(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2013년03월13일
(11) 등록번호 10-1243943
(24) 등록일자 2013년03월07일

(51) 국제특허분류(Int. Cl.)
H02J 13/00 (2006.01) *H02J 3/38* (2006.01)
G06Q 50/06 (2012.01)
(21) 출원번호 10-2011-0087167
(22) 출원일자 2011년08월30일
심사청구일자 2011년08월30일
(65) 공개번호 10-2013-0024014
(43) 공개일자 2013년03월08일
(56) 선행기술조사문헌
KR1020110013788 A*
KR1020110021636 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
고려대학교 산학협력단

(72) 발명자
이희조
서동원

(74) 대리인
특허법인엠에이피에스

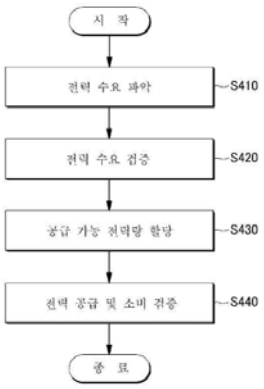
전체 청구항 수 : 총 11 항 심사관 : 추형석

(54) 발명의 명칭 **스마트 그리드를 위한 전력 관리 시스템 및 방법**

(57) 요 약

본 발명은 스마트 그리드를 통한 전력 관리 방법에 대한 것으로, (a) 루트 노드가 수요 파악용 공개키 및 수요 파악용 비밀키 쌍을 생성하고, 상기 수요 파악용 공개키가 상위 노드에서 하위 노드로 순차적으로 전송되어 스마트 그리드의 각 노드들에서 공유되는 단계; (b) 리프 노드의 전력 수요량이 상기 수요 파악용 공개키로 암호화되어 상기 루트 노드로 전송되는 단계;및 (c) 상기 루트 노드가 상기 (b) 단계에서 수신한 데이터를 상기 수요 파악용 비밀키로 복호화하여 전력 총수요를 산출하는 단계를 포함하되, 상기 (b) 단계는 상기 수요 파악용 공개키로 암호화된 전력 수요들이 하위 노드에서 상위 노드로 순차적으로 모아지며 보고되는 단계를 포함하는 스마트 그리드 전력 관리 방법을 제공한다.

대 표 도 - 도4



이 발명을 지원한 국가연구개발사업

과제고유번호	ITAB1100110100020001000200200
부처명	한국소프트웨어진흥원
연구사업명	SW공학 요소기술 개발과 전문인력 양성사업
연구과제명	융합소프트웨어 신뢰성 기술개발 연구
주관기관	고려대학교 산학협력단
연구기간	2011.01.01 ~ 2011.12.31

특허청구의 범위

청구항 1

스마트 그리드를 통한 전력 관리 방법에 있어서,

(a) 루트 노드가 수요 파악용 공개키 및 수요 파악용 비밀키 쌍을 생성하고, 상기 수요 파악용 공개키가 상위 노드에서 하위 노드로 순차적으로 전송되어 스마트 그리드의 각 노드들에서 공유되는 단계;

(b) 리프 노드의 전력 수요량이 상기 수요 파악용 공개키로 암호화되어 상기 루트 노드로 전송되는 단계;및

(c) 상기 루트 노드가 상기 (b) 단계에서 수신한 데이터를 상기 수요 파악용 비밀키로 복호화하여 전력 총수요를 산출하는 단계를 포함하되,

상기 (b) 단계는,

상기 수요 파악용 공개키로 암호화된 전력 수요들이 하위 노드에서 상위 노드로 순차적으로 모아지며 보고되는 단계를 포함하며,

상기 (a) 단계는

각 부모-자식 노드 쌍이 고유한 대칭 암호키를 서로 교환하는 단계를 더 포함하며,

상기 암호 키는 상기 부모-자식 노드 간 통신에 사용되는 스마트 그리드 전력 관리 방법.

청구항 2

삭제

청구항 3

제 1 항에 있어서,

상기 (a) 단계는,

상기 루트 노드가 서명용 공개키 및 서명용 비밀키 쌍을 생성하고, 상기 서명용 공개키가 상위 노드에서 하위 노드로 순차적으로 전송되어 스마트 그리드의 각 노드들에서 공유되는 단계를 더 포함하며,

상기 서명용 공개키 및 서명용 비밀키 쌍은 루트 노드가 보낸 메시지의 발신자가 루트 노드 자신임을 보증하기 위한 것인 스마트 그리드 전력 관리 방법.

청구항 4

제 3 항에 있어서,

(d) 상기 루트 노드가 검증용 총수요를 생성하여, 자식 노드의 형제 노드들의 전력 수요 총합을 덧붙여 검증 메시지로서 자식 노드로 전송하는 단계; 및

(e) 상기 자식 노드를 시작으로 상위 수준에서 하위 수준으로 내려가면서,

검증 메시지를 수신한 노드가 상기 검증 메시지에 기초하여 자신의 전력 수요를 검증하고, 자신의 자식 노드에게 상기 수신한 검증 메시지에 상기 자식 노드의 형제 노드들의 전력 수요 총합을 덧붙인 것을 검증 메시지로서 전송하는 과정을 순차적으로 진행하는 단계;를 더 포함하되,

상기 (e) 단계는

상기 검증 메시지를 수신한 노드가 자신의 전력 수요와 수신한 형제 노드들의 전력 수요 총합들을 모두 합한 것이 수신한 검증용 총수요와 일치하는지 여부로 자신의 전력 수요를 검증하는 단계를 포함하는 것인 스마트 그리드 전력 관리 방법.

청구항 5

제 4 항에 있어서,

상기 검증용 총수요는 상기 (d) 단계에서 전력 총수요를 상기 수요 파악용 공개키로 암호화하고 상기 서명용 비밀키로 서명하여 생성된 후,

상기 (e) 단계에서 검증에 사용되기 전에 상기 서명용 공개키로 복호화되는 것인 스마트 그리드 전력 관리 방법.

청구항 6

제 4 항에 있어서,

(f) 상기 루트 노드가 생산할 수 있는 전력 총공급을 상기 전력 총수요와 비교하는 단계; 및

(g) 각 노드에 대한 전력 공급 할당량을 전력 공급 축소 비율로 축소하여 전력을 공급하는 축소 모드로 운영되는 단계를 더 포함하되,

상기 전력 공급 축소 비율은 상기 전력 총수요를 상기 전력 총공급으로 나눈 값인 스마트 그리드 전력 관리 방법.

청구항 7

제 6 항에 있어서,

상기 축소 모드로 운영되는 단계는

(h) 상기 루트 노드부터 시작하여 하위 수준으로 내려가면서, 리프 노드를 제외한 각 노드가 자식 노드에게 상기 전력 공급 축소 비율을 전송하는 단계; 및

(i) 상기 자식 노드가 자신의 전력 수요와 상기 전력 공급 축소 비율을 곱하여 자신에게 할당된 전력 공급량을 계산하는 단계를 포함하되,

상기 전력 공급 축소 비율은 상기 루트 노드에서 상기 서명용 비밀키로 서명되고, 각 노드들은 상기 서명용 공개키를 사용하여 이를 확인하는 스마트 그리드 전력 관리 방법.

청구항 8

제 7 항에 있어서,

상기 (h) 단계는 상기 부모 노드가 수요 파악용 비밀키를 서명용 비밀키로 서명한 것과 상기 자식 노드의 전력 수요를 전송하는 단계를 더 포함하고,

상기 (i) 단계는 상기 자식 노드가 자신의 전력 수요가 수요 파악용 공개키로 암호화된 값과 상기 수신된 자신의 전력 수요를 비교하여 검증하는 단계를 더 포함하되;

상기 수요 파악용 비밀키를 서명용 비밀키로 서명한 것은 상기 리프 노드의 조부모 노드까지만 전달되는 것을 특징으로 하는 스마트 그리드 전력 관리 방법.

청구항 9

제 6 항에 있어서,

상기 축소 모드로 운영되는 단계는

(j) 상기 리프 노드의 부모 노드가 상기 리프 노드에게 전력 공급 조각 크기를 전송하는 단계;

(k) 상기 리프 노드가 상기 수신한 전력 공급 조각 크기에 기초하여, 상기 부모 노드에게 전력 공급 만료 조건 및 검증 코드를 전송하는 단계;

(l) 상기 전력 공급 만료 조건에 기초하여, 전력 공급 조각이 소진될 때까지, 상기 리프 노드가 상기 부모 노드에게 전력 공급을 요청하는 단계; 및

(m) 상기 부모 노드가 상기 검증 코드에 기초하여 상기 리프 노드의 요청을 검증하고, 상기 리프 노드에게 상기 전력 공급 조각 크기 만큼의 전력을 공급하는 단계;를 더 포함하는 스마트 그리드 전력 관리 방법.

청구항 10

스마트 그리드를 통한 전력 관리 시스템에 있어서,

수요 파악용 공개키 및 수요 파악용 비밀키 쌍을 생성하여 상기 스마트 그리드의 각 노드들에 배포하는 루트 노드;

자신의 전력 수요량을 상기 수요 파악용 공개키로 암호화하여 자신의 부모 노드로 전송하는 리프 노드; 및

상기 수요 파악용 공개키로 암호화된 전력 수요들을 모아 자신의 부모 노드로 전송하는 중간 노드;를 포함하되,

상기 루트 노드는

수신한 데이터를 상기 수요 파악용 비밀키로 복호화하여 전력 총수요를 산출하되,

상기 스마트 그리드의 각 노드는

각 부모-자식 노드 쌍이 고유한 대칭 암호키를 서로 교환하고, 상기 암호 키를 상기 부모-자식 노드 간 통신에 사용하는 것인 스마트 그리드 전력 관리 시스템.

청구항 11

제 10 항에 있어서,

상기 루트 노드는 검증용 총수요를 생성하여, 자식 노드의 형제 노드들의 전력 수요 총합을 덧붙여 검증 메시지로서 자식 노드로 전송하고,

상기 중간 노드는 상기 검증 메시지에 기초하여 자신의 전력 수요와 수신한 형제 노드들의 전력 수요 총합들을 모두 합한 것이 수신한 검증용 총수요와 일치하는지 여부로 자신의 전력 수요를 검증하고, 자신의 자식 노드에게 상기 수신한 검증 메시지에 상기 자식 노드의 형제 노드들의 전력 수요 총합을 덧붙인 것을 검증 메시지로서 전송하는 스마트 그리드 전력 관리 시스템.

청구항 12

제 10 항에 있어서,

상기 루트 노드는 생산할 수 있는 전력 총공급을 상기 전력 총수요와 비교하여, 각 노드에 대한 전력 공급 할당량을 전력 공급 축소 비율로 축소하여 전력을 공급하는 축소 모드로 운영할 것인지 판단하고, 상기 전력 공급 축소 비율을 자식 노드로 전송하되,

상기 전력 공급 축소 비율은 상기 전력 총수요를 상기 전력 총공급으로 나눈 값인 스마트 그리드 전력 관리 시스템.

명 세 서

기 술 분 야

[0001] 본 발명은 스마트 그리드 전력 관리 시스템 및 방법에 관한 것이다.

배 경 기 술

[0002] 최근 기존 전력망에 정보 기술을 접목하여 전력 공급자 측과 사용자 측이 양방향으로 실시간 정보를 교환하는 지능형 전력망인 스마트 그리드에 대한 관심이 높아지고 있다. 사용자의 시간대별 전력 사용량이 실시간으로 측정되어 전력 공급자 측에 전송되기 때문에, 양측 모두에서 에너지 효율을 최적화하고 비용을 절감할 수 있다. 전력 공급자 측은 이렇게 실시간으로 파악한 전력 사용 현황을 바탕으로 전력 공급량을 탄력적으로 조절할 수 있으며, 사용자 또한 요금이 비싼 시간대를 피하여 사용 시간과 사용량을 조절할 수 있는 것이다. 또한 풍량과 일조량 등에 따라 전력 생산이 불규칙하다는 한계 때문에 활용도가 낮았던 풍력 발전, 태양광 발전 등 신재생 에너지의 활용도도 높아진다. 에너지 위기 및 지구 온난화 문제가 점점 심각해지는 현 상황에서 스마트 그리드는 이렇게 다양한 경제적, 환경적 장점들을 갖고 있기 때문에 세계적으로 차세대 전력망으로 각광받고 있다.

[0003] 특히 파악한 사용자의 전력 소비 패턴을 활용하여 전력을 좀더 효율적이고 안정적으로 관리할 수 있다는 장점을

최대화하기 위한 연구가 최근 많이 이루어지고 있다. 예를 들어, 여름철과 같이 에너지 소비량이 증가할 때는 전력 소비가 전력 공급을 넘어서서 정전 사태가 벌어질 위험이 있는데, 이는 막대한 사회적, 경제적 피해로 이어지게 된다. 그렇다고 한시적인 전력 소비 증가에 대비하기 위해 전력 생산 시설을 늘리는 것은 경제적, 환경적인 측면에서 바람직하지 않다. 즉, 각 사용자의 전력 소비를 전체 전력 소비량에 따라 조절하는 것이 효율적이고 안정적인 전력 관리 방법이다. 각 사용자가 전력 소비를 조금씩만 줄여도 전체 시스템의 부하는 훨씬 줄어들게 된다.

[0004] 그러나 여름철과 같이 전력 수요가 많을 수 밖에 없는 때에 사용자 각각에게 에너지 소비를 줄여달라고 설득하기는 쉽지 않은 일이다. 따라서 시스템이 자동으로 사용자의 전력 소비를 제어하는 것이 해결책이 될 수 있다. 스마트 그리드는 전력 공급자 측과 사용자 측이 양방향으로 실시간 정보를 교환하므로 이러한 해결책을 구현하기에 적합하다.

[0005] 이와 관련하여 한국등록특허 제10-1002396호(“스마트 미터 제어기 및 이를 구비한 지능형 전자식 세대 분전반 시스템”)에는 전기제품의 대기전력 상태를 실시간으로 판단하여 불필요한 대기전력을 자동으로 차단하고, 원격에서 자동 또는 수동으로 대기 전원을 복귀시킬 수 있는 스마트 미터 제어기 및 이를 구비한 지능형 전자식 세대 분전반 시스템의 구성이 개시되어 있다.

[0006] 한편, 한국공개특허 제10-2011-0070654호(“전력 소비를 제어하는 스마트 에너지 관리 장치 및 그 방법”)는 게이트웨이를 통해 연결된 하나 이상의 전기 기기 사용 그룹으로부터 전력 소비 정보를 수집하여 임계치 이상으로 전력 소비가 발생할 것으로 예상되면, 게이트웨이를 통해 연결된 부하 제어기로 제어명령을 출력하여 전기 기기 사용 그룹에 속한 전기기기들의 전력 사용을 제어하는 구성을 개시하고 있다.

[0007] 이들 선행 기술들은 대기 전력을 차단하거나 전기 기기의 동작을 정지시켜 전력 소비를 제한하는 것을 특징으로 한다. 예로 든 선행 기술들 뿐 아니라, 기존 전력 관리 방식은 악의적인 공격이나 불법 사용자를 막기 위해서도 전력을 차단하여 대응하는 경우가 많다. 하지만 부분적으로라도 전력을 아예 차단해버리는 이러한 해결법은 덜 안정적이다. 특히 악의적인 사용자의 전력 시스템 공격에 취약하다. 기존의 정보 네트워크에서 행해지는 서비스 거부 공격과 유사한 공격이 스마트 그리드에 대해 행해질 경우, 예를 들어 고의로 과도한 전력 수요를 전력 공급자 측에 보내는 경우, 많은 적법한 사용자가 전력 공급이 끊기는 피해를 입을 가능성이 높다.

[0008] 게다가 스마트 그리드는 기존 전력망보다 이러한 공격을 당할 잠재적인 위험이 크다. 스마트 그리드의 정보 네트워크를 통해 결재 정보 등 민감한 사용자 정보를 해킹해 경제적인 이득을 보려는 불법 사용자가 침투할 위험 또한 크다. 따라서 사용자 정보를 보호하고 전력 공급 시스템을 공격으로부터 보호하는 것 또한 스마트 그리드를 통해 전력을 안정적이고 효율적으로 공급하기 위해 필요하다.

발명의 내용

해결하려는 과제

[0009] 본 발명은 전술한 문제를 해결하기 위한 것으로서, 그 목적은 안정적이고 효율적인 스마트 그리드 전력 관리 시스템 및 방법을 제공하는 것이다.

과제의 해결 수단

[0010] 상기와 같은 목적을 달성하기 위한 본 발명의 제 1 측면에 따른 스마트 그리드 전력 관리 방법은 (a) 루트 노드가 수요 파악용 공개키 및 수요 파악용 비밀키 쌍을 생성하고, 상기 수요 파악용 공개키가 상위 노드에서 하위 노드로 순차적으로 전송되어 스마트 그리드의 각 노드들에서 공유되는 단계; (b) 리프 노드의 전력 수요량이 상기 수요 파악용 공개키로 암호화되어 상기 루트 노드로 전송되는 단계;및 (c) 상기 루트 노드가 상기 (b) 단계에서 수신한 데이터를 상기 수요 파악용 비밀키로 복호화하여 전력 총수요를 산출하는 단계를 포함하되, 상기 (b) 단계는, 상기 수요 파악용 공개키로 암호화된 전력 수요들이 하위 노드에서 상위 노드로 순차적으로 모아지며 보고되는 단계를 포함하는 포함하는 것을 특징으로 한다.

[0011] 상기와 같은 목적을 달성하기 위한 본 발명의 제 2 측면에 따른 스마트 그리드 전력 관리 시스템은 수요 파악용 공개키 및 수요 파악용 비밀키 쌍을 생성하여 상기 스마트 그리드의 각 노드들에 배포하는 루트 노드; 자신의 전력 수요량을 상기 수요 파악용 공개키로 암호화하여 자신의 부모 노드로 전송하는 리프 노드; 및 상기 수요 파악용 공개키로 암호화된 전력 수요들을 모아 자신의 부모 노드로 전송하는 중간 노드;를 포함하되, 상기 루트 노드는 수신한 데이터를 상기 수요 파악용 비밀키로 복호화하여 전력 총수요를 산출하는 것을 특징으로 한다.

발명의 효과

[0012] 이상에서 설명한 바와 같이, 본 발명에 따르면 다음과 같은 효과들을 얻을 수 있다.

[0013] 본 발명에 따르면 전력 소비자들에게 전력을 안정적으로 공급할 수 있다.

[0014] 또한, 본 발명에 따르면 발전소, 변전소, 송전소, 분전소, 전력 분배기, 스마트 미터 등 전력 공급 시스템의 많은 구성 요소들을 효율적으로 다루어, 전력 수요 파악 및 전력 공급의 효율성을 높일 수 있다.

[0015] 또한, 본 발명에 따르면 전력 소비량 등 소비자의 개인 정보가 누출되는 것을 방지할 수 있다.

[0016] 또한, 본 발명에 따르면 전력 공급 시스템을 마비시킬 위험이 있는 공격을 감지해내어 시스템을 보호할 수 있다.

도면의 간단한 설명

[0017] 도1은 본 발명에 따른 스마트 그리드 시스템의 구조를 도시하고 있는 구조도이다.

도2는 본 발명에 따른 스마트 그리드 시스템의 동작을 나타낸 흐름도이다.

도3은 본 발명에 따른 스마트 그리드 시스템의 준비 단계에서의 노드간 자료 흐름을 도시하고 있는 구조도이다.

도4는 본 발명에 따른 스마트 그리드 시스템의 축소 모드에서의 동작을 나타낸 흐름도이다.

도5는 본 발명에 따른 스마트 그리드 시스템의 전력 수요 파악 단계에서의 노드간 자료 흐름을 도시하고 있는 구조도이다.

도6은 본 발명에 따른 스마트 그리드 시스템의 전력 수요 파악 단계에서의 동작을 나타낸 흐름도이다.

도7는 본 발명에 따른 스마트 그리드 시스템의 전력 수요 검증 단계에서의 노드간 자료 흐름을 도시하고 있는 구조도이다.

도8은 본 발명에 따른 스마트 그리드 시스템의 전력 수요 검증 단계에서의 동작을 나타낸 흐름도이다.

도9는 본 발명에 따른 스마트 그리드 시스템의 공급 가능 전력량 할당 단계에서의 노드간 자료 흐름을 도시하고 있는 구조도이다.

도10은 본 발명에 따른 스마트 그리드 시스템의 공급 가능 전력량 할당 단계에서의 동작을 나타낸 흐름도이다.

도11은 본 발명에 따른 스마트 그리드 시스템의 전력 공급 및 소비 검증 단계에서의 동작을 나타낸 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0018] 아래에서는 첨부한 도면을 참조하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 본 발명의 실시예를 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

[0019] 명세서 전체에서, 어떤 부분이 다른 부분과 "연결"되어 있다고 할 때, 이는 "직접적으로 연결"되어 있는 경우뿐 아니라, 그 중간에 다른 소자를 사이에 두고 "전기적으로 연결"되어 있는 경우도 포함한다. 또한 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다.

[0020] 도1은 본 발명에 따른 스마트 그리드 시스템의 구조를 도시하고 있는 구조도이다.

[0021] 전력 공급자가 전기를 생산하여 소비자에게 공급하기까지는 발전소, 송전소, 변전소, 분전소, 전력 분배기 등 여러 시설들을 거치게 된다. 본 발명은 이들을 트리 구조로 연결한 것이 특징이다. 본 발명에 따른 스마트 그리드 트리(100)의 루트 노드(110)는 전력 생산자인 발전소일 수 있고, 중간 노드(120)들은 송전소, 변전소, 분전소, 전력 분배기 등 전력 분배자일 수 있으며, 리프 노드(130)들은 사용자, 즉 전력 소비자일 수 있다.

[0022] 실제 물리적인 전력망은 각 구성 요소가 그물망 형태로 연결되어 있을 수 있다. 본 발명은 이를 각 발전소를 루트로 하여 논리적으로 분해해서 여러 개의 트리 구조(100)로 단순화시킴으로써, 시스템의 많은 구성 요소들을 효율적으로 관리하는 효과를 얻는다. 예를 들면, 그물망 구조에서와는 달리 트리 구조에서는 각 노드의 통신 방

향이 부모-자식간으로 한정된다는 장점이 있다. 이러한 단순화된 구조는 본 발명에 따른 스마트 그리드가 전력 수요를 파악하고 전력을 공급하는 일을 효율적으로 해낼 수 있는 기초가 된다.

[0023] 본 발명은 트리의 중간 노드(120)들이나 리프 노드(130)들은 악의적인 사용자나 불법 사용자의 공격을 받아 비정상적인 행위를 할 수 있지만, 루트 노드(110)는 안전하다고 가정한다.

[0024] 또한 각 노드들간의 통신이 안전하고 원활하게 이루어지게 하기 위해, 본 발명은 대칭 암호와 비대칭 암호를 모두 사용한다. 먼저, 각 부모-자식 간의 통신에는 해당 부모-자식 간에만 공유되는 고유한 대칭 암호 키가 사용된다. 예를 들어, 도1에서 N1과 N2 사이의 통신에 사용되는 암호 키는 N2와 N4 사이에 사용되는 암호 키와 다를 수 있다. 이후 설명에서 각 노드들의 통신은 각 고유 키를 사용한 암호화, 복호화 과정을 거친다고 가정하며, 이에 대한 기술을 생략한다.

[0025] 비대칭 암호에는 루트 노드(110)가 생성하는 두 가지 (공개키, 비밀키) 쌍이 사용된다. 하나는 (수요 파악용 공개키, 수요 파악용 비밀키) 쌍이고, 다른 하나는 (서명용 공개키, 서명용 비밀키) 쌍이다. 이에 대한 자세한 설명은 후술하며, 기술을 간략하게 하기 위해 이후 수요 파악용 공개키 및 비밀키는 각각 Pv 및 Sv, 서명용 공개키 및 비밀키는 각각 Ps 및 Ss로 기술하겠다.

[0026] 도2는 본 발명에 따른 스마트 그리드 시스템의 동작을 나타낸 흐름도이다.

[0027] 준비 단계(S210)에서 노드들은 상술한 암호 키들을 교환하는데, 구현에 따라 준비 단계(S210)는 후술할 축소 모드 작동 단계(S240)에 포함되는 것도 가능하다.

[0028] 스마트 그리드는 평소에는 전력 소비자들의 전력 수요를 모두 충족시킬 만큼 전력을 공급하는 정상 모드(S220)에서 작동한다.

[0029] 이때 루트 노드(110)는 전력 총수요가 전력 공급 가용량을 넘어서는지 판단하여(S230), 계속하여 정상 모드로 작동할 것인지, 일정 시간 동안 축소 모드로 작동할 것인지(S240) 결정한다.

[0030] 도3은 본 발명에 따른 스마트 그리드 시스템의 준비 단계(S210)에서의 노드간 자료 흐름을 도시하고 있는 구조도이다.

[0031] 각 부모-자식 간에는 해당 부모-자식 간에만 공유되는 고유한 대칭 암호 키가 교환되며(S310), 루트 노드(110)는 전술한 두가지 비대칭형 암호키 쌍을 생성한 후, 수요 파악용 공개키 Pv와 서명용 공개키 Ps를 자식 노드들에 배포하고, 이들 비대칭 암호에 사용될 공개키들은 트리 구조를 타고 내려가며 전달돼, 결국 모든 노드가 Pv와 Ps를 보유하게 된다(S320).

[0032] 도4는 본 발명에 따른 스마트 그리드 시스템의 축소 모드(S240)에서의 동작을 나타낸 흐름도이다.

[0033] 축소 모드(S240)는 전력 수요 파악 단계(S410), 전력 수요 검증 단계(S420), 공급 가능 전력량 할당 단계(S430), 전력 공급 및 소비 검증 단계(S440)로 구성된다.

[0034] 도5와 도6는 도4의 전력 수요 파악 단계(S410)에서의 노드간 자료 흐름과 동작을 각각 도시하고 있다.

[0035] 리프 노드(130)는 자신의 전력 수요를 Pv로 암호화하여(S610), 이 자기수요를 부모 노드로 전송한다(S620). 예를 들어, 도5에서 N4가 N2로 전송하는 것은 Pv{V4}가 된다. 여기에서 V4는 리프 노드 N4의 전력 수요이며, Pv{}는 Pv로 암호화했다는 뜻이며, 이후 설명에서는 이에 대한 기술을 생략하겠다.

[0036] 다음으로, 자식 노드로부터 전력 수요를 수신한 부모 노드는 이번에는 자식 노드의 입장이 되어 부모 노드에게 자신의 전력 수요를 전송하는데(S630), 이는 자기 자식들의 전력 수요를 모두 모은 값이 된다. 예를 들어, N2가 N1로 전송하는 것은 Pv{V4+V5}가 된다. 즉, N2 자신의 전력 수요인 Pv{V2}는 N2의 자식 노드들인 N4와 N5의 전력 수요를 합한 Pv{V4+V5}가 되는 것이다. 따라서 전체 시스템에 대한 전력 총수요, 즉 루트 노드(110) N1의 전력 수요 Pv{V1}는 결국 리프 노드(130)들의 전력 수요들의 합인 Pv{V4+V5+V6+V7}이 된다.

[0037] 다음으로, 루트 노드(110)는 Pv로 암호화된 상태로 모인 자식들의 전력 수요를 Sv로 해독하여 총수요를 산출한다(S640). 주목할 것은 Sv를 가지고 있는 것은 루트 노드(110) 밖에 없기 때문에, 본 발명에 따른 전력 수요 파악 단계에서 리프 노드(130)의 전력 수요는 중간 노드(120)들에게 노출되지 않는다는 것이다. 부모-자식간 통신에 각 부모-자식간에 고유한 대칭 암호 키를 사용하면서도, 이렇게 중요한 데이터를 주고 받을 때는 비대칭 암호를 또한번 사용함으로써, 중간 노드(120)가 오염되더라도 사용자의 전력 소비량과 같은 민감한 정보가 누출되지 않도록 보안을 한층 더 강화한 것이 본 발명의 특징이다.

[0038] 앞서 기술한 바와 같이 시스템이 불법 사용자나 악의적인 사용자로부터 공격을 받을 경우 적법한 사용자에게 전력 공급이 안정적으로 이루어지지 못할 위험이 있기 때문에, 중요한 정보가 누출되는 것을 막고 공격을 감지해 내는 것은 시스템의 안정성을 위해서도 중요하다. 이에 따라 본 발명은 스마트 그리드의 보안 및 개인 정보 보호 수준을 향상시키려는 목표를 갖고 있다. 본 발명은 특히 전력 수요를 오염시켜 허위로 요청하거나 과잉 전력 수요를 요청하는 공격을 막는 것에 초점을 맞추고 있다. 공격자는 사용자 정보를 빼내어 이러한 공격을 위한 기반으로 삼는 경우가 많기 때문에, 본 발명에 따른 스마트 그리드는 이렇게 대칭 암호와 비대칭 암호를 이중으로 사용하여 이를 막고 있다.

[0039] 주목해야 할 또하나의 장점은 본 발명에 따른 스마트 그리드에서는 이렇게 트리 구조의 하위 수준에서 상위 수준으로 전력 수요가 자연스럽게 모아지며 올라가기 때문에, 전체 전력 수요를 효율적으로 파악할 수 있다는 것이다. 본 발명은 트리 구조를 사용함으로써 메시 구조를 사용하는 것보다 데이터의 전송 방향 및 합산 방법을 단순화하는 효과를 얻고 있다. 즉, 본 발명은 보안 및 개인 정보 보호 이외에도 스마트 그리드 전력 공급 시스템 및 방법의 효율성까지 추구하고 있다.

[0040] 본 발명이 전력 수요를 효율적으로 모을 수 있는 이유는 예를 들어, Pv{V4}와 Pv{V5}를 Pv{V4+V5}로 모으는 데 많은 노력이 들지 않기 때문이다. 본 발명은 공개키 암호화에 Paillier 암호화 방식을 사용하는데, 이는 가산적 준동형 암호화(additive homomorphic encryption) 방식이다. 즉, 공개키와 메시지 m1, m2를 암호화한 값만 있으면, m1+m2를 암호화한 값을 계산해낼 수 있다. 따라서 본 발명은 Pv{V4}와 Pv{V5}를 쉽게 Pv{V4+V5}로 모을 수 있다.

[0041] 도7과 도8은 도4의 전력 수요 검증 단계(S420)에서의 노드간 자료 흐름과 동작을 각각 도시하고 있다.

[0042] 본 발명에서 각 노드가 자신의 전력 수요가 제대로 보고되었는지 검증하는 방법은 자신의 전력 수요와 자신의 형제 노드들의 전력 수요의 합이 총수요와 같은지 확인하는 것이다. 예를 들어, 도7에서 N2의 입장에서 자신의 전력 수요 V2가 제대로 보고되었는지 검증하기 위해서는 V2와 V3를 합한 값이 V1과 같은지 보면 된다. N4 입장에서는 V4+V5가 V2와 같은지 확인하면 되므로, 결국 V4+V5+V3=V1인지 여부를 보면 된다. 따라서 V1, 즉 총수요가 각 노드들에 전송될 필요가 있다.

[0043] 도8은 이러한 과정을 일반화해서 보여주고 있다. 설명의 편의를 위해 형제수요 Ai를 노드 Ni의 형제 노드들의 전력 수요 총합, 자기수요를 노드 Ni 자신의 전력 수요라고 하자. 예를 들어, 도7에서 N2의 형제 수요는 N2의 형제 노드인 N3의 전력 수요 V3가 될 것이며, N4의 형제수요는 N4의 형제 노드인 N5의 전력 수요 V5가 될 것이다. 또한 N2의 자기수요는 V2, N4의 자기수요는 V4가 될 것이다.

[0044] 노드 Ni-1은 자신의 자식 노드인 노드 Ni로 검증용 총수요와 함께 형제수요 Ai를 전송한다(S810).

[0045] 다음으로, 노드 Ni는 수신한 검증용 총수요와 형제수요 Ai를 기초로 자신의 전력 수요가 제대로 보고되었는지 검증한다(S820). 즉, 자기수요와 수신한 형제수요 Ai의 합이 수신한 검증용 총수요와 일치하는지 확인한다.

[0046] 다음으로, 노드 Ni는 자신의 자식 노드인 노드 Ni+1로 자신이 수신한 검증용 총수요, 형제수요 Ai와 함께 형제수요 Ai+1을 전송한다(S830).

[0047] 이런 식으로, 전력 수요 검증은 루트 노드(110)부터 시작하여 상위 수준에서 하위 수준으로 내려가면서 단계적으로 이루어지게 된다. 최종적으로 리프 노드(130) N4가 자신의 전력 수요가 성공적으로 보고되었는지 여부를 루트 노드(110) N1으로 보고하면 된다.

[0048] 단, 보안과 개인 정보 보호를 위해 위 전력 수요들은 암호화되고 복호화되는 과정을 거쳐야 한다. 루트 노드(110)는 전력 총수요 V1을 수요 파악용 공개키 Pv로 암호화한 후 서명용 비밀키 Ss로 서명하여 검증용 총수요를 생성한다. 이때 이 과정은 해싱 과정을 포함할 수 있다. 따라서 생성된 검증용 총수요는 Ss{H(Pv{V1})}로 나타낼 수 있는데, 여기서 H()는 해싱했다는 의미이다. 이후 설명에서는 이에 대한 기술을 생략한다. 여기에서 서명용 비밀키 Ss로 서명하는 이유는 검증용 총수요를 보낸 발신자가 루트 노드(110)임을 보증하기 위해서이다. 준비 단계(S210)에서 각 노드에게 루트 노드(110)가 생성한 서명용 공개키 Ps가 전송된 이유가 이것이다.

[0049] 따라서 검증용 총수요 Ss{H(Pv{V1})}를 수신한 노드는 상기 서명용 공개키 Ps로 Ss{H(Pv{V1})}를 복호화하여 H(Pv{V1})를 얻은 후에 검증 작업을 수행해야 한다. 예를 들어, N2는 H(Pv{V1})를 산출한 후, 자기수요 Pv{V2}와 형제수요 Pv{V3}를 합하여 얻은 H(Pv{V2}+Pv{V3})와 비교해서, 두 값이 일치하는지 여부로 자기수요가 제대로 보고되었는지 검증한다. N4에서는 H(Pv{V1})와 H(Pv{V4}+Pv{V3}+Pv{V5})를 비교하게 될 것이다.

[0050] 도9와 도10은 도4의 공급 가능 전력량 할당 단계(S430)에서의 노드간 자료 흐름과 동작을 각각 도시하고 있다.

[0051] 전력 총수요 파악 및 검증을 마치고 나면, 루트 노드(110)는 자신이 공급할 수 있는 전력 공급 가능량을 파악된 총수요로 나누어, 공급 축소 비율 S를 산출한다. 이 공급 축소 비율에 따라 각 노드의 전력 수요를 축소하면, 모든 전력 소비자에게 공급되는 전력을 공평하게 축소할 수 있을 것이다. 따라서 S는 트리 구조를 타고 내려가며 전달되고, 각 노드는 수신한 S와 자신의 전력 수요를 곱하여 자신에게 할당된 전력 공급량을 계산한다. 예를 들어, 총수요가 1,000kw/h이지만, 루트 노드(110)가 생산할 수 있는 공급 가능량은 500kw/h라면, S는 0.5가 될 것이다. 만약 도9의 N2가 요청한 전력 수요가 100kw/h였다면, N2에게 할당되는 전력 공급량은 50kw/h가 될 것이다. 이때, 전력 수요 검증 단계에서처럼 S도 Ss로 서명되어 전송되므로, 각 노드는 S를 보내온 발신지가 루트 노드(110)임을 확인할 수 있으며, 물론 이 확인 과정에는 Ps가 사용된다. 즉, S=Ps{Ss{S}}이다.

[0052] 검증을 위해 Ss로 서명된 Sv와 해당 자식 노드인 노드 Ni의 전력 수요 Vi도 전달된다. 편의상 이를 검증용 자기수요 Bi라고 하자. 자식 노드는 Ps를 사용하여 Sv를 얻고, Sv를 사용하여 자신이 보유하고 있던 Pv{Vi}를 복호화한 후, 수신한 Vi와 비교하여, 두 값이 일치하는지 여부로 검증한다. 즉, Sv{Pv{Vi}}가 부모 노드로부터 수신한 검증용 자기수요 Bi인 Vi와 일치하는지 비교한다.

[0053] 따라서 공급 가능 전력량 할당 단계의 동작은 도10과 같이 일반화해서 표현할 수 있다.

[0054] 부모 노드인 노드 Ni-1은 자식 노드인 노드 Ni에게 서명된 축소 비율, 검증용 자기수요 Bi, 검증용 비밀키를 전송한다(S1010). 전술한 바와 같이, 서명된 축소 비율은 Ss{S}이고, 검증용 자기수요 Bi는 노드 Ni의 전력 수요인 Vi이다. 검증용 비밀키는 Ss로 서명된 수요 파악용 비밀키 Sv인 Ss{Sv}이다.

[0055] 다음으로, 노드 Ni는 검증 과정을 수행한다(S1020). 자세하게는 전술한 바와 같이, Ps{Ss{S}}하여 S를 구하고, Ps{Ss{Sv}}하여 구한 Sv를 가지고 Sv{Pv{Vi}}하여 Vi를 구한 후, 이를 수신한 Vi와 비교하여 검증한다.

[0056] 다음으로, 노드 Ni는 자신에게 공급될 전력 할당량을 계산한다(S1030). 이는 전술한 바와 같이, S와 Vi를 곱해 산출된다.

[0057] 이때, 주의할 점은 도9에 나와있는 바와 같이, 검증용 비밀키 즉, Ss{Sv}는 리프 노드(130)의 조부모 노드까지만 전송된다는 것이다. 왜냐하면 리프 노드(130)의 부모 노드인 경우 Sv가 있으면 리프 노드(130)의 전력 수요를 바로 산출해버릴 수 있기 때문이다. 해당 노드가 오염되어 있을 경우, 이는 사용자의 전력 수요라는 민감한 정보의 외부 누출을 의미하므로, 이런 위험을 없애기 위해 본 발명은 Sv 전송을 리프 노드(130)의 조부모까지로만 제한하고 있다.

[0058] 도11은 도4의 전력 공급 및 소비 검증 단계(S440)에서의 동작을 나타낸 흐름도이다.

[0059] 본 발명은 리프 노드(130)에 대한 전력 공급을 전력 공급 할당량을 여러 조각들로 나누어 리프 노드(130)가 각 조각에 대한 요청을 보내오면 그 부모 노드(120)가 검증 과정을 거쳐 전력 조각을 공급해주도록 하고 있다. 소비자의 개인 정보를 보호한다는 본 발명의 목적에 따라, 부모 노드(120)가 각 소비자의 전력 수요를 모르고도 전력을 공급할 수 있게 한 것이다. 따라서 도11은 리프 노드(130)와 부모 노드(120) 사이에 수행되는 동작을 나타내고 있다. 예를 들면, 도9의 N4와 N8 사이의 동작을 보이고 있다.

[0060] 부모 노드(120)는 리프 노드(130)에 티켓 크기, 즉 티켓 생성 비율을 전송한다(S1110). 예를 들어, 전력 공급 할당량이 100kw/h이고, 티켓 크기가 5kw/h라면, N8은 5kw/h를 소비할 때마다 N4에 티켓을 전송하여 다음 5kw/h를 공급해줄 것을 요청해야 할 것이며, 총 티켓 수는 20개가 될 것이다.

[0061] 다음으로, 리프 노드(130)는 부모 노드(120)에 티켓 만료 조건과 검증 코드를 전송한다(S1120). 검증에는 해시 체인이 사용되며, 이를 위해 리프 노드(130)는 두개의 첨자 i, j를 선택한다. 만료 조건은 두 첨자 각각의 해시 값의 해시 값 즉, H(H(i)||H(j))이다. 검증 코드는 Hn(i)가 길이 n의 해시 체인을 나타낼 때, [H20(i), H20(j)]의 각 해시 값의 마지막 해시 체인 값이다.

[0062] 다음으로, 리프 노드(130)는 부모 노드(120)에 티켓을 전송하여 전력 공급을 요청한다(S1130). 티켓은 [H19(i), H19(j)]가 된다.

[0063] 다음으로, 부모 노드(120)는 티켓을 검증한다(S1140). 수신한 티켓의 각 값을 해시하여 [H(H19(i)), H(H19(j))]를 얻은 후, [H(H19(i)), H(H19(j))]를 [H20(i), H20(j)]와 비교하여 수신한 티켓을 검증한다.

[0064] 다음으로, 부모 노드(120)는 티켓 크기만큼 전력을 공급하며(S1150), 리프 노드(130)는 그 전력을 소비한다

(S1160).

[0065] 다음으로, 리프 노드(130)는 티켓을 다 써버리지 않았다면(S1170), 상기 티켓 요청 단계(S1130)를 반복한다. 즉, 마지막 티켓 [H20(i), H20(j)]이 전송된 후에는 부모 노드(120)는 리프 노드(130)에 대한 전력 공급을 중단한다.

[0066] 여기에서, 2개의 첨자를 사용한 이유는 부모 노드(120)가 해시 체인의 길이를 알아내는 것을 막기 위해서이다. 첨자를 하나만 사용한다면, 부모 노드(120)는 만료 조건이 H(i)이므로 쉽게 티켓 수를 알아낼 수 있을 것이다. 하지만, 2개의 첨자를 사용하면 Hn(H(i)||H(j))와 H(Hn(i)||Hn(j))는 같지 않기 때문에, 티켓 수를 알아낼 수 없다.

[0067] 전술한 본 발명의 설명은 예시를 위한 것이며, 본 발명이 속하는 기술분야의 통상의 지식을 가진 자는 본 발명의 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 쉽게 변형이 가능하다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적이 아닌 것으로 이해해야만 한다. 예를 들어, 단일형으로 설명되어 있는 각 구성 요소는 분산되어 실시될 수도 있으며, 마찬가지로 분산된 것으로 설명되어 있는 구성 요소들도 결합된 형태로 실시될 수 있다.

[0068] 본 발명의 범위는 상기 상세한 설명보다는 후술하는 특허청구범위에 의하여 나타내어지며, 특허청구범위의 의미 및 범위 그리고 그 균등 개념으로부터 도출되는 모든 변경 또는 변형된 형태가 본 발명의 범위에 포함되는 것으로 해석되어야 한다.

부호의 설명

[0069] 100: 스마트 그리드

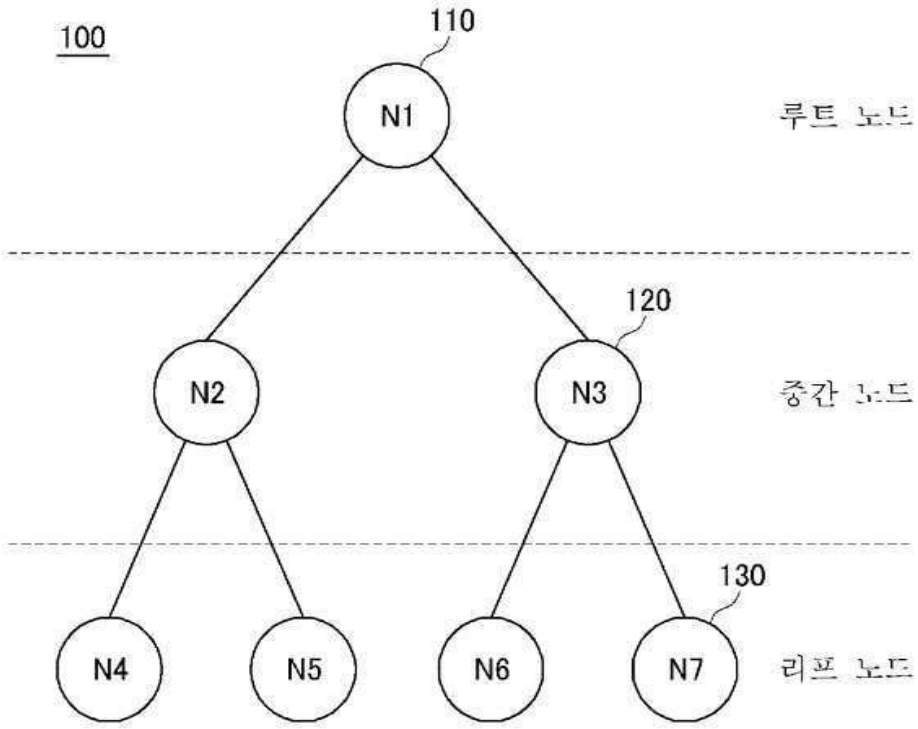
110: 루트 노드

120: 중간 노드

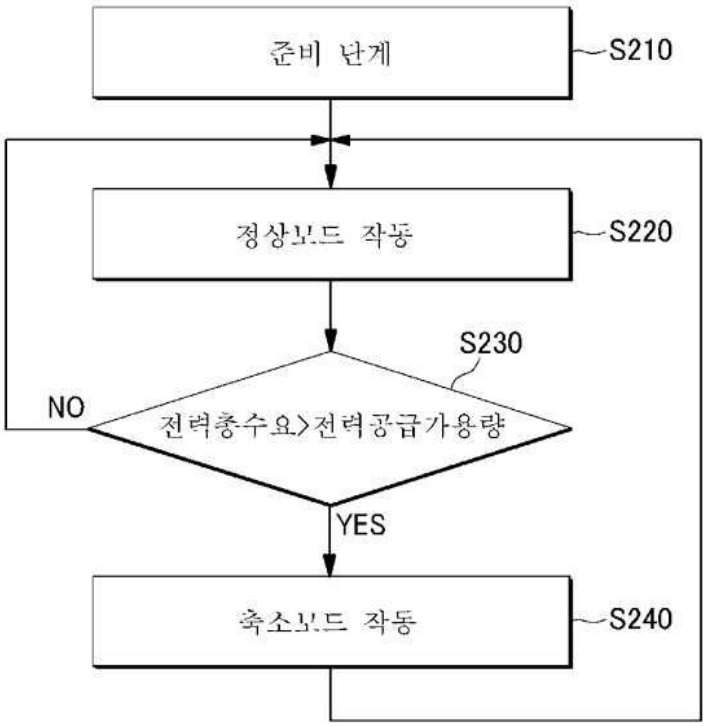
130: 리프 노드

도면

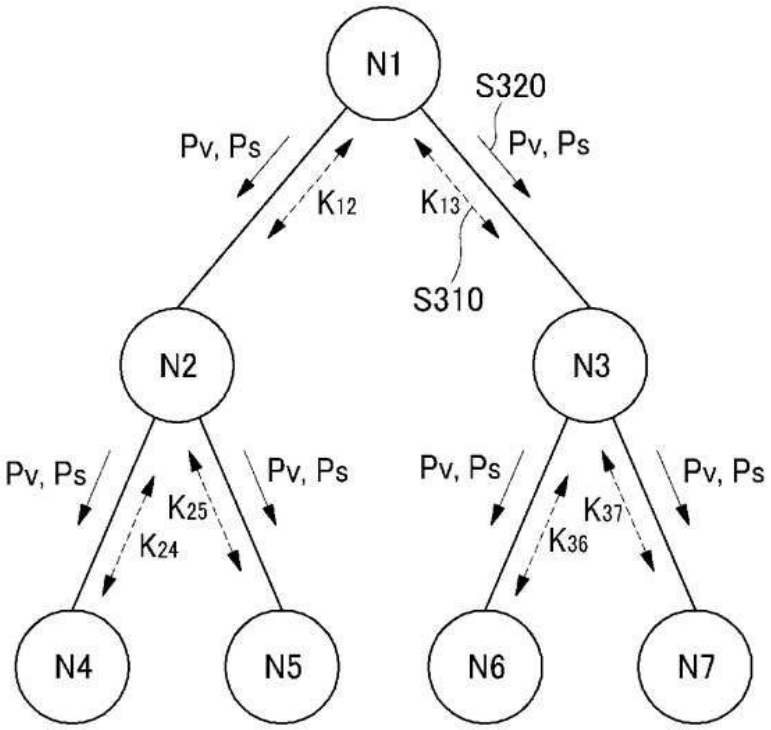
도면1



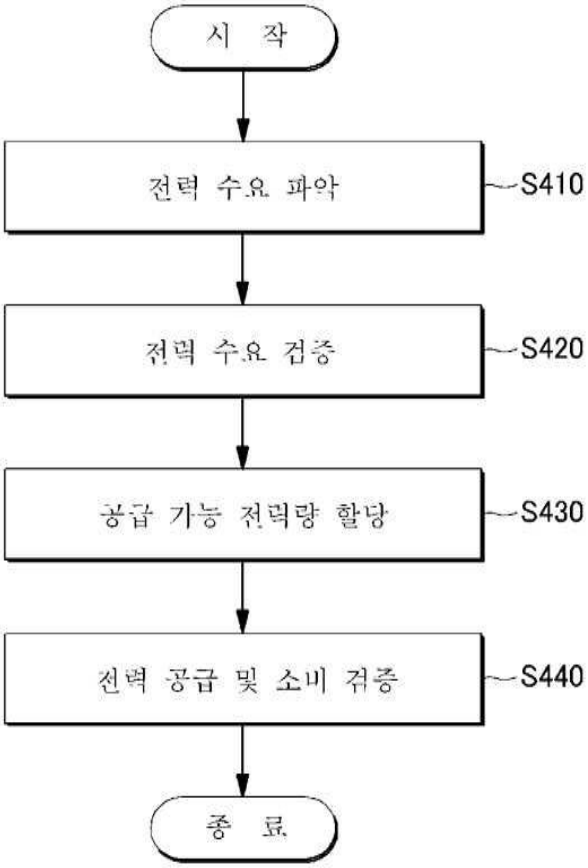
도면2


준비 단계
S210
정상모드 작동
S220
S230
NO
전력총수요>전력공급가용량
YES
축소모드 작동
S240

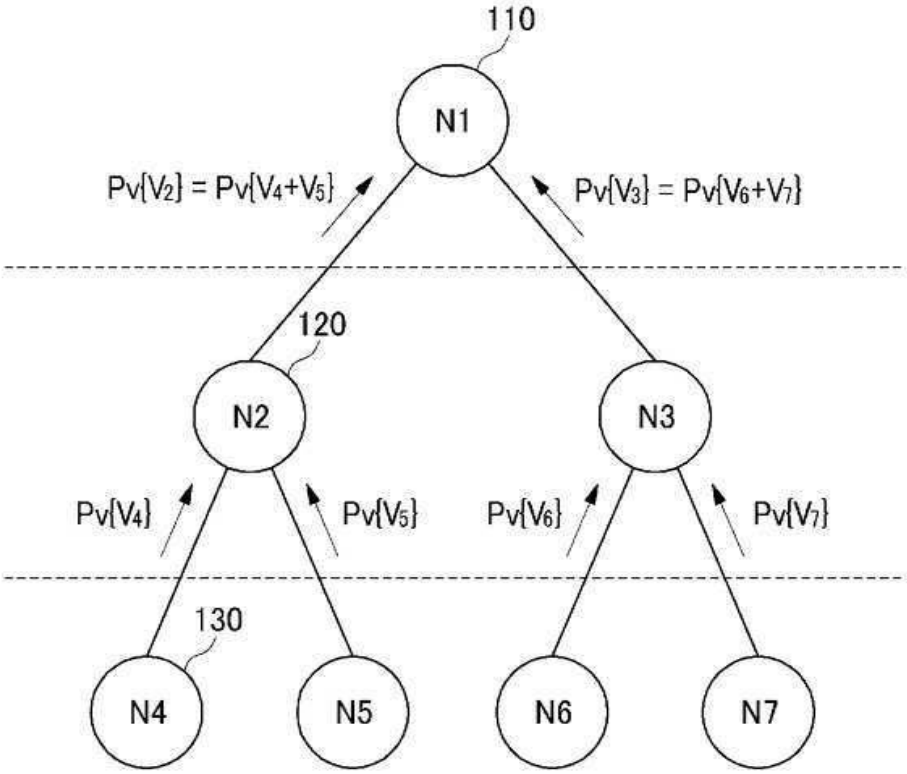
도면3


N1
S320
Pv, Ps
Pv, Ps
K12
K13
S310
N2
N3
Pv, Ps
Pv, Ps
Pv, Ps
Pv, Ps
K25
K24
K37
K36
N4
N5
N6
N7

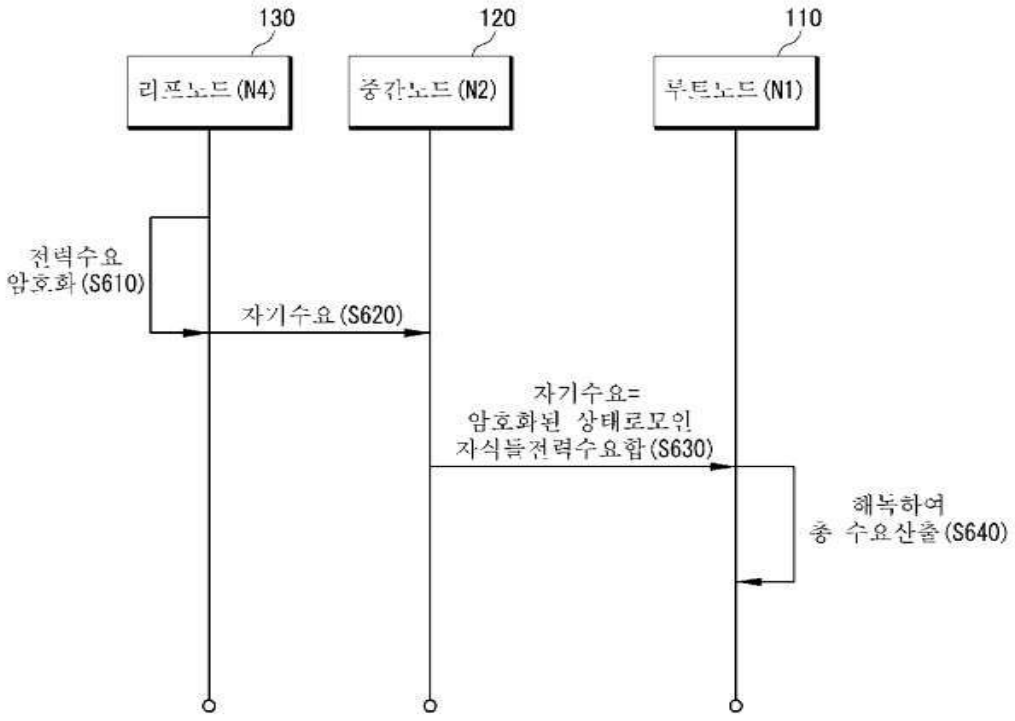
도면4


시 작
전력 수요 파악
S410
전력 수요 검증
S420
공급 가능 전력량 할당
S430
전력 공급 및 소비 검증
S440
종 료

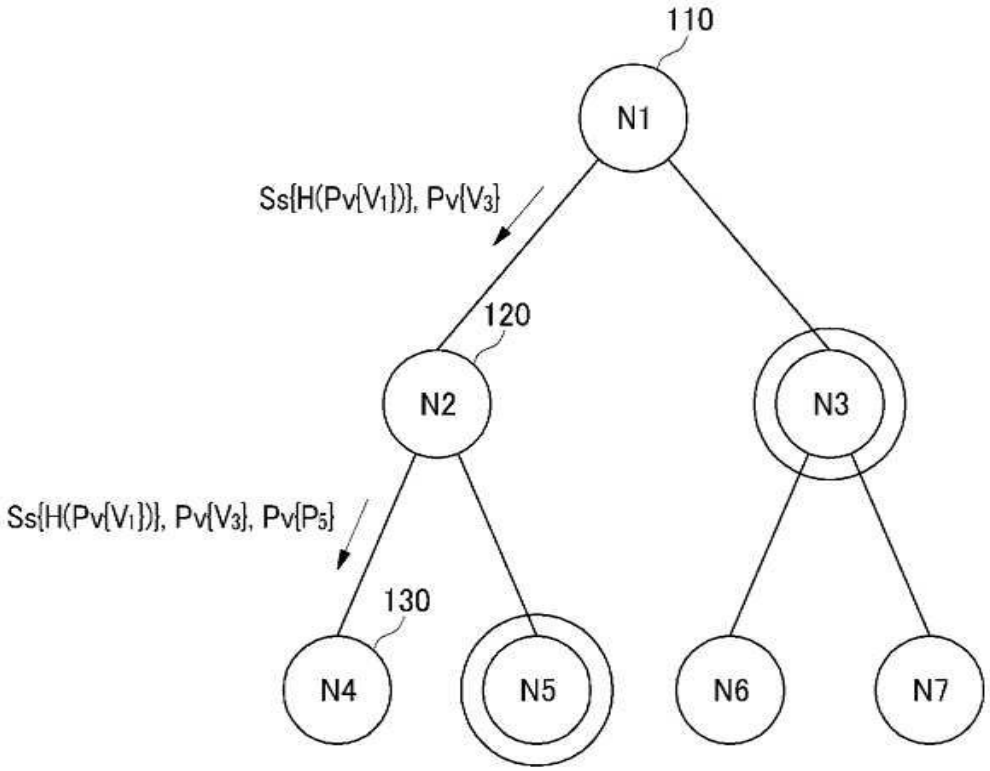
도면5


110
N1
Pv{V2} = Pv{V4+V5}
Pv{V3} = Pv{V6+V7}
120
N2
N3
Pv{V4}
Pv{V5}
Pv{V6}
Pv{V7}
130
N4
N5
N6
N7

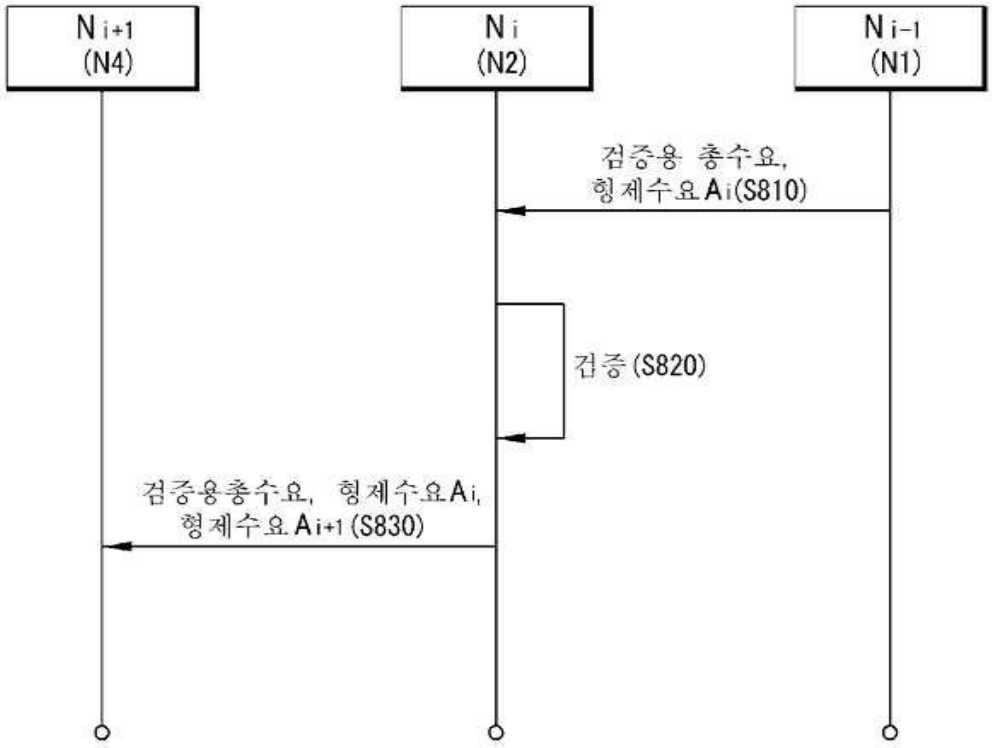
도면6


130
120
110
리프노드 (N4)
중간노드 (N2)
루트노드 (N1)
전력수요
암호화 (S610)
자기수요 (S620)
자기수요=
암호화된 상태로모인
자식들전력수요합 (S630)
해독하여
총 수요산출 (S640)

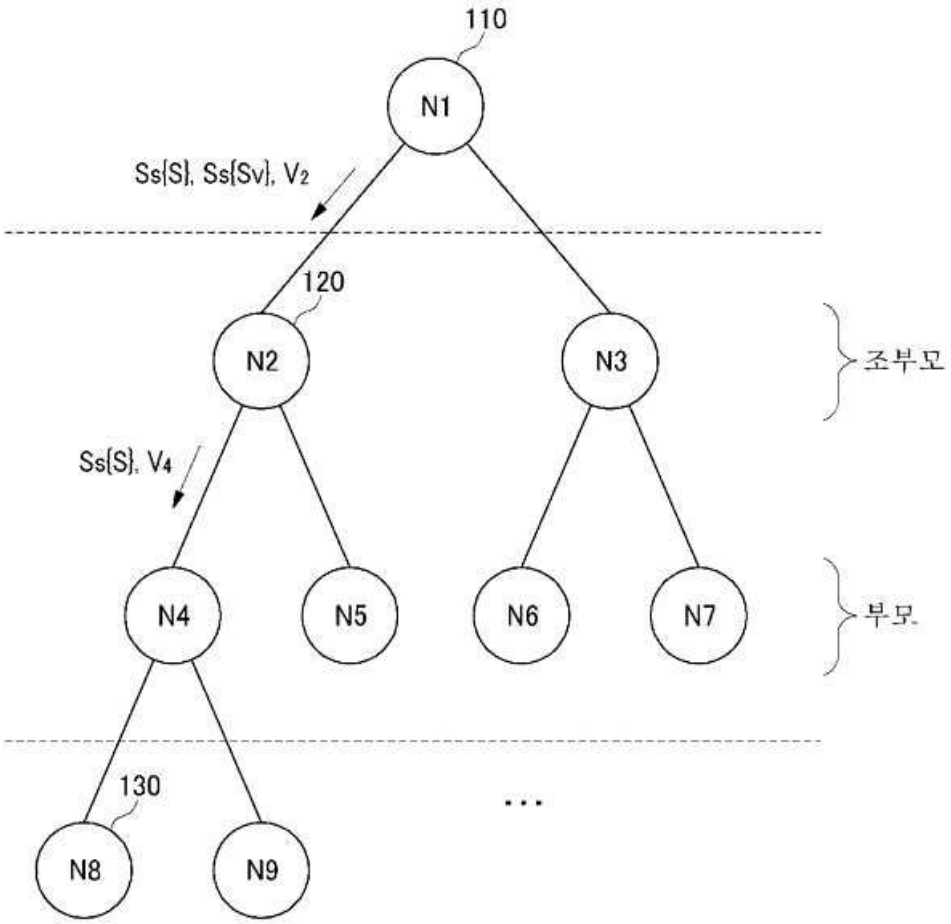
도면7


110
N1
Ss{H(Pv{V1})}, Pv{V3}
120
N2
N3
Ss{H(Pv{V1})}, Pv{V3}, Pv{P5}
130
N4
N5
N6
N7

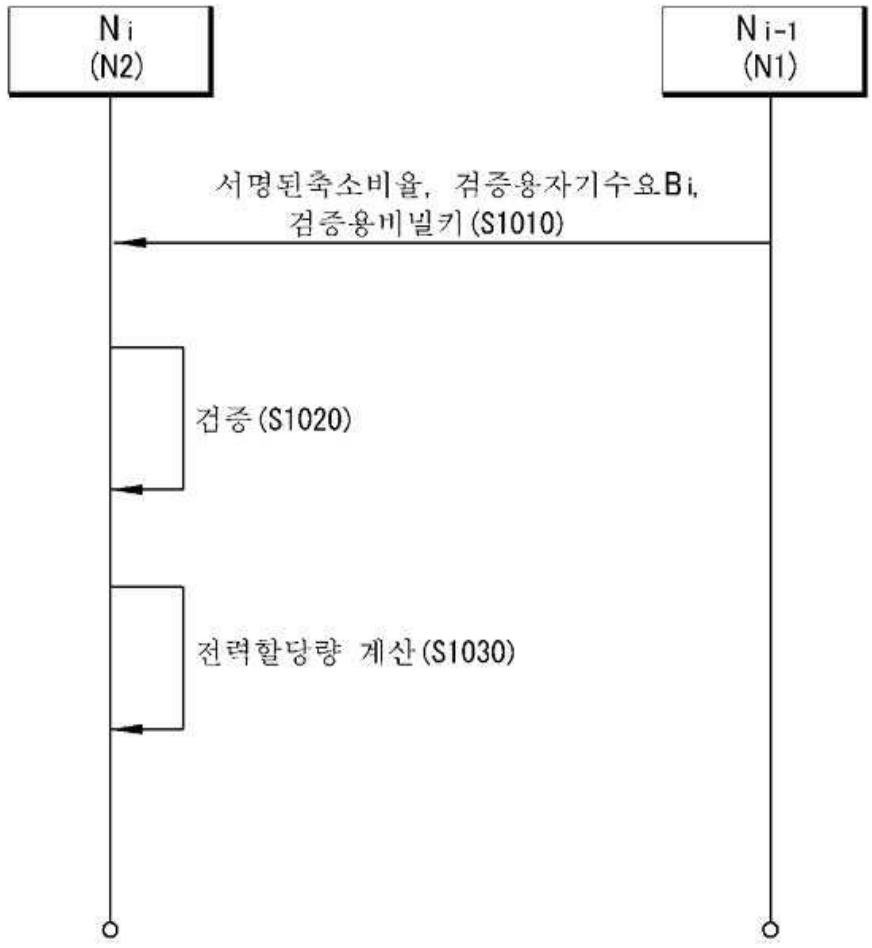
도면8


N i+1
(N4)
N i
(N2)
N i-1
(N1)
검증용 총수요,
형제수요 Ai (S810)
검증 (S820)
검증용총수요, 형제수요Ai,
형제수요 Ai+1 (S830)

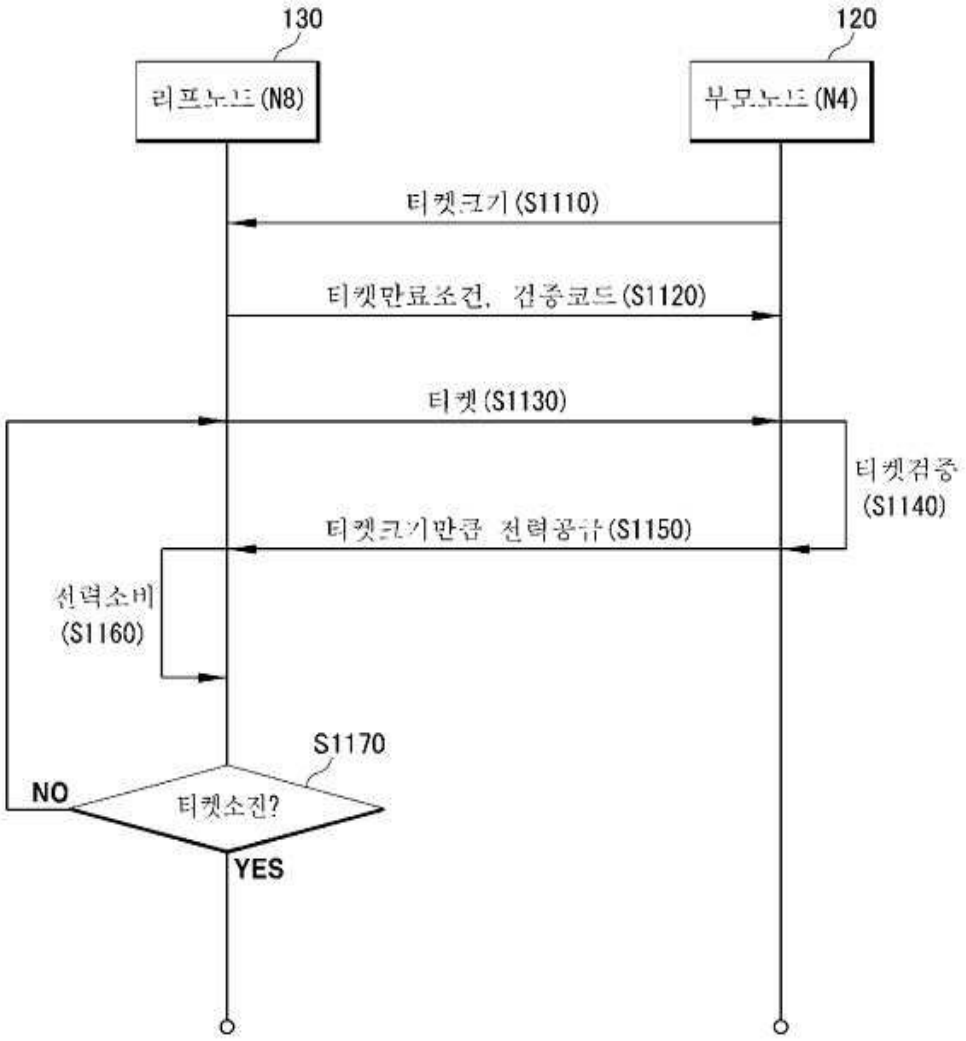
도면9



도면10


Ni
(N2)
Ni-1
(N1)
서명된축소비율, 검증용자기수요Bi,
검증용비밀키(S1010)
검증(S1020)
전력할당량 계산(S1030)

도면11


130
120
리프노드(N8)
부모노드(N4)
티켓크기(S1110)
티켓만료조건, 검증코드(S1120)
티켓(S1130)
티켓검증
(S1140)
티켓크기만큼 전력공급(S1150)
전력소비
(S1160)
S1170
NO
티켓소진?
YES