석사학위 논문

분산형 에너지 시스템 환경에서 안전한 전력 수급을 위한 스마트 미터 인증 기법 설계

Design of Smart Meter Authentication System for Electricity Secure Supply and Demand in the Distributed Energy System

2017년 12월

숭실대학교 대학원

컴퓨터학과

정 하 규

석사학위 논문

분산형 에너지 시스템 환경에서 안전한 전력 수급을 위한 스마트 미터 인증 기법 설계

Design of Smart Meter Authentication System for Electricity Secure Supply and Demand in the Distributed Energy System

2017년 12월

숭실대학교 대학원

컴퓨터학과

정 하 규

석사학위 논문

분산형 에너지 시스템 환경에서 안전한 전력 수급을 위한 스마트 미터 인증 기법 설계

지도교수 전 문 석

이 논문을 석사학위 논문으로 제출함

2017년 12월

숭실대학교 대학원

컴퓨터학과

정 하 규

정 하 규의 석사학위 논문을 인준함

심 사 위 원 장 박 재 표 인

심 사 위 원 김 재 각 인

심 사 위 원 전 문 석 인

2017년 12월

숭실대학교 대학원

목 차

표 목 차

그 림 목 차

국문초록

분산형 에너지 시스템 환경에서 안전한 전력 수급을 위한 스마트 미터 인증 기법 설계

정 하 규
컴퓨터학과
숭실대학교 대학원

스마트 그리드는 기존의 전력망에 ICT 기술을 접목하여 제공되는 기술이다. 스마트 그리드 기술은 양방향 통신을 통하여 합리적인 의사결정이 가능하게 하였다. 하지만 스마트 그리드의 경우 ICT 기반의 네트워크를 통하여 정보를 공유하고 있기 때문에 악의적인 공격자에 의하여 취약하다는 약점이 있다.

따라서 본 논문에서는 스마트 그리드 환경에서 보안성을 제공하면서 악의적인 공격자를 통한 문제를 최소화 할 수 있는 인증 기법을 목적으로 한다. 제안하는 기법은 각 통신 구간별 공유되는 세션 키를 이용하여 상호인증을 수행한다. 상호인증과정에서는 각 통신 구간별 난수 값들과 해시 알고리즘 등을 통항 연산을 수행한다. 통신 구간 중에는 지속적으로 갱신되는 세션 키를 통하여 이후 전송되어지는 전력요청, 제어 정보 및 과금 정보에 대한 안전성을 높인다.

ABSTRACT

Design of Smart Meter Authentication System for Electricity Secure Supply and Demand in the Distributed Energy System

Chung, Hague

Department of Computer Science and Engineering

Graduate School of Soongsil University

Smart grid is technology provided by connecting existing power grid with ICT technology. Smart grid technology made it possible to make rational decision-making through two-way communications. However, as smart grid shares information through ICT-based network, it is vulnerable to vicious attacker.

Accordingly, this paper develops an authorization technique which can provide security to grid environment, while minimizing problems caused by vicious attackers. The suggested technique performs mutual authorization using session key shared in each session. In the mutual authorization process, calculation is performed using random values and hash algorithm per each communication section. In the communication section, continuously renewed keys heighten safety on power demand, control information and billing information.

제 1 장 서 론

1.1 연구 배경 및 목적

최근 에너지의 무분별한 사용과 그에 따른 전력 사용량이 공급량을 초과하면서 에너지 관리의 효율성 문제가 대두되기 시작하였다. 전력을 안정적으로 확보하기 위해 전력수요에 대비하여 발전소와 같은 공급원을 확대하는 방법을 제안하고 있다. 하지만 이는 막대한 비용과 시간이 투자되어야 하기 때문에 좋은 해결책은 아니다.

스마트 그리드(Smart Grid)는 이러한 전력사업의 문제 해결을 위해 개발되고 있는 대표적인 신기술이다. 기존의 전력망에 ICT 기술을 접목하여 전력생산 및 소비정보를 양방향과 실시간으로 교환함으로써 에너지 소비를 합리적이고 효율적으로 유도하고 이를 운영함으로써 다양하고 부가적인 서비스를 창출한다. 현재 국내에서는 2009년 12월부터 제주 구좌읍에 스마트 그리드 실증단지를 구축하여 한국형 스마트 그리드 모델을 구축하여 우리 기술과 제품을 실생활에서 직접 시험·평가한 다음 세계시장을 이끌어 나가도록 추진하여 2030년까지 국가 단위의 스마트 그리드 완성을 도모하고 있다[7]. 효율적인 에너지 창출이라는 슬로건 아래 스마트 그리드에서는 서비스 프로바이더와 스마트 디바이스 사이에 대량의 트래픽을 수집하고 이를 관리하며, 제 3자에 의해 가공, 처리, 분석, 보관이 가능하다. 하지만 이러한 수집 과정에서 저장 데이터, 통신 데이터 등의 유출이 가능하고 네트워크 부당 접속, 불법 기능사용, 서비스 거부 공격 등의 위협이 가능하다.

또한, 암호화 하지 않은 검침 데이터를 전송할 때, 사용자의 프라이버시 침해 위협도 존재한다.

따라서 본 논문에서는 초기 사용자 등록 과정에서 서비스 프로바이더와 데이터 수집 장치 그리고 스마트 미터 간의 상호 인증과 검침 데이터, 제어정보 및 과금 정보를 안전하게 전송하기 위한 프로토콜을 제안한다.

1.2 연구 내용 및 범위

본 논문에서는 스마트 그리드 환경에서 고려해야할 보안 위협을 분석하고 한국정보통신기술협회에서 발행한 표준에 따라 안전하고 효율적인 사용자 인증 기법을 제안한다.

스마트 그리드 서비스 프로바이더, 데이터 수집 장치 및 스마트 미터 간의 인증을 위한 서비스 가입, 인증 및 정보 전송 기법을 제안하며 이를 통해 상호간의 안전한 인증과 실시간 세션키 합의 등을 통해 보안성 향상과 통신 효율성 향상을 위한 기법을 제안한다.

1.3 논문의 구성

본 논문의 구성은 총 5개의 장으로 구성되어 있다. 제 1장에서는 연구 배경, 목적, 내용 및 범위에 대해 기술한다. 제 2장에서는 관련 연구로 스마트 그리드 환경에 대해 기술하고, 스마트 그리드의 구조와 내부 환경에 따른 보안위협에 대해 기술한다.

제 3장은 제 2장에서 기술한 정보를 고려하여 안전한 스마트 그리드 환경 구현에 최적화한 인증 기법을 제안한다. 제안하는 기법은 인증, 교환 및 합의 과정의 단계와 구성을 제안하고, 각 단계에서의 상세한 동작 과정을 제안한다.

제 4장에서는 제안한 기법의 보안 안정성에 대해 이를 정성적 분석으로 평가하고, 제 5장에서 본 논문에 대하여 결론을 맺는다.

제 2 장 관련 연구

제 2장에서는 스마트 그리드에 대한 개념과 스마트 그리드의 구조, 그리고 보안 위협에 대해 설명한다.

2.1 스마트 그리드

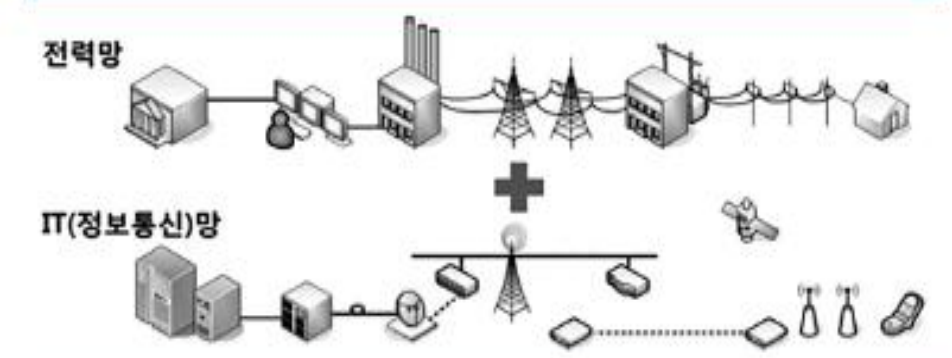
스마트 그리드는 기존의 전력망에 정보기술을 접목한 지능형 전력망으로 불린다[2,3]. 공급자와 소비자가 양방향 정보의 교류를 가능하게 하며 실시간 에너지 사용정보를 교환함으로 가정이나 기업 등의 소비자에게 공급하는 구조이다.

특히, 스마트홈 가전기기들은 스마트 그리드용 기기를 통해 전력 공급과 통신을 수행하며, 전력 사용량, 스마트 기기 정보, 사용자 정보 등 중요한 정보가 송수신 되므로 소비자 입장에서 좀 더 편리하고 전력 사용량 최적화, 효율적인 데이터 관리 및 전송, 원격 진단 및 업그레이드와 비용절감 효과를 가져 올 수 있는 핵심적인 영역이라 할 수 있다[4].

그러나, ICT 인프라를 접목한 스마트 그리드의 특성상 주요 정보에 대한 악의적인 접근이나 요금 청구 및 사용량 데이터 위조에 대한 불법 접근 및 공급 단절 등 다양한 보안 위협에 노출되는 문제가 발생할 수 있다[8].

본 절에서는 스마트 그리드의 개념과 구조 및 보안요구 사항 등에 대하여 설명한다.

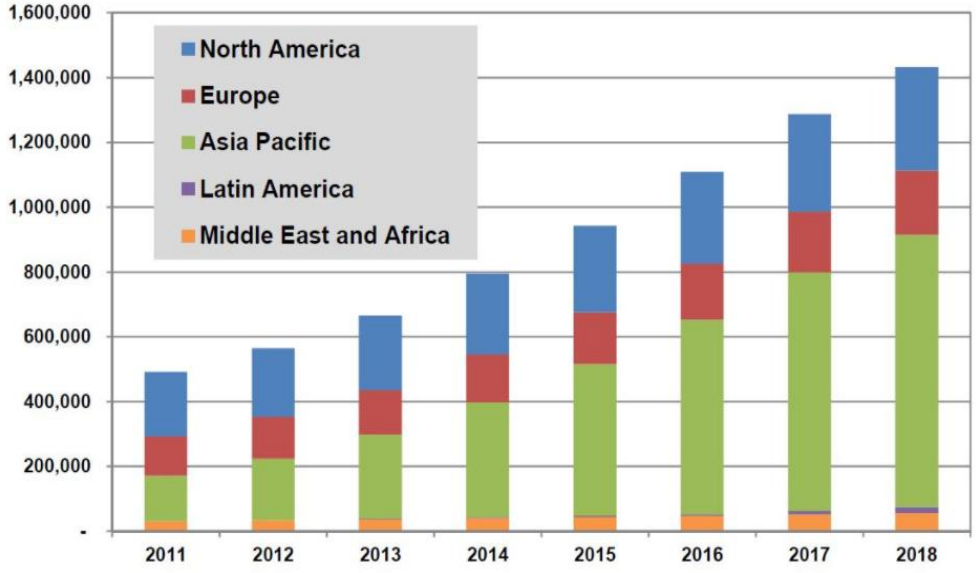
2.1.1 개요



[그림 2-1] 스마트 그리드 개념도

스마트 그리드 기술이란 기존의 전력망에 정보기술을 접목하여 공급자와 소비자가 실시간 정보를 양방향으로 교환하는 시스템을 구축하는 것을 기본 개념으로 [그림 2-1]과 같이 나타낼 수 있다. 세부적으로는 전력산업과 IT기술을 결합한 안정적이고 고성능의 지능화된 전력망을 뜻하는 것이다. 즉, 발전→송·배전→판매로 이어지는 기존 단방향의 전력망 비즈니스 구조에 정보통신기술을 접목하여 에너지 효율을 최적화한 차세대 지능형 전력망을 말한다[10].

스마트 그리드는 효율적인 에너지 활용으로 이산화탄소 배출을 최소화하며 능동적으로 기후 온난화에 대처 할 수 있는 기술로 고평가 받고 있다[5,20]. 현재 국내에서는 제주 구좌읍 실증단지, 남양주시 등 효율적인 에너지 활용을 위한 단지가 시범적으로 설치되어있다.

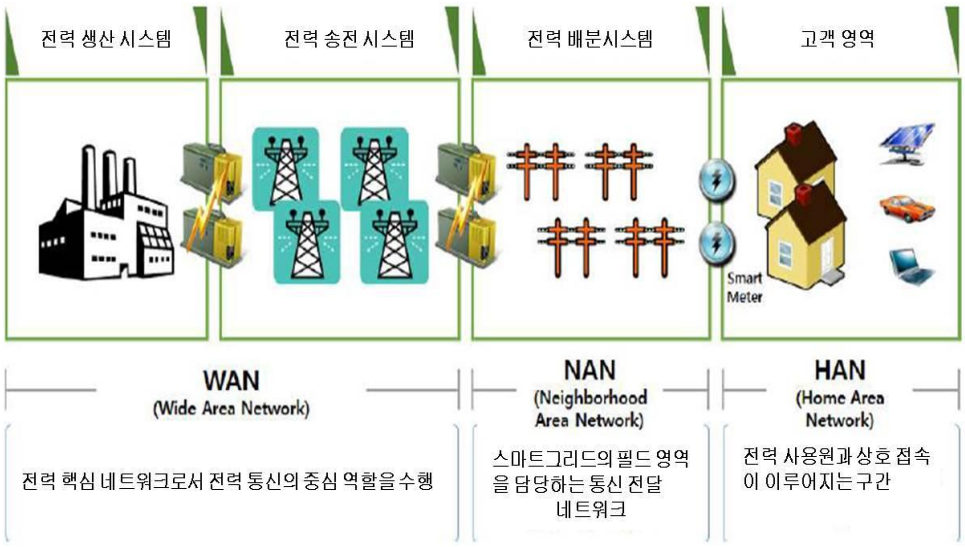


[그림 2-2] 스마트 그리드 시장 규모

스마트 그리드 시장규모는 지속적으로 성장세를 나타내고 있다. 2014년 이후 국제적인 저유가 상황이 지속되고 있음에도 전 세계 스마트 그리드 시장은 안정적인 성장을 지속하고 있다[6,17]. 스마트 그리드 시장은 2015년 기준 약 194억 달러 규모로 성장하였다. 이는 여러 국가들이 시행하고 있는 에너지 수요관리 정책이 일괄적으로 유지되고 있고, 에너지이용 효율화를 위한 노력이 스마트 그리드 산업 성장으로 시현되고 있음을 의미하고 있다. 유럽은 스마트 그리드 시장 구축을 '20-20-20목표'를 위해 적극적으로 추진하고 있으며, 2020년까지 스마트미터 보급에 연간 95억 달러를 투자할 예정이다[19,21]. 또한 온실가스(GHG) 배출량을 1990년 배출량 대비 20% 감축, 재생 에너지의 에너지 분담률을 20%까지 증대 시킬 예정이다. 아태 지역의 스마트 그리드 투자 현황은 일본, 중국, 한국이 주도하고 있으며, 일본, 중국, 한국을 제외한 아태 지역 국가에서는 스마트 그리드 투자활동이 미비한 것으로 분석된다[1,9].

2.1.2 스마트 그리드 구조 및 통신 영역

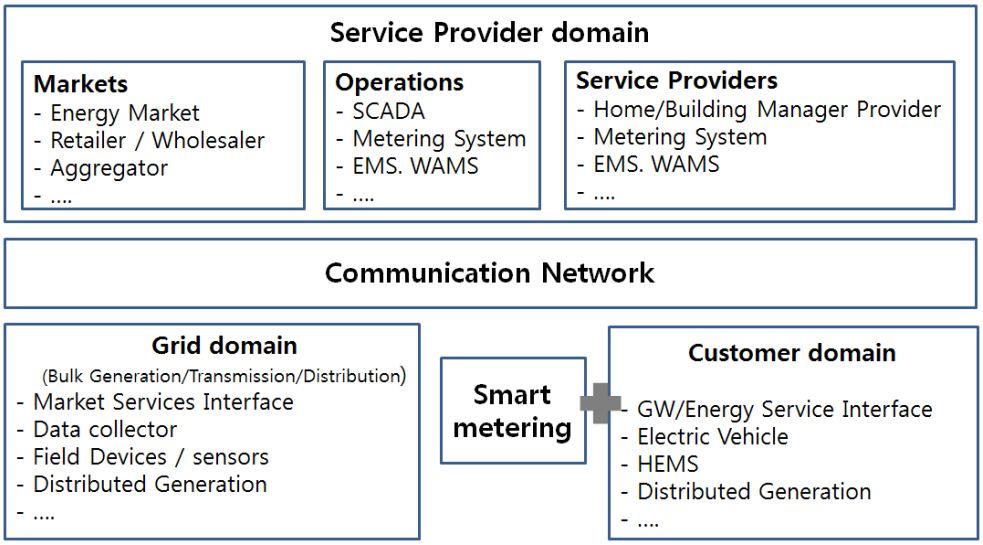
스마트 그리드 환경은 기존의 전력망에 ICT 기술을 접목한 기술이다. 전력 공급자와 전력 소비자 간 스마트 그리드 정보를 양방향으로 실시간 교환한다. 이를 통하여 에너지 효율성을 높일 수 있다. 또한 물리적으로 보면 전력망에 통신 네트워크를 합친 구조이며 논리적으로는 전력 계통, 통신, 보안 및 응용 계층까지 합쳐진 복합 계층 구조를 가진다[14,15]. 따라서 기존의 접목된 통신망을 따라 WAN(Wide Area Network), NAN(Neighborhood Area Network), HAN(Home Area Network)로 구분하여 나타내고 있다. 다음 그림은 스마트 그리드 환경의 구성과 통신 영역의 구분을 나타내고 있다.



[그림 2-3] 스마트 그리드 구조 및 통신 영역

2.1.2.1 HAN 영역 구조

HAN(Home Area Network)은 다양한 유무선 기술을 적용하여 가정의 개인용 컴퓨터, 가전 기기, 제어 기기, 각종 시설 등을 포함하는 영역으로 스마트 그리드의 영역이다.



[그림 2-4] HAN 영역 구조

ITU-T FG SMART(Focus Group on SmartGrid)의 Telecommunication Standardization Sector에서는 스마트 그리드의 모델을 ICT 관점으로 단순화하여 정의하고 있다[12,16]. 해당 모델은 Service Provider domain, Communication Network, Grid domain, Smart metering, Customer domain의 5개의 도메인으로 구성되어 있다.

HAN 기기는 HAN 영역에서 스마트 그리드 환경을 구성하는 스마트 그리드용 기기 및 스마트 가전기기를 포함한다[18,22]. 스마트 그리드용 기기는 IHD, HEMS, 스마트미터, ESI 등이며, 스마트 가전기기는 전력 사용을 제어할 수 있는 TV, 냉장고, 컴퓨터 등이 해당된다. 해당 기기들

은 통신 기능을 지원하기 위하여 PLC, ZigBee, Wi-Fi, 전화선, Bluetooth 등이 사용된다.

2.1.2.2 NAN 영역 구조

NAN은 스마트 그리드의 필드 영역을 담당하는 통신 네트워크로 전력회사의 정보통신망과 집적 연결되는 통신 인프라 영역이다.

변전소에서부터 소비자 사이의 데이터 전송을 담당하는 통신 네트워크를 NAN이라고 부른다[11,23]. 송전망이나 집안에서는 통신 네트워크가 이미 구축 되어 있는 경우가 많으나 배전망에서의 통신 네트워크가 새롭게 구축되는 경우가 많아 새로운 통신 네트워크가 테스트되고 있다.

2.1.2.3 WAN 영역 구조

WAN은 전력 설비의 종단과 다양한 관련 기기들이 연계된 통신망을 뜻하며 스마트 그리드 주요 네트워크 및 백홀(Backhaul)을 포함한 영역이다.

스마트 그리드 WAN 통신 분야를 지원하기 위한 시스템은 넓은 커버리지와 적은 전송 지연의 요구사항을 만족시켜야 한다[7]. 특히 높은 데이터 전송율과 전송 지연을 만족시키기 위해서는 높은 성능의 통신 네트워크가 필요하다[13,24]. 이런 요구사항을 만족시키는 통신 기술은 광통신과 셀룰라 시스템이 존재한다.

2.1.3 스마트 그리드 보안 위협

스마트 그리드 영역의 보안위협 분류는 기밀성, 무결성, 가용성 측면에서 11가지 위협으로 분류할 수 있다. 한국정보통신기술협회에서 발행한 보안 위협은 아래 [표2-1]과 같다. 이 보안 위협은 HAN 영역의 스마트 그리드용 기기, HAN 기기 간 통신 구간에서 도출하였다.

[표 2-1] 스마트 그리드 보안 위협

분류	보안 위협	측면	내용
①	저장 데이터 유출	기밀성	물리적 또는 통신을 원격에서 HAN 기기에 접근하여 데이터를 유출 시킬 수 있음
②	통신 데이터 유출	기밀성	HAN의 통신 과정에서 메시지를 공격자가 획득함으로써 데이터가 유출될 수 있음
③	저장 데이터 삭제	무결성 가용성	HAN 기기에서 서비스 운영 및 제공을 위해 저장하고 있던 데이터를 삭제시킴으로써 정상적인 동작을 수행할 수 없게 만들 수 있음
④	저장 데이터 변조	무결성	HAN 기기에 저장된 데이터를 공격자가 임의로 변경함으로써 잘못된 데이터를 사용하여 실시간 요금이나 전력수요예측 등에 문제가 발생될 수 있음
⑤	통신 데이터 변조	무결성	HAN의 통신 과정에서 공격자가 데이터를 변조하여 최종목적지로 전달하면 실시간 요금이나 전력수요 예측 등에 문제가 발생될 수 있음
⑥	통신 데이터 위조	무결성	HAN의 통신 과정에서 위조된 데이터를 특정 기기에 전달함으로써 문제를 발생시키며, 만약 제어명령이 위조될 경우, 시스템이

			점령달할 수도 있음
⑦	물리적 기기 조작	가용성	공격자가 HAN 기기에 직접 접근하여 네트워크에 접속하거나, 취득한 정보를 통해 위장된 기기를 설치하여 지속적인 공격이 가능할 수 있음
⑧	네트워크 부당 접속	무결성	HAN 영역에 정상적인 행세를 하는 악성기기를 연결하여 정보를 취득하거나 잘못된 기능을 수행하도록 할 수 있음
⑨	동작 행위 부인	무결성	HAN 기기에서 수행한 메시지 전송, 명령 수행 등의 사실을 부인할 수 있음
⑩	불법적 기능사용	가용성	HAN 기기의 기능 중 허용되지 않는 기능을 사용함으로써 기기 오작동을 유발할 수 있음
⑪	서비스 거부 공격	가용성	HAN 기기 및 네트워크의 자원을 과도하게 사용함으로써 네트워크 마비 또는 기기 오작동 유발 가능

제 3 장 분산형 에너지 시스템 환경에서 안전한 전력 수급을 위한 스마트 미터 인증 기법 설계

3.1 개요

기존의 스마트 그리드와 스마트 미터가 가지고 있는 보안 취약점과 안전한 전력 수급을 위한 방안으로 인증 기법을 제안한다. 인증 기법은 Service Provider – Data Collector, Service Provider – Smart Meter, Data Collector – Smart Meter 간의 인증 기법을 제안한다.

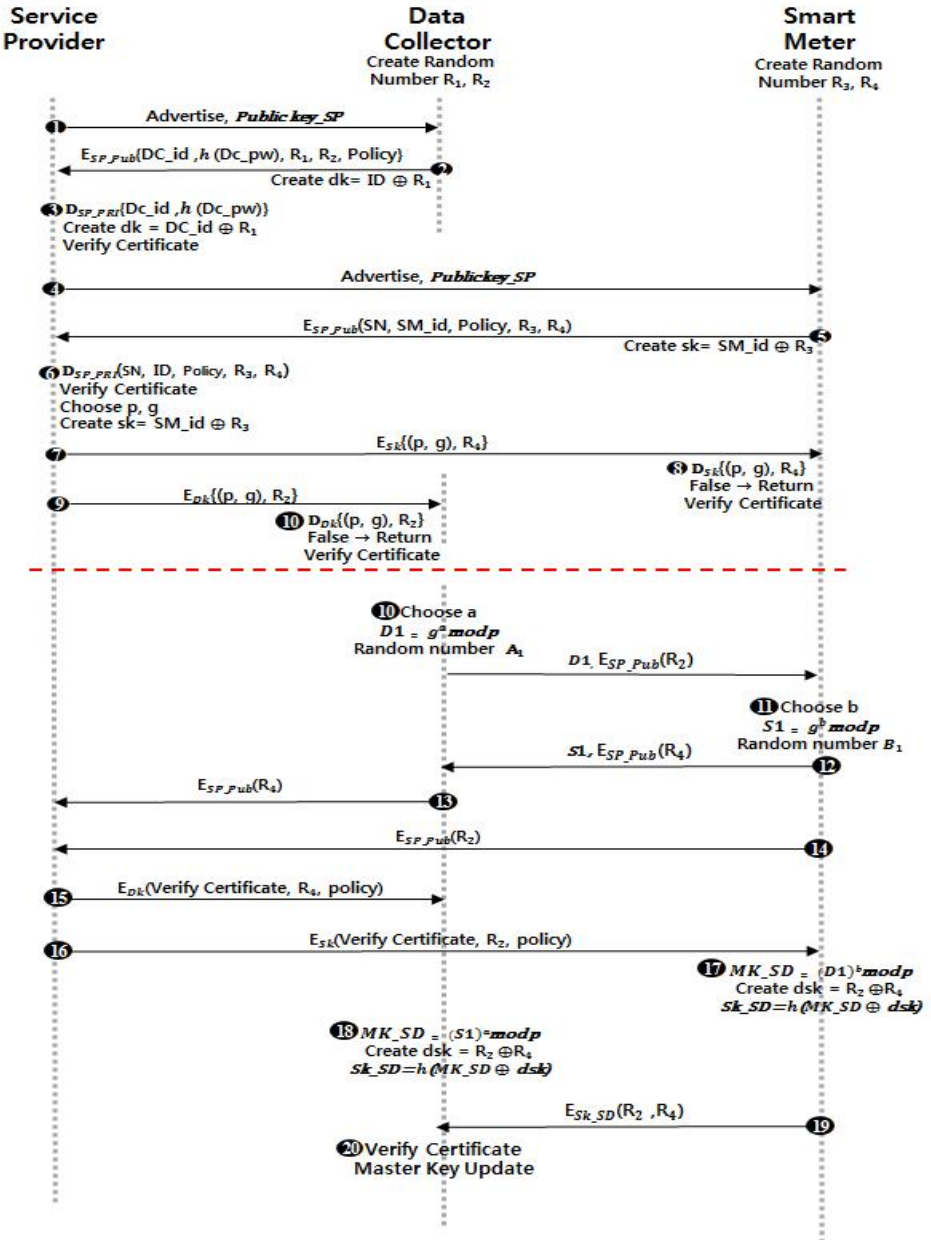
제안하는 분산형 에너지 시스템 환경에서 안전한 전력 수급을 위한 스마트 미터 인증 기법 프로토콜에서 사용하는 약어는 다음 [표2]과 같다.

[표 3-1] 제안하는 프로토콜에서 사용하는 약어

약어	설명
Service Provider	서비스 프로바이더
Data Collector	데이터 수집 장치
Smart Meter	스마트 미터
SP_PUB	서비스 프로바이더의 공개키
Dc_id	데이터 수집 장치의 아이디
Dc_pw	데이터 수집 장치의 비밀번호
SM_ID	스마트 미터의 아이디
R1,R2,R3,R4	랜덤 값
h()	암호학적 해시 함수
⊕	배타적 논리합(XOR)
Token	토큰

3.2 서비스 가입 및 인증

서비스 가입 및 인증 기법에서는 서비스를 이용하기 위해 Service Provider, Data Collector, Smart Meter 단계 별로 인증하는 단계이다.

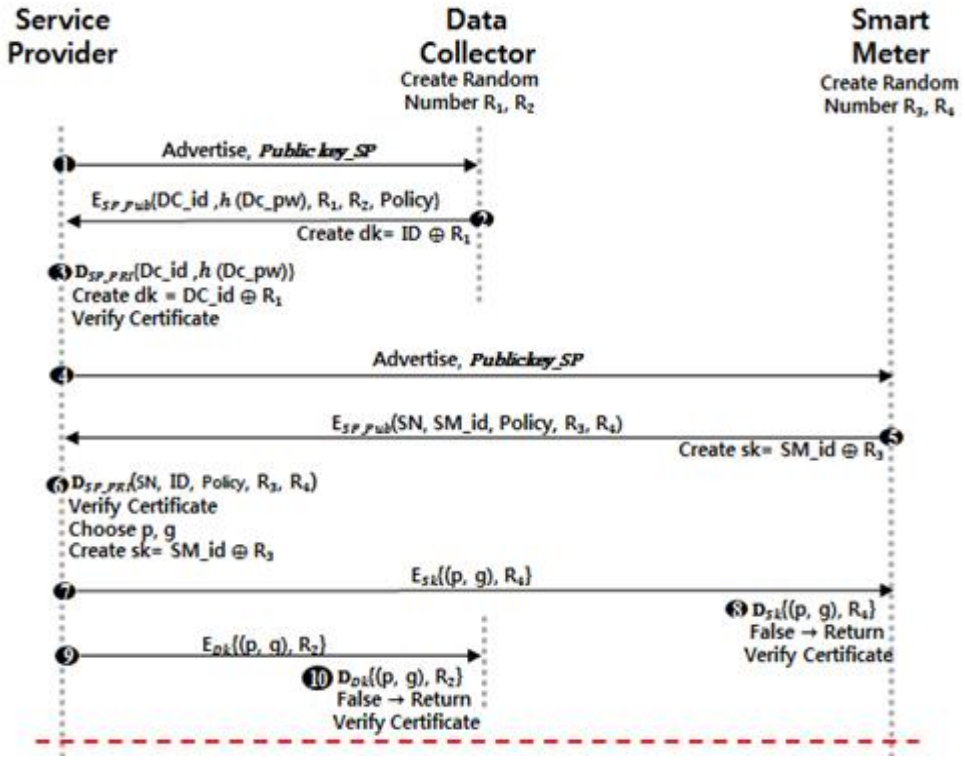


[그림 3-1] 서비스 가입 및 인증 기법의 프로토콜

해당 기법에서는 Smart Meter, Data Collector가 Service Provider의 참여 하에 서비스에 가입하고 상호 인증 및 키 합의를 진행하는 단계이다. 키 합의는 Diffie - Hellman의 키 교환 방법을 응용하여 안전하게 키 합의를 할 수 있도록 한다. 또한 이후 Smart Meter가 서비스를 제공 받기 위해 매번 세션을 성립할 때 상호인증 및 갱신하는 과정을 포함한다.

3.2.1 서비스 가입 및 인증에서의 사전 절차

이 절차는 Data Collector, Smart Meter가 Service Provider를 통하여 서로간의 인증을 하는 과정의 일부이다. Data Collector와 Smart Meter는 사전에 각각 난수를 두 개씩 생성한다.



[그림 3-2] 서비스 가입 및 인증에서의 사전 절차

(1) Service Provider는 Data Collector 에게 자신의 공개키인 *Public key_SP*를 보낸다.

(2) Data Collector는 사전에 생성한 자신의 랜덤 값 *R1, R2* 값을 보내며 자신이 올바른 Data Collector 라는 것을 증명하기 위하여 자신의 아이디인 *DC_id*와 해쉬한 자신의 패스워드 *h(DC_pw)*를 Service Provider의 공개키로 정책과 함께 암호화 하여 보내준다. 또한 이 후 Service Provider와 통신할 때 쓰일 *dk*를 *DC_id* 와 *R1*값을 *xor* 연산을 통하여 생성한다.

(3) Service Provider는 전달 받은 내용들을 자신의 개인키로 복호화한 후에 확인하여 올바른 Data Collector라는 것을 확인한다. 또한 이 후에 Data Collector와 통신할 때 쓰일 *dk*값을 생성한다.

(4) Service Provider는 Data Collector 에게 보냈던 것과 마찬가지로 Smart Meter에게 자신의 공개키인 *Public key_SP*를 보낸다.

(5) Smart Meter는 사전에 생성한 자신의 랜덤 값 *R3, R4* 값을 보내며 자신이 올바른 Smart Meter 라는 것을 증명하기 위하여 자신의 아이디인 *SM_id*와 Smart Meter 의 serial number를 Service Provider의 공개키로 정책과 함께 암호화 하여 보내준다. 또한 이 후 Service Provider와 통신할 때 쓰일 s*k*를 *SM_id* 와 *R3*값을 *xor* 연산을 통하여 생성한다.

(6) Service Provider는 전달 받은 내용들을 자신의 개인키로 복호화한 후에 확인하여 올바른 Smart Meter 라는 것을 확인한다. 또한 이후에 Data Collector와 통신할 때 쓰일 *dk*값을 생성한다. 이와 같은 방식으로 올바른 Data Collector와 Smart Meter라는 것을 검증하고 올바르다고 판단 될 경우에는 키 합의를 위한 값 소수 *p*, 정수 *g*를 선택한다. 이때 *p*는 매우 큰 소수이며 g는 군$<Z^*_p, x>$의 원소로서 위수가 *p-1*인 생성자이다.

(7) Service Provider는 Smart Meter에게 사전에 합의된 s*k*로 암호화하여 생성된 재료값 소수 *p*, 정수 *g*와 기존에 Smart Meter에게 받은 *R4*를 다시 보냄으로서 중간에 악의적인 사용자로부터 변경되지 않은 것을 확인시켜준다.

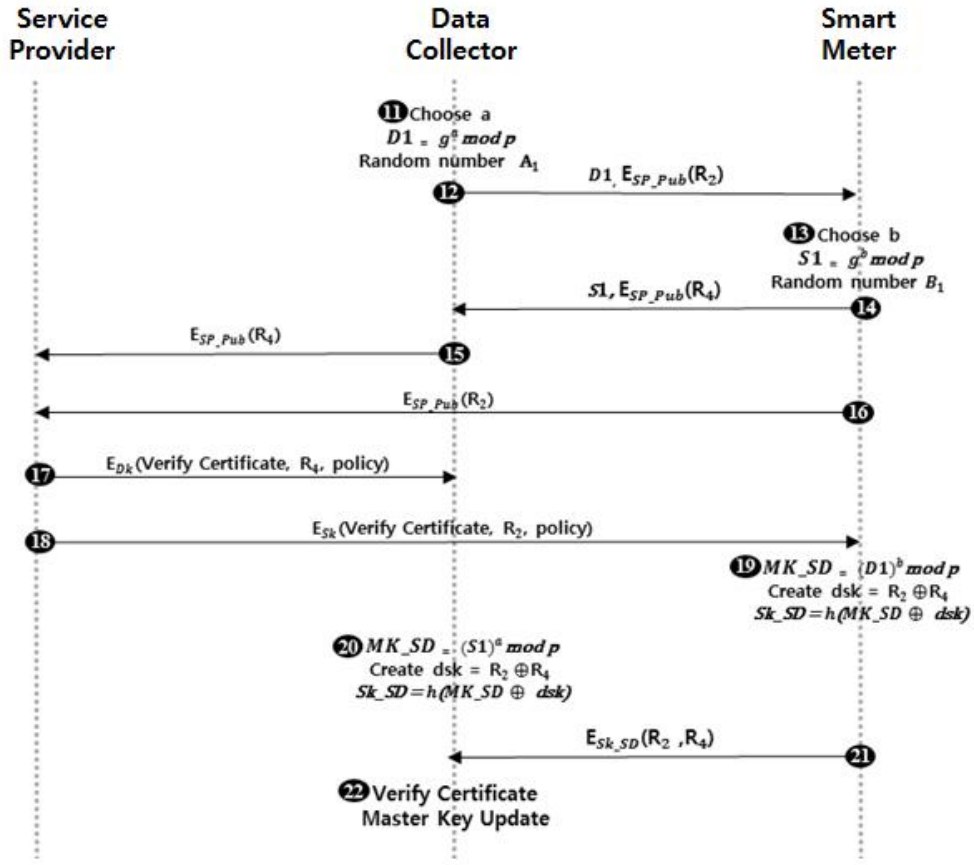
(8) Smart Meter는 전달받은 내용을 확인하여 검증 결과가 적법하다고 판달 될 경우 인증을 마친다. 만약 적법하지 않다고 판단 될 경우 통신을 종료한다.

(9) Service Provider는 Data Collector에게 사전에 합의된 d*k*로 암호화 하여 생성된 재료값 소수 *p*, 정수 *g*와 기존에 Data Collector에게 받은 *R2*를 다시 보냄으로서 중간에 악의적인 사용자로부터 변경되지 않은 것을 확인시켜준다.

(10) Data Collector는 전달받은 내용을 확인하여 자신이 보낸 값과 비교하여 검증 결과가 올바르다고 판달 될 경우 인증을 마친다. 만약 적법하지 않다고 판단 될 경우 통신을 종료한다.

3.2.2 서비스 가입 및 인증에서의 대칭키 합의 및 상호 인증

이 절차는 Data Collector와 Smart Meter가 Service Provider로부터 전달 받았던 대칭키 재료값 소수 p, 정수 g를 이용해 대칭키를 합의하고 세션을 성립하는 단계이다.



[그림 3-3] 서비스 가입 및 인증에서의 대칭키 합의 및 상호 인증

(11) Data Collector는 키 합의에 사용할 부분키 생성을 위해 a(단, $0 \leq a \leq p-1$)를 *선택하고* 부분키 $D1=g^a \bmod p$ 연산한다.

(12) Data Collector는 부분키 *D1*을 전달 받는다. SP1의 공개키 *SP_pub*로 암호화된 생성된 난수 R_2을 Smart Meter에게 전송한다.

(13) Smart Meter는 대칭키 합의에 사용할 부분키 생성을 위해 b(단, $0 \leq b \leq p-1$)를 *선택하고* 부분키 $S1=g^b \bmod p$ 연산한다.

(14) Smart Meter는 부분키 *S1*을 Data Collector에게 전달한다. SP1의 공개키 *SP_pub*로 암호화된 생성된 난수 R_4를 Data Collector에게 전송한다.

(15) Data Collector는 악의적인 공격자로 인하여 변경된 내용이 없는지 확인하기 위하여 Smart Meter로부터 받은 난수 R_4를 Service Provider의 공개키인 *SP_pub*로 암호화 하여 전달한다.

(16) 마찬가지로 Smart Meter도 Data Collector와 통신과정에 변경된 내용이 없는지 확인하기 위하여 Smart Meter로부터 받은 난수 R_2를 Service Provider의 공개키인 *SP_pub*로 암호화 하여 전달한다.

(17) Service Provider는 앞서 받은 난수 값을 확인한 후 정당한 사용자라는 것을 확인해주며 정책과 Smart Meter의 난수인 R_4를 보

내준다. 이때 사용되는 키는 사전에 합의 하였던 *dk* 키로 암호화 하여 보내준다.

(18) 앞서와 마찬가지로 Service Provider는 앞서 받은 난수 값을 확인한 후 정당한 사용자라는 것을 확인해주며 정책과 Data Collector의 난수인 R_2를 보내준다. 이때 사용되는 키는 사전에 합의 하였던 *sk* 키로 암호화 하여 보내준다.

(19) Service Provider로부터 난수 값과 향후 통신 간 사용할 정책을 받은 Smart Meter는 Data Collector와 통신 할 Sk_SD값을 만들 재료값인 MK_SD를 생성한다. 또한 자신의 난수 값인 R_4 와 Data Collector의 난수 값 R_2를 가지고 dsk를 xor 연산을 통하여 생성한다. 그 후 통신에 사용할 Sk_SD를 생성한다.

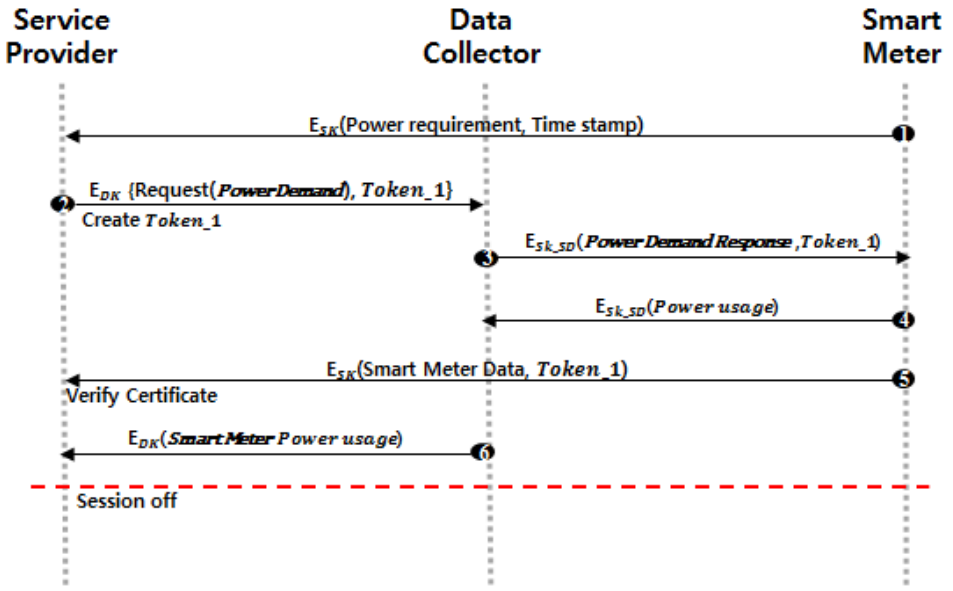
(20) 마찬가지로 Service Provider로부터 난수 값과 향후 통신 간 사용할 정책을 받은 Data Collector는 Smart Meter와 통신 할 Sk_SD 값을 만들 재료값인 MK_SD를 생성한다. 또한 자신의 난수 값인 R_2 와 Smart Meter의 난수 값 R_4를 가지고 dsk를 xor 연산을 통하여 생성한다. 그 후 통신에 사용할 Sk_SD를 생성한다.

(21) 상호 간의 세션키가 성립이 되고 난 후에는 Smart Meter는 Sk_SD 킷값으로 암호화한 난수 R_2 ,R_4 난수 값을 보내어 악의적인 공격자로부터 데이터 위·변조가 일어나지 않았다는 것을 확인한다.

(22) 안전한 사용자라는 것이 확인이 되고 난 후 매 통신 구간 마다 같은 과정을 반복하여 세션키를 생성해주어 지속적으로 마스터키를 업데이트 해준다.

3.2.3 세션 생성 및 통신 데이터 전송 프로토콜

이 절차는 상호 간의 인증 이후 Smart Meter가 서비스를 이용하고자 할 때 성립하는 것이다.



[그림 3-4] 세션 생성 및 통신 데이터 전송 프로토콜

(1) Smart Meter가 Service Provider에게 기존에 합의한 세션키 sk값으로 전력 요구와 보내는 시간에 맞는 타임스탬프 값을 암호화하여 요청한다.

(2) Service Provider는 Smart Meter가 보낸 값을 복호화 하여 확인하고 향후 통신할 때 사용할 Token 값을 생성하여 Data Collector에게 보내준다. 이때 생성된 Token 값은 Smart Meter와 Data Collector간 향후 통신 할 때 같은 인증 값이 반복되지 않기 위함에 생성된다.

(3) Data Collector는 Smart Meter와의 합의된 세션키를 통하여 원하는 전력량과 향후 통신할 때 쓰일 Token 값을 sk_sd 키값으로 암호화 하여 전송한다.

(4) Smart Meter는 요청한 전력에 대하여 알맞게 사용을 한 후 Data Collector에게 자신이 사용한 전력에 대하여 sk_sd 키값으로 암호화 하여 리포트 한다.

(5) 또한 Service Provider에게 자신의 전력량에 대한 값과 토큰 값을 보냄으로서 중간에 악의적인 공격자로부터 데이터 위·변조 혹은 유출이 있었는지에 대하여 확인한다.

(6) Service Provider는 안전한 Token값인 것을 확인하고 인증을 완료한다. 또한 Data Collector에게 Smart Meter로부터 받은 리포트를 확인하여 비교 한 후 중간에 악의적인 공격자로부터 데이터 위·변조, 유출이 없었다는 것을 확인하고 세션을 종료 한다.

제 4 장 성능분석 및 보안성 평가

본 장에서는 제안한 상호인증 프로토콜에 대한 안정성 평가를 한다. 4.1에서는 제안 프로토콜에 대한 보안 측면의 비교 분석을 진행하고 4.2절에서는 보안 요구사항에 대해 검토한다. 마지막으로 4.3절에서는 효율성에 대해 정리한다.

4.1 비교 분석

제안한 상호인증 프로토콜에 대한 보안성 평가를 한다. 보안성 평가의 요점은 각 구간별 보안성, 효율성을 비교 진행한다.

[표 4-1] 보안성 평가

보안위협	기존 방식	제안 프로토콜
저장 데이터 유출	가능	불가능
통신 데이터 유출	가능	불가능
저장 데이터 변조	가능	불가능
통신 데이터 위·변조	가능	불가능
네트워크 부당 접속	가능	불가능

보안성 평가의 요점은 한국정보통신기술협회에서 발행한 저장 데이터 유출, 통신 데이터 유출, 저장 데이터 변조, 통신 데이터 위·변조, 네트워크 부당 접속 측면에서의 진행한다. 또한 상호 인증에 사용되었던 키 갱신을 통해 전송되는 검침정보, 전력 요청과 같은 메시지에 대하여 보안성 분석을 진행한다.

4.2 보안 요구사항

4.2.1 저장 데이터 유출

악의적인 공격자가 Data Collector의 계량 정보, 전력 요청에 대한 정보를 탈취하여 저장 데이터가 유출되어 사용자의 정보를 무단으로 수집하는 공격이다. 하지만 사전에 협의 된 세션키를 통하여 정보를 전송하기 때문에 안전하다.

4.2.2 통신 데이터 유출

전송되어 지는 통신 데이터를 엿보는 공격 방법이다. Service Provider, Data Collector, Smart Meter 간에는 사전에 협의 된 정보를 가지고 매번 새롭게 세션키를 생성·갱신하기 때문에 통신 데이터에 대한 공격에 안전하다.

4.2.3 저장 데이터 변조

악의적인 공격자는 통신 데이터간 저장되어 있는 전력 요청, 검침 데이터 등 저장 데이터를 변조 할 수 있다. 하지만 세션키에 타임스템프 값에 따라 지속적으로 갱신되기 때문에 저장 데이터 변조 공격에 대하여 안전하다.

4.2.4 통신 데이터 위·변조

악의적인 공격자가 통신 구간 별 전송되어 지는 통신 데이터를 탈취하여 메시지를 위·변조하여 전송하는 방식의 공격이다. 하지만 메시지를 탈취한 당시의 세션키를 사용하는 것이 아니라 매번 새롭게 생성·갱신되어진 세션키를 사용하기 때문에 공격에 안전 한다.

4.2.5 네트워크 부당 접속

임의의 사용자는 자신이 Data Collector, Smart Meter 간의 메시지를 탈취하여 부당 접속을 시도 할 수 있다. 하지만 사전에 Service Provider 에서 Data Collector에 대한 인증정보와 Smart Meter의 고유 번호를 가지고 있기 때문에 안전하다.

4.3 효율성 분석

4.3.1 제안프로토콜 연산량 비교

본 장에서는 제안한 분산형 에너지 시스템 환경에서 안전한 전력 수급을 위한 스마트 미터 인증 기법 설계에 대한 효율성을 분석하였다.

[표 4-2] 제안 프로토콜 연산량

	Service Provider	Data Collector	Smart Meter
해시	5	4	5
암호화	6	4	5
복호화	4	5	6
세션키 연산	2	2	2
토큰 연산	1	1	1

[표4-2] 에서는 세션키 성립 과정과 정보교환 과정에서 Service Provider, Data Collector, Smart Meter 각 1개 일 때 연산되는 자원 분석을 보여준다. Service Provider, Data Collector, Smart Meter 는 비슷한 연산량을 가졌기 때문에 어느 한 통신객체가 더욱 복잡한 연산을 수행하지 않는다. 컴퓨팅 자원에 맞춰 비슷한 컴퓨팅 연산이 분산되었고,

최소한의 연산으로 상호인증 및 보안채널을 구축하도록 하였다.

4.3.2 제안프로토콜 저장량 비교

[표 4-3] 제안 프로토콜 저장량

	Service Provider	Data Collector	Smart Meter
난수	-	2	2
인증서	1	-	-
세션키	4	5	6
타임 스탬프	-	2	2
토큰	1	1	1

[표4-3]은 제안하는 프로토콜에서 세션키 성립 과정과 정보교환 과정에서 Service Provider, Data Collector, Smart Meter가 각 1개 일 때 연산되는 양을 보여준다. 저장 공간은 통신객체들 마다 비슷한 양을 보유하고 있으며 Data Collector, Smart Meter 각각 난수 두 개를 보유하고 있다. Service Provider는 초기 인증을 위한 인증서를 지니고 있다. 각 통신 구간마다 생성되는 세션키는 각 4, 5, 6개를 보유하고 있다. 또한 정보교환 과정에서 하나의 토큰과 두 개의 타임 스탬프 값을 가진다. 각각의 용량에 따라 비슷한 저장량을 할당하였다.

제 5 장 결론

본 논문은 분산형 에너지 시스템 환경에서 안전한 전력 수급을 위한 스마트 미터 인증 기법 설계를 제안하였다. 스마트 그리드 환경에서 발생할 수 있는 기존의 보안위협에 대한 문제점을 보완을 하였으며, 효율성과 안전성을 높이기 위하여 상호인증 프로토콜을 제안하였다.

각 통신 구간 별 상호인증과 인증과정에서 사용되는 세션키 생성과 랜덤 값의 통한 연산으로 기존 스마트 그리드 환경에서 발생 할 수 있는 저장 데이터 유출, 통신 데이터 유출, 저장 데이터 변조, 통신 데이터 위·변조, 네트워크 부당 접속 측면의 보안 위협에 대하여 보완을 하였으며 상호 인증 이후 Smart Meter에서 Data Collector, Service Provider에게 전송 되는 검침 데이터와 제어정보 등 안전성과 효율성을 향상 시켰다.

기존 스마트 그리드 환경 시스템은 사용자 인증, 암호화와 같은 보안적인 측면이 미비하기 때문에 안정성 평가 및 효율성을 분석하였다. 효율성 및 안전성 측면에서는 각 연산 구간에서 연산 소요시간을 줄일 수 있도록 하였다. 보안성 분석을 통해 보안성 측면에서 안전성을 제공하는 것을 정성적 방법을 통하여 증명 하였다. 또한 인증 및 서비스 단계의 통신 구간에서 기존 연구에 비해 악의적인 공격자를 통한 공격 문제 발생의 여지를 최소화 하였다.

향후 제안한 프로토콜이 통신 구간이 증가하는 스마트 그리드 환경에서 스마트 미터 간 통신을 그룹화 시켜 관리하여 효율성을 높이며, 더욱

안전한 스마트 그리드 사용자 관리체계에 대한 연구가 필요할 것으로 보인다. 또한 아직 발견되지 않은 스마트 그리드에 관한 다양한 보안 위협들에 대한 대비책도 필요할 것으로 보인다.

참고문헌

[1] 양일권, 정남준, 최승환, 이상호. (2010). AMI시스템 구현을 위한 보안 요구사항 분석 및 추진 방향 제안. 대한전기학회 학술대회 논문집, , 1898-1899.

[2] 박남제, 안길준. (2010). 스마트 그리드에서의 프라이버시 보호. 정보보호학회지, 20(3), 62-78.

[3] 유성민, 김남균, 김윤기. (2014). 스마트 그리드 보안기술 동향분석 및 대응방안. 한국통신학회지(정보와통신), 31(5), 8-14.

[4] 서정택, 국경수. (2013). 스마트 그리드 사이버 보안 기술 소개 및 동향. 전기의세계, 62(9), 38-42.

[5] 권오훈. “스마트 그리드 환경에서 프라이버시 보호를 위한 연구”. 동국대학교 석사학위 논문. 2014

[6] 김유진, 조병선, 심진보. (2010). 산업연관분석을 활용한 스마트 그리드산업의 경제적 파급효과. 한국통신학회논문지, 35(8), 1241-1250.

[7] 최원규. ″스마트 그리드 환경에서 데이터 난독화 및 상호인증 기반의 이중 암호화 기법 설계″. 숭실대학교 석사학위 논문. 2014

[8] 정교일, 박한나, 정부금, 장종수, 정명애. (2012). 스마트 그리드의 안전성과 보안 이슈. 정보보호학회지, 22(5), 54-61.

[9] 전용희, 장종수. (2012). 스마트 그리드 통신ko망의 보안 특성, 고려사항, 구조, 설계 원칙과 연구동향에 관한 고찰. 정보보호학회지, 22(5), 40-53.

[10] 윤성국. (2014). 스마트그리드 통신 네트워크 구성과 전력선 통신의 역할. 한국통신학회지(정보와통신), 31(11), 95-101.

[11] 안기봉, 한태환. (2009). 스마트 그리드(지능형 전력망)와 스마트 세

대분전반. 조명·전기설비, 23(4), 18-26.

[12] Alamri, Atif, et al. "A survey on sensor-cloud: architecture, applications, and approaches". International Journal of Distributed Sensor Networks 2013. 2013.

[13] IDC. "IDC Worldwide Predictions 2015: Accelerating Innoation on the 3rd Platform". 2015.

[14] Oh, Soo-Hyun, and Sun-Ki Eun. "Remote user Access control Mechanism in Smart Grid environments." The Transactions of The Korean Institute of Electrical Engineers 60.2 (2011): 416-422.

[15] Mell, Peter, Timothy Grance. "The NIST Definition of Cloud Computing (Draft)". NIST Special Publication 800. 2011.

[16] Hwang, Humor, and Jung-Hoon Kim. "Interpretation works and online terminology information system for the standardization of smart grid terminologies." The Transactions of The Korean Institute of Electrical Engineers 62.3 (2013): 293-299.

[17] 이경복, 독고지은, 유지연, 이숙연, 임종인. (2009). 스마트 그리드에서의 소비자 참여와 보안 이슈. 정보보호학회지, 19(4), 21-35.

[18] Li, Jin, et al. "A hybrid cloud approach for secure authorized deduplication". Parallel and Distributed Systems, IEEE Transactions on 26.5. 2015.

[19] 손태식, 고종빈. "Cloud Computing 에서의 IoT (Internet of Things) 보안 동향". 정보보호학회지 22.1. 2012.

[20] 김홍래, 문승일. (2009). 스마트 그리드(Smart Grid)의 이해. 전기의 세계, 58(8), 22-26.

[21] Zissis, Dimitrios, Dimitrios Lekkas. "Addressing cloud computing

security issues". Future Generation computer systems 28.3. 2012.

[22] Celesti, Antonio, et al. "Three-phase cross-cloud federation model: The cloud sso authentication". Advances in Future Internet (AFIN). 2010 Second International Conference on. IEEE. 2010.

[23] Huang, Jingwei, David M. Nicol. "Trust mechanisms for cloud computing". Journal of Cloud Computing 2.1. 2013.

[24] S Song, et al. "User Authentication Method Design Based on Biometrics in a Multi-cloud Environment". Advances in Computer Science and Ubiquitous Computing. Springer Singapore. 2015.