



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2017-0079089
(43) 공개일자 2017년07월10일

(51) 국제특허분류(Int. Cl.)
H04L 9/14 (2006.01) H04L 29/06 (2006.01)
H04L 9/08 (2006.01) H04L 9/32 (2006.01)
(52) CPC특허분류
H04L 9/14 (2013.01)
H04L 63/20 (2013.01)
(21) 출원번호 10-2015-0189271
(22) 출원일자 2015년12월30일
심사청구일자 2015년12월30일

(71) 출원인
이화여자대학교 산학협력단
서울특별시 서대문구 이화여대길 52 (대현동, 이화여자대학교)
(72) 발명자
도인실
인천광역시 연수구 센트럴로 194, 201동 2705호(송도동, 더샵 센트럴파크2)
채기준
서울특별시 강남구 강남대로136길 34
(74) 대리인
특허법인(유한)아이시스

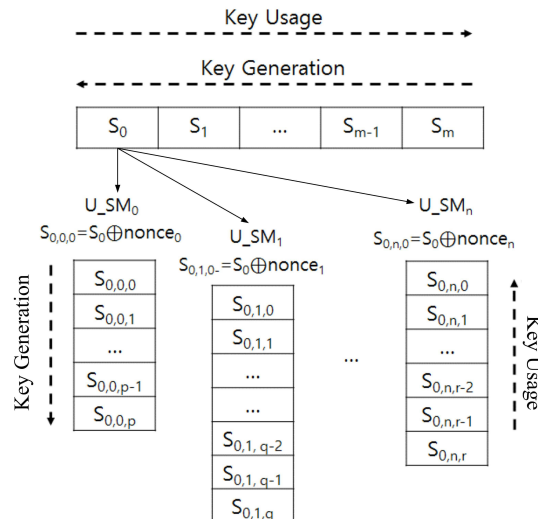
전체 청구항 수 : 총 8 항

(54) 발명의 명칭 스마트 그리드 시스템에서 정보 전달을 위한 인증 방법 및 스마트 그리드 시스템에서 정보를 수집하는 방법

(57) 요약

스마트 그리드 시스템에서 정보 전달을 위한 인증 방법은 스마트 그리드 시스템에서 제어 서버가 복수의 스마트 미터에 계층적 구조를 형성하기 위한 정책을 전달하는 단계, 동일 그룹에 속하는 상기 복수의 스마트 미터가 스마트 미터 중 어느 하나를 상위 계층 스마트 미터와 나머지 스마트 미터인 하위 계층 스마트 미터로 구분되는 단계, 상기 제어 서버가 TESLA 기법을 사용하여 제1 키 체인을 생성하는 단계, 상기 상위 계층 스마트 미터가 상기 제1 키 체인의 요소와 임의의 이진 비트를 이용하여 시드 키를 생성하는 단계 및 상기 상위 계층 스마트 미터가 상기 시드 키를 시작값으로 TESLA 기법을 사용하여 제2 키 체인을 생성하는 단계를 포함한다.

대표도 - 도4



(52) CPC특허분류

H04L 9/0869 (2013.01)

H04L 9/3236 (2013.01)

Y04S 40/24 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호 2012R1A1A3019459

부처명 미래창조과학부

연구관리전문기관 한국연구재단

연구사업명 기초연구사업(학술진흥)-일반연구자지원사업-여성과학자

연구과제명 사물지능통신(M2M) 응용분야 보안 연구

기 여 율 1/1

주관기관 이화여자대학교 산학협력단

연구기간 2012.05.01 ~ 2015.04.30

명세서

청구범위

청구항 1

스마트 그리드 시스템에서 제어 서버가 복수의 스마트 미터에 계층적 구조를 형성하기 위한 정책을 전달하는 단계;

동일 그룹에 속하는 상기 복수의 스마트 미터가 스마트 미터 중 어느 하나를 상위 계층 스마트 미터와 나머지 스마트 미터인 하위 계층 스마트 미터로 구분되는 단계;

상기 제어 서버가 TESLA 기법을 사용하여 제1 키 체인을 생성하는 단계;

상기 상위 계층 스마트 미터가 상기 제1 키 체인의 요소와 임의의 이진 비트를 이용하여 시드 키를 생성하는 단계; 및

상기 상위 계층 스마트 미터가 상기 시드 키를 시작값으로 TESLA 기법을 사용하여 제2 키 체인을 생성하는 단계를 포함하는 스마트 그리드 시스템에서 정보 전달을 위한 인증 방법.

청구항 2

제1항에 있어서,

상기 제어 서버는 상기 상위 계층 스마트 미터와 통신을 수행하는 과정에서 상기 제1 키 체인을 사용하여 인증을 수행하는 단계를 더 포함하는 스마트 그리드 시스템에서 정보 전달을 위한 인증 방법.

청구항 3

제1항에 있어서,

상기 상위 계층 스마트 미터는 상기 하위 계층 스마트 미터와 통신을 수행하는 과정에서 상기 제2 키 체인을 사용하여 인증을 수행하는 단계를 더 포함하는 스마트 그리드 시스템에서 정보 전달을 위한 인증 방법.

청구항 4

제3항에 있어서,

상기 상위 계층 스마트 미터는 타임 슬롯 또는 상기 하위 계층 스마트 미터의 식별자를 기준으로 상기 제2 키 체인에 해싱 함수를 적용하여 상기 인증을 수행하는 스마트 그리드 시스템에서 정보 전달을 위한 인증 방법.

청구항 5

제1항에 있어서,

상기 시드 키를 생성하는 단계에서 상기 상위 계층 스마트 미터는 상기 제어 서버가 상기 제1 키 체인을 생성하고 전달한 상기 최종값과 상기 이진 비트를 XOR연산하여 상기 시드 키를 생성하는 스마트 그리드 시스템에서 정보 전달을 위한 인증 방법.

청구항 6

제1항에 있어서,

상기 시드 키를 생성하는 단계에서 상기 상위 계층 스마트 미터는 타임 슬롯을 기준으로 상기 제1 키 체인 중 어느 하나의 요소를 결정하고, 상기 어느 하나의 요소와 상기 이진 비트를 XOR 연산하여 상기 시드 키를 생성하는 스마트 그리드 시스템에서 정보 전달을 위한 인증 방법.

청구항 7

스마트 그리드 시스템에서 제어 서버가 어느 하나를 상위 계층 스마트 미터와 나머지 스마트 미터인 하위 계층

스마트 미터를 포함하는 복수의 스마트 미터에 계층적 구조를 형성하기 위한 정책을 전달하는 단계;

상기 제어 서버가 TESLA 기법을 사용하여 제1 키 체인을 생성하는 단계;

상기 상위 계층 스마트 미터가 상기 제1 키 체인의 요소를 기준으로 TESLA 기법을 사용하여 제2 키 체인을 생성하는 단계;

상기 하위 계층 스마트 미터가 타임 슬롯 또는 하위 계층 스마트 미터의 식별자를 기준으로 상기 제2 키 체인의 요소 중 어느 하나를 사용하여 전기 기기가로부터 수집한 정보를 암호화하는 단계;

상기 상위 계층 스마트 미터가 상기 하위 계층 스마트 미터가 암호화한 정보를 취합하여 유틸리티 시스템에 전달하는 단계; 및

상기 유틸리티 시스템이 상기 암호화한 정보를 상기 제1 키 체인 및 상기 제2 키 체인을 기준으로 복호하는 단계를 포함하는 스마트 그리드 시스템에서 정보를 수집하는 방법.

청구항 8

제7항에 있어서,

상기 유틸리티 시스템은 상기 상위 계층 스마트 미터가 상기 제1 키 체인의 요소를 결정한 기준 및 상기 하위 계층 스마트 미터가 상기 제2 키 체인의 요소를 결정한 기준을 사용하여 복호키를 생성하고, 상기 복호키를 이용하여 상기 암호화된 정보를 복호하는 스마트 그리드 시스템에서 정보를 수집하는 방법.

발명의 설명

기술 분야

[0001] 이하 설명하는 기술은 스마트 그리드 시스템에서의 인증 기법에 관한 것이다.

배경 기술

[0002] 스마트 그리드(smart grid)는 기존의 전력 망에 정보통신 기술을 접목하여 전력 공급자와 소비자가 양 방향으로 실시간 정보를 교환함으로써 에너지 효율을 최적화하는 차세대 지능형 전력 망이다.

[0003] 스마트 그리드는 가정의 스마트 미터기(smart meter)로부터 일정한 정보를 게이트웨이를 통해 전력망에 전달한다. 스마트 그리드는 서로 다른 종류 또는 사업자가 서로 다른 네트워크를 거쳐 정보를 전송할 수 있다. 즉 스마트 그리드는 매우 다양한 종류의 게이트웨이 또는 다양한 종류의 AP(access point)로 정보를 전달할 필요가 있다.

선행기술문헌

비특허문헌

[0004] (비특허문헌 0001) Priti V. Jasud, Manish D. Katkar, S. D. Kamble, "Authentication Mechanism for Smart Grid Network," International Journal of Soft Computing and Engineering, ISSN: 2231-2307, Volume-4, Issue-1, March 2014.

(비특허문헌 0002) Yaghmaee, Mohammad Hossein, and Fatemeh Naji Mohades. "A Lightweight mechanism for Mutual Authentication in SmartGrid ,"CIRED Workshop, Rome, 11-12 June 2014.

(비특허문헌 0003) Bekara, Chakib, Thomas Luckenbach, and Kheira Bekara. "A privacy preserving and secure authentication protocol for the advanced metering infrastructure with non-repudiation service," ENERGY 2012, The Second International Conference on Smart Grids, Green Communications and IT Energy-aware Technologies. 2012.

(비특허문헌 0004) Adrian Perrig, Ran Canetti, J. D. Tygar, Dawn Song, "The TESLA Broadcast Authentication Protocol," In CryptoBytes, 2002.

발명의 내용

해결하려는 과제

- [0005] 다양한 네트워크 또는/및 다양한 시스템으로 구성되는 스마트 그리드는 그만큼 네트워크 공격에 취약할 수 있다. 다양한 지점이 공격 타깃이 될 수 있기 때문이다. 이하 설명하는 기술은 계층적 구조에 기반한 인증 과정을 갖는 스마트 그리드 시스템을 제공하고자 한다. 나아가 이하 설명하는 기술은 인증 과정에 사용하는 키를 이용하여 암호화된 정보를 전달하는 스마트 그리드 시스템을 제공하고자 한다.

과제의 해결 수단

- [0006] 스마트 그리드 시스템에서 정보 전달을 위한 인증 방법은 스마트 그리드 시스템에서 제어 서버가 복수의 스마트 미터에 계층적 구조를 형성하기 위한 정책을 전달하는 단계, 동일 그룹에 속하는 상기 복수의 스마트 미터가 스마트 미터 중 어느 하나를 상위 계층 스마트 미터와 나머지 스마트 미터인 하위 계층 스마트 미터로 구분되는 단계, 상기 제어 서버가 TESLA 기법을 사용하여 제1 키 체인을 생성하는 단계, 상기 상위 계층 스마트 미터가 상기 제1 키 체인의 요소와 임의의 이진 비트를 이용하여 시드 키를 생성하는 단계 및 상기 상위 계층 스마트 미터가 상기 시드 키를 시작값으로 TESLA 기법을 사용하여 제2 키 체인을 생성하는 단계를 포함한다.
- [0007] 스마트 그리드 시스템에서 정보를 수집하는 방법은 스마트 그리드 시스템에서 제어 서버가 어느 하나를 상위 계층 스마트 미터와 나머지 스마트 미터인 하위 계층 스마트 미터를 포함하는 복수의 스마트 미터에 계층적 구조를 형성하기 위한 정책을 전달하는 단계, 상기 제어 서버가 TESLA 기법을 사용하여 제1 키 체인을 생성하는 단계, 상기 상위 계층 스마트 미터가 상기 제1 키 체인의 요소를 기준으로 TESLA 기법을 사용하여 제2 키 체인을 생성하는 단계, 상기 하위 계층 스마트 미터가 타임 슬롯 또는 하위 계층 스마트 미터의 식별자를 기준으로 상기 제2 키 체인의 요소 중 어느 하나를 사용하여 전기 기기가로부터 수집한 정보를 암호화하는 단계, 상기 상위 계층 스마트 미터가 상기 하위 계층 스마트 미터가 암호화한 정보를 취합하여 유틸리티 시스템에 전달하는 단계 및 상기 유틸리티 시스템이 상기 암호화한 정보를 상기 제1 키 체인 및 상기 제2 키 체인을 기준으로 복호하는 단계를 포함한다.

발명의 효과

- [0008] 이하 설명하는 기술은 계층적 구조로 인증을 수행하여 스마트 미터가 수집한 데이터를 안정하게 전력망에 전달할 수 있다.

도면의 간단한 설명

- [0009] 도 1은 스마트 그리드 시스템의 구조를 도시한 예이다.
- 도 2는 계층적 구조를 갖는 스마트 그리드 시스템에 대한 예이다.
- 도 3은 TESLA 기법에 따라 생성되는 키에 대한 예이다.
- 도 4는 계층적 스마트 그리드 시스템에서 인증을 위한 키 생성 과정에 대한 예이다.
- 도 5는 스마트 그리드 시스템에서 사용되는 키를 나타내는 테이블에 대한 예이다.
- 도 6은 스마트 그리드 시스템에서 정보 전달을 위한 키 설정 방법에 대한 순서도의 예이다.
- 도 7은 스마트 그리드 시스템에서 정보를 수집하는 방법에 대한 순서도의 예이다.

발명을 실시하기 위한 구체적인 내용

- [0010] 이하 설명하는 기술은 다양한 변형을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세하게 설명하고자 한다. 그러나, 이는 이하 설명하는 기술을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 이하 설명하는 기술의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다.
- [0011] 제1, 제2, A, B 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 해당 구성요소들은 상기 용어들에 의해 한정되지는 않으며, 단지 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다. 예를 들어, 이하 설명하는 기술의 권리 범위를 벗어나지 않으면서 제1 구성요소는 제2 구성요소로 명명될 수

있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다. 및/또는 이라는 용어는 복수의 관련된 기재된 항목들의 조합 또는 복수의 관련된 기재된 항목들 중의 어느 항목을 포함한다.

[0012] 본 명세서에서 사용되는 용어에서 단수의 표현은 문맥상 명백하게 다르게 해석되지 않는 한 복수의 표현을 포함하는 것으로 이해되어야 하고, "포함한다" 등의 용어는 실시된 특징, 개수, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것이 존재함을 의미하는 것이지, 하나 또는 그 이상의 다른 특징들이나 개수, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 배제하지 않는 것으로 이해되어야 한다.

[0013] 도면에 대한 상세한 설명을 하기에 앞서, 본 명세서에서의 구성부들에 대한 구분은 각 구성부가 담당하는 주기능 별로 구분한 것에 불과함을 명확히 하고자 한다. 즉, 이하에서 설명할 2개 이상의 구성부가 하나의 구성부로 합쳐지거나 또는 하나의 구성부가 보다 세분화된 기능별로 2개 이상으로 분화되어 구비될 수도 있다. 그리고 이하에서 설명할 구성부 각각은 자신이 담당하는 주기능 이외에도 다른 구성부가 담당하는 기능 중 일부 또는 전부의 기능을 추가적으로 수행할 수도 있으며, 구성부 각각이 담당하는 주기능 중 일부 기능이 다른 구성부에 의해 전담되어 수행될 수도 있음은 물론이다.

[0014] 또, 방법 또는 동작 방법을 수행함에 있어서, 상기 방법을 이루는 각 과정들은 문맥상 명백하게 특정 순서를 기재하지 않은 이상 명기된 순서와 다르게 일어날 수 있다. 즉, 각 과정들은 명기된 순서와 동일하게 일어날 수도 있고 실질적으로 동시에 수행될 수도 있으며 반대의 순서대로 수행될 수도 있다.

[0016] 이하에서는 도면을 참조하면서 에 관하여 구체적으로 설명하겠다.

[0018] 도 1은 스마트 그리드 시스템(100)의 구조를 도시한 예이다. 스마트 그리드 시스템(100)은 제어 서버(140), 복수의 스마트 미터(110) 및 유틸리티 시스템(utility system, 120)을 구비한다. 제어 서버(140)는 스마트 그리드 시스템을 전반적으로 제어하는 주체이다. 제어 서버(140)는 스마트 미터(110)와 유틸리티 시스템(130) 사이의 인증을 위한 정보를 제공한다. 수행한다. 스마트 미터(110)는 스마트 미터가 관리하는 일정한 영역(건물 등)에 배치된 전기 기기로부터 일정한 정보를 수집한다. 유틸리티 시스템(130)은 에너지 소비 데이터를 분석하여 전기 기기에 적절한 에너지를 제공한다. 스마트 그리드 시스템(100)을 구성하는 각 객체(entity)는 서로 통신할 수 있다. 스마트 미터(110)가 전달하는 데이터는 전달 과정에서 변형되거나 공개되지 않고, 안전하게 목표까지 전달되어야 한다. 스마트 미터(110)는 특정 영역(건물, 특정 지역 등)에 배치된 전기 기기(50)로부터 일정한 정보를 수집한다. 도 1에서는 가정에 배치된 전기 기기(50)로부터 정보를 수집하는 예를 도시하였다. 전기 기기(50)는 가정인 경우 TV, 에어컨, 냉장고 등과 같은 가전 제품을 포함하고, 공장인 경우 각종 기계 장치를 포함하고, 사무실인 경우 컴퓨터, 조명 장치, 냉난방 장치 등을 포함한다. 한편 스마트 미터(110)가 수집한 정보는 게이트웨이(120)를 통해 유틸리티 시스템(130)에 전달될 수 있다.

[0020] 이하 설명하는 기법은 복수의 스마트 미터가 계층적 구조를 이루는 스마트 그리드 시스템을 전제로 한다. 도 2는 계층적 구조를 갖는 스마트 그리드 시스템(200)에 대한 예이다.

[0021] 먼저 계층적 구조에 대해 설명한다. 가장 하위 계층에 있는 스마트 미터는 일정한 지역, 영역 또는 건물 단위로 구분될 수 있다. 가장 하위 계층을 제1 계층이라고 명명한다. 제1 계층은 예컨대, HAN(Home Area Network), BAN(Building Area Network), NAN(Neighborhood Area Network) 등과 같은 단위로 그룹을 형성할 수 있다. 다른 말로 표현하면 물리적 계층인 제1 계층에 속한 스마트 미터는 일정한 영역 단위의 네트워크에서 정보 수집을 한다. 도 2에서는 하위 계층에 4개의 네트워크가 존재한다. 네트워크(210, 240 및 250)는 NAN이고, 네트워크(220)는 BAN이고, 네트워크(230)는 HAN이다.

[0022] 제1 계층을 구성하는 복수의 스마트 미터 중에서 특정한 조건을 만족하는 스마트 미터가 상위 계층을 구성한다. 즉 상위 계층은 하위 계층에 존재하는 물리적인 스마트 미터 중 일부가 구성하는 가상적 계층에 해당한다. 하위 계층에 위치하는 스마트 미터를 하위 계층 스마트 미터라고 명명하고, 상위 계층에 위치하는 스마트 미터를 상위 계층 스마트 미터라고 명명한다. 제1 계층이 도 2와 같이 일정한 그룹으로 구분되는 경우 각 그룹에 속한 스마트 미터 중 어느 하나를 특정한 기준에 따라 상위 계층(제2 계층) 스마트 미터로 선택할 수 있다. 어느 하나의 상위 계층 스마트 미터는 하위 계층에서 특정 그룹을 대표한다. 하위 계층 스마트 미터 중 특정 그룹에 소속된 스마트 미터를 그룹 스마트 미터라고 명명한다. 여기서 하나의 그룹은 하나의 개별 네트워크인 HAN, BAN,

NAN 등일 수 있다. 도 2에서 네트워크(210)는 5개의 스마트 미터(211 내지 215)를 포함하고, 스마트 미터(215)가 상위 계층 스마트 미터로 선택된 예를 도시한다. 네트워크(210)에 소속된 스마트 미터(211 내지 214)가 그룹 스마트 미터에 해당한다. 도 2에서 다른 네트워크(220, 230, 240 및 250)는 각각 하나의 스마트 미터(225, 235, 245 및 255)가 상위 계층 스마트 미터로 선택된 예를 도시한다.

[0023] 제1 계층 중 선택된 스마트 미터는 제1 계층의 바로 위 순위의 계층(제2 계층)을 형성한다. 제2 계층을 형성하는 스마트 미터는 제1 계층을 구성하는 스마트 미터가 수집한 정보를 취합한다. 즉 제2 계층을 형성하는 스마트 미터는 하위 계층의 스마트 미터의 정보를 모두 갖고 있다. 도 2에서 상위 계층 스마트 미터(215)는 그룹 스마트 미터(211 내지 214)가 수집한 정보를 취합한다. 나아가 상위 계층 스마트 미터(215)는 자신이 수집한 정보도 취합하여 유틸리티 시스템(260)에 전달할 수 있다.

[0024] 정리하면 상위 계층은 해당 상위 계층 바로 아래에 있는 계층을 구성하는 스마트 미터 중 선택된 스마트 미터로 구성된다. 상위 계층 스마트 미터는 자신이 대표하는 하위 계층의 스마트 미터가 수집한 데이터를 모두 취합하여 상위 계층으로 전달한다. 상위 계층 스마트 미터는 일정한 네트워크 정책(policy)에 따라 하위 계층에 존재하는 스마트 미터 중 선택된다. 상위 계층 스마트 미터를 결정하는 과정은 주기적으로 반복될 수 있다.

[0025] 도 2는 2개의 계층만을 예로 도시하였으나, 제2 계층 위에 또 다른 상위 계층이 존재할 수도 있다. 이하 2개의 계층을 갖는 구조를 기준으로 설명한다. 따라서 이하 하위 계층(제1 계층)의 스마트 미터 및 상위 계층(제2 계층)의 스마트 미터를 포함하는 계층적 스마트 그리드 시스템을 전체로 설명한다.

[0027] 도 2의 스마트 그리드 시스템(200)에서 정보를 수집하는 절차 흐름을 간략하게 설명한다. 기본적으로 제어 서버(270), 유틸리티 시스템(260) 및 스마트 미터는 각각 정보를 수신하는 다른 객체와 비밀키를 사용하여 암호화된 정보를 주고받는다. (1) 제어 서버(270)는 유틸리티 시스템(260) 및 스마트 미터에 정보 수집과 관련된 일정한 정책(policy)을 전달한다. (2) 스마트 미터는 수신한 정책에 따라 계층적 구조를 형성한다. 제1 계층에서 각 그룹은 대표 스마트 미터가 루트(root)가 되는 트리 구조를 갖는다. (3) 스마트 미터는 전기 기기로부터 일정한 정보를 수집하여 상위 계층에 전달한다. 상위 계층 스마트 미터가 자신이 속한 그룹의 그룹 스마트 미터로부터 정보를 취합한다. (4) 상위 계층(제2 계층) 스마트 미터는 자신이 취합한 정보를 유틸리티 시스템(260)에 전달한다. 이하 상위 계층 스마트 미터가 취합하여 유틸리티 시스템(260)에 전달하는 정보를 취합 정보라고 명명한다. (5) 유틸리티 시스템은 스마트 미터가 전달한 취합 정보를 인증하고, 정보를 분석한다. 정보가 전달되는 경로는 전기기기 → 하위 계층 스마트 미터(그룹 스마트 미터) → 상위 계층 스마트 미터 → 유틸리티 시스템이다.

[0028] 제어 서버(270)는 보안 관련 정보를 상위 계층 스마트 미터에 전달한다. 보안 관련 정보는 스마트 미터 및 유틸리티 시스템(260)이 정보를 주고 받는 과정에서 사용하는 인증을 위한 정보를 포함한다. 상위 계층 스마트 미터는 자신이 속한 하위 계층 스마트 미터에 보안 관련 정보를 전달한다. 네트워크 정책에 따라 하위 계층 스마트 미터는 전기 기기로부터 에너지 사용 데이터(energy usage data)를 수집하여 상위 계층 스마트 미터에 전달한다. 상위 계층 스마트 미터는 복수의 하위 계층 스마트 미터가 전달한 정보를 취합한 취합 정보를 유틸리티 시스템(260)에 전달한다. 전송한 바와 같이 이 과정에서 스마트 미터와 유틸리티 시스템(260)은 암호화된 정보를 전달한다. 정보를 암호화하기 위해서는 기본적으로 특정 키(key)가 필요하다. 스마트 미터와 유틸리티 시스템(260)은 키 분배에 앞서 상호 간 인증이 필요하다.

[0030] 스마트 그리드 시스템에서 사용하는 인증 기법에 대해 설명한다. 이하 설명하는 인증 기법은 TESLA(Timed Efficient Stream Loss-tolerant Authentication) 기법에 기반한다(Adrian Perrig, Ran Canetti, J. D. Tygar, Dawn Song, "The TESLA Broadcast Authentication Protocol," In CryptoBytes, 2002.참조). 이하 설명하는 인증 기법은 TESLA를 변형한 기법에 해당한다.

[0031] 제어 서버(인증 서버)는 일 방향 체인(one-way chain)을 사용하여 세션 키(session key)를 생성한다. 즉, 키가 일정한 순서로 해시 함수를 적용하여 생성된다. 생성된 키는 이후 키가 생성된 순서의 역 순으로 한 단계씩 복호되어 사용된다. TESLA 기법은 일 방향 체인을 사용하여 최초 값을 일정하게 가공하여 연속된 일련의 값을 생성한다. 예컨대, 일 방향 체인은 해시 함수일 수 있다. 이하 해시 함수를 기준으로 설명한다. 도 3은 TESLA 기법에 따라 생성되는 키에 대한 예이다. 제어 서버는 길이 ℓ 을 갖는 체인을 생성하기 위해 체인 s_{ℓ} 의 마지막 요

소(element)를 랜덤하게 선택한다. 제어 서버는 최초 선택한 요소를 해시 함수 F 에 적용하여 $s_{\ell-1}$ 을 생성하고, 생성된 결과값에 대해 연속적으로 해시 함수를 적용하여 최종적으로 s_0 을 생성한다. 생성한 키를 검증하는 과정도 간략하게 설명한다. 예컨대, s_i 가 해시 체인의 i 번째 요소인지 확인하려면 $F^i(s_i) = s_0$ 인지 여부를 확인한다. 이는 s_i 를 시작으로 해시 함수 F 를 i 번 연속으로 적용한다는 의미이다. 보다 일반적으로 s_i 가 체인의 i 번째 요소라고 알고 있는 상황에서 s_j 가 체인의 일부인지를 검증한다면 ($i < j$), $F^{j-i}(s_j) = s_i$ 라는 결과가 나오는지를 확인하면 된다.

[0033] 도 4는 계층적 스마트 그리드 시스템에서 인증을 위한 키 생성 과정에 대한 예이다. 제어 서버는 TESLA 기법에 따라 기본 키 체인을 생성하고, 생성한 기본 키 체인을 상위 계층 스마트 미터에 전달한다. 첫 번째 키로 S_0 가 사용된다. S_0 는 제어 서버가 최초로 스마트 미터에 전달한 기본 키 체인의 최종 결과값에 해당한다. 상위 계층 스마트 미터는 S_0 을 공유한다. 이 키는 제어 서버에서 스마트 미터 방향(하위 방향)으로 전달하는 보안 관련 정보, 시스템 파라미터, 하위 계층의 그룹 내에서 트리를 구성하기 위한 정보 등을 전달하는데 사용된다. 상위 계층의 스마트 미터는 수신한 키 값에 대해 해시 함수를 $j-i$ 번 적용하여 키 값을 인증한다.

[0034] 상위 계층의 각 스마트 미터는 자신이 대표하는 하위 계층의 그룹(예컨대, HAN 등)을 위한 키 체인을 생성한다. 여기서 상위 계층 스마트 미터가 해당 그룹을 위해 생성하는 키 체인을 그룹 키 체인이라고 명명한다. 각 네트워크마다 사용되는 키값은 서로 달라야 한다. 따라서 상위 계층의 스마트 미터는 1회성 숫자(이진 코드)인 nonce(number used once)를 생성하고, 제어 서버로부터 수신한 기본 키 체인과 XOR 연산을 하여 시드 키(seed key)를 생성한다. 하위 계층의 하나의 그룹에 속한 그룹 스마트 미터의 개수가 서로 다를 수 있기 때문에 상위 계층 스마트 미터가 생성하는 그룹 키 체인의 길이도 그룹마다 다를 수 있다. 상위 계층 스마트 미터는 그룹 키 체인을 생성한 후 새로운 키를 자신의 그룹에 소속된 하위 계층 스마트 미터에 전달한다. 상위 계층 스마트 미터가 생성하는 그룹 키 체인은 제어 서버가 생성했던 기본 키 체인을 이용하여 생성된다. 즉 그룹 키 체인은 기본 키 체인 중 하나의 요소를 기준으로 생성된다.

[0035] 도 4를 기준으로 키 생성 방법에 대해 설명한다.

[0036] (1) 제어 서버는 상위 계층 스마트 미터를 위한 기본 키 체인을 생성하고, 기본 키 체인을 상위 계층 스마트 미터에 전달한다. 기본 키 체인은 $S_0 \sim S_m$ 까지의 요소를 갖는다.

[0037] (2) 각 상위 계층 스마트 미터(U_{SM_0} 내지 U_{SM_n})는 S_0 와 자신의 nonce를 XOR 연산하여 시드 키를 생성한다. U_{SM_0} 은 $S_0 \oplus \text{nonce}_0$ 연산을 통해 시드 키 $S_{0,0,0}$ 을 생성한다. 여기서 $\oplus$ 는 XOR 연산자를 의미한다. U_{SM_1} 은 $S_0 \oplus \text{nonce}_1$ 연산을 통해 시드 키 $S_{0,1,0}$ 을 생성한다. U_{SM_n} 은 $S_0 \oplus \text{nonce}_n$ 연산을 통해 시드 키 $S_{0,n,0}$ 을 생성한다. 각 상위 계층 스마트 미터는 시드 키를 기준으로 그룹 키 체인을 생성한다. 예컨대, U_{SM_0} 은 최종적으로 S 를 $S_{0,0,0,p}$ 를 생성한다. 상위 계층 스마트 미터도 제어 서버와 같이 일 방향 해시 함수를 연속으로 사용하여 그룹 키 체인을 생성한다. 상위 계층 스마트 미터는 제어 서버가 기본 키 체인 생성에 사용한 동일한 해시 함수를 사용할 수 있다. 또는 상위 계층 스마트 미터는 제어 서버가 사용한 해시 함수와는 다른 해시 함수를 사용하여 그룹 키 체인을 생성할 수도 있다.

[0038] 그룹 키 체인은 상위 계층 스마트 미터가 자신이 소속한 그룹 내의 다른 스마트 미터인 그룹 스마트 미터와 통신하는데 사용한다. U_{SM_0} 은 $p+1$ 길이의 그룹 키 체인을 생성하고, U_{SM_1} 은 $q+1$ 길이를 갖는 그룹 키 체인을 생성하였고, U_{SM_n} 은 $r+1$ 길이를 갖는 그룹 키 체인을 생성하였다.

[0039] (3) 상위 계층 스마트 미터는 생성한 그룹 키 체인을 소속 그룹의 하위 계층 스마트 미터(그룹 스마트 미터)에 분배한다. 그룹 키 체인은 그룹 스마트 미터가 수집한 데이터를 상위 계층 스마트 미터에 전달하는 과정에 사용된다.

- [0041] 도 5는 스마트 그리드 시스템에서 사용되는 키를 나타내는 테이블에 대한 예이다. 도 5는 타임 슬롯(slot)과 해당 타임 슬롯에서의 정보 전달 과정에 사용되는 키에 대한 예를 나타낸다. 도 5에서 n 은 상위 계층 스마트 미터(U_SM)의 식별자에 해당하는 번호이다. 상위 계층 스마트 미터(U_SM)는 도 4와 같이 $U_SM_0 \sim U_SM_n$ 을 갖는 예이다. r 은 마지막 상위 계층 스마트 미터 S_n 가 속한 그룹의 하위 계층 스마트미터(L_SM)의 식별자에 해당하는 번호이다. 도 5는 상위 계층 스마트 미터 S_n 가 해당 하위 계층 스마트 미터와 통신에서 사용하는 키를 도시한 예이다.
- [0042] 유틸리티 시스템과 상위 계층 스마트 미터 사이의 통신은 타임 슬롯 0(slot 0)에서 S_0 이 먼저 사용된다. 상위 계층 스마트 미터는 해당 키를 검증하여 보안 정보, 네트워크 파라미터 등을 인증한다. 다음 타임 슬롯 1(slot 1)에서는 S_1 이 사용되고, 마지막 타임 슬롯 m (slot m)에서는 S_m 이 사용된다. 즉 유틸리티 시스템과 상위 계층 스마트 미터 사이에 시간이 동기화된 것을 전제로 일정한 시간 구역을 기준으로 기본 키 체인에서 검증하는 키를 다른 것으로 사용하는 것이다. S_n 뿐만 아니라 유틸리티 시스템과 다른 상위 계층 스마트 미터도 동일한 키를 사용하여 정보를 전송한다.
- [0043] 상위 계층 스마트 미터와 하위 계층 스마트 미터 사이의 통신은 해당 상위 계층 스마트 미터가 생성한 그룹 키 체인을 사용한다. 도 4에서는 상위 계층 스마트 미터가 S_0 를 사용하여 그룹 키 체인을 생성한 예를 도시하였고, 도 5에서는 타임 슬롯에 따라 상위 계층 스마트 미터 S_n 가 사용하는 기본 키값이 다른 경우를 도시한다. 즉 타임 슬롯 1에서 상위 계층 스마트 미터 S_n 는 S_1 을 사용하여 그룹 키 체인을 생성하고, 타임 슬롯 n 에서 상위 계층 스마트 미터 S_n 는 S_m 을 사용하여 그룹 키 체인을 생성한다.
- [0044] 상위 계층 스마트 미터 S_n 는 하위 계층 스마트 미터(L_SM)과 타임 슬롯 1에서는 최초로 $S_{0,n,r}$ 을 사용한다. 도 5에 도시하지 않았지만 상위 계층 스마트 미터와 소속 하위 계층 스마트 미터도 다른 타임 슬롯을 사용하여 그룹 키 체인 중 어떤 요소를 사용하여 인증을 수행할지 결정할 수도 있다. 즉 그룹 키 체인에서 몇 번째 요소(즉 몇 번의 해싱 함수 적용할지)를 사용할지는 일정한 시간에 따라 결정할 수도 있다. 또는 시간이 아닌 다른 변수를 기준으로 그룹 키 체인에서 몇 번째 요소를 기준으로 인증을 수행할지 결정할 수 있다. 예컨대 하위 계층 스마트 미터의 식별자(번호)에 따라 그룹 키 체인 중 특정 요소를 인증 기준으로 사용할 수도 있다. 물론 이러한 기준은 사전에 제어 서버가 각 스마트 미터에 전달해야 할 것이다.
- [0046] 도 4 및 도 5는 제어 서버로부터 일정한 정보가 하위 계층 스마트 미터까지 전달되는 하위 방향의 정보 전달에 사용될 수 있다. 하위 계층 스마트 미터는 전기 기기의 에너지 사용 정보를 수집한다. 에너지 사용 정보는 상위 계층 스마트 미터를 통해 유틸리티 시스템에 전달된다. 이제 하위 방향의 정보 전달에서 해당 정보의 유효성을 인증하기 위해 사용했던 키를 사용하여 스마트 미터가 수집한 정보를 유틸리티 시스템에 전달하는 과정에 대해 설명한다. 즉 키 체인에서 공개된 키를 사용하여 데이터 암호화에 사용하는 것이다. 예컨대, U_SM_n 에 속한 하위 계층 스마트 미터가 전기 기기로부터 에너지 사용 정보를 수집하고, 공개된 키 $S_{0,n,0}$ 를 사용하여 정보를 암호화할 수 있다. 최종적으로 유틸리티 시스템이 $S_{0,n,0}$ 를 사용하여 암호화된 정보를 복호하기 위해서는 U_SM_n 의 $nonce_n$ 과 제어 서버가 생성한 기본 키 체인에 대한 정보를 알고 있어야 한다. 제어 서버는 기본 키 체인 정보, 특정 상위 계층 스마트 미터의 $nonce$ 등을 유틸리티 시스템에 사전에 공유해야 한다.
- [0047] 결국 유틸리티 시스템은 상위 계층 스마트 미터가 기본 키 체인에서 인증에 사용한 체인 요소를 결정한 기준 및 하위 계층 스마트 미터가 상기 그룹 키 체인에서 인증에 사용한 요소를 결정한 기준을 사용하여 복호키를 생성하고, 복호키를 이용하여 암호화된 정보를 복호할 수 있다.
- [0048] 상위 계층 스마트 미터는 주기적으로 결정될 수 있고, 따라서 주기적으로 변경될 수도 있다. 이러한 주기에 따라 스마트 그리드 시스템은 인증과 관련된 정책을 다시 전달할 수 있고, 네트워크의 계층적 구조를 다시 설계할 수도 있다.
- [0050] 도 6은 스마트 그리드 시스템에서 정보 전달을 위한 키 설정 방법(300)에 대한 순서도의 예이다. 제어 서버는

복수의 스마트 미터에 계층적 구조를 형성하기 위한 정책을 전달한다(310). 한편 제어 서버가 전달하는 정책은 인증을 위한 정보를 포함할 수 있다. 인증을 위한 정보는 키 체인을 생성하는 규칙, 시드 키를 생성하는 규칙 등을 포함할 수 있다. 복수의 스마트 미터는 제어 서버의 정책에 따라 계층적 구조를 형성한다(320). 복수의 스마트 미터가 스스로 상위 계층 스마트 미터를 선택하고, 동일 네트워크 그룹 내에서 트리를 형성할 수 있다. 또는 제어 서버가 복수의 스마트 미터 중 상위 계층 스마트 미터를 선택하여 계층적 구조를 생성할 수도 있다.

[0051] 제어 서버는 전술한 바와 같이 TESLA 기법으로 기본 키 체인을 생성하고, 생성한 기본 키 체인을 상위 계층 스마트 미터에 분배한다(330). 상위 계층 스마트 미터는 기본 키 체인 요소 중 어느 하나의 임의의 이진 비트 (nonce)를 사용하여 시드 키를 생성할 수 있다(340). 이때 상위 계층 스마트 미터는 타임 슬롯을 기준으로 기본 키 체인 요소 중 어느 하나를 이용할 수 있다. 도 3에서 설명한 바와 같이 상위 계층 스마트 미터는 기본 키 체인이 생성된 역 순으로 특정 요소를 추출할 수 있다. 상위 계층 스마트 미터는 전술한 바와 같이 생성한 시드 키를 기준으로 그룹 키 체인을 생성하고, 이를 그룹 스마트 미터에 분배한다(350). 이 과정까지가 통해 정보 전달(통신)시 인증을 위한 작업이 준비작업에 해당한다.

[0052] 이후 제어 서버로부터 특정 정보가 상위 계층 스마트 미터에 전달되면 상위 계층 스마트 미터는 기본 키 체인을 사용하여 키 인증을 수행한다(360). 인증에 성공하면 상위 계층 스마트 미터는 자신이 관리하는 그룹 스마트 미터(하위 계층 스마트 미터)에 정보를 전달한다. 하위 계층 스마트 미터는 그룹 키 체인을 사용하여 다시 키 인증을 수행할 수 있다(370).

[0053] 제어 서버는 계층적 구조를 주기적으로 변경할 수 있다. 예컨대, 상위 계층 스마트 미터를 선택하는 정책이 변경되면 계층적 구조는 변경될 수 있다. 또는 일정한 시간 간격을 두고 계층적 구조를 주기적으로 변경할 수도 있다. 제어 서버는 계층적 구조의 재구성이 필요한지 여부를 확인하고(380), 재구성이 필요한 경우 새로운 정책 정보를 스마트 미터에 전달하여 도 6의 과정을 반복한다. 한편 일정한 시간이 경과하여 보안성을 높이기 위해 키 재설정이 필요한 경우에도 제어 서버는 새로운 정책을 스마트 미터에 전달할 수 있다.

[0055] 도 7은 스마트 그리드 시스템에서 정보를 수집하는 방법(400)에 대한 순서도의 예이다. 제어 서버는 복수의 스마트 미터에 계층적 구조를 형성하기 위한 정책을 전달한다(410). 복수의 스마트 미터는 제어 서버의 정책에 따라 계층적 구조를 형성한다(420).

[0056] 제어 서버는 전술한 바와 같이 TESLA 기법으로 기본 키 체인을 생성하고, 생성한 기본 키 체인을 상위 계층 스마트 미터에 분배한다(430). 상위 계층 스마트 미터는 기본 키 체인 요소 중 어느 하나의 임의의 이진 비트 (nonce)를 사용하여 시드 키를 생성할 수 있다(440). 상위 계층 스마트 미터는 전술한 바와 같이 생성한 시드 키를 기준으로 그룹 키 체인을 생성하고, 이를 그룹 스마트 미터에 분배한다(450).

[0057] 이제 하위 계층 스마트 미터는 전기 기기로부터 수집한 정보(전력 사용량 등)를 그룹 키 체인의 요소 중 하나를 사용하여 암호화할 수 있다(460). 하위 계층 스마트 미터는 타임 슬롯을 기준으로 특정 요소를 추출하거나, 자신의 식별자를 기준으로 특정 요소를 추출할 수도 있다. 예컨대, 그룹에 포함된 스마트 미터의 순번에 따라 그룹 키 체인의 시작값에서 몇 번 해싱을 할지를 결정할 수 있다. 상위 계층 스마트 미터는 하위 계층 스마트 미터가 수집한 정보를 취합하여 유틸리티 시스템에 전달한다(470).

[0058] 유틸리티 시스템은 전술한 바와 같이 복호에 필요한 정보를 이용하여 암호화된 정보를 복호할 수 있다(480). 또 유틸리티 시스템은 전력 사용량을 분석하여 일정한 제어 정보를 제어 서버에 전달할 수 있다.

[0060] 본 실시예 및 본 명세서에 첨부된 도면은 전술한 기술에 포함되는 기술적 사상의 일부를 명확하게 나타내고 있는 것에 불과하며, 전술한 기술의 명세서 및 도면에 포함된 기술적 사상의 범위 내에서 당업자가 용이하게 유추할 수 있는 변형 예와 구체적인 실시예는 모두 전술한 기술의 권리범위에 포함되는 것이 자명하다고 할 것이다.

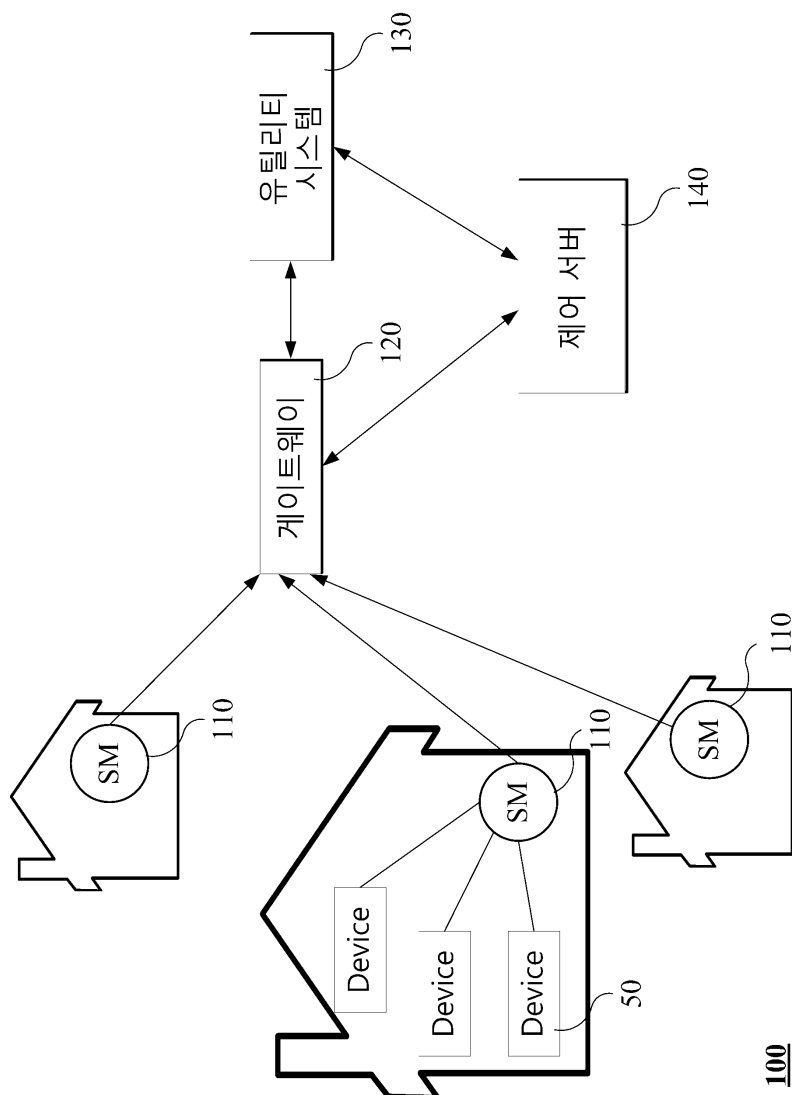
부호의 설명

[0061] 100 : 스마트 그리드 시스템
110 : 스마트 미터
120 : 게이트웨이

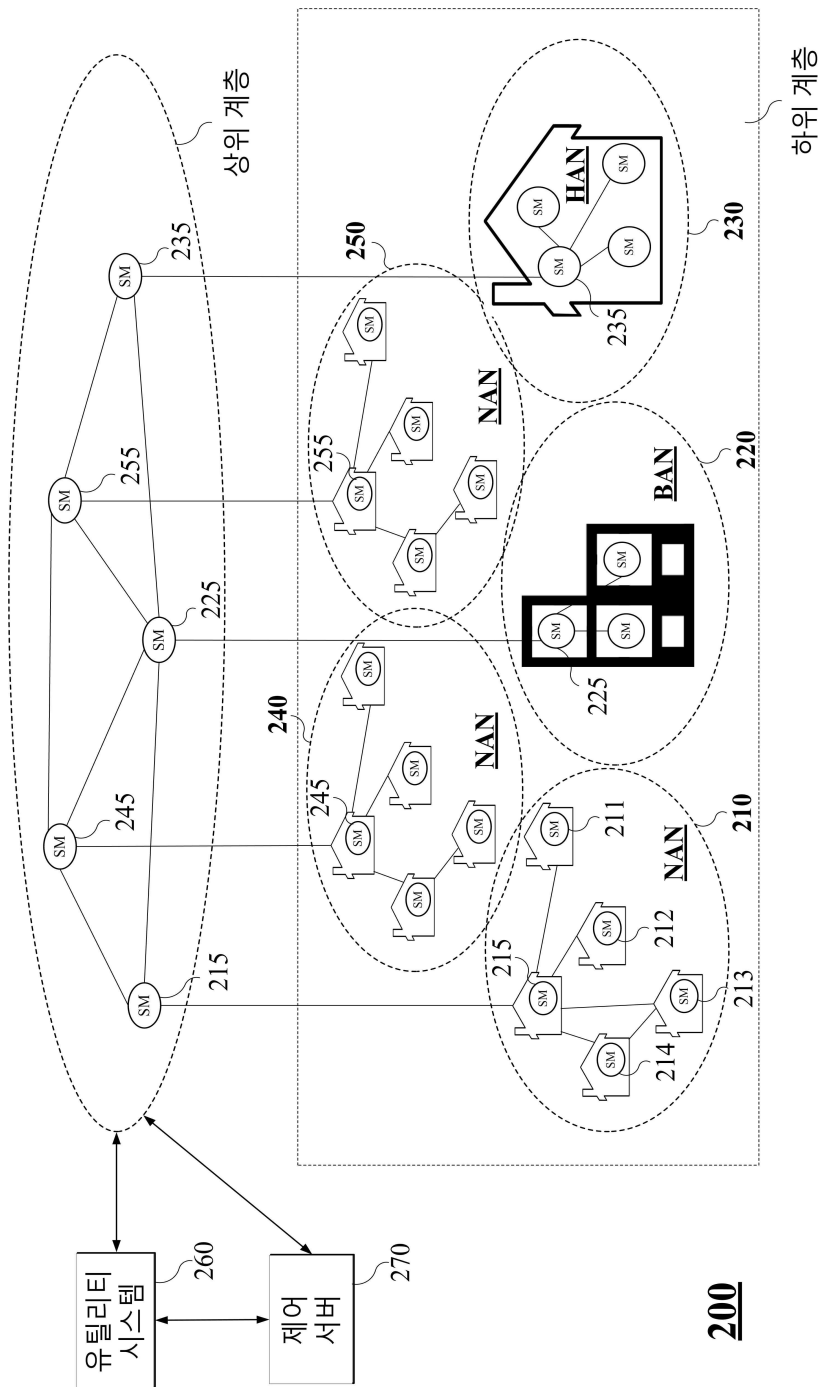
- 130 : 유틸리티 시스템
- 140 : 제어 서버
- 200 : 스마트 그리드 시스템
- 210 : 네트워크
- 211, 212, 213, 214, 215, 225, 235, 245, 255 : 스마트 미터
- 260 : 유틸리티 시스템
- 270 : 제어 서버

도면

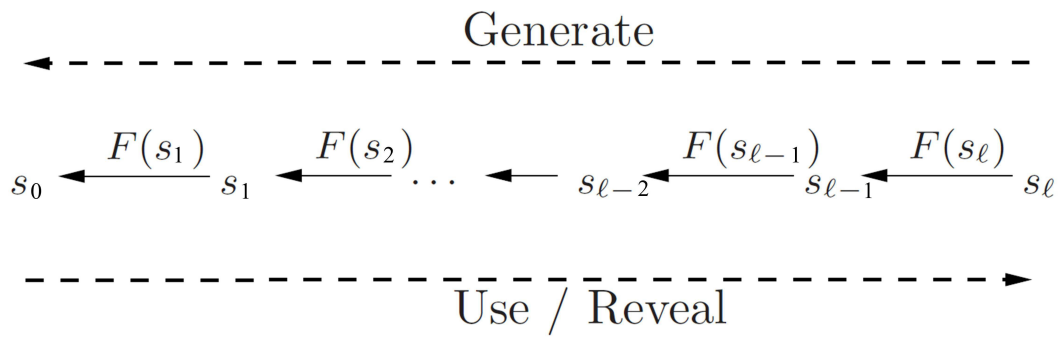
도면1



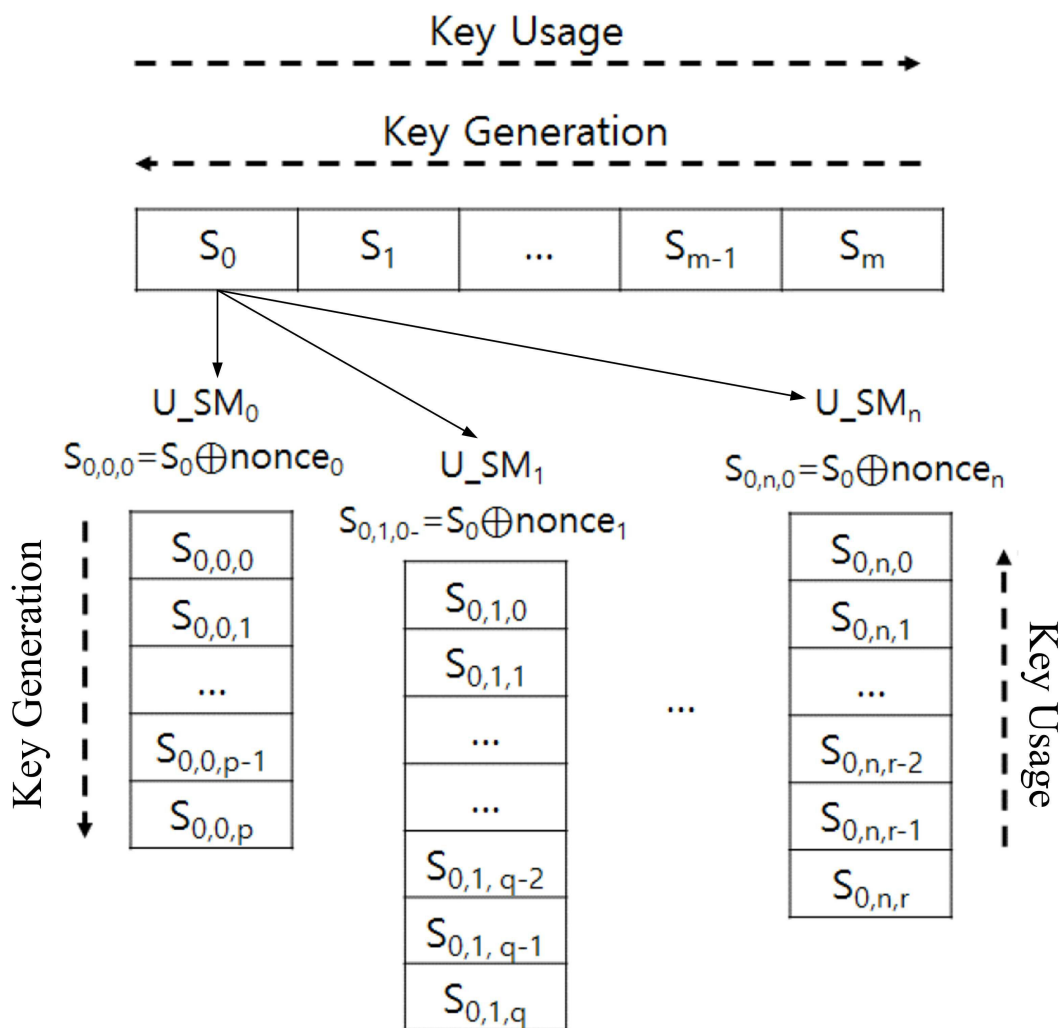
도면2



도면3



도면4

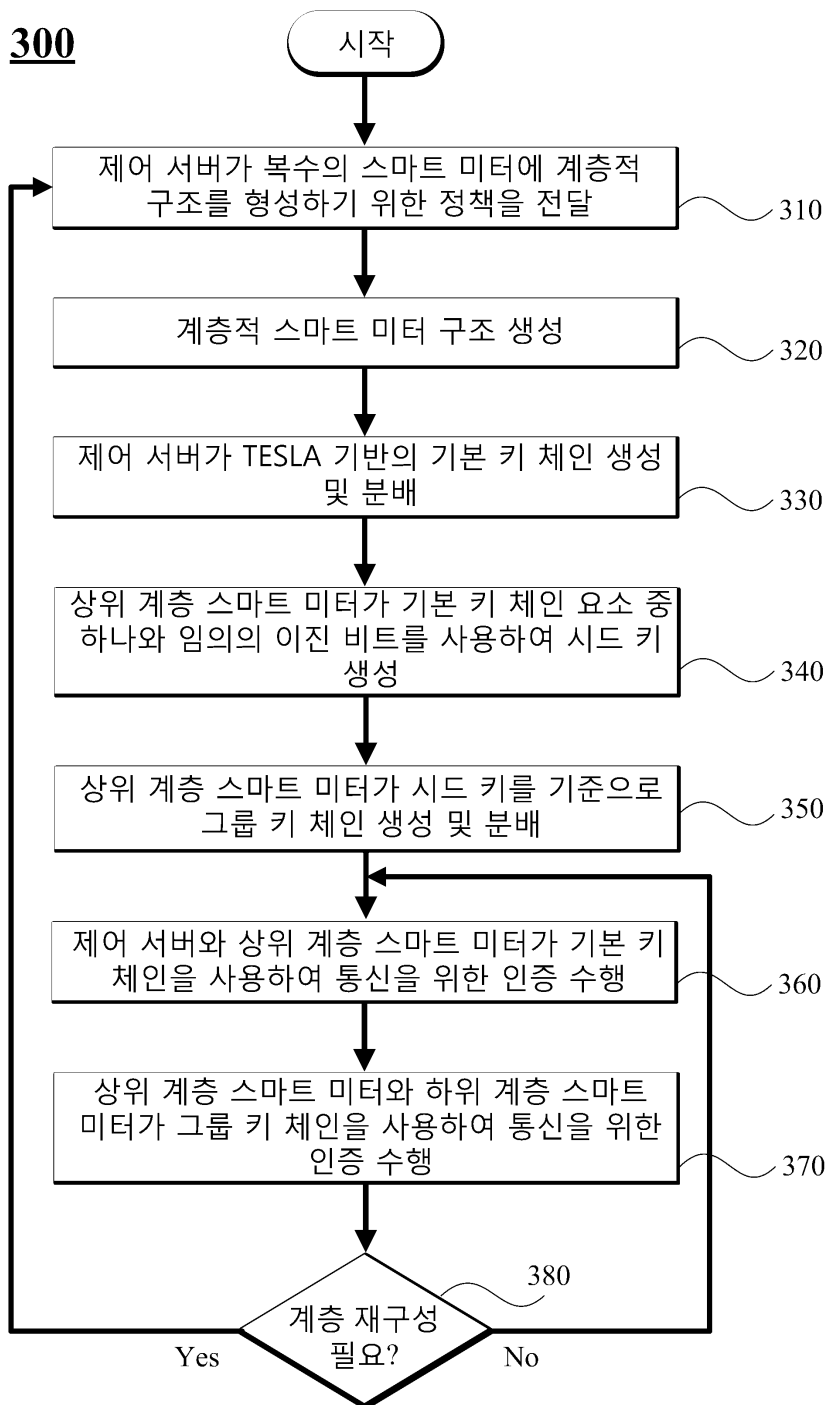


도면5

Time Slot	Keys used	
	Between Utility and U_SM	Between U_SM and L_SM
Slot 0	S_0	$S_{0,n,0} \sim S_{0,n,r}$
Slot 1	S_1	$S_{1,n,0} \sim S_{1,n,r}$
Slot 2	S_2	$S_{2,n,0} \sim S_{2,n,r}$
...	...	...
Slot m	S_m	$S_{m,n,0} \sim S_{m,n,r}$

도면6

300



도면7

