



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2013-0066024
(43) 공개일자 2013년06월20일

(51) 국제특허분류(Int. Cl.)

H04L 9/30 (2006.01) H04L 9/32 (2006.01)

(21) 출원번호 10-2011-0132682

(22) 출원일자 2011년12월12일

심사청구일자 2011년12월12일

(71) 출원인

고려대학교 산학협력단

서울 성북구 안암동5가 1

(72) 발명자

이동훈

서울특별시 종로구 사직로8길 34, 경희궁의아침3
단지아파트 1404호 (내수동)

김현

서울특별시 동대문구 회기로4길 13, 301호 (제기
동)

(74) 대리인

박종한

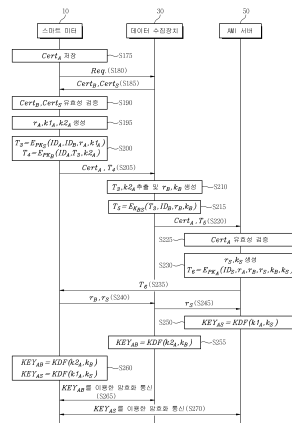
전체 청구항 수 : 총 12 항

(54) 발명의 명칭 공개키 기반의 키 공유 메커니즘을 이용한 보안 키 설정 방법

(57) 요약

본 발명은 스마트 그리드 환경에서, 스마트 미터와 데이터 수집 장치와 AMI 서버 간에 암호화 통신을 위한 보안 키를 효율적으로 설정할 수 있는 공개키 기반의 키 공유 메커니즘을 이용한 보안 키 설정 방법에 관한 것으로서, 암호화 통신을 하고자 하는 두 장치가 각각 두 개의 랜덤값을 생성하고, 공개키 기반 암호화 방식을 통해서 상호 생성한 두 랜덤값을 교환하고, 교환한 상대방의 랜덤값 중 하나의 랜덤값을 다시 상대방에 전달함으로써 상호 키 동의를 수행하고, 키 동의가 이루어지면 두 장치가 각각 생성한 랜덤값 중에서 나머지 랜덤값을 이용하여 보안 키를 설정하는 것이다.

대표도 - 도3



이 발명을 지원한 국가연구개발사업

과제고유번호	ITAC1090111100020001000100100
부처명	정보통신산업진흥원
연구사업명	대학IT연구센터육성지원사업
연구과제명	스마트 그리드 보안 연구센터(스마트 그리드 보안기술발)
주관기관	고려대학교 산학협력단
연구기간	2011.01.01 ~ 2011.12.31

특허청구의 범위

청구항 1

제1 장치가 제2 장치에서 생성된 제1, 제2 랜덤값을 포함하고 제1 장치의 공개키로 암호화된 제1 메시지를 제2 장치로부터 수신하는 단계;

상기 제1 장치가 상기 수신한 제1 메시지에 포함된 제1 랜덤값, 자신이 생성한 제3, 제4 랜덤값을 포함하고 상기 제2 장치의 공개키로 암호화된 제2 메시지를 상기 제2 장치로 전송하는 단계; 및

제1 장치가 상기 제2 메시지의 전송 후에 상기 제2 장치로부터 제3 랜덤값이 수신되면, 키 동의를 이루어진 것으로 판단하여, 상기 제1 메시지에 포함된 제2 랜덤값 및 자신이 생성한 제4 랜덤값으로부터 제2 장치와의 암호화 통신에 사용될 제1 보안 키를 생성하는 단계를 포함하는 것을 특징으로 하는 공개키 기반의 키 공유 메커니즘을 이용한 보안 키 설정 방법.

청구항 2

제1항에 있어서,

상기 제1 장치가, 상기 제1 메시지를 제2 장치로부터 수신하기 전에, 제2 장치로부터의 보안 키 설정 요청에 따라서 자신의 인증서를 상기 제1 장치로 전송하는 단계를 더 포함하는 것을 특징으로 하는 공개키 기반의 키 공유 메커니즘을 이용한 보안 키 설정 방법.

청구항 3

제1항에 있어서,

상기 제1 장치는 상기 제2 장치의 인증서를 상기 제1 메시지와 함께 수신하여, 상기 제2 장치의 인증서에 대한 유효성을 검증하는 단계를 더 포함하고,

상기 제2 장치의 인증서가 유효한 경우, 상기 제2 메시지를 제2 장치로 전송하도록 하는 것을 특징으로 하는 공개키 기반의 키 공유 메커니즘을 이용한 보안 키 설정 방법.

청구항 4

제1항에 있어서,

제1 장치가 제3 장치에서 생성된 제5, 제6 랜덤값을 포함하고 제1 장치의 공개키로 암호화된 제3 메시지 및 제2 장치에서 생성된 제1, 제2 랜덤값을 포함하고, 상기 제1 보안키로 암호화된 메시지를 상기 제2 장치로부터 수신하는 단계;

상기 제1 장치가 상기 제3 메시지에 포함된 제5 랜덤값, 상기 제2 장치로부터 수신된 메시지에 포함된 제1, 제2 랜덤값 및 자신이 생성한 제3, 제4 랜덤값을 포함하고 제3 장치의 공개키로 암호화된 제6 메시지를 상기 제3 장치로 전송하는 단계;

제1 장치가 상기 제6 메시지를 전송한 후, 제2 장치를 통해 제3 장치로부터 제3 랜덤값이 수신되면 키 동의를 이루어진 것으로 판단하여, 자신이 생성한 제4 랜덤값 및 상기 제3 메시지에 포함된 제6 랜덤값을 이용하여 제3 장치와의 암호화 통신에 사용될 제2 보안키를 생성하는 단계를 더 포함하는 것을 특징으로 하는 공개키 기반의 키 공유 메커니즘을 이용한 보안 키 설정 방법.

청구항 5

제4항에 있어서,

상기 제1 장치는 제2 장치를 통해 상기 제3 장치의 인증서를 수신하고 수신된 제3 장치의 인증서에 대한 유효성을 검증하는 단계를 더 포함하고,

상기 제3 장치의 인증서가 유효한 경우, 상기 제6 메시지를 제3 장치로 전송하도록 하는 것을 특징으로 하는 공개키 기반의 키 공유 메커니즘을 이용한 보안 키 설정 방법.

청구항 6

제2 장치가, 자신이 생성한 제1, 제2 랜덤값을 포함하고 제1 장치의 공개키로 암호화된 제1 메시지를 제1 장치로 전송하는 단계;

상기 제2 장치가 제1 장치에서 생성된 제3, 제4 랜덤값 및 상기 제1 랜덤값을 포함하고 제2 장치의 공개키로 암호화된 제2 메시지를 수신하는 단계;

상기 제2 장치가 상기 제2 메시지를 복호화하여 제2 메시지에 포함된 상기 제3, 제4 랜덤값중에서 제3 랜덤값을 제1 장치로 전송하는 단계; 및

상기 제2 장치가 상기 제2 메시지에 포함된 제1 랜덤값을 확인하여, 상기 생성한 제1 랜덤값과 일치하는 경우, 키 동의가 이루어진 것으로 판단하여, 자신이 생성한 제2 랜덤값 및 상기 제2 메시지에 포함된 제4 랜덤값으로부터 제1 장치와의 암호화 통신에 사용될 제1 보안 키를 생성하는 단계를 포함하는 것을 특징으로 하는 공개키 기반의 키 공유 메커니즘을 이용한 보안 키 설정 방법.

청구항 7

제6항에 있어서,

제2 장치가 키 설정 요청을 제1 장치로 전송하여 상기 제1 장치의 인증서를 수신하는 단계; 및

상기 제2 장치가 상기 제1 장치의 인증서에 대한 유효성을 검증하는 단계를 더 포함하고,

상기 제1 장치의 인증서가 유효한 경우, 상기 제1 메시지를 제1 장치로 전송하도록 하는 것을 특징으로 하는 공개키 기반의 키 공유 메커니즘을 이용한 보안 키 설정 방법.

청구항 8

제6항에 있어서, 상기 제2 장치가,

제3 장치에서 생성된 제5, 제6 랜덤값을 포함하고 제1 장치의 공개키로 암호화된 제3 메시지, 제3 장치에서 생성된 제7 랜덤값을 포함하고 제2 장치의 공개키로 암호화된 제4 메시지를 제3 장치로부터 수신하는 단계;

상기 제4 메시지에 포함된 제3 메시지, 자신이 생성한 제1, 제2 랜덤값을 포함하고 제1 보안키로 암호화된 제5 메시지를 제1 장치로 전송하는 단계;

상기 제3 장치로부터 제1 랜덤값 및 제3 랜덤값을 수신하여, 제3 랜덤값을 상기 제1 장치로 전송하는 단계;

상기 수신한 제1 랜덤값이 상기 자신이 생성한 제1 랜덤값과 일치하면, 상기 제4 메시지에 포함된 제7 랜덤값과 상기 자신이 생성한 제2 랜덤값을 이용하여, 제3 장치와의 암호화 통신을 위한 제3 보안키를 생성하는 단계를 더 포함하는 것을 특징으로 하는 공개키 기반의 키 공유 메커니즘을 이용한 보안 키 설정 방법.

청구항 9

제8항에 있어서,

상기 제2 장치가 상기 제4 메시지를 수신하기 전에, 제3 장치로부터의 키 설정 요청이 수신되면, 상기 제3 장치로 자신의 인증서와 상기 제1 장치의 인증서를 전송하는 단계를 더 포함하는 것을 특징으로 하는 공개키 기반의 키 공유 메커니즘을 이용한 보안 키 설정 방법.

청구항 10

제8항에 있어서, 상기 제2 장치는

제3 장치로부터 상기 제4 메시지와 함께 제3 장치의 인증서를 수신하고, 상기 수신한 제3 장치의 인증서를 상기 제5 메시지와 함께 제1 장치로 전송하는 것을 특징으로 하는 공개키 기반의 키 공유 메커니즘을 이용한 보안 키 설정 방법.

청구항 11

제3 장치가 제1, 제2 장치와의 암호화 통신을 위한 보안 키를 설정하는 방법에 있어서, 상기 제3 장치가

제5, 제6, 제7 랜덤값을 생성하고, 상기 제5, 제6 랜덤값을 제1 장치의 공개키로 암호화한 제3 메시지를 생성하고, 상기 제3 메시지, 제3 장치의 식별 정보 및 상기 제7 랜덤값을 상기 제2 장치의 공개키로 암호화한 제4 메시지를 생성하여, 상기 제4 메시지를 제2 장치로 전송하는 단계;

상기 제2 장치를 통해 상기 제3 메시지를 수신한 제1 장치로부터, 제2 장치에서 생성된 제1, 제2 랜덤값, 제1 장치에서 생성된 제3, 제4 랜덤값 및 상기 제5 랜덤값을 포함하고 제3 장치의 공개키로 암호화된 제6 메시지를 수신하는 단계;

상기 제6 메시지에서 제1, 제3 랜덤값을 추출하여, 상기 제2 장치로 전송하는 단계;

상기 제6 메시지에 포함된 제5 랜덤값과 자신이 생성한 제5 랜덤값이 일치하면, 상기 제6 메시지에 포함된 제2 랜덤값과 자신이 생성한 제7 랜덤값으로부터 제2 장치와의 암호화 통신을 위한 제3 보안 키를 생성하고, 상기 제6 메시지에 포함된 제4 랜덤값과 자신이 생성한 제6 랜덤값으로부터 제1 장치와의 암호화 통신을 위한 제2 보안 키를 생성하는 단계를 포함하는 것을 특징으로 하는 공개키 기반의 키 공유 메커니즘을 이용한 보안 키 설정 방법.

청구항 12

제11항에 있어서,

상기 제3 장치가 제2 장치로 키 설정을 요청하여, 제1, 제2 장치의 인증서를 획득하는 단계;

제1, 제2 장치의 인증서에 대한 유효성을 검증하는 단계를 더 포함하여,

상기 제1, 제2 장치의 인증서가 유효한 경우, 상기 제4 메시지를 제2 장치로 전송하도록 하는 것을 특징으로 하는 공개키 기반의 키 공유 메커니즘을 이용한 보안 키 설정 방법.

명세서

기술분야

[0001] 본 발명은 스마트 그리드 환경에서, 스마트 미터와 데이터 수집 장치와 AMI(Advanced Metering Infrastructure) 서버 간에 암호화 통신을 위한 보안 키를 효율적으로 설정할 수 있는 스마트 그리드에서의 보안 키 설정 방법에 관한 것이다.

배경기술

[0002] 기술의 고도화와 경제 성장에 따라 전력의 생산 및 공급은 전 세계적으로 가장 중요한 필수요소로 자리매김하였으나, 아직 화석연료에 의존하여, 그 효율성은 매우 낮은 편이다. 이러한 화석연료의 사용으로 인해 환경파괴에 대한 경각심이 늘어나게 되었고, 기존의 단방향 전력망 시스템에 정보통신 기술을 접목한 스마트 그리드(Smart Grid) 기술에 대한 관심이 선진국을 중심으로 증대되어 활발하게 연구가 진행되고 있다.

[0003] 스마트 그리드는 기존의 전력망에 정보기술(IT)을 접목하여 전력 공급자와 소비자가 양방향으로 실시간 정보를 교환함으로써 전력 공급 및 사용의 효율성을 증대시키는 차세대 지능형 전력망이다.

[0004] 스마트 그리드에서는 전기로 작동되는 모든 기기들이 유·무선 네트워크로 연결되며, 서로 간의 정보 교환을 통하여 유기적인 관계로 이루어진다. 기존의 전력 시스템은 전력사용예측이 불가능하기 때문에 일반적으로 10%이상의 예비전력을 보유하여 저장하고 있으나, 스마트 그리드 환경에서는 스마트 미터(Smart Meter)를 통해 실시간으로 사용되는 에너지를 분석함으로써 전력 사용 예측이 가능하여, 에너지를 효율적으로 분배할 수 있다.

[0005] 이러한 스마트 그리드의 핵심 인프라로 원격 검침 시스템인 AMI(Advanced Metering Infrastructure)가 있다. 이는 에너지를 효율적으로 관리하기 위한 체계로써, 도 1에 도시된 바와 같이, 각 가정 내 설치되어 각 가정의 디바이스 이용 정보 및 전력 이용량을 측정하는 스마트 미터(10)와, 상기 스마트 미터(10)를 통해 각 가정의 디바이스 이용 정보 및 전력 이용량을 수집하는 AMI 서버(50)로 구성된다. 이때, 상기 AMI 서버(50)는 데이터 수집 장치(Data collection Unit)(30)의 매개로 다수 스마트 미터(10)의 데이터를 수집할 수 있다. 여기서, 데이터 수집 장치(30)는 인접한 다수의 스마트 미터(10)와 NAN(Neighborhood Area Network)를 통해서 통신하고, AMI 서버(50)와는 WAN(Wide Area network)를 통해서 통신한다.

[0006] 이러한 AMI를 통해 실시간 에너지 사용량 정보를 수집할 수 있으며, 이를 기반으로 에너지를 관리함으로써 가정

및 기업의 에너지 비용을 절감할 수 있으며, 전체의 에너지 사용량을 효율적으로 관리할 수 있다.

[0007] AMI는 최종 소비자와 전력회사 사이의 전력 서비스 정보화 인프라로서 스마트 그리드 운용에 필수적인 스마트 미터 기반의 핵심 인프라 시스템이다. 단순히 계량 값을 읽어가는 기존의 AMR(Automated Meter Reading)과는 다르게 스마트 미터를 중심으로 양방향 통신과 오픈 프로토콜(Open Protocol)에 기반해 원격 전력 차단(Remote Connect/Disconnect)이 가능하고, 선불요금제(Prepayment), 실시간 요금제(RTP), 피크 요금제(Critical Peak Pricing), TOU(Time-of-Use) 요금제 등 다양한 요금제의 적용을 가능하게 한다.

[0008] 스마트 그리드 시스템이 이렇게 다양한 장점을 가지는 반면, 외부 네트워크에서 접근이 불가능한 폐쇄적인 구조이기 때문에 보안에 대한 별다른 위협이 없었던 기존의 전력망 시스템과 달리, 유, 무선을 통한 외부네트워크 접속이 가능해지고 각 가정의 스마트 미터로 접속할 수 있기 때문에 해킹, 악성코드 웜 및 바이러스들과 같은 다양한 위협요소에 노출될 수 있으며, 이로 인해 소비자의 개인정보 노출 및 산업 시스템 마비 등의 손실을 발생할 수 있다는 문제점이 있다.

[0009] 때문에 스마트 그리드에 있어서, 보안성 강화를 위해 AMI 미터(10)에 대한 인증은 반드시 필요하다.

발명의 내용

해결하려는 과제

[0010] 본 발명은 스마트 그리드 환경에서, 스마트 미터와 데이터 수집 장치와 AMI 서버 간에 암호화 통신을 위한 보안 키를 효율적으로 설정할 수 있는 공개키 기반의 키 공유 메커니즘을 이용한 보안 키 설정 방법을 제공하고자 한다.

과제의 해결 수단

[0011] 상술한 과제의 해결 수단으로서, 본 발명은 제1 장치가 제2 장치에서 생성된 제1, 제2 랜덤값을 포함하고 제1 장치의 공개키로 암호화된 제1 메시지를 제2 장치로부터 수신하는 단계; 상기 제1 장치가 상기 수신한 제1 메시지에 포함된 제1 랜덤값, 자신이 생성한 제3, 제4 랜덤값을 포함하고 상기 제2 장치의 공개키로 암호화된 제2 메시지를 상기 제2 장치로 전송하는 단계; 및 제1 장치가 상기 제2 메시지의 전송 후에 상기 제2 장치로부터 제3 랜덤값이 수신되면, 키 동의를 이루어진 것으로 판단하여, 상기 제1 메시지에 포함된 제2 랜덤값 및 자신이 생성한 제4 랜덤값으로부터 제2 장치와의 암호화 통신에 사용될 제1 보안 키를 생성하는 단계를 포함하는 것을 특징으로 하는 공개키 기반의 키 공유 메커니즘을 이용한 보안 키 설정 방법을 제공한다.

[0012] 상기 보안 키 설정 방법은, 상기 제1 장치가, 상기 제1 메시지를 제2 장치로부터 수신하기 전에, 제2 장치로부터의 보안 키 설정 요청에 따라서 자신의 인증서를 상기 제1 장치로 전송하는 단계를 더 포함할 수 있다.

[0013] 상기 보안 키 설정 방법은, 상기 제1 장치는 상기 제2 장치의 인증서를 상기 제1 메시지와 함께 수신하여, 상기 제2 장치의 인증서에 대한 유효성을 검증하는 단계를 더 포함하고, 상기 제2 장치의 인증서가 유효한 경우, 상기 제2 메시지를 제2 장치로 전송하도록 할 수 있다.

[0014] 상기 보안 키 설정 방법은, 제1 장치가 제3 장치에서 생성된 제5, 제6 랜덤값을 포함하고 제1 장치의 공개키로 암호화된 제3 메시지 및 제2 장치에서 생성된 제1, 제2 랜덤값을 포함하고, 상기 제1 보안키로 암호화된 메시지를 상기 제2 장치로부터 수신하는 단계; 상기 제1 장치가 상기 제3 메시지에 포함된 제5 랜덤값, 상기 제2 장치로부터 수신된 메시지에 포함된 제1, 제2 랜덤값 및 자신이 생성한 제3, 제4 랜덤값을 포함하고 제3 장치의 공개키로 암호화된 제6 메시지를 상기 제3 장치로 전송하는 단계; 제1 장치가 상기 제6 메시지를 전송한 후, 제2 장치를 통해 제3 장치로부터 제3 랜덤값이 수신되면 키 동의를 이루어진 것으로 판단하여, 자신이 생성한 제4 랜덤값 및 상기 제3 메시지에 포함된 제6 랜덤값을 이용하여 제3 장치와의 암호화 통신에 사용될 제2 보안키를 생성하는 단계를 더 포함할 수 있다.

[0015] 상기 보안 키 설정 방법은, 상기 제1 장치는 제2 장치를 통해 상기 제3 장치의 인증서를 수신하고 수신된 제3 장치의 인증서에 대한 유효성을 검증하는 단계를 더 포함하고, 상기 제3 장치의 인증서가 유효한 경우, 상기 제6 메시지를 제3 장치로 전송하도록 할 수 있다.

[0016] 또한, 본 발명은 상술한 과제를 해결하기 위한 다른 수단으로서, 제2 장치가, 자신이 생성한 제1, 제2 랜덤값을 포함하고 제1 장치의 공개키로 암호화된 제1 메시지를 제1 장치로 전송하는 단계; 상기 제2 장치가 제1 장치에서 생성된 제3, 제4 랜덤값 및 상기 제1 랜덤값을 포함하고 제2 장치의 공개키로 암호화된 제2 메시지를 수신하

는 단계; 상기 제2 장치가 상기 제2 메시지를 복호화하여 제2 메시지에 포함된 상기 제3, 제4 랜덤값중에서 제3 랜덤값을 제1 장치로 전송하는 단계; 및 상기 제2 장치가 상기 제2 메시지에 포함된 제1 랜덤값을 확인하여, 상기 생성한 제1 랜덤값과 일치하는 경우, 키 동의가 이루어진 것으로 판단하여, 자신이 생성한 제2 랜덤값 및 상기 제2 메시지에 포함된 제4 랜덤값으로부터 제1 장치와의 암호화 통신에 사용될 제1 보안 키를 생성하는 단계를 포함하는 것을 특징으로 하는 공개키 기반의 키 공유 메커니즘을 이용한 보안 키 설정 방법을 제공한다.

[0017] 상기 보안 키 설정 방법은, 제2 장치가 키 설정 요청을 제1 장치로 전송하여 상기 제1 장치의 인증서를 수신하는 단계; 및 상기 제2 장치가 상기 제1 장치의 인증서에 대한 유효성을 검증하는 단계를 더 포함하고, 상기 제1 장치의 인증서가 유효한 경우, 상기 제1 메시지를 제1 장치로 전송하도록 할 수 있다.

[0018] 상기 보안 키 설정 방법은, 상기 제2 장치가, 제3 장치에서 생성된 제5, 제6 랜덤값을 포함하고 제1 장치의 공개키로 암호화된 제3 메시지, 제3 장치에서 생성된 제7 랜덤값을 포함하고 제2 장치의 공개키로 암호화된 제4 메시지를 제3 장치로부터 수신하는 단계; 상기 제4 메시지에 포함된 제3 메시지, 자신이 생성한 제1, 제2 랜덤값을 포함하고 제1 보안키로 암호화된 제5 메시지를 제1 장치로 전송하는 단계; 상기 제3 장치로부터 제1 랜덤값 및 제3 랜덤값을 수신하여, 제3 랜덤값을 상기 제1 장치로 전송하는 단계; 상기 수신한 제1 랜덤값이 상기 자신이 생성한 제1 랜덤값과 일치하면, 상기 제4 메시지에 포함된 제7 랜덤값과 상기 자신이 생성한 제2 랜덤값을 이용하여, 제3 장치와의 암호화 통신을 위한 제3 보안키를 생성하는 단계를 더 포함할 수 있다.

[0019] 상기 보안 키 설정 방법은, 상기 제2 장치가 상기 제4 메시지를 수신하기 전에, 제3 장치로부터의 키 설정 요청이 수신되면, 상기 제3 장치로 자신의 인증서와 상기 제1 장치의 인증서를 전송하는 단계를 더 포함할 수 있으며, 제3 장치로부터 상기 제4 메시지와 함께 제3 장치의 인증서를 수신하고, 상기 수신한 제3 장치의 인증서를 상기 제5 메시지와 함께 제1 장치로 전송할 수 있다.

[0020] 더하여 본 발명은 상술한 과제를 해결하기 위한 또 다른 수단으로서, 제3 장치가 제1, 제2 장치와의 암호화 통신을 위한 보안 키를 설정하는 방법에 있어서, 상기 제3 장치가, 제5, 제6, 제7 랜덤값을 생성하고, 상기 제5, 제6 랜덤값을 제1 장치의 공개키로 암호화한 제3 메시지를 생성하고, 상기 제3 메시지, 제3 장치의 식별 정보 및 상기 제7 랜덤값을 상기 제2 장치의 공개키로 암호화한 제4 메시지를 생성하여, 상기 제4 메시지를 제2 장치로 전송하는 단계; 상기 제2 장치를 통해 상기 제3 메시지를 수신한 제1 장치로부터, 제2 장치에서 생성된 제1, 제2 랜덤값, 제1 장치에서 생성된 제3, 제4 랜덤값 및 상기 제5 랜덤값을 포함하고 제3 장치의 공개키로 암호화된 제6 메시지를 수신하는 단계; 상기 제6 메시지에서부터 제1, 제3 랜덤값을 추출하여, 상기 제2 장치로 전송하는 단계; 및 상기 제6 메시지에 포함된 제5 랜덤값과 자신이 생성한 제5 랜덤값이 일치하면, 상기 제6 메시지에 포함된 제2 랜덤값과 자신이 생성한 제7 랜덤값으로부터 제2 장치와의 암호화 통신을 위한 제3 보안 키를 생성하고, 상기 제6 메시지에 포함된 제4 랜덤값과 자신이 생성한 제6 랜덤값으로부터 제1 장치와의 암호화 통신을 위한 제2 보안 키를 생성하는 단계를 포함하는 것을 특징으로 하는 공개키 기반의 키 공유 메커니즘을 이용한 보안 키 설정 방법을 제공할 수 있다.

[0021] 상기 보안 키 설정 방법은, 상기 제3 장치가 제2 장치로 키 설정을 요청하여, 제1, 제2 장치의 인증서를 획득하는 단계; 제1, 제2 장치의 인증서에 대한 유효성을 검증하는 단계를 더 포함하여, 상기 제1, 제2 장치의 인증서가 유효한 경우, 상기 제4 메시지를 제2 장치로 전송하도록 할 수 있다.

발명의 효과

[0022] 본 발명에 따르면, 스마트 그리드 시스템에 있어서, 공개 키 기반의 키 동의 메커니즘을 이용하여 수용가에 설치된 스마트 미터, 다수 스마트 미터 간의 데이터를 수집하는 데이터 수집 장치, 및 AMI 서버 간에 암호화 통신을 위한 보안 키를 설정함으로써, 미리 암호화를 위한 키를 설정하는 일 없이 보안 키의 설정이 가능하며, 더불어 키 수립을 위해 전송되는 데이터 및 설정된 키에 대한 기밀성을 유지할 수 있으며, 또한 적은 연산량으로 양방향 인증 및 키 설정이 가능한 효과가 있다.

도면의 간단한 설명

[0023] 도 1은 본 발명이 적용되는 스마트 그리드의 AMI 구조를 나타낸 블록도이다.

도 2는 본 발명의 일 실시 예에 따른 데이터 수집 장치와 AMI 서버간 보안 키 설정 절차를 나타낸 메시지 흐름도이다.

도 3은 본 발명의 일 실시 예에 따른 스마트 미터에 대한 보안 키 설정 절차를 나타낸 메시지 흐름도이다.

발명을 실시하기 위한 구체적인 내용

- [0024] 이하 본 발명의 바람직한 실시 예를 첨부한 도면을 참조하여 상세히 설명한다. 다만, 하기의 설명 및 첨부된 도면에서 본 발명의 요지를 흐릴 수 있는 공지 기능 또는 구성에 대한 상세한 설명은 생략한다. 또한, 도면 전체에 걸쳐 동일한 구성 요소들은 가능한 한 동일한 도면 부호로 나타내고 있음에 유의하여야 한다.
- [0025] 도 1과 같은 스마트 그리드의 AMI 환경에서, 보안성을 보장하기 위해서는, 통신하는 기기, 구체적으로 스마트 미터(10)와 데이터 수집 장치(30)와 AMI 서버(50) 간의 최초 인증 및 키 설정 시 전송되는 데이터, 수요 반응(DR: Demand Response) 정보를 포함하여 AMI 서버(50)와 주고받는 주요 데이터들, 및 데이터 수집 장치(30)에 저장되는 검침 정보에 대한 기밀성(confidentiality) 유지, AMI의 각 통신 구간(스마트 미터(10)와 데이터 수집 장치(30) 구간, 데이터 수집 장치(30)와 AMI 서버(50) 구간, 스마트 미터(10)와 AMI 서버(50) 구간 등)을 통해 전송되는 모든 정보에 대한 무결성(Integrity) 보장, 검침 정보나 수요 반응 정보 등에 대한 부인 방지(Non-repudiation), 최초 기기 등록시의 상호 인증(Authentication)이 필요하다.
- [0026] 본 발명은 상술한 보안 요구 사항 중에서, 스마트 그리드에서의 키 수립 시 전송되는 데이터에 대한 기밀성 유지와 관련된다.
- [0027] 본 발명은 스마트 그리드의 AMI 구현에 있어서, 스마트 미터(10)와 데이터 수집 장치(30)와 AMI 서버(50) 간의 보안 키를 수립하는데 있어서, 공개 키 기반의 키 동의 매커니즘을 이용한다. 구체적으로는, ISO/IEC 11770-3에서 제안된 키 동의 매커니즘들에 대한 분석을 통해서, 양방향 인증이 가능하며 연산량이 적은 키 동의 매커니즘을 선택하여 이용한다. 본 발명에서 이용되는 키 동의 매커니즘은 보안 키를 수립하고자 하는 두 장치가 각각 랜덤값을 생성하고, 공개키 구조를 통해 생성한 랜덤값의 교환을 통해서 키 동의를 수행하는 것으로서, 본 발명은 이러한 공개키 구조의 키 동의 매커니즘을 이용하여 스마트 미터(10)와 데이터 수집 장치(30)와 AMI 서버(50) 간의 암호화 통신에 사용될 보안 키를 안정적이면서 효율적으로 설정하고자 한다.
- [0028] 이러한 본 발명에 따른 공개 키 기반의 키 동의 매커니즘을 이용한 보안 키 설정 방법을 이하에서 구체적으로 설명하는데 있어서, 이해의 편의를 위하여, 데이터 수집 장치(30)에서 키 동의를 위하여 생성되는 두 개의 랜덤값을 제1, 제2 랜덤값이라 하고, AMI 서버(50)에서 키 동의를 위하여 생성되는 두 개의 랜덤값을 제3, 제4 랜덤값이라 하고, 스마트 미터(50)에서 키 동의를 위하여 생성되는 세 개의 랜덤값을 제5, 제6, 제7 랜덤값이라 부르기로 한다.
- [0029] 도 2 및 도 3은 본 발명에 따른 보안 키 설정 방법을 나타낸 메시지 흐름도로서, 도 1에 나타난 AMI 구조에 적용된 예를 도시한 것이다.
- [0030] 본 발명에 따르면, 먼저, 일정 범위 내에 위치한 다수의 스마트 미터(10)로부터 전송된 데이터를 수집하여 저장한 후, 일정 주기로 AMI 서버(50)로 전송하는 데이터 수집 장치(30)와 AMI 서버(50) 간의 보안 키 설정이 이루어지며, 그 과정을 도 2를 참조하여 설명하면 다음과 같다.
- [0031] 먼저, 데이터 수집 장치(30)와 AMI 서버(50)는 공개키 기반의 키 동의 절차를 수행하기 위하여, 각각 자신의 공개키를 인증하기 위한 자신의 인증서($Cert_B$, $Cert_S$)는 데이터 수집 장치(30)와 AMI 서버(50) 양측에서 모두 신뢰할 수 있는 공인된 인증 기관(CA: Certification Authority)에서 발급될 수 있으며, 상기 인증 기관을 통해서 유효성을 검증할 수 있다.
- [0032] 더불어, 데이터 수집 장치(30)와 AMI 서버(50) 간의 보안 키 설정은, 데이터 수집 장치(30)가 AMI 서버(50)로 보안 키 설정 요청(Request)을 전송함에 의해 시작될 수 있다(S115).
- [0033] 그리고, 데이터 수집 장치(30)로부터 보안 키 설정 요청을 수신한 AMI 서버(50)는 공개키에 대한 인증을 위해서, 자신의 인증서($Cert_S$)를 데이터 수집 장치(30)로 전송할 수 있다(S120).
- [0034] 상기 데이터 수집 장치(30)는 보안 키 설정 요청 후 수신된 AMI 서버(50)의 인증서($Cert_S$)에 대한 유효성을 검증하여(S125), 상기 인증서($Cert_S$)가 유효한 경우, 두 개의 랜덤값 r_B , k_B (이하, 제1, 제2 랜덤값이라 함)을 생성하고, 상기 생성한 제1, 제2 랜덤값을 AMI 서버(50)의 공개키로 암호화하여 제1 메시지(T_1)를 생성

한다(S130). 여기서, 자신을 식별할 수 있는 데이터 수집 장치(30)의 식별 정보(ID_B)를 상기 제1, 제2 랜덤값과 함께 암호화할 수 있다.

[0035] 그리고 데이터 수집 장치(30)는 상기 생성한 제1 메시지를 AMI 서버(50)로 전송한다(S135). 이때, 상기 데이터 수집 장치(30)는 제1 메시지와 함께 자신의 인증서($Cert_B$)를 더 전송할 수 있다.

[0036] AMI 서버(50)는 상기 데이터 수집 장치(30)에서 생성한 제1, 제2 랜덤값을 포함하는 암호화된 제1 메시지 및 데이터 수집 장치(30)의 인증서를 수신하면, 상기 수신된 데이터 수집 장치(30)의 인증서에 대한 유효성을 검증하고(S140), 상기 데이터 수집 장치(30)의 인증서가 유효한 경우, 두 개의 랜덤값 r_s , k_s (이하, 제3, 제4 랜덤값이라 함)을 생성하고, 상기 생성한 제3, 제4 랜덤값을 데이터 수집 장치(30)로 전달하기 위한 제2 메시지(T_2)를 생성한다(S145). 상기 제2 메시지는 자신이 생성한 제3, 제4 랜덤값을 데이터 수집 장치(30)의 공개키로 암호화하여 생성할 수 있으며, 데이터 수집 장치(30)로부터 제1, 제2 랜덤값을 수신하였음을 확인하기 위해 상기 수신한 제1 메시지에서 획득한 제1 랜덤값과, 보안 키 설정 대상을 식별하기 위한 자신, 즉, AMI 서버(50)의 식별 정보(ID_S)가 더 포함되어 암호화될 수 있다.

[0037] AMI 서버(50)는 상기 생성한 제2 메시지를 데이터 수집 장치(30)로 전송한다(S150).

[0038] 그리고, AMI 서버(50)로부터 전송된 제2 메시지를 수신한 데이터 수집 장치(30)는 수신한 제2 메시지를 자신의 비밀키로 복호화하여 해당 메시지에 포함된 제1 랜덤값, 제3, 제4 랜덤값을 획득한 후, 이 중 제3 랜덤값 r_s 을 AMI 서버(50)로 전송하여, 자신이 제3, 제4 랜덤값을 안전하게 수신하였음을 알린다(S155).

[0039] 이상의 과정을 통해서, 각자 자신이 생성한 두 랜덤값을 서로 교환하고, 상대방이 이를 수신하였음을 확인한 AMI 서버(50)와 데이터 수집 장치(30)는 각각, 자신이 수신한 메시지(제1 메시지 또는 제2 메시지)에서 획득한 상대방의 랜덤값중 하나(제2 랜덤값 또는 제4 랜덤값)과 자신이 생성한 랜덤값중 하나(제4 랜덤값 또는 제2 랜덤값)으로부터 상호간의 암호화 통신에 사용할 공통의 보안 키 KEY_{BS} (이하, 제1 보안키라 함)를 도출하여 설정한다(S160, S165). 이때, 상기 제1 보안키는 특정 키 유도 함수(Key derivation function)를 통해서 도출될 수 있다.

[0040] 상기에 의하여, 데이터 수집 장치(30)와 AMI 서버(50)는 상호간에 암호화 통신에 사용할 동일한 제1 보안키를 설정할 수 있게 되며, 이후에는, 상기 제1 보안키를 이용하여 암호화 통신이 이루어진다(S170).

[0041] 본 발명에 따른 스마트 그리드 환경에서는, 상술한 바와 같이, 데이터 수집 장치(30)와 AMI 서버(50) 간에 보안 키가 설정된 후, 스마트 미터(10)와 데이터 수집 장치(30) 및 스마트 미터(10)와 AMI 서버(50) 간의 보안 키가 설정된다. 도 1의 AMI 구조에 있어서, 스마트 미터(10)는 데이터 수집 장치(30)를 통해서 AMI 서버(50)와 연결되는 것으로 되어 있으나, 다양한 스마트 그리드의 응용 범위를 고려할 때, 스마트 미터(10)가 직접 AMI 서버(50)와 통신할 필요도 있을 수 있다. 본 발명은 이를 고려하여 스마트 미터(10)와 AMI 서버(50) 간의 보안 키를 설정할 수 있도록 한다. 스마트 미터(10)와 AMI 서버(50) 간의 직접 통신 시에, 데이터 수집 장치(30)는 해당 데이터에 대한 별도의 처리 없이 그대로 전달하게 된다.

[0042] 도 3을 참조하여, 스마트 미터(10)와 데이터 수집 장치(30)와 AMI 서버(50) 간의 보안 키 설정 절차를 설명하면 다음과 같다.

[0043] 사용자 측에 설치되는 스마트 미터(10)는 데이터 수집 장치(30) 및 AMI 서버(50)와 마찬가지로, 신뢰할 수 있는 인증기관을 통해 발급된 인증서($Cert_A$)를 저장하고 있다.

[0044] 그리고, 상기 스마트 미터(10)는 데이터 수집 장치(30) 및 AMI 서버(50)와 통신하고자 하는 경우, 연결된 데이터 통신 장치(30)로 보안 키 설정 요청(Req.)를 전송한다(S175).

[0045] 이에 데이터 수집 장치(30)는 상기 데이터 수집 장치(30)와 AMI 서버(50)의 공개키 인증을 위한 인증서

($Cert_B, Cert_S$)를 상기 스마트 미터(10)로 전송한다(S180).

[0046] 상기 스마트 미터(10)는 수신된 데이터 수집 장치(30)와 AMI 서버(50)의 인증서에 대한 유효성을 검증하고 (S190), 유효한 경우 세 개의 랜덤값 r_A, k_A^1, k_A^2 (이하, 제5, 제6, 제7 랜덤값이라 함)을 생성한다(S195). 여기서 제5 랜덤값을 키 동의를 위한 랜덤값이고, 제6, 제7 랜덤값은 각각 AMI 서버(50) 및 데이터 수집 장치(30)와의 보안키 유도를 위한 랜덤값이다.

[0047] 상기 스마트 미터(10)는 이러한 제5 내지 제7 랜덤값을 이용하여 데이터 수집 장치(30) 및 AMI 서버(50) 각각에 대하여 키 동의를 위한 암호화된 제3, 제4 메시지 T_3, T_4 를 생성한다(S200). 구체적으로 설명하면, 우선 제5, 제6 랜덤값을 AMI 서버(50)의 공개키로 암호화하여 AMI 서버(50)와의 키 동의를 위한 제3 메시지를 생성한다. 더불어, 상기 스마트 미터(10)는 상기 제3 메시지에 스마트 미터(10)의 식별 정보 ID_A 및 데이터 수집 장치(30)의 식별정보 ID_B 를 더 포함시킬 수 있다. 이는 상기 제3 메시지를 수신하게 될 AMI 서버(50)에서 보안키 설정 대상이 데이터 수집 장치(30)에 연결된 스마트 미터(10)임을 알 수 있도록 한다. 이어서 상기 스마트 미터(10)는 상기 생성한 제3 메시지와 데이터 수집 장치(30)에 전달된 제6 랜덤값을 데이터 수집 장치(30)의 공개키로 암호화하여 제4 메시지를 생성한다. 상기 제4 메시지에는 스마트 미터(10)의 식별 정보 ID_A 가 더 포함될 수 있다.

[0048] 스마트 미터(10)는 상기 생성한 제4 메시지를 데이터 수집 장치(30)로 전송한다(S205). 이때, 스마트 미터(10)는 제4 메시지와 함께 자신의 공개키 인증을 위해 스마트 미터(10)의 인증서 $Cert_A$ 를 더 전송할 수 있다.

[0049] 데이터 수집 장치(30)는 상기 제4 메시지 및 스마트 미터(10)의 인증서가 수신되면, 상기 제4 메시지를 복호화하여 상기 제4 메시지에 포함된 제3 메시지 및 제7 랜덤값을 획득하고, 제1, 제2 랜덤값을 생성한(S210) 후에, 상기 생성한 제1, 제2 랜덤값과 상기 제4 메시지에서 획득한 제3 메시지를 앞서 도 2에서 설정된 제1 보안키로 암호화하여 제5 메시지 T_5 를 생성한다(S215). 상기 단계 S210에서 생성한 제1, 제2 랜덤값은 앞서 도 2의 단계 S130에서 데이터 수집 장치(30)와 AMI 서버(50)와의 보안 키 설정을 위해 생성한 제1, 제2 랜덤값과는 다를 수 있다.

[0050] 그리고 데이터 수집 장치(30)는 상기 생성한 제5 메시지를 AMI 서버(50)로 전송한다(S220). 이때, 상기 수신한 스마트 미터(10)의 인증서를 함께 전송한다.

[0051] 즉, 데이터 수집 장치(30)는 스마트 미터(10)의 인증서에 대한 유효성 검증을 수행하지 않고 단지 AMI 서버(50)로 전달하며, AMI 서버(50)에서 스마트 미터(10)의 인증서에 대한 유효성 검증이 이루어진다.

[0052] 상기 AMI 서버(50)는 데이터 수집 장치(30)로부터 스마트 미터(10)의 인증서와 함께 제5 메시지가 수신되면, 상기 수신된 스마트 미터(10)의 인증서에 대한 유효성을 검증하고(S225), 유효한 경우 제3, 제4 랜덤값(도 2의 단계 S145에서 생성한 제3, 제4 랜덤값과는 다를 수 있음)을 생성하고, 상기 수신한 제5 메시지를 제1 보안키로 복호화하여 제3 메시지, 제1, 제2 랜덤값을 획득하고, 또한 상기 제3 메시지를 다시 자신의 비밀키로 복호화하여 제5, 제6 랜덤값을 획득한 후, 자신이 생성한 제3, 제4 랜덤값과, 상기 획득한 제1, 제2, 제5 랜덤값을 스마트 미터(10)의 공개키로 암호화하여 제6 메시지를 생성한다(S230). 상기 제6 메시지에는 AMI 서버(50)의 식별 정보 ID_S 를 더 포함할 수 있다.

[0053] 그리고, 상기 AMI 서버(50)는 상기 생성한 제6 메시지를 데이터 수집 장치(30)를 통해서 스마트 미터(10)로 전송한다(S235). 이때 데이터 수집 장치(30)는 상기 제6 메시지를 그대로 스마트 미터(10)로 전달한다.

[0054] 상기 제6 메시지를 수신한 스마트 미터(10)는 상기 제6 메시지를 자신의 비밀키로 복호화하여 해당 메시지에 포함된 제1, 제2, 제3, 제4, 제5 랜덤값을 획득하고, 제5 랜덤값이 상기 단계 S195에서 자신이 생성한 제5 랜덤값과 일치하는 지를 확인하여, 일치하는 경우 키 동의를 이루어진 것으로 인식하여, 키 동의 확인을 위해 이 중 제1 랜덤값 및 제3 랜덤값을 데이터 수집 장치(30)로 전송한다(S240).

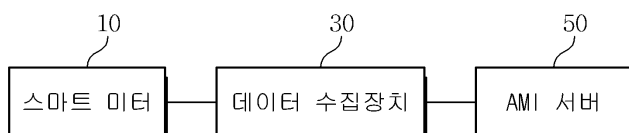
- [0055] 상기 데이터 수집 장치(30)는 수신된 제1, 제3 랜덤값 중에서 제1 랜덤값을 상기 단계 S210에서 생성한 제1 랜덤값과 일치하는 지를 확인하고, 일치하는 경우 키 동의를 이루어진 것으로 인식하여, 나머지 제3 랜덤값은 AMI 서버(50)로 전달한다(S245).
- [0056] 이후, AMI 서버(50)는 데이터 수집 장치(30)를 통해서 수신된 제3 랜덤값을 상기 단계 S230에서 생성한 제3 랜덤값과 일치하는 지를 확인하고, 일치하는 경우 키 동의를 이루어진 것으로 인식하여, 단계 S230에서 자신이 생성한 제4 랜덤값과 상기 제3 메시지에서 획득한 제6 랜덤값으로부터 스마트 미터(10)와의 통신에 사용될 제2 보안을 생성하여 설정한다(S250).
- [0057] 그리고, 데이터 수집 장치(30)는 자신이 생성한 제2 랜덤값과 앞서 수신한 제4 메시지에서 획득한 제7 랜덤값으로부터 스마트 미터(10)와의 암호화 통신에 사용할 제3 보안을 생성하여 설정한다(S255).
- [0058] 이어서, 스마트 미터(10)는 AMI 서버(50)와의 통신을 위한 제2 보안키 및 데이터 수집 장치(30)와의 통신을 위한 제3 보안키를 함께 생성한다(S260). 구체적으로 설명하면, 스마트 미터(10)는 제6 메시지에서 획득한 제4 랜덤값과 단계 S195에서 자신이 생성한 제6 랜덤값으로부터 제2 보안을 생성하고, 제6 메시지에서 획득한 제2 랜덤값과 단계 S195에서 자신이 생성한 제7 랜덤값을 이용하여 제3 보안을 생성하여 설정한다.
- [0059] 이후, 스마트 미터(10)와 데이터 수집 장치(30)는 제3 보안을 이용한 암호화 통신이 이루어지며, 스마트 미터(10)와 AMI 서버(50) 간에는 제2 보안을 이용한 암호화 통신이 이루어진다(S265, S270).
- [0060] 이상과 같이 설명한 본 발명의 보안 키 설정 방법은 다양한 컴퓨터 수단을 통하여 관독 가능한 소프트웨어 형태로 구현되어 컴퓨터로 관독 가능한 기록매체에 기록될 수 있다. 여기서, 기록매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 기록매체에 기록되는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 예컨대 기록매체는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(Magnetic Media), CD-ROM(Compact Disk Read Only Memory), DVD(Digital Video Disk)와 같은 광 기록 매체(Optical Media), 플롭티컬 디스크(Floptical Disk)와 같은 자기-광 매체(Magneto-Optical Media), 및 롬(ROM), 램(RAM, Random Access Memory), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치를 포함한다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함할 수 있다. 이러한 하드웨어 장치는 본 발명의 동작을 수행하기 위해 하나 이상의 소프트웨어로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.
- [0061] 더불어, 본 명세서와 도면에는 본 발명의 바람직한 실시 예에 대하여 개시하였으나, 여기에 개시된 실시 예외에도 본 발명의 기술적 사상에 바탕을 둔 다른 변형 예들이 실시 가능하다는 것은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에게 자명한 것이다. 또한, 본 명세서와 도면에서 특정 용어들이 사용되었으나, 이는 단지 본 발명의 기술 내용을 쉽게 설명하고 발명의 이해를 돕기 위한 일반적인 의미에서 사용된 것이지, 본 발명의 범위를 한정하고자 하는 것은 아니다.

부호의 설명

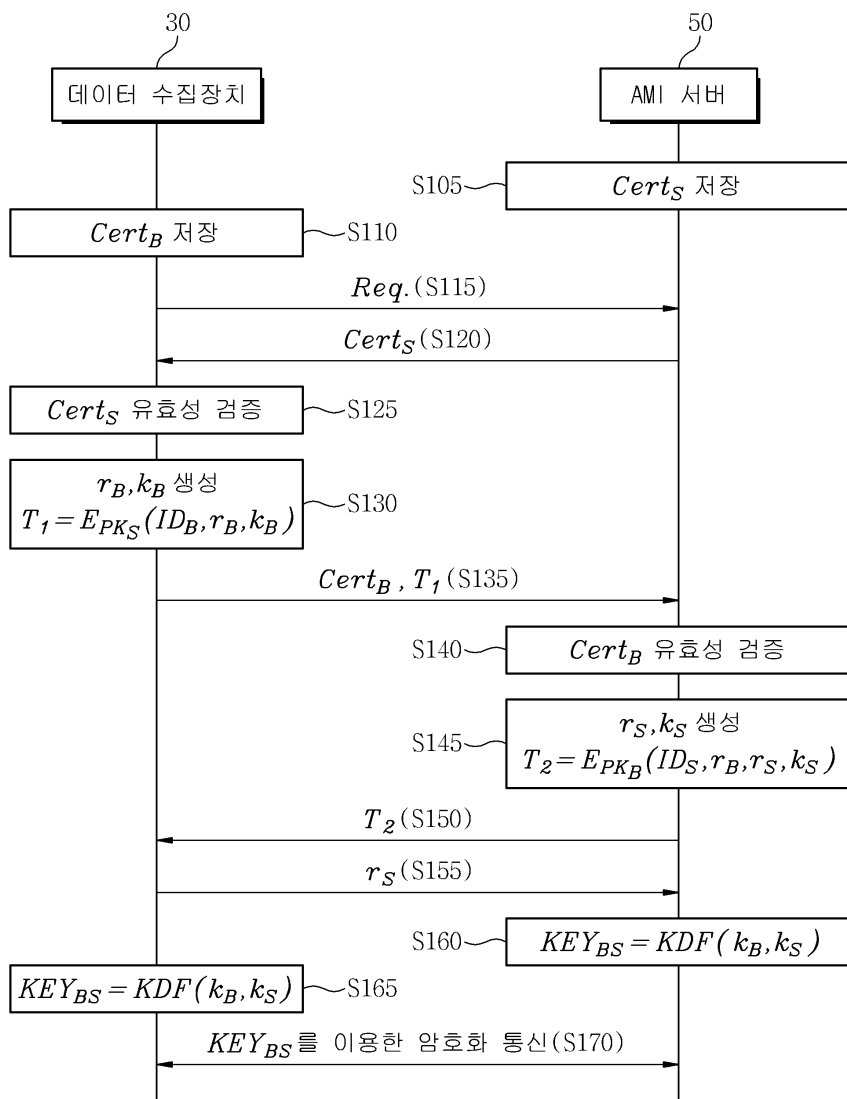
- [0062] 10: 스마트 미터(Smart Meter)
30: 데이터 수집 장치(DCU: Data Collection Unit)
50: AMI(Advanced Metering Infrastructure) 서버

도면

도면1



도면2



도면3

