스마트 기기 상호 인증을 통한 스마트그리드 AMI 네트워크 보안 강화 방안 연구

이상지*, 박상진, 신용태
*숭실대학교 컴퓨터학과
e-mail:{sjlee, sjpark}@icn.ssu.ac.kr
e-mail:shin@ssu.ac.kr

A Study on Enhancing Security of Smart Grid AMI Network Through Smart Device Mutual Authentication

Sang-JI Lee*, Sang-Jin Park, Young-Tae Sin
*Dept of Computer Science, Soong-Sil University

요 약

차세대 전력망인 스마트그리드의 구축에 필수적인 AMI는 소비자의 전력 사용 관리를 위해 양방향 통신이 가능한 스마트 기기로 구성된다. 스마트 기기 간의 송수신 되는 소비자의 전력 사용 정보 흐름의 안전성 확보를 위해 제안하는 상호 인증 방안은 MDMS를 통한 지역적 인증이 가능하고, ID를 기반으로 스마트 기기 간 상호 인증을 제공한다. 이에 따라 스마트 기기 간의 안전한 통신 환경을 제공한다.

1. 서론

최근 에너지 자원의 고갈과 지구 온난화 등의 문제를 해결하기 위해 기존의 전력망에 ICT(Information & Communication Technology) 기술을 접목한 스마트그리드가 등장하였다. 스마트그리드 구축에 필수적인 역할을 하는 AMI(Advanced Metering Infrastructure)는 단순히 전력만을 공급하는 기기가 아닌 양방향 통신이 가능한 스마트 기기로 구성된다. AMI는 기본적으로 소비자의 전력량을 상위 데이터 저장소인 MDMS(Meter Data Management System)에 전송한다. 스마트 기기 간에 전송되는 정보의 관리가 중요해짐에 따라 스마트 기기간의 안전한 통신 환경을 제공하여야 한다.[1]

기존 인증 기술인 공개키기반구조는 인증서를 사용하여 보안성을 제공하지만 인증서 성생을 위한 통신횟수가 많다. 또한, ID 기반 인증 기술은 ID를 사용하여 통신횟수가 감소하지만 사용자 기기와 스마트 미터 간의 상호 인증을 제공하지 않는다. 따라서 사용자의 전력 사용 정보 흐름의 안전성 확보를 위해 본 논문에서는 MDMS를 통한 지역적 인증을 제공하고, ID를 기반으로 스마트 기기간의 상호 인증 방안을 제안한다.

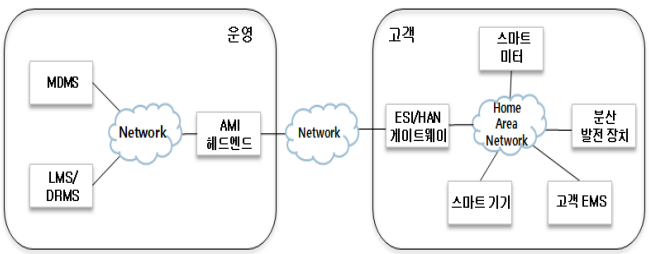
본 논문의 구성은 다음과 같다. 서론에 이어 2장에서는 스마트그리드 AMI 네트워크의 구조 및 구성요소와 기존 인증 기술에 대해 살펴보고, 3장에서는 스마트 기기 간의 상호 인증 방안을 제안한다. 마지막 4장에서는 결론을 맺는다.

2. 관련연구

2.1 스마트그리드 AMI 네트워크

스마트그리드는 기존의 전력망에 ICT 기술을 접목하여 전력 공급자와 소비자가 양방향으로 실시간 정보를 교환하는 차세대 전력망이다. 스마트그리드 실행에 있어 필수적인 역할을 담당하는 AMI 네트워크는 양방향 통신이 가능한 스마트 기기로 구성되어 소비자의 수요 및 전력가격에 따라 소비자의 전력 사용량 조절을 가능하게 한다.[2]

(그림 1)은 AMI의 논리적 구조 및 구성요소들 간의 연결을 나타낸다. AMI는 주로 배전 및 수용가 부문에서 수요의 측면을 구성하고 있다



(그림 1) AMI 구조 및 구성요소

AMI 헤드엔드는 운영 도메인의 여러 서버에 소비자의 전력 사용 정보를 전달하고, 전력망의 정보를 고객 도메인

1 본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT 연구센터 지원사업의 연구결과로 수행되었음(NIPA-2012-H0301-12-4008)

에 전달하는 기능을 수행한다.

MDMS는 전력 사용 정보, 발전, 저장 등의 미터 데이터를 수집하고 특정 목적으로 사용할 수 있도록 해준다.

LMS/DRMS(Load Management System/Demand Response Management System)은 소비자의 전력 요금 정보에 따라 수요를 조절하는 기능을 한다.

ESI/HAN(Energy Service Interface/Home Area Network) 게이트웨이는 고객 도메인에 속해 있는 기기들 간에 접속 능력 및 관리 기능을 수행하며, 운영 도메인과 연결하는 게이트웨이 역할을 한다.

스마트 미터는 HAN에 연결된 기기들의 전력 사용량을 실시간 측정 및 기록하며, 양방향 통신이 가능하도록 설계된 미터기이다.

분산 발전 장치는 가정용 소규모 발전 장치 및 에너지 저장 장치를 말하며, 고객 EMS(Energy Management System)은 스마트 미터를 포함한 고객 전력 장치들의 동작과 상태를 관리한다.[3]

2.2 인증기술

2.2.1 공개키기반구조(Public Key Infrastructure, PKI)

PKI는 인증서버에서 생성한 사설인증서를 사용하여 해당기기에 대한 권한을 차등 부여하는 방식이다. 이는 허가 받지 않은 사용자의 접근을 제어하고, 공개키 및 개인키 관리를 통해 기밀성, 무결성을 제공한다.[4]

그러나 통신 횟수가 많고 인증서 생성을 포함한 전송단계에서 연산량이 많아 스마트그리드 환경에 그대로 적용하기는 어렵다. 또한, 수 천만 개에 이르게 되는 스마트 기기에 배포된 인증서를 관리하는 어려움도 따른다.

2.2.2 ID기반

ID를 기반으로 사용자 기기와 스마트 미터 간의 인증을 수행하는 방식이며 등록단계, 인증단계로 구분된다. 등록단계에서는 사용자 기기에서 생성한 난수값, ID, PW를 이용하여 N의 값을 생성하여 이를 스마트 미터에 저장한 후 디바이스 인증 시에 사용한다. 인증단계에서는 사용자 기기와 스마트 미터가 생성한 값을 서로 추출하여 인증을 수행한다.[5]

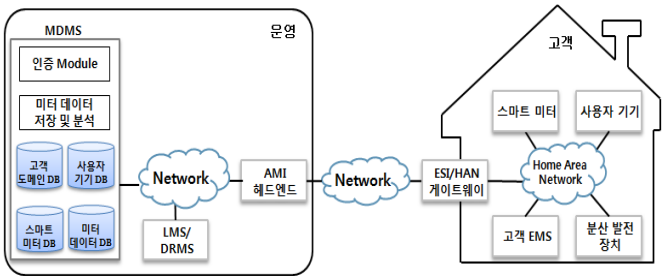
그러나 공격자로 가장한 사용자 기기 및 스마트 미터로 인해 소비자의 전력 사용 정보를 변경하여 과금에 영향을 미칠 수 있다. 따라서 사용자 기기와 스마트 미터가 연결되기 전에 스마트 기기간의 상호 인증이 필요하다.

3. 스마트 기기 상호 인증 방안

3.1 상호 인증 방안 구조 및 구성요소

제안하는 스마트 기기 간 상호 인증은 MDMS를 통해 지역적으로 스마트 기기를 인증하고, 스마트 기기의 ID를 기반으로 스마트 미터와 사용자 기기 사이의 상호 인증 방안이다.

스마트 기기 상호 인증 방안 구조는 (그림 2)과 같다.



(그림 2) 스마트 기기 상호 인증 방안 구조

제안하는 상호 인증 방안은 사용자 기기의 전력 사용량을 측정하기 위한 구성요소들의 인증 방안을 제안하였기 때문에 각 도메인에서 사용되는 구성요소들만을 새롭게 정의하였다.

운영 도메인은 소비자의 전력 사용을 관리하는 도메인이고, 고객 도메인은 고객의 기기 및 장치들로 구성된 도메인이며 고객 도메인 위치 정보(Customer Domain Location Information, CDLI), 고객 도메인 식별 번호(Customer Domain Identification Number, CDIN)로 다수의 고객 도메인을 구분할 수 있다. Network는 전력 운영을 위한 통신 및 운영 도메인과 고객 도메인간의 통신을 제공하며, Home Area Network는 고객 도메인 내의 기기 및 장치들 간의 통신을 제공한다.

다음 <표 1>은 각 도메인에 해당하는 구성요소의 기능 및 구성요소가 가지고 있는 정보를 나타낸다.

<표 1> 구성요소의 기능 및 정보

구분	기능	정보
MDMS	· 고객 도메인 관리 · 스마트 기기의 인증 수행 · 스마트 기기 상호 인증을 위한 정보 전송 · 미터 데이터 관리	· ID(MDID) · 공유키(MDU) · 개인키(MDP) · 위치정보(MDLI)
스마트 미터 (SM)	· 사용자 기기의 전력 사용량 (미터 데이터) 측정 · MDMS에게 미터 데이터 전송 · 사용자 기기에게 SMLI, MDLI 제공	· ID(SMID) · MDMS의 공유키(MDU) · 개인키(SMP) · 위치정보(SMLI) · MDLI
사용자 기기(D)	· 고객 도메인 내에서 사용되는 스마트 가전 기기	· ID(DID) · MDMS의 공유키(MDU) · 개인키(DP)

MDMS와 스마트 기기는 상위 인증 서버에서 인증을 받아 공유키 및 개인키를 가지고 있다고 가정한다.

1) MDMS
- 고객 도메인 관리 : 스마트 미터가 위치한 고객 도메인의 등록 및 제거를 수행하며, CDLI와 CDIN은 고객 도메인 DB에 저장된다.
- 스마트 기기 인증 : 스마트 기기의 인증을 수행하고, 스마트 기기에게 공유키 및 개인키를 할당해준다.
- 스마트 기기 상호 인증을 위한 정보 관리 : 스마트 기기간의 상호 인증을 위한 스마트 기기의 정보를 DB에 저장하고, 사용자 기기에게는 스마트 미터 정보를 스마트 미터에게는 사용자 기기 정보를 전송한다.
- 미터 데이터 관리 : 스마트 미터에서 수집된 미터 데이터를 미터 데이터 DB에 저장한다.

2) 스마트 미터

스마트 미터는 고객 도메인에 존재하는 사용자 기기의 전력 사용량을 주기적으로 실시간 측정하여 MDMS에게 전송한다. 또한, 새로운 사용자 기기에게 MDMS의 위치 정보와 스마트 미터의 위치 정보를 전송한다. 스마트 미터는 ID, MDMS의 공유키와 위치 정보, 스마트 미터의 개인키와 위치 정보를 저장하고 있다.

3) 사용자 기기

사용자 기기는 고객 도메인 내에서 사용되는 스마트 기기를 말한다. 사용자 기기는 ID, MDMS의 공유키, 사용자 기기의 개인키를 저장하고 있다.

3.2 상호 인증 방안 과정

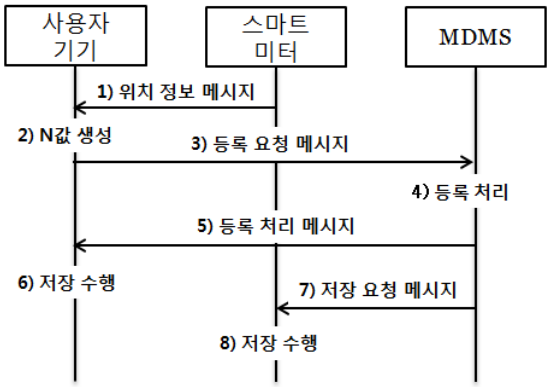
상호 인증 방안 과정에 사용된 표기법은 <표 2>와 같다.

<표 2> 표기법

표기	설명
K_*	*의 개인키
T_*	*이 전송한 시간 값
$h()$	일방향 해쉬 함수
$E_*[\,]$	*키를 이용한 암호화
$D_*[\,]$	*키를 이용한 복호화
N	Nonce 값
S, S_1, S', S'_1	임시 변수

3.2.1 사용자 기기 등록

새로운 사용자 기기는 MDMS에게 CDIN을 통해 등록하기 위한 과정이며 (그림 2)와 같다. 등록이 완료되면 MDMS는 사용자 기기에게 스마트 미터의 정보를 전송하고, 스마트 미터에게는 사용자 기기의 정보를 전송한다.



(그림 3) 사용자 기기 등록 과정

1) 스마트 미터는 사용자 기기에게 SMLI, MDLI를 전송한다.

2) 사용자 기기는 $CDIN, DID, h(K_{DP})$을 XOR 연산하여 N 값을 생성한다.

$$D: N = CDIN \oplus DID \oplus h(K_{DP})$$

3) 사용자 기기는 스마트 미터에게 전송 받은 MDLI를 통해 $N, T_D, DID, CDIN$을 연접하여 MDU로 암호화한 등록 요청 메시지를 MDMS에게 전송한다.

$$D \rightarrow MDMS: E_{MDU}[N \| T_D \| DID \| CDIN]$$

4) MDMS는 등록 요청 메시지를 MDP로 복호화한다. 복호화 한 후 $N, DID, CDIN$을 이용하여 $h(K_{DP})$를 생성하여 사용자 기기 DB에 $h(K_{DP}), DID, CDIN$을 저장한다.

$$MDMS: D_{MDP}[E_{MDU}[N \| T_D \| DID \| CDIN]]$$
$$h(K_{DP}) = N \oplus CDIN \oplus DID$$
$$Save\ h(K_{DP}), DID, CDIN$$

5) MDMS는 사용자 기기에게 $T_D, SMID$를 $h(K_{DP})$로 암호화하여 등록 처리 메시지를 전송한다. 실패할 경우에는 NAK을 전송한다.

$$MDMS \rightarrow D: E_{h(K_{DP})}[T_D \| SMID]$$

6) 사용자 기기는 등록 처리 메시지를 $h(K_{DP})$로 복호화하고, $SMID$를 S에 저장한다.

$$D: D_{h(K_{DP})}[E_{h(K_{DP})}[T_D \| SMID]]$$
$$Save\ S = SMID$$

7) MDMS는 스마트 미터에게 T_D, DID를 $h(K_{SMP})$로 암호화하여, 사용자 기기의 정보 저장을 요청한다.

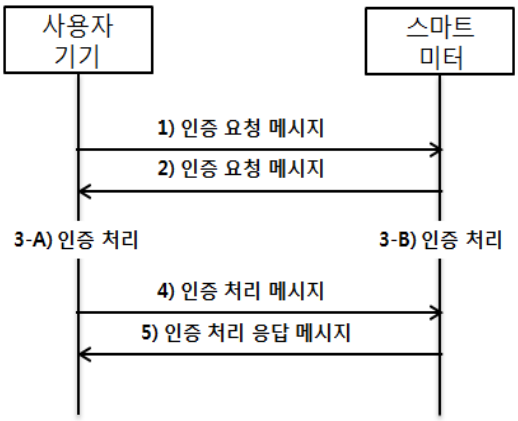
$$MDMS \rightarrow SM: E_{h(K_{SMP})}[T_D \| DID]$$

8) 스마트 미터는 저장 요청 메시지를 $h(K_{SMP})$로 복호화하고, DID를 S_1에 저장한다.

$$SM: D_{h(K_{SMP})}[E_{h(K_{SMP})}[T_D \| DID]]$$
$$Save\ S_1 = DID$$

3.2.2 스마트 기기간의 상호 인증 및 연결

사용자 기기와 스마트 미터는 MDMS에게 전송 받은 정보를 통해 상호 인증을 수행하고 연결을 하는 단계이며, (그림 4)과 같다.



(그림 4) 스마트 기기간의 상호 인증 및 연결 과정

1) 사용자 기기는 난수 DR을 생성하고, $h(DR), DID, DR$을 연접하여 MDU로 암호화한 인증 요청 메시지를 스마트 미터에게 전송한다.

$$D \rightarrow SM: E_{MDU}[h(DR) \| DID \| DR]$$

2) 스마트 미터는 난수 SMR을 생성하고, $h(SMR), SMID, SMR$을 연접하여 MDU로 암호화한 인증 요청 메시지를 스마트 미터에게 전송한다.

3-A) 사용자 기기는 인증 요청 메시지를 MDU로 복호화한다. SMR 값을 S'에 저장하여 $h(S')$값과 $h(SMR)$rqkt을 비교하여 메시지의 무결성을 검사한다. 검사한 후 이전에 SMID을 저장해 놓은 S와 스마트 미터에게 받은 SMID를 비교하여 인증을 수행한다.

$$D: D_{MDU}[E_{MDU}[h(SMR) \| SMID \| SMR]]$$
$$S' = SMR$$
$$h(S') = ?\ h(SMR)$$
$$S = ?\ SMID$$

3-B) 스마트 미터는 인증 요청 메시지를 MDU로 복호화한다. DR값을 S'_1에 저장하여 $h(S'_1)$값과 $h(DR)$값을 비교하여 메시지의 부결성을 검사한다. 검사한 후 이전에 DID를 저장해 놓은 S_1과 사용자 기기에게 받은 DID를 비교하여 인증을 수행한다.

$$SM: D_{MDU}[E_{MDU}[h(DR) \| DID \| DR]]$$
$$S_1' = DR$$
$$h(S_1') = ?\ h(DR)$$
$$S_1 = ?\ DID$$

4) 사용자 기기는 스마트 미터의 인증을 처리한 후 인증에 성공하면 연결을 위한 연결 요청 메시지를 전송한다. 인증에 실패할 경우 NAK을 전송한다.

5) 스마트 미터는 사용자 기기의 인증을 처리한 후 인증에 성공하면 연결 요청 메시지에 대한 연결 요청 응답 메시지를 전송한다. 인증에 실패할 경우 NAK을 전송한다.

4. 결론

본 논문에서는 스마트그리드 AMI 네트워크와 기존 인증 기술에 대해 살펴보았다. 또한, 사용자 기기와 스마트 미터 간의 상호 인증 방안을 제안하였다.

제안하는 방안은 MDMS가 스마트 기기의 인증을 수행하여 공개키 및 개인키를 할당하여 고객 도메인별로 지역적 인증이 가능하다. MDMS는 사용자 기기와 스마트 미터 간의 상호 인증을 위해 ID를 기반으로 정보를 제공해준다. 따라서 지역적 인증 및 상호 인증을 제공함으로써 스마트그리드 AMI 네트워크에서의 사용자 전력 사용 정보 흐름의 안정성 및 안전성을 확보할 수 있으며, 안전한 네트워크 운영구조를 제공한다.

향후 MDMS에서 스마트 기기의 인증을 위해 사용되는 스마트 기기의 개인키 관리에 대한 연구가 필요하다.

참고문헌

[1] NIST, "NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0," 2012. 02.

[2] Zhang Luhua; Yi Zhonglin; Wang Sitong; Yuan Ruiming; Zhou Hui; Yin Qingduo, "Effects of Advanced Metering Infrastructure (AMI) on relations of Power Supply and Application in smart grid," Electricity Distribution (CICED), 2010 China International Conference on, pp.1-8, 2010. 09.

[3] Jun Wang, Leung, V.C.M, "A survey of technical requirements and consumer application standards for IP-based smart grid AMI network," Information Networking 2011 International Confernece on, pp.114-119, 2011. 01.

[4] 이영구, 김정재, 김현철, 전문석, "PKI 기반 홈 네트워크 시스템 인증 및 접근제어 프로토콜에 관한 연구," 한국통신학회 논문지, 제35권 제4호, pp.592-598, 2010.04.

[5] 김홍기, 이임영, "스마트그리드 AMI환경에서의 ID기반 인증기법에 관한 연구," 정보처리학회 논문지, 제18권 제6호, pp.397-404, 2011.12.