한국항행학회 논문지 제16권 제4호 2012년 8월

ID 기반 키 분배 기법을 활용한 전력사용량 정보 전송 프로토콜

Electricity Consumption Information Transmission Protocol with ID-based Key Distribution Method

정수영*, 곽 진**

Su-Young Jung*, Jin Kwak**

요 약

최근 기존의 단방향 전력 시스템을 개선하여 안정적인 전력공급, 효율적인 에너지 관리 등을 가능하게 하는 스마트그리드가 관심을 받고 있다. 전력선통신(PLC : Power Line Communication)기술을 활용한 스마트그리드 환경은 각 가정의 PLC 모듈에서 수집한 정보를 데이터전송장치(IRM : Integrated Regional Manager)에 전송하고, 다시 그 정보를 전력서버로 전송한다. 이러한 통신 과정에서는 기존의 IT환경에서 발생하는 보안위협을 포함한 소비자의 개인정보유출, 전력망 마비 등의 다양한 문제가 발생할 수 있다. 그러므로 본 논문에서는 전력사용량 정보 전송과정에서 발생할 수 있는 보안위협에 대응하기 위해 ID 기반 키 분배 기법을 활용한 전력사용량 정보 전송 프로토콜을 제안한다.

Abstract

Recently, smartgrid has interested in enable to existing electrical grid to supplying stably and efficient energy management. Smartgrid environment using PLC is transmit PLC module collected electricity consumption information in each house from PLC module to server. This communication process can occurred security threats such as personal information leak of consumer, electrical grid paralysis. In this paper, we propose efficient electricity consumption information transmission protocol with ID-based key distribution method for respond to security threats.

Key words : Smartgrid, ID-based Key Distribution, Electricity Consumption Information Transmission

I. 서 론

스마트그리드는 기존의 전력망에 IT기술을 융합한 형태로 신재생에너지의 효율적 활용, 안정적인 전력 공급 등의 장점을 갖는 시스템이다[1]. 이와 같은 장점은 소비자와 전력 공급자간의 양방향 통신을 통해 가능하다. 스마트그리드를 구성하는 통신 기술은 전력선통신 PLC, 무선 통신기술인 ZigBee, 광케이블 통신으로 이루어져 있다. 그 중에서 PLC는 기존의 전력선(90~240V.60Hz)에 통신 신호를 결합하여 데이터를 송·수신하는 통신방식을 말한다. 9~450kHz 대역을 사용하여 수 kbps급 통신 속도를 실현하는 협대역 PLC, 1.7~30MHz 대역을 사용하여 수 Mbps에서 100Mbps급의 통신을 가능하게 하는 광대역 PLC 등

* 순천향대학교 정보보호학과 정보보호응용및보증연구실(ISAA Lab, Department of Information security Engineering, Soonchunhyang University)
** 순천향대학교 정보보호학과(Department of Information security Engineering, Soonchunhyang University)
· 제1저자 (First Author) : 정수영 · 교신저자(Corresponding Author) : 곽진
· 투고일자 : 2012년 7월 16일
· 심사(수정)일자 : 2012년 7월 16일 (수정일자 : 2012년 8월 23일)
· 게재일자 : 2012년 8월 30일

으로 나눌 수 있다. 또한 기존의 전력시설을 활용하기 때문에 새로운 통신망을 구축하는 것보다는 비용 측면에서 효율적이라 할 수 있고, 단일 인프라를 통하여 음성, 영상, 데이터 등을 쉽게 통합하여 서비스를 제공할 수 있게 된다[2].

스마트그리드 환경은 인터넷을 이용한 공개망과 기존의 전력망을 융합한 형태이기 때문에 IT환경에서 발생 가능한 보안위협들이 동일하게 발생할 수 있다. 특히 각 가정에 있는 PLC 모듈을 통해 수집된 정보가 IRM을 거쳐 전력서버로 전송되는 과정에서 발생할 수 있는 보안위협들에 대한 대책이 필요하다[3]. 전송되는 정보는 전력사용량 정보, 소비자 정보 등을 포함하고 있기 때문에 이러한 정보가 유출될 경우에는 전력사용량 조작, 전력사용요금 조작, 개인정보유출 등의 문제가 발생할 수 있다[4],[5]. 따라서 전력사용량 정보가 전송되는 과정에서 정보의 조작 및 유출에 대한 보안위협에 대응이 필요하다.

본 논문에서는 원격 검침 보안 프로토콜(SSMP : Secure Smart Metering Protocol)의 문제점을 개선하기 위해 ID 기반 키 분배 기법을 활용한 전력사용량 정보 전송 프로토콜을 제안한다[6],[7].

본 논문의 구성은 다음과 같다. 2장에서는 SSMP에 대하여 간략하게 설명하고, 보안취약점을 분석한다. 3장에서는 전력사용량 정보가 보안위협으로부터 안전하기 위한 보안 요구사항에 대해 분석하고, 4장에서는 PLC 모듈-IRM-전력서버 간의 안전한 전력사용량 정보 전송을 위한 ID 기반 기 분배 기법을 활용한 전력사용량 정보 전송 프로토콜을 제안한다. 5장에서는 제안한 프로토콜의 안전성과 효율성에 대하여 분석하고, 마지막으로 6장에서는 결론을 맺는다.

Ⅱ. 관련연구

2-1 SSMP

SSMP는 인증서 발급, 키 분배, 전력사용량 정보 전송단계로 나눠 안전하게 전력사용량 정보를 전송하는 프로토콜을 제안하고 있다. 다음 그림 1은 SSMP 구조를 나타낸 것이다[8].

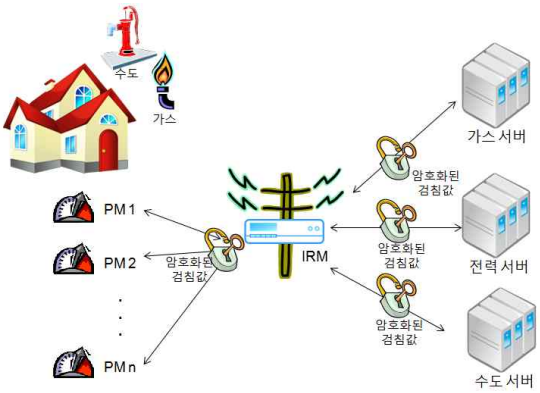

그림 1. SSMP 구조
Fig. 1. Structure of SSMP

SSMP는 각 가정의 PLC 모듈, IRM, 전력서버 간의 전력사용량 정보 전송에 대한 프로토콜이다. 이 프로토콜의 특징은 사전에 제조사가 공개키와 개인키 쌍을 분배하고, 이 키 쌍을 이용하여 PLC 모듈-IRM- 전력서버 간의 통신에서 필요한 키를 공유한다[9],[10].

그림 2는 SSMP의 키 분배 단계이다 이 단계에서는 인증서를 이용하여 IRM과 PLC 모듈을 인증하고 전력사용량 정보 전송 단계에서 사용할 키를 PLC 모듈-IRM-전력서버 간에 분배한다. 각 전송 과정에서 전송되는 값의 무결성을 보장하기 위해 개인키를 이용한 서명을 사용한다.

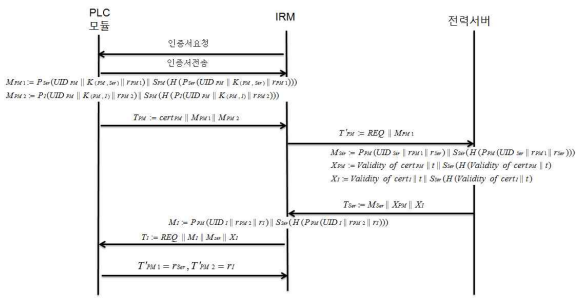

그림 2. SSMP 키 분배 단계
Fig. 2. Key distribution phase of SSMP

그림 2에서 전력사용량 정보를 암호화할 키 뿐만 아니라 각 개체를 인증하기 위해 필요한 값 또한 분배한다.

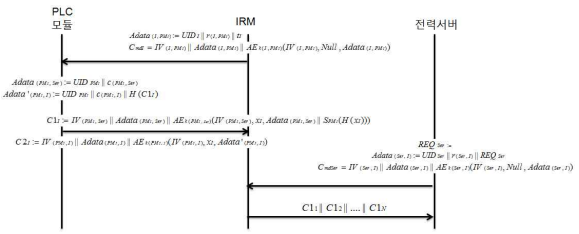

그림 3. SSMP 전력사용량 정보 전송 단계
Fig. 3. Electricity consumption information transmission phase of SSMP

전력사용량 정보 전송 단계에서는 서로 분배한 값을 활용하여 각 개체를 인증하고 전력사용량 정보를 전송한다. 이 단계의 특징은 IRM이 전력사용량 정보를 PLC 모듈로부터 전송받아 데이터 블록을 생성하고, 이 데이터 블록을 전력서버로 전송하는 특징을 갖고 있다. 이 과정에서 전력사용량 정보는 세션이 종료 될 때까지 동일한 키를 이용하여 전력사용량 정보를 암호화한다.

2-2 SSMP 문제점 분석

기존의 SSMP는 PLC 모듈-IRM-전력서버 간의 키 분배 과정에서 전력사용량 정보를 전송하기 위해 암호화할 때 이용하는 키를 공개키 기반 구조를 이용하여 분배한다. 또한 PLC 모듈-IRM-전력서버 간의 통신 과정에서 전송하는 값에 대한 무결성을 보장하기 위해 전송하는 객체가 자신의 개인키를 이용하여 서명을 한다. 이와 같이 공개키 기반의 인증 방식을 사용할 경우 안전성은 높지만 연산량이 커지게 된다.

전력사용량 정보를 전송하는 단계에서는 전력사용량 정보를 IRM이 PLC 모듈로부터 전송받아 데이터 블록을 생성하여 전력서버로 전송 한다. 이 데이터 들은 모두 같은 키로 전력사용량 정보를 암호화한다. 만약 이 키가 노출될 경우 데이터 블록에 있는 모든 전력사용량 정보가 유출될 수 있다.

하지만 스마트그리드 환경은 일정한 시간 간격으로 각 가정에서 수집된 정보가 전력서버로 전송되기 때문에 전송과정에 대한 경량화가 요구되고 전력사용량 정보를 안전하게 전송해야 하므로 유출 및 변조 대한 대응방법이 필요하다.

Ⅲ. 보안 요구사항

• 기밀성 : 전력사용량 정보는 기밀성이 보장되어야 한다. 전력사용량 정보는 각 가정의 전력사용 정보를 담고 있기 때문에 분석할 경우 전력사용 패턴을 유추할 수 있고 이를 이용하여 다른 범죄에 이용할 가능성이 있다. 이를 위해서는 암호화에 이용하는 키는 분배 단계에서 제3자에게 노출되거나 키를 유추할 수 없도록 기밀성이 보장되어야 한다. 또한 PLC 모듈-IRM-전력서버 간의 키 분배 과정에서 IRM이 전력사용량 정보를 암호화하는 키를 유추할 수 없고 PLC 모듈과 전력서버만이 암호화키를 알 수 있도록 해야 한다.

• 전력사용량 정보 무결성 : 전력사용량 정보는 사용자의 정보, 전력사용 패턴, 금전적인 부분과 연관이 있기 때문에 무결성이 보장되어야 한다. 전력사용량 정보가 유출될 경우 실제 사용 전력량 보다 많거나 적게 변조되어 금전적인 문제가 발생하고, 전력사용량 정보에서 사용자의 전력사용 패턴을 분석하여 또 다른 범죄에 이용될 가능성이 있다.

• 상호인증 : PLC 모듈과 전력서버는 상호인증이 제공되어야 한다. PLC 모듈이 전력사용량 정보를 전송하기 위해서는 전력서버의 정당성 여부를 판별할 수 있어야 한다. 또한 전력서버는 각 PLC 모듈에서 전송되는 정보가 정당한 PLC 모듈에서 전송된 것 인지 판별할 수 있어야 한다. 상호인증이 제공되지 않을 경우 A의 전력사용량 정보가 B 또는 C로 전송되어 문제가 발생하거나 실제 사용량 보다 적거나 많게 조작된 정보를 전송받는 등의 문제가 발생할 가능성이 있다[11].

• 연산량 : 각 가정의 PLC 모듈은 일정한 시간을 간격으로 자신이 갖고 있는 정보를 전력서버로 전송하고, 전력서버는 한 번에 많은 양의 정보를 전송 받게 된다. 따라서 이렇게 많은 양의 정보를 한 번에 전송받을 때 연산량이 많을 경우 전력서버의 과부하 또는 장애가 발생할 수 있으므로 연산량을 줄이면서도 안전한 방법이 필요하다.

• 키 안전성 : 전력사용량 정보는 민감한 정보이기 때문에 공격자의 변조, 유출 등의 보안위협에 노출되어있다. 따라서 안전하게 전송하기 위해서는 암호화가 필요하다. 이와 같이 전력사용량 정보를 암호화하기 위해 사용되는 암호화키는 PLC 모듈과 전력서버만이 알 수 있도록 공유 되어야 한다. 또한 키가 갱신되지 않을 경우 공격자가 이전과정에서 얻은 키를 이용하여 복호화를 시도할 수 있으므로 키는 분배 후에 갱신이 될 수 있도록 해야 한다.

Ⅳ. 제안 프로토콜

본 장에서는 ID 기반 키 분배 기법을 활용한 전력사용량 정보 전송 프로토콜을 제안한다.

제안한 프로토콜은 등록 단계, 키 분배 단계, 전력사용량 정보 전송 단계로 구성된다. 등록 단계에서 저장한 값을 PLC 모듈과 전력서버 인증에 사용하고, 키 분배 단계에서 분배한 키를 전력사용량 정보 암호화키로 사용한다. 표 1은 제안한 프로토콜에서 사용하는 시스템 파라미터를 나타낸다.

표 1. 시스템 파라미터
Table 1. System parameter

계수	설명
ID_M	모듈의 ID
PW_M	모듈의 패스워드
y	전력서버의 비밀정보
x	전력사용량 정보
MAC_*	*의 MAC Address
R_*	*의 랜덤한 값
T_*	*의 타임스탬프
$h(\bullet)$	해쉬 연산
$\oplus$	XOR 연산
$\|\|$	연접 연산

4-1 등록 단계

PLC 모듈과 전력서버의 등록 단계이다. 이 단계는 PLC 모듈과 전력서버 사이의 물리적인 안전한 채널을 통해 이루어진다.

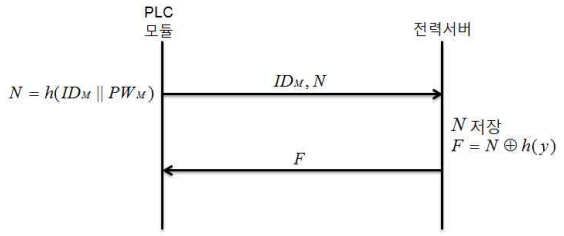

그림 4. 등록 단계
Fig. 4. PLC module registration phase

Step1 : PLC 모듈은 전력서버에 등록하기 위한 값인 $N = h(ID_M \| PW_M)$을 생성한다.

Step2 : PLC 모듈은 Step1에서 생성한 N과 자신의 ID인 ID_M를 전력서버에게 전송한다.

Step3 : 전력서버는 Step2에서 전송받은 값인 N을 이후 키 분배 단계와 전력사용량 정보 전송단계에서 PLC 모듈을 식별에 사용하기 위해 PLC 모듈의 ID와 함께 저장한다. 이후 전력서버는 키 분배 단계와 전력사용량 정보 전송단계에서 PLC 모듈과 전력서버의 인증에 이용하는 $F = N \oplus h(y)$를 생성한다.

Step4 : 전력서버는 Step3에서 생성한 F를 PLC 모듈에게 전송하고, PLC 모듈은 이 값을 저장한다.

4-2 키 분배 단계

PLC 모듈과 전력서버 간의 등록 단계를 통해 저장한 값을 활용하여 PLC 모듈-IRM-전력서버 간의 통신에서 PLC 모듈과 전력서버를 식별하고 전력사용량 정보 전송 단계에서 전력사용량 정보를 암호화하기 위한 암호화키를 분배한다.

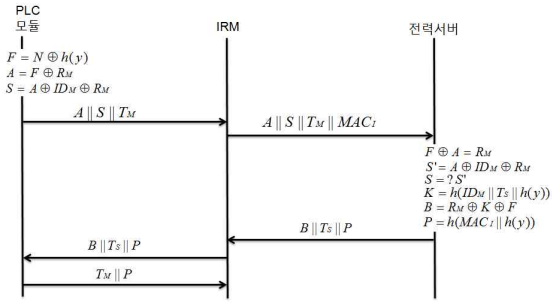

그림 5. 키 분배 단계
Fig. 5. Key distribution phase

Step1 : PLC 모듈은 랜덤한 값 R_M을 생성하고 이 값을 이용하여 R_M을 전력서버로 안전하게 전송하기 위한 $A = F \oplus R_M$를 생성한다. A를 생성한 후 전력서버에서 PLC 모듈의 인증을 위해 사용할 $S = A \oplus ID_M \oplus R_M$를 생성한다.

Step2 : PLC 모듈은 A, S, T_M을 전송한다.

Step:3 : IRM은 PLC 모듈로부터 전송받은 값과 자신의 MAC 주소인 MAC_I를 전송한다.

Step4 : 전력서버는 IRM으로부터 전송받은 T_M을 확인한다. 이상이 없을 경우 자신이 갖고 있는 F를 이용하여 A로부터 R_M을 얻는다. 이후 S'를 생성하여 Step3에서 전송받은 S값과 비교하여 일치 여부를 확인한다. 확인 후 이상이 없을 경우 전력사용량 정보 전송 과정에서 암호화키로 사용할 K를 생성한다. 이후 이 값을 이용하여 B를 생성하고, IRM으로부터 받은 MAC 주소를 이용하여 IRM 인증에 사용하는 P를 생성한다.

$$R_M = F \oplus A \tag{1}$$

$$S' = A \oplus ID_M \oplus R_M \tag{2}$$

$$S = S' \tag{3}$$

$$K = h(ID_M || T_S || h(u)) \tag{4}$$

$$B = R_M \oplus K \oplus F \tag{5}$$

$$P = h(MAC_I \oplus h(y)) \tag{6}$$

Step5 : 전력서버는 IRM에게 자신이 생성한 B, P, T_S를 전송한다.

Step6 : IRM은 전력서버로부터 전송받은 값을 다시 PLC 모듈에게 전송한다. 이후 PLC 모듈은 전송받은 T_S를 확인한다. 이후 R_M, F, B를 이용하여 K를 얻는다.

$$K = R_M \oplus B \oplus F \tag{7}$$

Step7 : PLC 모듈은 K를 얻은 후 IRM에게 T_M', P를 IRM에게 전송한다.

Step8 : IRM은 PLC 모듈로부터 전송받은 T_M'을 확인하고 이상이 없을 경우 P를 저장한다.

4-3 전력사용량 정보 전송 단계

키 분배가 완료되면 PLC 모듈과 전력서버는 각각 전력사용량 정보 전송 단계에서 사용하게 될 같은 키를 갖는다. 이 키를 이용하여 PLC 모듈은 전력사용량 정보를 암호화하고 키의 값을 알고 있는 전력서버만이 암호화된 값을 복호화 할 수 있다.

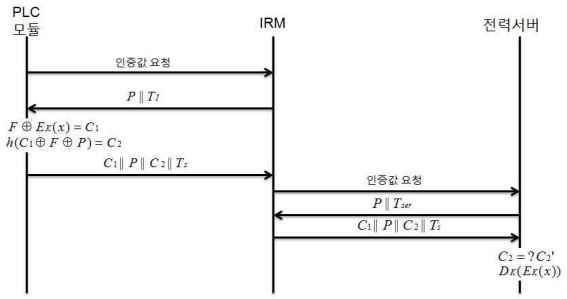

그림 6. 전력사용량 정보 전송 단계
Fig. 6. Electricity consumption information transmission phase

Step1 : PLC 모듈은 IRM에게 인증값 전송을 요청

한다.

Step2 : IRM은 PLC 모듈에게서 이전의 키 분배 단계에서 전송받은 P, T_I를 PLC 모듈에게 전송한다.

Step3 : PLC 모듈은 IRM으로부터 전송받은 P값의 정당성 여부를 확인한다. 확인 후 이상이 없을 경우 F와 앞의 키 분배 단계에서 얻은 K를 암호화키로 이용하여 전력사용량 정보 x를 암호화한 값인 C_1를 생성한다. 생성한 후 C_1과 F, P를 이용하여 C_2를 생성한다.

$$F \oplus E_K(x) = C_1 \tag{8}$$

$$h(C_1 \oplus F \oplus P) = C_2 \tag{9}$$

Step4 : PLC 모듈은 C_1, C_2, P, T_M을 IRM에게 전송한다.

Step5 : IRM은 PLC 모듈로부터 받은 값을 다시 전력서버로 전송한다. 전력서버는 이 값을 이용해 얻는다.

Step6 : 전력서버는 갖고 있는 F, P와 IRM으로부터 전송받은 C_1을 이용하여 C_2'을 생성한다. C_2'를 IRM으로부터 전송받은 C_2와 비교하여 동일할 경우 C_1에서 $E_K(x)$를 얻는다. $E_K(x)$는 키 분배 단계를 통해 갖고 있는 K로 복호화하여 전력사용량 정보 x를 얻고 해당 PLC 모듈의 정보로 저장한다.

$$C_2 = ? C_2' \tag{10}$$

$$D_K(E_K(x)) \tag{11}$$

Ⅴ. 안전성 및 효율성 분석

본 장에서는 ID 기반 키 분배 기법을 활용한 전력사용량 정보 전송 프로토콜의 안전성 및 효율성을 분석한다.

5-1 안전성 분석

• 기밀성 : 전력사용량 정보의 기밀성을 보장하기 위해서는 정보를 안전하게 전송해야 한다. 본 논문에서 제안한 프로토콜은 전력사용량 정보를 안전하게 전송하기 위해 PLC 모듈과 전력서버가 분배한 키 $K = h(ID_M \| T_S \| h(u))$를 이용하여 암호화 하였다. 키 K는 PLC 모듈과 전력서버가 사전에 안전한 경로를 통해 등록한 $F = N \oplus h(y)$를 이용하여 키 분배, 전력사용량 정보 전송 등에 활용한다. 이 F는 PLC 모듈과 전력서버만 알고 있고 전송 과정에서 직접적으로 노출되지 않으므로 기밀성이 보장된다.

• 전력사용량 정보 무결성 : 전력사용량 정보 x는 암호화키 $K = h(ID_M \| T_S \| h(u))$를 사용하여 암호화한다. 키 K를 분배하기 위해 전송하는 $B = R_M \oplus K \oplus F$를 이루고 있는 R_M은 PLC 모듈에서 생성되어 PLC 모듈과 전력서버만이 안전한 경로를 통해 공유한 $F = N \oplus h(y)$를 알아야 얻을 수 있다, 이와 같이 전력사용량 정보를 암호화키 K를 알아내기 어렵기 때문에 암호화된 전력사용량 정보 또한 복호화하기 어려워 전력사용량 정보의 무결성이 보장된다.

또한 PLC 모듈에서 전송 사용량 정보를 같은 암호화키를 K는 전력사용량 정보 별로 각각 다른 키 값으로 암호화하기 때문에 안전하다.

• 상호인증 : 전력서버는 등록 단계에서 저장한 $F = N \oplus h(y)$를 이용하여 $A = F \oplus R_M$에서 R_M를 얻는다. 이후 전력서버는 R_M을 이용하여 $S' = A \oplus ID_M \oplus R_M$를 생성하고 PLC 모듈에서 전송받은 $S = A \oplus ID_M \oplus R_M$와 비교하여 전력서버는 PLC 모듈을 인증한다.

또한 PLC 모듈은 전력서버에서 전송받은 $B = R_M \oplus K \oplus F$에서 자신이 전력서버로 전송한 R_M을 이용하여 $K = h(ID_M \| T_S \| h(u))$를 얻게 되므로, PLC 모듈이 전력서버를 인증하게 된다. 따라

서 본 논문에서 제안한 프로토콜은 상호인증을 제공한다.

• 키 안전성 : 본 논문에서 제안한 프로토콜은 전력사용량 정보를 전송하기 위해 암호화키로 사용되는 $K = h(ID_M || T_S || h(u))$는 해당 PLC 모듈의 ID와 타임스탬프 값, 전력서버의 비밀정보를 연접하여 해쉬 연산한 값으로 이루어져 있다. 이 값은 각 PLC 모듈의 ID로 이루어져 있기 때문에 PLC 모듈에 따라 달라지고 타임스탬프 값에 따라 달라지기 때문에 키의 안전성이 보장된다. 또한 전력서버의 비밀정보 $h(y)$는 전력서버 자신만이 알고 있기 때문에 PLC 모듈의 ID나 타임스탬프 값을 유추하여도 키 K를 만들 수 없다. 따라서 키에 대한 안전성이 보장된다.

5-2 효율성 분석

• 키 분배방식 : SSMP와 본 논문에서 제안한 프로토콜은 키 분배 방식에서 차이가 난다. SSMP는 공개키 기반 구조를 이용하기 때문에 인증서 발급, 관리 등이 필요하고 안전성은 높지만 연산량이 많다. 하지만 스마트그리드 환경에서는 각 가정에 있는 PLC 모듈로부터 정보가 전송되기 때문에 방대한 양의 정보가 한 번에 전력서버로 전송되고 일정한 시간 간격으로 지속적으로 통신을 하기 때문에 연산량의 경량화가 필요하다. 본 논문에서 제안한 프로토콜은 PLC 모듈이 자신의 ID와 패스워드를 이용하여 인증에 사용하기 때문에 별도의 인증서가 필요 없고 XOR 연산, 해쉬 연산을 이용하기 때문에 연산량을 줄일 수 있어 스마트그리드 환경에 적합하다.

• 연산량 : 연산량은 키 분배 단계와 전력사용량 정보 전송 단계로 나눌 수 있다. 표 2와 같이 키 분배 과정에서는 SSMP는 본 논문에서 제안한 프로토콜과 많은 연산량의 차이가 난다. 또한 전력사용량 정보 전송 단계에서도 비교하면 본 논문에서 제안한 프로토콜이 경량화된 것으로 보여진다. SSMP는 공개키 기반 구조를 사용하고 많은 대칭키 연산을 갖고 있어 이에 대한 경량화가 필요하다. 본 논문에서 제안한 프로토콜은 안전성 비교에서 볼 수 있듯이 SSMP에 준하는 안전성을 제공하면서 경량화된 것을 볼 수 있다.

표 2. 안전성 및 효율성 비교·분석
Table 2. Comparison·analysis of security and efficiency

구분		SSMP	제안사항
기밀성		O	O
전력사용량 정보 무결성		X	O
상호인증		O	O
		인증서를 활용한 인증	PLC 모듈의 ID/PW와 전력서버의 비밀정보를 통한 인증
키 안전성		X	O
키 분배 방식		공개키 기반 구조 이용	ID 기반 이용
연산량	키 분배	4U+6S	6H
	전력사용량 정보 전송	9E+1S+H	2E+2H

E: 대칭키 연산, U: 공개키 연산, H: 해쉬 연산, S:개인키 서명

Ⅵ. 결 론

스마트그리드는 기존의 폐쇄적이고, 단방향 통신망을 다양한 IT기술을 활용하여 양방향 통신이 가능하도록 했다. 안전상의 이유로 폐쇄적으로 운영하던 기존의 전력망에 인터넷을 이용한 공개망이 접목되면서, 기존에 인터넷을 이용한 공개망이 갖고 있는 보안위협이 동일하게 발생할 수 있다. 특히 전력사용량 정보를 전송하는 단계는 전력사용량 정보 조작, 유출 등의 위협이 발생할 수 있다. 따라서 본 논문에서 제안한 프로토콜은 전력사용량 정보가 PLC 모듈에서 전력서버로 변조, 유출 등의 보안위협으로 부터 안전하게 전송될 수 있는 프로토콜을 제안하였다.

또한 기밀성, 전력사용량 정보 무결성을 제공하고 키 안전성과 연산량을 향상시켜 기존의 프로토콜이 갖고 있는 문제점을 보완한 ID 기반 키 분배 기법을

활용한 전력사용량 정보 전송 프로토콜을 제안하였다.

본 논문에서 제안한 프로토콜은 향후 전력사용량 정보 전송에 관한 참고자료로 활용될 수 있도록 기대한다.

참 고 문 헌

[1] "클라우드 기반 스마트그리드를 위한 보안기술 연구," *한국인터넷진흥원*, 2010.12

[2] 홍정대, 천정희, 주성호, 최문석, "원격 검침용 PLC 기술 (KS X 4600-1 / ISO IEC 12139-1) 보안성 분석," *한국정보보호학회 논문지, 제21권 제4호*, pp. 65-75, 2011.02.

[3] NIST, Smart grid cyber security strategy and requirements. Aug. 2010. [Online]. Available: http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf

[4] 주성호, 임용훈, 박병석, 김태완, 김영현, 최문석, 이범석, "PLC 홈네트워크의 보안 취약성 및 대응방안 분석," *전력전자학술대회 논문집*, pp. 478-480, 2006.06.

[5] 정수영, 박대식, 곽진, "스마트그리드 환경에서 안전한 데이터 전송 프로토콜 연구," *한국 지식정보기술학회 2011 년도 추계학술발표대회 논문집*, 제5권 제2호, pp. 99-102, 2011.11.

[6] Khanh V. Nguyen, "Simplifying Peer-to-Peer Device Authentication Using Identity-Based Cryptography," *In proceedings of IEEE ICNS 2006,* pp. 43-47, July 2004.

[7] Joon Heo, Choong Seon Hong, Moon Seok Choi, Seong Ho Ju, Yong Hoon Lim, "Identity-Based Mutual Device Authentication Schemes for PLC System," *IEEE International Symposium on, Power Line Communications and Its Applications(ISPLC 2008).*

[8] 주성호, 최문석, 백종목, 임용훈, "PLC기반 원격검침인프라 보안시스템," *전력전자학회 2009 년도 추계학술대회 논문집*, pp. 256-258, 2009. 11.

[9] Sungwook Kim, Eun Young Kwon, Myungsun Kim, Jung Hee Cheon, Seong-ho Ju, Yong-hoon Lim, and Moon-seok Choi, "A Secure Smart-Metering Protocol Over Power-Line Communication," *IEEE TRANSACTIONS ON POWER DELIVERY*, vol. 26, no. 4, October 2011.

[10] S. Goldwasser, S. Micali, and R. Rivest, "A digital signature scheme secure against adaptive chosen message attacks", *SIAM J. Comput., vol. 17,* no. 2, pp. 281–308, April. 1988.

[11] Open Smart Grid Users Group, AMI System Security Requirements v1.01 Dec. 2008. [Online].Available: http://www.oe.energy.gov/DocumentsandMedia/14-AMI_System_Security_Requirements.pdf

정 수 영 (丁壽榮)

2012년 2월 : 순천향대학교 정보보호학과(공학사)
2012년 3월~현재 : 순천향대학교 정보보호학과 석사과정
관심분야 : 스마트그리드 보안, 클라우드 컴퓨팅 보안 등

곽 진 (郭鎭)

1994년~2006년 : 성균관대학교 학사, 석사, 박사
2006년 4월 : 일본 큐슈대학교 시스템정보공학부 방문연구원
2006년 8월~2006년 11월 : 일본 큐슈 시스템정보기술연구소 특별연구원
2006~2007년 : 정보통신부 개인정보보호기획단 개인정보보호팀 통신사무관
2007~현재 : 순천향대학교 정보보호학과 교수
2007~2009년 : 정보통신연구진흥원 집필위원
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, 순천향 BIT 창업보육센터 센터장, 순천향대학교 중소기업산학협력센터 센터장
관심분야 : 암호프로토콜, 응용시스템보안, 개인정보보호, 정보보호제품평가, 클라우드 컴퓨팅 보안, 스마트워크 등