情報保護學會論文誌
第 22 卷 第 3 號, 2012. 6

스마트그리드 보호를 위한 AMI 망 분리 및 인증 프레임워크*

최 재 덕,† 서 정 택‡
ETRI 부설연구소

Separate Networks and an Authentication Framework in AMI for Secure Smart Grid*

Jaeduck Choi,† Jungtaek Seo‡
The Attached Institute of ETRI

요 약

본 논문에서는 스마트그리드 통신망 보호를 위한 AMI 망 분리와 인증 프레임워크를 제안한다. 기존 AMI 구조에서는 기기들이 직·간접적으로 인터넷과 연계되어 있고, AMI 네트워크에 대한 접근제어 인증을 고려하지 않아 악의적인 목적의 전력망 침투 공격에 취약하다. 또한 AMI 전력망에 존재하는 여러 인증 구간과 AMI 연계장치에 다양한 인증 프로토콜을 수용해야 하는 환경을 고려한 효율적인 인증 프레임워크 연구가 이루어지고 있지 않다. 제안하는 AMI 전력망 분리는 스마트미터를 댁내 기기 및 인터넷과 물리적으로 분리하고, 인증 프레임워크는 네트워크 및 응용 레벨 인증을 EAP 기반의 인증 구조 및 절차로 통합한다. 제시된 AMI 전력망 보안대책은 안전하고 효율적이며, 향후 스마트그리드 AMI 구축 설계에 유용하게 활용될 것으로 기대된다.

ABSTRACT

This paper proposes methods of securing Smart Grid system against various types of cyber threats by separating AMI networks from the public network, the Internet, and providing an AMI specific authentication framework. Due to the fact that thousands and millions of AMI devices to be deployed would be directly or indirectly connected to the public network without any authentication procedures for access control, currently being developed AMI architectures could be widely exposed to considerable number of penetrating attacks. Furthermore, there have not been a sufficient number of researches on authentication frameworks with basis on the specific circumstances of AMI networking that should support varied authentication protocols among security associations and AMI linking devices. This work makes a proposal of isolating smart meters from HAN devices and the Internet and integrating network/application level authentication frameworks with an EAP-based authentication architecture. These approaches are beneficial to deploy AMI with security and efficiency.

Keywords: Smart Grid, AMI, Security, Separate Networks, Authentication

접수일(2011년 9월 8일), 수정일(2011년 11월 11일), 게재확정일(2011년 11월 14일)
* 본 연구는 2010년도 지식경제부의 재원으로 한국에너지기술평가원(KETEP)의 지원을 받아 수행한 연구 과제입니다. (No. 2010101040046A)
† 주저자, cjduck@ensec.re.kr
‡ 교신저자, seojt@ensec.re.kr

I. 서 론

스마트그리드는 기존 전력망에 IT 기술을 활용하여 전력공급자와 소비자 간에 실시간으로 전력 관련 정보를 양방향으로 교환 및 활용함으로써 에너지 효율성을 증진시키기 위한 융합 기술이다. 현재 국내·외적으로 전력망 지능화에 공감하고 있으며 스마트그리드 구축을 위해 법·제도, 표준화, 연구개발 측면에서 다양한 노력이 이루어지고 있다[1-3]. 이와 같은 스마트그리드 구축 노력과 함께 중요한 이슈로 부각되는 것이 스마트그리드 보안이다[4-6]. 국가 산업의 근간이 되는 전력망에 IT 기술이 융합되면서 기존 IT 보안위협이 그대로 전력망에 상속되어 국가에 재앙적 수준의 피해가 가해질 수 있기 때문이다.

스마트그리드의 주요 보안위협 요인은 전국적으로 산재되어 있는 스마트그리드 기기를 통해 악의적인 공격자가 온·오프라인으로 전력망에 쉽게 접근이 가능해졌다는 점이다[6]. 기존 전력망에서는 발·송·배전망 자동화를 위한 네트워크 구축 및 운영이 이루어졌으며, 전력망 자체가 주요 보호시설로 지정되어 있어 일반인 및 전력소비자들이 접근하기 쉽지 않은 환경이었다. 그러나 스마트그리드는 악의적인 전력소비자들이 댁내에 설치된 스마트미터를 통해 AMI (Advanced Metering Infrastructure) 망 및 전력공급자 내부 망에 접근할 수 있는 용이한 환경이다. 예를 들어, 악의적인 공격자가 댁내에 설치된 스마트미터의 유선 통신라인에 물리적으로 접근할 수 있으며, 스마트미터와 DCU(Data Concentration Unit) 간 무선 통신구간을 통해 AMI 망에 접근할 수 있다. 또한 스마트미터가 다양한 전력서비스 제공을 위해 댁내 기기들과 함께 직·간접적으로 인터넷과 연결되어 있을 경우에 전국적으로 분포되어 있는 스마트미터가 AMI 망 접근을 위한 경유지로 악용될 수 있다.

현재 국내·외적으로 스마트그리드 보안가이드라인, 스마트미터 보안 요구사항 및 보안기술 등을 위주로 활발하게 연구가 진행되고 있지만, AMI 망 접근제어 및 통합 인증 구조 측면은 고려하고 있지 않다[7-9]. 먼저, NISTIR 7628[7] 및 국·내외에서 고려하는 스마트그리드 환경[11-12]에서는 스마트미터가 인터넷과 직·간접적으로 연결되어 있는 댁내 기기들과 물리적으로 연결되어 있어, 스마트미터를 경유하여 AMI 망 및 전력시스템 내부 운영 망까지 접근할 수 있는 가능성이 있다. 기존 스마트미터 보안기술들은 미터링 데이터의 유출 및 변조를 방지하기 위한 응용 레벨의 보안대책에 국한되며[8-9], DCU와 같은 AMI 연계장치를 통해서 AMI 망에 접근하는 시도를 차단할 수 있는 네트워크 레벨의 보안대책을 고려하고 있지 않다. 또한 AMI 연계장치에서 네트워크 레벨 인증 및 다양한 전력사업자의 스마트미터 인증 프로토콜을 수용해야 하는 환경을 고려한 효율적인 인증 프레임워크 연구가 이루어지고 있지 않다. 따라서 AMI 망 보호를 위해 스마트미터를 댁내 기기들과 물리적으로 분리하여 운영할 필요가 있으며, 더불어 AMI 망 접근제어를 위한 네트워크 레벨의 인증과 다양한 응용 레벨 인증을 수용할 수 있는 효율적인 인증 프레임워크 연구가 필요하다.

본 논문에서는 스마트그리드 전력망 보호를 위한 AMI 망 분리 구조 및 인증 프레임워크를 제안한다. 먼저, AMI 네트워크를 AMI 전력망과 전력서비스 망으로 구분하고 물리적으로 분리된 구조를 제시한다. AMI 전력망 인증 프레임워크로는 네트워크 및 응용 레벨 인증의 효율성을 고려하여 EAP (Extensible Authentication Protocol)[10] 기반의 인증 구조 및 절차를 제시한다. AMI 전력망 분리 구조 및 인증 프레임워크는 인터넷과 직·간접적으로 연결되어 있는 댁내 기기들을 통한 무분별한 스마트미터 접근 및 스마트미터를 경유한 AMI 전력망 접근 시도를 근본적으로 차단한다. 또한, 제안하는 EAP 기반의 AMI 전력망 인증 구조 및 절차는 유·무선 통신기술별 다양한 기존 및 신규 인증 기술 수용이 용이하고, 네트워크 레벨의 인증 절차를 간소화한다. 기존 스마트그리드 보안 연구에서는 미터링 서비스에 대한 보안프로토콜 위주의 연구가 이루어졌으며, 본 논문에서 제시한 것과 같은 AMI 망 분리 및 인증 프레임워크는 기존에 연구되지 않았다. 제안한 AMI 망 분리 및 인증 프레임워크는 안전성과 효율성을 갖추었으며, 향후 안전한 AMI 구축에 유용하게 활용될 것으로 기대된다.

본 논문의 구성은 다음과 같다. Ⅱ 장에서 기존 AMI 구조와 인증기술 현황 분석 및 문제점에 대해서 고찰하고, Ⅲ 장에서 스마트그리드 보호를 위한 AMI 망 분리 구조와 인증 프레임워크에 대해서 제안하고, Ⅳ 장에서 제안 구조 및 인증 프레임워크의 안전성 및 효율성에 대해서 분석하고, 마지막으로 5장에서 결론을 맺는다.

II. AMI 구조 및 인증 기술 현황, 문제점 고찰

본 장에서는 기존 AMI 네트워크 구조 및 인증 기술들을 살펴보고, 스마트그리드 전력망 보호를 위한 AMI 망 분리 및 응용·네트워크 레벨의 인증 필요성과 인증 적용에 있어서 효율성 제고를 위한 인증 프레임워크 필요성에 대해서 고찰한다.

2.1 AMI 네트워크 구조

스마트그리드는 전력 사용의 효율성을 제고하기 위해 발·송·배전, 전력거래시장, 수용가 사이의 전력 시스템들이 다양한 유·무선 통신기술로 연결되어 있는 거대한 네트워크이다. 각 수용가에서 스마트미터에 의해 검침되는 전력소모량 데이터는 발전사의 발전량 조절 및 전력사의 송·배전 계통 운영에 반영되어 전력 사용을 효율적으로 사용하는데 중요한 정보이다. 이를 위해 NIST에서는 스마트그리드의 논리적 아키텍처 및 각 구성요소별 논리 인터페이스를 정의하였다[7]. 스마트미터는 수용가 내적으로 3rd Party 및 고객정보시스템 등과 외부 네트워크(인터넷)로 연계된 HAN(Home Area Network) 게이트웨이 및 에너지관리시스템들과 연결되어 있으며, 수용가 외적으로 AMI-Headend를 통해 MDMS (Meter Data Management System)로 연결된다. MDMS는 논리적 인터페이스로 연계된 배전 SCADA(Supervisory Control And Data Acquisition), 송전SCADA, 발전시스템 등과 연계되어 있다.

AMI는 스마트그리드 네트워크의 핵심 인프라로 배전 및 수용가와 전력사 간에 전력 관련 정보의 양방향 통신을 위해 다양한 유·무선 통신 기술로 구성된다. AMI는 전력사 내의 미터링 데이터 관리 시스템인 MDMS, 전력사와 수용가를 연결하는 연계장치(DCU), 수용가 미터링 데이터를 검침하는 스마트미터, HAN 영역 내 기기들로 나눌 수 있다. 이들 기기 및 시스템들은 PLC, 이더넷, 광통신, ZigBee, Wi-Fi, WiBro, CDMA 등의 통신기술로 연결되며, 특정 지역이나 특정 전력사의 선호도에 따라서 인터넷 연결과 함께 다양하게 조합될 수 있다. 국내외 사례를 통해서 AMI는 댁내 기기, 스마트미터 또는 HAN 게이트웨이, AMI 네트워크 연계장치, 전력사업자 제어센터들이 유·무선 통신 기술로 상호 연계되어 있는 구조로 연구 및 실증되고 있음을 확인할 수 있다[11-12].

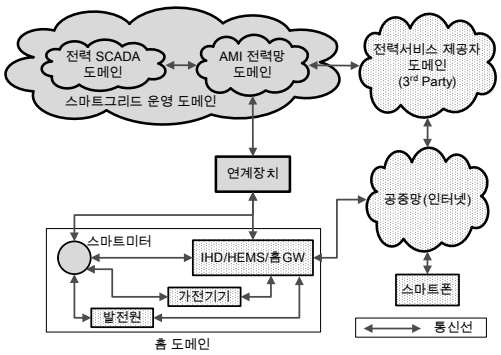
2.2 AMI 인증 기술 현황

현재 다양한 유·무선 통신 기술이 사용되는 AMI에서 각 유·무선 통신 기술별 인증 및 키교환 프로토콜들에 대해서 살펴본다. 먼저, 유선 통신 환경을 살펴보면, 하위 계층에서 통신 방식을 정의한 PLC, 이더넷, 광통신 기술에서는 별도의 인증 및 키교환 프로토콜이 정의되어 있지 않으며, AMI 서비스에 따라 상위 계층에서 IPSec(IP Security), TLS (Transport Layer Security)와 같은 인증 및 키교환 프로토콜들이 사용된다. 이와는 별도로 AMI 기기·시스템·네트워크·서비스 특성을 고려하여 다양한 공개키 또는 비밀키 기반의 인증 및 키교환 기술들이 적용될 수도 있다. Wi-Fi, WiBro, 3GPP 무선 네트워크에서는 무선 단말의 네트워크 액세스 인증과 무선 구간에서 데이터 기밀성 및 무결성을 제공하기 위해 EAP-TLS [13], EAP-PKMv2(EAP-Privacy Key Management) [14], AKA(Authentication and Key Agreement)[15], EAP-AKA[16]가 표준으로 정의되어 있다. 이들 인증 및 키교환 프로토콜들은 무선 기지국에서 인증되지 않은 임의 단말들에 대해 네트워크 접근을 차단하며, 무선 구간에서 교환되는 데이터의 무결성 및 기밀성을 제공하기 위한 비밀키를 제공한다. ZigBee의 경우, ZigBee SEP(Smart Energy Profile) 2.0에서는 네트워크 및 응용 계층에서 인증 및 키교환을 다루고 있으며, 응용 계층에서 HTTP over TLS 사용을 규정하고 있다[17]. 유·무선 통신 기술별 표준 인증 및 키교환 기술 이외에, 스마트그리드에서 안전한 미터링 서비스를 위한 인증 및 키교환 프로토콜로 AKA 프로토콜을 적용한 연구도 발표되었다[9].

2.3 문제점 고찰

• AMI 전력망 분리

스마트그리드 전력망을 악의적인 공격자의 무분별한 접근 시도로부터 보호하기 위해 AMI 핵심 필드 기기들을 댁내 기기 및 인터넷과의 연계로부터 차단해야 한다. 스마트그리드 환경에서 발·송·배전 도메인은 여전히 일반인들이 접근하기 어려운 망으로 구성되어 있으나, AMI 도메인의 경우 실시간 전력소



〔그림 1〕 기존 AMI 기기·시스템 간 연계도

모 현황, 실시간 전력 요금제, 수요반응 전력서비스, 댁내 가전기기 제어 등과 같은 전력서비스 제공을 위해 스마트미터, IHD(In-Home Display), HEMS(Home Energy Management System), 홈게이트웨이 등의 댁내 기기들이 AMI 도메인 및 인터넷과 연계되어 있다. 〔그림 1〕은 앞서 살펴본 NISTIR 7628의 스마트그리드 논리적 아키텍처 및 국·내외 AMI 네트워크 구조 사례를 바탕으로 일반화한 AMI 구성도이다. 〔그림 1〕과 같은 AMI 구조에서는 공격자들이 온라인으로 댁내 기기들에 접근할 수 있으며, 더 나아가 댁내 기기들을 경유하여 스마트미터 및 스마트그리드 전력 운영망에 접근시도 또는 사이버 공격도 가능하다. 방화벽 등의 정보보호제품을 사용하여 이와 같은 불법접근을 차단할 수도 있지만, 방화벽 정책설정 및 관리 부실에 따른 보안위협이 여전히 발생할 수 있다. 따라서 다양한 연계접점을 통한 온라인 접근위협으로부터 스마트그리드 전력망을 보호하기 위해 최소한의 AMI 필드기기로 구성된 AMI 전력망과 인터넷을 통해 다양한 전력서비스 제공을 위한 AMI 전력서비스망이 물리적으로 분리될 필요가 있다.

• AMI 응용 레벨 인증

AMI 응용 레벨 인증의 정의는 미터링 서비스, 기기 상태정보 모니터링 서비스, 기기 관리·제어 서비스 등이 안전하게 수행될 수 있도록 기기 간 상호인증 수행 후 교환되는 데이터를 보호하기 위한 비밀키를 공유하는 것이다. 응용 레벨 인증은 AMI 전력망을 보호하기 위한 기본 보안 서비스이다. 미터링 데이터는 전력 공급에 중요한 지표가 되기 때문에 변조될 경우 전력 공급 과잉 또는 부족 문제가 발생할 수 있다. 미터링 데이터의 유출은 전력 사용 패턴 분석을 통해 사생활 침해를 유발할 수 있다. 기기 상태정보 모니터링 및 관리·제어 데이터의 유출·변조는 전력망 침투 및 운영 장애에 유용한 정보로 악용될 수 있다. 따라서 이와 같은 보안위협으로부터 AMI 전력망을 보호하기 위한 서비스별 응용 레벨 인증이 필요하다.

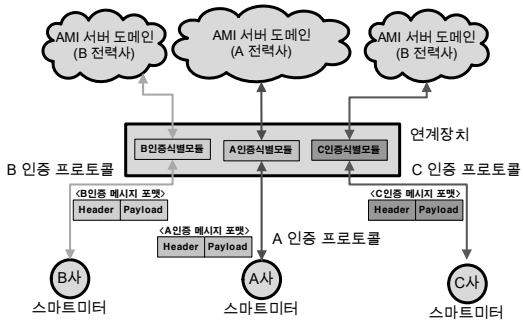
• AMI 네트워크 레벨 인증

AMI 네트워크 레벨 인증의 정의는 비인가된 노드들이 AMI 통신망을 이용하여 연계장치 또는 AMI 서버에 접근하는 행위 등을 차단할 수 있도록 AMI 구성 노드 구간별로 상호인증 수행 후 비인가 패킷 검증을 위한 비밀키를 공유하는 것이다. 즉, 각 AMI 노드들이 수신하는 패킷들의 MAC(Message Authentication Code) 값 검증을 통해 네트워크 액세스를 제어하는 것이다. 앞서 언급한 AMI 망 분리 구조를 통해 악의적인 공격자들의 스마트미터 온라인 접근을 차단하더라도, 지리적으로 광범위하게 분포되어 있는 스마트미터 및 연계장치의 유·무선 통신구간에 물리적으로 접근하여 AMI 망에 액세스를 시도할 수 있다. 예를 들어, 악의적인 댁내 공격자가 스마트그리드 운영 도메인에 접근하기 위해 댁내 스마트미터, IHD/HEMS/홈게이트웨이의 PLC, ZigBee, 이더넷 등의 통신라인을 직접 악용할 수 있다. 또한 악의적인 외부 공격자는 ZigBee, Wi-Fi와 같은 무선 통신 구간을 통해 직접 AMI 망에 침투를 시도하거나 AMI 망 자체에 불필요한 대량 패킷 전송을 통해 네트워크 성능 저하 공격을 감행할 수 있다. 따라서 비인가 기기들의 AMI 망 접근을 차단하기 위해 AMI 망 분리와 함께 AMI 망 내 필드 기기들에 대해 암호학적 인증 기술을 사용하여 인증된 필드기기들의 통신만 허용할 수 있는 네트워크 레벨의 액세스 인증이 필요하다.

• AMI 인증 프레임워크

앞서 살펴본 AMI 망 분리, 응용 및 네트워크 레벨 인증과 같은 스마트그리드의 안전성을 확보하기 위한 보안대책과 함께 보안대책에 대한 효율성도 고려해야 한다. 보안대책 효율성을 고려하기 위해서는 암호알고리즘, 프로토콜 차원의 효율성 측면도 있지만, 본 논문에서는 인증 구조 측면에서의 효율성에 대해서 살펴본다.

인증 프레임워크 연구를 통해 응용 및 네트워크 레벨의 여러 인증 절차들을 구조적으로 간소화하여



〔그림 2〕 연계장치에서 멀티 인증 프로토콜 수용 구조

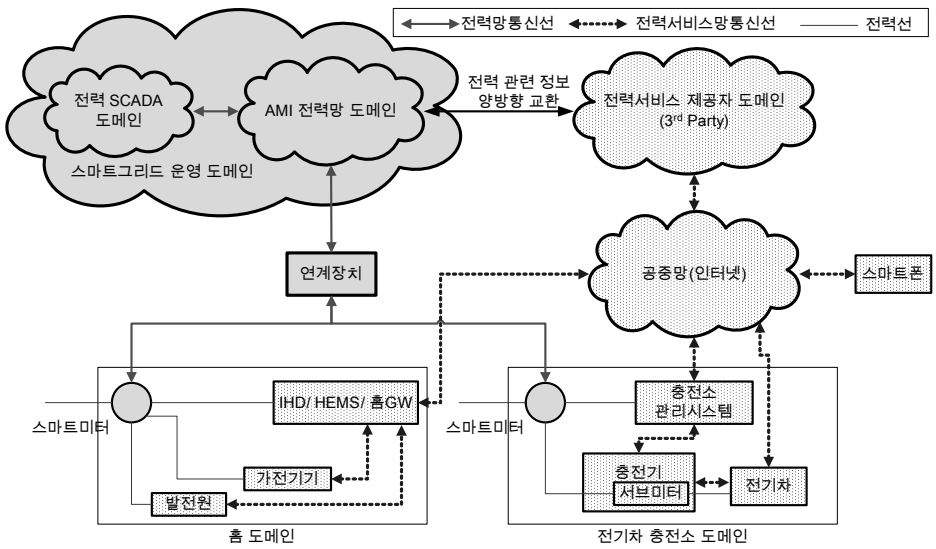
효율성을 증대시킬 수 있으며, 다양한 기존 및 신규 인증 프로토콜들을 구조적으로 수용할 수 있는 확장성을 통해 비용 절감 효과를 얻을 수 있다. 예를 들어, 스마트미터는 AMI 서버와 응용 레벨 인증 절차를 수행해야 하며, 연계장치와도 네트워크 레벨 인증 절차를 수행해야 하는 중복성 때문에 암호학적 연산 부담이 발생하고 메시지 교환 횟수도 증가한다. 또한 스마트미터와 AMI 서버 간에는 미터링 데이터에 대한 과금 분쟁을 해소하기 위해 미터링 데이터에 대한 서명 기능이 필요하므로 공개키 기반의 인증 프로토콜이 요구되지만, 서명 기능이 요구되지 않는 연계장치와 AMI 서버 간에도 동일한 공개키 기반의 인증을 적용한다면 공개키 연산 수행에 따른 추가적인 암호학적 연산이 요구된다.

운영 측면의 효율성 저하 요인을 살펴보면, 여러 전력사업자들이 공존하는 스마트그리드 환경에서 〔그림 2〕와 같이 전력사업자들이 개별 스마트미터를 설치하고, 전력사업자별 응용 레벨 인증 프로토콜을 운영할 경우 전력사업자들이 공유하는 AMI 연계장치에서는 모든 스마트미터의 인증 프로토콜 메시지를 식별할 수 있는 모듈을 탑재해야 하는 부담이 있다. AMI 연계장치는 스마트미터로부터 수신한 메시지가 인증 요청 메시지인지 확인한 후 AMI 서버에 포워딩해야 하므로 모든 인증 프로토콜 메시지를 식별해야 한다. 인증 요청 메시지 여부를 식별하지 않으면, AMI 서버에 불법적으로 접근을 시도하는 행위 등을 차단할 수 없다. 또한 AMI 연계장치에서는 암호의 경량화 기술이 진보되면서 현재 스마트미터에 적용된 응용 레벨 인증 프로토콜들에 대한 스펙 및 절차 등의 규격이 변경될 때마다 신규 인증 프로토콜 메시지를 식별할 수 있는 모듈을 업데이트해야 하는 부담도 발생한다. 따라서 AMI 망에 존재하는 여러 인증 구간과 AMI 연계장치에서 다양한 인증 프로토콜을 수용해야 하는 환경을 고려한 효율적인 인증 프레임워크 연구가 필요하다.

III. 제안하는 AMI 망 분리 및 인증 프레임워크

3.1 AMI 망 분리

〔그림 3〕은 제안하는 AMI 전력망의 물리적 분리



〔그림 3〕 제안하는 AMI 전력망 및 전력서비스망 분리 구조

구조를 보여준다. AMI 전력망은 스마트미터와 DCU와 같은 연계장치, AMI 서버만으로 구성되며, AMI 전력서비스망은 IHD, HEMS, 홈게이트웨이, 발전원 등과 같은 댁내 기기들이 상호 연계되어 있고 인터넷과도 연결되어 전력 소비자에게 다양한 전력서비스를 제공할 수 있도록 구성된다. 제안 구조에서 AMI 전력망은 미터링 서비스 및 기기 제어·모니터링 기능만 수행하고, AMI 전력서비스망은 AMI 전력망 서버으로부터 전력서비스 가입자별 검침데이터, 실시간 전력거래 가격 등을 제공받아 실시간 전력 소모량, 일별·주별·월별 전력 사용량, 실시간요금제, 수요반응 서비스, 댁내 기기 원격 제어, 전기차 충전 과금 서비스 등과 같은 다양한 전력서비스를 인터넷을 통해 전력 소비자에게 제공한다. 제안 구조는 스마트그리드에서 전력 소비자의 전력 소모량, 전력거래 가격 정보, 소비자의 전력 예상 수요 정보 등을 AMI 전력망과 AMI 전력서비스망 도메인 차원에서 양방향 교환함으로써 기존에 다양한 스마트그리드 서비스를 제공할 수 있다.

3.2 AMI 인증 프레임워크

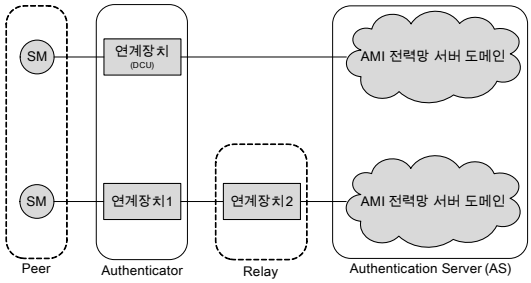
앞 절에서 인터넷으로부터 AMI 전력망의 무분별한 접근 시도를 차단할 수 있도록 AMI 전력망을 분리하였지만, 여전히 악의적인 공격자가 스마트미터의 유·무선 통신 라인을 통해 AMI 전력망에 접근할 수 있기 때문에 네트워크 레벨의 인증이 필요하다. 또한 다양한 서비스 정보 보호를 위한 응용 레벨의 인증이 요구된다. 본 절에서는 응용 및 네트워크 레벨이 통합된 AMI 전력망 인증 프레임워크에 대해서 설명한다.

3.2.1 AMI 전력망 인증 프레임워크

제안하는 인증 프레임워크는 AMI 전력망 구조, 구간 별 보안협상, 응용 및 네트워크 레벨 보안협상 절차, 노드별 비밀키 생성 구조로 구성된다.

• AMI 전력망 구조

본 논문에서 고려하는 인증 적용을 위한 AMI 전력망은 〔그림 4〕와 같다. AMI 전력망에 스마트미터, 스마트미터와 AMI 서버 사이의 연계장치 (예, DCU, 무선 통신 기지국 등), AMI 서버들이 존재하고, 이들이 〔그림 4〕과 같이 2가지 유형으로 존재

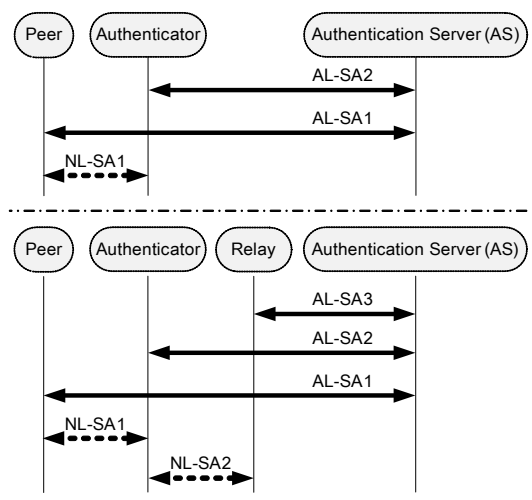


〔그림 4〕 AMI 전력망 구성

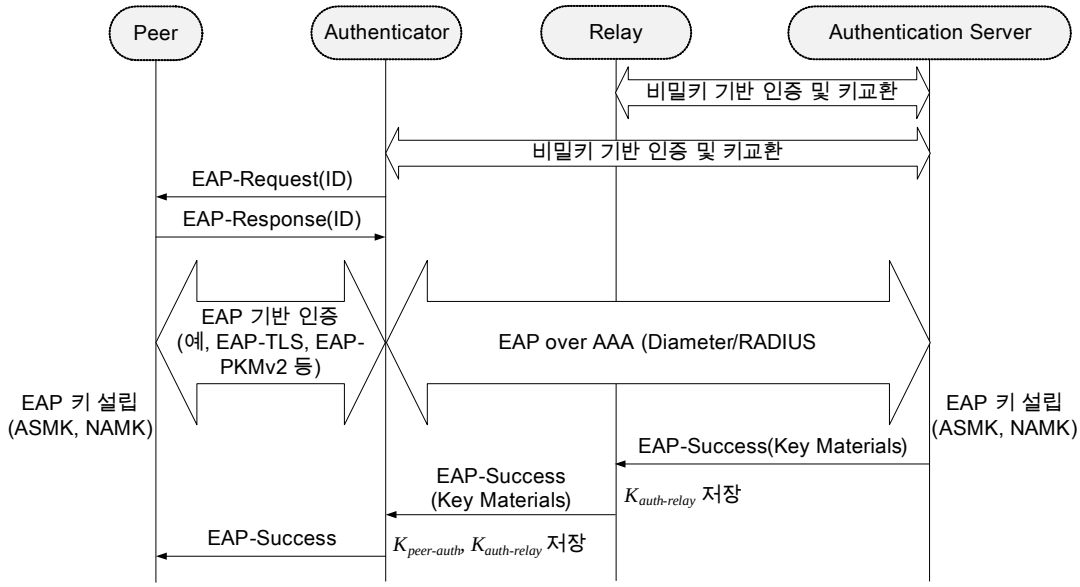
하는 것을 가정한다. AMI 전력망 구성 노드들 간 유·무선 통신은 다양한 유·무선 통신 기술들의 조합으로 구성될 수 있다.

• 보안협상 구간

AMI 전력망 인증 프레임워크에서 네트워크 및 응용 레벨의 보안협상 SA(Security Association)는 〔그림 5〕와 같다. Peer는 AMI 전력망 접근제어 대상이 되는 스마트미터이고, Authenticator는 Peer의 AMI 전력망 접근제어를 수행하는 DCU와 같은 연계장치이고, Relay는 네트워크 구성에 따라 Authenticator와 AS(Authentication Server) 사이에서 인증 관련 파라미터들을 전달해주는 선택적 연계장치이며 네트워크 구성에 따라 Authenticator에 대한 AMI 전력망 접근제어를 수행한다. AS는 Peer, Authenticator, Relay와 필요한 서비스를 수행하며 서비스 보호를 위해 기기들과 상호 인증 및 키교환을 수행하는 AMI 서버이다. 응용 레



〔그림 5〕 AMI 전력망의 논리적 노드 구간별 보안협상



〔그림 6〕 AMI 전력망 보안협상 절차

벨 보안협상 AL-SA(Application Level-SA)는 스마트미터와 AMI 서버 사이에서 미터링 데이터 보호 및 스마트미터 제어 메시지, 연계장치와 AMI 서버 사이에서 연계장치 관리 및 제어 메시지 등을 보호하기 위한 상호인증 및 키교환을 의미하고, 네트워크 레벨 보안협상 NL-SA(Network Level-SA)는 인가된 AMI 전력망 노드들만 AMI 전력망에 접근할 수 있도록 접근제어를 수행하기 위한 상호인증 및 키교환을 의미한다.

• 응용 및 네트워크 레벨 보안협상 절차

AMI 전력망 인증 프레임워크는 응용 및 네트워크 레벨 보안협상의 다양한 인증 프로토콜을 수용할 수 있고, 중복된 인증 절차를 간소화하기 위하여 EAP 기반의 인증 구조 및 절차를 갖는다. 〔그림 6〕은 Peer, Authenticator, Relay, AS로 구성된 AMI 전력망에서 제안하는 응용 및 네트워크 레벨 보안협상 절차를 보여주며, 세부 단계는 아래와 같다. Peer, Authentication, AS로만 구성된 AMI 전력망에 대한 보안협상은 아래 절차에서 AL-SA3와 NL-SA2 관련 부분을 제외하여 수행할 수 있다.

단계 1. Relay와 AS 간 AL-SA3, Authenticator와 AS 간 AL-SA2 수행 (AL-SA3과 AL-SA2는 비밀키 기반의 인증 및 키교환 프로토콜로 수행되며, 본 논문에서는 특정 프로토콜을 정의하지는 않는다. 또한 EAP 기반의 인증 방식도 AL-SA3과 2에서는 해당되지 않는다.)

① AL-SA별 노드 간 비밀키 기반의 상호 인증 수행

② AL-SA별 노드 간 마스터 키 MK (SA3_MK, SA2_MK) 생성

③ 각 노드가 MK로부터 서비스별 세션 비밀키 생성 (예, KEK1, KEK2 등)

단계 2. Peer와 AS 간 AL-SA1 수행 (AL-SA1은 EAP 기반의 공개키 인증 및 키교환 프로토콜로 수행되며, 본 논문에서는 특정 프로토콜을 정의하지는 않는다. 또한, 전체 인증 과정은 EAP 및 EAP over AAA로 동작한다〔10〕〔18-19〕.)

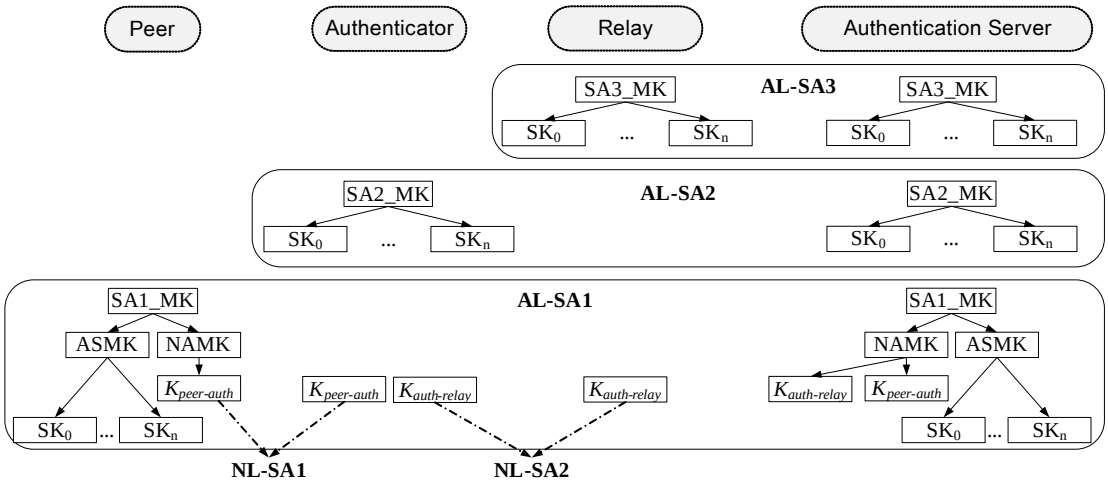
① Peer와 AS 간 인증서 기반의 상호 인증 수행

② Peer와 AS 간 MK 생성 및 MK로부터 ASMK(Application Service Master Key)와 NAMK(Network Access Master Key) 생성

③ AS는 NAMK로부터 비밀키 $K_{auth-relay}$와 $K_{peer-auth}$를 해쉬함수와 같은 비밀키 생성함수를 통해 생성

④ Peer는 NAMK로부터 비밀키 $K_{peer-auth}$를 해쉬함수와 같은 비밀키 생성함수를 통해 생성

⑤ AS는 비밀키 $K_{auth-relay}$를 Relay와 AS 간



〔그림 7〕 AMI 전력망 비밀키 계층 구조

공유된 세션 비밀키 KEK1(Key Encryption Key)로 암호화 $Enc_{KEK1}(K_{auth\text{-}relay})$, 2개의 비밀키 $K_{peer\text{-}auth}$과 $K_{auth\text{-}relay}$를 Authenticator와 AS 간 공유된 세션 비밀키 KEK2로 암호화 $Enc_{KEK2}(K_{peer\text{-}auth}||K_{auth\text{-}relay})$

⑥ 단계 ⑤에서 암호화된 비밀키들을 EAP-Success 메시지에 포함하여 Peer에게 전송

⑦ EAP-Success 메시지를 수신한 Relay는 비밀키 $K_{auth\text{-}relay}$를 복호화 ($Dec_{KEK1}(K_{auth\text{-}relay})$) 및 비밀키 저장, 수신한 EAP-Success의 파라미터 $Enc_{KEK1}(K_{auth\text{-}relay})$는 제거하고 Authenticator로 전송

⑧ EAP-Success 메시지를 수신한 Authenticator는 2개의 비밀키 $K_{peer\text{-}auth}$과 $K_{auth\text{-}relay}$를 복호화 ($Dec_{KEK2}(K_{peer\text{-}auth}||K_{auth\text{-}relay})$) 및 비밀키 저장, 수신한 EAP-Success의 파라미터 Enc_{KEK2} ($K_{peer\text{-}auth}||K_{auth\text{-}relay}$)는 제거하고 Peer로 전송

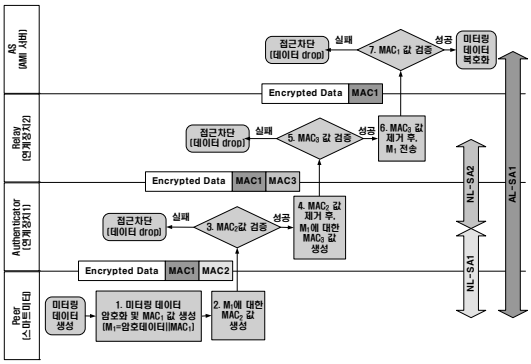
⑨ Peer는 EAP-Success 메시지 수신 및 AL-SA1 종료

• 노드별 비밀키 생성 구조

각 노드에서 생성되는 비밀키 구조는 〔그림 7〕과 같다. AL-SA3, AL-SA2, AL-SA1으로부터 각 노드들은 마스터키 SA3_MK, SA2_MK, SA1_MK를 공유하고, 마스터키로부터 보호하고자 하는 서비스에 맞춰 별도 세션키 SK(SK_0, …, SK_n)들을 해쉬함수 등을 사용하여 생성한다. 예를 들면, AS가 Relay와 Authenticator로 네트워크 액세스 제어 비밀키($K_{peer\text{-}auth}$, $K_{auth\text{-}relay}$)들을 암호화하여 전송하기 위한 KEK1과 KEK2를 SA3_MK와 SA2_MK로부터 각각 생성할 수 있다. 또한 스마트미터와 AS는 브로드캐스트 메시지를 위한 그룹키와 그룹키를 안전하게 전송하기 위한 KEK3을 ASMK로부터 생성하여 사용할 수 있다. 각 구간별 네트워크 액세스 인증을 위한 비밀키의 경우, Peer는 NAMK로부터 생성하고, Authenticator와 Relay는 AS로부터 전달받는다.

• AMI 전력망 액세스 제어 및 미터링 데이터 보호 Use Case

AMI 전력망 인증 프레임워크를 통해 응용 및 네트워크 보안협상 절차가 모두 완료되면, 미터링 데이터 보호를 위해 ASMK를 사용하는 것과 별도로 Peer, Authenticator, Relay는 $K_{peer\text{-}auth}$와 $K_{auth\text{-}relay}$를 사용하여 AMI 전력망 접근제어를 수행한다. 〔그림 8〕은 AMI 전력망 액세스 제어 및 미터링 데이터 보호의 예시를 보여준다. Peer는 ASMK로부터 유도된 기밀성 및 무결성 비밀키를 사용하여 미터링 데이터를 암호화하고 MAC_1 값을 생성한다. 또한 Peer는 Authenticator와 공유하고 있는 비밀키 $K_{peer\text{-}auth}$를 사용하여 MAC_2를 생성하고, 암호화된 미터링 데이터 및 MAC_1 값과 함께 Authenticator에게 전송한다. 여기서, MAC_2값은



〔그림 8〕 AMI 전력망 인증 프레임워크 기반의 보안 Use Case

Authenticator를 통해 AMI 전력망에 무단으로 접근하는 시도를 차단하는 역할을 수행한다. Authenticator에서 MAC_2 값 검증에 성공하면, Relay와 공유하고 있는 비밀키 $K_{auth\text{-}relay}$를 사용하여 MAC_3 값을 생성하고 암호화된 미터링 데이터 및 MAC_1과 함께 Relay 노드에게 포워딩한다. 동일한 방법으로 Relay 노드에서 MAC_3 값 검증에 성공하면, Relay 노드는 암호화된 미터링 데이터와 MAC_1 값만을 AS에게 전달한다. 여기서, MAC_3 값은 Relay를 통해 AMI 전력망에 무단으로 접근하는 시도를 차단하는 역할을 수행한다. 이와 같은 방법으로 AMI 전력망에서 각 통신 구간별 공유한 비밀키를 사용한 MAC 값 검증을 통해 인가되지 않은 노드로부터 수신되는 패킷들을 버림으로서 불필요한 패킷들의 AMI 전력망 접근을 차단하고, 미터링 데이터에 대한 기밀성 및 무결성을 제공한다.

IV. 안전성 및 효율성 분석

4.1 안전성

• AMI 전력망 비인가 접근

제안 구조 및 인증 프레임워크는 원격지 공격자들의 스마트미터 및 연계장치에 접근을 근본적으로 차단하며, AMI 전력망의 각 통신 구간에 물리적으로 불법접근이 이루어지더라도 AMI 각 연계장치에서 MAC 값으로 접근제어를 수행하기 때문에 비인가 접근으로부터 AMI 전력망을 보호한다. 제안하는 AMI 전력망 분리 구조를 살펴보면, 스마트미터와 AMI 연계장치는 댁내 기기 및 인터넷과 물리적으로 어떠한 연계점도 있지 않다. 따라서 임의의 공격자들이 인터넷을 통해 AMI 전력망에 접근할 수 있는 시도가 불가능하다. AMI 전력망 내에서 공격자들이 스마트미터의 유선 통신 라인에 물리적으로 접근하거나 무선통신으로 연계장치에 통신을 시도하더라도, NL-SA1에 의해서 스마트미터와 연계장치 간에 공유된 비밀키 $K_{peer\text{-}auth}$가 없는 공격자는 연계장치에 접근할 수 없다. 연계장치와 연계장치 사이에서도 NL-SA2에 의해서 생성된 비밀키 $K_{auth\text{-}relay}$로 생성된 MAC 값 검증을 통해 비인가 통신 노드의 AMI 전력망 접근 시도를 차단한다.

제안 구조는 필드기기 영역에서 AMI 전력망과 전력서비스망이 물리적으로 분리되어 있지만, AMI 전력망 서버 도메인과 전력서비스 제공자 도메인은 양방향으로 전력 관련 정보 교환을 위해 연계되어 있다. 이 연계점을 통해 공격자가 AMI 전력망에 침투할 수 있는 가능성은 존재하지만, AMI 전력망과 전력서비스망에서 각각의 인증 절차, 침입탐지 및 차단 등의 다양한 보안정책이 적용된다면 공격자가 침투하기 어렵다.

• 네트워크 레벨 보안협상의 안전성

NL-SA1과 NL-SA2의 산출물로 간주하는 비밀키 $K_{peer\text{-}auth}$와 $K_{auth\text{-}relay}$는 Peer, Authenticator, Relay, AS 간에 신뢰관계를 통해 생성되었으므로 안전하다. 제안하는 인증 프레임워크에서는 중복된 인증 절차를 줄이기 위하여 Peer, Authenticator, Relay 노드들이 수행해야 하는 네트워크 레벨 인증 NL-SA1과 NL-SA2를 직접적으로 수행하지 않는다. 대신 Peer와 AS 간에 수행하는 AL-SA1이 성공적으로 수행되면, AS는 Authenticator와 Relay에게 $K_{peer\text{-}auth}$와 $K_{auth\text{-}relay}$를 생성하여 안전하게 전달한다. Peer 측의 $K_{peer\text{-}auth}$는 Peer가 직접 생성하고, Authenticator 측의 $K_{peer\text{-}auth}$는 Peer와 상호 인증된 AS가 생성하여 안전하게 Authenticator에게 전달한다. Authenticator와 Relay 측의 $K_{auth\text{-}relay}$는 AL-SA2와 AL-SA3를 통해 상호 인증된 AS로부터 전달받는다. 따라서 비밀키 $K_{peer\text{-}auth}$와 $K_{auth\text{-}relay}$는 상호 인증을 통해 신뢰관계가 형성된 노드들로부터 생성 및 전달되기 때문에 안전한 비밀키 교환이 분배되었다고 할 수 있다.

• AMI 전력망 DDoS 공격

제안하는 AMI 전력망은 불필요한 트래픽 유발을 통해 네트워크 자원을 소모하는 DDoS 공격에 대응

할 수 있다. AMI 전력망 내에서 DDoS 공격 유발 트래픽은 인가된 스마트미터 또는 비인가된 스마트미터들끼리의 공모를 통해 이루어질 수 있다. 인가된 스마트미터에서의 DDoS 공격 유발 트래픽은 인가된 스마트미터의 IP 접속 차단 등을 통해서 대응할 수 있으며, 비인가된 스마트미터에서 유발된 대규모 더미(dummy) 트래픽들은 AMI 전력망의 각 통신 구간에서 생성된 비밀키 $K_{peer\text{-}auth}$와 $K_{auth\text{-}relay}$를 사용하여 AMI 전력망에 유입되는 더미 트래픽들을 차단할 수 있다.

• 데이터 위·변조 및 유출

제안하는 AMI 전력망에서 교환되는 데이터들은 각 응용 레벨 보안협상에 의해 데이터 무결성 및 기밀성이 제공된다. AMI 전력망 인증 프레임워크에서는 미터링 데이터의 양단간 전송 구간에서 응용 레벨 보안협상 AL-SA1을 통해 데이터의 무결성 및 기밀성을 제공한다. AL-SA1의 수행 결과로 ASMK가 생성되고, ASMK는 해쉬함수 등 비밀키 생성 함수를 통해 무결성 및 기밀성 비밀키들을 별도 생성하여 미터링 데이터를 보호한다. 스마트미터 및 연계장치 등의 관리 및 제어를 위한 데이터들도 AL-SA1, AL-SA2, AL-SA3 수행 결과로 생성된 ASMK, SA2_MK, SA3_MK로부터 별도의 세션키들을 생성하여 공격자들의 데이터 위·변조 및 유출 공격으로부터 보호할 수 있다.

• 인증 프레임워크 안전성

제안하는 인증 프레임워크의 안전성은 향후 본 인증 프레임워크에 적용될 인증 프로토콜, 비밀키 생성 함수, 기기 및 시스템에 저장되는 비밀정보에 의존한다. 기존 및 신규 인증 프로토콜이 인증 프레임워크에 적용될 때, 공개적으로 안전성이 입증된 프로토콜을 사용해야 한다. AL-SA1, AL-SA2, AL-SA3 수행 결과로 생성되는 마스터키 SA_MK1, SA_MK2, SA_MK3로부터 데이터 기밀성 및 무결성 비밀키, KEK 등의 세션키들은 해쉬함수 등과 같은 안전한 비밀키 생성 함수를 사용해야 하며, 기기 및 시스템에 저장되는 개인키, 비밀키, 비밀정보 등은 기기 및 시스템에 안전하게 저장되어야 한다.

4.2 효율성

• AMI 전력망 보안협상 절차 간소화

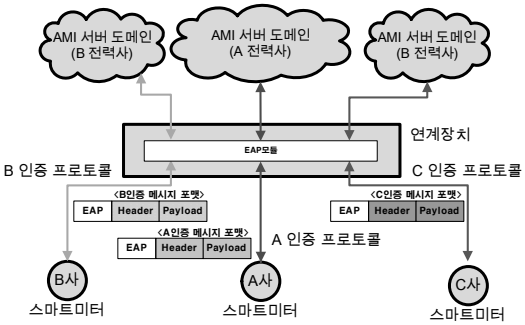
〔표 1〕 인증 절차 횟수 비교

	기존 방식	제안 방식
스마트미터	2	1
연계장치1	3	1
연계장치2	2	1
AMI 서버	3	3

제안 인증 프레임워크는 스마트미터 및 연계장치에서 수행하는 네트워크 레벨 보안협상 절차를 간소화한다. 스마트미터에서는 AL-SA1과 NL-SA1이 요구되지만, 2번의 인증 절차 AL-SA1과 NL-SA1를 수행하지 않고 AL-SA1을 수행하면서 스마트미터와 연계장치에서 필요한 비밀키 $K_{peer\text{-}auth}$를 분배하는 것으로 NL-SA1을 대체하였다. 즉, 스마트미터는 NL-SA1을 수행하기 위한 인증 프로토콜 메시지 교환 절차, 암호학적 연산 수행 과정이 필요하지 않다. 연계장치 간에도 NL-SA2를 AL-SA1을 수행하면서 비밀키 $K_{auth\text{-}relay}$를 분배하기 때문에, 추가적으로 NL-SA2를 수행하기 위한 인증 프로토콜 메시지 교환 절차 및 암호학적 연산 수행과정이 필요하지 않다. 〔표 1〕은 본 논문에서 제시한 인증 구조를 기반으로 인증 절차 측면에서 기존 방식과 제안 방식에서 각 노드의 인증 절차 횟수를 비교한 표이다. 또한 제시하는 AMI 전력망 비밀키 계층 구조에서 비밀키 생성에 따른 연산량 측면을 고려해 볼 때, 각 노드의 비밀키 생성은 암호학적 계산량이 적은 해쉬함수 등을 사용하기 때문에 큰 부담이 되지 않는다. 이와 같이 제안하는 인증 프레임워크는 네트워크 레벨 보안협상 NL-SA1과 NL-SA2의 인증 메시지 교환 측면과 암호학적 연산 부담 측면에서 효율적이다.

• EAP 인증 방식 적용에 따른 비용절감

EAP 기반의 인증 프레임워크에서 DCU와 같은 연계장치는 다양한 인증 프로토콜들을 수정 없이 수용할 수 있을 뿐만 아니라, 향후 스마트미터의 하드웨어 특성을 고려한 경량 인증 프로토콜들이 개발 될 경우에도 연계장치에서 특별한 업그레이드 없이 적용 가능하다. AMI 전력망 내 통신 노드들이 EAP 기반의 인증 구조를 따를 경우, 연계장치에서는 현재 표준 인증 프로토콜 및 향후 개발될 다양한 인증 프로토콜 규격에 상관없이 EAP 모듈만 탑재되어 개발되면 된다. 참고로, EAP는 여러 인증 방식의 수용성을 높이기 위해 개발된 프로토콜로서 경량 모듈로 구현할 수 있다. 따라서 AMI 전력망 연계장치에서



〔그림 9〕 연계장치에서 EAP 기반의 멀티 인증 프로토콜 수용 구조

는 새로운 인증 프로토콜 기술이 개발되어도 연계장치에 수정을 가하거나 교체할 필요가 없어 경제적으로 비용 절감 효과가 있다. 또한 하나의 연계장치가 다양한 제조사의 스마트미터 및 인증 프로토콜을 수용할 경우, 제안하는 EAP 인증 프레임워크는 연계장치에서 모든 인증 프로토콜 식별 모듈을 탑재하지 않고 EAP 모듈만 탑재하여 경량화 할 수 있다. 〔그림 9〕와 같이 연계장치에서는 스마트미터 및 AMI 서버로부터 수신하는 EAP 인증 메시지만을 확인하여 각 전력판매사의 AMI 서버 및 스마트미터로 포워딩하면 된다.

V. 결론

본 논문에서는 스마트그리드 전력망을 보호하기 위한 AMI 망 분리와 인증 프레임워크를 제안하였다. 기존 스마트그리드 보안 연구에서는 미터링 서비스와 같은 응용 레벨 수준의 보안 프로토콜 위주로 연구가 진행되었지만, 본 논문에서는 AMI 접근제어 측면에서 AMI 망 분리와 함께 네트워크 및 응용 레벨 수준의 효율적인 인증 프레임워크를 제시하였다. 제안하는 AMI 망 분리는 스마트그리드 환경에 산재해 있는 수많은 기기들을 통해 국가 기반 시설의 핵심인 전력망에 인터넷으로 접속할 수 있는 여건을 물리적으로 차단한다. 또한 AMI 전력망 인증 프레임워크는 AMI 데이터 보호 및 AMI 네트워크 액세스 제어를 통해 AMI 전력망의 안전성을 제공하며, AMI 전력망에서 중복된 인증 절차를 제거하고 다양한 기존 및 신규 인증 프로토콜들 적용에 있어서 연계장치에 비용 절감 효과가 있다. 향후 AMI 전력망 분리와 함께 다양한 응용 레벨 인증 프로토콜이 제안 인증 프레임워크에 적용되어 안전하면서 효율적인 AMI 전력망 구축에 기여할 것으로 기대한다.

참고문헌

〔1〕 NIST, "Draft NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 2.0," July 2011.

〔2〕 전황수, 하영욱, 조병선, "주요 국가의 스마트그리드 정책 동향," 전자통신동향분석, 25(3), pp. 89-98, 2010년 6월.

〔3〕 박창민, "스마트그리드 표준 기술," 한국통신학회지, 27(4), pp. 31-37, 2010년 3월.

〔4〕 전용희, "지능형 전력망(Smart Grid)과 정보보호," 정보보호학회지, 19(4), pp. 65-71, 2009년 8월.

〔5〕 이경복, 독고지은, 유지연, 이숙연, 임종인, "스마트 그리드에서의 소비자 참여와 보안 이슈," 정보보호학회지, 19(4), pp. 21-35. 2009년 8월.

〔6〕 이건희, 서정택, 이철원, "스마트그리드 사이버 보안 추진 현황," 정보보호학회지, 20(5), pp. 7-13, 2010년 10월.

〔7〕 NIST, "Guidelines for Smart Grid Cyber Security," NISTIR 7628, Aug. 2010.

〔8〕 J. Naruchiptparames, M.H Gunes, and C.Y Evrenosoglu, "Secure Communications in the Smart Grid," IEEE Consumer Communications and Networking Conference (CCNC) 2011, pp. 1171-1175, Jan. 2011.

〔9〕 전재우, 임선희, 이옥연, "스마트 그리드를 위한 Binary CDMA 기반의 AMI 무선 네트워크 구조 및 AKA 프로토콜," 정보보호학회논문지, 20(5), pp. 111-124, 2010년 10월.

〔10〕 B. Aboba, L. Blunk, J. vollbrecht, J. Carlson, and H. Levkowetz, "Extensible Authentication Protocol (EAP)," RFC 3748, June 2004.

〔11〕 Z.M Fadlullah, M.M Fouda, N. Kato, A. Takeuchi, N. Iwasaki, and Y. Nozaki, "Toward Intelligent Machine-to-Machine Communications in Smart Grid," IEEE Communications Magazine, vol. 49, no. 4, pp. 60-65, Apr. 2011.

〔12〕 이근철, 오재영, 김윤기, "스마트그리드 홈 서비스,"

한국통신학회지(정보와통신), 27(4), pp. 38-42, 2010년 3월.
〔13〕 IEEE standard, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 6: Medium Access Control (MAC) Security Enhancements," IEEE 802.11i, 2004.
〔14〕 IEEE standard, "Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands," IEEE 802.16e, 2005.
〔15〕 3GPP standard, "Technical Specification Group Services and System Aspects; 3G Security; Security architecture (Release 10)," 2010.
〔16〕 J. Arkko and H. Haverinen, "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)," RFC 4187, Jan. 2006.
〔17〕 ZigBee Alliance, "Zigbee Smart Energy Profile 2.0 Public Application Protocol Specification," Mar. 2011.
〔18〕 P. Calhoun, J. Loughney, E. Guttman, G. Zorn, and J. Arkko, "Diameter Base Protocol," RFC 3588, Sep. 2003.
〔19〕 P. Eronen, T. Hiller, and G. Zorn, "Diameter Extensible Authentication Protocol (EAP) Application," RFC 4072, Aug. 2005.

〈著者紹介〉

사 진

최 재 덕 (Jaeduck Choi) 정회원
2002년 2월: 숭실대학교 정보통신전자공학부 졸업
2004년 2월: 숭실대학교 정보통신공학과 석사
2009년 2월: 숭실대학교 전자공학과 박사
2004년 1월~12월: (주)애드팍테크놀러지 S/W 연구원
2009년 3월~2010년 1월: 숭실대학교 전자공학과 박사후 연구원
2010년 2월~현재: ETRI 부설연구소 연구원
〈관심분야〉 스마트그리드 보안, 제어시스템 보안, 유무선 네트워크 인증 및 키교환

사 진

서 정 택 (Jungtaek Seo) 종신회원
1999년 2월: 충주대학교 컴퓨터공학과 졸업
2001년 2월: 아주대학교 컴퓨터공학과 석사
2006년 2월: 고려대학교 정보보호대학원 정보보호공학 공학박사
2000년 12월~현재: ETRI 부설연구소 선임연구원/과제책임자
〈관심분야〉 스마트그리드 보안, 제어시스템 보안, 제어시스템 통신 프로토콜 보안, 취약성 분석평가, DDoS 공격 탐지 및 대응