력 소비 패턴 등을 분석할 수 있다. 또한 사용자가 집에 있는지 여부를 확인할 수 있어서 가정 내 침입 등의 피해로 이어질 수 있다.

본 논문에서 제안한 프로토콜에서는 사용자의 프라이버시를 보호하기 위하여 암호화된 데이터와 XOR 연산을 이용한다. 암호화 데이터는 전력회사의 공개키 및 개인키(Kp, Ks)와 스마트미터에 삽입된 암복호화키(K_{SM}), 사용자의 패스워드(pw)를 이용한다. 또한, 가전기기 ID와 난수를 이용하여 해시한 값과 전력사용량을 XOR 연산하여 $Ex(a)$ 값을 생성하고 이를 이용한다.

예를 들어 전송단계에서 공격자가 전송되는 정보 $E_{K_{SM}}(U_{ID} \| HA_{ID} \| E_{Kp}(r) \| EC)$, $Ex(a)$를 도청하여 사용자 정보를 알아내려고 한다면, 반드시 스마트미터에 최초 삽입된 암복호화키(K_{SM})을 알아야 한다. 만약 암복호화키를 알아낸다고 하더라도 복호화된 가전기기 ID(HA_{ID})에서 가전기기의 종류를 알 수 있는 가전기기 고유번호(HA)를 알아낼 수 없다. 이를 알기 위해서는 사용자의 패스워드가 필요하다. 그러나 이와 같은 암복호화키 및 사용자 비밀번호를 알아내기란 어려우므로 공격자에 의한 프라이버시 노출을 방지할 수 있다.

두 번째로 요청 단계에서 사용자의 정보를 알아내기 위해서는 전력회사의 비밀키(Ks)와 스마트미터의 암복호화키(K_{SM})을 알아야한다. 요청단계에서 전송되는 $E_{Kp}(U_{ID} \| HA_{ID})$는 전력회사의 공개키로 암호화되어 있으므로, 비밀키를 알지 못하면 복호화가 불가능하다.

또한, 복호화 한다고 하더라도 사용자의 비밀번호(pw)를 알지 못하면 가전기기 ID(HA_{ID})에서 가전기기 고유번호(HA)를 알아낼 수 없다. 마찬가지로 전력회사에서 사용자에게 전송되는 정보 $E_{K_{SM}}(U_{ID} \| E_{Ks}(EC))$에서 사용자의 ID를 알아내려고 해도 스마트미터의 암복호화키(K_{SM})가 필요하므로 프라이버시 보호가 가능하다.

3.2. 불법적인 전력사용량 변경 방지

제안하는 프로토콜에서는 전송되는 전력사용량(EC)를 보호하기 위하여 사용자의 비밀번호(pw), 난수값(r)과 XOR 연산, 스마트미터의 암복호화키(K_{SM}), 전력회사의 비밀키(Ks)를 이용한 서명을 이용한다.

전송단계에서 가전기기의 고유번호(HA)와 사용자의 비밀번호(pw)를 이용하여 가전기기 ID(HA_{ID})를 만들고 난수값(r)을 생성한다. 이 정보를 연접한 후 해시하여 $H(a)$값을 생성하고, 이를 다시 전력사용량과 XOR 연산하여 $Ex(a)$값을 생성한다. 이 정보는 전력사용량의 무결성을 검증하기 위하여 사용된다. 예를 들어 공격자가 전송되는 정보를 도청하더라도 스마트미터의 암복호화키(K_{SM})을 알지 못하면 암호문에서 전력사용량을 알아낼 수 없다. 따라서 임의의 변경이 불가능하다. 만약 공격자가 임의로 전력사용량을 변경하여 정보를 생성하더라도 스마트미터의 암복호화키가 다르므로 전력회사에서 정상적인 복호화가 수행되지 않아 검출이 가능하다.

또한 공격자가 스마트미터의 암복호화키(K_{SM})을 알아내어 전력사용량을 임의로 변경하더라도 무결성 검증을 위한 값($Ex(a)$)으로 전력회사에서 검출 가능하다.

- 공격자 : $D_{K_{SM}}(E_{K_{SM}}(U_{ID} \| HA_{ID} \| E_{Kp}(r) \| EC) = U'_{ID} \| HA'_{ID} \| E_{Kp}(r)' \| EC'$
- 전력사용량 변경 후, 다시 암호화 후 전송
  $E_{K_{SM}}(U'_{ID} \| HA'_{ID} \| E_{Kp}(r) \| EC_A), Ex(a)$
  A: 공격자
- 전력회사에서 복호화 후, 무결성 검증 값($Ex(a)'$) 생성
  $Ex(a)' = H(a)' \oplus EC_A$
- 무결성 검증 값 비교
  $Ex(a) \neq Ex(a)'$

이와 같이 공격자가 전력사용량을 임의로 변경하여도 전력사용량 검증 값이 다르므로 불법적인 변경을 탐지할 수 있다.

두 번째로 요청단계에서 전력회사에서 사용자에게 보내는 전력사용량을 변경하고자 할 때에는 스마트미터의 암복호화키(K_{SM})과 전력회사의 개인키(Ks)를 알아야 한다. 만약 공격자가 스마트미터의 암복호화키를 알아낸다고 가정하더라도 사용자 ID와 서명된 전력사용량 정보만 알 수 있다. 또한, 어떠한 가전기기의 전력사용량이 전송되는지는 알 수 없다. 또한 임의로 전력사용량을 변경하려고 하더라도 전력회사의 서명값을 만들 수 없으므로 공격이 불가능하다.

Ⅵ. 결 론

프라이버시에 대한 문제는 대부분의 네트워크를 활용하는 환경에서 반드시 해결해야 하는 문제이다. 특히, 양방향 통신을 통해 보다 효율적이고 유용하게 전력을 사용하기 위한 스마트 그리드 환경에서는 무엇보다 중요하다고 할 수 있다.

스마트 그리드에서는 전력을 효율적으로 관리하기 위해서 필수적으로 사용자의 정보가 이용되며, 이를 통해 함께 수집되는 전력사용량을 체계적으로 관리할 수 있다. 마찬가지로 사용자 역시 자신이 사용하는 전력사용량을 실시간으로 확인하고 효율적으로 활용할 수 있다.

그러나 기존의 정보통신기술이 적용된 네트워크를 활용함에 따라 이와 같은 정보가 노출될 가능성이 존재한다. 스마트 그리드에서 활용되는 개인정보와 전력사용량이 결합하게 되면, 사용자의 생활 패턴, 전력 사용

패턴, 행동 패턴, 가전기기 유형, 가정 내 사람의 유무 등 단순한 정보 노출 문제만 아니라 침입, 도난 등의 물리적 피해가 발생 할 수 있는 분석이 가능하게 된다. 따라서 프라이버시 정보의 노출을 방지하기 위한 기술이 필요하다.

이에 본 논문에서는 사용자의 프라이버시 보호를 위하여 스마트 그리드 환경에서의 안전한 데이터 전송 프로토콜을 제안하였다. 제안된 프로토콜은 프라이버시 문제를 해결하기 위하여 전송되는 정보를 암호화하고, 전력사용량과 사용자의 정보가 공격자에게 노출되어도 실제 정보를 알 수 없도록 구성하였다.

제안된 프로토콜을 통해 스마트 그리드 환경에서 사용자의 프라이버시를 보호하고 안전성을 향상시킬 수 있을 것으로 기대한다.

참고문헌

[1] H.Tai and E.O.Hogain, "Behind the Buzz [In My View]," *IEEE Power and Energy Magazine,* vol.7, no.2, pp.87 – 92, 2009.

[2] R.M.Anthony and L.E.Randy, "Smart Grid Security Technology," *Innovative Smart Grid Technologies (ISGT),* pp.1 – 6, 2010.

[3] NIST, *Guidelines for Smart Grid Cyber Security vol. 1, Smart Grid Cyber Security Strategy,* DRAFT NISTIR 7628, pp.1 – 236, 2010.

[4] 이건희, 서정택, 이철원, "스마트그리드와 사이버 보안", 한국통신학회지, 제27권, 제4호, pp.23-30, 2010.

[5] National Energy Technology Laboratory, *Appendix B1: A systems view of the modern grid integrated communications v2.0,* 2007.

[6] 전용희, "스마트 그리드의 취약성, 특성, 설계 원칙 및 보안 요구사항 분석," 정보보호학회지, 제20권, 제3호, pp.79-89, 2010.

[7] W.Wang, Y.Xu and M.Khanna, "A Survey on the Communication Architectures in Smart Grid," *Computer Networks,* vol.55, no.15, pp.3604 – 3629, 2011.

[8] S.D'Antonio, L.Coppolino, I.A.Elia and V.Formicola, "Security Issues of a phasor data concentrator for smart grid infrastructure," *Proc. 13th European Workshop on Dependable Computing,* pp.3 – 8, 2011.

[9] F.Sun, M.Lei and C.Yang, *Establishing Smart Power Grid and Innovating Management Method-A New thought of the Development of Electric in China,* IBM Corp, 2006. Available: http://www-900.ibm.com/cn/services/bcs/iibv/industry/utilities.shtml.

[10] NIST, *Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy,* DRAFT NISTIR 7628, pp.1-236, 2010.

[11] S.Drenker. "Nonintrusive Monitoring of Electric Loads," *IEEE Computer Applications in Power,* vol.12, no.4, pp.47-51, 1999.

[12] E.L.Quinn, *Smart Metering and Privacy: Existing Laws and Competing Policies,* Colorado Public Utitlies Commision, 2009. Available at SSRN: http://ssrn.com/abstract=1462285 or http://dx.doi.org/10. 2139/ssrn.1462285, (2009)

저자소개

고웅(Woong Go)

2002～2008년 : 순천향대학교 정보보호학과 공학사
2008～2010년 : 순천향대학교 정보보호학과 공학석사
2010～ 현재 : 순천향대학교 정보보호학과 박사과정
※관심분야 : 스마트 그리드 보안, 클라우드 컴퓨팅 보안, 융합 보안, 개인정보보호

곽진(Jin Kwak)

1994～2006년 : 성균관대학교 전자공학과(공학사, 공학석사, 공학박사)
2006～2006년 : 일본 큐슈대학교 방문연구원
2006～2006년 : 일본 큐슈시스템 정보기술연구소 특별연구원
2006～2007년 : 정보통신부 개인정보보호기획단 개인정보보호팀 통신사무관
2007～2009년 : 정보통신연구진흥원 집필위원
2007～ 현재 : 순천향대학교 정보보호학과 교수
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, 순천향BIT 창업보육센터 센터장, 순천향대학교 중소기업산학협력센터 센터장

※관심분야 : 암호프로토콜, RFID 시스템 응용보안, 개인정보보호, 정보보호제품평가, 클라우드 컴퓨팅보안