(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2013-0052411
(43) 공개일자 2013년05월22일

(51) 국제특허분류(Int. Cl.)
*G08C 19/02* (2006.01) *G01R 22/06* (2006.01)
(21) 출원번호 10-2011-0117830
(22) 출원일자 2011년11월11일
심사청구일자 2011년11월11일

(71) 출원인
**고려대학교 산학협력단**
서울 성북구 안암동5가 1
(72) 발명자
**김홍기**
경기도 부천시 오정구 역곡로504번길 91-3, 한영다동 201호 (고강동)
**이임영**
충청남도 천안시 서북구 봉서산1길 35, 121동 902호 (쌍용동, 천안동일하이빌)
(74) 대리인
**박종한**

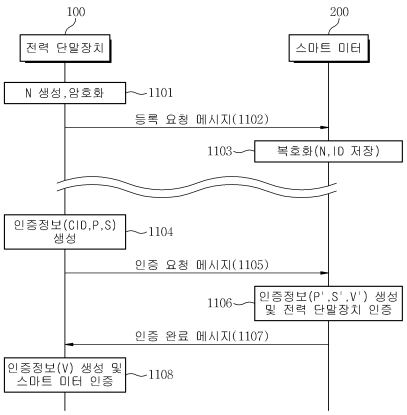
전체 청구항 수 : 총 12 항

(54) 발명의 명칭 **원격 검침 시스템, 그 시스템에서의 아이디를 이용한 상호 인증을 위한 장치 및 방법**

## (57) 요 약

본 발명은 스마트 그리드 환경의 전력망 시스템에서 안전한 전력량 전송을 위해 ID를 기반으로 각 장치들간의 상호 인증을 수행하기 위한 원격 검침 시스템, 장치 및 방법에 관한 것으로서, 스마트 미터와 각 가정의 전력 단말 장치간 및 스마트 미터와 미터 데이터 관리 장치 간의 상호 간의 상호 인증을 수행하고, 스마트 미터에서 세션 간 사용할 세션키를 생성하고 정당한 미터 데이터 관리 장치가 아니면 세션키를 생성 불가능하도록 설계하고, 재암호화 방식을 통해 전력데이터를 보다 안전하게 전송할 수 있으며, 미터 데이터 관리 장치가 정당한 장치인지를 확인할 수 있으므로 외부의 다양한 위험 요소의 노출에 의한 전력 데이터의 손상을 방지할 수 있는 효과가 있다.

*대 표 도* - 도5



## *특허청구의 범위*

**청구항 1**

임의의 아이디(N)를 이용하여 암호화된 등록 데이터를 전송하고, 자신의 인증을 위한 제1 인증 정보를 생성하고, 생성된 제1 인증 정보를 전송하여 인증을 요청하는 전력 단말 장치; 및

상기 암호화된 등록 데이터를 수신하여 복호화하고, 복호화된 등록 데이터를 이용하여 상기 전력 단말 장치를 등록하고, 상기 전력 단말 장치로부터 인증 요청 시 수신된 상기 제1 인증 정보 및 상기 등록 데이터를 이용하여 상기 전력 단말 장치의 인증을 수행하고, 상기 전력 단말 장치의 전력량을 검침하는 스마트 미터를 포함하며,

상기 전력 단말 장치는 상기 스마트 미터로부터 상기 제1 인증 정보를 이용하여 생성된 스마트 미터의 제2 인증 정보를 수신하고, 수신된 스마트 미터의 제2 인증 정보를 이용하여 상기 스마트 미터를 인증하는 것을 특징으로 하는 원격 검침 시스템.

**청구항 2**

제1항에 있어서,

상기 스마트 미터를 등록하고, 자신의 아이디를 암호화하여 상기 스마트 미터로 전송하고, 상기 스마트 미터에서 수신된 자신만이 복호 가능하도록 재 암호화된 전력 데이터를 상기 등록 시 저장된 상기 스마트 미터의 개인키를 이용하여 복호화하고, 자신의 아이디를 이용하여 생성된 세션키를 통해 암호화된 전력 데이터를 다시 복호화하여 상기 검침된 전력량에 대한 전력 데이터를 저장하는 미터 데이터 관리 장치를 더 포함하며;

상기 스마트 미터는 임의의 아이디($N_A$)를 이용하여 암호화된 등록 데이터를 상기 미터 데이터 관리 장치로 전송하고, 상기 전력 데이터를 상기 미터 데이터 관리 장치로부터 수신된 미터 데이터 관리 장치의 아이디를 이용하여 생성된 세션키를 통해 암호화하고, 암호화된 전력 데이터를 상기 개인키를 이용하여 재 암호화하여 상기 미터 데이터 관리 장치로 전송하는 것을 특징으로 하는 원격 검침 시스템.

**청구항 3**

전력량을 검침하는 스마트 미터와 데이터를 송수신하는 통신부;

임의의 아이디(N)를 이용하여 암호화된 등록 데이터를 상기 스마트 미터로 상기 통신부를 통해 전송하고, 자신의 인증을 위한 제1 인증 정보를 생성하고, 자신의 인증 요청을 위해 상기 스마트 미터로 상기 제1 인증 정보를 전송하고, 상기 스마트 미터에서 상기 제1 인증 정보를 이용하여 인증 수행 후 생성된 제2 인증 정보를 수신하여 수신된 제2 인증 정보를 이용하여 상기 스마트 미터의 인증을 수행하는 제어부; 및

상기 등록 데이터 및 인증을 위한 정보들을 저장하는 저장부를 포함하는 것을 특징으로 하는 아이디(ID)를 이용한 상호 인증을 위한 전력 단말 장치.

**청구항 4**

제3항에 있어서, 상기 제어부는,

상기 스마트 미터로부터 수신된 제2 인증 값을 포함한 상기 제2 인증 정보 및 타임 스템프($T_{SM}$)를 이용하여 제2 비교 인증 값을 생성하고, 생성된 상기 제2 비교 인증 값과 상기 제2 인증값을 비교하여 상기 스마트 미터의 인증을 수행하고, 자신의 인증을 위해 상기 스마트 미터에서 상기 인증 정보를 이용하여 생성된 제1 비교 인증 값과 비교되는 제1 인증 값을 생성하고, 생성된 제1 인증 값을 상기 제1 인증 정보에 포함하여 상기 스마트 미터로 전송함을 특징으로 하는 아이디(ID)를 이용한 상호 인증을 위한 전력 단말 장치.

**청구항 5**

전력량을 검침하기 위한 전력 단말 장치와 데이터를 송수신하는 통신부;

상기 전력 단말 장치의 전력량을 검침하는 전력 검침부;

상기 전력 단말 장치로부터 임의의 아이디를 이용하여 암호화된 등록 데이터를 수신하여 복호화하고, 복호화된 등록 데이터를 이용하여 상기 전력 단말 장치를 등록하고, 상기 전력 단말 장치로부터 인증 요청 시 수신된 제1 인증 값을 포함하는 인증 정보 및 상기 등록 데이터를 이용하여 상기 전력 단말 장치의 인증을 수행하고, 자신을 인증하도록 상기 인증 수행 후 생성된 제2 인증 값을 상기 전력 단말 장치로 전송하는 제어부; 및

상기 등록 데이터 및 인증을 위한 정보들을 저장하는 저장부를 포함하는 것을 특징으로 하는 아이디(ID)를 이용한 상호 인증을 위한 스마트 미터.

**청구항 6**

제5항에 있어서, 상기 제어부는,

상기 제1 인증 정보와, 상기 등록 데이터에 포함된 상기 임의의 아이디 및 상기 전력 단말 장치의 아이디(ID)를 이용하여 제1 비교 인증 값을 포함하는 상기 비교 인증 정보를 생성하고, 상기 제1 비교 인증 값과 상기 제1 인증 정보에 포함된 제1 인증 값을 비교하여 전력 단말 장치의 인증을 수행하고, 상기 전력 단말 장치에서 생성된 제2 비교 인증 값과 비교되는 제2 인증 값을 상기 비교 인증 정보 및 타임 스템프($T_{SM}$)를 이용하여 생성하고, 생성된 제2 인증 값을 상기 제2 인증 정보에 포함하여 상기 전력 단말 장치로 전송함을 특징으로 하는 아이디(ID)를 이용한 상호 인증을 위한 스마트 미터.

**청구항 7**

제5항에 있어서, 상기 제어부는,

임의의 아이디($N_A$)를 이용하여 암호화된 등록 데이터를 상기 미터 데이터 관리 장치로 전송하고, 상기 전력 데이터를 상기 미터 데이터 관리 장치로부터 수신된 미터 데이터 관리 장치의 아이디를 이용하여 생성된 세션키를 통해 암호화하고, 암호화된 전력 데이터를 상기 개인키를 이용하여 재 암호화하여 상기 미터 데이터 관리 장치로 전송함을 특징으로 하는 아이디(ID)를 이용한 상호 인증을 위한 스마트 미터.

**청구항 8**

전력 단말 장치의 전력량을 검출하는 스마트 미터와 데이터를 송수신하는 통신부;

자신의 아이디를 암호화하여 상기 스마트 미터로 전송하고, 상기 스마트 미터에서 수신된 자신만이 복호 가능하도록 재 암호화된 전력 데이터를 상기 등록 시 저장된 상기 스마트 미터의 개인키를 이용하여 복호화하고, 상기 자신의 아이디를 이용하여 생성된 세션키를 통해 암호화된 전력 데이터를 다시 복호화하는 제어부; 및

상기 등록 및 상호 인증을 위한 데이터 및 복호화된 상기 전력 데이터를 저장하는 저장부를 포함하는 것을 특징으로 하는 아이디(ID)를 이용한 상호 인증을 위한 미터 데이터 관리 장치.

**청구항 9**

각 가정의 하나 이상의 전력 단말 장치와 상기 전력 단말 장치의 전력량을 검출하는 스마트 미터를 구비한 원격 검침 시스템에서, 상기 전력 단말 장치와 상기 스마트 미터간 상호 인증을 위한 방법에 있어서,

상기 전력 단말 장치가 임의의 아이디(N)를 생성하고, 생성된 임의의 아이디를 이용하여 암호화된 등록 데이터를 상기 스마트 미터로 전송하여 등록을 요청하는 단계;

상기 스마트 미터가 상기 등록 데이터를 수신하여 상기 등록 데이터에 포함된 상기 임의의 아이디 및 상기 전력 단말 장치의 아이디를 저장하여 상기 전력 단말 장치를 등록하는 단계;

상기 전력 단말 장치가 자신의 인증을 위한 제1 인증 정보를 생성하여 생성된 제1 인증 정보를 상기 스마트 미터로 전송하여 인증을 요청하는 단계;

상기 스마트 미터가 수신된 상기 제1 인증 정보 및 미리 저장된 상기 임의의 아이디를 이용하여 생성된 비교 인증 정보 및 상기 제1 인증 정보를 이용하여 상기 전력 단말 장치의 인증을 수행하는 단계; 및

상기 전력 단말 장치가 상기 스마트 미터에서 상기 비교 인증 정보를 이용하여 생성된 제2 인증 정보 수신하면, 상기 제2 인증 정보를 이용하여 상기 스마트 미터의 인증을 수행하는 단계를 포함하는 것을 특징으로 하는 상기 아이디(ID)를 이용한 상호 인증을 위한 방법.

**청구항 10**

제9항에 있어서, 상기 스마트 미터가 상기 전력 단말 장치의 인증을 수행하는 단계는,

수신된 상기 제1 인증 정보 및 미리 저장된 상기 임의의 아이디를 이용하여 제1 비교 인증 값을 포함하는 상기 비교 인증 정보를 생성하는 단계;

상기 제1 인증 정보에 포함된 제1 인증 값과 상기 제1 비교 인증 값을 비교하는 단계;

상기 제1 인증 값과 상기 제1 비교 인증 값이 일치하여 인증이 성공하면, 자신의 인증을 위한 제2 인증 값을 생성하는 단계; 및

생성된 제2 인증 값과 타임스탬프($T_{SM}$)를 포함한 상기 제2 인증 정보를 상기 전력 단말 장치로 전송하는 단계를 포함하는 것을 특징으로 하는 상기 아이디(ID)를 이용한 상호 인증을 위한 방법.

**청구항 11**

제9항에 있어서, 상기 전력 단말 장치가 상기 스마트 미터의 인증을 수행하는 단계는,

상기 스마트 미터로부터 상기 제2 인증 정보를 수신하는 단계;

상기 제2 인증 정보에 포함된 타임스탬프($T_{SM}$)와, 상기 제1 인증 정보를 이용하여 제2 비교 인증 값을 생성하는 단계; 및

생성된 제2 비교 인증 값과 상기 제2 인증 정보에 포함된 제2 인증 값을 비교하는 단계를 포함하는 것을 특징으로 하는 상기 아이디(ID)를 이용한 상호 인증을 위한 방법.

**청구항 12**

각 가정의 하나 이상의 전력 단말 장치와, 상기 전력 단말 장치의 전력량을 검출하는 스마트 미터와, 상기 스마트 미터로부터 검출된 전력량을 수신하여 관리하는 미터 데이터 관리 장치를 구비한 원격 검침 시스템에서, 상기 스마트 미터와 상기 미터 데이터 관리 장치간 상호 인증을 위한 방법에 있어서,

상기 스마트 미터가 개인키를 이용하여 임의의 아이디(N)를 생성하고, 생성된 임의의 아이디를 이용하여 암호화된 등록 데이터를 상기 미터 데이터 관리 장치로 전송하여 등록을 요청하는 단계;

상기 미터 데이터 관리 장치가 수신된 등록 데이터를 복호화하여 복호화된 등록 데이터에 포함된 상기 개인키를 저장하여 상기 스마트 미터를 등록하는 단계;

상기 미터 데이터 관리 장치가 자신의 아이디를 상기 개인키로 암호화하여 암호화된 등록 데이터를 상기 스마트 미터로 전송하는 단계;

상기 스마트 미터가 상 미터 데이터 관리 장치로부터 수신한 암호화된 등록 데이터를 복호화하여 상기 미터 데이터 관리 장치의 아이디를 저장하여 등록을 완료하는 단계;

상기 스마트 미터가 상기 개인키 및 상기 미터 데이터 관리 장치의 아이디를 이용하여 생성된 세션키를 이용하여 전력 데이터를 암호화하는 단계;

상기 스마트 미터가 암호화된 전력 데이터를 상기 미터 데이터 관리 장치만이 복호화할 수 있도록 상기 개인키를 이용하여 재 암호화하는 단계;

상기 데이터 관리 장치가 상기 스마트 미터로부터 재 암호화된 전력 데이터를 수신하면, 수신된 전력 데이터를 등록 시 저장된 상기 개인키를 이용하여 복호화하는 단계;

상기 데이터 관리 장치가 세션키를 생성하여 복호화 후 남은 전력 데이터의 암호문을 생성된 세션키를 이용하여 다시 복호화하는 단계; 및

상기 데이터 관리 장치가 다시 복호화한 전력 데이터를 저장하는 단계를 포함하는 것을 특징으로 하는 상기 아이디(ID)를 이용한 상호 인증을 위한 방법.

## *명 세 서*

## 기 술 분 야

[0001] 본 발명은 스마트 그리드 환경에서의 전력망 시스템에 관한 것으로서, 특히, 전력망 시스템에서 안전한 전력량 전송을 위해 ID를 기반으로 각 장치들간의 상호 인증을 수행하기 위한 원격 검침 시스템, 장치 및 방법에 관한 것이다.

## 배 경 기 술

[0002] 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 스마트 그리드 기술에 대한 관심이 선진국을 중심으로 증대되어 활발하게 연구가 진행되고 있다.

[0003] 스마트 그리드(Smart Grid)는 기존의 전력망에 정보기술(IT)을 접목하여 전력 공급자와 소비자가 양방향으로 실시간 정보를 교환함으로써 사용 과금 및 전력공급의 효율성을 증대시키는 차세대 지능형 전력망이다.

[0004] 스마트 그리드에서는 전기로 작동되는 모든 기기들이 유?무선 네트워크로 연결되며, 서로 간의 정보 교환을 통하여 유기적인 관계로 이루어진다. 현재 제공되는 전력 시스템은 전력사용예측이 불가능하기 때문에 일반적으로 10%이상의 예비전력을 보유하여 저장하고 있다. 그러나 스마트 그리드 환경에서는 스마트 미터(Smart Meter)를 통해 실시간으로 사용되는 에너지를 분석함으로써 에너지를 효율적으로 분배할 수 있다.

[0005] 스마트 그리드의 핵심 인프라로 원격 검침 시스템인 AMI(Advanced Metering Infrastructure)이 있다. 이는 에너지를 효율적으로 관리하기 위한 체계로써, 각 가정 내 설치되는 스마트 미터와 각 가정의 디바이스 및 전력량을 취합하는 미터 데이터 관리 시스템(MDMS: Meter Data Management System)으로 구성된다. 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.

[0006] AMI는 최종 소비자와 전력회사 사이의 전력 서비스 정보화 인프라로서 스마트 그리드 운용에 필수적인 스마트 미터 기반의 핵심 인프라 시스템이다. 단순히 계량 값만을 읽어가는 기존의 AMR(Automated Meter Reading)과는 다르게 소비자의 수요 및 전력가격을 실시간으로 양방향 전송하는 역할을 담당한다.

[0007] AMI는 기존의 AMR과는 다르게 스마트 미터를 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. 또한, AMI는 수요반응 메커니즘에는 없어서는 안될 내용이며 더 나아가서는 홈 오토메이션, 홈 네트워킹과 연결되고, 결국 스마트 그리드 기본 인프라가 된다.

[0008] 기존의 전력망 시스템은 외부네트워크에서 접근이 불가능한 폐쇄적인 구조로 되어 있었기 때문에 보안에 대한 별다른 위협이 없다.

[0009] 그러나 스마트 그리드 환경으로 진화하면서 유, 무선을 통한 외부네트워크 접속이 가능해지고 각 가정의 스마트 미터로 접속이 가능하기 때문에 스마트 미터는 해킹, 악성코드 웜 및 바이러스들과 같은 다양한 위험요소에 노출될 수 있으며, 이로 인해 소비자의 개인정보 노출 및 산업 시스템 마비 등의 손실을 발생할 수 있는 문제점이 있다.

[0010] 때문에 위험요소의 노출을 방지하기 위해 AMI의 인증을 수행해야 하나, 스마트 미터는 15분에서 1시간의 간격으로 MDMS와 전력량을 전송받고 있기 때문에 적은 연산량과 빠른 속도로 인증을 수행할 필요가 있다.

## 발명의 내용

### 해결하려는 과제

[0011] 이에 본 발명은 종래의 불편함을 해소하기 위하여 제안된 것으로서, 각 가정의 전력 단말 장치 및 스마트 미터의 아이디를 이용하여 상호 인증을 제공하기 위한 원격 검침 시스템, 장치 및 방법을 제공하고자 한다.

[0012] 더하여, 본 발명은 ID를 이용하여 안전한 전력량 전송을 위해 각 가정의 전력 단말 장치와 스마트 미터 간의 상

호 인증을 수행하고, 스마트 미터와 미터 데이터 관리 장치 간의 재 암호화를 통한 상호 인증을 수행하기 위한 원격 검침 시스템, 장치 및 방법을 제공하고자 한다.

## *과제의 해결 수단*

[0013] 본 발명은 과제를 해결하기 위한 수단으로서, 임의의 아이디(N)를 이용하여 암호화된 등록 데이터를 전송하고, 자신의 인증을 위한 제1 인증 정보를 생성하고, 생성된 제1 인증 정보를 전송하여 인증을 요청하는 전력 단말 장치; 및 상기 암호화된 등록 데이터를 수신하여 복호화하고, 복호화된 등록 데이터를 이용하여 상기 전력 단말 장치를 등록하고, 상기 전력 단말 장치로부터 인증 요청 시 수신된 상기 제1 인증 정보 및 상기 등록 데이터를 이용하여 상기 전력 단말 장치의 인증을 수행하고, 상기 전력 단말 장치의 전력량을 검침하는 스마트 미터를 포함하며, 상기 전력 단말 장치는 상기 스마트 미터로부터 상기 제1 인증 정보를 이용하여 생성된 제2 인증 정보를 수신하고, 수신된 제2 인증 정보를 이용하여 상기 스마트 미터를 인증하는 것을 특징으로 하는 원격 검침 시스템을 제공한다.

[0014] 본 발명에 의한 원격 검침 시스템은 상기 스마트 미터를 등록하고, 자신의 아이디를 암호화하여 상기 스마트 미터로 전송하고, 상기 스마트 미터에서 수신된 자신만이 복호 가능하도록 재 암호화된 전력 데이터를 상기 등록 시 저장된 상기 스마트 미터의 개인키를 이용하여 복호화하고, 자신의 아이디를 이용하여 생성된 세션키를 통해 암호화된 전력 데이터를 다시 복호화하여 상기 검침된 전력량에 대한 전력 데이터를 저장하는 미터 데이터 관리 장치를 더 포함하며; 상기 스마트 미터는 임의의 아이디(NA)를 이용하여 암호화된 등록 데이터를 상기 미터 데이터 관리 장치로 전송하고, 상기 전력 데이터를 상기 미터 데이터 관리 장치로부터 수신된 미터 데이터 관리 장치의 아이디를 이용하여 생성된 세션키를 통해 암호화하고, 암호화된 전력 데이터를 상기 개인키를 이용하여 재 암호화하여 상기 미터 데이터 관리 장치로 전송할 수 있다.

[0015] 더하여, 본 발명은 과제를 해결하기 위한 다른 수단으로서, 전력량을 검침하는 스마트 미터와 데이터를 송수신하는 통신부; 임의의 아이디(N)를 이용하여 암호화된 등록 데이터를 상기 스마트 미터로 상기 통신부를 통해 전송하고, 상호 인증을 위한 인증 정보를 생성하고, 자신의 인증 요청을 위해 상기 스마트 미터로 상기 제1 인증 정보를 전송하고, 상기 스마트 미터에서 인증 정보를 이용하여 인증 수행 후 생성된 제2 인증 정보를 수신하여 수신된 제2 인증 정보를 이용하여 상기 스마트 미터의 인증을 수행하는 제어부; 및 상기 등록 데이터 및 인증을 위한 정보들을 저장하는 저장부를 포함하는 것을 특징으로 하는 아이디(ID)를 이용한 상호 인증을 위한 전력 단말 장치를 제공한다.

[0016] 본 발명에 의한 아이디(ID)를 이용한 상호 인증을 위한 전력 단말 장치에 있어서, 상기 제어부는, 상기 스마트 미터로부터 수신된 제2 인증 값을 포함한 상기 제2 인증 정보 및 타임 스템프($T_{SM}$)를 이용하여 제2 비교 인증 값을 생성하고, 생성된 상기 제2 비교 인증 값과 상기 제2 인증값을 비교하여 상기 스마트 미터의 인증을 수행하고, 자신의 인증을 위해 상기 스마트 미터에서 상기 인증 정보를 이용하여 생성된 제1 비교 인증 값과 비교되는 제1 인증 값을 생성하고, 생성된 제1 인증 값을 상기 제1 인증 정보에 포함하여 상기 스마트 미터로 전송할 수 있다.

[0017] 더하여, 본 발명은 과제를 해결하기 위한 또 다른 수단으로서, 전력량을 검침하기 위한 전력 단말 장치와 데이터를 송수신하는 통신부; 상기 전력 단말 장치의 전력량을 검침하는 전력 검침부; 상기 전력 단말 장치로부터 임의의 아이디를 이용하여 암호화된 등록 데이터를 수신하여 복호화하고, 복호화된 등록 데이터를 이용하여 상기 전력 단말 장치를 등록하고, 상기 전력 단말 장치로부터 인증 요청 시 수신된 제1 인증 정보 및 상기 등록 데이터를 이용하여 상기 전력 단말 장치의 인증을 수행하고, 자신을 인증하도록 상기 인증 수행 후 생성된 제2 인증 정보를 상기 전력 단말 장치로 전송하는 제어부; 및 상기 등록 데이터 및 인증을 위한 정보들을 저장하는 저장부를 포함하는 것을 특징으로 하는 아이디(ID)를 이용한 상호 인증을 위한 스마트 미터를 제공한다.

[0018] 본 발명에 의한 아이디(ID)를 이용한 상호 인증을 위한 스마트 미터에 있어서, 상기 제어부는, 상기 제1 인증 정보와, 상기 등록 데이터에 포함된 상기 임의의 아이디 및 상기 전력 단말 장치의 아이디(ID)를 이용하여 제1 비교 인증 값을 포함하는 상기 비교 인증 정보를 생성하고, 상기 제1 비교 인증 값과 상기 제1 인증 정보에 포함된 제1 인증 값을 비교하여 전력 단말 장치의 인증을 수행하고, 상기 전력 단말 장치에서 생성된 제2 비교 인증 값과 비교되는 제2 인증 값을 상기 비교 인증 정보 및 타임 스템프($T_{SM}$)를 이용하여 생성하고, 생성된 제2 인증 값을 상기 제2 인증 정보에 포함하여 상기 전력 단말 장치로 전송할 수 있다.

[0019] 본 발명에 의한 아이디(ID)를 이용한 상호 인증을 위한 스마트 미터에 있어서, 상기 제어부는, 임의의 아이디

($N_A$)를 이용하여 암호화된 등록 데이터를 상기 미터 데이터 관리 장치로 전송하고, 상기 전력 데이터를 상기 미터 데이터 관리 장치로부터 수신된 미터 데이터 관리 장치의 아이디를 이용하여 생성된 세션키를 통해 암호화하고, 암호화된 전력 데이터를 상기 개인키를 이용하여 재 암호화하여 상기 미터 데이터 관리 장치로 전송할 수 있다.

[0020] 더하여, 본 발명은 과제를 해결하기 위한 또 다른 수단으로서, 전력 단말 장치의 전력량을 검출하는 스마트 미터와 데이터를 송수신하는 통신부; 자신의 아이디를 암호화하여 상기 스마트 미터로 전송하고, 상기 스마트 미터에서 수신된 자신만이 복호 가능하도록 재 암호화된 전력 데이터를 상기 등록 시 저장된 상기 스마트 미터의 개인키를 이용하여 복호화하고, 상기 자신의 아이디를 이용하여 생성된 세션키를 통해 암호화된 전력 데이터를 다시 복호화하는 제어부; 및 상기 등록 및 상호 인증을 위한 데이터 및 복호화된 상기 전력 데이터를 저장하는 저장부를 포함하는 것을 특징으로 하는 아이디(ID)를 이용한 상호 인증을 위한 미터 데이터 관리 장치를 제공한다.

[0021] 더하여, 본 발명은 과제를 해결하기 위한 또 다른 수단으로서, 각 가정의 하나 이상의 전력 단말 장치와 상기 전력 단말 장치의 전력량을 검출하는 스마트 미터를 구비한 원격 검침 시스템에서, 상기 전력 단말 장치와 상기 스마트 미터간 아이디(ID)를 이용한 상호 인증을 위한 방법은, 상기 전력 단말 장치가 임의의 아이디(N)를 생성하고, 생성된 임의의 아이디를 이용하여 암호화된 등록 데이터를 상기 스마트 미터로 전송하여 등록을 요청하는 단계; 상기 스마트 미터가 상기 등록 데이터를 수신하여 상기 등록 데이터에 포함된 상기 임의의 아이디 및 상기 전력 단말 장치의 아이디를 저장하여 상기 전력 단말 장치를 등록하는 단계; 상기 전력 단말 장치가 자신의 인증을 위한 제1 인증 정보를 생성하여 생성된 제1 인증 정보를 상기 스마트 미터로 전송하여 인증을 요청하는 단계; 상기 스마트 미터가 수신된 상기 제1 인증 정보 및 미리 저장된 상기 임의의 아이디를 이용하여 생성된 비교 인증 정보 및 상기 제1 인증 정보를 이용하여 상기 전력 단말 장치의 인증을 수행하는 단계; 및 상기 전력 단말 장치가 상기 스마트 미터에서 상기 비교 인증 정보를 이용하여 생성된 제2 인증 정보를 수신하면, 상기 제2 인증 정보를 이용하여 상기 스마트 미터의 인증을 수행하는 단계를 포함할 수 있다.

[0022] 본 발명에 의한 아이디(ID)를 이용한 상호 인증을 위한 방법에 있어서, 상기 스마트 미터가 상기 전력 단말 장치의 인증을 수행하는 단계는, 수신된 상기 제1 인증 정보 및 미리 저장된 상기 임의의 아이디를 이용하여 제1 비교 인증 값을 포함하는 상기 비교 인증 정보를 생성하는 단계; 상기 제1 인증 정보에 포함된 제1 인증 값과 상기 제1 비교 인증 값을 비교하는 단계; 상기 제1 인증 값과 상기 제1 비교 인증 값이 일치하여 인증이 성공하면, 자신의 인증을 위한 제2 인증 값을 생성하는 단계; 및 생성된 제2 인증 값과 타임스템프($T_{SM}$)를 포함한 상기 제2 인증 정보를 상기 전력 단말 장치로 전송하는 단계를 포함할 수 있다.

[0023] 본 발명에 의한 아이디(ID)를 이용한 상호 인증을 위한 방법에 있어서, 기 전력 단말 장치가 상기 스마트 미터의 인증을 수행하는 단계는, 상기 스마트 미터로부터 상기 제2 인증 정보를 수신하는 단계; 상기 제2 인증 정보에 포함된 타임스탬프($T_{SM}$)와, 상기 제1 인증 정보를 이용하여 제2 비교 인증 값을 생성하는 단계; 및 생성된 제2 비교 인증 값과 상기 제2 인증 정보에 포함된 제2 인증 값을 비교하는 단계를 포함할 수 있다.

[0024] 더하여, 본 발명은 과제를 해결하기 위한 또 다른 수단으로서, 각 가정의 하나 이상의 전력 단말 장치와, 상기 전력 단말 장치의 전력량을 검출하는 스마트 미터와, 상기 스마트 미터로부터 검출된 전력량을 수신하여 관리하는 미터 데이터 관리 장치를 구비한 원격 검침 시스템에서, 상기 스마트 미터와 상기 미터 데이터 관리 장치간 아이디(ID)를 이용한 상호 인증을 위한 방법은, 상기 스마트 미터가 개인키를 이용하여 임의의 아이디(N)를 생성하고, 생성된 임의의 아이디를 이용하여 암호화된 등록 데이터를 상기 미터 데이터 관리 장치로 전송하여 등록을 요청하는 단계; 상기 미터 데이터 관리 장치가 수신된 등록 데이터를 복호화하여 복호화된 등록 데이터에 포함된 상기 개인키를 저장하여 상기 스마트 미터를 등록하는 단계; 상기 미터 데이터 관리 장치가 자신의 아이디를 상기 개인키로 암호화하여 암호화된 등록 데이터를 상기 스마트 미터로 전송하는 단계; 상기 스마트 미터가 상 미터 데이터 관리 장치로부터 수신한 암호화된 등록 데이터를 복호화하여 상기 미터 데이터 관리 장치의 아이디를 저장하여 등록을 완료하는 단계; 상기 스마트 미터가 상기 개인키 및 상기 미터 데이터 관리 장치의 아이디를 이용하여 생성된 세션키를 이용하여 전력 데이터를 암호화하는 단계; 상기 스마트 미터가 암호화된 전력 데이터를 상기 미터 데이터 관리 장치만이 복호화할 수 있도록 상기 개인키를 이용하여 재 암호화하는 단계; 상기 데이터 관리 장치가 상기 스마트 미터로부터 재 암호화된 전력 데이터를 수신하면, 수신된 전력 데이터를 등록 시 저장된 상기 개인키를 이용하여 복호화하는 단계; 상기 데이터 관리 장치가 세션키를 생성하여 복호화 후 남은 전력 데이터의 암호문을 생성된 세션키를 이용하여 다시 복호화하는 단계; 및 상기 데이터 관리 장치가 다시 복호화한 전력 데이터를 저장하는 단계를 포함할 수 있다.

## 발명의 효과

[0025] 본 발명은 스마트 미터와 각 가정의 전력 단말 장치 간 및 스마트 미터와 미터 데이터 관리 장치 간의 상호 간의 상호 인증을 수행함으로써 스마트 미터가 보다 안전하게 전력 단말 장치에서 검침한 전력량을 전송할 수 있으며, 미터 데이터 관리 장치가 정당한 장치인지를 확인할 수 있으므로 외부의 다양한 위험 요소의 노출에 의한 전력 데이터의 손상을 방지할 수 있는 효과가 있다.

[0026] 또한, 본 발명은 전력 단말 장치의 아이디를 이용하여 XOR 연산 및 해쉬 연산만으로 이용하여 암호화를 수행하므로 기존의 암호알고리즘을 이용한 인증방식보다 경량화된 방식을 통해 스마트 미터를 인증하고, 안전하게 전력데이터를 전송할 수 있는 효과가 있다.

[0027] 또한, 본 발명은 스마트 미터에서 세션 간 사용할 세션키를 생성하고 정당한 미터 데이터 관리 장치가 아니면 세션키를 생성 불가능하도록 설계하고, 재 암호화 방식을 통해 전력데이터를 안전하게 전송할 수 있는 효과가 있다.

## 도면의 간단한 설명

[0028] 도 1은 본 발명의 실시 예들에 따른 스마트 그리드 환경에서의 원격 검침 시스템을 나타낸 블럭도이다.

도 2는 본 발명의 실시 예들에 따른 원격 검침 시스템에서의 상호 인증을 위한 전력 단말 장치의 구성을 나타낸 블럭도이다.

도 3는 본 발명의 실시 예들에 따른 원격 검침 시스템에서의 상호 인증을 위한 스마트 미터의 구성을 나타낸 블럭도이다.

도 4는 본 발명의 실시 예들에 따른 원격 검침 시스템에서의 상호 인증을 위한 미터 데이터 관리 장치의 구성을 나타낸 블럭도이다.

도 5는 본 발명의 일 실시예에 따라 전력 단말 장치와 스마트 미터 간의 상호 인증을 위한 과정을 나타낸 순서도이다.

도 6은 본 발명의 다른 실시예에 따라 스마트 미터와 미터 데이터 관리 장치 간의 상호 인증을 위한 과정을 나타낸 순서도이다.

## 발명을 실시하기 위한 구체적인 내용

[0029] 이하 본 발명의 바람직한 실시 예를 첨부한 도면을 참조하여 상세히 설명한다. 다만, 하기의 설명 및 첨부된 도면에서 본 발명의 요지를 흐릴 수 있는 공지 기능 또는 구성에 대한 상세한 설명은 생략한다. 또한, 도면 전체에 걸쳐 동일한 구성 요소들은 가능한 한 동일한 도면 부호로 나타내고 있음에 유의하여야 한다.

[0030] 그러면 본 발명의 실시예들에 따른 스마트 그리드 환경에서 각 가정에서 사용되는 전력을 원격으로 검침하여 관리하고, 각 장치들 간 상호 인증을 수행하여 안전한 전력량을 전송하기 위한 원격 검침 시스템(AMI: Advanced Metering Infrastructure)에 대해 도면들을 참조하여 구체적으로 설명하기로 한다.

[0031] 도 1은 본 발명의 실시 예들에 따른 스마트 그리드 환경에서의 원격 검침 시스템을 나타낸 블럭도이다.

[0032] 도 1을 참조하면, 본 발명의 실시 예에 따른 스마트 그리드 환경에서의 원격 검침 시스템은 각 가정의 적어도 하나 이상의 전력 단말 장치(100)와, 스마트 미터(200)와, 미터 데이터 관리 장치(300)로 구성될 수 있다.

[0033] 적어도 하나 이상의 전력 단말 장치(100)는 첨부된 도 2에 도시된 바와 같이, 스마트 미터(200)와 유/무선으로 통신하여 상호 인증을 수행하며, 통신부(110), 제어부(120), 저장부(130) 및 출력부(140)를 포함하여 구성될 수 있다. 여기서 전력 단말 장치(100)는 각 가정에서 이용되는 전력 소비 기기 또는 전력 생성 기기들 일 수 있다.

[0034] 통신부(110)는 스마트 미터(200)와 데이터를 송수신하기 위한 것으로서, 유선 방식 및 무선 방식뿐만 아니라 다양한 통신 방식을 통해서 다른 단말 장치와 데이터를 송수신할 수 있다. 더하여, 하나 이상의 통신 방식을 사용하여 데이터를 송수신할 수 있으며, 이를 위하여 통신부(110)는 각각 서로 다른 통신 방식에 따라서 데이터를 송수신하는 복수의 통신 모듈을 포함할 수 있다

[0035] 제어부(120)는 스마트 미터(200)와 통신 및 상호 인증을 위한 전반적인 제어를 수행하며, 등록 단계 및 로그인 단계를 통해 상호 인증을 수행한다.

[0036] 등록 단계에서, 제어부(120)는 난수(R)를 생성하고, 전력 단말 장치(100)의 아이디(ID) 및 패스워드(PW)를 이용하여 XOR 연산을 통해 임의의 아이디(N)를 생성하고, 이를 자신의 ID와 연접하여 스마트 미터(200)와 사전에 공유된 공유키로 암호화하여 암호된 등록 데이터를 스마트 미터(200)로 통신부(110)를 통해 전송한다.

[0037] 로그인 단계에서, 제어부(120)는 아이디(ID), 타임스탬프(T), 등록단계에서 사용한 N 값 및 R 값을 이용하여 인증 정보(CID, P, S 값)를 생성하고, 생성된 난수 확인 값인 CID 및 제1 인증 값인 S 값과, 자신의 ID 및 T 값을 인증 요청 메시지에 포함하여 통신부(110)를 통해 스마트 미터(200)로 전송한다. 그리고 제어부(120)는 스마트 미터(200)로부터 스마트 미터(200)의 인증 값 즉, 제2 인증 값(V' 값)을 포함한 인증 완료 메시지를 통신부(110)를 통해 수신하면, 인증 완료 메시지에 포함된 $T_{SM}$ 값을 이용하여 제2 비교 인증 값인 V 값을 생성하고, 인증 완료 메시지에 포함된 V' 값을 생성된 V 값과 비교하여 스마트 미터(200)의 인증을 수행한다. 이러한 인증 수행은 별도 구비된 인증 모듈과의 연동을 통해 수행될 수도 있다.

[0038] 저장부(130)는 전력 단말 장치(100)의 동작에 필요한 프로그램 및 데이터를 저장하며, 특히 본 발명에 의한 등록에 필요한 정보들 및 인증에 필요한 정보들을 저장한다. 이러한 저장부(130)는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(Magnetic Media), CD-ROM(Compact Disk Read Only Memory), DVD(Digital Video Disk)와 같은 광 기록 매체(Optical Media), 플롭티컬 디스크(Floptical Disk)와 같은 자기-광 매체(Magneto-Optical Media), 및 롬(ROM), 램(RAM, Random Access Memory), 플래시 메모리를 포함한다.

[0039] 출력부(140)는 전력 단말 장치(100)의 동작 결과나 상태를 사용자가 인식할 수 있도록 제공하는 수단으로서, 예를 들면, 화면을 통해 시각적으로 출력하는 표시부나, 가청음을 출력하는 스피커 등을 포함할 수 있다.

[0040] 다음으로, 스마트 미터(200)는 전력 사용량을 실시간으로 검침하여 시간대별 요금을 알 수 있는 전자식 전력량계로서, 전력 요금 정보 및 실시간으로 검침한 전력 사용량을 저장하고, 미터 데이터 관리 장치(300)와 통신 접속을 진행하여 전력 요금 정보, 실시간 전력 사용량 정보에 대한 데이터 통신을 수행한다. 이를 위해, 스마트 미터(200)는 첨부된 도 3에 도시된 바와 같이, 전력 단말 장치(100) 또는 미터 데이터 관리 장치(300)와 상호 인증을 수행하며, 통신부(210), 제어부(220), 전력 검침부(230), 저장부(240) 및 출력부(250)를 포함하여 구성될 수 있다.

[0041] 통신부(210)는 스마트 미터(200) 및 미터 데이터 관리 장치(300)와 데이터를 송수신하기 위한 것으로서, 유선 방식 및 무선 방식뿐만 아니라 다양한 통신 방식을 통해서 다른 단말 장치와 데이터를 송수신할 수 있다. 더하여, 하나 이상의 통신 방식을 사용하여 데이터를 송수신할 수 있으며, 이를 위하여 통신부(210)는 각각 서로 다른 통신 방식에 따라서 데이터를 송수신하는 복수의 통신 모듈을 포함할 수 있다.

[0042] 제어부(220)는 전력 단말 장치(100) 및 미터 데이터 관리 장치(300)의 통신 및 상호 인증을 위한 전반적인 제어를 수행하며, 등록 단계 및 로그인 단계를 통해 상호 인증을 수행하고, 각 가정의 전력 단말 장치(100)의 실시간으로 전력을 검침하기 위한 제어를 수행한다.

[0043] 등록 단계에서, 제어부(220)는 전력 단말 장치(100)로부터 통신부(210)를 통해 등록 요청 메시지를 수신하면, 등록 요청 메시지에 포함된 암호화된 등록 데이터를 사전에 공유된 공유키(KS)로 복호화하고, 복호화된 등록 데이터에서 N 값과 전력 단말 장치의 ID를 추출하여 저장부(240)에 저장시켜서 전력 단말 장치(100)의 등록을 완료한다.

[0044] 로그인 단계에서, 제어부(220)는 전력 단말 장치(100)로부터 통신부(210)를 통해 인증 요청 메시지를 수신하면, 인증 요청 메시지에 포함된 정보들을 이용하여 비교 인증 정보(P', S' 값)를 생성하고, 수신된 CID 값을 통해 난수 R 값을 추출하고, 인증 요청 메시지에 포함된 제1 인증 값인 S 값과 생성된 제1 비교 인증 값인 S' 값을 비교하여 전력 단말 장치(100)의 인증을 수행한다. 또한, 제어부(220)는 인증이 완료되면, V' 값을 생성하고, 생성된 V' 값을 인증 완료 메시지에 포함하여 통신부(210)를 통해 전력 단말 장치(100)로 전송한다. 여기서 인증 수행은 별도 구비된 인증 모듈과의 연동을 통해 수행될 수도 있다.

[0045] 한편, 제어부(220)는 미터 데이터 관리 장치(300)와의 통신 및 상호 인증을 위한 전반적인 제어를 수행하며, 등록 단계 및 로그인 단계를 통해 상호 인증을 수행하고, 전력 검침부(230)에서 실시간으로 검침한 전력 데이터를 미터 데이터 관리 장치(300) 전송한다. 여기서 등록 단계는 스마트 미터(200)가 최초로 등록될 때 1회 수행하며, 이후, 모든 인증 및 데이터 전송 시에 등록단계는 수행되지 않는다.

[0046] 등록 단계에서, 제어부(220)는 자신의 MAC 어드레스(address)와 개인키($K_A$)를 통해 제2 임의의 아이디($N_A$)를 생성하고, 미터 데이터 관리 장치(300)의 공개키($K_{MDU}$)를 이용하여 생성된 $N_A$에 타임 스탬프(T)를 포함하여 등록

데이터를 암호화하고, MAC 어드레스를 추가한 암화화된 등록 데이터를 포함한 등록 요청 메시지 통신부(210)를 통해 미터 데이터 관리 장치(300)로 전송한다. 또한, 제어부(220)는 미터 데이터 관리 장치(300)로부터 등록 완료 메시지를 수신하면, 등록 완료 메시지에 포함된 암호화된 등록 데이터를 복호화하고, 복호화된 등록 데이터에서 미터 데이터 관리 장치(300)의 아이디(MDMS ID)를 저장부(240)에 저장시킨 후 등록 단계를 종료한다.

[0047] 로그인 단계에서, 제어부(220)는 측정된 전력 데이터를 전송하기 위해 사용될 스마트 미터(200)의 세션키($K_{SA}$)를 등록 단계에서 사용된 개인키($K_A$), MDMS ID 및 T 값을 추가하여 생성하고, 생성된 $K_{SA}$를 통해 측정된 전력량을 포함한 전력 데이터를 암호화한다. 제어부(220)는 암호화된 전력 데이터를 T 값을 포함하여 스마트 미터(200)의 개인키($H(K_A)$)를 사용하여 미터 데이터 관리 장치(300)만이 복호화 할 수 있도록 재 암호화하고, MAC 어드레스를 추가한 재 암호화된 전력 데이터를 전력 데이터 메시지에 포함하여 통신부(210)를 통해 미터 데이터 관리 장치(300)로 전송한다.

[0048] 전력 검침부(230)는 각 가정의 전력 단말 장치(100)의 전력량을 검침하여 검침된 전력량 정보를 제어부(220)로 전달한다.

[0049] 저장부(240)는 스마트 미터(200)의 동작에 필요한 프로그램 및 데이터를 저장하며, 특히 전력 단말 장치(100)와 상호 인증을 하기 위해 필요한 등록 정보들 및 인증 정보들을 저장하고, 미터 데이터 관리 장치(300)와 상호 인증을 하기 위해 필요한 등록 정보들 및 인증 정보들을 저장하고, 각 가정의 전력 단말 장치(100)에서 검침한 전력 데이터를 저장한다. 이러한 저장부(240)는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(Magnetic Media), CD-ROM(Compact Disk Read Only Memory), DVD(Digital Video Disk)와 같은 광 기록 매체(Optical Media), 플롭티컬 디스크(Floptical Disk)와 같은 자기-광 매체(Magneto-Optical Media), 및 롬(ROM), 램(RAM, Random Access Memory), 플래시 메모리를 포함한다.

[0050] 출력부(250)는 스마트 미터(200)의 동작 결과나 상태를 사용자가 인식할 수 있도록 제공하는 수단으로서, 예를 들면, 화면을 통해 시각적으로 출력하는 표시부나, 가청음을 출력하는 스피커 등을 포함할 수 있다. 특히, 본 발명의 실시예에 따른 출력부(260)는 각 가정의 전력 단말 장치(100)에서 측정한 전력량을 표시한다.

[0051] 다음으로, 미터 데이터 관리 장치(300)는 스마트 미터(200)와 통신하여 상호 인증을 수행하고, 스마트 미터(200)로부터 검침된 전력 데이터를 수신하여 관리하며, 첨부된 도 4에 도시된 바와 같이, 통신부(310), 제어부(320), 저장부(330) 및 출력부(340)를 포함하여 구성될 수 있다. 여기서 미터 데이터 관리 장치(300)는 MDMS(Meter Data Management System)에 포함된 서버 장치의 일종이다.

[0052] 통신부(310)는 스마트 미터(200)와 데이터를 송수신하기 위한 것으로서, 유선 방식 및 무선 방식뿐만 아니라 다양한 통신 방식을 통해서 다른 단말 장치와 데이터를 송수신할 수 있다. 더하여, 하나 이상의 통신 방식을 사용하여 데이터를 송수신할 수 있으며, 이를 위하여 통신부(310)는 각각 서로 다른 통신 방식에 따라서 데이터를 송수신하는 복수의 통신 모듈을 포함할 수 있다.

[0053] 제어부(320)는 스마트 미터(200)와의 통신 및 상호 인증을 위한 전반적인 제어를 수행하며, 등록 단계 및 로그인 단계를 통해 상호 인증을 수행하고, 스마트 미터(200)에서 검침된 각 가정의 전력 단말 장치(100)의 전력 데이터를 관리한다.

[0054] 등록 단계에서 제어부(320)는 스마트 미터(200)로부터 등록 요청 메시지를 수신하면, 수신된 등록 요청 메시지에 포함된 암화화된 등록 데이터를 자신의 개인키($K_{MDP}$)를 통해 복호화하여 MAC 어드레스를 확인하고, 확인된 MAC 어드레스와 $N_A$ 값에 포함되어 있는 해쉬 연산된 스마트 미터(200)의 개인키($H(K_A)$를 추출하여 추출된 $H(K_A)$를 저장부(330)에 저장한다. 그리고 제어부(320)는 자신의 아이디(MDMS ID)를 등록 요청 메시지 수신 시간($T_S$)를 포함하여 스마트 미터(200)에서만 확인이 가능하도록 $H(K_A)$로 암호화 한 후 암호화된 데이터를 등록 완료 메시지에 포함하여 스마트 미터(200)로 전송한다.

[0055] 로그인 단계에서 제어부(320)는 스마트 미터(200)로부터 전력 데이터 메시지를 수신하면, 수신된 전력 데이터 메시지에 포함된 MAC 어드레스를 통해 스마트 미터(200)의 $H(K_A)$를 검색하고, 검색된 $H(K_A)$를 이용하여 암호화된 전력 데이터를 복호화한다. 그리고 제어부(320)는 복호화 후, MDMS ID, $H(K_A)$ 및 T를 이용하여 $K_{SA}$를 생성하고, 생성된 $K_{SA}$를 통해 복호화된 전력 데이터의 남은 암호문을 다시 복호화하여 스마트 미터(200)에서 측정된 전력량에 대한 전력 데이터를 저장부(330)에 저장시킨다.

[0056] 저장부(330)는 미터 데이터 관리 장치(300)의 동작에 필요한 프로그램 및 데이터를 저장하며, 특히 스마트 미터(200)와 상호 인증을 하기 위해 필요한 등록 정보들 및 인증 정보들을 저장하고, 스마트 미터(200)로부터 수신한 전력 량 데이터를 저장한다. 이러한 저장부(150)는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(Magnetic Media), CD-ROM(Compact Disk Read Only Memory), DVD(Digital Video Disk)와 같은 광 기록 매체(Optical Media), 플롭티컬 디스크(Floptical Disk)와 같은 자기-광 매체(Magneto-Optical Media), 및 롬(ROM), 램(RAM, Random Access Memory), 플래시 메모리를 포함한다.

[0057] 출력부(340)는 미터 데이터 관리 장치(300)의 동작 결과나 상태를 사용자가 인식할 수 있도록 제공하는 수단으로서, 예를 들면, 화면을 통해 시각적으로 출력하는 표시부나, 가청음을 출력하는 스피커 등을 포함할 수 있다. 특히, 본 발명에 있어서, 출력부(130)는 그룹 대화 메시지들에 포함된 그룹 대화 내용 및 첨부된 자료 등을 사용자가 확인할 수 있도록 화면에 출력할 수 있다.

[0058] 그러면 이와 같이 구성된 스마트 그리스 환경에서 원격 검침 시스템에서의 상호 인증을 위한 방법에 대해 첨부된 도면들을 참조하여 구체적으로 설명하기로 한다.

[0059] 우선, 본 발명의 일 실시예에 따라 원격 검침 시스템에서의 전력 단말 장치(100)와 스마트 미터(200) 간의 상호 인증을 위한 과정을 설명하기로 한다.

[0060] 도 5는 본 발명의 일 실시예에 따라 전력 단말 장치와 스마트 미터 간의 상호 인증을 위한 과정을 나타낸 순서도이다.

[0061] 도 5를 참조하면, 우선, 전력 단말 장치(100)는 스마트 미터(200)에 자신을 등록하기 위한 등록 단계를 수행한다.

[0062] 이에 따라 1101단계에서 전력 단말 장치(100)는 난수(R 값)를 생성하고, 하기 <수학식 1>과 같이 자신의 아이디(ID)와 동기화 시 입력한 패스워드($PW_D$)를 XOR 연산한 후, 해쉬 값(h) 값을 생성하고, 생성된 해쉬값을 난수 R과 XOR 연산하여 임의의 아이디인 N 값을 생성한다.

*수학식 1*

[0063] $$N = R \oplus h(ID \oplus PW_D)$$

[0064] 또한, 1101단계에서 전력 단말 장치(100)는 하기 <수학식 2>와 같이, 생성된 N 값을 사전에 공유된 공유키(KS)로 암호화하고, 디바이스의 ID값과 연접하여 등록 데이터를 생성한다.

*수학식 2*

[0065] $$E_{k_3}[N] \| ID$$

[0066] 그런 다음 1102단계에서 전력 단말 장치(100)는 생성된 등록 데이터를 등록 요청 메시지에 포함하여 스마트 미터(200)로 전송한다.

[0067] 이후, 1103단계에서 스마트 미터(200)는 하기 <수학식 3>과 같이 수신한 등록 요청 메시지에 포함된 암호화된 등록 데이터를 공유키($K_S$)로 복호화하고, 복호화된 등록 데이터에서 N 값과 ID를 추출하여 저장한다.

*수학식 3*

[0068] $$D_{k_3}[E_{k_3}[N]]$$

[0069] 이와 같이, 등록단계를 수행함에 따라 스마트 미터(200)는 전력 단말 장치(100)의 ID와 N의 값을 저장하게 되므로 이후, 스마트 미터(200)는 전력 단말 장치(100)를 식별하여 전력량을 검침할 수 있으며, 저장된 ID 및 N 값

을 이용하여 전력 단말 장치(100)의 인증을 수행할 수 있다.

[0070] 등록단계 이후, 전력 단말 장치(100)와 스마트 미터(200)는 로그인 단계를 통해 상호 인증을 수행한다.

[0071] 이에 따라 1104단계에서 전력 단말 장치(100)는 ID와 타임스템프($T_D$), 등록단계 시 사용한 N 값과 R 값을 이용하여 하기 <수학식 4> 내지 <수학식 6>과 같이 제1 인증 정보(CID, P, S 값)를 생성한다. 여기서 CID는 인증 시 난수(R)를 확인하기 위한 값으로 스마트 미터(200)에서 난수를 확인하기 위한 값으로 사용된다. P 값은 S 값을 생성하기 위한 고유의 ID로 S 값에 포함된다. 제1 인증 값인 S 값은 전력 단말 장치(100)를 인증하기 위한 인증 값으로써, 스마트 미터에서는 제1 비교 인증 값인 S' 값을 생성하여 전력 단말 장치(100)를 인증한다.

[0072] 구체적으로, 전력 단말 장치(100)는 N 값을 해쉬 값(h)으로 해쉬 연산하고, R 값을 추가하여 CID 값을 생성하고, 생성된 CID 값 및 N 값을 해쉬 연산하여 P 값을 생성한다. 그리고 전력 단말 장치(100)는 R 값, $T_D$ 값, N 값 및 생성된 P 값을 해쉬 연산하여 S 값을 생성한다.

*수학식 4*

[0073] $$CID = R + h(ID + T_D + N)$$

*수학식 5*

[0074] $$P = h(CID + N)$$

*수학식 6*

[0075] $$S = h(R + T_D + P + N)$$

[0076] 1105단계에서 전력 관리 장치(100)는 제1 인증 정보를 포함하여 인증 요청 메시지를 생성하고, 생성된 인증 요청 메시지를 스마트 미터(200)로 전송한다. 여기서 전송되는 제1 인증 정보에는 생성한 CID, S값과 자신의 ID, $T_D$ 값이 포함된다.

[0077] 이에 따라 1106단계에서 스마트 미터(200)는 수신한 인증 요청 메시지에 포함된 제1 인증 정보를 이용하여 비교 인증 정보(P', S' 값) 및 난수 R 값을 생성한다. 즉, 스마트 미터(200)는 하기 <수학식 7>과 같이 P' 값을 생성하고, 하기 <수학식 8>과 같이 CID 값을 이용하여 난수 R 값을 추출한다. 구체적으로 스마트 미터(200)는 수신한 CID 값과 등록 단계에서 저장된 N 값을 해쉬 연산하여 P' 값을 생성하고, 수신한 ID, $T_D$ 값과 N 값을 해쉬 연산하고 여기에 생성된 CID 값을 추가하여 R 값을 생성한다.

*수학식 7*

[0078] $$P' = h(CID + N)$$

*수학식 8*

[0079] $$R = CID + h(ID + T_D + N)$$

[0080] 그리고 1106단계에서 스마트 미터(200)는 하기 <수학식 9>와 같이, 생성된 R, P' 값에 N 값과 수신된 TD 값을

해쉬 연산하여 제1 비교 인증 값인 S' 값을 생성한다.

*수학식 9*

[0081] $$S' = h(R + T_D + P' + N)$$

[0082] 또한, 1106단계에서 스마트 미터(200)는 이렇게 생성한 S' 값과 제1 인증 정보에 포함된 S값을 비교하여 전력 단말 장치(10)의 인증을 수행하고, 두 값이 일치하여 인증이 성공하면, 자신의 인증을 위한 제2 인증 값을 생성한다. 즉, 인증이 완료되면, 하기 <수학식 10>과 같이 타임 스템프($T_{SM}$), 수신된 CID 값 및 생성된 P 값을 해쉬 연산하여 제2 인증 값인 V' 값을 생성한다.

*수학식 10*

[0083] $$V' = h(CID + T_{sm} + P')$$

[0084] 이후, 1107단계에서 스마트 미터(200)는 생성된 V' 값과 타임스템프($T_{SM}$)를 포함하는 제2 인증 정보를 포함하여 인증 완료 메시지를 생성하고, 생성된 인증 완료 메시지를 전력 단말 장치(100)로 전송한다.

[0085] 이에 따라 1108단계에서 전력 단말 장치(100)는 인증 완료 메시지를 수신하면, 제2 인증 정보에 포함된 $T_{SM}$ 값을 이용하여 하기 <수학식 11>에 포함된 제2 비교 인증 값인 V 값을 생성한다. 구체적으로, 전력 단말 장치(100)는 1104단계에서 생성되어 저장된 CID 값, P 값과, 수신한 $T_{SM}$ 값을 해쉬 연산하여 V 값을 생성한다.

*수학식 11*

[0086] $$V = h(CID + T_{sm} + P)$$

[0087] 그리고 1108단계에서 전력 단말 장치(100)는 생성한 V 값과 인증 완료 메시지에 포함된 V' 값을 비교하여 스마트 미터(200)의 인증을 수행한다. 이때, V 값과 V' 값이 일치하는 경우, 전력 단말 장치(100)는 인증 성공으로 전력량 전송에 안전한 것으로 판단하고, 인증 성공을 출력부(140)를 통해 사용자에게 알린다. 반면, V 값과 V' 값이 일치하지 않는 경우, 전력 단말 장치(100)는 인증에 실패한 것으로 판단하여 스마트 미터(200)와 통신을 중단하고, 인증 실패를 사용자에게 알린다.

[0088] 이와 같은 등록 단계 및 로그인 단계의 과정을 통해 전력 단말 장치(100)와 스마트 미터(200) 간의 상호 인증을 할 수 있으며, 이를 통해 안전하게 데이터를 송수신할 수 있게 된다.

[0089] 다음으로, 본 발명의 다른 실시예에 따라 원격 검침 시스템에서의 스마트 미터(200)와 미터 데이터 관리 장치(300) 간의 상호 인증을 위한 과정을 설명하기로 한다.

[0090] 도 6은 본 발명의 다른 실시예에 따라 스마트 미터와 미터 데이터 관리 장치 간의 상호 인증을 위한 과정을 나타낸 순서도이다.

[0091] 도 6을 참조하면, 우선, 스마트 미터(200)와 미터 데이터 관리 장치(300) 간에 자신을 등록하기 위한 등록 단계를 수행한다.

[0092] 1201단계에서 스마트 미터(200)는 하기 <수학식 12>와 같이 MAC 어드레스와 자신의 개인키($H(K_A)$)를 이용하여 임의의 아이디 $N_A$를 생성하고, 하기 <수학식 13>과 같이 생성된 $N_A$에 타임 스탬프를 추가하고 미터 데이터 관리 장치(300)의 공개키($K_{MDU}$)를 사용하여 암호화한다.

수학식 12

[0093] $$N_A = MACAddr + H(K_A)$$

수학식 13

[0094] $$E_{KMDU}[N_A || T] || MACAddr$$

[0095] 1202단계에서 스마트 미터(200)는 암호화된 등록 데이터에 MAC 어드레스를 추가하여 등록 요청 메시지를 생성하고, 생성된 등록 요청 메시지를 미터 데이터 관리 장치(300)로 전송한다.

[0096] 이에 따라 1203단계에서 미터 데이터 관리 장치(300)는 하기 <수학식 14>와 같이 등록 요청 메시지에 포함된 암호화된 등록 데이터를 자신의 개인키($K_{MDP}$)로 복호화하여 MAC 어드레스를 확인하고, MAC 어드레스와, $N_A$에 포함되어 있는 해쉬 연산 된 스마트 미터(200)의 개인키($H(K_A)$)를 저장한다. 저장된 $H(K_A)$는 이후 미터 데이터 관리 장치(300)에서 상호 인증을 위한 암호화 시 암호화키로 이용된다.

수학식 14

[0097] $$D_{KMDP}[E_{KMDU}[N_A || T]]$$

[0098] 1204단계에서 미터 데이터 관리 장치(300)는 스마트 미터(200)의 $H(K_A)$를 저장 후, 하기 <수학식 15>와 같이 자신의 ID(MDMS ID)와 스마트 미터(200)로부터 등록 요청 메시지를 수신한 시각($T_S$)을 포함하여 $H(K_A)$로 등록 데이터를 암호화한다.

수학식 15

[0099] $$E_{H(KA)}[MDMSID || T_s]$$

[0100] 암호화가 완료되면, 1205단계에서 미터 데이터 관리 장치(300)는 암호화된 등록 데이터를 포함한 등록 완료 메시지를 생성하여 생성된 등록 완료 메시지를 스마트 미터(200)로 전송한다.

[0101] 이에 따라 1206단계에서 스마트 미터(200)는 등록 완료 메시지를 수신하면, 하기 <수학식 16>와 같이 수신한 등록 완료 메시지에 포함된 암호화된 등록 데이터를 자신의 개인키(H(KA))를 복호화하고, 복호화된 등록 데이터에서 미터 데이터 관리 장치(300)의 아이디인 MDMS ID를 저장하고 등록단계를 마친다.

수학식 16

[0102] $$D_{H(KA)}[E_{H(KA)}[MDMSID || T_s]]$$

[0103] 등록단계가 완료되면, 스마트 미터(200)와 미터 데이터 관리 장치(300)는 로그인 단계를 통해 상호 인증을 수행한다. 이때, 스마트 미터(200)는 MDMS ID를 저장하고 있고, 미터 데이터 관리 장치(300)는 해쉬 연산된 스마트 미터(200)의 개인키($H(K_A)$)와 MAC 어드레스를 저장하고 있다.

[0104] 1207단계에서 스마트 미터(200)는 하기 <수학식 17>과 같이 등록단계에서 사용된 H(KA)와 MDMS ID, T를 이용하여 각 가정의 전력 단말 장치(100)에서 측정된 전력량을 전송하기 위하여 사용될 키 즉, 스마트 미터(200)의 세

션키($K_{SA}$)를 생성한다.

*수학식 17*

[0105] $$K_{SA} = H(T + H(KA) + MDMSID)$$

[0106] 이후, 1208단계에서 스마트 미터(200)는 하기 <수학식 18>과 같이 생성된 $K_{SA}$를 통해 전력 데이터를 암호화하고, 암호화된 전력 데이터를 미터 데이터 관리 장치(300)에서 복호화할 수 있도록 T를 추가하여 $H(K_A)$를 사용하여 재 암호화한다.

*수학식 18*

[0107] $$E_{H(KA)}[T \| E_{SA}[M]] \| MACAddr$$

[0108] 재 암호화 후, 1209단계에서 스마트 미터(200)는 암호화된 전력 데이터에 MAC 어드레스를 추가하여 전력 데이터 메시지를 생성하고, 생성된 전력 데이터 메시지를 미터 데이터 관리 장치(300)로 전송한다.

[0109] 이에 따라 1210단계에서 미터 데이터 관리 장치(300)는 전력 데이터 메시지를 수신하면, 수신한 전력 데이터 메시지에 포함된 MAC 어드레스를 통해 등록 단계에서 미리 저장된 $H(K_A)$를 검색하고, 하기 <수학식 19>와 같이, 검색된 $H(K_A)$를 이용하여 암호화된 전력 데이터를 복호화한다.

*수학식 19*

[0110] $$D_{H(KA)}[E_{H(KA)}[T \| E_{SA}[M]]]$$

[0111] 복호화 후, 1211단계에서 미터 데이터 관리 장치(300)는 남아 있는 암호문을 복호화하기 위해 하기 <수학식 20>과 같이 세션키($K_{SA}$)를 생성하고,

*수학식 20*

[0112] $$K_{SA} = H(T + H(KA) + MDMSID)$$

[0113] 그리고 1211단계에서 미터 데이터 관리 장치(300)는 하기 <수학식 21>과 같이 생성된 $K_{SA}$를 통해 남은 암호문($E_{SA}[M]$)을 복호화하여 전력 데이터(M)를 저장부에 저장한다.

*수학식 21*

[0114] $$D_{SA}[E_{SA}[M]]$$

[0115] 이와 같은 등록 단계 및 로그인 단계의 과정을 통해 본 발명은 스마트 미터(200)와 미터 데이터 관리 장치(300) 간의 상호 인증을 할 수 있으며, 미터 데이터 관리 장치(300)가 정당한 장치인지를 판단할 수 있다. 또한, 본 발명은 스마트 미터(200)에서 재 암호화 방식을 통해 전력 데이터를 안전하게 전송할 수 있으며, 세션 간 생성할 세션키를 생성하고, 미터 데이터 관리 장치(300)가 정당한 장치가 아니면 미터 데이터 관리 장치(300)에서

세션키를 생성 불가능하도록 할 수 있다.

[0116] 본 발명에 따른 상호 인증 방법은 다양한 컴퓨터 수단을 통하여 판독 가능한 소프트웨어 형태로 구현되어 컴퓨터로 판독 가능한 기록매체에 기록될 수 있다. 여기서, 기록매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 기록매체에 기록되는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 예컨대 기록매체는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(Magnetic Media), CD-ROM(Compact Disk Read Only Memory), DVD(Digital Video Disk)와 같은 광 기록 매체(Optical Media), 플롭티컬 디스크(Floptical Disk)와 같은 자기-광 매체(Magneto-Optical Media), 및 롬(ROM), 램(RAM, Random Access Memory), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치를 포함한다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함할 수 있다. 이러한 하드웨어 장치는 본 발명의 동작을 수행하기 위해 하나 이상의 소프트웨어 모로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0117] 이상과 같이, 본 명세서와 도면에는 본 발명의 바람직한 실시 예에 대하여 개시하였으나, 여기에 개시된 실시 예외에도 본 발명의 기술적 사상에 바탕을 둔 다른 변형 예들이 실시 가능하다는 것은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에게 자명한 것이다. 또한, 본 명세서와 도면에서 특정 용어들이 사용되었으나, 이는 단지 본 발명의 기술 내용을 쉽게 설명하고 발명의 이해를 돕기 위한 일반적인 의미에서 사용된 것이지, 본 발명의 범위를 한정하고자 하는 것은 아니다.

## *산업상 이용가능성*

[0118] 본 발명은, 스마트 그리드 환경의 전력망 시스템에서 안전한 전력량 전송을 위해 ID를 기반으로 각 장치들간의 상호 인증을 수행하기 위한 원격 검침 시스템, 장치 및 방법에 관한 것으로서, 스마트 미터와 각 가정의 전력 단말 장치간 및 스마트 미터와 미터 데이터 관리 장치 간의 상호 간의 상호 인증을 수행함으로써 스마트 미터가 보다 안전하게 전력 단말 장치에서 검침한 전력량을 전송할 수 있으며, 미터 데이터 관리 장치가 정당한 장치인지를 확인할 수 있으므로 외부의 다양한 위험 요소의 노출에 의한 전력 데이터의 손상을 방지할 수 있다.

[0119] 또한, 본 발명은 전력 단말 장치의 아이디를 이용하여 XOR 연산 및 해쉬 연산만으로 이용하여 암호화를 수행하므로 기존의 암호알고리즘을 이용한 인증방식보다 경량화된 방식을 통해 스마트 미터를 인증하고, 안전하게 전력데이터를 전송할 수 있으며, 스마트 미터에서 세션 간 사용할 세션키를 생성하고 정당한 미터 데이터 관리 장치가 아니면 세션키를 생성 불가능하도록 설계하고, 재 암호화 방식을 통해 전력데이터를 안전하게 전송할 수 있다.

## *부호의 설명*

[0120] 100: 전력 단말 장치 110: 통신부

120: 제어부 130: 저장부

140: 출력부 200: 스마트 미터

210: 통신부 220: 제어부

230: 전력 검출부 240: 저장부

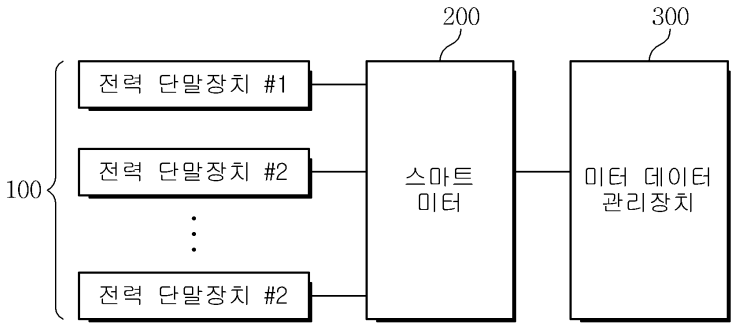
300: 미터 데이터 관리 장치 310: 통신부

320: 제어부 330: 저장부

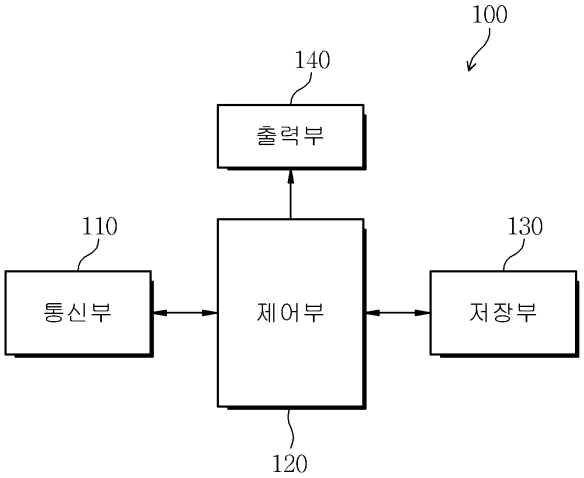
340: 출력부

## 도면

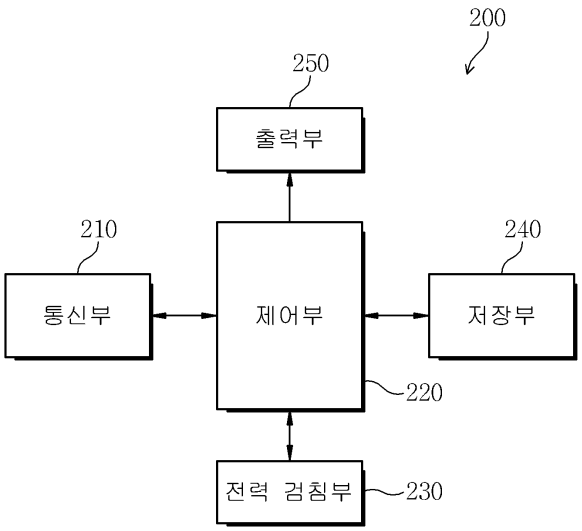
### 도면1



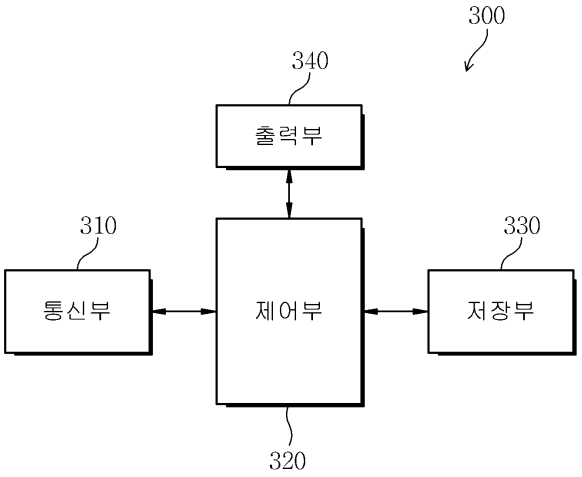

### 도면2



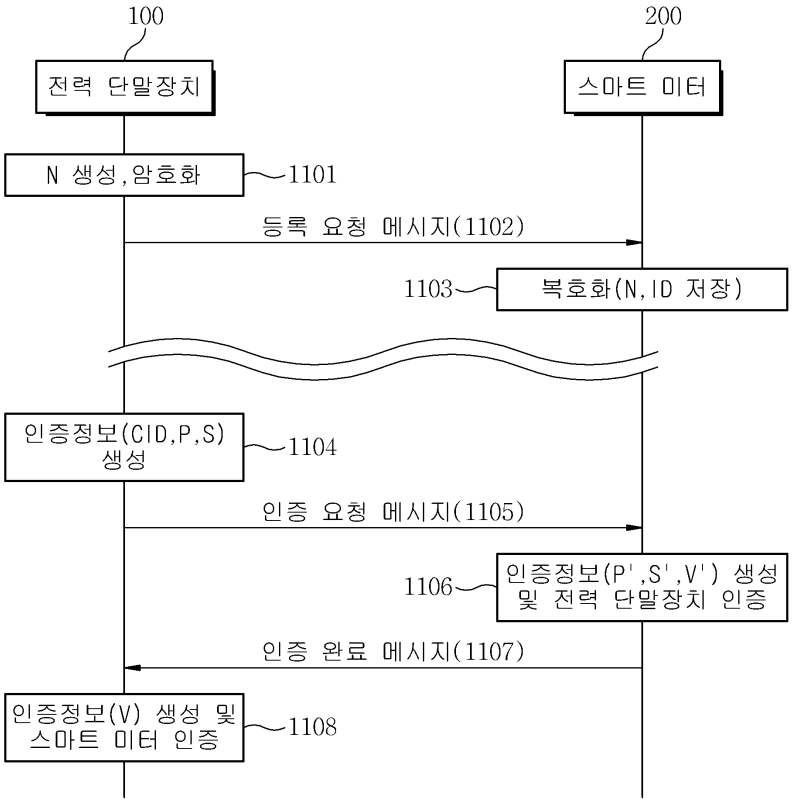

### 도면3



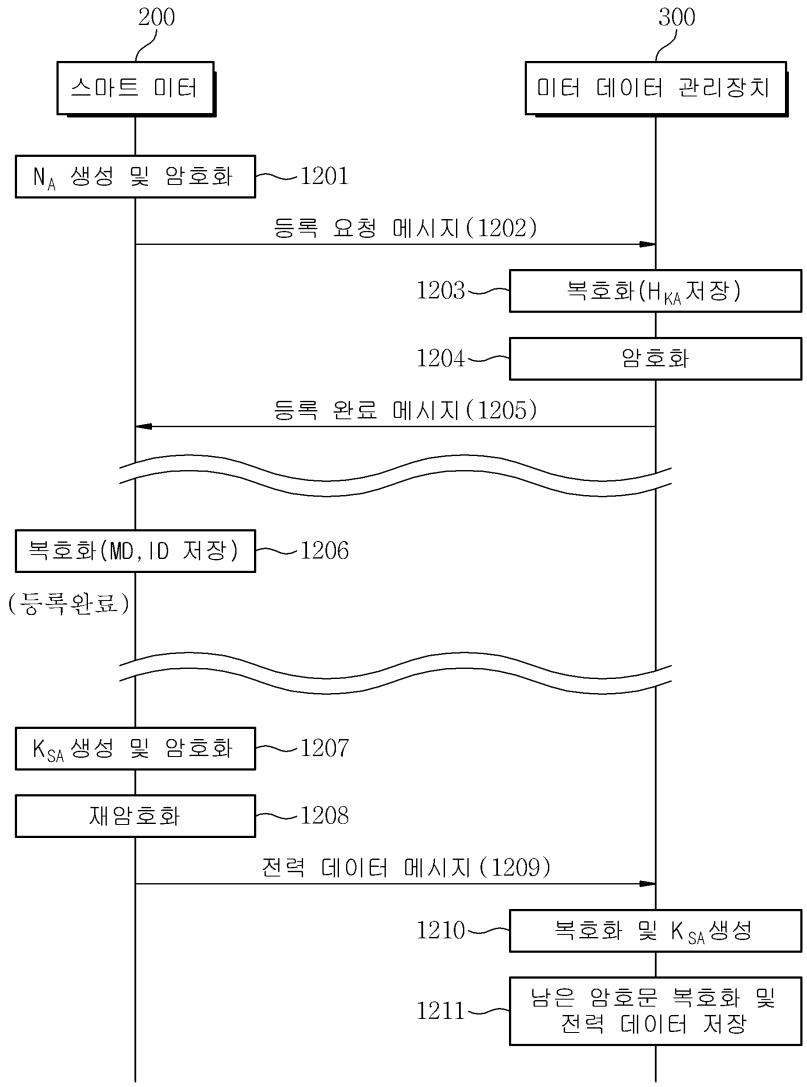
도면4


300
340
출력부
310
330
통신부
제어부
저장부
320

도면5


100
200
전력 단말장치
스마트 미터
N 생성,암호화
1101
등록 요청 메시지(1102)
1103
복호화(N,ID 저장)
인증정보(CID,P,S) 생성
1104
인증 요청 메시지(1105)
1106
인증정보(P',S',V') 생성 및 전력 단말장치 인증
인증 완료 메시지(1107)
인증정보(V) 생성 및 스마트 미터 인증
1108

도면6


200
300
스마트 미터
미터 데이터 관리장치
$N_A$ 생성 및 암호화
1201
등록 요청 메시지(1202)
1203
복호화($H_{KA}$저장)
1204
암호화
등록 완료 메시지(1205)
복호화(MD,ID 저장)
1206
(등록완료)
$K_{SA}$ 생성 및 암호화
1207
재암호화
1208
전력 데이터 메시지(1209)
1210
복호화 및 $K_{SA}$생성
1211
남은 암호문 복호화 및
전력 데이터 저장