



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2018년02월13일
(11) 등록번호 10-1828819
(24) 등록일자 2018년02월07일

(51) 국제특허분류(Int. Cl.)
G08C 17/02 (2006.01) H04L 9/08 (2006.01)
(52) CPC특허분류
G08C 17/02 (2013.01)
H04L 9/0819 (2013.01)
(21) 출원번호 10-2016-0121263
(22) 출원일자 2016년09월22일
심사청구일자 2016년09월22일
(56) 선행기술조사문헌
KR101380868 B1*
KR1020130024014 A*
KR1020130068872 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
이화여자대학교 산학협력단
서울특별시 서대문구 이화여대길 52 (대현동, 이화여자대학교)
(72) 발명자
도인실
인천광역시 연수구 센트럴로 194, 201동 2705호
(더샵센트럴파크2단지아파트)
채기준
서울특별시 강남구 강남대로136길 34
(74) 대리인
윤귀상

전체 청구항 수 : 총 9 항

심사관 : 복상문

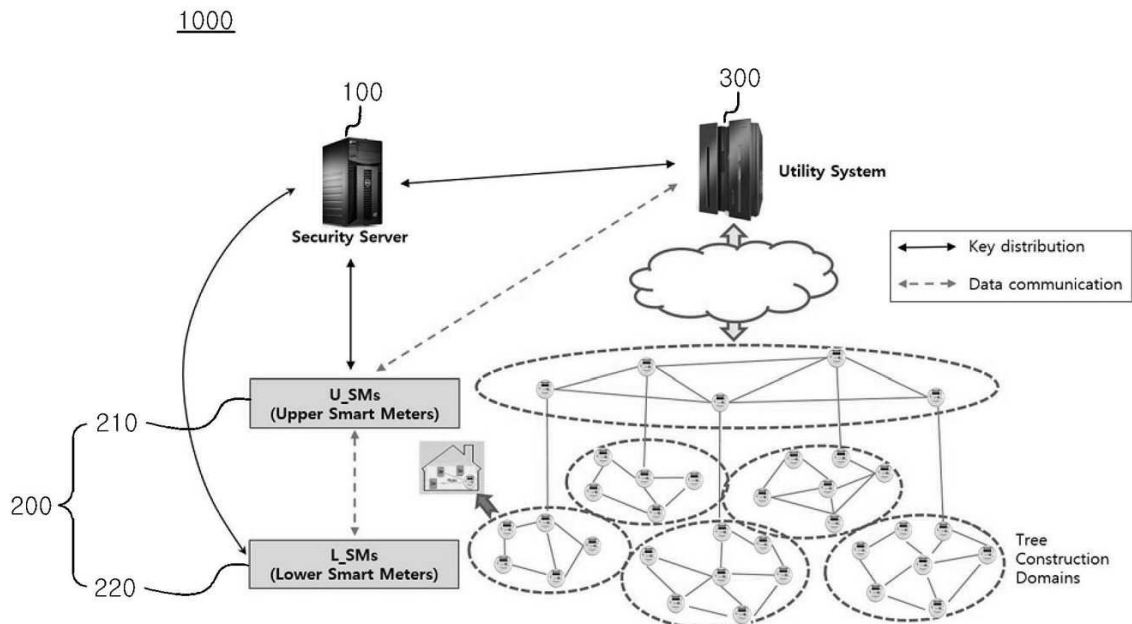
(54) 발명의 명칭 스마트 그리드 환경에서의 데이터 전송 방법 및 스마트 그리드 환경에서 스마트 디바이스의 에너지 사용정보를 수집하는 스마트미터의 제어방법

(57) 요약

스마트미터에서 스마트 디바이스의 에너지 사용량을 수집하고, 보안 서버로부터 수신하는 보안 관련 정보로 암호화하여, 스마트 그리드 환경을 제어하는 유틸리티 시스템으로 전송하는 스마트 그리드 환경에서의 데이터 전송 방법에 있어서, 상기 보안 서버가 복수의 스마트미터 중 다른 스마트미터에서 수집하는 복수의 스마트 디바이스

(뒷면에 계속)

대표도 - 도1



의 에너지 사용량을 병합하여 상기 유틸리티 시스템으로 전송할 상위 스마트미터를 선택하고, 상기 상위 스마트 미터에서 통신 시 적용할 키 정보 및 스마트 디바이스의 에너지 사용량을 암호화하기 위한 키 정보를 생성하여 상기 상위 스마트미터로 전송하면, 상기 상위 스마트미터가 에너지 사용량을 수신할 적어도 하나의 하위 스마트 미터로 상기 보안 서버로부터 수신하는 두 종류의 키 정보를 분배하며, 상기 상위 스마트미터가 적어도 하나의 상기 하위 스마트미터로부터 암호화된 스마트 디바이스의 에너지 사용량을 수신하면 해당 정보를 매트릭스 형태로 병합한 뒤 파쇄하여 상기 유틸리티 시스템으로 전송하는 스마트 그리드 환경에서의 데이터 전송 방법이 개시된다.

(52) CPC특허분류

H04L 9/0861 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호 2016R1A2B4015899

부처명 미래창조과학부

연구관리전문기관 한국연구재단

연구사업명 기초연구사업(학술진흥)-중견연구자지원사업

연구과제명 CPS환경에서의신뢰성있는서비스제공을위한보안기법및공격대응방안

기 여 율 1/1

주관기관 이화여자대학교 산학협력단

연구기간 2016.06.01 ~ 2019.05.31

명세서

청구범위

청구항 1

스마트미터에서 스마트 디바이스의 에너지 사용량을 수집하고, 보안 서버로부터 수신하는 보안 관련 정보로 암호화하여, 스마트 그리드 환경을 제어하는 유틸리티 시스템으로 전송하는 스마트 그리드 환경에서의 데이터 전송 방법에 있어서,

상기 보안 서버가 복수의 스마트미터 중 다른 스마트미터에서 수집하는 복수의 스마트 디바이스의 에너지 사용량을 병합하여 상기 유틸리티 시스템으로 전송할 상위 스마트미터를 선택하고, 상기 상위 스마트미터에서 통신 시 적용할 키 정보인 기본 키 및 스마트 디바이스의 에너지 사용량을 암호화하기 위한 키 정보인 키 매트릭스를 생성하여 상기 상위 스마트미터로 전송하면, 상기 상위 스마트미터가 상기 기본 키로부터 서브 키 체인을 생성하고, 서브 키 및 상기 키 매트릭스의 각 행을 에너지 사용량을 수신할 적어도 하나의 하위 스마트미터로 분배하며,

상기 상위 스마트미터가 적어도 하나의 상기 하위 스마트미터로부터 상기 키 매트릭스의 각 행에 의해 암호화된 스마트 디바이스의 에너지 사용량을 수신하면 해당 정보를 매트릭스 형태로 병합한 뒤 파쇄하여 상기 유틸리티 시스템으로 전송하는 스마트 그리드 환경에서의 데이터 전송 방법.

청구항 2

제1항에 있어서,

상기 보안 서버가 상기 상위 스마트미터에서 통신 시 적용할 키 정보 및 스마트 디바이스의 에너지 사용량을 암호화하기 위한 키 정보를 생성하여 상기 상위 스마트미터로 전송하면, 상기 상위 스마트미터가 에너지 사용량을 수신할 적어도 하나의 하위 스마트미터로 상기 보안 서버로부터 수신하는 두 종류의 키 정보를 분배하는 것은,

상기 보안 서버가 상기 상위 스마트미터에서 통신 시 적용할 키 정보로 해쉬 함수 기반의 기본 키 체인을 생성하고, 상기 기본 키 체인의 생성 방향과 반대 방향에 따라 상기 상위 스마트미터로 기본 키를 분배하면, 상기 상위 스마트미터가 적어도 하나의 하위 스마트미터로부터 에너지 사용량을 수신할 수 있도록 상기 기본 키로부터 서브 키 체인을 생성하고, 적어도 하나의 상기 하위 스마트미터로 서브 키를 분배하여 서브 트리를 구축하는 것을 포함하는 스마트 그리드 환경에서의 데이터 전송 방법.

청구항 3

삭제

청구항 4

제1항에 있어서,

상기 상위 스마트미터가 적어도 하나의 상기 하위 스마트미터로부터 암호화된 스마트 디바이스의 에너지 사용량을 수신하면 해당 정보를 매트릭스 형태로 병합한 뒤 파쇄하여 상기 유틸리티 시스템으로 전송하는 것은,

상기 상위 스마트미터가 적어도 하나의 상기 하위 스마트미터로부터 키 매트릭스의 각 행으로 암호화된 스마트 디바이스의 에너지 사용량을 수신하면, 해당 정보를 매트릭스 형태로 병합한 뒤 열 방향으로 파쇄하여 상기 유틸리티 시스템으로 전송하는 것인 스마트 그리드 환경에서의 데이터 전송 방법.

청구항 5

제4항에 있어서,

상기 상위 스마트미터가 적어도 하나의 상기 하위 스마트미터로부터 암호화된 스마트 디바이스의 에너지 사용량을 수신하면 해당 정보를 매트릭스 형태로 병합한 뒤 파쇄하여 상기 유틸리티 시스템으로 전송하는 것은,

상기 유틸리티 시스템에서 각 열을 재병합할 수 있도록, 파쇄된 매트릭스의 각 열에 ID를 부여하여 상기 유틸리

터 시스템으로 전송하는 것인 스마트 그리드 환경에서의 데이터 전송 방법.

청구항 6

스마트 디바이스의 에너지 사용량을 수집하고, 보안 서버로부터 수신하는 보안 관련 정보로 암호화하여, 스마트 그리드 환경을 제어하는 유틸리티 시스템으로 전송하는 스마트미터의 제어방법에 있어서,

상기 보안 서버에 의해 적어도 하나의 다른 스마트미터를 관리하는 상위 스마트미터로 선택받으면, 상기 보안 서버로부터 기본 키를 수신하고, 상기 기본 키로부터 서브 키 체인을 생성하여 적어도 하나의 다른 스마트미터인 하위 스마트미터로 분배하고,

상기 보안 서버로부터 키 매트릭스를 수신하고, 상기 키 매트릭스의 각 행을 상기 적어도 하나의 하위 스마트미터로 분배하며,

상기 적어도 하나의 하위 스마트미터로부터 상기 키 매트릭스의 각 행에 의해 암호화된 스마트 디바이스의 사용량을 수신하면, 해당 정보를 매트릭스 형태로 병합한 뒤 파쇄하여 상기 유틸리티 시스템으로 전송하는 스마트미터의 제어방법.

청구항 7

제6항에 있어서,

상기 적어도 하나의 하위 스마트미터로부터 상기 키 매트릭스의 각 행에 의해 암호화된 스마트 디바이스의 사용량을 수신하면, 해당 정보를 매트릭스 형태로 병합한 뒤 파쇄하여 상기 유틸리티 시스템으로 전송하는 것은,

상기 상위 스마트미터가 매트릭스를 열 방향으로 파쇄하고, 상기 유틸리티 시스템에서 각 열을 재병합할 수 있도록 각 열에 ID를 부여하여 상기 유틸리티 시스템으로 전송하는 것인 스마트미터의 제어방법.

청구항 8

제6항에 있어서,

상기 보안 서버에 의해 적어도 하나의 다른 스마트미터를 관리하는 상위 스마트미터로 선택받으면, 상기 보안 서버로부터 기본 키를 수신하는 것은,

상기 보안 서버로부터 해쉬 함수에 기반하여 생성되는 기본 키를 수신하는 것인 스마트미터의 제어방법.

청구항 9

제6항에 있어서,

상기 기본 키로부터 서브 키 체인을 생성하여 적어도 하나의 다른 스마트미터인 하위 스마트미터로 분배하는 것은,

상기 기본 키로부터 인접한 홈 영역 네트워크 또는 빌딩 영역 네트워크에 접속되는 적어도 하나의 하위 스마트미터의 개수와 동일한 개수의 서브 키로 이루어지는 서브 키 체인을 생성하고 상기 적어도 하나의 하위 스마트미터로 분배하여 서브 트리를 구축하는 것인 스마트미터의 제어방법.

청구항 10

제6항에 있어서,

홈 영역 네트워크 또는 빌딩 영역 네트워크에 접속되는 적어도 하나의 스마트 디바이스의 에너지 사용량을 획득하는 것을 더 포함하는 스마트미터의 제어방법.

발명의 설명

기술 분야

본 발명은 스마트 그리드 환경에서의 데이터 전송 방법 및 스마트 그리드 환경에서 스마트 디바이스의 에너지 사용정보를 수집하는 스마트미터의 제어방법에 관한 것으로, 보다 상세하게는 공공 네트워크를 이용하는 스마트

[0001]

그리드 환경에서의 보안성을 강화하기 위한 데이터 전송 방법 및 스마트미터의 제어방법에 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] 이러한 스마트 그리드 시스템은 서로 다른 다양한 시스템 및 서브 시스템의 조합으로 이루어져, 다양한 공격에 취약하며 이는 스마트 기기 나아가 사회 전반적으로 위험을 초래하게 된다.
- [0004] 이에 따라, 최근 스마트 그리드 시스템에서의 보안성을 향상시키기 위한 다양한 기술들이 개발되었다.
- [0005] 예를 들면, "Jinfeng Yang, Rong Cheng, Wenming Liu, Yong Xiao, Fangguo Zhang, (2013) 'Cryptoanalysis and improvement of smart prepayment meter protocol in standard Q/GDW 365' International Journal of Grid and Utility Computing, Vol.4 No.1, pp.40-46" 에는 스마트미터에서의 정보 교환을 위한 인증 기술이 개시되어 있다.
- [0006] 또한, 한국공개특허 제2010-0069447호 등에서는 준동형 암호화를 이용한 데이터 병합을 통해 다수의 데이터를 더하거나 곱한 결과에 따른 암호문을 생성하여 전송하는 방법을 제안하고 있다. 즉, x , y 라는 데이터가 있을 때, 이를 암호화하여 암호문 $E(x)$ 와 $E(y)$ 를 생성하고, 데이터 병합을 통해 단일의 암호문 $E(x + y)$ 또는 $E(x \cdot y)$ 를 생성하여 전송하는 방법을 제안하고 있다.
- [0007] 이외에도, 서로 다른 특징을 갖는 다양한 구성 요소들로 이루어지는 것을 특징으로 하는 스마트 그리드 시스템에서의 안전한 통신을 수행하기 위한 다양한 기술 개발이 활발히 이루어지고 있다.

발명의 내용

해결하려는 과제

- [0008] 본 발명의 일측면은 데이터 암호화 시 적용되는 키 정보뿐만 아니라 데이터 전송 시 적용되는 키 정보를 생성하고 이를 이용하여 데이터를 전송하는 스마트 그리드 환경에서의 데이터 전송 방법을 제공한다.
- [0009] 또한, 복수의 에너지 사용량을 매트릭스 형태로 병합하고, 데이터 전송 시 매트릭스 형태의 데이터를 열 방향으로 파쇄하여 전송하는 스마트미터의 제어방법을 제공한다.

과제의 해결 수단

- [0010] 본 발명의 일측면은 스마트미터에서 스마트 디바이스의 에너지 사용량을 수집하고, 보안 서버로부터 수신하는 보안 관련 정보로 암호화하여, 스마트 그리드 환경을 제어하는 유틸리티 시스템으로 전송하는 스마트 그리드 환경에서의 데이터 전송 방법에 있어서, 상기 보안 서버가 복수의 스마트미터 중 다른 스마트미터에서 수집하는 복수의 스마트 디바이스의 에너지 사용량을 병합하여 상기 유틸리티 시스템으로 전송할 상위 스마트미터를 선택하고, 상기 상위 스마트미터에서 통신 시 적용할 키 정보 및 스마트 디바이스의 에너지 사용량을 암호화하기 위한 키 정보를 생성하여 상기 상위 스마트미터로 전송하면, 상기 상위 스마트미터가 에너지 사용량을 수신할 적어도 하나의 하위 스마트미터로 상기 보안 서버로부터 수신하는 두 종류의 키 정보를 분배하며, 상기 상위 스마트미터가 적어도 하나의 상기 하위 스마트미터로부터 암호화된 스마트 디바이스의 에너지 사용량을 수신하면 해당 정보를 매트릭스 형태로 병합한 뒤 파쇄하여 상기 유틸리티 시스템으로 전송한다.
- [0011] 한편, 상기 보안 서버가 상기 상위 스마트미터에서 통신 시 적용할 키 정보 및 스마트 디바이스의 에너지 사용량을 암호화하기 위한 키 정보를 생성하여 상기 상위 스마트미터로 전송하면, 상기 상위 스마트미터가 에너지 사용량을 수신할 적어도 하나의 하위 스마트미터로 상기 보안 서버로부터 수신하는 두 종류의 키 정보를 분배하는 것은, 상기 보안 서버가 상기 상위 스마트미터에서 통신 시 적용할 키 정보로 해쉬 함수 기반의 기본 키 체인을 생성하고, 상기 기본 키 체인의 생성 방향과 반대 방향에 따라 상기 상위 스마트미터로 기본 키를 분배하면, 상기 상위 스마트미터가 적어도 하나의 하위 스마트미터로부터 에너지 사용량을 수신할 수 있도록 상기 기본 키로부터 서브 키 체인을 생성하고, 적어도 하나의 상기 하위 스마트미터로 서브 키를 분배하여 서브 트리를 구축하는 것을 포함할 수 있다.
- [0012] 또한, 상기 보안 서버가 상기 상위 스마트미터에서 통신 시 적용할 키 정보 및 스마트 디바이스의 에너지 사용량을 암호화하기 위한 키 정보를 생성하여 상기 상위 스마트미터로 전송하면, 상기 상위 스마트미터가 에너지

사용량을 수신할 적어도 하나의 하위 스마트미터로 상기 보안 서버로부터 수신하는 두 종류의 키 정보를 분배하는 것은, 상기 보안 서버가 스마트 디바이스의 에너지 사용량을 암호화하기 위한 키 정보로 키 매트릭스를 생성하여 상기 상위 스마트미터로 전송하면, 상기 상위 스마트미터가 상기 키 매트릭스의 각 행을 적어도 하나의 상기 하위 스마트미터로 분배하는 것을 포함할 수 있다.

[0013] 또한, 상기 상위 스마트미터가 적어도 하나의 상기 하위 스마트미터로부터 암호화된 스마트 디바이스의 에너지 사용량을 수신하면 해당 정보를 매트릭스 형태로 병합한 뒤 파쇄하여 상기 유틸리티 시스템으로 전송하는 것은, 상기 상위 스마트미터가 적어도 하나의 상기 하위 스마트미터로부터 키 매트릭스의 각 행으로 암호화된 스마트 디바이스의 에너지 사용량을 수신하면, 해당 정보를 매트릭스 형태로 병합한 뒤 열 방향으로 파쇄하여 상기 유틸리티 시스템으로 전송하는 것일 수 있다.

[0014] 또한, 상기 상위 스마트미터가 적어도 하나의 상기 하위 스마트미터로부터 암호화된 스마트 디바이스의 에너지 사용량을 수신하면 해당 정보를 매트릭스 형태로 병합한 뒤 파쇄하여 상기 유틸리티 시스템으로 전송하는 것은, 상기 유틸리티 시스템에서 각 열을 재병합할 수 있도록, 파쇄된 매트릭스의 각 열에 ID를 부여하여 상기 유틸리티 시스템으로 전송하는 것일 수 있다.

[0015] 한편, 본 발명의 다른 측면은 스마트 디바이스의 에너지 사용량을 수집하고, 보안 서버로부터 수신하는 보안 관련 정보로 암호화하여, 스마트 그리드 환경을 제어하는 유틸리티 시스템으로 전송하는 스마트미터의 제어방법에 있어서, 상기 보안 서버에 의해 적어도 하나의 다른 스마트미터를 관리하는 상위 스마트미터로 선택받으면, 상기 보안 서버로부터 기본 키를 수신하고, 상기 기본 키로부터 서브 키 체인을 생성하여 적어도 하나의 다른 스마트미터인 하위 스마트미터로 분배하고, 상기 보안 서버로부터 키 매트릭스를 수신하고, 상기 키 매트릭스의 각 행을 상기 적어도 하나의 하위 스마트미터로 분배하며, 상기 적어도 하나의 하위 스마트미터로부터 상기 키 매트릭스의 각 행에 의해 암호화된 스마트 디바이스의 사용량을 수신하면, 해당 정보를 매트릭스 형태로 병합한 뒤 파쇄하여 상기 유틸리티 시스템으로 전송한다.

[0016] 한편, 상기 적어도 하나의 하위 스마트미터로부터 상기 키 매트릭스의 각 행에 의해 암호화된 스마트 디바이스의 사용량을 수신하면, 해당 정보를 매트릭스 형태로 병합한 뒤 파쇄하여 상기 유틸리티 시스템으로 전송하는 것은, 상기 상위 스마트미터가 매트릭스를 열 방향으로 파쇄하고, 상기 유틸리티 시스템에서 각 열을 재병합할 수 있도록 각 열에 ID를 부여하여 상기 유틸리티 시스템으로 전송하는 것일 수 있다.

[0017] 또한, 상기 보안 서버에 의해 적어도 하나의 다른 스마트미터를 관리하는 상위 스마트미터로 선택받으면, 상기 보안 서버로부터 기본 키를 수신하는 것은, 상기 보안 서버로부터 해쉬 함수에 기반하여 생성되는 기본 키를 수신하는 것일 수 있다.

[0018] 또한, 상기 기본 키로부터 서브 키 체인을 생성하여 적어도 하나의 다른 스마트미터인 하위 스마트미터로 분배하는 것은, 상기 기본 키로부터 인접한 홈 영역 네트워크 또는 빌딩 영역 네트워크에 접속되는 적어도 하나의 하위 스마트미터의 개수와 동일한 개수의 서브 키로 이루어지는 서브 키 체인을 생성하고 상기 적어도 하나의 하위 스마트미터로 분배하여 서브 트리를 구축하는 것일 수 있다.

[0019] 또한, 홈 영역 네트워크 또는 빌딩 영역 네트워크에 접속되는 적어도 하나의 스마트 디바이스의 에너지 사용량을 획득하는 것을 더 포함할 수 있다.

발명의 효과

[0020] 상술한 본 발명의 일측면에 따르면 스마트 그리드 시스템의 보안성을 강화할 수 있으며, 스마트미터의 연산량을 최소화함과 동시에 외부 공격으로부터의 데이터 손상을 방지할 수 있다.

도면의 간단한 설명

[0021] 도 1은 본 발명의 일 실시예에 따른 스마트 그리드 시스템의 구성을 개략적으로 도시한 블록도이다.

도 2는 도 1에 도시된 보안 서버의 제어 블록도이다.

도 3은 본 발명의 일 실시예에 따른 스마트 그리드 시스템에서 통신 보안을 위한 키를 생성하는 방법을 설명하기 위한 도면이다.

도 4는 본 발명의 일 실시예에 따른 스마트 그리드 시스템에서 데이터 암호화를 위한 키를 생성하는 방법을 설명하기 위한 도면이다.

도 5는 도 1에 도시된 스마트미터의 제어 블록도이다.

도 6은 본 발명의 일 실시예에 따른 스마트 그리드 시스템에서 데이터 병합 및 전송 방법을 설명하기 위한 도면이다.

도 7 및 도 8은 도 5에 도시된 스마트미터의 제어방법을 설명하기 위한 순서도이다.

도 9는 도 1에 도시된 유틸리티 시스템의 제어 블록도이다.

도 10은 본 발명의 일 실시예에 따른 스마트 그리드 환경에서의 데이터 전송 방법의 순서도이다.

발명을 실시하기 위한 구체적인 내용

- [0022] 후술하는 본 발명에 대한 상세한 설명은, 본 발명이 실시될 수 있는 특정 실시예를 예시로서 도시하는 첨부 도면을 참조한다. 이들 실시예는 당업자가 본 발명을 실시할 수 있기에 충분하도록 상세히 설명된다. 본 발명의 다양한 실시예는 서로 다르지만 상호 배타적일 필요는 없음이 이해되어야 한다. 예를 들어, 여기에 기재되어 있는 특정 형상, 구조 및 특성은 일 실시예와 관련하여 본 발명의 정신 및 범위를 벗어나지 않으면서 다른 실시예로 구현될 수 있다. 또한, 각각의 개시된 실시예 내의 개별 구성요소의 위치 또는 배치는 본 발명의 정신 및 범위를 벗어나지 않으면서 변경될 수 있음이 이해되어야 한다. 따라서, 후술하는 상세한 설명은 한정적인 의미로서 취하려는 것이 아니며, 본 발명의 범위는, 적절하게 설명된다면, 그 청구항들이 주장하는 것과 균등한 모든 범위와 더불어 첨부된 청구항에 의해서만 한정된다. 도면에서 유사한 참조부호는 여러 측면에 걸쳐서 동일하거나 유사한 기능을 지칭한다.
- [0023] 이하, 도면들을 참조하여 본 발명의 바람직한 실시예들을 보다 상세하게 설명하기로 한다.
- [0024] 도 1은 본 발명의 일 실시예에 따른 스마트 그리드 시스템의 구성을 개략적으로 도시한 블록도이다.
- [0025] 도 1을 참조하면, 본 발명의 일 실시예에 따른 스마트 그리드 시스템(1000)은 보안 서버(100), 복수의 스마트미터(200) 및 유틸리티 시스템(300)을 포함하여 구성되며, 복수의 스마트미터(200)에서 복수의 스마트 디바이스의 에너지 사용량을 수집하여 유틸리티 시스템(300)으로 전송하면, 유틸리티 시스템(300)에서 이를 분석하여 복수의 스마트 디바이스의 에너지 소비 패턴 등을 판단하고, 추후 에너지 공급 시, 효율적으로 분배되도록 제어할 수 있다.
- [0026] 또한, 본 발명의 일 실시예에 따른 스마트 그리드 시스템(1000)은 공공 네트워크를 통하여 복수의 스마트미터(200)와 유틸리티 시스템(300)간의 데이터 전송이 이루어지는데, 따라서, 보안 서버(100)는 외부 공격으로부터 안전한 데이터 전송이 이루어질 수 있도록, 보안 관련 정보를 생성하여 복수의 스마트미터(200) 및 유틸리티 시스템(300)으로 전달할 수 있다.
- [0027] 여기에서, 보안 서버(100)는 크게 두 종류의 보안 관련 정보를 생성하는데, 두 종류의 보안 관련 정보는 스마트미터(200)와 유틸리티 시스템(300) 간의 통신 시 적용되는 기본 키 체인과, 스마트미터(200)에서 수집하는 스마트 디바이스의 에너지 사용량 암호화 시 적용되는 키 매트릭스일 수 있다. 이와 관련하여 구체적인 설명은 후술하기로 한다.
- [0028] 한편, 본 발명의 일 실시예에 따른 스마트 그리드 시스템(1000)은 계층형 스마트 그리드 시스템으로, 복수의 스마트미터(200)가 상위 스마트미터(210) 및 하위 스마트미터(220)로 나누어질 수 있다. 하위 스마트미터(220)는 홈 영역 네트워크(HAN: Home Area Network) 또는 빌딩 영역 네트워크(BAN: Building Area Network)에 접속되는 복수의 스마트 디바이스의 에너지 사용량을 수집하여 상위 스마트미터(210)로 전송할 수 있다. 이때, 하위 스마트미터(220)는 수집한 에너지 사용량을 보안 서버(100)에서 생성하는 키 매트릭스에 기반하여 암호화한 뒤 상위 스마트미터(210)로 전송할 수 있다. 상위 스마트미터(210)는 인접한 지역의 복수의 하위 스마트미터(220)로부터 수신하는 홈 영역 네트워크 또는 빌딩 영역 네트워크의 에너지 사용량을 병합(aggregation)하여 유틸리티 시스템(300)으로 전송할 수 있다.
- [0029] 여기에서, 상위 스마트미터(210)는 복수의 하위 스마트미터(220)로부터 수신하는 행(row) 형태의 암호화된 에너지 사용량을 매트릭스 형태로 병합할 수 있으며, 매트릭스 형태의 데이터를 열(column) 방향으로 좌회하여 각 열을 유틸리티 시스템(300)으로 전송함으로써, 외부 공격으로부터 데이터를 보호할 수 있다. 이와 같은 경우, 유틸리티 시스템(300)은 상위 스마트미터(210)로부터 수신하는 각 열을 매트릭스 형태로 재병합한 뒤 복호화하여 각 홈 영역 네트워크 또는 빌딩 영역 네트워크의 에너지 사용량을 확인할 수 있으며, 아울러 외부 공격에 의해 데이터가 손상되었는지 등의 상황인지가 가능하다. 이와 관련하여 구체적인 설명은 후술하기로 한다.

- [0030] 이와 같이, 본 발명의 일 실시예에 따른 스마트 그리드 시스템(1000)은 보안 서버(100)에서 데이터 암호화 시 적용되는 키 정보뿐만 아니라 데이터 전송 시 적용되는 키 정보를 생성하여 스마트미터(200) 또는 유틸리티 시스템(300)으로 분배함으로써 스마트 그리드 시스템(1000)의 보안성을 강화할 수 있다. 이에 더하여, 스마트미터(200)에서 복수의 에너지 사용량을 매트릭스 형태로 병합하고, 유틸리티 시스템(300)으로 데이터 전송 시 매트릭스 형태의 데이터를 열 방향으로 파쇄하여 전송하는데, 이와 같은 방식은 스마트미터(200)의 연산량을 최소화함과 동시에 외부 공격으로부터의 데이터 손상을 방지할 수 있다.
- [0031] 이하, 도 2 내지 도 9에 도시된 스마트 그리드 시스템(1000)에 포함되는 각 구성요소에 대하여 구체적으로 설명하기로 한다.
- [0032] 먼저, 도 2는 도 1에 도시된 보안 서버의 제어 블록도이다.
- [0033] 도 2를 참조하면, 보안 서버(100)는 보안 서버 통신부(110), 보안 서버 제어부(120) 및 보안 서버 메모리부(130)를 포함하여 구성될 수 있으며, 복수의 스마트미터(200)와 유틸리티 시스템(300) 간의 데이터 전송 시 보안을 위한 보안 관련 정보를 생성하여 복수의 스마트미터(200) 및 유틸리티 시스템(300)으로 전송할 수 있다. 이하, 상술한 보안 서버(100)의 각 구성요소들에 대해 설명하기로 한다.
- [0034] 보안 서버 통신부(110)는 보안 서버(100)와 유틸리티 시스템(300) 또는 스마트미터(200) 간의 통신을 가능하게 하며, 이를 위해, 무선 통신 또는 근거리 무선 통신을 수행하게 하는 하나 이상의 구성요소를 포함하여 구현될 수 있다.
- [0035] 예를 들면, 보안 서버 통신부(110)는 복수의 스마트미터(200) 중 후술하는 보안 서버 제어부(120)에 의해 선택되는 상위 스마트미터(210)로 보안 관련 정보를 송신할 수 있다. 또한, 보안 서버 통신부(110)는 유틸리티 시스템(300)으로 보안 관련 정보를 송신하거나, 유틸리티 시스템(300)으로부터 스마트미터(200)와 유틸리티 시스템(300) 간의 데이터 전송 결과와 관련된 정보를 수신할 수 있다.
- [0036] 보안 서버 제어부(120)는 보안 서버(100)의 전반적인 동작을 제어할 수 있다. 특히, 보안 서버 제어부(120)는 복수의 스마트미터(200) 중 상위 스마트미터(210)를 선택하고, 상위 스마트미터(210) 및 유틸리티 시스템(300)으로 전송할 두 종류의 보안 관련 정보를 생성할 수 있다. 이를 위해, 보안 서버 제어부(120)는 상위 스마트미터 선택부(121), 기본 키 체인 생성부(122) 및 키 매트릭스 생성부(123)를 포함할 수 있다.
- [0037] 상위 스마트미터 선택부(121)는 복수의 스마트미터(200) 중 적어도 하나의 다른 스마트미터(200)에서 수집하는 스마트 디바이스의 에너지 사용량을 병합하여 유틸리티 시스템(300)으로 송신할 상위 스마트미터(210)를 선택할 수 있다.
- [0038] 여기에서, 상위 스마트미터 선택부(121)는 유틸리티 시스템(300)으로부터 상위 스마트미터(210)로부터 수신하는 데이터 손상 여부 등의 상황인지 정보를 수신하며, 이러한 상황인지 정보를 반영하여 상위 스마트미터(210)를 선택할 수 있다.
- [0039] 한편, 상위 스마트미터 선택부(121)에 의해 선택되는 상위 스마트미터(210)는 인접한 지역의 하위 스마트미터(220)들을 관리하며, 하위 스마트미터(220)들로부터 홈 영역 네트워크(HAN) 또는 빌딩 영역 네트워크(BAN)에 접속되는 스마트 디바이스들의 에너지 사용량 정보를 병합하여 유틸리티 시스템(300)으로 송신할 수 있다.
- [0040] 기본 키 체인 생성부(122)는 상위 스마트미터(210)와 유틸리티 시스템(300) 간에 통신 시 적용할 키 체인을 생성할 수 있다. 이와 관련하여, 도 3을 참조하여 설명하기로 한다.
- [0041] 도 3은 본 발명의 일 실시예에 따른 스마트 그리드 시스템(1000)에서 통신 보안을 위한 키를 생성하는 방법을 설명하기 위한 도면이다.
- [0042] 도 3을 참조하면, 기본 키 체인 생성부(122)는 적어도 하나의 상위 스마트미터(210)와 유틸리티 시스템(300) 간에 통신 시 적용하기 위한 기본 키 체인을 생성하여, 적어도 하나의 상위 스마트미터(210)로 분배할 수 있다. 이때, 기본 키 체인 생성부(122)는 일방향 해쉬 체인을 반복적으로 이용하여 기본 키 체인을 생성할 수 있다. 해쉬 체인의 구성요소들은 일방향 해쉬 함수에 반복적으로 적용하여 계산될 수 있다. 이러한 기본 키는 적어도 하나의 상위 스마트미터(210)와 유틸리티 시스템(300) 간의 네트워크 세션에서 공유될 수 있다.
- [0043] 또한, 기본 키 체인 생성부(122)는 기본 키 체인을 생성하면, 기본 키 체인 생성 방향과 반대 방향에 따라 상위 스마트미터(210)로 기본 키를 분배할 수 있다. 예를 들면, 기본 키 체인 생성부(122)는 $S_m \rightarrow \dots \rightarrow S_2 \rightarrow S_1 \rightarrow S_0$ 순으로 기본 키 체인을 생성하면, 그 반대인 $S_0 \rightarrow S_1 \rightarrow S_2 \rightarrow \dots \rightarrow S_{m-1} \rightarrow S_m$ 순으로 적어도 하나의 상위

스마트미터($U_SM_0, U_SM_1, \dots, U_SM_n$)로 기본 키를 분배할 수 있다. 즉, 타임 슬롯 0 에서 적어도 하나의 상위 스마트미터($U_SM_0, U_SM_1, \dots, U_SM_n$)은 보안 서버(100)로부터 기본 키 S_0 을 수신하며, 이러한 기본 키 S_0 을 이용하여 유틸리티 시스템(300)과 시스템 파라미터들 또는 서브 트리 정보 등을 송수신할 수 있다. 이와 같은 방식으로 기본 키 체인이 모두 사용되면, 기본 키 체인 생성부(122)는 새로운 기본 키 체인을 생성할 수 있다.

[0044] 한편, 상위 스마트미터(210)는 기본 키를 분배받으면, 기본 키로부터 서브 키 체인을 생성하여 하위 스마트미터(220)로 분배하는데, 이와 관련하여 구체적인 설명은 후술하기로 한다.

[0045] 키 매트릭스 생성부(123)는 스마트미터(200)에서 수집하는 스마트 디바이스의 에너지 사용량을 암호화하기 위한 키를 생성하여 스마트미터(200)로 송신할 수 있다. 이와 관련하여, 도 4를 참조하여 설명하기로 한다.

[0046] 도 4는 본 발명의 일 실시예에 따른 스마트 그리드 시스템(1000)에서 데이터 암호화를 위한 키를 생성하는 방법을 설명하기 위한 도면이다.

[0047] 도 4를 참조하면, 키 매트릭스 생성부(123)는 매트릭스 형태의 데이터 암호화 키인 키 매트릭스를 생성하여 상위 스마트미터(210)로 송신할 수 있다. 이와 같은 경우, 상위 스마트미터(210)는 키 매트릭스의 각 행을 하위 스마트미터(220)로 전송할 수 있으며, 하위 스마트미터(220)는 키 매트릭스의 각 행을 이용하여 수집한 스마트 디바이스의 에너지 사용량을 암호화할 수 있다.

[0048] 한편, 키 매트릭스 생성부(123)는 키 매트릭스를 복호화할 수 있는 페어와이즈(pairwise) 키를 유틸리티 시스템(300)으로 전송할 수 있다. 또한, 상위 스마트미터(210)에서의 하위 스마트미터(220)로의 키 매트릭스 분배 테이블 정보를 유틸리티 시스템(300)으로 전송할 수 있다. 유틸리티 시스템(300)은 이와 같은 정보들을 이용하여 상위 스마트미터(210)로부터 수신하는 암호화된 에너지 사용량 정보를 복호화할 수 있다.

[0049] 보안 서버 메모리부(130)는 보안 서버(100)의 처리 및 제어를 위한 프로그램이 저장될 수 있으며, 입출력되는 데이터들의 임시 저장을 위한 기능을 수행할 수 있다.

[0050] 한편, 도 5는 도 1에 도시된 스마트미터의 제어 블록도이다.

[0051] 도 5를 참조하면, 스마트미터(200)는 스마트미터 통신부(210), 스마트미터 제어부(220) 및 스마트미터 메모리부(230)를 포함하여 구성될 수 있으며, 스마트 디바이스의 에너지 사용 정보를 수집하여 유틸리티 시스템(300)으로 전송하되, 보안 서버(100)로부터 수집하는 보안 관련 정보로 데이터를 암호화하여 유틸리티 시스템(300)으로 전송할 수 있다.

[0052] 한편, 스마트미터(200)는 상위 스마트미터(210)와 하위 스마트미터(220)로 나누어질 수 있는데, 상위 스마트미터(210)와 하위 스마트미터(220)는 모두 스마트 디바이스의 에너지 사용 정보를 수집하여 암호화하는 역할을 수행할 수 있다. 다만, 하위 스마트미터(220)는 에너지 사용 정보를 직접 유틸리티 시스템(300)으로 전송하지 않고 상위 스마트미터(210)를 통해 전송할 수 있다. 즉, 상위 스마트미터(210)는 하위 스마트미터(220)에서 수집하는 에너지 사용 정보를 병합하여 유틸리티 시스템(300)으로 전송하며, 이를 위해, 하위 스마트미터(220)와의 통신을 위한 서브 키 체인을 생성하여 하위 스마트미터(220)로 분배하며, 데이터 암호화를 위한 암호화 키 정보를 하위 스마트미터(220)로 분배할 수 있다. 이러한 상위 스마트미터(210)는 보안 서버(100)에 의해 주기적 또는 외부의 공격이 있을 때마다 선택될 수 있다. 즉, 복수의 스마트미터(200)는 보안 서버(100)에 의해 상위 스마트미터(210)의 역할을 수행하거나, 하위 스마트미터(220)의 역할을 수행할 수 있다.

[0053] 이하, 도 5에 도시된 스마트미터(200) 각 구성요소들에 대해 설명하기로 한다.

[0054] 스마트미터 통신부(210)는 스마트미터(200)와 보안 서버(100) 또는 유틸리티 시스템(300) 간의 통신을 가능하게 할 수 있다. 또한, 스마트미터 통신부(210)는 스마트미터(200)와 다른 스마트미터(200) 또는 스마트 디바이스와의 통신을 가능하게 하며, 이를 위해, 무선 통신 또는 근거리 무선 통신을 수행하게 하는 하나 이상의 구성요소를 포함하여 구현될 수 있다.

[0055] 예를 들면, 보안 서버(100)에 의해 선택된 상위 스마트미터(210)의 경우, 스마트미터 통신부(210)는 보안 서버(100)로부터 보안 관련 정보를 수신할 수 있다. 또한, 유틸리티 시스템(300)으로 에너지 사용 정보를 송신할 수 있다. 또한, 하위 스마트미터(220)로 보안 관련 정보를 송신하며, 에너지 사용 정보를 수신할 수 있다. 또한, 홈 영역 네트워크(HAN) 또는 빌딩 영역 네트워크(BAN)에 접속하여 해당 네트워크에 접속되어 있는 스마트 디바이스들의 에너지 사용량 정보를 수신할 수 있다.

[0056] 또는, 하위 스마트미터(220)의 경우, 홈 영역 네트워크(HAN) 또는 빌딩 영역 네트워크(BAN)에 접속하여 해당 네

트위크에 접속되어 있는 스마트 디바이스들의 에너지 사용량 정보를 수신할 수 있다. 상위 스마트미터(210)로부터 보안 관련 정보를 수신하고, 상위 스마트미터(210)로 스마트 디바이스의 에너지 사용 정보를 송신할 수 있다.

[0057] 스마트미터 제어부(220)는 스마트미터(200)의 전반적인 동작을 제어할 수 있다. 특히, 상위 스마트미터(210)로 선택되면, 스마트미터 제어부(220)는 하위 스마트미터(220)로 두 종류의 보안 관련 정보를 분배할 수 있으며, 하위 스마트미터(220)로부터 수신하는 에너지 사용량 정보를 병합할 수 있다. 또는, 하위 스마트미터(220)로 선택되면, 스마트 디바이스의 에너지 사용량 정보를 암호화할 수 있다. 이를 위해, 스마트미터 제어부(220)는 서버 키 체인 생성부(221), 키 매트릭스 분배부(222), 데이터 암호화부(223) 및 데이터 병합부(224)를 포함할 수 있다.

[0058] 서버 키 체인 생성부(221)는 상위 스마트미터(210)에서 관리하는 적어도 하나의 하위 스마트미터(220)와의 통신을 위한 서버 트리를 구축하기 위해 서버 키 체인을 생성할 수 있다. 서버 키 체인 생성부(221)는 보안 서버(100)로부터 수신하는 기본 키로부터 서버 키 체인을 생성하여 하위 스마트미터(220)로 분배할 수 있다. 이때, 서버 키 체인의 길이는 상위 스마트미터(210)에서 관리하는 하위 스마트미터(220)의 수에 해당한다.

[0059] 구체적으로는, 도 3을 참조하면, 서버 키 체인 생성부(221)는 보안 서버(100)로부터 수신하는 기본 키 $S_k(k=0, \dots, m)$ 를 이용하여 서버 키 체인을 생성할 수 있다. 이때, 서버 키 체인 생성부(221)는 서버 키 체인을 생성하기 전에, 기본 키를 해쉬 함수에 적용하여 기본 키가 정상인지 여부를 먼저 판단할 수 있다. 서버 키 체인 생성부(221)는 임의의 난수를 생성하고, 임의의 난수와 기본 키 및 적어도 하나의 하위 스마트미터(220) 각각의 ID를 exclusive-OR 연산하여 서버 키 체인을 생성할 수 있다.

[0060] 서버 키 체인 생성부(221)는 이와 같이 서버 키 체인을 생성하여, 적어도 하나의 하위 스마트미터(220)로 분배하여 서버 트리를 구축하고, 이를 통해 하위 스마트미터(220)로부터 스마트 디바이스의 에너지 사용량을 수신할 수 있다. 한편, 이러한 서버 트리 구축 정보는 보안 서버(100) 및 유틸리티 시스템(300)으로 송신될 수 있다.

[0061] 키 매트릭스 분배부(222)는 보안 서버(100)로부터 수신하는 키 매트릭스를 상위 스마트미터(210)에서 관리하는 적어도 하나의 하위 스마트미터(220)로 분배할 수 있다. 이와 관련하여, 도 4를 참조하여 설명하기로 한다.

[0062] 도 4를 참조하면, 키 매트릭스 분배부(222)는 보안 서버(100)로부터 매트릭스 형태의 암호화 키를 수신할 수 있다. 또한, 키 매트릭스 분배부(222)는 보안 서버(100)로부터 키 매트릭스 분배 테이블을 수신할 수 있다. 이때, 키 매트릭스 분배 테이블에는 상위 스마트미터(210)의 아이디와 하위 스마트미터(220)의 아이디 별로 키 매트릭스의 행(row) 번호가 매칭되어 있을 수 있다. 키 매트릭스 분배부(222)는 이러한 키 매트릭스 분배 테이블을 참조하여, 상위 스마트미터(210)에서 관리하는 적어도 하나의 하위 스마트미터(220)로 키 매트릭스의 각 행(row)을 분배할 수 있다.

[0063] 예를 들면, 도 4를 참조하면, 상위 스마트미터(U_SM_1)은 키 매트릭스 분배 테이블을 참조하여 제1 하위 스마트미터(L_SM_{11})으로 5 번째 행을 분배하고, 제2 하위 스마트미터(L_SM_{12})로 3 번째 행을 분배하며, 제3 하위 스마트미터(L_SM_{13})로 7 번째 행을 분배할 수 있다.

[0064] 데이터 암호화부(223)는 이와 같이 상위 스마트미터(210)로부터 수신하는 키 매트릭스의 행(row)을 이용하여 복수의 스마트 디바이스로부터 수집하는 스마트 디바이스의 에너지 사용량을 암호화하고, 암호화된 에너지 사용량 정보를 상위 스마트미터(210)로 전송할 수 있다.

[0065] 데이터 병합부(224)는 적어도 하나의 하위 스마트미터(220)로부터 암호화된 에너지 사용량 정보를 수신하면, 수신한 정보를 병합하여 유틸리티 시스템(300)으로 전송할 수 있다. 이와 관련하여, 도 6을 참조하여 설명하기로 한다.

[0066] 도 6은 본 발명의 일 실시예에 따른 스마트 그리드 시스템에서 데이터 병합 및 전송 방법을 설명하기 위한 도면이다.

[0067] 도 6을 참조하면, 적어도 하나의 하위 스마트미터($L_SM_{10}, L_SM_{11}, \dots, L_SM_{1p}$)는 각각 상위 스마트미터(U_SM_1)로부터 수신한 키 매트릭스의 행(row)을 이용하여 스마트 디바이스의 에너지 사용량을 암호화하고, 암호화된 스마트 디바이스의 에너지 사용량 행($R_{10}, R_{11}, \dots, R_{1p}$)을 상위 스마트미터(U_SM_1)로 전송할 수 있다. 상위 스마트미터(U_SM_1)의 데이터 병합부(224)는 이와 같이 적어도 하나의 하위 스마트미터($L_SM_{10}, L_SM_{11}, \dots, L_SM_{1p}$)로부터

수신하는 암호화된 에너지 사용량 행($R_{10}, R_{11}, \dots, R_{1p}$)을 매트릭스 형태로 병합할 수 있다.

- [0068] 그리고, 데이터 병합부(224)는 매트릭스 형태로 병합한 암호화된 에너지 사용량 정보를 열(column) 방향으로 파쇄하고, 각 열을 유틸리티 시스템(300)으로 전송할 수 있다. 이때, 각 열에는 그 순서대로 ID($C_0, \dots, C_q$)가 부여될 수 있다. 데이터 병합부(224)는 각 열에 부여된 ID와 함께 각 열을 유틸리티 시스템(300)으로 전송할 수 있다. 이와 같은 경우, 유틸리티 시스템(300)은 하나의 상위 스마트미터(210)로부터 수신하는 복수의 열을 다시 병합하고, 보안 서버(100)로부터 수신한 키 매트릭스를 이용하여 각 행을 복호화함으로써 복수의 스마트 디바이스의 에너지 사용량을 확인할 수 있다. 이와 관련하여 구체적인 설명은 후술하기로 한다.
- [0069] 한편, 스마트미터 메모리부(230)는 스마트미터(200)의 처리 및 제어를 위한 프로그램이 저장될 수 있으며, 입출력되는 데이터들의 임시 저장을 위한 기능을 수행할 수 있다.
- [0070] 이하에서는, 도 7을 참조하여, 도 5에 도시된 스마트미터(200)의 제어방법에 대하여 설명하기로 한다.
- [0071] 도 7 및 도 8은 도 5에 도시된 스마트미터의 제어방법을 설명하기 위한 순서도이다.
- [0072] 도 7을 참조하면, 스마트미터(200)는 보안 서버(100)에 의해 적어도 하나의 하위 스마트미터(220)를 관리하는 상위 스마트미터(210)로 선택받을 수 있다(700).
- [0073] 스마트미터(200)는 보안 서버(100)에 의해 상위 스마트미터(210)로 선택되면, 보안 서버(100)로부터 기본 키를 수신할 수 있으며(710), 기본 키로부터 서브 키 체인을 생성하고 적어도 하나의 하위 스마트미터(220)로 분배하여 서브 트리를 구축할 수 있다(720).
- [0074] 그리고, 스마트미터(200)는 보안 서버(100)로부터 키 매트릭스를 수신할 수 있으며(730), 키 매트릭스의 각 행(row)을 적어도 하나의 하위 스마트미터(220)로 분배할 수 있다(740).
- [0075] 그리고, 스마트미터(200)는 적어도 하나의 하위 스마트미터(220)로부터 키 매트릭스의 각 행(row)에 의해 암호화된 에너지 사용량 행을 수신하고(750), 적어도 하나의 암호화된 에너지 사용량 행을 매트릭스 형태로 병합할 수 있다(760).
- [0076] 그리고, 스마트미터(200)는 매트릭스 형태로 병합한 암호화된 에너지 사용량 정보를 열(column) 방향으로 파쇄하고, 각 열을 유틸리티 시스템(300)으로 전송할 수 있다(770).
- [0077] 한편, 스마트미터(200)는 보안 서버(100)에 의해 상위 스마트미터(210)로 선택받지 못하면(700), 하위 스마트미터(220)의 역할을 수행할 수 있다. 이와 같은 경우, 도 8을 참조하면, 스마트미터(200)는 상위 스마트미터(210)로부터 키 매트릭스의 행(row)을 수신할 수 있다(800).
- [0078] 그리고, 스마트미터(200)는 홈 영역 네트워크(HAN) 또는 빌딩 영역 네트워크(BAN)에 접속하여 해당 네트워크에 접속된 적어도 하나의 스마트 디바이스의 에너지 사용량을 획득할 수 있다(810).
- [0079] 스마트미터(200)는 적어도 하나의 디바이스의 에너지 사용량을 상위 스마트미터(210)로부터 수신한 키 매트릭스의 행(row)으로 암호화하여, 상위 스마트미터(210)로 송신할 수 있다(820).
- [0080] 이와 같이, 본 발명의 일 실시예에 따른 스마트 그리드 시스템(1000)에 포함되는 복수의 스마트미터(200)는 비교적 많은 연산을 수행하지 않아 에너지 소비 측면에서 효율적이다. 예를 들면, 상위 스마트미터(210)에서 수행하는 가장 큰 연산은 서브 키 체인을 생성하는 것일 수 있는데, 이때, exclusive-OR을 이용할 뿐이므로 비교적 간단하게 서브 키 체인을 생성할 수 있다.
- [0081] 한편, 도 9는 도 1에 도시된 유틸리티 시스템의 제어 블록도이다.
- [0082] 도 9를 참조하면, 유틸리티 시스템(300)은 유틸리티 시스템 통신부(310), 유틸리티 시스템 제어부(320) 및 유틸리티 시스템 메모리부(330)를 포함하여 구성될 수 있으며, 상위 스마트미터(210)로부터 복수의 스마트 디바이스의 에너지 사용 정보를 수신하고 이를 분석하여 추후 에너지 복수의 스마트 디바이스로의 에너지 분배를 제어할 수 있다. 이하, 도 9에 도시된 유틸리티 시스템(300)의 각 구성요소에 대하여 구체적으로 설명하기로 한다.
- [0083] 유틸리티 시스템 통신부(310)는 유틸리티 시스템(300)과 보안 서버(100) 또는 스마트미터(200) 간의 통신을 가능하게 할 수 있으며, 이를 위해, 무선 통신 또는 근거리 무선 통신을 수행하게 하는 하나 이상의 구성요소를 포함하여 구현될 수 있다.
- [0084] 예를 들면, 유틸리티 시스템 통신부(310)는 복수의 스마트미터(200) 중 상위 스마트미터(210)로부터 에너지 사

용 정보를 수신할 수 있다. 또는, 유틸리티 시스템 통신부(310)는 보안 서버(100)로부터 보안 관련 정보를 수신하고, 보안 서버(100)로 상황인지 결과에 따른 정보를 송신할 수 있다.

[0085] 유틸리티 시스템 제어부(320)는 유틸리티 시스템(300)의 전반적인 동작을 제어할 수 있다. 특히, 유틸리티 시스템 제어부(320)는 상위 스마트미터(210)로부터 수신하는 과채된 에너지 사용량 정보를 재병합할 수 있으며, 데이터 전송이 정상적으로 이루어졌는지에 대한 상황인지를 수행할 수 있다. 이를 위해, 유틸리티 시스템 제어부(320)는 데이터 재병합부(321), 데이터 복호화부(322) 및 상황인지부(323)를 포함할 수 있다.

[0086] 데이터 재병합부(321)는 상위 스마트미터(210)로부터 열(column) 방향으로 과채된 암호화된 에너지 사용량 정보를 수신할 수 있다. 이때, 각 열에는 ID가 부여된 상태일 수 있다. 데이터 재병합부(321)는 이러한 각 열에 부여된 ID를 이용하여 각 열을 매트릭스 형태로 재병합할 수 있다.

[0087] 예를 들어, 도 6을 참조하면, 데이터 재병합부(321)는 $C_0, C_j, \dots, C_q$ 의 ID가 부여된 각 열을 수신할 수 있다. 데이터 재병합부(321)는 각 열의 ID에 따라 각 열을 매트릭스 형태로 병합할 수 있다. 이와 같은 경우, 매트릭스의 각 행(row)은 적어도 하나의 하위 스마트미터(220)에서 수집하여 암호화된 홈 영역 네트워크(HAN) 또는 빌딩 영역 네트워크(BAN)의 에너지 사용량 정보일 수 있다.

[0088] 데이터 복호화부(322)는 이와 같이 재병합된 매트릭스의 각 행(row)을 복호화할 수 있다. 이때, 데이터 복호화부(322)는 보안 서버(100)로부터 키 매트릭스를 복호화할 수 있는 페어와이즈(pairwise) 키 및 상위 스마트미터(210)에서의 하위 스마트미터(220)로의 키 매트릭스 분배 테이블 정보를 수신할 수 있다. 데이터 복호화부(322)는 각 열을 송신한 상위 스마트미터(210)를 확인하고, 키 매트릭스를 복호화할 수 있는 페어와이즈(pairwise) 키 및 상위 스마트미터(210)에서의 하위 스마트미터(220)로의 키 매트릭스 분배 테이블을 참조하여, 재병합된 매트릭스의 각 행(row)을 복호화할 수 있다. 이처럼, 데이터 복호화부(322)에 의해 홈 영역 네트워크(HAN) 또는 빌딩 영역 네트워크(BAN)의 전체 에너지 사용량 정보가 확인되며, 유틸리티 시스템(300)은 이러한 정보를 이용하여 각 홈 영역 네트워크(HAN) 또는 빌딩 영역 네트워크(BAN)의 에너지 소비 패턴을 파악하고, 추후 에너지 분배 시 각 홈 영역 네트워크(HAN) 또는 빌딩 영역 네트워크(BAN)의 에너지 소비 패턴에 따라 효율적으로 에너지를 분배할 수 있다.

[0089] 상황인지부(323)는 데이터 복호화부(322)에서의 데이터 복호화 결과에 따라 상위 스마트미터(210)로부터 수신하는 데이터의 손상 여부에 대한 상황인지를 수행하고, 그 결과를 보안 서버(100)로 송신할 수 있다.

[0090] 예를 들면, 상황인지부(323)는 데이터 복호화부(322)에서 데이터가 복호화되지 않거나, 복호화된 데이터가 해당 홈 영역 네트워크(HAN) 또는 빌딩 영역 네트워크(BAN)의 평균 에너지 사용량과 차이가 큰 경우, 상위 스마트미터(210)로부터 데이터 전송 시 외부 공격이 발생하거나, 상위 스마트미터(210)의 보안 체계에 문제가 생긴 것으로 판단할 수 있으며, 해당 정보를 보안 서버(100)로 전송할 수 있다. 보안 서버(100)는 추후 상위 스마트미터(210)를 선택하는 데에 이러한 정보를 반영할 수 있다.

[0091] 유틸리티 시스템 메모리부(330)는 유틸리티 시스템(300)의 처리 및 제어를 위한 프로그램이 저장될 수 있으며, 입출력되는 데이터들의 임시 저장을 위한 기능을 수행할 수 있다.

[0092] 이하에서는, 도 10을 참조하여, 본 발명의 일 실시예에 따른 스마트 그리드 환경에서의 데이터 전송 방법에 대하여 설명하기로 한다. 본 발명의 일 실시예에 따른 스마트 그리드 환경에서의 데이터 전송 방법은 도 1에 도시된 스마트 그리드 시스템(1000)과 실질적으로 동일한 구성에서 진행될 수 있다. 따라서, 도 1의 스마트 그리드 시스템(1000)과 동일한 구성요소는 동일한 도면부호를 부여하고, 반복되는 설명은 생략하기로 한다.

[0093] 도 10은 본 발명의 일 실시예에 따른 스마트 그리드 환경에서의 데이터 전송 방법의 순서도이다.

[0094] 도 10을 참조하면, 보안 서버(100)가 복수의 스마트미터(200) 중 적어도 하나의 상위 스마트미터(210)를 선택할 수 있다(1100).

[0095] 그리고, 보안 서버(100)가 적어도 하나의 상위 스마트미터(210)로 분배할 기본 키 체인을 생성하고(1101), 적어도 하나의 상위 스마트미터(210)로 기본 키를 분배할 수 있다(1102). 이때, 보안 서버(100)는 해쉬 함수에 기반한 기본 키 체인을 생성하고, 생성 방향과 반대 방향에 따라 기본 키를 분배할 수 있다.

[0096] 상위 스마트미터(210)가 보안 서버(100)로부터 기본 키를 수신하면, 기본 키로부터 서브 키 체인을 생성하고, 적어도 하나의 하위 스마트미터(220)로 분배하여 서브 트리를 구축할 수 있다(1103). 상위 스마트미터(210)는 인접한 영역의 적어도 하나의 하위 스마트미터(220)를 관리하며, 해당 하위 스마트미터(220)로부터 홈 영역 네

트위크(HAN) 또는 빌딩 영역 네트워크(BAN)에 접속되는 스마트 디바이스들의 에너지 사용량을 수집할 수 있도록 서버 트리를 구축할 수 있다.

[0097] 또한, 상위 스마트미터(210)가 서버 트리를 구축하면, 해당 정보를 이용하여 보안 서버(100)가 에너지 사용량을 암호화하기 위한 키 매트릭스를 생성하여 적어도 하나의 상위 스마트미터(210)로 송신할 수 있다(1104). 이때, 보안 서버(100)는 키 매트릭스로 암호화되는 정보를 복호화할 수 있는 키 정보를 유틸리티 시스템(300)으로 송신할 수 있다.

[0098] 상위 스마트미터(210)는 보안 서버(100)로부터 키 매트릭스를 수신하면, 각각 관리하는 적어도 하나의 하위 스마트미터(220)로 키 매트릭스의 각 행을 분배할 수 있다(1105).

[0099] 또한, 상위 스마트미터(210)는 각각 관리하는 적어도 하나의 하위 스마트미터(220)로부터 키 매트릭스의 각 행에 의해 암호화된 에너지 사용량 행을 수신하면(1106), 암호화된 에너지 사용량 행을 매트릭스 형태로 병합할 수 있다(1107). 그리고, 상위 스마트미터(210)는 매트릭스 형태로 병합한 에너지 사용량 행을 열 방향으로 파쇄하여 각 열을 유틸리티 시스템(300)으로 송신할 수 있다(1108). 이때, 상위 스마트미터(210)는 각 열에 ID를 부여하여 유틸리티 시스템(300)으로 송신할 수 있다.

[0100] 마지막으로, 유틸리티 시스템(300)은 각 열을 수신하면, 다시 매트릭스 형태로 재병합하여 에너지 사용량을 확인할 수 있다(1109). 유틸리티 시스템(300)은 각 열에 부여된 ID를 이용하여 매트릭스 형태로 재병합할 수 있으며, 보안 서버(100)로부터 수신한 키 정보를 이용하여 매트릭스의 각 행을 복호화함으로써 에너지 사용량을 확인할 수 있다. 유틸리티 시스템(300)은 이에 더하여, 데이터가 손상되었는지 등을 확인하고 해당 정보를 보안 서버(100)로 전송하며, 보안 서버(100)는 이러한 정보를 반영하여 추후 상위 스마트미터(210)를 선택할 수 있다.

[0101] 이와 같은, 본 발명의 일 실시예에 따른 스마트 그리드 환경에서의 데이터 전송 방법은 애플리케이션으로 구현되거나 다양한 컴퓨터 구성요소를 통하여 수행될 수 있는 프로그램 명령어의 형태로 구현되어 컴퓨터 판독 가능한 기록 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능한 기록 매체는 프로그램 명령어, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다.

[0102] 상기 컴퓨터 판독 가능한 기록 매체에 기록되는 프로그램 명령어는 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 분야의 당업자에게 공지되어 사용 가능한 것일 수도 있다.

[0103] 컴퓨터 판독 가능한 기록 매체의 예에는, 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CD-ROM, DVD 와 같은 광기록 매체, 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 ROM, RAM, 플래시 메모리 등과 같은 프로그램 명령어를 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다.

[0104] 프로그램 명령어의 예에는, 컴파일러에 의해 만들어지는 것과 같은 기계어 코드 뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드도 포함된다. 상기 하드웨어 장치는 본 발명에 따른 처리를 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0105] 이상에서는 실시예들을 참조하여 설명하였지만, 해당 기술 분야의 숙련된 당업자는 하기의 특허 청구범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다.

부호의 설명

[0106] 1000: 스마트 그리드 시스템

100: 보안 서버

200: 스마트 미터

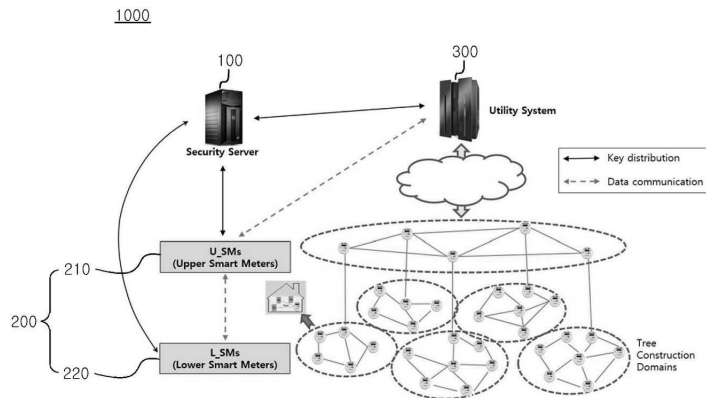
210: 상위 스마트 미터

220: 하위 스마트 미터

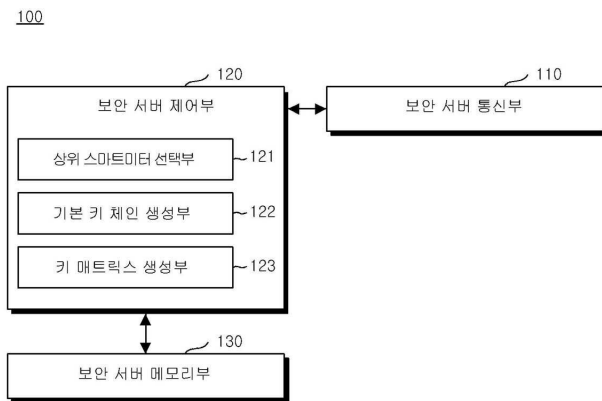
300: 유틸리티 시스템

도면

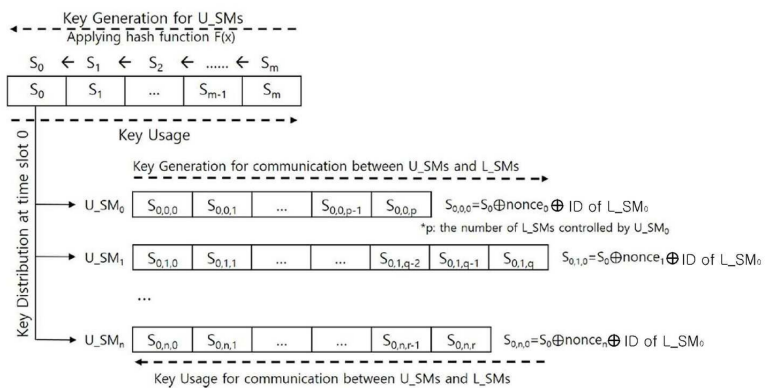
도면1



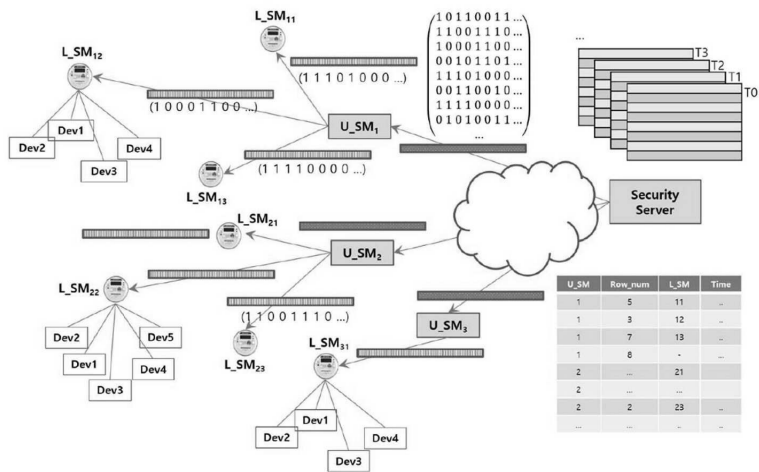
도면2



도면3

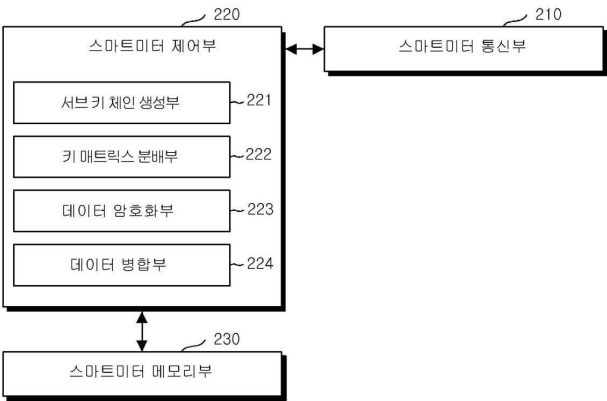


도면4

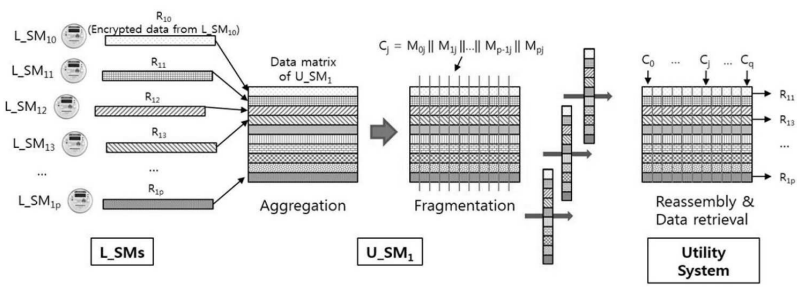


도면5

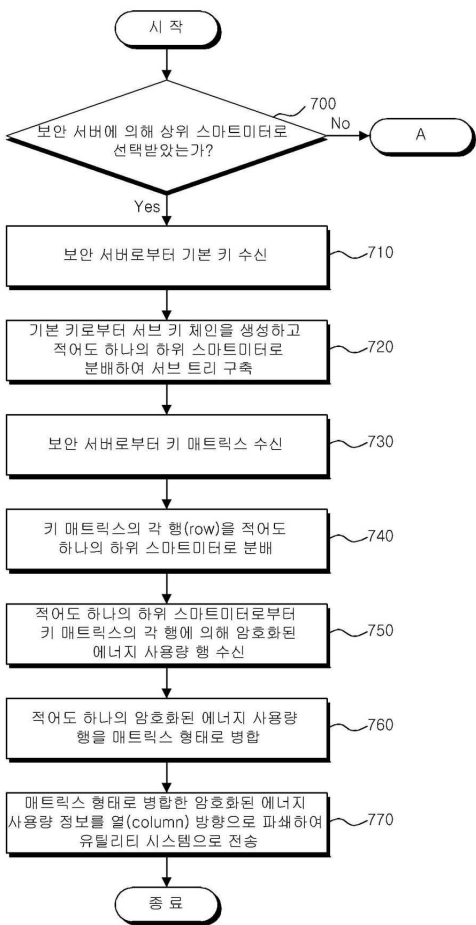
200



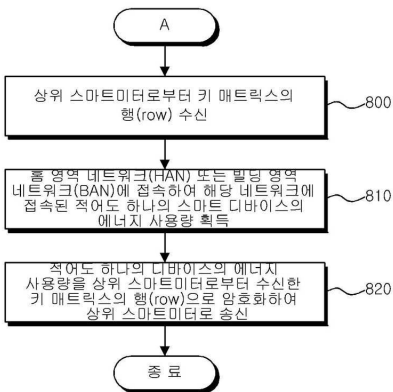
도면6



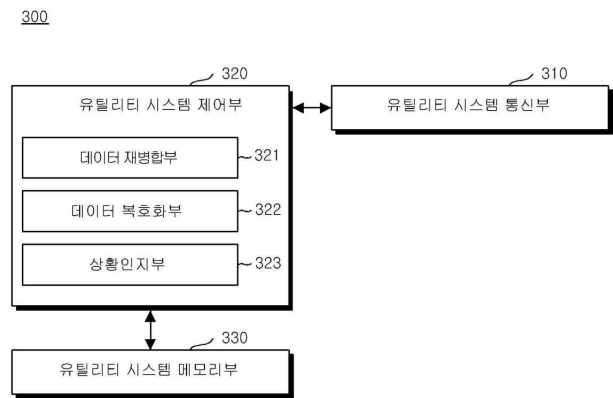
도면7



도면8



도면9



도면10

