



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2010-0026114
(43) 공개일자 2010년03월10일

(51) Int. Cl.

H04L 9/32 (2006.01)

(21) 출원번호 10-2008-0084986

(22) 출원일자 2008년08월29일

심사청구일자 2008년08월29일

(71) 출원인

경희대학교 산학협력단

경기도 용인시 기흥구 서천동 1 경희대학교 국제 캠퍼스내

(72) 발명자

홍충선

경기 용인시 수지구 상현동 성원3차상떼빌아파트 233-101

허준

경기도 군포시 궁내동 우륵주공아파트 711-1601

조웅준

경기도 수원시 영통구 영통1동 1029-12번지 103호

(74) 대리인

서재승

전체 청구항 수 : 총 5 항

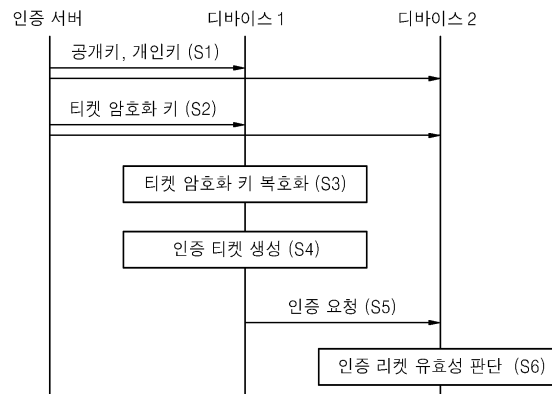
(54) 디바이스의 인증 방법

(57) 요약

본 발명은 디바이스의 인증 방법에 관한 것으로, 보다 구체적으로 인증 서버에 등록된 디바이스에게만 제공되는 티켓 암호화 키로 암호화된 인증 티켓을 이용하여 인증 서버의 중계없이 디바이스가 직접 상대방 디바이스를 인증할 수 있는 디바이스의 인증 방법에 관한 것이다.

본 발명에 따른 디바이스의 인증 방법은 디바이스에서 생성하는 인증 티켓을 이용하여 상대방 디바이스를 인증함으로써, 사용자를 통해 입력되는 디바이스의 인증 정보없이도 디바이스를 인증할 수 있다. 또한, 본 발명에 따른 디바이스의 인증 방법은 일정 유효 상태에서에서만 사용되는 유효 티켓 암호화 키를 이용하여 상대방 디바이스를 인증함으로써, 안전하게 디바이스를 인증할 수 있다.

대표도 - 도4



특허청구의 범위

청구항 1

인증 서버와 다수의 디바이스들로 구성된 네트워크에서 상기 디바이스를 인증하는 방법에 있어서,

- (a) 상기 인증 서버로부터 상기 다수의 디바이스들 중 제1 디바이스의 공개키(K_A)와 개인키(K_A^{-1})를 수신하는 단계;
- (b) 상기 인증 서버로부터 상기 제1 디바이스의 공개키로 암호화된 티켓 암호화 키를 수신하는 단계;
- (c) 상기 수신한 티켓 암호화 키를 상기 제1 디바이스의 개인키로 복호화하고, 상기 복호화한 티켓 암호화 키로 암호화된 상기 제1 디바이스의 인증 티켓을 생성하는 단계; 및
- (d) 상기 생성한 상기 제1 디바이스의 인증 티켓을 상기 다수의 디바이스들 중 제2 디바이스로 송신하여 상기 제1 디바이스의 인증을 요청하는 단계를 포함하는 디바이스의 인증 방법.

청구항 2

제 1 항에 있어서, 상기 디바이스의 인증 방법은

상기 제1 디바이스의 공개키로 암호화된 현재 유효 상태, 남아 있는 유효 기간을 수신하는 단계를 더 포함하며,

상기 티켓 암호화 키는 상기 수신한 현재 유효 상태에서만 유효하게 사용되는 것을 특징으로 하는 디바이스의 인증 방법.

청구항 3

제 2 항에 있어서, 상기 인증 티켓은

상기 인증 서버에 대한 정보, 상기 디바이스 1에 대한 정보 및 상기 현재 유효상태에 대한 정보를 포함하는 것을 특징으로 하는 디바이스의 인증 방법.

청구항 4

제 3 항에 있어서, 상기 티켓 암호화 키는

상기 인증 서버에서 난수 생성 함수에 의해 난수로 생성되는 것을 특징으로 하는 디바이스의 인증 방법.

청구항 5

인증 서버와 다수의 디바이스들로 구성된 네트워크에서 상기 디바이스를 인증하는 방법에 있어서,

- (a) 유효 상태 동안만 사용되는 티켓 암호화 키를 생성하고 상기 생성한 티켓 암호화 키를 상기 디바이스로 송신하는 단계;
- (b) 상기 디바이스에서 상기 인증 서버로부터 수신한 상기 티켓 암호화 키로 암호화된 디바이스의 인증 티켓을 생성하는 단계;
- (c) 상기 생성한 인증 티켓을 서로 인증 요청하는 상대방 디바이스로 각각 송신하는 단계; 및
- (d) 상기 수신한 상대방의 인증 티켓을 상기 티켓 암호화 키로 복호화하고 상기 복호화된 인증 티켓의 유효성을 판단하여 상기 상대방 디바이스를 인증하는 단계를 포함하는 것을 특징으로 하는 디바이스의 인증 방법.

명세서

발명의 상세한 설명

기술 분야

본 발명은 디바이스의 인증 방법에 관한 것으로, 보다 구체적으로 인증 서버에 등록된 디바이스에게만 제공되

는 티켓 암호화 키로 암호화된 인증 티켓을 이용하여 인증 서버의 중계없이 디바이스가 직접 상대방 디바이스를 인증할 수 있는 디바이스의 인증 방법에 관한 것이다.

배경 기술

- [0002] 최근 들어, 센서 네트워크, 전력선 통신 네트워크, 무선 메쉬 네트워크 등 데이터 전달 매체의 특징과 사용자 환경을 고려한 새로운 네트워크 기술들이 개발되고 있으며, 이들 새로운 네트워크 기술을 상용화하기 위한 노력들이 진행되고 있다. 새롭게 개발된 네트워크에서도 네트워크의 확장에 따른 관리 개체의 증가에도 효율적으로 디바이스를 관리할 수 있으며 안전한 통신망 구축을 위하여 필수적인 보안키 관리 매커니즘의 개발이 요구된다.
- [0003] 도 1은 종래 전력선 통신을 이용하여 수용가의 사용 전력량을 검침하는 시스템에서 각 수용가에 설치되는 검침 디바이스의 인증을 위한 검침 디바이스의 등록 과정을 설명하기 위한 도면이다.
- [0004] 도 1을 참고로 살펴보면, 전력 사업자 서버(10)는 TCP/IP(Transmission Control Protocol/Internet Protocol)를 기반으로 네트워크(20)(예컨대, 광대역 중합 통신망, 광역 통신망, 인터넷, 구내정보 통신망 등 포함)을 통해 검침 제어부(30)와 고속 양방향 통신을 수행한다. 전력 사업자 서버(10)는 네트워크(20)를 통해 검침 제어부(30)로부터 각 수용가(40-1, 40-2, ..., 40-n)의 전력 검침량을 실시간으로 제공받는다. 여기서, 전력 검침량이라 함은 각 수용가(40-1, 40-2, ..., 40-n)에서 사용하는 사용 전력량을 말한다. 전력 사업자 서버(10)는 검침 제어부(30)로부터 제공된 전력 검침량을 기초로 각 수용가(40-1, 40-2, ..., 40-n)의 전력 사용 요금을 책정하여 부과하게 된다. 여기서, 전력 검침량으로는 검침 제어부(30)에 할당된 모든 수용가(40-1, 40-2, ..., 40-n)의 월별, 주간별, 야간별, 날짜별, 시간대별 사용 전력량의 총합, 각 수용가(40-1, 40-2, ..., 40-n)의 월별, 주간별, 야간별, 날짜별, 시간대별 사용 전력량 및 순시 전력량 등이 될 수 있다.
- [0005] 검침 제어부(30)는 각 수용가(40-1, 40-2, ..., 40-n)에 각각 하나씩 설치된 검침 디바이스로부터 전력선(45)을 통해 고속 전력선 통신을 수행한다. 검침 제어부(30)는 전력선(45)을 통해 각 수용가(40-1, 40-2, ..., 40-n)에 설치된 검침 디바이스로부터 검침 데이터를 전송받아 네트워크(20)를 통해 전력 사업자 서버(10)로 제공한다.
- [0006] 이때, 검침 제어부(30)는 각 수용가(40-1, 40-2, ..., 40-n)의 검침 디바이스로부터 전송된 검침 데이터를 임시적으로 데이터 저장부(도시되지 않음)에 저장하고 있다가 전력 사업자 서버(10)로부터 검침 데이터에 대한 요청 신호가 수신되는 경우 데이터 저장부에 저장된 검침 데이터를 인출하여 네트워크(20)를 통해 전력 사업자 서버(10)로 제공한다.
- [0007] 전력 사업자 서버(10)는 각 수용가(40-1, 40-2, ..., 40-n)에 설치되어 있는 검침 디바이스로부터 수신한 검침 데이터에 기초하여 각 수용가(40-1, 40-2, ..., 40-n)에 과금을 하기 위하여, 먼저 각 수용가(40-1, 40-2, ..., 40-n)에 등록되어 있는 검침 디바이스를 전력 사업자 서버(10)에 등록하여야 한다. 검침 디바이스를 전력 사업자 서버(10)에 등록하기 위하여 검침 디바이스의 설치 기사는 직접 각 수용가(40-1, 40-2, ..., 40-n)를 방문하고 각 수용가(40-1, 40-2, ..., 40-n)에 설치되는 검침 디바이스의 물리적 주소, 식별 정보 등을 직접 전력 사업자 서버(10)에 등록하여야 한다.
- [0008] 도 2는 다수의 디바이스를 구비하는 통신 네트워크에서 디바이스 간의 인증 시스템을 설명하기 위한 기능 블록도이다.
- [0009] 도 2를 참고로 살펴보면, 서로 데이터 통신을 수행하고자 하는 다수의 디바이스들(51, 52, 53)이 통신 네트워크(60), 예를 들어 센서 네트워크, 전력선 통신 네트워크, 무선 메쉬 네트워크에 접속되어 있다. 또한 등록 기관의 등록 서버(70)와 인증 기관의 인증 서버(80)도 통신 네트워크(60)에 접속되어 있다. 다수의 디바이스들(51, 52, 53)은 등록 서버(70)에 등록되어 있다.
- [0010] 디바이스 1(51)이 디바이스 2(52)와 데이터 통신을 수행하기 위하여, 먼저 디바이스 1(51)과 디바이스 2(52)는 서로 상대방 디바이스가 정당한 디바이스인지 인증하여야 한다.
- [0011] 디바이스 1(51)과 디바이스 2(52)의 인증 과정을 보다 구체적으로 살펴보면, 디바이스 1(51)은 통신 네트워크(60)를 통해 인증 기관(80)에 디바이스 2(52)의 인증을 요청한다. 인증 서버(80)는 디바이스 1(51)의 인증 요청에 따라 등록 서버(70)에 저장되어 있는 디바이스 2(52)의 등록 정보에 기초하여 디바이스 2(52)를 인증한다. 이와 동일하게 디바이스 2(52)로부터 디바이스 1(51)의 인증 요청이 있으면, 인증 서버(80)는 디바이스 2(52)의 인증 요청에 따라 등록 서버(70)에 저장되어 있는 디바이스 1(51)의 등록 정보에 기초하여 디바이스 1(51)을 인증한다.

발명의 내용

해결 하고자하는 과제

- [0012] 위에서 설명한 종래 디바이스의 등록 방법은 통신 네트워크에 구성되어 있는 디바이스를 등록하기 위하여 디바이스의 설치 기사가 각 디바이스의 물리적 주소 또는 식별 정보 등을 개별적으로 인증 서버에 등록하여야 하는 불편함이 있다.
- [0013] 또한 종래 디바이스의 인증 시스템은 통신 네트워크를 구성하는 디바이스들 사이에서 데이터 통신을 하기 위하여 접속을 시도하는 경우, 반드시 인증 서버를 통해서 등록 서버에 등록되어 있는 디바이스의 등록 정보를 이용하여 상대방 디바이스를 인증하여야 한다. 따라서 종래 디바이스의 인증 시스템은 디바이스의 인증 절차로 인하여 통신 네트워크에 오버헤드가 발생할 수 있다는 문제점과 디바이스의 인증 절차 과정에서 디바이스의 인증 정보가 허락받지 않은 제3자에 해킹될 수 있다는 문제점을 가진다.
- [0014] 본 발명은 종래 디바이스의 등록 방법과 종래 디바이스의 인증 시스템이 가지는 문제점들을 해결하기 위한 것으로, 본 발명이 이루고자 하는 과제는 디바이스 설치자의 입력 정보에 근거하지 않고 디바이스들 사이에서 스스로 상대방 디바이스를 안전하게 인증할 수 있는 방법을 제공한다.
- [0015] 본 발명이 이루고자 하는 다른 과제는 별도의 인증 서버의 도움없이도 통신을 수행하고자 하는 상대방 디바이스를 인증할 수 있는 방법을 제공하는 것이다.
- [0016] 본 발명이 이루고자 하는 또 다른 과제는 유효 상태에 기초하여 유효 상태 동안에만 사용할 수 있는 티켓 암호화 키를 이용하여 안전하게 상대방 디바이스를 인증할 수 있는 방법을 제공하는 것이다.
- [0017] 본 발명이 이루고자 하는 또 다른 과제는 유효 상태 동안에만 사용할 수 있는 티켓 암호화 키를 이용하여 사용 기간을 가지는 서비스에서 사용 기간이 만료된 디바이스의 접속을 간편하게 제한할 수 있는 디바이스의 인증 방법을 제공하는 것이다.

과제 해결수단

- [0018] 위에서 설명한 본 발명의 목적을 달성하기 위한 디바이스의 인증 방법은 공개키 발생 장치로부터 다수의 디바이스들 중 제1 디바이스의 공개키(K_A)와 개인키(K_A^{-1})를 수신하는 단계와, 공개키 발생 장치로부터 제1 디바이스의 공개키로 암호화된 티켓 암호화 키를 수신하는 단계와, 수신한 티켓 암호화 키를 제1 디바이스의 개인키로 복호화하고 복호화한 티켓 암호화 키를 이용하여 제1 디바이스의 인증 티켓을 생성하는 단계와, 생성한 제1 디바이스의 인증 티켓을 다수의 디바이스들 중 제2 디바이스로 송신하여 제1 디바이스의 인증을 요청하는 단계를 포함하는 것을 특징으로 한다.
- [0019] 바람직하게, 본 발명에 따른 디바이스의 인증 방법은 제1 디바이스의 공개키로 암호화된 현재 유효 상태, 남아 있는 유효 기간을 수신하는 단계를 더 포함하며, 티켓 암호화 키는 수신한 현재 유효 상태에서부터 유효하게 사용될 수 있는 것을 특징으로 한다.
- [0020] 본 발명의 목적을 달성하기 위한 디바이스의 인증 방법은 유효 상태 동안만 사용되는 티켓 암호화 키를 생성하고 생성한 티켓 암호화 키를 디바이스로 송신하는 단계와, 디바이스에서 공개키 발생 장치로부터 수신한 상기 티켓 암호화 키로 암호화된 디바이스의 인증 티켓을 생성하는 단계와, 생성한 인증 티켓을 서로 인증 요청하는 상대방 디바이스로 각각 송신하는 단계 및 수신한 상대방의 인증 티켓을 티켓 암호화 키로 복호화하고 복호화된 인증 티켓의 유효성을 판단하여 상대방 디바이스를 인증하는 단계를 포함하는 것을 특징으로 한다.

효 과

- [0021] 본 발명에 따른 디바이스의 인증 방법은 종래 디바이스의 인증 방법에 비해 다음과 같은 다양한 효과들을 가진다.
- [0022] 첫째, 본 발명에 따른 디바이스의 인증 방법은 각 디바이스가 저장하고 있는 티켓 암호화 키로 상대방 디바이스를 인증함으로써, 인증 서버의 인증 절차를 없애 통신 네트워크에 과부하를 발생시키지 않으며 상대방 디바이스를 간단하게 인증할 수 있다.
- [0023] 둘째, 본 발명에 따른 디바이스의 인증 방법은 디바이스에서 생성하는 인증 티켓을 이용하여 상대방 디바이스를

인증함으로써, 사용자를 통해 입력되는 디바이스의 인증 정보없이도 디바이스를 인증할 수 있다.

[0024] 셋째, 본 발명에 따른 디바이스의 인증 방법은 일정 유효 상태에서에서만 사용되는 유효 티켓 암호화 키를 이용하여 상대방 디바이스를 인증함으로써, 안전하게 디바이스를 인증할 수 있다.

[0025] 넷째, 본 발명에 따른 디바이스의 인증 방법은 일정 유효 상태에서에서만 사용되는 유효 티켓 암호화 키를 이용하여 디바이스를 인증함으로써, 사용 기간을 가진 서비스에서 기간이 종료한 디바이스의 통신 네트워크 접속을 간단하게 차단할 수 있다.

발명의 실시를 위한 구체적인 내용

[0026] 이하 첨부한 도면을 참고로 본 발명에 따른 보안키 생성 방법에 대해 보다 구체적으로 살펴본다.

[0027] 도 3은 본 발명의 일 실시예에 따른 디바이스 인증 시스템(100)을 설명하기 위한 기능 블록도이다.

[0028] 도 3을 참고로 살펴보면, 다수의 디바이스들(121, 122, 123)들이 통신 네트워크(130)를 통해 인증 서버(110)에 접속되어 있다. 인증 서버(110)는 디바이스들(121, 122, 123)의 공개키와 개인키를 생성하여 각 디바이스(121, 122, 123)로 제공한다. 즉, 인증 서버(110)은 공개키 발생 장치의 역할을 수행한다. 또한 인증 서버(110)는 일정한 또는 유효 상태에서에서만 사용되는 티켓 암호화 키를 생성하여 각 디바이스(121, 122, 123)로 제공한다.

[0029] 각 디바이스(121, 122, 123)는 인증 티켓을 생성하여 통신하고자 하는 상대방 디바이스로 인증 티켓을 송신한다. 인증 티켓은 티켓 암호화 키로 암호화되어 있으며, 인증 티켓을 수신한 상대방 디바이스는 인증 티켓을 티켓 암호화 키로 복호화 가능한지 여부로 인증 티켓의 유효성을 판단하여 상대방 디바이스를 인증한다.

[0030] 즉, 각 디바이스(121, 122, 123)은 통신하고자 하는 상대방 디바이스로부터 직접 인증 티켓을 수신하고 수신한 인증 티켓의 유효성을 판단하여 상대방 디바이스를 인증함으로써, 인증 서버(110)의 중개없이도 상대방 디바이스를 인증할 수 있다.

[0031] 도 4는 본 발명의 일 실시예에 따른 디바이스의 인증 방법을 설명하는 흐름도이다.

[0032] 도 4를 참고로 보다 구체적으로 살펴보면, 디바이스1 또는 디바이스 2로부터 공개키와 개인키의 요청이 있는 경우 인증 서버는 안전한 채널 또는 임시키로 암호화된 디바이스 1 또는 디바이스 2의 공개키와 개인키를 안전하지 않은 채널을 통해 디바이스 1, 디바이스 2로 각각 송신한다(S1). 여기서 안전한 통신 채널이란 허가받지 못한 제3자가 인증 서버와 디바이스 사이의 통신 채널에 접속하지 못하도록 보안된 채널을 의미하며, 유선의 통신 채널 또는 초기에 인증화 단계를 통해 접속되어 있는 통신 채널이 안전한 통신 채널의 일 예이다. 한편 안전하지 않은 통신 채널에서는 인증 서버와 디바이스 1 또는 인증 서버와 디바이스 2만 알고 있는 임시키로 암호화된 디바이스 1 또는 디바이스 2의 공개키와 개인키를 각각 디바이스 1과 디바이스 2로 송신한다.

[0033] 인증 서버는 송신한 디바이스 1의 공개키로 암호화된 티켓 암호화 키를 디바이스 1로 송신하며 송신한 디바이스 2의 공개키로 암호화된 티켓 암호화 키를 디바이스 2로 송신한다(S2).

[0034] 디바이스 1은 수신한 티켓 암호화 키를 디바이스 1의 개인키로 복호화하고(S3), 복호화한 티켓 암호화 키로 암호화된 인증 티켓을 생성한다(S4). 디바이스 1에서 생성한 인증 티켓의 포맷에 대한 일 예를 도시하고 있는 도 9를 참고로 살펴보면, 인증 티켓에는 티켓 암호화 키를 발행한 인증 서버의 식별 정보와 디바이스 1의 식별 정보가 포함되어 있다.

[0035] 디바이스 1은 통신을 수행하고자 하는 디바이스 2로 생성한 인증 티켓을 송신하여 디바이스 1의 인증을 요청한다(S5). 디바이스 2는 디바이스 1로부터 수신한 인증 티켓을 수신한 티켓 암호화 키로 복호화하여 디바이스 1로부터 수신한 인증 티켓의 유효성을 판단함으로써 디바이스 1을 인증한다(S6). 이와 동일하게 디바이스 2는 수신한 티켓 암호화 키로 암호화된 인증 티켓을 생성하고, 생성한 인증 티켓을 디바이스 1로 송신한다. 디바이스 1은 디바이스 2로부터 수신한 인증 티켓을 티켓 암호화 키로 복호화하여 디바이스 2로부터 수신한 인증 티켓의 유효성을 판단함으로써 디바이스 2를 인증한다.

[0036] 도 5는 본 발명의 일 실시예에 따른 디바이스 인증 방법에 따라 다수의 이중 네트워크로 구성된 통신 네트워크에서 디바이스를 인증하는 방법을 설명하는 도면이다.

[0037] 도 5를 참고로 살펴보면, 인증 서버(200)에 다수의 이중 네트워크들(210, 220, 230, 240)이 접속되어 있다. 각 이중 네트워크는 서로 분리되어 있으며, 각 이중 네트워크에 속한 디바이스들은 자신이 속한 네트워크의 상대방 디바이스와 통신을 수행한다.

- [0038] 인증 서버(200)는 각 이종 네트워크(210, 220, 230, 240)에 서로 다른 티켓 암호화 키를 송신한다. 바람직하게, 인증 서버(200)는 각 이종 네트워크(210, 220, 230, 240)에서 사용하는 난수 발생 함수의 종류에 따라 서로 다른 길이의 티켓 암호화 키를 생성한다. 따라서 네트워크 1(210)에 속한 디바이스들은 네트워크 1(210)에 할당된 티켓 암호화 키를 공유하며, 네트워크 1(210)에 속한 상대방 디바이스로부터 수신한 인증 티켓을 네트워크 1(210)에 할당된 티켓 암호화 키로 복호화하여 상대방 디바이스를 인증할 수 있다.
- [0039] 한편, 네트워크 4(240)에 속하지 않은, 허락받지 않은 외부 디바이스(250)는 네트워크 4(240)에 할당된 티켓 암호화 키를 알지 못한다. 따라서, 외부 디바이스(250)가 네트워크 4(240)에 속한 디바이스와 통신을 위하여 네트워크 4(240)에 속한 디바이스로 인증을 요구하는 경우 외부 디바이스(250)로부터 수신한 인증 티켓은 네트워크 4(240)에 할당된 티켓 암호화 키로 복호화되어 있지 않기 때문에, 외부 디바이스(250)로부터 수신한 인증 티켓의 유효성은 부정된다. 따라서 외부 디바이스(250)는 네트워크 4(240)에 접속될 수 없다.
- [0040] 도 6은 본 발명의 다른 실시예에 따른 디바이스의 인증 방법을 설명하는 흐름도이다.
- [0041] 도 6은 공개키 발생 장치와 디바이스 1에서 디바이스 1의 공개키와 개인키를 생성하는 과정을 설명하기 위한 흐름도이다.
- [0042] 도 6을 참고로 보다 구체적으로 살펴보면, 디바이스1 또는 디바이스 2로부터 공개키와 개인키의 요청이 있는 경우 인증 서버는 안전한 채널 또는 임시키로 암호화된 디바이스 1 또는 디바이스 2의 공개키와 개인키를 안전하지 않은 채널을 통해 디바이스 1, 디바이스 2로 각각 송신한다(S11). 또한 인증 서버는 디바이스 1의 공개키로 암호화된 티켓 암호화 키와 디바이스 2의 공개키로 암호화된 티켓 암호화 키를 현재 유효 상태 및 남아 있는 유효 기간에 대한 정보와 함께 각각 디바이스 1과 디바이스 2로 송신한다(S12, S13). 인증 서버에서 디바이스 1과 디바이스 2로 송신하는 티켓 암호화 키는 유효 상태에서에서만 유효하게 사용할 수 있는 암호화 키이다.
- [0043] 디바이스 1은 수신한 티켓 암호화 키를 디바이스 1의 개인키로 복호화하고(S14), 복호화된 티켓 암호화 키로 암호화된 인증 티켓을 생성한다(S15). 디바이스 1에서 생성한 인증 티켓의 포맷에 대한 일 예를 도시하고 있는 도 9를 참고로 살펴보면, 인증 티켓에는 티켓 암호화 키를 발행한 인증 서버의 식별 정보, 디바이스 1의 식별 정보 및 현재 유효 상태에 대한 정보가 포함되어 있다.
- [0044] 디바이스 1은 통신을 수행하고자 하는 디바이스 2로 생성한 인증 티켓을 송신하여 디바이스 1의 인증을 요청한다(S16). 디바이스 2는 디바이스 1로부터 수신한 인증 티켓을 수신한 티켓 암호화 키로 복호화하여 디바이스 1로부터 수신한 인증 티켓의 유효성을 판단함으로써 디바이스 1을 인증한다(S17).
- [0045] 도 7은 유효 상태를 설명하기 위한 도면이다.
- [0046] 티켓 암호화 키는 허락받지 않은 제3자에 의해 해킹 가능성 있다. 따라서 디바이스가 항상 일정한 티켓 암호화 키로 암호화된 인증 티켓을 이용하여 상대방 디바이스를 인증하는 경우, 허락받지 않은 제3자가 해킹한 티켓 암호화 키를 이용하여 네트워크에 접속할 수 있으며 이는 통신 시스템에 심각한 위협 요소로 작용할 수 있다. 따라서 인증 서버는 단위 시간별로 구분된 현재 유효 상태에서에서만 유효하게 사용할 수 있는 티켓 암호화 키를 생성하고 생성한 티켓 암호화 키를 유효 상태에 대한 정보 및 남아 있는 유효 기간에 대한 정보와 함께 인증 서버에 접속되어 있는 디바이스로 송신한다.
- [0047] 도 7을 참고로 유효 상태에 대해 보다 구체적으로 살펴보면, 인증 서버는 단위 시간별로 구분된 유효 상태($\dots, i-1, i, i+1, \dots$)별로 유효하게 사용할 수 있는 티켓 암호화 키를 상이하게 생성하고, 티켓 암호화 키를 생성할 때의 시점에서 지나간 유효 기간(T_c)를 빼서 남은 유효 기간(v)을 계산한다.
- [0048] 도 8은 본 발명의 다른 실시예에 따른 디바이스 인증 방법의 사용 예를 설명하기 위한 도면이다.
- [0049] 도 8을 참고로 살펴보면, 인증 서버(300)가 통신 네트워크(310)에 접속되어 있으며, 통신 네트워크(310)는 서로 데이터를 송수신하는 다수의 디바이스들이 포함되어 있다.
- [0050] 인증 서버(300)는 유효 상태별로 사용할 티켓 암호화 키를 통신 네트워크(310)에 존재하는 다수의 디바이스들에게 송신한다. 여기서 인증 서버(300)가 사용 기간을 정해 서비스를 제공하고, 제공한 서비스에 대해 과금하는 서비스 업체의 인증 서버(300)인 경우, 인증 서버(300)는 과금 정보에 기초하여 사용 중인 디바이스(312)에게만 유효 상태별로 티켓 암호화 키를 제공하며, 사용 기간이 종료된 디바이스(314)에게는 유효 상태별로 제공되는 티켓 암호화 키를 제공하지 않는다. 따라서 서비스 업체는 유효 상태별 티켓 암호화 키를 이용하여 손쉽게 과금 서비스를 수행할 수 있다.

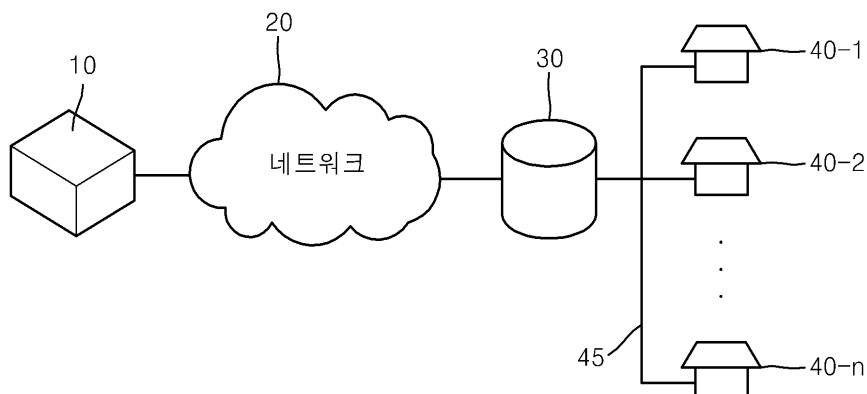
- [0051] 또한, 등록하지 않은 외부 디바이스(316)가 통신 네트워크(310)에 불법으로 접속하려고 하는 경우, 인증 서버(300)는 단위 유효 상태별로 서로 상이한 티켓 암호화 키를 등록된 디바이스로 제공하기 때문에 외부 디바이스(316)의 불법 접속을 보다 완벽하게 차단할 수 있다.
- [0052] 한편, 상술한 본 발명의 일 실시예들은 컴퓨터에서 실행될 수 있는 프로그램으로 작성 가능하고, 컴퓨터로 읽을 수 있는 기록 매체를 이용하여 상기 프로그램을 동작시키는 범용 디지털 컴퓨터에서 구현될 수 있다.
- [0053] 상기 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.
- [0054] 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.

도면의 간단한 설명

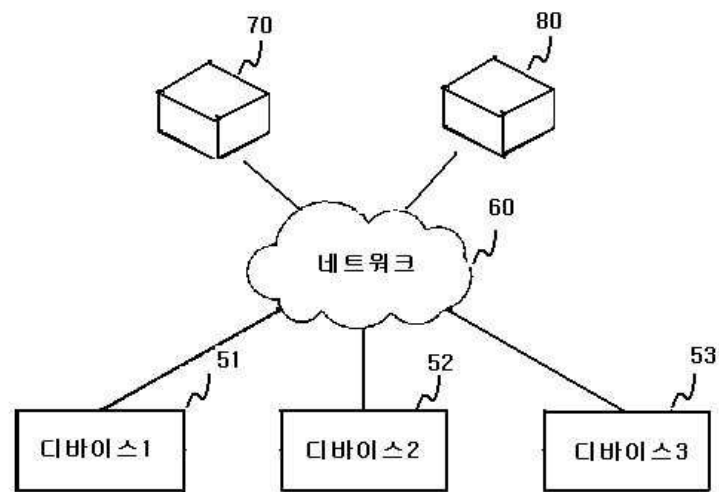
- [0055] 도 1은 종래 전력선 통신을 이용하여 수용가의 사용 전력량을 검침하는 시스템에서 각 수용가에 설치되는 검침 디바이스의 인증을 위한 검침 디바이스의 등록 과정을 설명하기 위한 도면이다.
- [0056] 도 2는 다수의 디바이스를 구비하는 통신 네트워크에서 디바이스 간의 인증 시스템을 설명하기 위한 기능 블록도이다.
- [0057] 도 3은 본 발명의 일 실시예에 따른 디바이스 인증 시스템(100)을 설명하기 위한 기능 블록도이다.
- [0058] 도 4는 본 발명의 일 실시예에 따른 디바이스의 인증 방법을 설명하는 흐름도이다.
- [0059] 도 5는 본 발명의 일 실시예에 따른 디바이스 인증 방법에 따라 다수의 이중 네트워크로 구성된 통신 네트워크에서 디바이스를 인증하는 방법을 설명하는 도면이다.
- [0060] 도 6은 본 발명의 다른 실시예에 따른 디바이스의 인증 방법을 설명하는 흐름도이다.
- [0061] 도 7은 유효 상태를 설명하기 위한 도면이다.
- [0062] 도 8은 본 발명의 다른 실시예에 따른 디바이스 인증 방법의 사용 예를 설명하기 위한 도면이다.
- [0063] 도 9는 인증 티켓 포맷의 일 예를 도시하고 있다.

도면

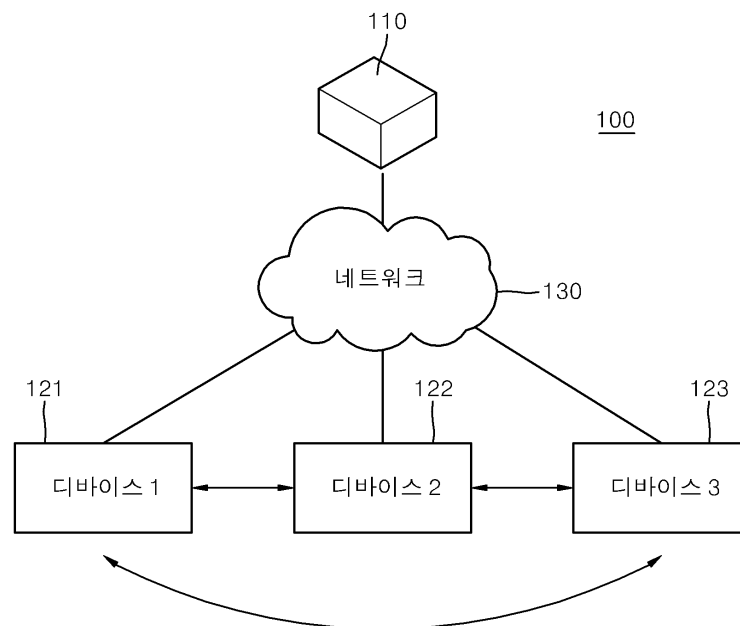
도면1



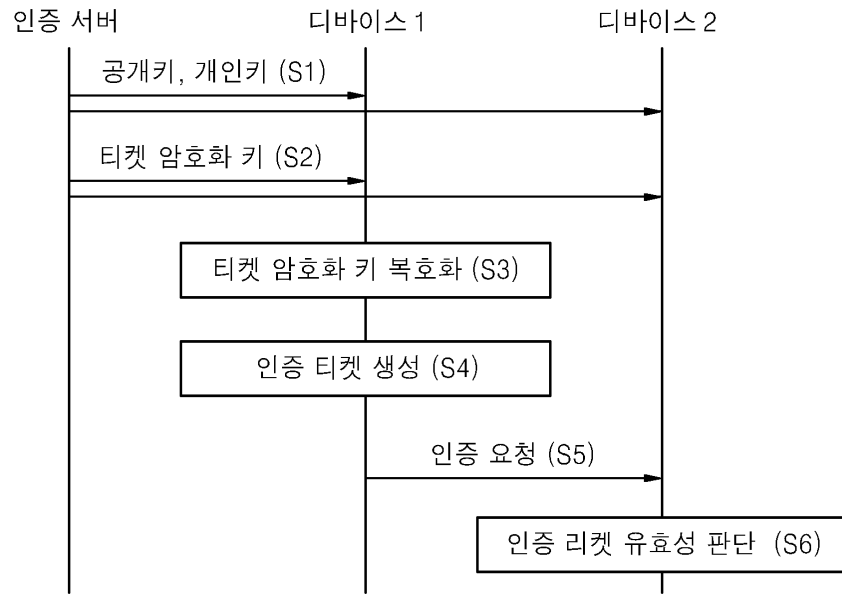
도면2



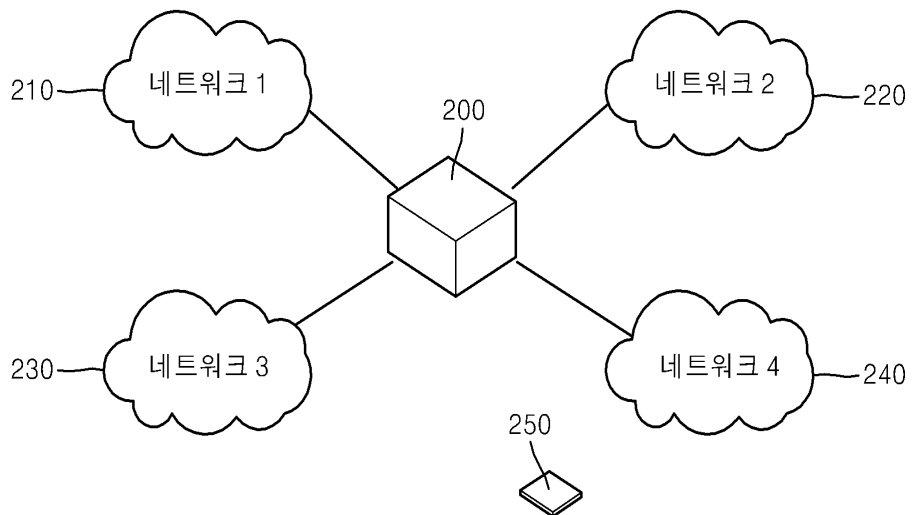
도면3



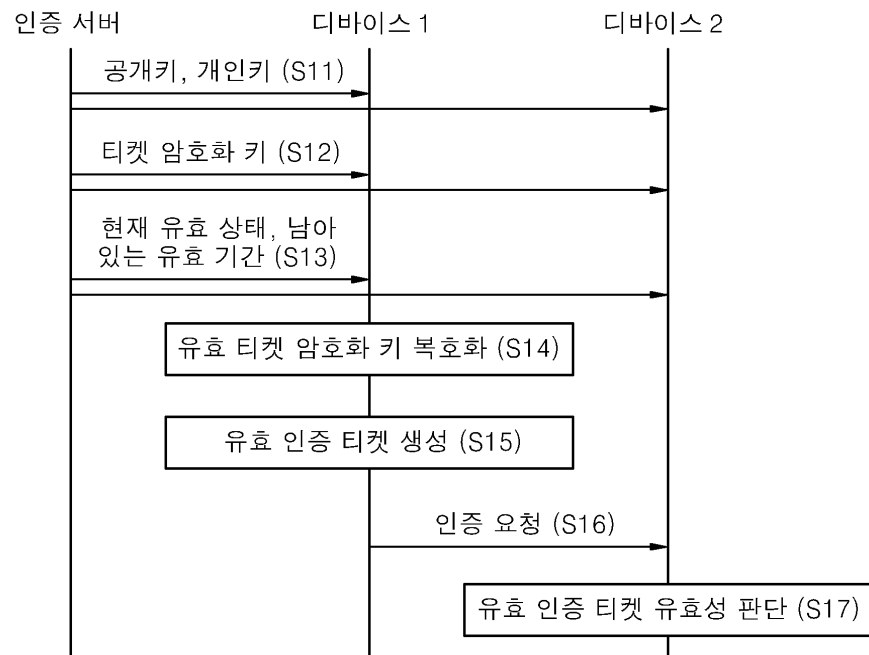
도면4



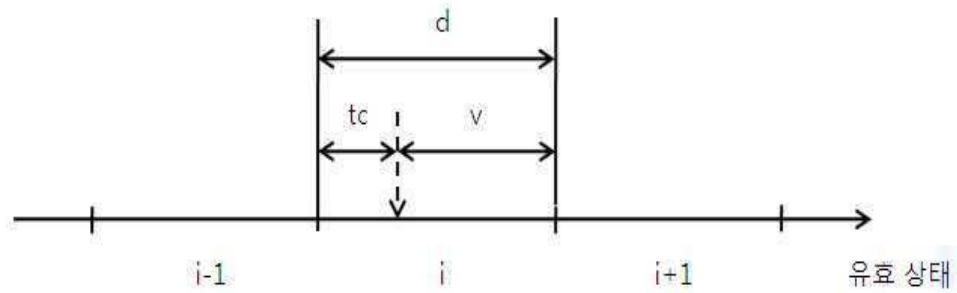
도면5



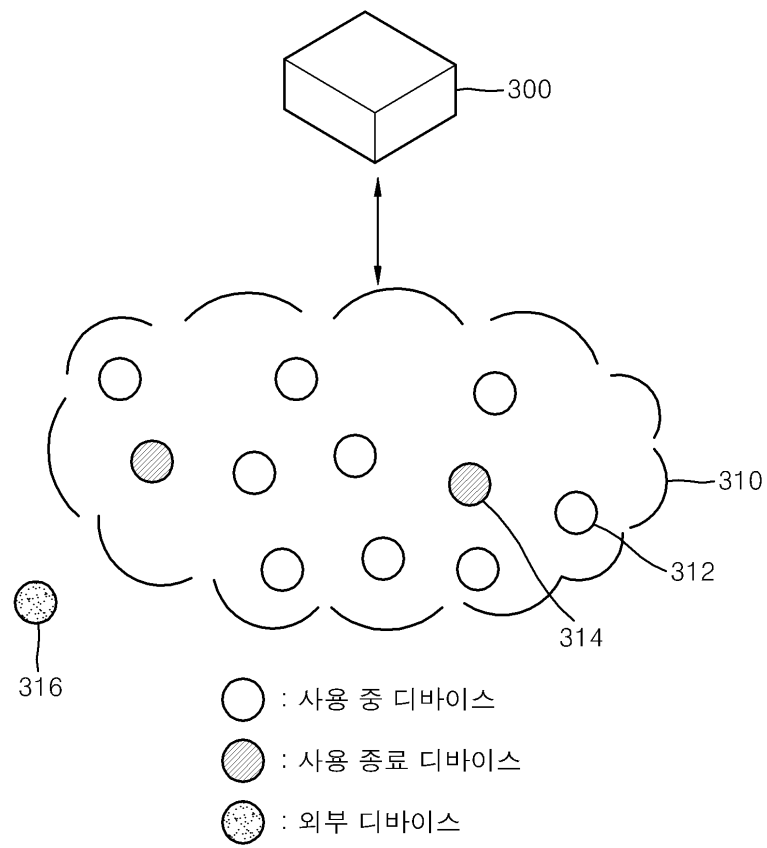
도면6



도면7



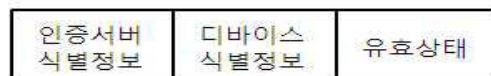
도면8



도면9



(a)



(b)