http://dx.doi.org/10.3745/KIPSTC.2011.18C.6.397

# 스마트그리드 AMI환경에서의 ID기반 인증기법에 관한 연구

김 홍 기[†] · 이 임 영[††]


## 요 약

최근 기존의 단 방향 전력망 시스템에 정보통신기술을 접목한 스마트그리드 기술의 개발이 활발하게 이루어지고 있다. 스마트그리드의 핵심 인프라로 원격검침시스템인 AMI는 스마트미터에서 측정한 전력량을 상위 데이터 저장소인 MDMS에 전송한다. 스마트미터는 정보통신기술을 활용하여 전력데이터를 전송하고 있기 때문에 기존 보안위협을 포함한 추가적인 보안위협이 예상된다. 이는 소비자의 개인정보노출 및 산업시스템 마비 등의 손실이 발생할 가능성이 있다. 따라서 본 논문은 이러한 보안위협에 대응하기 위해 스마트그리드 환경에서 스마트미터와 MDMS간 그리고 각 가정의 디바이스와 MDMS간의 상호인증과 전력량 데이터 전송방식에 관하여 제안하였다.


**키워드 : 스마트그리드, AMI 인증, 사용자 인증**

# A Study on ID-based Authentication Scheme in AMI SmartGird Environment

Hong Gi Kim[†] · Im Yeong Lee[††]


## ABSTRACT

Recently the existing one-way electricity system that combines information and communications technology to develop smart grid technology is made active. The core infrastructure of the smart grid, AMI smart meters to AMR system, the amount of power measured at the top to MDMS transmits data store. Smart meters utilizing information and communication technology to transfer data and power because of the existing security threats are expected, including the additional security threats. It exposes the privacy of consumers and industrial systems, such as paralysis is likely to result in the loss. In this paper to respond to these security threats in the environment smart grid. Also, We propose data transfer methods between smartmeter and MDMS and between home device and MDMS.


**Keywords : SmartGrid, AMI Authentication, User Authentication**

## 1. 서 론

기술의 고도화와 경제 성장에 따라 전력의 생산 및 공급은 전 세계적으로 가장 중요한 필수요소로 자리매김 하였으나, 아직 화석연료에 의존하여, 그 효율성은 매우 낮은 편이다. 이러한 화석연료의 사용으로 인해 환경파괴에 대한 경각심이 늘어나게 되었고, 기존의 단방향 전력망 시스템에 정보통신 기술을 접목한 스마트그리드 기술에 대한 관심이 선진국을 중심으로 증대되어 활발하게 연구가 진행되고 있다.

스마트그리드 기술은 발전소와 사용자가 실시간으로 정보를 교환하며, 사용 과금 및 전력공급의 효율성을 증대시키는 기술이다.

스마트그리드에서는 전기로 작동되는 모든 기기들이 유·무선 네트워크로 연결되며, 서로간의 정보 교환을 통하여 유기적인 관계로 이루어진다. 현재 제공되는 전력 시스템은 전력사용예측이 불가능하기 때문에 일반적으로 10%이상의 예비전력을 보유하여 저장하고 있다. 그러나 스마트그리드 환경에서는 스마트미터(Smart Meter)를 통해 실시간으로 사용되는 에너지를 분석함으로써 에너지를 효율적으로 분배할 수 있다[1].

스마트그리드의 핵심 인프라로 원격 검침 시스템인 AMI(Advanced Metering Infrastructure)가 있다. 이는 에너지를 효율적으로 관리하기 위한 체계로써, 각 가정 내 설치되는 스마트미터와 각 가정의 디바이스, 그리고 전력량을 취합하는 MDMS(Meter Data Management System)로 구성

† 준 회 원 : 순천향대학교 컴퓨터학과 석사과정
†† 종신회원 : 순천향대학교 컴퓨터소프트웨어공학과 교수
논문접수 : 2011년 9월 28일
수 정 일 : 1차 2011년 11월 8일
심사완료 : 2011년 11월 10일

된다. 소비자들은 AMI를 통해 실시간 에너지 사용량 정보를 기반으로 에너지를 관리함으로써 가정 및 기업의 에너지 비용을 절감할 수 있으며, 전체 에너지 사용량을 효율적으로 관리할 수 있다[2].

본 논문의 구성은 다음과 같다. 2장에서는 AMI의 구조와 기존의 다양한 인증기술들에 대해 알아보고, 3장에서는 관련연구를 기반으로 한 AMI 인증 및 데이터 전송기법에서의 보안요구사항에 대하여 기술한다. 4장에서는 동적 ID를 이용한 AMI환경에서의 인증기법에 대하여 제안하고, 5장에서는 보안 요구사항에 의하여 제안방식을 분석한다. 마지막으로 6장에서 결론을 맺는다.

## 2. 관련 연구

본 장에서는 AMI의 구조를 분석하고, 기존의 스마트기기와 서버 간 제공되고 있는 인증기술에 대하여 분석한다.

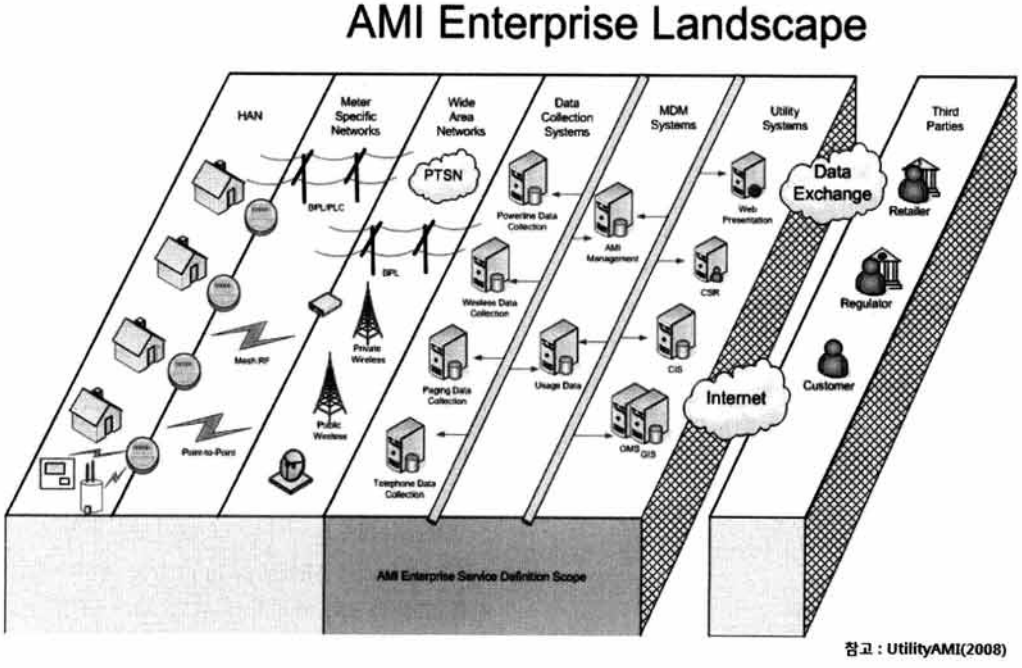
### 2.1 AMI 구조

AMI는 스마트그리드 분야 중 배전 및 수용가 부문에서 수요의 측면을 구성하며, 최종 소비자와 전력회사 사이의 전력 서비스 정보화 인프라로서 스마트그리드 운용에 필수적인 스마트미터 기반의 핵심 인프라 시스템이다. 단순히 계량 값만을 읽어가는 기존의 AMR(Automated Meter Reading)과는 다르게 소비자의 수요 및 전력가격을 실시간으로 양방향 전송하는 역할을 담당한다. 특히 전통적인 전력망에서는 볼 수 없었던 전력 소비자의 적극적인 참여가 요구되는 시스템이다.

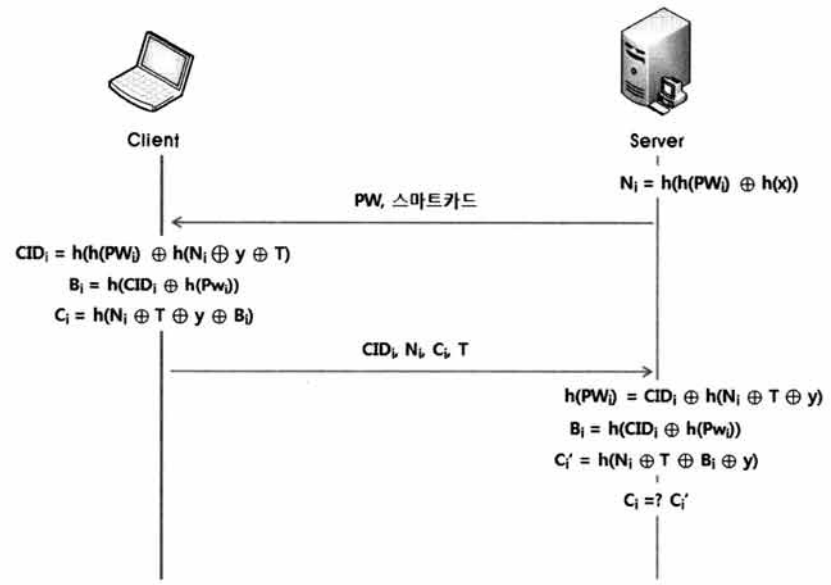
AMI는 기존의 AMR과는 다르게 스마트미터를 중심으로 양방향 통신과 오픈 프로토콜(Open Protocol)에 기반해 원격 전력 차단(Remote Connect/Disconnect)이 가능하고 선불형 계량(Prepayment)의 인프라가 될 수 있으며 실시간 요금제(RTP), 피크 요금제(Critical Peak Pricing), TOU (Time-of-Use)요금제 등 다양한 요금제의 적용도 가능하다. 수요반응 메커니즘에는 없어서는 안 될 내용이며 더 나아가서는 홈오토메이션, 홈네트워킹과 연결되고, 결국 스마트그리드 기본 인프라가 되는 것이 AMI이다.

AMI의 구성요소는 크게 MDMS(Meter Data Management System)를 중심으로 한 전력사 내의 상위 시스템, 전력사와 수용가의 스마트 미터 간을 연결시켜주는 통신 시스템, 스마트미터, 그리고 HAN(Home Area Network)내의 가정용 기기들로 크게 나눌 수 있다. 미국의 국가전력연구소인 EPRI(Electric Power Research Institute)와 전력사들 및 제품 공급자들의 모임으로 구성된 UCAIug(Utility Communication Architecture International Users Group)에서는 AMI Enterprise Reference Model이라는 AMI 기본 모델을 (그림 1)과 같이 제시하기도 했으며 이 모델에서도 위의 분류와 크게 다르지 않다.

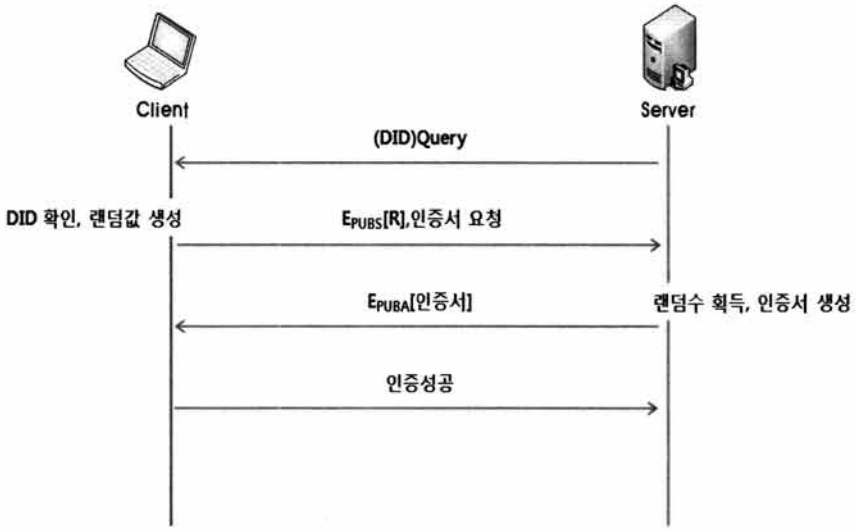
통상적으로 AMI환경에서는 통신의 구간에 따라 세 구간으로 나누게 되는데, 각 가정의 디바이스와 스마트미터는 HAN(Home Area Network)를 통해 전력선 통신인 PLC (Power Line Communication)와 ZigBee를 사용하고 있고, 스마트미터와 MDMS간 통신에서는 NAN(Neighborhood Area Network)를 사용하여 데이터를 전송하고 있다. 그리고 MDMS에서 통신 사업자가 제공하는 공중망을 이용해 상위 시스템과 인터페이스하는 접점인 헤드엔드(Head End)까지의 구간을 WAN(Wide Area Network)를 통하여 연결된다[3, 4].




(그림 1) AMI 레퍼런스 모델




(그림 2) 동적 ID기반 인증방식




(그림 3) PKI기반 인증방식

### 2.2 동적 ID기반 원격 사용자 인증 기술

본 방식은 스마트카드의 연산기능을 이용하여 패스워드를 생성하고, 연산량이 적은 XOR과 해쉬연산을 이용하여 인증을 수행하는 기술이다. 또한 임시 검색 테이블을 이용하여 원격 시스템에서 인증시마다 수시로 변경되는 임시 검색 테이블을 추가하여 난수 값이 변화되도록 고안하였다. 본 방식은 통신량이 등록단계 및 인증단계를 포함하여 3회로 적다는 장점이 있지만 해쉬연산 및 XOR연산이 매우 많아 다수의 스마드미터에서 전송한 데이터를 서버에서 연산하여 처리하기 힘들다는 단점이 존재한다. 또한 환경의 특성상 스마트카드를 이용하여 사용자를 인증하고 있기 때문에 보안채널을 통하여 등록단계를 수행하고 있다. 그러나 스마트그리드 환경의 특성상 가정 내 디바이스는 네트워크로 연결되어있기 때문에 별도의 암호화 절차가 필요하다. 따라서 본 방식을 그대로 적용하기에 문제가 있다[5].

### 2.3 PKI기반 인증 및 접근제어 기술

본 방식은 외부 클라이언트에서 홈 네트워크를 컨트롤하기 위한 사용자 인증 기술을 공개키 인증서를 이용하여 수행한다. 또한 인증서버에서 생성한 사설인증서를 이용하여 해당기기에 대한 권한을 차등 부여함으로 허가 받지 않은 사용자의 접근을 제어한다. 본 방식은 인증 스푸핑 및 스니핑 공격, 재전송공격등에 안전성을 제공하고 있다. 그러나 통신 횟수가 많고, 인증서 생성을 포함한 전송단계에서 연산량이 많아 스마트그리드 환경에 적용하기 어렵다는 단점이 있다[6].

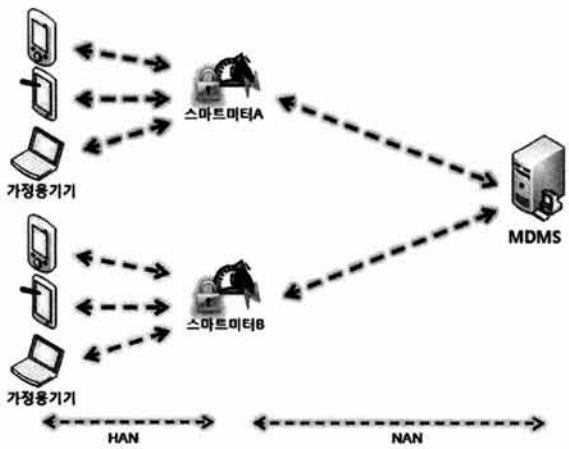
## 3. 보안요구사항

유선 및 무선으로 연결되는 인터넷 환경에서는 해킹, 악성코드인 웜 그리고 바이러스들과 같은 다양한 위험요소에 노출되어 있다. 또한 스마트미터는 15분에서 1시간의 간격으로 MDMS와 전력량을 전송받고 있기 때문에 적은 연산량과 빠른 속도로 인증을 수행해야 한다. 따라서 스마트그리드 환경에서의 안전한 AMI 인증기법을 설계하기 위해서는 다음의 보안요구사항들이 고려되어야 한다[7].

- 기밀성 : 통신에 사용되는 데이터들은 정당한 통신 객체들만이 공유되어야 하며, 통신 중간에 노출되더라도 데이터의 값을 유추하지 못해야 한다.
- 무결성 : 통신상에서 전송되는 데이터들은 과금 정보를 포함하고 있어, 금전거래의 근거가 되므로 통신 중 위조 및 변조되지 않아야 한다.
- 상호인증 : 정당한 스마트미터와 MDMS의 확인 그리고 스마트미터와 디바이스의 확인을 위하여 서로간의 상호인증이 제공되어야 한다.
- 연산량 : 각각의 개체가 빠른 속도로 데이터를 암호화하고 복호화 하기 위하여 연산 효율성이 높아야 한다.

## 4. 제안방식

본 장에서는 3장의 보안요구사항을 만족하는 스마트그리드 환경에서의 AMI인증기법을 제안한다. AMI의 구성요소는 (그림 4)과 같이 MDMS를 중심으로 한 전력사 내의 상위 시스템, 전력사와 수용가의 스마트 미터간의 연결시켜주는 통신 시스템, 스마트미터, 가정용 기기 등으로 구분된다. 디바이스와 스마트미터 간 인증기법에서는 (그림 4)와 같이 HAN(Home Area Network)를 통해 전력선 통신인 PLC(Power Line Communication)와 ZigBee를 사용하고 있고, 스마트미터와 MDMS간 통신에서는 NAN(Neighborhood Area Network)를 사용하여 통해 데이터를 전송하고 있다.




(그림 4) AMI 구조

본 논문에서는 이러한 통신기법을 이용하여, 디바이스와 스마트미터 간, 스마트미터와 MDMS간 인증기법에 대하여 제안한다.

### 4.1 시스템 계수

본 제안방식에서 사용되는 시스템 계수는 다음과 같다.

- $*$ : 각각의 개체 ($D$ : 디바이스, $SM$ : 스마트미터, $MD$ : MDMS)
- $M$ : 전력량데이터
- $ks$ : 각각의 개체 간 공유된 세션 키
- $Addr$ : 스마트미터의 MAC Address
- $ID_*$ : $*$의 이름
- $T$ : 전송 시간 값
- $R_*$ : $*$에서 생성한 난수
- $PW_*$ : 동기화 시 $*$에서 입력한 비밀번호
- $E*[\ ]$ : $*$의 키를 이용한 암호화
- $h(\ )$ : 일방향 해쉬 함수

### 4.2 홈 디바이스와 스마트미터 간 인증기법

스마트그리드 환경에서는 외부 디바이스가 사용자 스마트미터에 접근하여 전력 사용량을 증가시키거나, 과금을 높이는 문제점이 발생할 수 있다. 이에 각 스마트미터는 가정에서 사용하고 있는 디바이스를 등록하고 등록된 디바이스의 전력량을 측정한다. 따라서 제안방식은 ID를 기반으로 각 디바이스를 인증한다. 본 제안방식은 등록단계, 인증 및 데이터 전송단계로 구분되며, 각 단계의 수행절차는 다음과 같다.

#### 4.2.1 등록단계

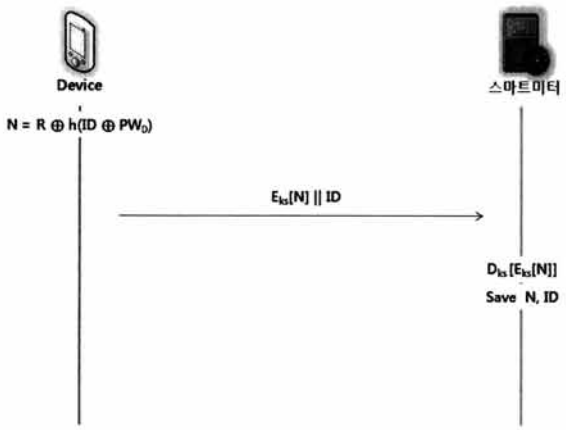
등록단계에서는 디바이스에서 생성한 $R$의 값과 디바이스의 아이디, 스마트미터와 동기화 시 사용자가 입력한 패스워드를 이용하여 $N$의 값을 생성한다. 이를 스마트미터에 디바이스의 아이디와 $N$의 값을 저장한다. 저장한 $N$의 값은 후에 디바이스의 인증 시 사용하고, $ID$는 $N$의 값을 확인 시 식별자로 사용한다. 등록단계는 다음과 같은 단계로 진행된다.

Step1 : 디바이스에서는 난수 $R$을 생성하고, 디바이스의 $ID$와 동기화 시 입력한 패스워드를 XOR연산한다. 이후 해쉬 값을 생성하고 난수 $R$과 XOR연산한다.

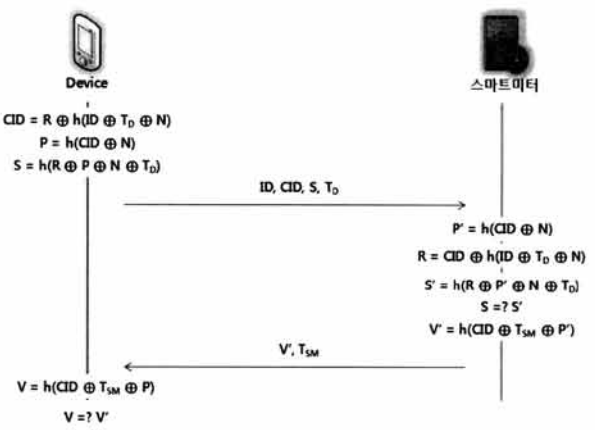
$$D : N = R \oplus h(ID \oplus PW_D)$$

Step2 : 디바이스는 생성한 $N$의 값을 사전에 공유 된 공유키로 암호화하고, 디바이스의 $ID$값과 연접하여 스마트미터에게 전송한다.

$$D \rightarrow SM : E_{ks}[N] \,||\, ID$$




(그림 5) 디바이스 등록단계




(그림 6) 디바이스 인증

Step3 : 스마트미터는 전송받은 암호화 값을 공유키로 복호화 하고 $N$의 값과 $ID$를 저장한다.

$$SM : D_{ks}[E_{ks}[N]]$$
$$SM : Save \quad N, ID$$

4.2.2 인증단계

등록단계를 수행하면 스마트미터는 디바이스의 아이디와 $N$의 값을 저장하고 있다. 저장한 값을 이용하여 디바이스는 $CID$, $P$, $S$값을 생성하고, $ID$와 $CID$, $S$, 타임스템프 값을 스마트미터에게 전송하게 된다. $N$의 값이 노출되지 않고, 스마트미터에게 전송하고 있는 값 중 $P$의 값이 노출되지 않고 있기 때문에 $N$의 값을 추측하기 어려우며, 이를 통해 안전성을 보장한다. 또한 스마트미터에서 인증 후 생성한 $P$의 값을 이용하여 $V$의 값을 생성하고 디바이스에서 이를 확인하여 상호인증을 수행한다. 인증단계는 다음과 같은 단계로 진행된다.

Step1 : 디바이스는 아이디와 타임스템프, 등록단계 시 사용한 $N$의 값과 난수 $R$의 값을 이용하여 $CID$, $P$, $S$값을 생성한다.

$$D : CID = R \oplus h(ID \oplus T_D \oplus N)$$
$$P = h(CID \oplus N)$$
$$S = h(R \oplus P \oplus T_D \oplus N)$$

Step2 : 디바이스는 스마트미터에게 생성한 $CID$, $S$값과 자신의 아이디, 타임스템프 값을 포함하여 전송한다.

$$D \rightarrow SM : ID, CID, S, T_D$$

Step3 : 스마트미터는 전송받은 값을 통해 $P'$ 값을 생성하고, $CID$값을 통해 난수 값 $R$을 추출한다.

$$SM : R = CID \oplus h(ID \oplus T_D \oplus N)$$
$$P' = h(CID \oplus N)$$
$$S' = h(R \oplus P' \oplus T_D \oplus N)$$

Step4 : 스마트미터에서는 전송받은 $S$값과 생성한 $S'$값을 비교한 후 인증을 완료하며, 인증 후 $V'$값을 생성하여 디바이스에게 타임스템프를 포함하여 전송한다.

$$SM : S' =? S$$
$$SM : V' = h(CID \oplus T_{SM} \oplus P')$$
$$SM \rightarrow D : V', T_{SM}$$

Step5 : 디바이스는 전송받은 $T_{SM}$값을 이용하여 $V$값을 생성하고 전송받은 $V'$값과 비교하여 스마트미터를 인증한다.

$$D : V = h(CID \oplus T_{SM} \oplus P)$$
$$D : V =? V'$$

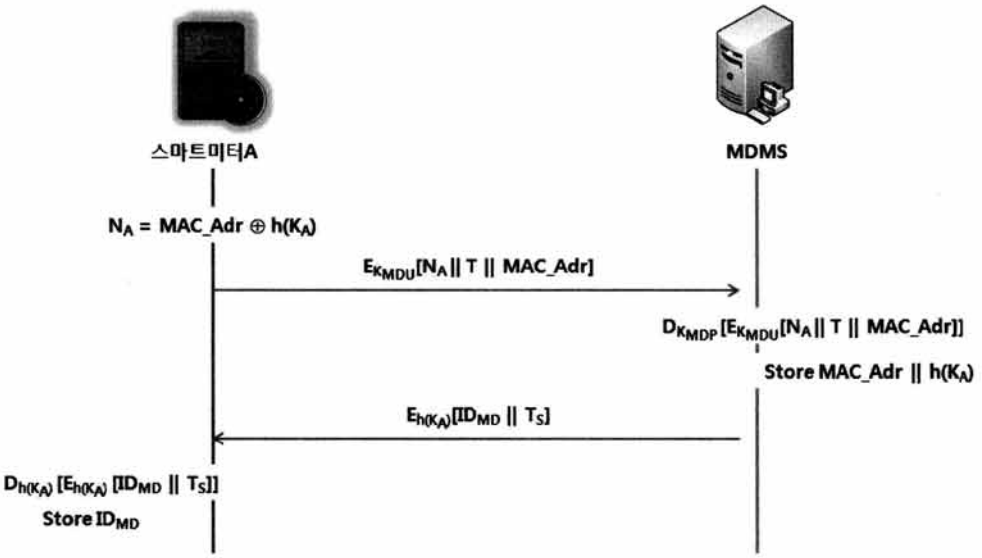
4.3 스마트미터와 MDMS 간 인증기법

스마트그리드 환경에서는 스마트미터와 MDMS가 주기적인 시간에 통신을 수행하므로 다수의 스마트미터에서 일괄적으로 데이터가 전송된다. 따라서 제안방식은 기존의 인증기법보다 적은 연산량과 통신횟수를 통해 안전하게 스마트미터를 인증하고 데이터를 전송하는 기법을 제안한다. 본 제안방식은 등록단계, 인증 및 데이터 전송단계로 구분되며, 각 단계의 수행절차는 다음과 같다.

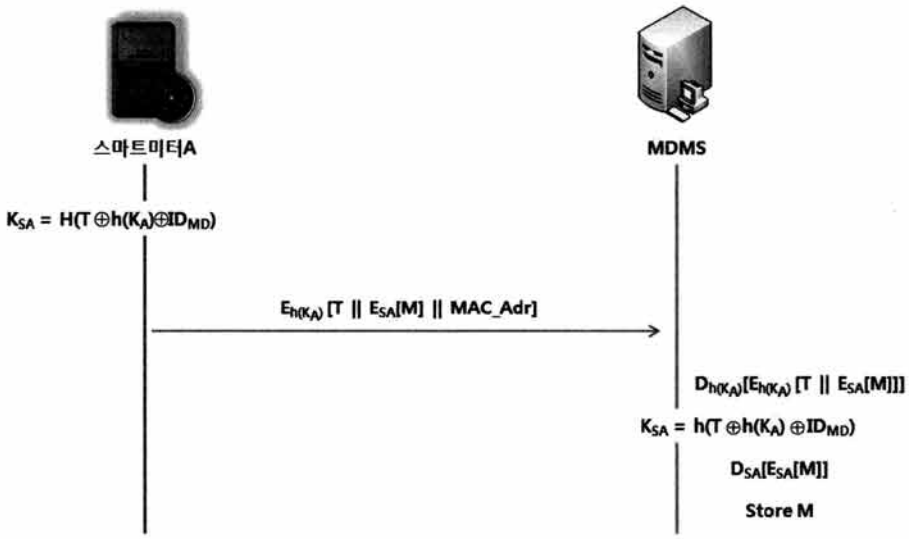
4.3.1 등록단계

등록단계에서는 인증 받는 스마트미터의 MAC Address와 해쉬연산 된 개인키를 전송하여 저장한다. 공개키 암호 알고리즘을 이용하여 자신이 등록하고자 하는 MDMS에게만 개인키를 전송하며, 전송받은 MDMS는 자신의 이름을 스마트미터에 전송하여 전력량을 전송할 때 자신이 등록한 MDMS만 확인할 수 있도록 MDMS의 이름을 통해 세션키를 생성한다.

등록단계는 스마트미터가 최초로 등록될 때 1회 수행하며, 이후 모든 인증 및 데이터 전송 시에 등록단계는 수행되지 않는다.




(그림 7) 스마트미터 등록단계




(그림 8) 스마트미터 인증 및 데이터 전송단계

Step1 : 스마트미터는 자신의 MAC Address와 개인키를 통해 $N_A$를 생성하고 타임 스탬프를 포함하여 MDMS의 공개키를 사용하여 암호화한다. 암호화된 데이터를 MDMS에게 MAC Address를 추가하여 전송한다.

$$SM : N_A = MAC\_Addr \oplus h(K_A)$$
$$SM \rightarrow MD : E_{MDU}[N_A \| T \| MAC\_Addr]$$

Step2 : MDMS에서는 전송받은 암호문을 MDMS의 개인키로 복호화하여 MAC Address를 확인하고, MAC Address와 $N_A$에 포함되어있는 해쉬 연산 된 스마트미터의 개인키 $H(K_A)$를 저장하여 후에 암호화키로 사용한다.

$$MD : D_{MDP}[E_{MDU}[N_A \| T \| MAC\_Addr]]$$
$$MD : h(K_A) = N_A \oplus MAC\_Addr$$
$$MD : Store \quad h(K_A) \| MAC\_Addr$$

Step3 : MDMS는 스마트미터의 개인키를 저장 후 자신의 이름과 스마트미터에게 전송받았던 시각을 포함하여 $h(K_A)$로 암호화 후 스마트미터에게 전송한다.

$$MD \rightarrow SM : E_{h(KA)}[ID_{MD} \| T_S \| MAC\_Addr]$$

Step4 : 스마트미터는 전송받은 암호화 값을 복호화하여 MDMS의 이름을 저장하고 등록단계를 마친다.

$$SM : D_{h(KA)}[E_{h(KA)}[ID_{MD} \| T_S \| MAC\_Addr]]$$
$$SM : Store \quad ID_{MD}$$

4.3.2 인증 및 데이터 전송단계

등록단계가 완료되면 스마트미터는 MDMS의 이름값을 저장하고 있고, MDMS는 해쉬연산 된 스마트미터의 개인키와 MAC Address를 저장하고 있다. 이를 이용하여 데이터 전송단계에서는 스마트미터에서 측정한 전력량을 등록한 MDMS만 복호화 가능하도록 세션키를 생성하여 암호화하여 전송한다.

Step1 : 스마트미터는 측정된 전력량을 전송하기 위하여 사용될 키 $K_{SA}$를 등록단계에서 사용된 $h_{(KA)}$와 $MDMS$의 이름값, 타임 스템프를 추가하여 생성한다.

$$SM : K_{SA} = h(T \oplus H(K_A) \oplus ID_{MD})$$

Step2 : 생성된 키 $K_{SA}$를 통해 측정된 전력량을 암호화하고 이를 MDMS가 복호화 할 수 있도록 타임스탬프를 포함하여 $h_{(KA)}$를 키로 사용하여 재 암호화한다. 재 암호화 후 생성된 값을 MAC Address를 포함하여 MDMS에게 전송한다.

$$SM \rightarrow MD : E_{h(KA)}[T \parallel E_{SA}[M]] \parallel MAC\_Addr$$

Step3 : MDMS는 전송받은 MAC Address를 통해 $h_{(KA)}$를 검색하고, 복호화를 수행한다.

$$MD : D_{h(KA)}[E_{h(KA)}[T \parallel E_{KSA}[M]]]$$

Step4 : 복호화 후 남아 있는 암호문을 $K_{SA}$를 생성하여 복호화하고 측정된 전력량을 저장한다.

$$MD : K_{SA} = H(T \oplus h(K_A) \oplus ID_{MD})$$
$$MD : D_{KSA}[E_{KSA}[M]]$$

## 5. 제안방식 분석

보안요구사항에 대한 제안방식 분석은 다음 <표 1>과 같다.

〈표 1〉 제안방식 분석

| 구분 | 디바이스인증 | | 스마트미터인증 | |
|---|---|---|---|---|
| | Das[5] | 제안방식 | Lee[6] | 제안방식 |
| 기밀성 | ○ | ○ | ○ | ○ |
| 무결성 | ○ | ○ | ○ | ○ |
| 상호인증 | × | ○ | ○ | ○ |
| 연산량 | 12H+2E | 6H+1E | 2H+3U | 4H+2E+1U |
| 통신횟수 | 3 | 3 | 4 | 3 |

○:제공, 좋음 △:보통, ×:제공안함, 나쁨
E:대칭키연산, U:공개키연산, H:해쉬연산

Das 방식은 동적ID를 기반으로 경량화 된 인증을 제공하고 있으나, 해쉬 연산량이 많고, 비밀통신을 통해 데이터를 2번이나 전송하고 있어, 일반 통신상에서는 공유키를 통한 암호화 연산이 2번 추가되게 된다. 또한 접속하고자 하는 원격 시스템과의 상호인증이 제공되지 않아 보안성 측면에서 위험한 부분이 많다.

PKI기반의 방식은 공개키 알고리즘을 사용하고 있어, 연산량이 많고, 인증서를 통한 인증을 수행함에 있어 통신횟수가 ID기반 인증방식보다 더 많은 것을 볼 수 있다. 따라서 스마트그리드 환경에서 적용하기에는 좀 더 보완이 필요할 것으로 보인다.

제안방식 중 디바이스 인증방식은 등록단계에서 암호화 처리를 통해 N값을 공유하고 N값의 안전성을 기반으로 인증을 수행하고 있다. 주요정보인 N을 통신 중간에 공유하지 않아 기밀성이 보장되며, 비밀키 KA를 해쉬함수 처리하여 무결성을 보장하고 있다. 또한 생성되는 CID, P, S값을 시간값을 추가하여 매 세션 변화되도록 하여 재사용공격에 대비하였다. 디바이스와 스마트미터는 서버/클라이언트 환경과 흡사한 것을 볼 수 있는데 자신의 스마트미터가 맞는지 확인하는 상호인증이 필요하게 되고, 본 제안방식은 V값 교환을 통해 상호인증을 제공하고 있다.

스마트미터와 MDMS간 인증방식은 스마트그리드 환경에 적합하도록 MDMS에서 수행하는 연산량을 감소시켜 빠른 속도로 인증이 가능하도록 고안하였다. 따라서 초기 등록이후에는 등록과정이 수행되지 않기 때문에 공개키 연산을 이용하여 안전하게 비밀값인 NA의 값을 교환하고, 1회의 통신만으로 MDMS에게 전력량을 안전하게 전송할 수 있도록 매 세션 변경되는 세션키를 통해 암호화 후 전송한다. 전송시에 암호화과정을 통해 기밀성을 제공하고, 타임스템프 값을 통해 재전송공격을 방지하며 공개키 암호화 과정으로 서버에서만 스마트미터의 정보를 확인할 수 있도록 하였다.

## 6. 결 론

IT기술의 발달로 기존의 폐쇄적인 단 방향 전력망에 외부와의 양방향 통신기술을 접목하여 실시간 양방향 정보교환 및 에너지 효율을 최적화하는 스마트그리드 기술의 개발이 활발하게 이루어지고 있다. 스마트그리드는 각 가정의 디바이스에 사용한 전력량을 스마트미터로 통합하여 취합한 전력량을 MDMS에게 전송하는 방식으로 전력데이터를 측정하고 있다. 이러한 전력데이터가 통신 중간에 공격자에게 노출될 경우 소비자의 개인정보 및 전력사용패턴이 노출되고, 크게 산업 시스템 전반에 피해를 줄 가능성이 있다.

따라서 본 논문에서는 디바이스와 스마트미터, MDMS간의 인증방식을 ID를 통하여 제안하였다. 각 디바이스는 15분의 간격을 통해 스마트미터에게 데이터를 전송하고 있어, 기존의 인증 기법보다 경량화 된 인증기술이 필요하다. 따라서 암호화 절차를 줄이고 ID를 기반으로 한 인증기법을 제공하며, 각 디바이스를 빠르게 처리할 수 있도록 XOR연

산과 해쉬 연산을 사용하여 연산량을 감소시킨 인증기법을 제안하였다. 따라서 스마트그리드 환경에서 안전한 AMI인증이 제공될 수 있을 것이라 사료된다.

## 참 고 문 헌


[1] 남궁완, 조효진, 조관태, 이동훈, "스마트미터 보안 연구", 한국정보보호학회지 제 20권 제 5호, pp.20~30, 2010. 10.

[2] 전재우, 임선희, 이옥연, "스마트그리드를 위한 Binary CDMA 기반의 AMI 무선 네트워크 구조 및 AKA 프로토콜", 한국정보보호학회논문지 제 20권 제 5호, pp.111~124, 2010. 10.

[3] 이정준, "AMI 기술 동향", 조명, 전기설비 학회지 제 23권 제 6호, pp.27~31, 2009. 12.

[4] NIST, "Guidelines for Smart Grid Cyber Security", The Smart Grid Interoperability Panel-Cyber Security Working Group, 2010. 8.

[5] M.L. Das, A. Saxena, V.P. Gulati, "A Dynamic ID-based Remote User Authentication Scheme", Consumer Electronics, IEEE, 2004.

[6] 이영구, 김정재, 김현철, 전문석, "PKI 기반 홈 네트워크 시스템 인증 및 접근제어 프로토콜에 관한 연구", 한국통신학회 논문지 제 35권 제 4호, pp.592~598, 2010. 4.

[7] David G. Hart, "Using AMI to Realize the Smart Grid", Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, 2008.



**김 홍 기**

e-mail : hgkim31@sch.ac.kr

2010년 순천향대학교 정보기술공학부 (학사)

2010년~현 재 순천향대학교 컴퓨터학과 석사과정

관심분야 : 컴퓨터보안, OTP, 스마트그리드



**이 임 영**

e-mail : imylee@sch.ac.kr

1981년 홍익대학교 전자공학과(학사)

1986년 오사카대학 통신공학전공(석사)

1989년 오사카대학 통신공학전공(박사)

1989년~1994년 한국전자통신연구원 선임연구원

1994년~현 재 순천향대학교 컴퓨터소프트웨어공학과 교수

관심분야 : 암호이론, 정보이론, 컴퓨터보안