스마트 그리드 환경을 위한 원격 사용자 접근제어 메커니즘

논 문
60-2-29

Remote user Access control Mechanism in Smart Grid environments

오 수 현† · 은 선 기*
(Soo-Hyun Oh · Sun-Ki Eun)

Abstract - Smart grid is the next generation intelligent power grid that combines the existing electric power infrastructure and information infrastructure. It can optimize the energy efficiency in both directions, suppliers and power consumers to exchange information in real time. In smart grid environments, with existing network security threats due to the smart grid characteristics, there are additional security threats. In this paper, we propose a security mechanism that provides mutual authentication and key agreement between a remote user and the device. The proposed mechanism has some advantages that provides secure mutual authentication and key agreement and secure against a replay attack and impersonation attacks.

Key Words : Smart grid, Security threat, Access control, Mutual authentication, Key agreement

1. 서 론

최근 정보통신 기술이 발전하면서 기존의 기술들을 융합하거나 결합시켜 보다 효율적인 서비스를 제공하기 위한 연구가 진행되고 있다. 특히 전력산업 분야에서는 에너지 소비가 증가함에 따라 에너지 소비를 줄이고 에너지 효율을 높일 수 있는 연구가 활발히 진행되고 있으며, 이와 관련하여 지능형 전력망이라 불리는 스마트 그리드(smart grid)에 대한 관심이 고조되고 있다. 또한 M2M(Machine-to-Machine) 통신에서도 스마트 그리드를 주요 응용 사례로 선정하여 이에 대한 연구가 활발히 진행되고 있다.[3][4]

스마트 그리드 환경에서는 스마트 미터기(smart meter), AMI(advanced metering infrastructure)와 같은 지능형 장치를 통한 양방향 통신을 제공하기 위해 기존의 정보통신망을 활용하므로, 데이터 노출, 데이터의 불법 변경 및 삭제, 프라이버시 문제, 디바이스 도난과 같은 다양한 보안 위협들이 존재할 가능성이 있다.[1] 이와 같은 보안 위협들은 소비자 측면에서는 개인 프라이버시와 관련된 문제가 발생할 수 있으며 궁극적으로는 국가적 사이버 보안과 관련된 보안문제로 야기 될 수 있다.[8]

본 논문에서는 보다 안전하고 신뢰할 수 있는 스마트 그리드 환경을 구축하기 위해 고려해야 하는 보안 요구사항을 분석하고, 스마트 그리드 환경에서 원격 사용자를 위한 접근제어 메커니즘을 제안한다.

† 교신저자, 정회원 : 호서대학교 정보보호학과 교수
E-mail : shoh@hoseo.edu
* 호서대학교 정보보호학과 석사과정
접수일자 : 2010년 7월 20일
최종완료 : 2010년 12월 21일

2. 관련 연구

2.1 스마트 그리드

2.1.1 개요

스마트 그리드란 기존의 전력망(Electric Power Infrastructure)에 정보통신망(Information Infrastructure)과 정보기술(Information Technology)을 융합시켜 전력계통에 실시간 양방향 통신을 제공함으로써 전력시스템을 효율적으로 관리하고 소비자에게 보다 다양한 서비스를 제공할 수 있는 차세대 지능형 전력망을 의미한다.

스마트 그리드를 구축하기 위해서는 양방향 정보통신 시스템, 스마트 미터기, AMI, 분산형 에너지 관리 시스템, 전기 품질 보상 장치, 감시 모니터링/진단 설비 등의 다양한 장비들과 장비들 사이의 통신을 위해 케이블, 광섬유, DSL, 위성, 무선랜, 전력선 통신 등을 포함한 다양한 통신 기술들이 사용된다. 이와 같은 스마트 그리드 환경을 간단히 표현하면 그림 1과 같다[2].

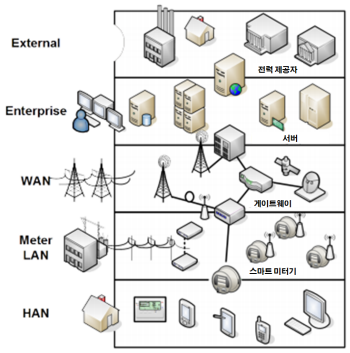

그림 1 스마트 그리드 환경
Fig. 1 Smart grid environments

우리나라에서는 스마트 그리드 기술이 국가발전 신 패러다임인 "저탄소 녹색성장"과 맞물려 주목을 최근 1~2년 사이에 주목받고 있으나, 미국의 경우는 노후화된 전력망의 현대화와 광대역 전력망의 효율적인 운영을 위해서 2000년 초반부터 전력연구원(Electric Power Research Institute: EPRI)을 중심으로 스마트 그리드에 대한 연구가 시작되었고 2007년에는 스마트 그리드 법안으로 알려진 'Energy Independence and Security Act of 2007'이 제정되면서 활발히 스마트 그리드 기술을 실현하고 있다. 유럽은 2000년 이후 높은 수준의 신재생에너지 보급으로 인해 발생된 전력 시스템의 다양한 복잡성을 해결하기 위해 스마트 그리드 기술에 대한 연구가 이루어지고 있으며 가까운 나라 일본에서도 저탄소 기술과 배터리 기술을 중심으로 적극적으로 스마트 그리드 기술을 추진하고 있다.

스마트 그리드 환경을 구축하게 됨으로써 실시간 변동 전기 요금제를 통한 소비자의 자율적인 전력 사용량 절감 유도와 신재생 에너지를 이용한 자연친화적인 환경을 구축함으로써 화석연료 사용량을 절감할 수 있고 이로 인해 CO2 배출량을 획기적으로 줄일 수 있을 것이다. 이외에도 소비전력 모니터링 및 무정전의 고품질 전력 제공과 같은 소비자 지향의 다양한 전력 서비스를 제공받을 수 있다. 이렇듯 차세대 전력망인 스마트 그리드를 구현함으로써 제공되는 서비스는 무궁무진할 것이며 이로 인한 경제적 효과 역시 상당할 것으로 예상된다.[6][9]

2.1.2 스마트 그리드의 통신 구조

양방향 통신을 지원함으로써 공급자와 수요자의 능동적인 참여를 이끌어 낼 수 있는 스마트 그리드의 통신 구조를 살펴보면 다음과 같다. 우선 가정이나 빌딩과 같은 소비자 영역(Customer Premise)의 네트워크를 구성하는 HAN(Home Area Network), BAN(Building Area Network) 그리고 IAN(Industrial Area Network)이 있고 여기에 사용되는 주요 표준 프로토콜로는 ZigBee, 802.11, HomePlug 등이 있다. 소비자 영역 외부에서는 가정 및 빌딩에 설치되는 스마트 미터(Smart Meter)들을 서로 연결함으로써 네트워크 망을 형성하는 NAN(Neighborhood Area Network)을 구축하게 되며 여기서는 Wimax, WLAN, RF Radio, FTTH, PLC 등과 같은 다양한 프로토콜을 사용한다.

이 후 공공망이나 사설망을 통해 보다 넓은 영역의 광대역 망인 WAN(Wide Area Network)을 형성하고 최종 제어센터 및 각종 서버들이 존재하는 엔터프라이즈 영역과 연결됨으로써 스마트 그리드의 전력서비스 네트워크를 구성하게 된다.

2.2 개체 인증 메커니즘

인증(Authentication)이란 신분의 검증을 의미하며 개체 인증은 인증을 요구하는 사용자가 본인임을 증명하는 과정으로, 고정된 패스워드나 스마트 카드 등을 이용하여 식별된 자신의 신분과 행위를 증명하는 것을 의미한다. 스마트그리드와 같은 M2M 통신 환경에서의 인증은 이러한 사용자 인증의 의미와 더불어 네트워크에 접속된 다양한 디바이스 또는 디바이스 소유자가 정당한지를 확인하는 과정까지 포함한다.

네트워크 환경에서 사용자를 인증하기 위해서는 일반적으로 사용자가 알고 있는 것, 사용자가 소유한 것, 사용자만의 고유한 특성 등을 이용하며, 패스워드 시스템, 대칭키/공개키 암호 시스템 또는 인증 서버를 사용하는 방식이 있다. 본 절에서는 인증 메커니즘의 대표적인 유형들의 특징에 대해 간략히 설명한다.

2.2.1 패스워드를 이용한 인증 시스템

사용자와 서버 사이에 사전에 공유한 패스워드를 이용한 인증 방식으로 구축이 용이하여 널리 사용되고 있으며, 대표적인 프로토콜로 Password Authentication Protocol(PAP), Challenge-Handshake Authentication Protocol(CHAP) 등이 있다. 그러나 사용하는 패스워드의 길이가 짧을 경우에 사전 공격에 대해 안전하지 않다는 문제점이 있다.

2.2.2 암호 시스템을 이용한 인증 시스템

대칭키 암호 시스템을 이용한 인증 방식은 사용자와 서버 사이에 사전에 공유한 비밀키를 이용한다. 이 방식에서는 서버가 매 세션마다 새롭게 생성한 challenge 값을 사용자에

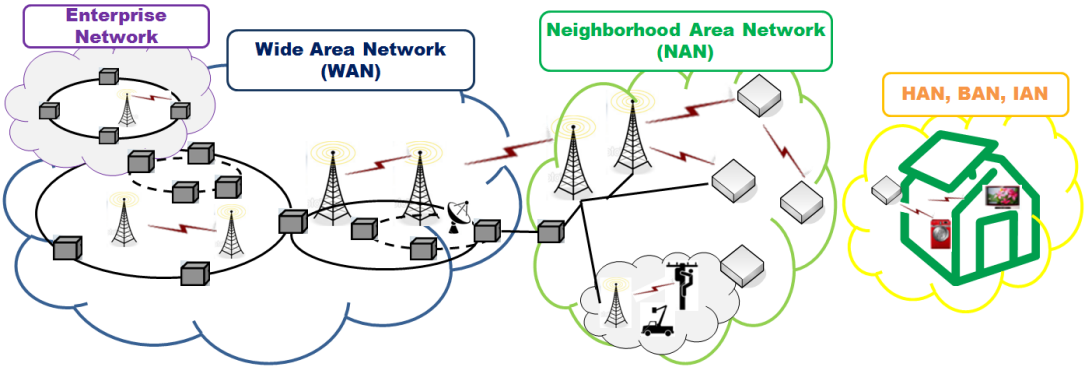

그림 2 스마트 그리드의 통신 구조
Fig. 2 Smart grid Communication architecture

게 전송하고, 사용자는 사전에 공유한 키로 이를 암호화하여 response를 전송함으로써 인증을 받게 된다. 기존의 패스워드 시스템에 비해 상대적으로 긴 키를 이용하기 때문에 안전하고, challenge 값이 재사용되지 않으므로 도청에 의한 재전송 공격이 불가능하다는 장점이 있다. 그러나 별도의 인증서버 없이 디바이스와 서버 간에 점대점(point-to-point) 인증을 수행하는 경우에는 각 서버에 사용자 계정 정보를 저장해야 하므로 안전성 및 관리적 측면에서 비 효율이고, 서버의 내부 관리자에 의한 비밀키 유출과 같은 보안 문제점이 존재한다.

반면에 공개키 암호 시스템을 이용한 인증 방식에서는 서버가 전송한 challenge 값에 대해 사용자가 전자서명을 생성하여 전송함으로써 인증을 수행한다. 대칭키 암호 시스템을 이용하는 방식과 달리 사전에 공유한 비밀정보가 없으므로 서버에는 사용자 인증을 위한 어떠한 비밀 정보도 저장되지 않는다는 장점이 있다. 그러나 공개키 암호 시스템을 사용하기 위해 공개키 기반구조(PKI)와 같은 부가적인 시스템이 필요하다.

2.2.3 인증 서버를 이용한 인증 시스템

인증 서버를 이용하는 인증 시스템은 중앙에 사용자들의 계정 정보를 저장하는 별도의 인증 서버를 설치하여 응용 서버들이 사용자 인증 및 과금 등을 처리할 수 있도록 하는 방식이다. 이 방식에서는 각 응용 서버들은 사용자 인증을 위한 별도의 정보를 유지할 필요가 없으며, 인증 서버와의 통신을 통해 사용자 인증을 수행하고 필요할 경우에는 사용자와 세션키를 설립할 수도 있다. 이 방식은 대규모 시스템에 적용 가능하고 인증 시스템의 유지·보수가 편리하다는 장점이 있다.

즉, 패스워드 기반의 인증 방식은 도청에 의한 재전송 공격, 온라인/오프라인 사전공격 등에 취약하고, 대칭키 암호 시스템을 이용한 디바이스와 서버 사이의 인증 방식은 안전성 및 관리 효율성 측면에 문제가 있으며, 공개키 암호 시스템을 사용하는 인증 방식은 PKI와 같은 별도의 인프라가 필요하다는 단점이 있다.

스마트그리드 환경은 다수의 스마트미터가 서버에 연결되어 있는 구조로, 각각의 서버가 사용자의 계정 정보를 유지하는 것은 바람직하지 않으며 PKI를 사용하는 경우 연산량이 과도하게 발생한다는 단점이 있다.

따라서, 본 논문에서는 스마트 그리드환경에 적합한 인증 메커니즘을 개발하기 위해 가장 적절한 인증 형태로 인증 서버를 이용하는 방식을 사용한다.

3. 스마트 그리드 보안

3.1 보안 위협

스마트 그리드는 다양한 통신 장비와 통신 기술을 이용하여 유무선의 통신 네트워크 환경을 구축한다. 따라서 스마트 그리드 환경에서는 기존의 통신 환경에 존재하는 보안 위협과 함께 스마트 그리드 환경이 갖고 있는 특징으로 인한 추가적인 보안 위협이 존재할 수 있다. 스마트 그리드 환경에서 발생할 수 있는 보안 위협은 프라이버시, 데이터 변조, 데이터 불법 도용 및 접근, 침투, 서비스 마비 등이 있으며, 스마트 그리드 통신 구조에서 발생할 수 있는 세부적인 보안 공격의 유형은 그림 3과 같다.

2.1 보안 요구사항

앞에서 설명한 스마트 그리드 환경에서 발생할 수 있는 보안 위협에 대응하기 위해서는 정보보호의 3대 목표인 기밀성(confidentiality), 무결성(integrity), 가용성(availability)에 관련된 보안 요구사항을 정의해야 한다. 안전한 스마트

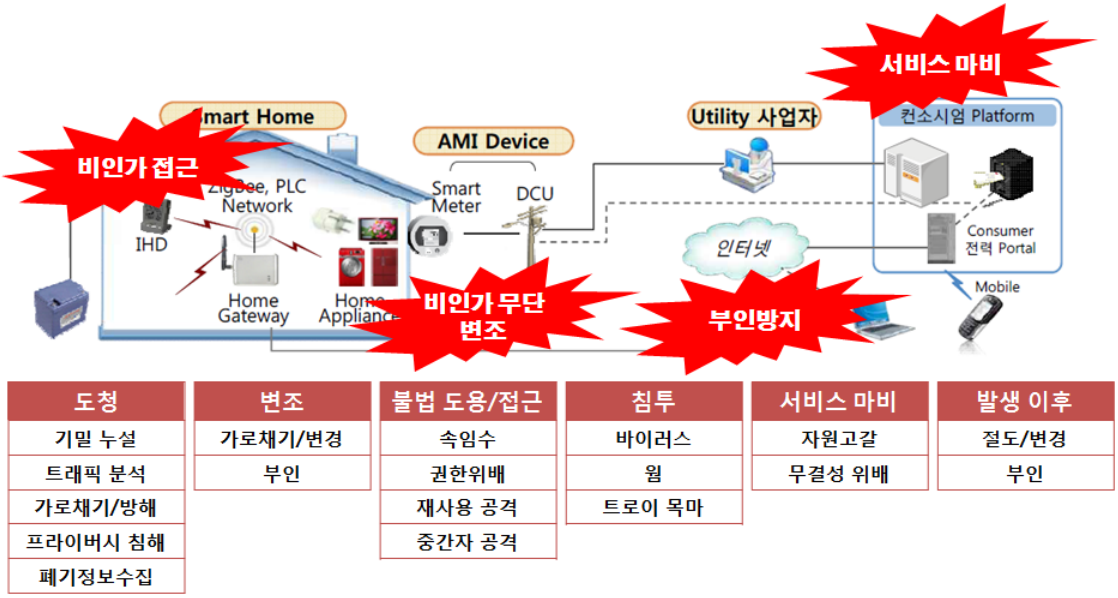

그림 3 스마트 그리드 환경의 보안 위협
Fig. 3 Security threats in Smart grid

그리드 환경을 구축하기 위해 고려해야 하는 보안 요구사항의 세부적인 내용은 다음과 같다.[10]

① 데이터 기밀성 : 스마트 그리드 환경에서 원격 디바이스로부터 수집되는 데이터의 경우, 사용량이나 요금 관련 정보 등 민감한 정보들이 네트워크를 통해 전송되므로 비인가된 제 3자가 데이터의 내용을 알 수 없도록 암호화 등의 메커니즘을 이용하여 중요 정보를 보호해야 한다.

② 데이터 무결성 : 스마트 그리드 환경의 경우 제 3자가 중간자 공격(man-in-the-middle attack)을 이용하여 서버와 디바이스 사이에 전송되는 메시지를 위·변조하는 공격이 가능하다. 따라서 이러한 보안 위협에 대응하기 위해 개체 사이에 전송되는 데이터의 무결성을 보장할 수 있는 메커니즘이이 필요하다.

③ 디바이스 무결성 검증 : 스마트 그리드 환경에서 스마트 미터기와 같은 디바이스들은 일반적으로 사람이나 다른 보호 수단에 의해 지켜지지 않거나 감시되지 않는 장소에 배치되며 서비스를 제공하기 위해 중요한 데이터를 처리하는 장치들이다. 이와 같은 디바이스들은 비용 감축 및 구현 용이성의 이유로 인해 대부분 개방형 인터페이스를 지닌 플랫폼에서 구현된다. 디바이스 무결성 검증이 보장되지 않는 경우에는 제 3자가 설치된 디바이스에 악성 소프트웨어를 삽입하거나 디바이스의 역할을 변경함으로써 네트워크를 오염시키거나 장치의 가용성을 손상 시킬 수 있다. 따라서 장치에 대한 무결성 검증이 추가적으로 요구된다.

④ 디바이스 가용성 : 가용성에 대한 대표적인 공격방법인 서비스 거부 공격(DoS: Denial of Service)은 시스템의 가용성 및 생산성을 훼손하는 방법으로 시스템 자원과 정보에 대한 접근 능력을 감소시킨다. 따라서 스마트 그리드 환경에서도 주체 또는 디바이스들의 정보 접근 능력을 침해하지 않도록 가용성을 보장할 수 있는 적절한 보안 메커니즘이 요구된다.

⑤ 디바이스 인증 : 스마트 그리드 환경에서 중앙의 서버가 원격 디바이스 또는 게이트웨이로부터 데이터를 수집한 후에 데이터가 올바르고 정당한 디바이스에서 온 것인지를 검증할 수 있는 디바이스 인증 절차를 제공해야 한다.

⑥ 서버 인증 : 스마트 그리드 환경의 서버에 대한 인증이 제공되지 않는 경우에는 공격자가 정당한 서버로 위장하여 정당한 디바이스들이 보내는 메시지를 획득하는 공격이 가능하다. 따라서 디바이스가 서버에게 메시지를 보내기 전에 정당한 서버인지를 확인할 수 있는 인증 절차가 요구된다.

⑦ 접근제어 및 인가 : 스마트 그리드 환경에서 관리자나 사용자들이 원격지에 배치된 디바이스에 접근하려는 경우 부적절한 접근 및 인가 권한을 초과하는 애플리케이션 및 사용자의 행위를 방어하기 위한 접근제어 및 인가 메커니즘이 필요하다.

⑧ 네트워크 오용 방지 : 스마트 미터기와 같은 디바이스는 비교적 도난의 위협에 쉽게 노출되어 있으며, 공격자가 불법적으로 획득한 통신 모듈을 이용하여 네트워크에 접속하여 허가 없이 네트워크를 사용할 수 있다. 따라서 보안 솔루션을 통하여 고의적 또는 실수로 인한 불법적 사용을 방지해야 한다.

⑨ 부인방지 : 스마트 그리드 환경에서 메시지 송수신 후 또는 통신이나 처리가 실행된 후에 그 사실을 증명함으로써 사실 부인을 방지하는 메커니즘이 필요하다. 이러한 메커니즘을 통해 메시지를 수신하고도 메시지가 전달된 사실이 없다고 주장하는 수신자 측의 부인을 방지하며 또는 역으로 메시지를 전달하지 않고도 송신하였다고 주장하는 송신자 측의 부인을 방지할 수 있다.

4. 제안하는 접근제어 메커니즘

스마트 그리드 환경에서 허가된 원격 사용자만이 디바이스에 접속하여 원하는 작업을 수행할 수 있게 하고, 반대로 원격 사용자가 불법 디바이스에 접속하여 원하지 않는 디바이스에게 자신의 정보를 누출하는 등의 보안 문제를 방지하기 위해 별도의 사용자 인증 메커니즘이 반드시 필요하다. 즉, 원격 사용자와 디바이스 간에 안전한 통신을 제공하기 위해서는 서로 간에 상호인증이 요구된다.

본 논문에서는 스마트그리드 환경의 통신 구조를 고려하여, 인증 서버로부터 발급받은 티켓을 이용한 상호인증 메커니즘을 제안한다. 인증서버와 티켓을 이용한 인증 메커니즘은 Kerberos를 비롯한 다양한 시스템에서 사용한 방식으로[5][7], 본 논문에서는 인증서버를 이용하여 원격 사용자와 디바이스 간에 상호인증을 수행하기 위해 메시지를 간소화하고 키 확인을 제공할 수 있는 메커니즘을 제안한다.

4.1 가정 사항 및 표기법

제안하는 메커니즘에서 디바이스는 항상 인증 서버와 통신이 가능한 범위 안에 존재하며 디바이스, 게이트웨이 그리고 인증서버는 부채널 공격 등의 물리적 공격에 대해 안전하고, 게이트웨이와 인증서버는 안전한 채널을 통해 메시지를 교환한다고 가정한다. 제안하는 메커니즘에서 사용하는 기호와 의미는 표 1과 같다.

4.2 제안하는 접근제어 메커니즘

제안하는 접근제어 메커니즘은 필요한 파라미터들을 등록하는 사전단계와 상호 인증 및 키 교환을 위한 단계로 구성된다. 그리고 디바이스에 저장된 공유 비밀키를 갱신하기 위한 과정이 필요하다.

표 1 기호
Table 1 Notaion

기호	의미
ID_A	사용자의 식별자
ID_D	디바이스의 식별자
ID_S	인증서버의 식별자
TS_i	타임스탬프
$lifetime$	티켓의 유효기간
IP_A	사용자 A의 네트워크 주소
K_A	사용자의 패스워드로 유도된 비밀키
K_S	인증서버와 디바이스 사이의 공유 비밀키
MAC_A	A의 메시지 인증 코드
$Ticket$	인증 서버가 발행한 티켓
SK	사용자와 디바이스 사이의 세션키
$f_{SK}(a)$	메시지 인증 코드를 생성하는 일방향 함수
$\{a\}_{SK}$	대칭키 SK를 이용한 메시지 a의 암호화

4.2.1 사전 단계

인증서버는 디바이스의 등록과정에서 디바이스의 ID_D와 공유 비밀키 K_S를 생성하여 디바이스의 메모리에 안전하게 저장하고, 자신의 데이터베이스에 디바이스의 ID_D와 공유 비밀키 K_S를 테이블로 보관한다. 인증서버와 등록된 디바이스 사이에 공유한 비밀키 K_S는 향후 원격 사용자 인증을 위한 티켓을 생성하는데 사용한다.

그리고 디바이스에 접근을 원하는 원격 사용자들은 인증서버에 자신의 ID와 패스워드를 사전에 등록한다. 이때 사용자의 패스워드는 디바이스 접근을 위한 티켓을 암호화에 사용하는 키 생성에 사용되므로, 제 3자의 사전공격(Dictionary attack)에 대응할 수 있도록 영문 대/소문자, 숫자, 특수문자 등을 포함하여 8자리 이상이 되도록 안전하게 생성하고 주기적으로 갱신하는 것이 필요하다.

4.2.2 상호인증 및 키 교환 프로토콜

원격 사용자 A는 그림 3과 같이 자신의 ID와 접근하고자 하는 디바이스의 ID를 인증서버에게 전송하고 해당 디바이스의 접근 허가를 받기위해 필요한 티켓 생성을 요구한다. 티켓을 받은 원격 사용자 A는 이를 디바이스에 전달함으로써 디바이스와 상호인증 및 세션키를 설립한다. 구체적인 동작과정은 다음과 같다.

① 원격 사용자는 디바이스에 접근하는데 필요한 티켓을 발급받기 위해 자신의 ID_A와 접근하고자 하는 디바이스의 ID_D, 타임 스탬프 TS_1을 인증서버에 전송한다.

② 인증서버는 디바이스와 원격 사용자를 위한 세션키 SK를 생성한 다음 디바이스와 공유한 비밀키 K_S를 이용하여 다음과 같이 티켓을 생성한다.

$$Ticket = \{ID_A \| IP_A \| SK \| lifetime \| TS_2\}_{K_S}$$

티켓에 포한되는 정보는 티켓의 유효기간을 나타내는 $lifetime$, 재전송 공격을 방지하기 위한 타임스탬프 TS_2와 세션키 SK, 원격 사용자의 식별자와 네트워크 주소를 포함한다.

③ 인증 서버는 사용자에게 티켓을 안전하게 전송하기 위해 원격 사용자 A의 패스워드로부터 유도된 비밀키 K_A로 세션키와 티켓, TS_2를 암호화하여 전송한다.

이때 $Ticket$은 사용자 A의 패스워드로부터 유도된 비밀키로 암호화되므로 사용자 A를 제외한 다른 사람은 해당 패킷을 획득하더라고 정당한 티켓을 얻을 수는 없다.

④ 원격 사용자는 자신의 패스워드를 이용하여 K_A를 생성하고 인증서버로부터 전달받은 메시지를 복호하여 티켓과 세션키 SK를 획득한다.

⑤ 원격 사용자는 타임스탬프 TS_3을 생성하고 디바이스에 전달할 메시지의 무결성을 검사하는데 필요한 메시지 인증 코드를 다음과 같이 생성한다.

$$MAC_A = f_{SK}(ID_A \| IP_A \| TS_3)$$

⑥ 원격 사용자는 $ID_A, ID_D, MAC_A, Ticket, TS_3$를 게이트웨이에게 전송한다.

⑦ 게이트웨이는 원격 사용자로부터 수신한 메시지의 ID_D를 통해 접근하려는 디바이스를 식별하고 해당 디바이스 D에게 $ID_A, MAC_A, Ticket, TS_3$을 전달한다.

⑧ 메시지를 전달받은 디바이스는 인증 서버와 공유한 비밀키 K_S를 통해 티켓을 복호하여 세션키 SK를 획득한다.

⑨ 디바이스 D는 획득한 세션키를 통해 MAC_A를 검증하여 원격 사용자를 인증한다.

⑩ 디바이스 D는 원격 사용자에게 디바이스의 정당성을 확인시키기 위해 획득한 세션키를 이용하여 $\{TS_3 + 1\}_{SK}$를 계산한다.

⑪ 디바이스 D는 원격 사용자의 식별자 ID_A와 $\{TS_3 + 1\}_{SK}$를 게이트웨이에게 전송한다.

⑫ 게이트웨이는 디바이스로부터 수신한 메시지 ID_A와 $\{TS_3 + 1\}_{SK}$를 원격 사용자에게 전달한다.

⑬ 원격 사용자는 SK를 이용하여 수신한 메시지를 복호함으로써 디바이스를 인증하고 공유된 세션키를 이용하여 보안 채널을 설립하고 비밀 통신을 수행한다.

4.2.3 공유 비밀키 갱신 프로토콜

원격 사용자를 위한 티켓의 암호화/복호화에 사용하는 인증서버와 등록된 디바이스 사이에 공유 비밀키 K_S는 주기적으로 갱신할 필요가 있다. 인증서버는 디바이스 D와 공유한 비밀키 K_S를 갱신하기 위해 다음과 같이 새롭게 생성한 공유 비밀키 K_S'를 기존의 공유 비밀키로 암호화하여 전송한다.

$$\text{공유 비밀키 갱신정보} = E_{K_s}(ID_S \| ID_D \| K_s' \| TS_1)$$

5. 안전성 분석 및 응용 분야

5.1 안전성 분석

제안하는 프로토콜에 대한 안전성 분석으로 재사용 공격, 위장 공격에 대해 안전한지 살펴보고 상호인증 및 키 교환에 대한 보안 요구사항을 만족한다는 것을 세부적으로 설명한다. 제안하는 프로토콜은 원격지에서 특정 디바이스에 접근하려는 사용자와 디바이스 사이에 상호인증 및 키 교환을 수행하며, 재사용 공격과 위장 공격에 대해 안전하다. 이에 대한 구체적인 내용은 다음과 같다.

① 상호인증 및 키 교환 : 제안하는 프로토콜은 인증 서버가 생성한 티켓과 세션키를 통해 원격 사용자와 디바이스의 상호인증 및 키 교환을 수행한다. 원격 사용자는 티켓과 MAC_A를 디바이스에게 전달함으로써 디바이스는 이 값의 검증을 통해 원격 사용자가 정당한 사용자임을 인증할 수 있다. 또한 인증 서버가 발행한 티켓은 오직 디바이스 D만이 복호할 수 있기 때문에 세션키를 이용하여 암호화 한 $\{TS_3+1\}_{SK}$를 원격 사용자에게 전달함으로써 원격 사용자는 디바이스를 인증할 수 있다. 그리고 원격 사용자와 디바이스 사이에 설립된 세션키 SK를 이용하여 보안 채널을 설립할 수 있으므로, 그림 3에서 나타낸 도청, 변조, 불법 도용/접근, 침투와 같은 공격으로부터 안전하다.

② 재사용 공격 : 제안하는 프로토콜에서는 타임스탬프를 이용하여 전달되는 메시지의 재사용 여부를 확인하므로 재사용 공격에 대해 안전하다.

③ 위장 공격 : 제안하는 프로토콜에서는 공격자가 디바이스에 대해 원격 사용자로의 위장하려는 경우, 공격자는 정당한 MAC_A 값을 생성해야 한다. 그러나 정당한 MAC_A값을 생성하기 위해서는 세션키 SK가 필요하고, 올바른 SK를 획득하기 위해서는 원격 사용자의 패스워드로부터 유도된 비밀키 K_A를 알아야 하므로, 이를 모르는 공격자는 정당한 MAC_A 값을 생성할 수 없으므로 원격 사용자로의 위장이 불가능하다. 또한 공격자가 원격 사용자에게 접근하려는 디바이스로 위장하려는 경우에도 공격자는 세션키 SK를 획득할 수 없으므로 디바이스로 위장하는 것이 불가능하다. 따라서 제안하는 상호인증 및 키 교환 프로토콜은 위장 공격에 대해 안전하다.

5.2 응용 분야

스마트 그리드 환경에서는 전력 소비자의 각 가정에 스마트 미터기를 설치함으로써 전력 업체와 전력 소비자 간의 양방향 통신을 제공한다. 이러한 스마트 그리드 환경의 특징으로 기존의 전력 계통과는 달리, 전력 업체에서는 미터기 점검을 위해 각 가정에 직접 방문하지 않고 각 가정의 스마트 미터기에 원격으로 접속하여 스마트 미터기를 점검하거나 이상이 있을 경우 조기에 탐지할 수 있게 된다. 그리고 전력 소비자들도 회사 또는 위치적으로 가정에서 멀리 떨어진 곳에 있더라도 가정의 스마트 미터기에 원격으로 접속함으로써 현재 가정에서 소비되는 전력이 어느 정도인지 확인할 수 있고 낭비되는 전력이 있다면 원격으로 해당 기기의 전원을 차단함으로써 낭비되는 전력을 방지할 수 있다. 최근 들어 생산 전력의 최대 수요처인 가정의 에너지 소비 효율을 높이기 위한 HEMS(Home Energy Management System)에 대한 연구가 활발히 진행되고 있다.

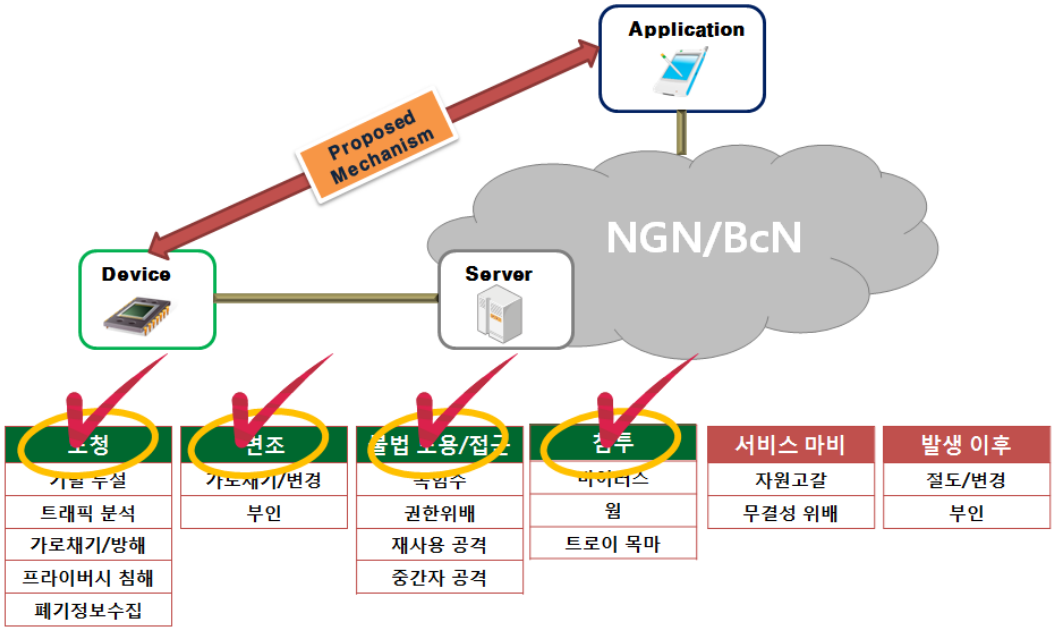

그림 4 제안하는 메커니즘의 안전성
Fig. 4 Security of the proposed mechanism

- 구글 파워미터 : 구글은 전력 소비자 각 가정에서 소비되는 전력량을 알려주는 구글 파워미터(Google Power Meter)를 계획하고 있다. 구글 파워미터는 스마트 미터기 또는 가정 내의 에너지 관리 장치 등을 통해 전기 사용량을 수집하고 이를 그래프로 나타내어 전기 사용량을 실시간이나 하루 동안의 사용량 합계 등의 다양한 형태로 제공한다. 이를 통해 전력 소비자들 각 가정의 전력 소비 패턴을 확인할 수 있고 또한 예상 요금을 미리 계산함으로써 자율적으로 소비 전력에 대한 낭비를 줄일 수 있다. 이러한 서비스를 위해 구글은 국외에서 2009년 10월 처음으로 디바이스 파트너인 북미 에너지사와 협력 관계를 체결하였다. 이에 따라 에너지사의 TED 5000단말을 구입한 전력 소비자는 자신의 휴대폰에서 아이구글(iGoogle) 화면을 통해 자신의 전력 사용량을 확인할 수 있다.

- DEHEMS : DEHEMS(The Digital Environment Home Energy Management System) 프로젝트는 유럽 연합의 주도하에 가정에서의 에너지 효율을 개선하기 위한 기술 프로젝트이다. DEHEMS는 에너지가 들어오고 이를 모니터링하는 수준을 넘어 에너지가 현재 어느 장비에서 사용되는지 실시간으로 모니터링하여 가전기기에 대한 서비스 효율을 높인다. 또한 이러한 가전기기 및 서비스를 휴대폰이나 PC를 통해 원격으로 제어할 수 있도록 서비스를 확대하고 있다.

6. 결 론

스마트 그리드란 기존의 전력망에 정보기술이나 첨단기술을 접목하여 공급자와 전력 소비자 사이에 양방향으로 실시간 정보를 교환함으로써 에너지 효율을 최적화하는 차세대 지능형 전력망이다. 그러나 이러한 스마트 그리드 환경은 스마트 미터기(smart meter), AMI(advanced metering infrastructure)와 같은 지능형 장치를 통한 양방향 통신 사이에서 데이터 노출 및 데이터 도용 등과 같은 다양한 보안 위협들이 존재할 가능성이 있다. 이와 같은 보안 위협들은 소비자 측면에서는 개인 프라이버시와 관련된 문제가 발생할 수 있으며 궁극적으로는 국가적 사이버 보안과 관련된 보안문제로 야기 될 수 있다.

본 논문에서는 스마트 그리드 환경에서 원격 사용자와 디바이스 사이에 상호인증 및 키 교환을 통해 기밀성, 무결성, 가용성을 보장할 수 있는 보안 메커니즘을 제안하였다. 제안하는 메커니즘은 양방향 상호 인증을 제공하고 세션마다 다른 공통키의 설립을 통해 재전송 공격 및 위장 공격에 대해 안전하다는 장점이 있다.

감사의 글

이 논문은 2010년도 호서대학교의 재원으로 학술연구비 지원을 받아 수행된 연구임“(2009-0489)

참 고 문 헌

[1] A. Aziz and W. Diffie, "A secure communications protocol to prevent unauthorized access, privacy and authentication for wireless local area networks" IEEE Personal Communications, vol. 1, no. 1 pp.25-31, 1994
[2] Erich W. Gunther, Aaron Snyder, Grant Gilchrist Darren Reece Highfill, Smart Grid Standards Assessment and Recommendations for Adoption and Development, 2009
[3] ETSI, “ETSI TR v 0.0.9 Machine-to-Machine communications(M2M); Smart Metering Use Cases, 2009
[4] ETSI, “ETSI TS 102 689 v 0.1.1 Machine-to-Machine communications(M2M); M2M service requirement, 2009
[5] RFC 1510, “The Kerberos Network Authentication Service”, 1993
[6] U.S. Department of Energy, The Smart Grid: An Introduction. 2009
[7] Yixin Jiang, et al, “Authentication and Key Exchange Protocols for Roaming Services in Wireless Mobile Networks”, 2006.
[8] 박찬국, 전력인프라 사이버보안 이슈와 정책 대응
[9] 장동원, 이영환, 스마트 그리드 표준화 동향 연구
[10] 은선기, 전서관, 안재영, 오수현, “안전한 M2M 통신 구축을 위한 상호인증 및 키 교환 프로토콜”, 한국정보보호학회 논문지, 제20권 제1호, pp. 73-83, 2010.

저 자 소 개

오 수 현 (吳 秀 賢)

1998년 2월: 성균관대학교 정보공학과 졸업(공학사)
2000년 2월: 성균관대학교 전기전자 및 컴퓨터공학과 석사(공학석사)
2003년 8월: 성균관대학교 전기전자 및 컴퓨터공학과 박사(공학박사)
2004년 3월~현재: 호서대학교 정보보호학과 교수
<관심분야> 암호학, 네트워크 보안, 정보보호 평가・인증

은 선 기

2008년 8월: 호서대학교 정보보호학과 졸업(공학사)
2009년 2월~현재: 호서대학교 정보보호학과 석사과정
<관심분야> 네트워크 보안, 보안 프로토콜, 시스템 평가 및 인증