(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2014년06월02일
(11) 등록번호 10-1403221
(24) 등록일자 2014년05월27일

(51) 국제특허분류(Int. Cl.)
G08C 17/02 (2006.01)
(21) 출원번호 10-2013-0064533
(22) 출원일자 2013년06월05일
심사청구일자 2013년06월05일
(56) 선행기술조사문헌
US20130003603 A1
KR1020010074910 A

(73) 특허권자
이화여자대학교 산학협력단
서울특별시 서대문구 이화여대길 52 (대현동, 이화여자대학교)
(72) 발명자
리, 시
서울특별시 서대문구 이화여대길 52
채기준
서울 강남구 강남대로136길 34, 402호 (논현동, 월드노블레스빌)
최경
서울 서대문구 통일로34길 43, 109동 201호 (홍제동, 홍제원현대아파트)
(74) 대리인
특허법인무한

전체 청구항 수 : 총 10 항 심사관 : 조광현

(54) 발명의 명칭 **스마트 그리드 환경에서 링 통신 구조와 수직코드를 사용한 유틸리티 사용량 측정 시스템 및 방법**

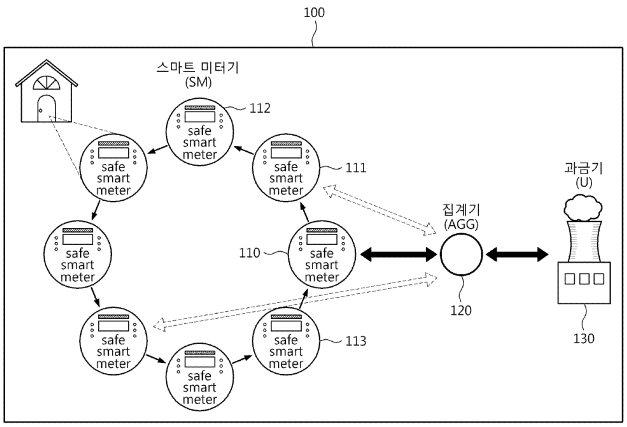
(57) 요 약

가입자(subscriber)의 유틸리티 사용량을 측정하여 측정 데이터를 얻고, 수직코드로 측정 데이터를 연산하여 연산 데이터를 얻는다. 연산 데이터를 집계기로 전송하고, 집계기를 통해 수신된 연산 데이터를 기반으로 하여 측정 데이터를 복원하며, 측정 데이터에 따라 개별 가입자에 대한 유틸리티 빌링을 수행하는 링 통신 구조(Ring Communication Architecture)와 수직코드(Ortho Code)를 사용한 유틸리티 사용량 측정 시스템 및 방법이 개시된다.

스마트 그리드를 위협하는 스누핑 공격(snooping attack), 수정공격(modification attack), 위장공격(masquerading attack), 재생공격(replaying attack)을 방지할 수 있으며, 적은 지연과 낮은 패킷 드롭 속도(low packet drop rate)를 달성할 수 있다.

유틸리티 사용량 측정 시스템 및 방법은 기밀성, 완전성 및 개인정보 보호 정책을 포함하는 보안 목표를 달성할 수 있다.

대 표 도



이 발명을 지원한 국가연구개발사업

과제고유번호	1345196379
부처명	교육과학기술부
연구사업명	WCU-1차선정-유형3
연구과제명	임베디드소프트웨어 분야 연구기반 구축 및 특성화
기 여 율	1/1
주관기관	이화여자대학교
연구기간	2008.12.01 ~ 2013.08.31

특허청구의 범위

청구항 1

하나 이상의 가입자에 대한 유틸리티 사용량 측정 시스템에서,

링 토폴로지 네트워크에 연결되고, 개별 가입자의 유틸리티 사용량을 측정하여 측정 데이터를 얻고, 수직코드로 상기 측정 데이터를 연산하여 연산 데이터를 얻는 하나 이상의 스마트 미터기 - 상기 수직코드는 상기 스마트 미터기 각각에 대해서 할당되어 있음 -;

상기 링 토폴로지 네트워크에 연결된 최말단 스마트 미터기로부터 상기 연산 데이터를 수신하고, 상기 연산 데이터를 집계기 수직코드를 이용하여 연산하는 집계기; 및

상기 집계기로부터 상기 각각의 스마트 미터기에 관련된 상기 연산 데이터를 수신하고, 상기 연산 데이터를 기반으로 하여 과금기 수직코드를 이용하여 상기 측정 데이터를 복원하며, 상기 측정 데이터에 따라 상기 개별 가입자에 대한 유틸리티 빌링을 수행하는 과금기

를 포함하는 유틸리티 사용량 측정 시스템.

청구항 2

제1항에 있어서,

상기 유틸리티 사용량 측정 시스템의 제1 스마트 미터기는 제1 연산 데이터를 제2 스마트 미터기로 전송하고, 상기 제2 스마트 미터기는 상기 제1 스마트 미터기로부터 수신한 상기 제1 연산 데이터를 복원하고, 상기 복원된 데이터와 상기 제2 스마트 미터기에서 얻은 제2 측정 데이터를 제2 수직코드로 연산하여 제2 연산 데이터를 얻는 유틸리티 사용량 측정 시스템.

청구항 3

제2항에 있어서,

상기 링 토폴로지 네트워크에는 n개의 스마트 미터기가 연결되어 있고,

상기 제1 스마트 미터기는 n번째 스마트 미터기의 제n 연산 데이터를 수신하고, 선정된 보안번호를 이용하여 다이제스트를 계산하며, 상기 제n 연산 데이터와 상기 다이제스트를 상기 집계기로 전송하는 유틸리티 사용량 측정 시스템.

청구항 4

제1항에 있어서,

상기 스마트 미터기는 일정시간 간격으로 전력 사용량을 측정하는 것을 특징으로 하는

유틸리티 사용량 측정 시스템.

청구항 5

제1항에 있어서,

상기 스마트 미터기는 상기 과금기와 공유하는 보안번호를 더 이용하여 상기 연산 데이터를 연산하는 유틸리티 사용량 측정 시스템.

청구항 6

제1항에 있어서,

상기 집계기는 상기 연산 데이터를 수직코드 매트릭스와 연산하여 새로운 매트릭스를 생성하고, 제2 다이제스트를 계산하는 유틸리티 사용량 측정 시스템.

청구항 7

제1항에 있어서,

상기 과금기는 상기 개별 가입자에 대해 수행된 상기 유틸리티 빌링 관련 데이터를 수직코드를 이용하여 피드백 데이터를 생성하고,

상기 집계기는 상기 피드백 데이터를 수신하여 상기 링 토폴로지 네트워크에 연결된 상기 스마트 미터기로 전송하는 유틸리티 사용량 측정 시스템.

청구항 8

하나 이상의 가입자에 대한 유틸리티 사용량 측정 시스템에서, 상기 가입자 단에 설치되는 스마트 미터기에 있어서,

링 토폴로지 네트워크에 연결되는 네트워크 어댑터;

상기 가입자의 상기 유틸리티 사용량을 측정하여 측정 데이터를 얻는 측정부; 및

수직코드로 상기 측정 데이터를 연산하여 연산 데이터를 얻는 연산부를 포함하고,

상기 유틸리티 사용량 측정 시스템에는 둘 이상의 스마트 미터기가 설치되며, 상기 스마트 미터기 각각에 대해서 각각의 수직코드가 부여되어 있고, 상기 유틸리티 사용량 측정 시스템의 제1 스마트 미터기는 제1 연산 데이터를 제2 스마트 미터기로 전송하고, 상기 제2 스마트 미터기는 상기 제1 스마트 미터기로부터 수신한 상기 제1 연산 데이터를 복원하고, 상기 복원된 데이터와 상기 제2 스마트 미터기에서 얻은 제2 측정 데이터를 제2 수직코드로 연산하여 제2 연산 데이터를 얻는 스마트 미터기.

청구항 9

제8항에 있어서,

상기 연산부는 상기 스마트 미터기에 해당하는 수직코드를 이용하여 상기 측정 데이터를 연산하고, 상기 스마트 미터기에 선정된 이동 비트수만큼 연산 결과를 천이시키며, 상기 천이된 연산 결과를 상기 제2 스마트 미터기로 전송하는 스마트 미터기.

청구항 10

하나 이상의 가입자에 대한 유틸리티 사용량 측정 방법에 있어서,

상기 가입자의 상기 유틸리티 사용량을 측정하여 측정 데이터를 얻는 단계;

수직코드로 상기 측정 데이터를 연산하여 연산 데이터를 얻는 단계;

상기 연산 데이터를 집계기로 전송하는 단계;

상기 집계기를 통해 수신된 상기 연산 데이터를 기반으로 하여 상기 측정 데이터를 복원하며, 상기 측정 데이터에 따라 상기 개별 가입자에 대한 유틸리티 빌링을 수행하는 단계;

둘 이상의 스마트 미터기가 설치되어 링 토폴로지 네트워크에 연결되어 있고, 상기 스마트 미터기 각각에 대해서 각각의 수직코드가 부여되어 있는 상기 유틸리티 사용량 측정 시스템에서, 제1 스마트 미터기는 제1 연산 데이터를 제2 스마트 미터기로 전송하는 단계;

상기 제2 스마트 미터기는 상기 제1 스마트 미터기로부터 수신한 상기 제1 연산 데이터를 복원하는 단계; 및

상기 복원된 데이터와 상기 제2 스마트 미터기에서 얻은 제2 측정 데이터를 제2 수직코드로 연산하여 제2 연산 데이터를 얻는 단계를 포함하는 유틸리티 사용량 측정 방법.

명 세 서

기 술 분 야

[0001] 링 통신 구조(Ring Communication Architecture; RCA)를 기반으로 가입자의 개인정보를 보호하기 위해 스마트 그리드 환경에서, 수직코드(Ortho Code)를 사용한 효율적인 유틸리티 사용량 측정 시스템 및 방법이 개시된다.

배 경 기 술

[0002] 스마트 미터란 주변 지능(Advanced Metering Infrastructure; AMI)를 구축하는 데 있어서 이종의 네트워크 시스템과 인터페이스를 지원하는 통신 시스템과 함께 AMI를 구성하는 핵심 설비이다. 미터(Meter)는 통상적으로 미터링(계량)을 위한 계량설비를 나타내는 말로, 스마트 그리드 시스템 기술에서 설명되고 있는 미터(Meter)는 주로 전력량계를 의미한다.

[0003] 스마트 미터링 기술은 현재의 집중화된 전력 공급망의 한계를 극복하고 공해배출의 억제 및 전력 효율의 향상을 도모할 수 있는 미래 혁신형 기술이라 할 수 있으며, 또한 전력 사용자의 전력에너지의 효율적인 이용과 재생에너지와 같은 다양한 전력공급방식 환경변화에 대해 사용자 입장에서 전력 수용변화에 대체하는 기술이다. 인텔리그리드와 스마트 그리드 등의 기술과 연계하여 발전되고 있는 전력 정보통신 기술의 일부분으로 단위 시스템으로 구분한다면, 지능형 전력량계(Smart Meter)와 지능형 통신 시스템(Intelligent Communication System)으로 구분할 수 있다.

[0004] 미터링 데이터 전송 시스템과 관련된 연구가 지속되어 왔다. 예를 들면, 선행기술로 미터링 데이터 전송 시스템, 이를 위한 방법, 이를 위한 장치 및 이 방법이 기록된 컴퓨터로 판독 가능한 기록 매체(특허공개번호 2013-0000062)가 있다.

[0005] 선행기술의 내용은 미터링 데이터 전송 시스템, 이를 위한 방법, 이를 위한 장치 및 이 방법이 기록된 컴퓨터로 판독 가능한 기록 매체에 관한 것으로, 수도, 가스, 전기 등의 에너지 사용에 따라 검침되는 미터링 데이터를 다양한 네트워크 토폴로지에 의해 수집할 수 있다. 이를 통해, 검침장치와 중계장치 간의 스타형 네트워크를 구성하는 경우, 미터링 데이터에 대한 신뢰도가 높아지며, 중계장치가 자체 라우팅 기능을 구현할 필요가 없어 장치의 단가를 줄일 수 있다. 또한, 관리장치가 다수의 중계장치와 메쉬형 네트워크를 구성하여 미터링 데이터를 수집함으로써, 수집된 미터링 데이터에 대한 신뢰도가 향상된다. 이러한 선행기술의 내용에는 측정 데이터가 공격자에게 노출되는 위험이 있어 가입자의 개인정보의 보호에 미흡한 점이 있다.

발명의 내용

해결하려는 과제

[0006] 제어 센터가 가입자의 전력 사용량에 따라 전력 분배를 관리할 때 다양한 개인 정보 보호 문제가 일상적으로 발생한다. 가입자의 전력 사용량은 자동으로 스마트 그리드 시스템의 스마트 미터에 의해 전송된다. 전력 사용량과 같은 데이터 전송이 공격자에게 노출되는 것을 방지하기 위한 강력한 보안기술 적용이 필요하다. 이를 위해, RCA(Ring Communication Architecture)를 기반으로 가입자의 개인정보를 보호하기 위해 스마트 그리드 환경에서 수직코드(Ortho Code)를 사용하여 효율적인 유틸리티 사용량 측정 시스템 및 방법이 개시된다.

[0007] 일실시예에 따르면, 가입자(subscriber)의 유틸리티 사용량을 측정하여 측정 데이터를 얻고, 수직코드로 측정 데이터를 연산하여 연산 데이터를 얻는다. 연산 데이터를 집계기로 전송하고, 집계기를 통해 수신된 연산 데이터를 기반으로 하여 측정 데이터를 복원하며, 측정 데이터에 따라 개별 가입자에 대한 유틸리티 빌링을 수행하는 링 통신 구조와 수직코드를 사용한 유틸리티 사용량 측정 시스템 및 방법이 개시된다.

[0008] 일실시예에 따르면, 스마트 그리드 환경에서 링 통신 구조와 수직코드를 사용한 유틸리티 사용량 측정 시스템의 구성 중 수직코드를 이용하여 측정된 데이터를 연산하는 스마트 미터기가 제공된다.

과제의 해결 수단

[0009] 일실시예에 따르면, 하나 이상의 가입자에 대한 유틸리티 사용량 측정 시스템은, 링 토폴로지(topology) 네트워크에 연결되고, 개별 가입자(subscriber)의 유틸리티 사용량을 측정하여 측정 데이터를 얻고, 수직코드로 측정 데이터를 연산하여 연산 데이터를 얻는 하나 이상의 스마트 미터기를 포함한다. 수직코드는 스마트 미터기 각각에 대해서 할당되어 있다. 링 토폴로지 네트워크에 연결된 최말단 스마트 미터기로부터 연산 데이터를 수신하고, 연산 데이터를 집계기 수직코드를 이용하여 연산하는 집계기(aggregator)를 포함한다. 집계기로부터 각각의 스마트 미터기에 관련된 연산 데이터를 수신하고, 연산 데이터를 기반으로 하여 과금기 수직코드를 이용하여 측정 데이터를 복원하며, 측정 데이터에 따라 개별 가입자에 대한 유틸리티 빌링을 수행하는 과금기를 포함한다.

[0010] 일실시예에 따르면, 하나 이상의 가입자에 대한 유틸리티 사용량 측정 시스템에서 가입자 단에 설치되는 스마트

미터기는 링 토폴로지(topology) 네트워크에 연결되는 네트워크 어댑터를 포함한다. 가입자(subscriber)의 유틸리티 사용량을 측정하여 측정 데이터를 얻는 측정부를 포함하고 수직코드로 측정 데이터를 연산하여 연산 데이터를 얻는 연산부를 포함한다. 유틸리티 사용량 측정 시스템에는 둘 이상의 스마트 미터기가 설치되며, 스마트 미터기 각각에 대해서 각각의 수직코드가 부여되어 있고, 유틸리티 사용량 측정 시스템의 제1 스마트 미터기는 제1 연산 데이터를 제2 스마트 미터기로 전송하고, 제2 스마트 미터기는 제1 스마트 미터기로부터 수신한 제1 연산 데이터를 복원하고, 복원된 데이터와 제2 스마트 미터기에서 얻은 제2 측정 데이터를 제2 수직코드로 연산하여 제2 연산 데이터를 얻는다.

[0011] 다른 일실시예에 따르면, 하나 이상의 가입자에 대한 유틸리티 사용량 측정 방법은, 가입자(subscriber)의 유틸리티 사용량을 측정하여 측정 데이터를 얻는 단계와, 수직코드로 측정 데이터를 연산하여 연산 데이터를 얻는 단계와, 연산 데이터를 집계기로 전송하는 단계와, 집계기를 통해 수신된 연산 데이터를 기반으로 하여 측정 데이터를 복원하며, 측정 데이터에 따라 개별 가입자에 대한 유틸리티 빌링을 수행하는 단계와, 둘 이상의 스마트 미터기가 설치되어 링 토폴로지 네트워크에 연결되어 있고, 스마트 미터기 각각에 대해서 각각의 수직코드가 부여되어 있는 유틸리티 사용량 측정 시스템에서, 제1 스마트 미터기는 제1 연산 데이터를 제2 스마트 미터기로 전송하는 단계와, 제2 스마트 미터기는 제1 스마트 미터기로부터 수신한 제1 연산 데이터를 복원하는 단계 및 복원된 데이터와 제2 스마트 미터기에서 얻은 제2 측정 데이터를 제2 수직코드로 연산하여 제2 연산 데이터를 얻는 단계를 포함한다.

발명의 효과

[0012] 스마트 그리드 환경에서 링 통신 구조(Ring Communication Architecture)와 수직코드(Ortho Code)를 사용한 유틸리티 사용량 측정 시스템 및 방법이 제시된다.

[0013] 스마트 그리드를 위협하는 스누핑 공격(snooping attack), 수정공격(modification attack), 위장공격(masquerading attack), 재생공격(replaying attack)을 방지할 수 있으며, 적은 지연과 낮은 패킷 드롭 속도(low packet drop rate)를 달성할 수 있다.

[0014] 유틸리티 사용량 측정 시스템 및 방법은 기밀성, 완전성 및 개인정보 보호 정책을 포함하는 보안 목표를 달성할 수 있다.

도면의 간단한 설명

[0015] 도 1은 일실시예에 따른 스마트 그리드 환경에서 링 통신 구조와 수직코드를 사용한 유틸리티 사용량 측정 시스템의 구성을 개략적인 구성을 도시한 블록도이다.

도 2는 일실시예에 따른 스마트 그리드 환경에서 링 통신 구조와 수직코드를 사용한 유틸리티 사용량 측정 시스템의 구성의 스마트 미터기를 개략적인 구성을 도시한 블록도이다.

도 3은 일실시예에 따른 스마트 그리드 환경에서 링 통신 구조와 수직코드를 사용한 유틸리티 사용량 측정 시스템의 구성의 측정 전송 프로세스를 나타낸 블록도이다.

도 4는 일실시예에 따른 스마트 그리드 환경에서 링 통신 구조와 수직코드를 사용한 유틸리티 사용량 측정 시스템의 구성의 지불 전송 프로세스를 나타낸 블록도이다.

도 5는 일실시예에 따른 스마트 미터기의 수직코드를 나타낸다.

도 6은 일실시예에 따른 스마트 그리드 환경에서 링 통신 구조와 수직코드를 사용한 유틸리티 사용량 측정 시스템의 구성의 측정 전송 프로세스 중에 도 3에 도시된 Step 3을 상세히 설명하는 도면이다.

도 7은 일실시예에 따른 스마트 그리드 환경에서 링 통신 구조와 수직코드를 사용한 유틸리티 사용량 측정 시스템의 구성의 측정 전송 프로세스 중에 도 3에 도시된 Step 5를 상세히 설명하는 도면이다.

도 8은 일실시예에 따른 스마트 그리드 환경에서 링 통신 구조와 수직코드를 사용한 유틸리티 사용량 측정 시스템의 구성의 측정 전송 프로세스 중에 도 3에 도시된 Step 7을 상세히 설명하는 도면이다.

발명을 실시하기 위한 구체적인 내용

[0016] 이하에서, 본 발명의 일부 실시예, 구체적인 특징 및 이점들은 첨부도면에 의거한 다음의 상세한 설명으로 더욱 명백해질 것이다. 본 발명이 실시예들에 의해 제한되거나 한정되는 것은 아니다.

[0017] 이에 앞서, 본 명세서 및 청구범위에 사용된 용어나 단어는 발명자가 그 자신의 발명을 가장 최선의 방법으로 설명하기 위해 용어의 개념을 적절하게 정의할 수 있다는 원칙에 입각하여 본 발명의 기술적 사상에 부합하는 의미와 개념으로 해석되어야 할 것이다. 또한, 본 발명에 관련된 공지 기능 및 그 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는, 그 구체적인 설명을 생략하였음에 유의해야 할 것이다. 각 도면에 제시된 동일한 참조 부호는 동일한 부재를 나타낸다.

[0018] 도 1은 일실시예에 따른 스마트 그리드 환경에서 링 통신 구조와 수직코드를 사용한 유틸리티 사용량 측정 시스템의 구성을 개략적인 구성을 도시한 블록도이다.

[0019] 도 1을 참조하면 본 발명의 일실시예에 따른 유틸리티 사용량 측정 시스템(140)은 크게 스마트 미터기(110), 집계기(120) 및 과금기(130)을 포함한다.

[0020] 스마트 미터기(110)은 일반적으로 전기의 소비를 기록하는 전기 미터를 나타낸다. 스마트 미터기(110)는 한 시간 또는 적은 시간 간격에서 모니터링 및 과금 목적을 위해 일정 주기에 따라 과금기(130)와 통신한다. 가정의 에너지 모니터와 다르게, 스마트 미터기(110)는 원격으로 데이터를 수집할 수 있다. 이러한 자동 미터 검침은 전통적인 자동 미터기 검침과 다르다.

[0021] 링 통신 구조(RCA)에서, 한 개의 스마트 미터기(110)는 (각 가정에 대해 하나의 스마트 미터기가 있다) 다음 스마트 미터기(111)로 데이터를 전송한다. 스마트 미터기(111)는 스마트 미터기(110)가 유효 기간 내에 데이터를 다시 전송할 때까지 자신의 데이터를 수신한 데이터에 추가하고 결합된 결합 데이터를 다음 스마트 미터기(112)로 전송한다. 링 통신 구조에서 스마트 미터기(110)는 수신한 결합 데이터를 집계기(120)로 전송한다.

[0022] 집계기(120)는 선택된 스마트 미터기(110)로부터 전송된 결합 데이터를 수신하고 데이터를 과금기(130)로 전송한다. 집계기(120)는 선택된 스마트 미터기(110)를 통해 과금기(130)에서 연산한 빌링(billing) 데이터를 스마트 미터기(110) 로 전송할 수 있다.

[0023] 과금기(130)는 집계기(120)로부터 각 스마트 미터기(110, 111, 112, 113 등)에서 수집한 결합 데이터를 수신한다. 이러한 결합 데이터를 기반으로 하여, 과금기(130)는 각 스마트 미터기(110, 111, 112, 113 등)에 대응하는 각 가입자에 대한 과금을 수행한다. 과금기(130)는 집계기(120)를 통해서 각 스마트 미터기(110, 111, 112, 113 등)에 다시 빌링 데이터를 전송할 수 있다.

[0024] 유틸리티 사용량 측정 시스템(140)에서 스마트 미터기(110)는 링 토폴로지(topology) 네트워크에 연결되고, 개별 가입자(subscriber)의 유틸리티 사용량을 측정하여 측정 데이터를 얻고, 수직코드로 측정 데이터를 연산하여 연산 데이터를 얻는다. 링 토폴로지 네트워크에는 둘 이상의 스마트 미터기(110)가 포함된다. 수직코드는 각 스마트 미터기(110, 111, 112, 113 등)에 대해서 할당되어 있다.

[0025] 집계기(120)는 링 토폴로지 네트워크에 연결된 스마트 미터기(110)로부터 결합 데이터를 수신하고, 결합 데이터를 집계기(120) 수직코드를 이용하여 연산한다.

[0026] 과금기(130)는 집계기(120)로부터 각각의 스마트 미터기에 관련된 결합 데이터를 수신하고, 결합 데이터를 기반으로 하여 과금기(130) 수직코드를 이용하여 측정 데이터를 복원하며, 측정 데이터에 따라 개별 가입자가 이용한 유틸리티 사용량에 대한 빌링을 수행한다.

[0027] 유틸리티 사용량 측정 시스템(140)의 스마트 미터기(110)는 제1 연산 데이터를 스마트 미터기(111)로 전송하고, 스마트 미터기(111)는 스마트 미터기(110)로부터 수신한 제1 연산 데이터를 복원하고, 복원된 데이터와 스마트 미터기(111)에서 얻은 제2 측정 데이터를 제2 수직코드로 연산하여 제2 연산 데이터를 얻는다.

[0028] 유틸리티 사용량 측정 시스템(140)에서 링 토폴로지 네트워크에는 n개의 스마트 미터기가 연결될 수 있고, 스마트 미터기(110)는 n번째 스마트 미터기(113)의 제n 연산 데이터를 수신하고, 선정된(predetermined) 보안번호를 이용하여 다이제스트(digest)를 계산하며, 제n 연산 데이터와 다이제스트(digest)를 집계기(120)로 전송한다. 스마트 미터기들은 일정시간 간격으로 전력 사용량을 측정할 수 있다.

[0029] 유틸리티 사용량 측정 시스템(140)에서 스마트 미터기(110)는 과금기(130)와 공유하는 보안번호를 더 이용하여 결합 데이터를 연산한다. 집계기(120)는 결합 데이터를 수직코드 행렬과 연산하여 새로운 행렬을 생성하고, 제2 다이제스트를 계산한다. 과금기(130)는 개별 가입자에 대해 수행된 유틸리티 빌링 데이터를 수직코드를 이용하여 연산하여 피드백 데이터를 생성한다. 집계기(120)는 피드백 데이터를 수신하여 링 토폴로지 네트워크에 연결된 스마트 미터기(110)로 전송한다. 스마트 미터기(110)는 수신한 피드백 데이터를 수직코드를 이용하여

연산하여 빌링 데이터를 얻는다.

[0030] 도 2는 일실시예에 따른 스마트 그리드 환경에서 링 통신 구조와 수직코드를 사용한 유틸리티 사용량 측정 시스템의 구성의 스마트 미터기를 개략적인 구성을 도시한 블록도이다.

[0031] 도 2를 참조하면 본 발명의 일실시예에 따른 스마트 미터기(210)은 네트워크 어댑터(211), 측정부(212), 및 연산부(213)을 포함한다.

[0032] 네트워크 어댑터(211)는 링 토폴로지(topology) 네트워크에 연결된다.

[0033] 측정부(212)는 가입자(subscriber)의 유틸리티 사용량을 측정하여 측정 데이터를 얻는다. 연산부(213)는 수직코드로 측정 데이터를 연산하여 연산 데이터를 얻는다.

[0034] 유틸리티 사용량 측정 시스템(140)에는 둘 이상의 스마트 미터기(210)를 포함할 수 있다. 스마트 미터기(210) 각각에 대해서는 각각의 수직코드가 부여되어 있고, 유틸리티 사용량 측정 시스템의 스마트 미터기(110)는 제1 연산 데이터를 스마트 미터기(111)로 전송하고, 스마트 미터기(111)는 스마트 미터기(110)로부터 수신한 제1 연산 데이터를 복원하고, 복원된 데이터와 스마트 미터기(111)에서 얻은 제2 측정 데이터를 제2 수직코드로 연산하여 제2 연산 데이터를 생성한다.

[0035] 연산부(213)는 스마트 미터기(110)에 해당하는 수직코드를 이용하여 측정 데이터를 연산하고, 스마트 미터기(110)에 선정된(predetermined) 이동 비트 수만큼 연산 결과를 천이(shift) 시키며, 천이된 연산 결과를 스마트 미터기(111)로 전송한다.

[0036] 도 3은 일실시예에 따른 스마트 그리드 환경에서 링 통신 구조와 수직코드를 사용한 유틸리티 사용량 측정 시스템의 구성의 측정 전송 프로세스를 나타낸 블록도이다.

[0037] 하나 이상의 가입자에 대한 유틸리티 사용량 측정 방법에 있어서, 가입자(subscriber)의 유틸리티 사용량을 측정하여 측정 데이터를 얻고, 수직코드로 측정 데이터를 연산하여 연산 데이터를 얻는다. 연산 데이터를 집계기로 전송하고, 집계기를 통해 수신된 연산 데이터를 기반으로 하여 측정 데이터를 복원하며, 측정 데이터에 따라 개별 가입자에 대한 유틸리티 빌링을 수행한다.

[0038] 링 토폴로지 네트워크에는 둘 이상의 스마트 미터기(110)가 연결될 수 있고, 스마트 미터기(110) 각각에 대해서 각각의 수직코드가 부여되어 있다. 스마트 미터기(110)는 제1 연산 데이터를 스마트 미터기(111)로 전송한다. 스마트 미터기(111)는 스마트 미터기(110)로부터 수신한 제1 연산 데이터를 복원하고 복원된 데이터와 스마트 미터기(111)에서 얻은 제2 측정 데이터를 제2 수직코드로 연산하여 제2 연산 데이터를 얻는다.

[0039] 하다마드 코드(Hadamard code)에 기초한 월시 함수(Walsh function)는 수직코드를 생성하는 다양한 방법 중 하나이다. 월시 코드(Walsh code)의 모든 코드들은 서로 수직(orthogonal)_하다. 각 행은 크기 n의 월시 코드이다. 일반적으로 하다마드 행렬의 각 다음 단계는 하다마드 변환에 의한 전 단계로부터 생성된다. 하다마드 행렬은 다음 [수학식 1]과 같이 계산된다.

수학식 1

[0040] $$H_{2n}=\begin{pmatrix} Hn & Hn \\ Hn & \overline{Hn} \end{pmatrix}$$

[0041] 스마트 그리드 환경에서 링 통신 구조와 수직코드를 사용한 유틸리티 사용량 측정 시스템은 스마트 그리드 시스템의 효율성을 보장하고 가입자의 개인정보를 보호하기 위해 효율적인 구조 및 전송 메커니즘을 제안한다. 이러한 전송 메커니즘을 설명하기 전에 유틸리티 사용량 측정 시스템에 대한 주목해야 할 몇 가지 가정이 있다.

[0042] 유틸리티 사용량 측정 시스템은 스마트 미터기(310), 집계기(320) 및 과금기(330)를 포함한다. 사전 배포 단계 동안, 외부에 영향을 받지 않고 스마트 미터기(310), 집계기(320) 및 과금기(330)의 모든 구성요소가 보안 상 안전하다고 가정한다. 이 단계에서, 집계기(320)는 각 스마트 미터기(310, 340, 350, 360 등)에 보안번호 S를 배포한다. 보안번호S는 스마트 미터기(310)와 집계기(320) 사이에 다이제스트를 생성하기 위해 해쉬함수를 사용할 수 있다. 집계기(320)는 또한 각 스마트 미터기(310, 340, 350, 360 등)에 [표 1]에서 예시된 테이블을 배포한다. 상기 테이블에서는 각 시퀀스 인덱스와 관련된 랜덤 정수가 있다. 테이블에 있는 엘레멘트의 숫자

는 시스템에서 스마트 미터의 숫자와 같다.

표 1

[0043]

Index	1	2	3	4	5	6	7	8	...
Value	3	4	8	7	6	5	2	1	...

[0044] 과금기(340)는 보안 번호X와 각 스마트 미터기에 [표 2]를 배포한다. [표 2]는 [표 1]의 크기 절반이다.

표 2

[0045]

Index	1	2	3	4	...
Value	3	4	2	1	...

[0046] 집계기(320) 및 과금기(330)는 보안 번호 S를 공유한다고 가정한다. 보안 번호 S는 스마트 미터기(310)와 집계기(320) 사이에 다이제스트를 생성하기 위해 해쉬함수를 사용할 수 있다.

[0047] 제안된 메커니즘에 적합한 수직 벡터를 만들기 위해 월시 함수의 변환과 새로운 수직 벡터 수직코드를 생성하는 월시 코드의 생성 방법들을 채택할 수 있다.

[0048] 수직코드는 월시 코드의 변환 양식으로부터 유래한다. 집계기(320)는 첫 번째로 [수학식 1]을 사용하여 수직코드 행렬을 생성한다. 행렬의 수는 이 영역에서 스마트 미터기(310)의 숫자와 관련된다. 둘째로, 생성된 수직코드 행렬을 변환한다. 모든 1은 월시 코드에서+1로 대체될 수 있다. 모든 0은 -1로 대체될 수 있다. 집계기는 무작위로 행과 열의 순서를 변경하고, 이를 변경된 행렬에 저장한다. 마지막으로, 이 저장된 행렬은 수직코드 행렬로 사용될 수 있다.

[0049] 도 5에는 수직코드 행렬 생성의 일례가 도시되어 있다.

[0050] 스마트 미터기(310)는 링 토폴로지의 네트워크에 연결된다. 각 스마트 미터기(310, 340, 350, 360 등)는 이웃 스마트 미터기를 알고 있다. 집계기는 무작위로 첫 번째 스마트 미터기를 선택하고, 첫 번째 스마트 미터기와 통신을 한다. 집계기는 도 1에서 점선으로 도시된 것과 같이 첫 번째 스마트 미터기와 통신하는 또 다른 스마트 미터기를 선택한다. 과금기는 도 1에 도시된 바와 같이 집계기를 통해서 스마트 미터기와 통신을 할 수 있다.

[0051] 아래의 [표 3]은 메커니즘을 설명하기 위해 표기와 설명을 나열한다.

표 3

[0052]

표기	설명
SM_i	스마트 미터기 i
AGG	집계기
U	과금기
M_i	스마트 미터기 i의 측정
P_i	스마트 미터기 i의 지불
O_i	스마트 미터기 i의 수직코드
$[O_{AGG}]$	집계기에 의해 저장된 수직코드 행렬, 행렬의 각 열은 각 스마트 미터기의 수직코드다.
x	보안번호는 스마트 미터기 i와 과금기 사이에 공유한다.
v_i	정보는 스마트 미터기 사이에서 비트수에 의해 전송된다. 비트수는 천이시키며, 이 값은 표1로부터 얻는다.
v_k'	정보는 스마트 미터기와 집계기 사이에서 비트수에 의해 전송된다. 비트수는 천이되며, 표2로부터 얻는다.

Index v_i	표1에서 v_i값의 인덱스
Index v_k'	표2에서 v_k'값의 인덱스
$<S>_{right_shift_b}$	b 비트만큼 S를 오른쪽 천이
$<S>_{left_shift_b}$	b 비트만큼 S를 왼쪽 천이
$[O]_{up_shift_b}$	b 비트만큼 행렬 O를 위로 천이
$[O]_{down_shift_b}$	b 비트만큼 행렬 O를 아래로 천이
S^{left}	S의 왼쪽 절반 부분
S^{right}	S의 오른쪽 절반 부분
$[O]^{left}$	행렬O의 왼쪽 절반 부분
$[O]^{right}$	행렬O의 오른쪽 절반 부분
$Digest_{(S)}$	해쉬함수와 보안번호를 사용하여 S를 다이제스트
n	시스템에서 스마트 미터기의 수
SN_{SM_AGG}	스마트 미터기와 집계기 사이의 보안번호 공유
SN_{AGG_U}	집계기와 과금기 사이의 보안번호 공유

[0053] 다시 도 3을 참조하면, Step 1(311)에서 선택된 스마트 미터기(SM_i)(340)는 보안번호 x를 자신의 측정 M_i에 추가하고, 상기 스마트 미터기(SM_i)(340)는 (M_i+x)를 직교코드 O_i와 곱한다. 한편, 무작위로(randomly) 위 표 1로부터 v_k의 값을 선택하고 v_k 비트만큼 (M_i+x)×O_i를 오른쪽으로 천이시킨다.

[0054] Step 2(312)에서 상기 스마트 미터기(SM_i)(340)는 선택된 v_k의 인덱스 및 오른쪽 천이결과 (M_i+x)×O_i를 다음 스마트 미터기(SM_{i+1})(350)로 전송한다.

[0055] Step 3(313)에서 스마트 미터기(SM_i)(340)로부터 정보를 수신한 후, 수신한 인덱스를 기반으로 v_k에 해당하는 값을 찾기 위해 먼저 저장된 표 1을 확인한다. 수신한 v_k 비트만큼 (M_i+x)×O_i를 왼쪽으로 천이하여 (M_i+x)×O_i를 복구한다. 수신된 정보가 변형되었는지 확인하기 위해, 스마트 미터기(SM_{i+1})(350)은 (M_i+x)×O_i를 자신의 수직코드 O_{i+1}을 곱한다. (M_i+x)×O_i×O_{i+1}의 결과가 0이면 복구된 정보 (M_i+x)×O_i은 나중에 사용될 수 있다. 이는 복구된 정보가 변형되지 않음을 의미한다. 왜냐하면 두 수직코드 O_i과 O_{i+1}가 서로 수직하기 때문이다. 그렇지 않으면, 곱셈 결과는 0이 되지 않고, 복구된 결과는 드롭된다. 이 경우, 스마트 미터기(SM_{i+1})(350)은 스마트 미터기(SM_i)(340)에게 정보를 다시 보내라고 요청한다. 스마트 미터기(SM_{i+1})(350)은 집계기(320)에 비정상적인 이벤트를 알려준다. 스마트 미터기(SM_{i+1})(350)은 자신의 (M_{i+1}+x)×O_{i+1}의 결과를 계산하고 그것을 (M_i+x)×O_i+(M_{i+1}+x)×O_{i+1} 를 얻기 위해 스마트 미터기(SM_i)(340)의 복구된 결과에 더한다. 이러한 결과의 보안성 및 기밀성을 높이기 위해, 스마트 미터기(SM_{i+1})(350)은 무작위로 표 1로부터 v_{k+1}값을 선택하고 v_{k+1}비트만큼 (M_i+x)×O_i+(M_{i+1}+x)×O_{i+1}를 오른쪽 천이한다. Step 3(313)의 과정은 도 6에 상세히 도시되어 있다. 도 6은 일실시예에 따른 스마트 그리드 환경에서 링 통신 구조와 수직코드를 사용한 유틸리티 사용량 측정 시스템의 구성의 측정 전송 프로세스 중에 도 3에 도시된 Step 3을 상세히 설명하는 도면이다.

[0056] Step 4(314)에서 스마트 미터기(SM_{i+1})(350)은 v_{k+1}의 인덱스 값을 전송하고 (M_i+x)×O_i+(M_{i+1}+x)×O_{i+1}천이한 결과를 스마트 미터기(SM_{i+2})(360)로 전송한다. 다음 스마트 미터기들은 모두 같은 Step 3(313)와 Step 4(314)를 수행한다.

[0057] Step 5(315)에서 스마트 미터기(SM_i)(340)은 마지막 스마트 미터기(SM)으로부터 $<\sum_{i=1}^{n}(M_i+x)\times O_i>_{right_shift_v_i}$ 를 수신하고, 이 정보를 복원하기 위해 v_i 비트만큼 왼쪽으로 천이시킨다. 그

리고 $\sum_{i=1}^{n}(M_i + x) \times O_i$의 정확성을 확인하기 위해 부여된 수직코드 O_n을 곱한다. 선택된 스마트 미터기(SM_i)(340)는 무작위로 표 2로부터 v_i'값을 선택한다. $< (\sum_{i=1}^{n}(M_i + x) \times O_i)^{right} >_{right_shift_v'_1}$를 얻기 위해 v_i'비트만큼 $\sum_{i=1}^{n}(M_i + x) \times O_i$의 오른쪽 절반을 오른쪽으로 천이시킨다. 선택된 스마트 미터기(SM_i)(340)은 도 7에 도시된 바와 같이 SN_{SM_AGG}보안번호를 공유한 해쉬함수를 이용하여 다이제스트를 계산한다. 도 7은 일실시예에 따른 스마트 그리드 환경에서 링 통신 구조와 수직코드를 사용한 유틸리티 사용량 측정 시스템의 구성의 측정 전송 프로세스 중에 도 3에 도시된 Step 5를 상세히 설명하는 도면이다.

[0058] Step 6(316)에서 스마트 미터기(SM_i)(340)은 집계기로 다음과 같은 정보를 전송한다.

[0059] $$(\sum_{i=1}^{n}(M_i + x) \times O_i)^{left} \| < (\sum_{i=1}^{n}(M_i + x) \times O_i)^{right} >_{right_shift_v'_1} \| Index_{v'_1} \|$$

[0060] $$Digest((\sum_{i=1}^{n}(M_i + x) \times O_i)^{left} \| < (\sum_{i=1}^{n}(M_i + x) \times O_i)^{right} >_{righ_shift_v'_1} \| Index_{v'_1})$$

[0061] Step 7(317)에서 스마트 미터기(SM_i)(340)으로부터 정보를 받을 때, 집계기(320)는 처음에 해쉬함수를 이용하여 다이제스트를 확인하고, 보안번호S_{SM_AGG}를 공유한다. 정보가 부정확한 경우, 집계기(320)는 정보를 드롭하고 선택된 스마트 미터기(SM_i)(340)에게 재전송을 요청한다. 정보가 정확한 경우, 집계기(320)는 저장된 수직코드 행렬$[O_{AGG}]^{left}$의 왼쪽 절반을 사용하여 수신한 $(\sum_{i=1}^{n}(M_i + x) \times O_i)^{left}$를 곱한다. 그리고 나서 n으로 나눈다. n은 수직코드의 크기이다. 계산되는 과정은 [수학식 2]와 같다.

수학식 2

$$\begin{bmatrix} O_1 \\ O_2 \\ \vdots \\ O_n \end{bmatrix}^{left} \times (\sum_{i=1}^{n}(M_i + x) \times O_i)^{left} \div n$$

$$= \begin{bmatrix} O_1 \times (\sum_{i=1}^{n}(M_i + x) \times O_i) \\ O_2 \times (\sum_{i=1}^{n}(M_i + x) \times O_i) \\ \vdots \\ O_n \times (\sum_{i=1}^{n}(M_i + x) \times O_i) \end{bmatrix}^{left} \div n$$

$$= \begin{bmatrix} (M_1 + x) \times (|O_1|^2) \\ (M_2 + x) \times (|O_2|^2) \\ \vdots \\ (M_n + x) \times (|O_n|^2) \end{bmatrix}^{left} \div n$$

$$= \begin{bmatrix} (M_1 + x) \\ (M_2 + x) \\ \vdots \\ (M_n + x) \end{bmatrix}^{left}$$

[0062]

[0063] 이러한 과정을 통하여, 각 스마트 미터기(310, 340, 350, 360 등)의 (M_i+x)부분인 n을 얻은 후에, 집계기(320)는 이러한 n값을 사용하여 수직코드 행렬의 왼쪽 절반에 대응하는 것을 바꾼다. 그리고 n×(n/2+1)의 크기로 새로운 행렬$[O_{AGG_new}]$를 얻는다.

$$[O_{AGG_new}] = \begin{bmatrix} (M_1 + x)^{left} & O_1{}^{right} \\ (M_2 + x)^{left} & O_2{}^{right} \\ \vdots & \vdots \\ (M_n + x)^{left} & O_n{}^{right} \end{bmatrix}$$

[0064]

[0065] 집계기는(320) $[[[O_{AGG_new}]^{right}]_{right/left_shift_p}]_{up/down_shift_q}$ 와 $[[O_{AGG_new}]^{left}]_{up/down_shift_q}$ 를 얻기 위해 p비트만큼 새로운 행렬의 오른쪽 절반을 천이시키고 q비트만큼 위/아래 천이한다. 이러한 변화는 [표 4]과 같이 설명된다. 집계기(320)는 모든 정보의 다이제스트를 계산한다. 정보는 도 8에서처럼 보안번호 S_{AGG_U}를 공유한 해쉬함수에 의해 과금기(330)로 전송된다.

표 4

Time	Change Style	Change Bit
Timestamp 1	Up	q
	Down	
Timestamp 2	Left	p
	Right	

[0066]

[0067] Step 8(318)에서 집계기(320)는 과금기(330)로 다음과 같은 정보를 전송한다.

[0068] $<< (\sum_{i=1}^{n}(M_i + x) \times O_i)^{right} >_{right_shift_v'_1} >_{right/left_shift_p} \| \text{Index}_{v'_1} \|$

[0069] $\text{Timestamp} \| [[[O_{AGG_new}]^{right}]_{right/left_shift_p}]_{up/down_shift_q} \| [[O_{AGG_new}]^{left}]_{up/down_shift_q} \|$

[0070] $\text{Digest}(<< (\sum_{i=1}^{n}(M_i + x) \times O_i)^{right} >_{right_shift_v'_1} >_{right/left_shift_p} \| [[O_{AGG_new}]^{left}]_{up/down_shift_q}$

[0071] $\| \text{Index}_{v'_1} \| [[[O_{AGG_new}]^{right}]_{right/left_shift_p}]_{up/down_shift_q} \| \text{Timestamp})$

[0072] Step 9(319)에서 집계기(320)로부터 정보를 받은 후에 과금기(330)는 처음에 해쉬함수와 공유하는 보안번호 S_{AGG_U}를 사용하여 다이제스트를 체크한다. 계산된 다이제스트가 수신된 다이제스트와 다르면, 과금기(330)는 수신된 정보를 드롭하고, 집계기(320)에 재전송을 요청한다. 다이제스트가 정확한 경우, 수신된 정보는 나중에 사용된다. 수신된 행렬 오른쪽 절반으로부터 복구된 정보와 곱하고 원래의 수직코드 n의 크기에 의해서 곱의 결과를 나눈다. 계산 과정은 [수학식 3]과 같다.

수학식 3

$$[[[O_{AGG_new}]^{right}]_{right/left_shift_p}]_{up/down_shift_q} \times <(\sum_{i=1}^{n}(M_i + x) \times O_i)^{right}>_{right/left_shift_p} \div n$$

$$= \left[\left[\begin{matrix} O_1^{right} \\ O_2^{right} \\ \vdots \\ O_n^{right} \end{matrix}\right]_{right/left_shift_p}\right]_{up/down_shift_q} \times <(\sum_{i=1}^{n}(M_i + x) \times O_i)^{right}>_{right/left_shift_p} \div n$$

$$= \left[\left[\begin{matrix} O_1^{right} \times (\sum_{i=1}^{n}(M_i + x) \times O_i)^{right} \\ O_2^{right} \times (\sum_{i=1}^{n}(M_i + x) \times O_i)^{right} \\ \vdots \\ O_n^{right} \times (\sum_{i=1}^{n}(M_i + x) \times O_i)^{right} \end{matrix}\right]_{right/left_shift_p}\right]_{up/down_shift_q} \div n$$

$$= \left[\begin{matrix} ((M_1 + x) \times |O_1|^2)^{right} \\ ((M_2 + x) \times |O_2|^2)^{right} \\ \vdots \\ ((M_n + x) \times |O_n|^2)^{right} \end{matrix}\right]_{up/down_shift_q} \div n$$

$$= \left[\begin{matrix} (M_1 + x)^{right} \\ (M_2 + x)^{right} \\ \vdots \\ (M_n + x)^{right} \end{matrix}\right]_{up/down_shift_q}$$

[0073]

[0074] 과금기(330)는 위 결과를 수신한 값 $[[O_{AGG_new}]^{left}]_{up/down_shift_q}$ 과 더하고, 비밀 번호 x에 의해 각각의 이러한 결과를 공제(subtract)한다. [수학식 4]에서는 상기 계산된 값은 nSMs를 측정값과 같음을 보여준다.

수학식 4

$$\left[\begin{matrix} (M_1 + x)^{left} + (M_1 + x)^{right} \\ (M_2 + x)^{left} + (M_2 + x)^{right} \\ \vdots \\ (M_n + x)^{left} + (M_n + x)^{right} \end{matrix}\right]_{up/down_shift_q} - x$$

$$= \left[\begin{matrix} (M_1 + x) \\ (M_2 + x) \\ \vdots \\ (M_n + x) \end{matrix}\right]_{up/down_shift_q} - x$$

$$= \left[\begin{matrix} M_1 \\ M_2 \\ \vdots \\ M_n \end{matrix}\right]_{up/down_shift_q}$$

[0075]

[0076] 도 4는 일실시예에 따른 스마트 그리드 환경에서 링 통신 구조와 수직코드를 사용한 유틸리티 사용량 측정 시스템의 구성의 지불 전송 프로세스를 나타낸 블록도이다.

[0077] 지불 전송 프로세스에서 과금기(430)는 수신한 측정을 기준으로 하여 해당 결제를 생성할 수 있다. 과금기(430)는 측정 전송과정에서 지불의 부분과 관련된 합산 결과를 생성하기 위해 수직코드 행렬의 수신 절반을 사용하여 각 스마트 미터기(440)에 집계기를 통하여 지불 정보를 보낸다. 집계기(420)는 지불의 다른 부분에 관련된 또 다른 합산 결과를 생성하기 위해 전체 수직코드를 사용한다. 두 가지 지불 합산에 기반하여, 각 스마

트 미터기(440)는 자신의 수직코드에 의해 지불을 복구 할 수 있다. 전송 과정은 도 4에서 볼 수 있으며, 각 단계는 다음과 같이 설명된다.

[0078] 10단계(410)에서 과금기(430) 는 각 측정 M_i를 기반으로 Pi를 계산할 수 있다. 그리고 또한 보안번호 x에 의해 이러한 측정을 추가할 수 있다. 각 결과 (Pi+ x)를 두 부분으로 나눈다. 즉, $(P_i + x) = (P_i + x)^{part\,1} + (P_i + x)^{part\,2}$ 이다. 과금기(430)는 수신한 수직코드 s 행렬 $[[[O_{AGG_new}]^{right}]_{right/left_shift_p}]_{up/down_shift_q}$ 를 두 그룹으로 나눈다. 하나의 그룹은 위쪽 반이다. 즉, $[[[[O_{AGG_new}]^{right}]_{right/left_shift_p}]_{up/down_shift_q}]^{up}$ 이다. 다른 그룹은 아래쪽 반이다. 즉, $[[[O_{AGG_new}]^{right}]_{right/left_shift_p}]_{up/down_shift_q}]^{down}$ 이다. 이러한 두 행렬의 크기는 n/2×n/2이다. 각 그룹에서, 수직코드는 서로 직교한다. $(Pi+x)^{part2}$의 각 값은 대응하는 수직코드 $< O_i^{right} >_{right/left_shift_p}$ 에 의해 곱해질 수 있다. 그리고 이 코드를 사용하여 유틸리티는 M_i를 계산한다. 이미 결정된 같은 부분에서 대응하는 수직코드의 결과는 합해진다. 그리고 이러한 두 합산 과정의 계산은 다음과 같다.

[0079] $$Sum^{up}{}_{right/left_shift_p} = \sum_{i=1}^{\frac{n}{2}} ((< O_i^{right} >_{right/left_shift_p})^{up} \times (P_i + x)^{part\,2})$$

[0080] $$Sum^{down}{}_{right/left_shift_p} = \sum_{i=1}^{\frac{n}{2}} ((< O_i^{right} >_{right/left_shift_p})^{down} \times (P_i + x)^{part\,2})$$

[0081] 과금기(430)는 무작위로 표 2에서 v2'을 찾는다. 그리고 v2'비트만큼 두 합산을 왼쪽으로 천이시킨다. 과금기(430)는 다이제스트를 생성하기 위해 공유하는 보안번호 S_{AGG_U}와 해쉬함수를 사용한다.

[0082] Step 11(411)에서 과금기(430)는 $List^{up}$과 $List^{down}$ 두 그룹에서 수직코드 리스트, $< Sum^{up}{}_{right/left_shift_p} >_{left_shift_v_2'} \parallel < Sum^{down}{}_{right/left_shift_p} >_{left_shift_v_2'}$, $[(P_i+x)^{part1}]$ 값의 첫 번째 부분, 표2에서 v2'와 관련된 인덱스, 집계기(420)로부터 수신한 타임스탬프 및 다이제스트 결과를 집계기(420)에 전송한다.

[0083] Step 12(412)에서 집계기(420)는 다이제스트에 의해 수신된 정보의 정확성을 확인한다. 집계기(420)는 수신된 정보와 관련된 수직코드 행렬을 찾기 위해 타임스탬프(timestamp)를 표 4에서 사용하여 검색한다. 수신한 $List^{up}$과 $List^{down}$을 기반으로 하여 집계기(420)는 원래의 수직코드를 Sum^{up} 및 Sum^{down} 연결할 수 있다. 집계기는 원래의 수직코드 O_i에 대응하여 각 $(P_i+x)^{part1}$지불의 첫 부분을 곱한다. 집계기(420)는 이들 곱셈 결과를 각각 더한다. 표 4에 도시된 변화를 기반으로 하여, 집계기(420)는 수신한 합산을 왼쪽/오른쪽으로 천이시킨다. 집계기(420)는 스마트 미터기(440) 사이의 관계의 새로운 리스트를 생성한다. 그리고 두 합산을 $List^{up}$과 $List^{down}$을 기반으로 하여 계산한다.

[0084] Step 13(413)에서 상기 정보들은 집계기(420)에 의해 선택된 스마트 미터기(440)에 보내진다.

[0085] Step 14(414)에서 선택된 스마트 미터기(440)는 다이제스트를 확인하고 표 2를 참조한다. 표 2를 참조하여, 인덱스 v2'를 기반으로 하여, v2'수를 찾고, v2'비트만큼 수신한 두 합계를 오른쪽 천이한다. 그리고 나서 스마트 미터기(440)는 자신의 수직코드 O_i에 의해서 수신된 정보를 곱한다. 그리고 자신의 지불과 관련된 첫부분을 복구하기 위해 n으로 나눈다. 계산과정은 도 3에 도시된 측정 전송 프로세스의 Step 7(317)와 유사하다. 스마트 미터기(440)는 대응하는 합산을 찾기 위해 수신한 리스트를 확인한다. 그리고 나서 자신의 수직코드의 오른쪽 절반과 이 합산을 곱한다. 스마트 미터기(440)는 이러한 두 결과를 더한다. 그리고 나서 자신의 빌링 데이터를 얻기 위한 보안번호 x에 의해 P_i+x를 공제한다.

[0086] Step 15(415)에서 스마트 미터기(440)는 스마트 미터기(450)에 $Sum^{up} \parallel Sum^{down} \parallel List \parallel \sum_{k=1}^{n}(O_k \times (P_k + x)^{part\,1})$ 를 전송한다.

[0087] Step 16(416)에서 첫 번째 스마트 미터기(440)가 정보를 다시 받을 때까지, 스마트 미터기(460 등)는 Step 14(414)와 Step 15(415)를 반복한다. 그리고 나서 스마트 미터기(440)는 두 정보(예를 들면, 내 보낸 정보와 마지막 스마트 미터기로(460)부터 받은 정보)를 비교한다. 수신된 정보가 내 보낸 정보와 같다면, 스마트 미터기(440)는 모든 스마트 미터기(450, 460 등)에게 계산된 지불을 저장할 수 있다. 수신된 정보가 내 보낸 정보와 다르다면, 스마트 미터기(440)는 모든 스마트 미터기에게(450, 460 등) 계산된 지불은 잘못된 것이고 드롭되어야 한다고 알린다. 그러는 동안 스마트 미터기(440)는 Step 15(415)에서 수신한 다음 스마트 미터기 정보를 재전송한다.

[0088] 이상과 같이 본 발명은 비록 한정된 실시예와 도면에 의해 설명되었으나, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상의 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다.

[0089] 그러므로, 본 발명의 범위는 설명된 실시예에 국한되어 정해져서는 아니 되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등한 것들에 의해 정해져야 한다.

부호의 설명

[0090] 100: 유틸리티 사용량 측정 시스템

110, 111, 112, 113: 스마트 미터기

120: 집계기

130: 과금기

210: 스마트 미터기

211: 네트워크 어댑터

212: 측정부

213: 연산부

310, 340, 350, 360: 스마트 미터기

320: 집계기

330: 과금기

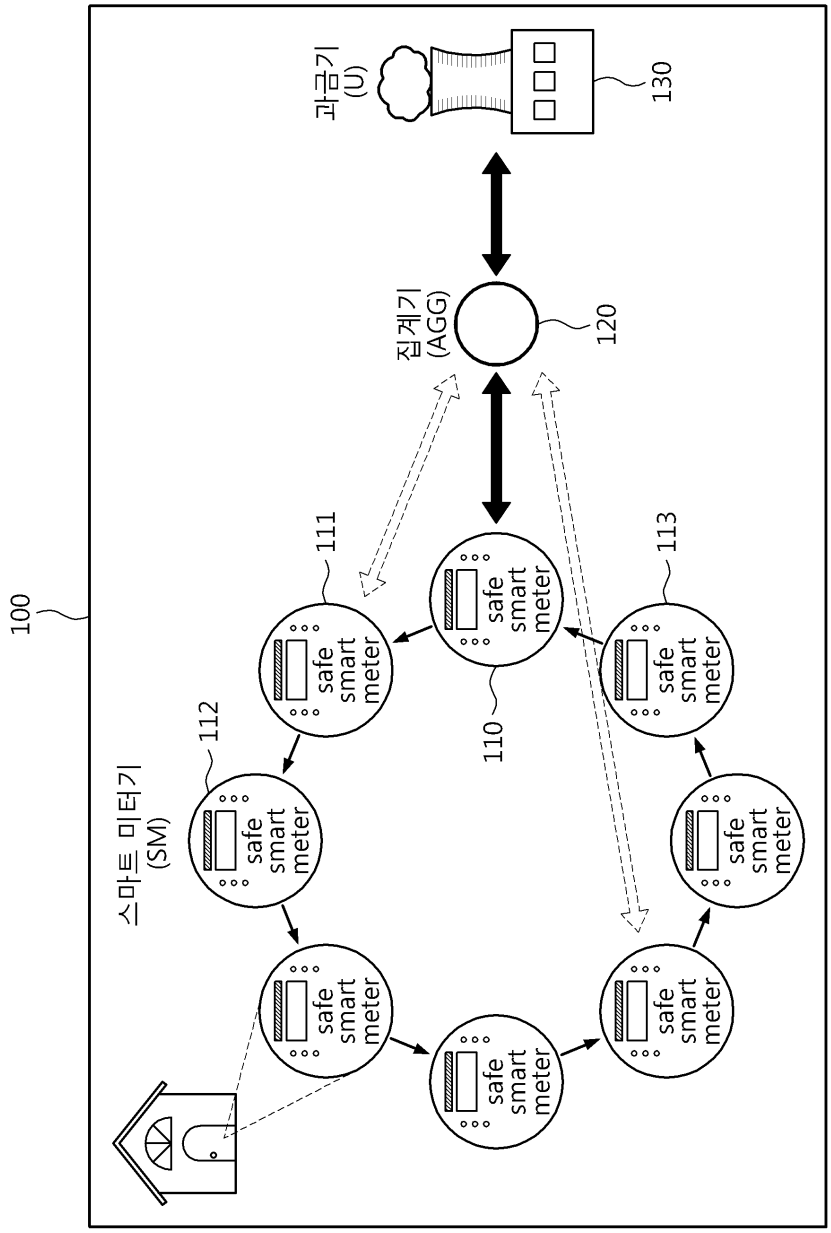
420: 집계기

430: 과금기

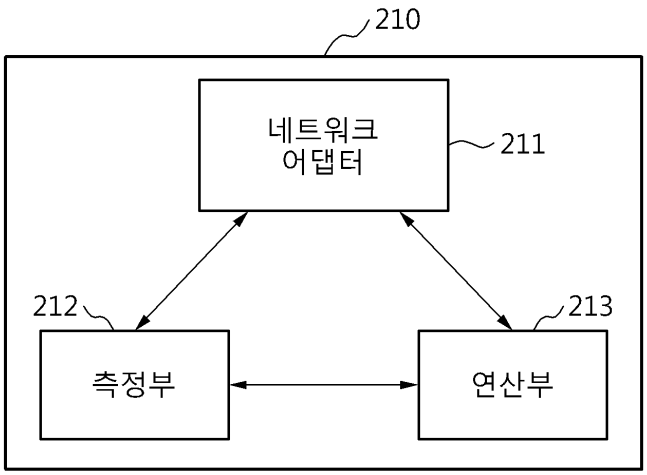
440, 450, 460: 스마트 미터기

도면

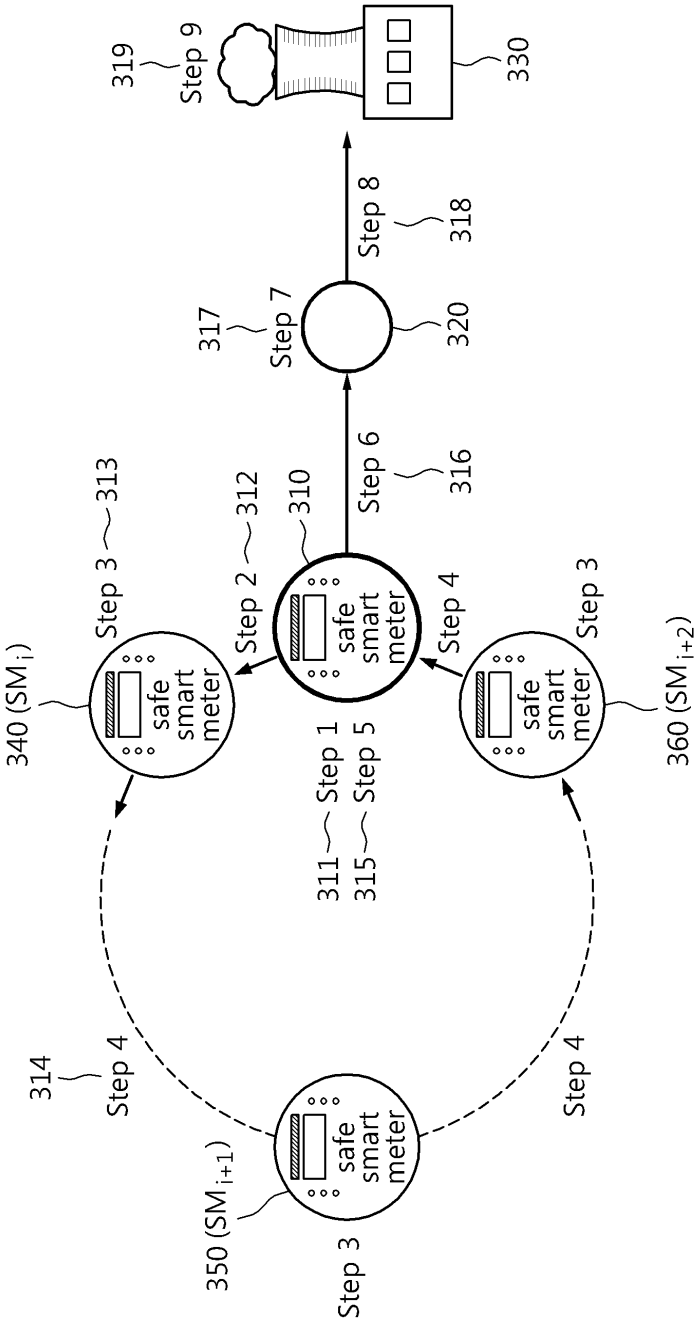
도면1


100
과금기
(U)
130
집계기
(AGG)
120
110
111
113
112
스마트 미터기
(SM)
safe
smart
meter

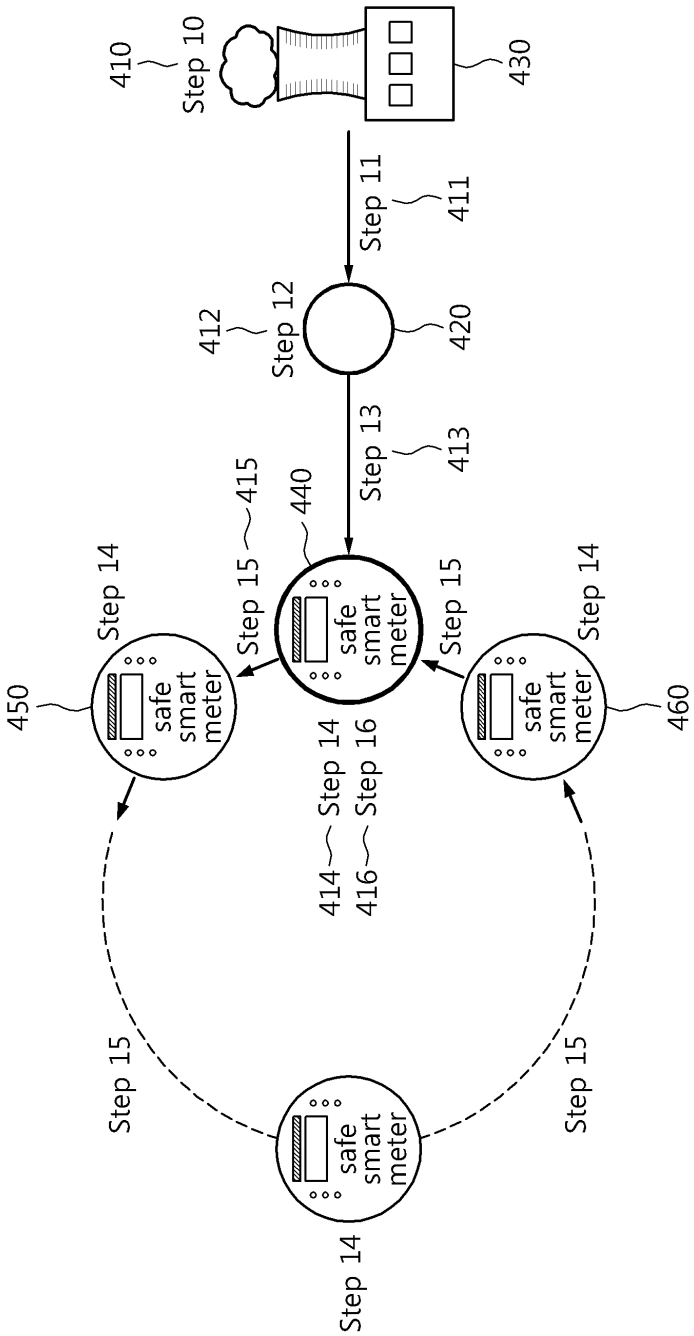
도면2



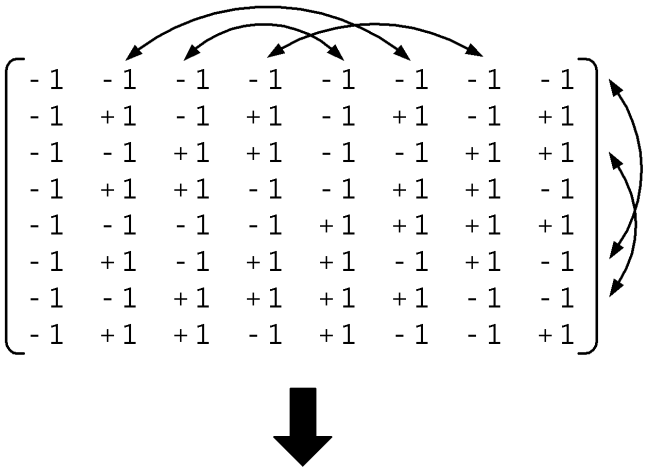
도면3


319
Step 9
330
Step 8
318
317
Step 7
320
Step 6
316
Step 3
313
Step 2
312
310
Step 4
Step 3
340 (SM$_i$)
safe smart meter
safe smart meter
safe smart meter
311
Step 1
315
Step 5
360 (SM$_{i+2}$)
314
Step 4
Step 4
350 (SM$_{i+1}$)
Step 3

도면4

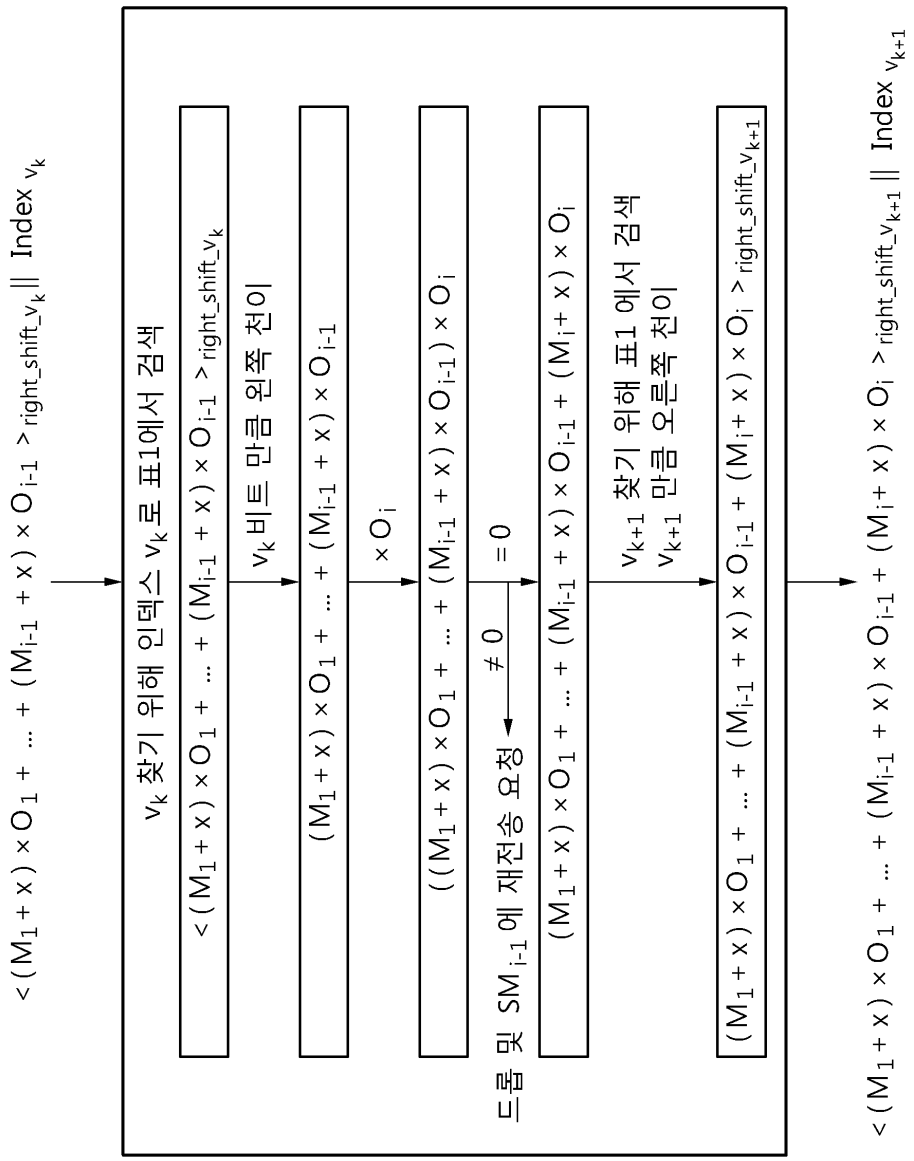

410
Step 10
430
Step 11
411
412
Step 12
420
Step 13
413
415
440
Step 15
Step 14
safe smart meter
450
460
414
Step 14
416
Step 16
Step 15

도면5

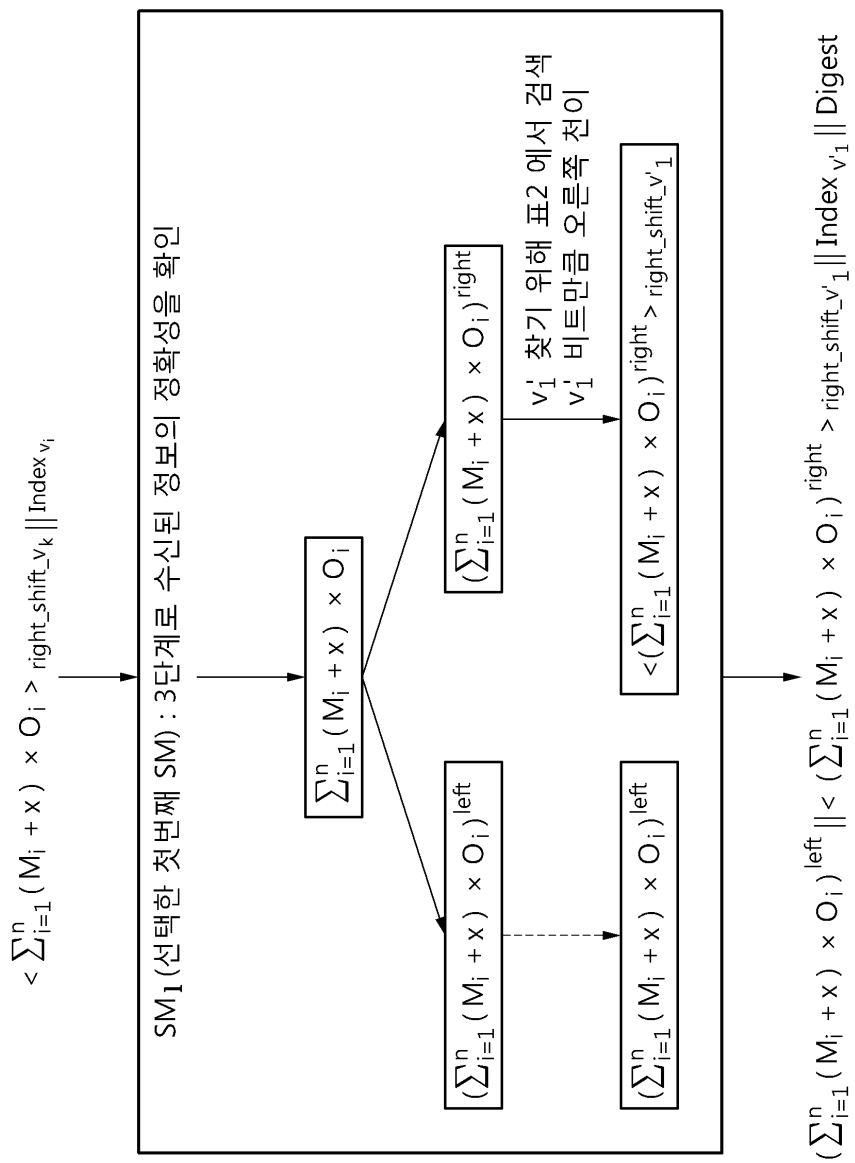


(-1 -1 +1 +1 -1 +1 +1 -1) → SM_1 의 수직코드
(-1 +1 -1 -1 -1 +1 +1 +1) → SM_2 의 수직코드
(-1 +1 +1 -1 +1 -1 +1 -1) → SM_3 의 수직코드
(-1 +1 -1 +1 +1 +1 -1 -1) → SM_4 의 수직코드
(-1 +1 +1 +1 -1 -1 -1 +1) → SM_5 의 수직코드
(-1 -1 -1 -1 -1 -1 -1 -1) → SM_6 의 수직코드
(-1 -1 -1 +1 +1 -1 +1 +1) → SM_7 의 수직코드
(-1 -1 +1 -1 +1 +1 -1 +1) → SM_8 의 수직코드

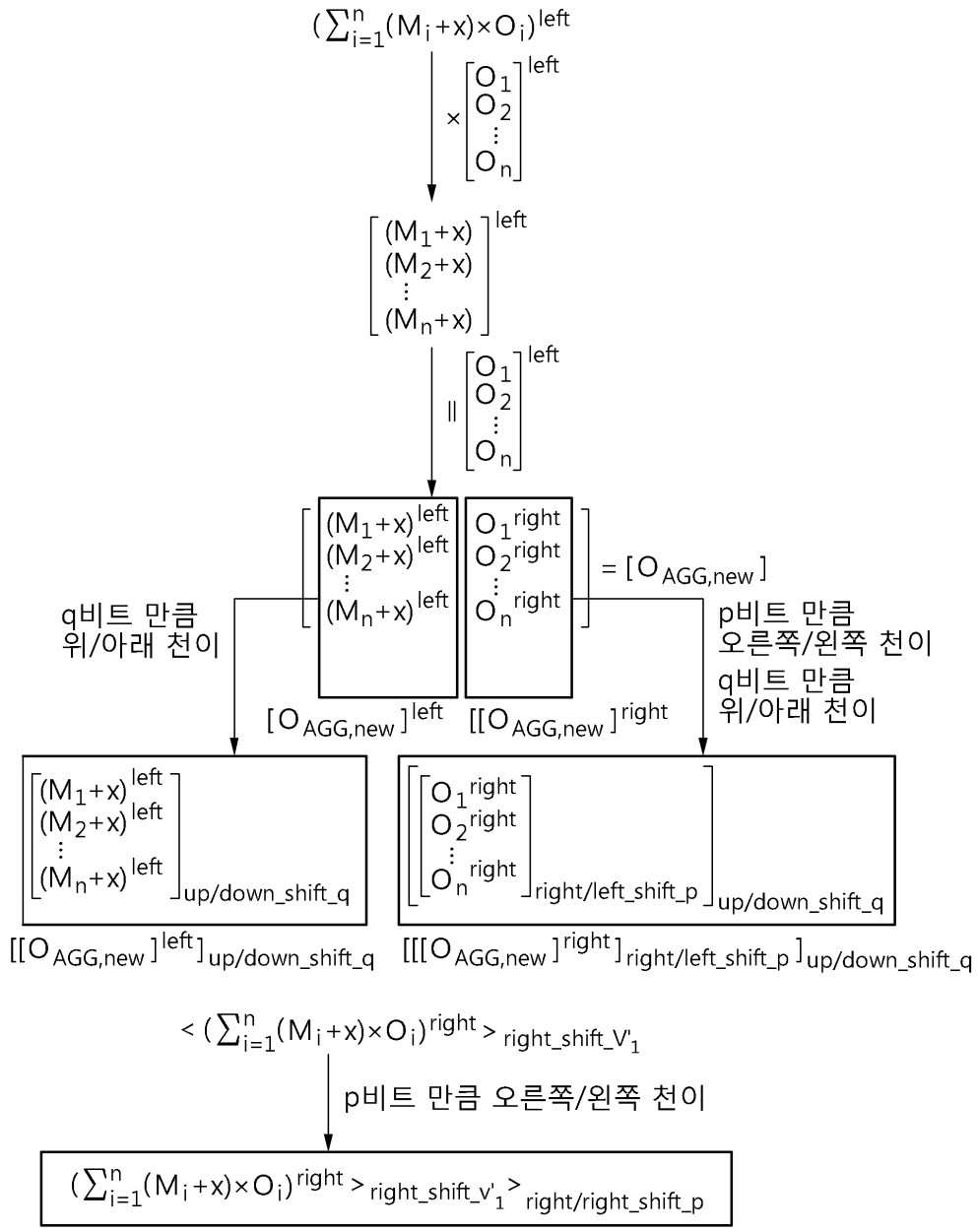
도면6


$< (M_1 + x) \times O_1 + \ldots + (M_{i-1} + x) \times O_{i-1} > \text{right_shift_}v_k \| \text{Index } v_k$
v_k 찾기 위해 인덱스 v_k로 표1에서 검색
$< (M_1 + x) \times O_1 + \ldots + (M_{i-1} + x) \times O_{i-1} > \text{right_shift_}v_k$
v_k비트 만큼 왼쪽 천이
$(M_1 + x) \times O_1 + \ldots + (M_{i-1} + x) \times O_{i-1}$
$\times O_i$
$((M_1 + x) \times O_1 + \ldots + (M_{i-1} + x) \times O_{i-1}) \times O_i$
드롭 및 SM_{i-1}에 재전송 요청
$\neq 0$
$= 0$
$(M_1 + x) \times O_1 + \ldots + (M_{i-1} + x) \times O_{i-1} + (M_i + x) \times O_i$
v_{k+1} 찾기 위해 표1 에서 검색
v_{k+1} 만큼 오른쪽 천이
$(M_1 + x) \times O_1 + \ldots + (M_{i-1} + x) \times O_{i-1} + (M_i + x) \times O_i > \text{right_shift_}v_{k+1}$
$< (M_1 + x) \times O_1 + \ldots + (M_{i-1} + x) \times O_{i-1} + (M_i + x) \times O_i > \text{right_shift_}v_{k+1} \| \text{Index } v_{k+1}$

도면7


$< \sum_{i=1}^{n} (M_i + x) \times O_i > \text{right_shift_v}_k \,||\, \text{Index}_{v_i}$
SM_1 (선택한 첫번째 SM) : 3단계로 수신된 정보의 정확성을 확인
$\sum_{i=1}^{n} (M_i + x) \times O_i$
$(\sum_{i=1}^{n} (M_i + x) \times O_i)^{left}$
$(\sum_{i=1}^{n} (M_i + x) \times O_i)^{right}$
v_1' 찾기 위해 표2 에서 검색
v_1' 비트만큼 오른쪽 천이
$(\sum_{i=1}^{n} (M_i + x) \times O_i)^{left}$
$<(\sum_{i=1}^{n} (M_i + x) \times O_i)^{right} > \text{right_shift_v'}_1$
$(\sum_{i=1}^{n} (M_i + x) \times O_i)^{left} \,||\, < (\sum_{i=1}^{n} (M_i + x) \times O_i)^{right} > \text{right_shift_v'}_1 \,||\, \text{Index}_{v'_1} \,||\, \text{Digest}$

도면8


$(\sum_{i=1}^{n}(M_i+x)\times O_i)^{left}$
$\times \begin{bmatrix} O_1 \\ O_2 \\ \vdots \\ O_n \end{bmatrix}^{left}$
$\begin{bmatrix} (M_1+x) \\ (M_2+x) \\ \vdots \\ (M_n+x) \end{bmatrix}^{left}$
$\| \begin{bmatrix} O_1 \\ O_2 \\ \vdots \\ O_n \end{bmatrix}^{left}$
$\begin{bmatrix} (M_1+x)^{left} \\ (M_2+x)^{left} \\ \vdots \\ (M_n+x)^{left} \end{bmatrix}$ $\begin{bmatrix} O_1^{right} \\ O_2^{right} \\ \vdots \\ O_n^{right} \end{bmatrix}$ $= [O_{AGG,new}]$
q비트 만큼 위/아래 천이
p비트 만큼 오른쪽/왼쪽 천이
q비트 만큼 위/아래 천이
$[O_{AGG,new}]^{left}$
$[[O_{AGG,new}]^{right}$
$\begin{bmatrix} (M_1+x)^{left} \\ (M_2+x)^{left} \\ \vdots \\ (M_n+x)^{left} \end{bmatrix}_{up/down_shift_q}$
$\begin{bmatrix} \begin{bmatrix} O_1^{right} \\ O_2^{right} \\ \vdots \\ O_n^{right} \end{bmatrix}_{right/left_shift_p} \end{bmatrix}_{up/down_shift_q}$
$[[O_{AGG,new}]^{left}]_{up/down_shift_q}$
$[[[O_{AGG,new}]^{right}]_{right/left_shift_p}]_{up/down_shift_q}$
$<(\sum_{i=1}^{n}(M_i+x)\times O_i)^{right}>_{right_shift_V'_1}$
p비트 만큼 오른쪽/왼쪽 천이
$(\sum_{i=1}^{n}(M_i+x)\times O_i)^{right}>_{right_shift_v'_1}>_{right/right_shift_p}$