



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2010-0036798
(43) 공개일자 2010년04월08일

(51) Int. Cl.

H04B 3/54 (2006.01)

(21) 출원번호 10-2008-0096181

(22) 출원일자 2008년09월30일

심사청구일자 2008년09월30일

(71) 출원인

경희대학교 산학협력단

경기도 용인시 기흥구 서천동 1 경희대학교 국제 캠퍼스내

한국전력공사

서울특별시 강남구 삼성동 167번지

(72) 발명자

홍충선

경기 용인시 수지구 상현동 성원3차상떼빌아파트 233-101

조웅준

경기도 수원시 영통구 영통1동 1029-12번지 103호

(뒷면에 계속)

(74) 대리인

서재승

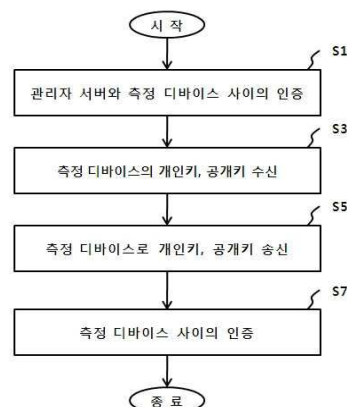
전체 청구항 수 : 총 5 항

(54) 전력선 통신 네트워크에서 측정 디바이스들 사이의 인증 방법

(57) 요약

본 발명은 통신 네트워크를 구성하는 디바이스들 사이의 인증 방법에 관한 것으로, 보다 구체적으로 전력선 통신 네트워크를 구성하는 다수의 측정 디바이스들 사이에서 별도의 인증 기관없이도 용이하게 상대방 측정 디바이스를 인증할 수 있는 방법에 관한 것이다. 본 발명에 따른 디바이스의 인증 방법은 관리자 서버와 디바이스 사이의 1차 인증과 디바이스 사이의 2차 인증을 통해 전력선 통신 네트워크를 구성하는 디바이스를 2중으로 인증함으로써, 정확하고 안전하게 디바이스를 인증할 수 있다. 또한, 본 발명에 따른 디바이스의 인증 방법은 메인 서버에서 할당받은 공개키와 개인키를 이용하여 디바이스들이 직접 서로를 인증함으로써, 디바이스의 인증 절차로 인하여 네트워크에 과부하가 발생하지 않으며 별도의 인증 서버를 구비하지 않은 전력선 네트워크에서 디바이스들이 서로를 인증할 수 있다.

대표도 - 도3



(72) 발명자

허준

경기도 군포시 궁내동 우록주공아파트 711-1601

주성호

대전광역시 유성구 문지동 103-16번지

최문석

대전광역시 유성구 문지동 103-16번지

임용훈

대전광역시 유성구 문지동 103-16번지

특허청구의 범위

청구항 1

메인 서버와 관리자 서버가 인터넷 네트워크로 접속되어 있으며, 상기 관리자 서버와 다수의 측정 디바이스들은 전력선 통신 네트워크로 접속되어 있는 통신 네트워크에서, 상기 측정 디바이스들 사이의 인증을 수행하는 방법에 있어서,

(a) 상기 관리자 서버에 저장된 상기 다수의 측정 디바이스들의 시리얼 번호와 상기 다수의 측정 디바이스들이 가지고 있는 시리얼 번호에 기초하여 상기 관리자 서버와 다수의 측정 디바이스들 사이의 인증을 수행하는 단계;

(b) 상기 관리자 서버에서, 상기 다수의 측정 디바이스들 각각에 대한 개인키와 공개키를 상기 메인 서버로부터 수신하고 상기 수신한 개인키와 공개키를 상기 측정 디바이스로 송신하는 단계;

(c) 상기 각 측정 디바이스의 공개키와 개인키를 이용하여 상대방 측정 디바이스를 인증하는 단계를 포함하는 것을 특징으로 하는 인증 수행 방법.

청구항 2

제 1 항에 있어서, 상기 (a) 단계는

상기 측정 디바이스에서 생성된 제1 난수와 상기 측정 디바이스의 MAC 주소를 상기 측정 디바이스로부터 상기 관리자 서버로 송신하고, 상기 제1 난수와 측정 디바이스의 MAC 주소에 기초하여 상기 관리자 서버에서 생성된 상기 관리자 서버의 검증값을 수신하여 상기 측정 디바이스에서 상기 관리자 서버를 인증하는 단계; 및

상기 관리자 서버의 검증값과 상기 측정 디바이스의 시리얼 번호로부터 생성된 상기 측정 디바이스의 검증값을 상기 측정 디바이스로부터 수신하여 상기 관리자 서버에서 상기 측정 디바이스를 인증하는 단계를 포함하며,

상기 관리자 서버의 검증값과 상기 측정 디바이스의 검증값은 각각 관리자 서버와 측정 디바이스에서 동일한 제 1 해쉬 함수를 이용하여 생성되는 것을 특징으로 하는 인증 수행 방법.

청구항 3

제 1 항에 있어서, 상기 (b) 단계는

상기 관리자 서버에서 상기 메인 서버로부터 상기 다수의 측정 디바이스들에 할당할 개인키와 공개키를 수신하고 상기 수신한 개인키와 공개키를 저장하는 단계;

상기 저장한 개인키를 각 측정 디바이스들에 송신하는 단계; 및

상기 다수의 측정 디바이스들 중 서로 인증하고자 하는 제1 측정 디바이스와 제2 측정 디바이스로부터 인증 요청 메시지를 수신하는 경우, 상기 제1 측정 디바이스와 제2 측정 디바이스에 각각 상기 제2 측정 디바이스와 제 1 측정 디바이스의 공개키를 송신하는 단계를 포함하는 것을 특징으로 하는 인증 수행 방법.

청구항 4

제 3 항에 있어서,

상기 개인키와 공개키는 상기 메인 서버로부터 주기적으로 갱신되어 생성되며,

상기 관리자 서버는 상기 갱신된 개인키와 공개키를 상기 메인 서버로부터 수신하여 상기 측정 디바이스에 할당하는 것을 특징으로 하는 인증 수행 방법.

청구항 5

제 3 항에 있어서, 상기 (c) 단계는

상기 제1 측정 디바이스에서 제2 난수를 생성하고, 상기 생성한 제2 난수를 상기 제2 측정 디바이스의 공개키로 암호화하여 상기 제2 측정 디바이스로 송신하는 단계;

상기 제2 측정 디바이스에서 제3 난수를 생성하고, 상기 생성한 제3 난수를 상기 제1 측정 디바이스의 공개키로

암호화하여 상기 제1 측정 디바이스로 송신하는 단계;

상기 제1 측정 디바이스와 제2 측정 디바이스에서 각각 상기 제2 난수와 제3 난수를 동일한 제2 해쉬 함수에 적용하여 인증값을 계산하는 단계; 및

상기 제1 측정 디바이스에서 계산한 인증값과 상기 제2 측정 디바이스에서 계산한 인증값이 서로 동일한지 여부로 상기 제1 측정 디바이스와 제2 측정 디바이스를 인증하는 단계를 포함하는 것을 특징으로 하는 인증 수행 방법.

명세서

발명의 상세한 설명

기술 분야

[0001] 본 발명은 통신 네트워크를 구성하는 디바이스들 사이의 인증 방법에 관한 것으로, 보다 구체적으로 전력선 통신 네트워크를 구성하는 다수의 측정 디바이스들 사이에서 별도의 인증 기관없이도 용이하게 상대방 측정 디바이스를 인증할 수 있는 방법에 관한 것이다.

배경 기술

[0002] 최근 들어, 센서 네트워크, 전력선 통신 네트워크, 무선 메쉬 네트워크 등 데이터 전달 매체의 특성과 사용자 환경을 고려한 새로운 네트워크 기술들이 개발되고 있으며, 이들 새로운 네트워크 기술을 상용화하기 위한 노력들이 진행되고 있다. 새롭게 개발된 네트워크에서 네트워크의 확장에 따른 관리 개체의 증가에도 효율적으로 디바이스를 관리할 수 있으며 안전한 통신망 구축을 위하여 네트워크를 구성하는 디바이스들의 인증 방법에 대한 연구가 진행되고 있다.

[0003] 도 1은 종래 전력선 통신을 이용하여 수용가의 전기, 가스, 수도의 사용량을 검침하는 시스템을 설명하기 위한 도면이다.

[0004] 도 1을 참고로 살펴보면, 각 수용가에서 사용하는 전기, 가스, 수도 등의 자원을 제공하는 사업을 수행하는 사업자의 메인 서버(10)는 TCP/IP(Transmission Control Protocol/Internet Protocol) 기반의 IP 네트워크(20) (예컨대, 광대역 중합 통신망, 광역 통신망, 인터넷, 구내정보 통신망 등 포함)을 통해 관리자 서버(30)와 고속 양방향 통신을 수행한다.

[0005] 각 수용가에는 사업자가 제공하는 자원의 사용량을 측정하기 위한 다수의 측정 디바이스들(60)이 설치되어 있다. 예를 들어, 측정 디바이스의 예로 각 수용가에서 사용된 전력량을 측정하는 전력 측정기(61), 각 수용가에서 사용된 가스의 사용량을 측정하는 가스 측정기(63), 각 수용가에서 사용된 수도의 사용량을 측정하는 수도 측정기(65)가 있다. 정보 수집기(50)는 전력 측정기(61), 가스 측정기(63), 수도 측정기(65)로부터 각 수용가에서 사용한 전기, 가스, 수도의 사용량에 대한 정보를 일정 주기로 수집하거나 관리자 서버(30)를 통해 메인 서버(10)로부터 수신한 측정 디바이스의 제어 명령을 전력 측정기(61), 가스 측정기(63) 및 수도 측정기(65)로 제공한다. 정보 수집기(50)와 다수의 측정 디바이스들(60)은 전력선을 통해 접속되어 있으며, 측정 디바이스(60)는 전력선을 통해 검침 정보를 정보 수집기(50)로 송신한다.

[0006] IP 네트워크에 접속되어 있으며 TCP/IP 프로토콜을 사용하는 관리자 서버(30)와 전력선 통신 프로토콜을 사용하는 정보 수집기(50)는 서로 다른 통신 프로토콜을 사용함으로 인하여, 관리자 서버(30)와 정보 수집기(50)는 직접 접속되어 정보를 송수신할 수 없으며 관리자 서버(30)와 정보 수집기(50) 사이에 PLC 게이트웨이(40)가 존재하여 관리자 서버(30)와 정보 수집기(50) 사이의 이종 프로토콜을 서로 변환시켜준다.

[0007] 관리자 서버(30)에 접속되어 있는 다수의 정보 수집기에서(본 발명에서는 설명의 편의를 위해 하나의 정보 수집기(50)만을 도시하고 있음) 수집한 검측 정보는 임시적으로 관리자 서버(30)의 데이터 저장부(도시되지 않음)에 저장되어 있다가 메인 서버(10)로부터 검침 정보에 대한 요청신호가 수신되는 경우 데이터 저장부에 저장된 검침 정보를 인출하여 IP 네트워크(20)를 통해 메인 서버(10)로 제공한다. 메인 서버(10)는 관리자 서버(30)로부터 수신한 각 수용가의 검측 정보에 기초하여 과금 정책을 수행한다.

[0008] 위에서 살펴본 검침 시스템에서 필요에 따라 측정 디바이스들 사이에서 데이터를 송수신하는 경우가 발생한다. 측정 디바이스들 사이에서 통신을 수행하고자 하는 경우 먼저 측정 디바이스들은 통신을 수행하고자 하는 상대

방 측정 디바이스가 안전한 측정 디바이스인지를 판단하기 위한 인증 절차를 수행하여야 한다.

[0009] 수용가에 설치되어 있는 다수의 측정 디바이스들 사이에서 수행되는 인증 절차를 설명하기 위한 도 2를 참고로 살펴보면, 수용가에는 다수의 측정 디바이스들(측정 디바이스 1 내지 측정 디바이스 4)이 설치되어 있으며, 측정 디바이스 1 내지 측정 디바이스 4는 전력선(110)을 통해 서로 접속되어 있다. 측정 디바이스 1 내지 측정 디바이스 4는 각각 전력선을 통해 데이터를 송수신한다.

[0010] 측정 디바이스 1 내지 측정 디바이스 4가 서로 데이터를 송수신하기 위하여, 먼저 측정 디바이스 1 내지 측정 디바이스 4는 상대방 측정 디바이스가 안전한 측정 디바이스인지 또는 등록된 측정 디바이스인지를 확인하여야 한다. 전력선(110) 통신을 수행하는 측정 디바이스 1 내지 측정 디바이스 4는 상대방 측정 디바이스를 인증하기 위한 별도의 인증 기관을 구비하지 않고 있으며, 측정 디바이스 1 내지 측정 디바이스 4가 자체적으로 상대방 측정 디바이스를 인증하여야 한다.

[0011] 측정 디바이스 1 내지 측정 디바이스 4가 자체적으로 상대방 측정 디바이스를 인증하기 위하여, 측정 디바이스 1 내지 측정 디바이스 4 각각에는 수용가(100)에 설치되어 있는 모든 측정 디바이스들에 대한 등록 정보를 구비하고 있어야 한다. 예를 들어, 측정 디바이스 1은 측정 디바이스 2 내지 측정 디바이스 4에 대한 등록 정보를 구비하고 있다. 측정 디바이스 1이 측정 디바이스 2와 통신을 수행하기 전에, 측정 디바이스 1은 측정 디바이스 2가 등록된 측정 디바이스인지를 확인하기 위하여 측정 디바이스 2가 송신한 등록 정보와 저장되어 있는 측정 디바이스 2의 등록 정보를 서로 비교한다. 비교 결과 측정 디바이스 2로부터 수신한 등록 정보와 저장된 측정 디바이스 2의 등록 정보가 동일한 경우, 측정 디바이스 2를 인증하여 통신을 수행한다.

발명의 내용

해결 하고자하는 과제

[0012] 통신을 수행하고자 하는 측정 디바이스들 사이에서 상대방 측정 디바이스를 인증하는 대표적인 방법으로 공개키 기반구조(Public Key Infrastructure, PKI)와 AKA(Authentication and Key Agreement) 방식이 있다.

[0013] 공개키 기반구조는 기본적으로 인증을 수행하는 인증 기관의 인증 서버와, 디바이스에 대한 정보를 이용하여 디바이스를 등록하는 등록 기관의 등록 서버를 구비하고 있으며 이들 인증 서버, 등록 서버 및 측정 디바이스들은 IP 네트워크에 서로 접속되어 있다. 인증 서버가 제1 디바이스로부터 제2 디바이스의 인증을 요청받는 경우, 인증 서버는 제2 디바이스가 가지고 있는 개인키와 등록 서버에 저장되어 있는 제2 디바이스의 공개키를 조회하여 제2 디바이스를 인증하게 된다.

[0014] 한편, AKA 방법은 제1 디바이스와 제2 디바이스 간 서로 같은 키를 공유하고 있다는 사실을 통해 상호 인증한다. 제1 디바이스는 자신의 식별자를 NAI(Network Access Identifier) 형식으로 제2 디바이스에 제공하며, 제2 디바이스는 제1 디바이스의 NAI에 맞는 Challenge 값을 제1 디바이스로 주고 제1 디바이스는 이에 대한 Response를 제2 디바이스로 보낸다. 제1 디바이스는 Challenge 정보를 이용해 계산된 값과 수신한 인증값의 비교를 통해 제2 디바이스를 인증하고, 제2 디바이스는 Response에 포함된 인증값과 직접 계산한 인증값을 비교해 제1 디바이스를 인증한다.

[0015] 위에서 설명한 인증 방법 중 공개키 기반구조는 인증 서버, 등록 서버를 요구하며 기본적으로 IP 네트워크를 기초로 한다는 점에서, IP 네트워크를 사용하지 않는 전력선 통신 네트워크에서는 그대로 사용할 수 없다는 문제점을 가진다. 또한, AKA 방법은 인증 절차를 수행하는 제1 디바이스와 제2 디바이스 사이에서 송수신되는 Challenge 데이터와 Response 데이터가 허락받지 않은 제3자에게 노출되는 경우 전력선 통신 네트워크 전체가 쉽게 해킹될 수 있다는 문제점을 가진다.

[0016] 따라서 본 발명은 종래 인증 방법이 가지는 문제점들을 해결하기 위한 것으로, 본 발명이 이루고자 하는 목적은 별도의 인증 서버나 등록 서버를 요구하지 않으며 전력선 통신 네트워크에서 사용할 수 있는 디바이스의 인증 방법을 제공하는 것이다.

[0017] 본 발명이 이루고자 하는 다른 목적은 2중의 인증 절차를 통해 허락받지 않은 제3자의 공격으로부터 자유로운 디바이스의 인증 방법을 제공하는 것이다.

과제 해결수단

[0018] 위에서 언급한 본 발명의 목적을 달성하기 위한 디바이스의 인증 방법은 (a) 관리자 서버에 저장된 다수의 측정

디바이스들의 시리얼 번호와 다수의 측정 디바이스들이 가지고 있는 시리얼 번호에 기초하여 관리자 서버와 다수의 측정 디바이스들 사이의 인증을 수행하는 단계(이하 (a) 단계)와, 관리자 서버에서 다수의 측정 디바이스들 각각에 대한 개인키와 공개키를 메인 서버로부터 수신하고 수신한 개인키와 공개키를 측정 디바이스로 송신하는 단계(이하 (b) 단계)와, 각 측정 디바이스의 공개키와 개인키를 이용하여 상대방 측정 디바이스를 인증하는 단계(이하 (c) 단계)를 포함한다.

[0019] 바람직하게, (a) 단계는 측정 디바이스에서 생성된 제1 난수와 측정 디바이스의 MAC 주소를 측정 디바이스로부터 관리자 서버로 송신하고, 제1 난수와 측정 디바이스의 MAC 주소에 기초하여 관리자 서버에서 생성된 관리자 서버의 검증값을 수신하여 측정 디바이스에서 상기 관리자 서버를 인증하는 단계 및 관리자 서버의 검증값과 측정 디바이스의 시리얼 번호로부터 생성된 측정 디바이스의 검증값을 측정 디바이스로부터 수신하여 관리자 서버에서 측정 디바이스를 인증하는 단계를 포함하며, 관리자 서버의 검증값과 측정 디바이스의 검증값은 각각 관리자 서버와 측정 디바이스에서 동일한 제1 해쉬 함수를 이용하여 생성되는 것을 특징으로 한다.

[0020] 바람직하게, (b) 단계는 관리자 서버에서 메인 서버로부터 다수의 측정 디바이스들에 할당할 개인키와 공개키를 수신하고 수신한 개인키와 공개키를 저장하는 단계와, 저장한 개인키를 각 측정 디바이스들에 할당하는 단계 및 다수의 측정 디바이스들 중 서로 인증하고자 하는 제1 측정 디바이스와 제2 측정 디바이스로부터 인증 요청 메시지를 수신하는 경우 제1 측정 디바이스와 제2 측정 디바이스에 각각 제2 측정 디바이스와 제1 측정 디바이스의 공개키를 송신하는 단계를 포함하는 것을 특징으로 한다.

[0021] 바람직하게, (c) 단계는 제1 측정 디바이스에서 제2 난수를 생성하고 생성한 제2 난수를 제2 측정 디바이스의 공개키로 암호화하여 제2 측정 디바이스로 송신하는 단계와, 제2 측정 디바이스에서 제3 난수를 생성하고 생성한 제3 난수를 제1 측정 디바이스의 공개키로 암호화하여 제1 측정 디바이스로 송신하는 단계와, 제1 측정 디바이스와 제2 측정 디바이스에서 각각 제2 난수와 제3 난수를 동일한 제2 해쉬 함수에 적용하여 인증 값을 계산하는 단계 및 제1 측정 디바이스에서 계산한 인증값과 제2 측정 디바이스에서 계산한 인증값이 서로 동일한지 여부로 제1 측정 디바이스와 제2 측정 디바이스를 인증하는 단계를 포함하는 것을 특징으로 한다.

효 과

[0022] 본 발명에 따른 디바이스의 인증 방법은 종래 인증 방법과 비교하여 다음과 같은 다양한 효과들을 가진다.

[0023] 첫째, 본 발명에 따른 디바이스의 인증 방법은 관리자 서버와 측정 디바이스 사이의 1차 인증과 측정 디바이스 사이의 2차 인증을 통해 전력선 통신 네트워크를 구성하는 측정 디바이스를 2중으로 인증함으로써, 정확하고 안전하게 측정 디바이스를 인증할 수 있다.

[0024] 둘째, 본 발명에 따른 측정 디바이스의 인증 방법은 메인 서버에서 할당받은 공개키와 개인키를 이용하여 측정 디바이스들이 직접 서로를 인증함으로써, 측정 디바이스의 인증 절차로 인하여 네트워크에 과부하가 발생하지 않도록 한다.

[0025] 셋째, 본 발명에 따른 측정 디바이스의 인증 방법은 별도의 인증 서버를 구비하지 않은 전력선 네트워크에서 측정 디바이스들이 직접 서로를 인증할 수 있다.

[0026] 넷째, 본 발명에 따른 측정 디바이스의 인증 방법은 메인 서버로부터 주기적으로 갱신되는 개인키와 공개키를 할당받아 측정 디바이스를 인증함으로써, 허락받지 않은 제3자의 해킹으로부터 안전하게 측정 디바이스를 인증할 수 있다.

발명의 실시를 위한 구체적인 내용

[0027] 도 3은 본 발명의 일 실시예에 따른, 전력선 통신 네트워크에서 측정 디바이스들을 인증하는 방법을 설명하는 흐름도이다.

[0028] 도 3을 참고로 보다 구체적으로 살펴보면, 관리자 서버와 다수의 측정 디바이스들 사이에서 인증 절차를 수행한다(S1). 측정 디바이스는 자신이 가지고 있는 시리얼 번호와 관리자 서버에 저장된 시리얼 번호에 기초하여 관리자 서버를 인증하며, 관리자 서버는 저장된 측정 디바이스의 시리얼 번호와 측정 디바이스로부터 수신한 시리얼 번호에 기초하여 측정 디바이스를 인증한다.

[0029] 관리자 서버와 다수의 측정 디바이스들 사이의 인증이 완료되면, 메인 서버는 인증을 완료한 다수의 측정 디바이스로 제공할 개인키와 공개키를 생성한다(S3). 관리자 서버는 메인 서버로부터 다수의 측정 디바이스들 각각에 대한 개인키와 공개키를 수신하고 수신한 개인키와 공개키를 다수의 측정 디바이스로 송신한다(S5). 관리자

서버는 메인 서버에서 생성된, 다수의 측정 디바이스들에 할당할 개인키와 공개키를 수신하고 수신한 개인키와 공개키를 관리자 서버의 저장부에 저장하며, 저장한 다수의 측정 디바이스들의 개인키를 각 측정 디바이스들로 송신한다. 한편, 다수의 측정 디바이스들 중 서로 통신을 수행하고자 하는 제1 측정 디바이스와 제2 측정 디바이스로부터 상대방 측정 디바이스의 인증 요청 메시지를 수신하는 경우, 제1 측정 디바이스와 제2 측정 디바이스로 각각 상대방 측정 디바이스의 공개키를 송신한다. 즉, 제1 측정 디바이스로 제2 측정 디바이스의 공개키를 송신하며, 제2 측정 디바이스로 제1 측정 디바이스의 공개키를 송신한다.

[0030] 바람직하게, 메인 서버는 일정 주기로 측정 디바이스에 할당할 새로운 개인키와 공개키를 생성하며, 새롭게 생성한 개인키와 공개키를 관리자 서버로 송신한다. 따라서 관리자 서버는 측정 디바이스에 할당할, 저장부에 저장되어 있는 개인키와 공개키를 일정 주기로 갱신한다.

[0031] 제1 측정 디바이스와 제2 측정 디바이스는 관리자 서버로부터 수신한 공개키와 개인키를 이용하여 상대방 측정 디바이스를 인증한다(S7).

[0032] 관리자 서버와 측정 디바이스 사이의 인증 방법을 설명하고 있는 도 4의 흐름도를 참고로 S1 단계를 보다 구체적으로 살펴보면, 측정 디바이스는 난수 발생기를 이용하여 제1 난수를 생성하고, 생성한 제1 난수와 측정 디바이스의 MAC 주소를 관리자 서버로 송신한다(S11). 관리자 서버는 측정 디바이스로부터 수신한 MAC 주소에 기초하여 측정 디바이스가 관리자 서버에 등록된 측정 디바이스인지를 판단하여 측정 디바이스를 1차 인증한다(S12). 관리자 서버에는 다수의 측정 디바이스의 MAC 주소와 MAC 주소에 매핑되어 있는 측정 디바이스의 시리얼 번호가 저장되어 있다. 1차 인증 결과 등록된 측정 디바이스로 판단되는 경우, 관리자 서버는 측정 디바이스로부터 수신한 제1 난수와 MAC 주소에 매핑되어 있는 시리얼 번호로부터 관리자 서버 검증값을 계산하고(S13), 계산한 관리자 서버의 검증값을 측정 디바이스로 송신한다(S14). 측정 디바이스는 제1 난수와 측정 디바이스가 가지고 있는 시리얼 번호로부터 인증값을 계산하고, 계산한 인증값과 관리자 서버로부터 수신한 관리자 서버의 검증값을 비교하여 관리자 서버를 인증한다(S15). 측정 디바이스에서 계산한 인증값과 관리자 서버로부터 수신한 검증값이 동일한 경우 관리자 서버를 정상적인 관리자 서버로 인증하며, 인증값과 검증값이 동일하지 않은 경우 관리자 서버의 인증을 거절한다.

[0033] 관리자 서버에서 제1 난수와 시리얼 번호로부터 계산되는 관리자 서버의 검증값과 측정 디바이스에서 제1 난수와 시리얼 번호로부터 계산되는 인증값은 동일한 무결성 검증 함수에 의해 계산된다. 예를 들어, 무결성 검증 함수에 제1 난수와 시리얼 번호의 합을 입력하여 계산되는 값을 검증값 또는 인증값으로 사용한다. 본 발명에서 무결성 검증 함수로 해쉬(Hash) 함수를 사용한다. 해쉬함수는 요약함수 또는 메시지 다이제스트 함수(message digest function)라고도 한다. 주어진 원문에서 고정된 길이의 의사난수를 생성하는 연산기법이다.

[0034] 측정 디바이스는 관리자 서버로부터 수신한 관리자 서버의 검증값과 측정 디바이스가 가지고 있는 시리얼 번호로부터 측정 디바이스의 검증값을 계산하고(S16), 계산한 측정 디바이스의 검증값을 관리자 서버로 송신한다(S17). 관리자 서버는 측정 디바이스로부터 수신한 검증값과 관리자 서버에서 계산한 측정 디바이스의 인증값을 비교하여 측정 디바이스를 인증한다(S18). 측정 디바이스의 검증값과 측정 디바이스의 인증값은 각각 관리자 서버의 인증값 또는 관리자 서버의 검증값과 측정 디바이스의 시리얼 번호의 합을 해쉬 함수에 입력하여 계산된다.

[0035] 측정 디바이스들 사이의 인증 방법을 설명하고 있는 도 5의 흐름도를 참고로 S7 단계를 보다 구체적으로 살펴보면, 다수의 측정 디바이스들 중 통신을 수행하고자 하는 제1 측정 디바이스와 제2 측정 디바이스는 각각 난수 발생기를 이용하여 제2 난수와 제3 난수를 생성한다(S21, S22). 제1 측정 디바이스는 관리자 서버로부터 수신한 제2 측정 디바이스의 공개키로 제2 난수를 암호화하여 제2 측정 디바이스로 송신하며(S23), 제2 측정 디바이스는 관리자 서버로부터 수신한 제1 측정 디바이스의 공개키로 제3 난수를 암호화하여 제2 측정 디바이스로 송신한다(S24). 제1 측정 디바이스는 제2 측정 디바이스로부터 수신한 제3 난수를 제1 측정 디바이스의 개인키로 복호화하고, 복호화한 제3 난수와 제2 난수로부터 제1 측정 디바이스의 검증값을 계산한다(S25). 이와 동일하게, 제2 측정 디바이스는 제1 측정 디바이스로부터 수신한 제2 난수를 제2 측정 디바이스의 개인키로 복호화하고, 복호화한 제2 난수와 제3 난수로부터 제2 측정 디바이스의 검증값을 계산한다(S26). 제1 측정 디바이스의 검증값과 제2 측정 디바이스의 검증값은 제2 난수와 제3 난수의 합을 해쉬 함수에 입력하여 계산된다. 바람직하게, S3 단계에서 관리자 서버와 측정 디바이스의 인증을 위해 사용되는 해쉬 함수와 S7 단계에서 측정 디바이스들 사이의 인증을 위해 사용되는 해쉬 함수는 서로 상이한 것을 특징으로 한다.

[0036] 제1 측정 디바이스는 계산한 제1 측정 디바이스의 검증값을 제2 측정 디바이스로 송신하며(S27), 제2 측정 디바이

이스는 계산한 제2 측정 디바이스의 검증값을 제1 측정 디바이스로 송신한다(S28). 제1 측정 디바이스는 제2 난수와 제3 난수로부터 제2 측정 디바이스의 인증값을 계산하고 계산한 인증값과 제2 측정 디바이스로부터 수신한 제2 측정 디바이스의 검증값을 비교하여 제2 측정 디바이스를 인증한다(S29). 이와 동일하게, 제2 측정 디바이스는 제2 난수와 제3 난수로부터 제1 측정 디바이스의 인증값을 계산하고 계산한 인증값과 제1 측정 디바이스로부터 수신한 제1 측정 디바이스의 검증값을 비교하여 제1 측정 디바이스를 인증한다(S30).

[0037] 한편, 상술한 본 발명의 일 실시예들은 컴퓨터에서 실행될 수 있는 프로그램으로 작성 가능하고, 컴퓨터로 읽을 수 있는 기록 매체를 이용하여 상기 프로그램을 동작시키는 범용 디지털 컴퓨터에서 구현될 수 있다.

[0038] 상기 컴퓨터로 읽을 수 있는 기록 매체는 마그네틱 저장 매체(예를 들어, 롬, 플로피 디스크, 하드 디스크 등), 광학적 판독 매체(예를 들어, 시디롬, 디브이디 등) 및 캐리어 웨이브(예를 들어, 인터넷을 통한 전송)와 같은 저장 매체를 포함한다.

[0039] 본 발명은 도면에 도시된 실시예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야에서 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 특허청구범위의 기술적 사상에 의해 정해져야 할 것이다.

[0040]

도면의 간단한 설명

[0041] 도 1은 종래 전력선 통신을 이용하여 수용가의 전기, 가스, 수도의 사용량을 검침하는 시스템을 설명하기 위한 도면이다.

[0042] 도 2는 수용가에 설치되어 있는 다수의 측정 디바이스들 사이에서 수행되는 인증 절차를 설명하기 위한 도면이다.

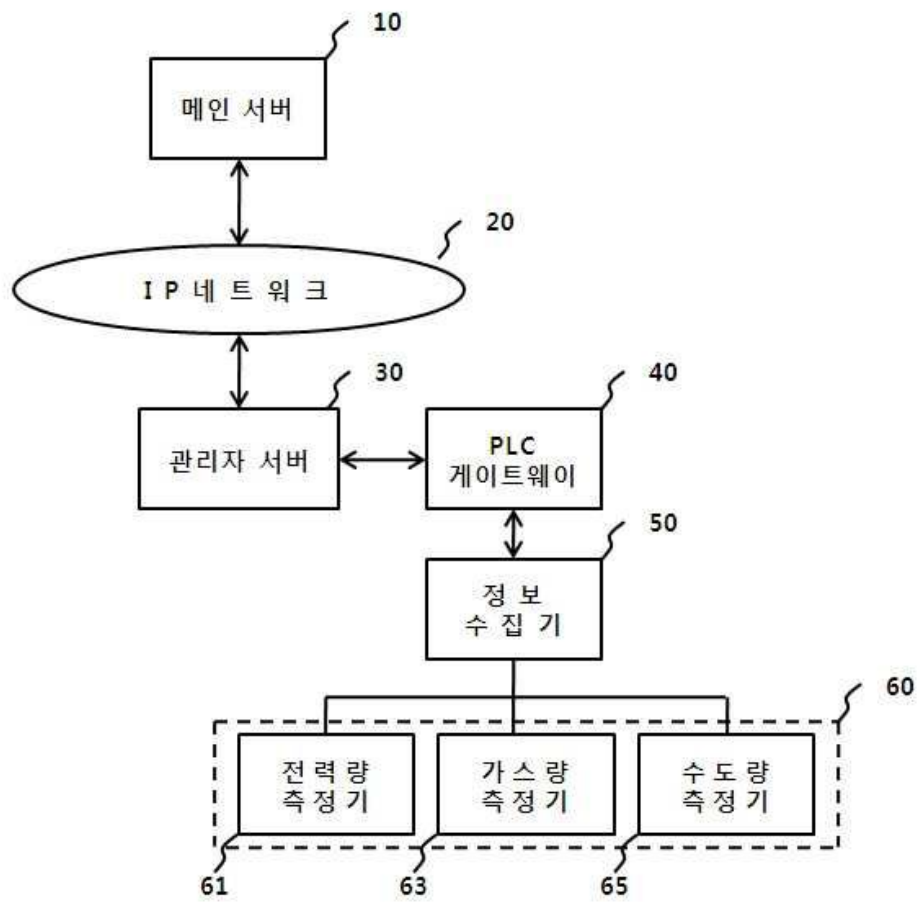
[0043] 도 3은 본 발명의 일 실시예에 따른, 전력선 통신 네트워크에서 측정 디바이스들을 인증하는 방법을 설명하는 흐름도이다.

[0044] 도 4는 관리자 서버와 측정 디바이스 사이의 인증 방법을 보다 구체적으로 설명하고 있는 흐름도이다.

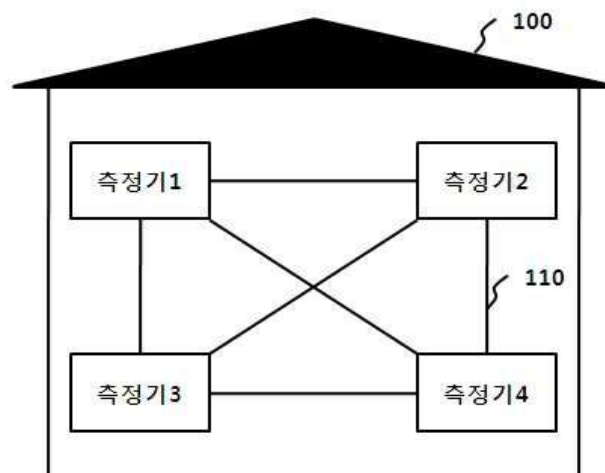
[0045] 도 5는 측정 디바이스들 사이의 인증 방법을 보다 구체적으로 설명하고 있는 흐름도이다.

도면

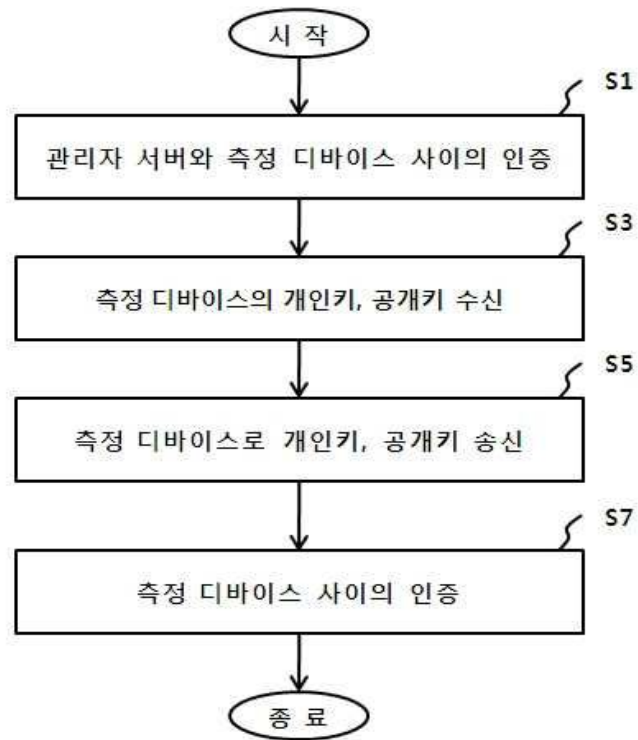
도면1



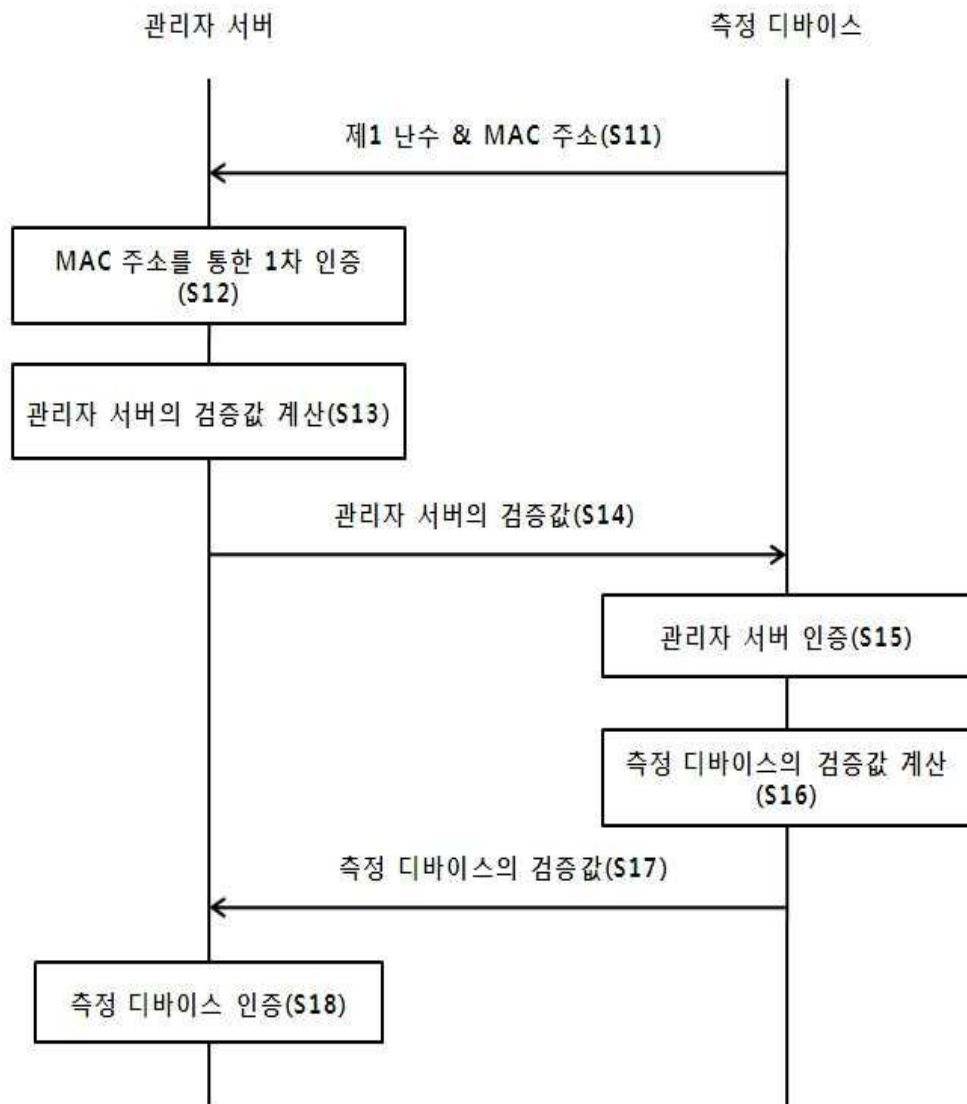
도면2



도면3



도면4



도면5

