



(19) 대한민국특허청(KR)

(12) 등록특허공보(B1)

(45) 공고일자 2016년03월04일

(11) 등록번호 10-1600204

(24) 등록일자 2016년02월26일

(51) 국제특허분류(Int. Cl.)

H04L 9/14 (2006.01) H04L 9/30 (2006.01)

(21) 출원번호 10-2014-0195534

(22) 출원일자 2014년12월31일

심사청구일자 2014년12월31일

(56) 선행기술조사문헌

KR100863448 B1

KR1020080110000 A

(73) 특허권자

이화여자대학교 산학협력단

서울특별시 서대문구 이화여대길 52 (대현동, 이화여자대학교)

(72) 발명자

최경

서울특별시 서대문구 통일로34길 43, 109동 201호 (홍제동, 홍제원현대아파트)

채기준

서울특별시 강남구 강남대로136길 34

(74) 대리인

특허법인 무한

전체 청구항 수 : 총 21 항

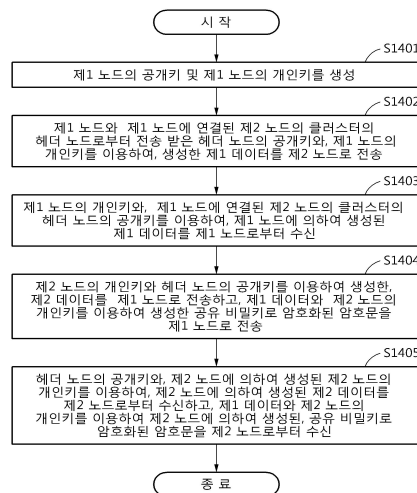
심사관 : 문형섭

(54) 발명의 명칭 데이터 암호화 전송 방법 및 노드 및 컴퓨터에서 판독 가능한 기록 매체

(57) 요약

본 발명은 데이터 암호화 전송 방법에 관한 것이다. 본 발명에 따르면, 제1 노드의 공개키 및 제1 노드의 개인키를 생성하는 단계;와 상기 제1 노드와 상기 제1 노드에 연결된 제2 노드의 클러스터의 헤더 노드로부터 전송 받은 헤더 노드의 공개키와, 상기 제1 노드의 개인키를 이용하여, 생성한 제1 데이터를 상기 제2 노드로 전송하는 단계; 및 상기 헤더 노드의 공개키와, 상기 제2 노드에 의하여 생성된 제2 노드의 개인키를 이용하여, 상기 제2 노드에 의하여 생성된 제2 데이터를 상기 제2 노드로부터 수신하고, 상기 제1 데이터와 상기 제2 노드의 개인키를 이용하여 상기 제2 노드에 의하여 생성된, 공유 비밀키로 암호화된 암호문을 상기 제2 노드로부터 수신하는 단계;를 포함하는 데이터 암호화 전송 방법이 제공된다. 본 발명에 따르면, 비밀키를 사용해서 메시지를 암호화해서 전송함으로써 안전한 데이터 전송을 제공할 수 있다.

대표도 - 도14



이 발명을 지원한 국가연구개발사업

과제고유번호 2013R1A1A2011788

부처명 교육부

연구관리전문기관 한국연구재단

연구사업명 기초연구사업(학술진흥)(2013)-일반연구자지원사업-기본연구

연구과제명 CDN 환경에서의 안전하고 효율적인 서비스 보안 기법

기 여 율 1/1

주관기관 이화여자대학교 산학협력단

연구기간 2013.06.01 ~ 2016.05.31

명세서

청구범위

청구항 1

제1 노드가 수행하는 데이터 암호화 전송 방법에 있어서,

제1 노드의 공개키 및 제1 노드의 개인키를 생성하는 단계;

상기 제1 노드와 상기 제1 노드에 연결된 제2 노드의 클러스터의 헤더 노드로부터 전송 받은 헤더 노드의 공개키와, 상기 제1 노드의 개인키를 이용하여, 생성한 제1 데이터를 상기 제2 노드로 전송하는 단계; 및

상기 헤더 노드의 공개키와, 상기 제2 노드에 의하여 생성된 제2 노드의 개인키를 이용하여, 상기 제2 노드에 의하여 생성된 제2 데이터를 상기 제2 노드로부터 수신하고, 상기 제1 데이터와 상기 제2 노드의 개인키를 이용하여 상기 제2 노드에 의하여 생성된, 공유 비밀키로 암호화된 암호문을 상기 제2 노드로부터 수신하는 단계;

를 포함하는 데이터 암호화 전송 방법.

청구항 2

제1항에 있어서,

상기 전송하는 단계는,

상기 제1 데이터와 상기 제1 노드의 아이디와 임의의 값인 제1 난스값을 전송하는 데이터 암호화 전송 방법.

청구항 3

제1항에 있어서,

상기 제1 데이터는,

상기 헤더 노드의 공개키 및 상기 제1 노드의 개인키를 이용하여 생성한 제1 비밀값과, 상기 제1 비밀값을 이용하여 생성한 제1 서브맥 메시지인 데이터 암호화 전송 방법.

청구항 4

제1항에 있어서,

상기 수신하는 단계는,

상기 제2 데이터를 인증하여 완료되면, 상기 제2 데이터와 상기 제1 노드의 개인키를 이용하여 상기 공유 비밀키를 생성하고, 상기 암호문을 상기 공유 비밀키로 복호화하여 상기 암호문의 원문 메시지를 획득하는 데이터 암호화 전송 방법.

청구항 5

제1항에 있어서,

상기 수신하는 단계는,

상기 제2 데이터와 상기 제2 노드의 아이디와 임의의 값인 제2 난스값을 상기 제2 노드로부터 수신하고, 상기 제2 데이터로서, 제2 비밀값과 상기 제2 비밀값을 이용하여 상기 제2 노드에 의하여 생성된 제2 서브맥 메시지를 상기 제2 노드로부터 수신하는 데이터 암호화 전송 방법.

청구항 6

제2 노드가 수행하는 데이터 암호화 전송 방법에 있어서,

제1 노드의 개인키와, 상기 제1 노드에 연결된 제2 노드의 클러스터의 헤더 노드의 공개키를 이용하여, 상기 제1 노드에 의하여 생성된 제1 데이터를 상기 제1 노드로부터 수신하는 단계;

제2 노드의 공개키 및 제2 노드의 개인키를 생성하는 단계; 및

상기 제2 노드의 개인키와 상기 헤더 노드의 공개키를 이용하여 생성한, 제2 데이터를 상기 제1 노드로 전송하고, 상기 제1 데이터와 상기 제2 노드의 개인키를 이용하여 생성한 공유 비밀키로 암호화된 암호문을 상기 제1 노드로 전송하는 단계;

를 포함하는 데이터 암호화 전송 방법.

청구항 7

제6항에 있어서,

상기 수신하는 단계는,

상기 제1 데이터와 상기 제1 노드의 아이디와 임의의 값인 제1 난스값을 수신하는 데이터 암호화 전송 방법.

청구항 8

제6항에 있어서,

상기 제1 데이터는,

상기 헤더 노드의 공개키 및 상기 제1 노드의 개인키를 이용하여, 상기 제1 노드에 의하여 생성된 제1 비밀값과, 상기 제1 비밀값을 이용하여 상기 제1 노드에 의하여 생성된 제1 서브맥 메시지를 데이터 암호화 전송 방법.

청구항 9

제6항에 있어서,

상기 전송하는 단계는,

상기 제1 데이터를 인증하여 완료되면, 상기 제1 데이터와 상기 제2 노드의 개인키를 이용하여 상기 공유 비밀키를 생성하고, 상기 암호문의 원문 메시지를 상기 공유 비밀키로 암호화하여 상기 암호문을 전송하는 데이터 암호화 전송 방법.

청구항 10

제6항에 있어서,

상기 전송하는 단계는,

상기 제2 데이터와 상기 제2 노드의 아이디와 임의의 값인 제2 난스값을 상기 제1 노드로 전송하고, 상기 제2 데이터로서, 제2 비밀값과 상기 제2 비밀값을 이용하여 생성한 제2 서브맥 메시지를 상기 제1 노드로 전송하는 데이터 암호화 전송 방법.

청구항 11

삭제

청구항 12

삭제

청구항 13

삭제

청구항 14

삭제

청구항 15

데이터 암호화 전송 노드에 있어서,

상기 데이터 암호화 전송 노드인, 제1 노드의 공개키 및 제1 노드의 개인키를 생성하고, 상기 제1 노드 및 상기 제1 노드에 연결된 제2 노드의 클러스터의 헤더 노드로부터 전송 받은 헤더 노드의 공개키와, 상기 제1 노드의 개인키를 이용하여, 생성한 제1 데이터를 생성하는 프로세서, 및

상기 제1 데이터를 상기 제1노드와 연결된 제2 노드로 전송하는 데이터 송수신부를 포함하되,

상기 데이터 송수신부는,

상기 헤더 노드의 공개키와, 상기 제2 노드에 의하여 생성된 제2 노드의 개인키를 이용하여, 상기 제2 노드에 의하여 생성된 제2 데이터를 상기 제2 노드로부터 수신하고, 상기 제1 데이터와 상기 제2 노드의 개인키를 이용하여 상기 제2 노드에 의하여 생성된, 공유 비밀키로 암호화된 암호문을 상기 제2 노드로부터 수신하는 데이터 암호화 전송 노드.

청구항 16

제15항에 있어서,

상기 데이터 송수신부는,

상기 제1 데이터와 상기 제1 노드의 아이디와 임의의 값인 제1 난스값을 전송하는 데이터 암호화 전송 노드.

청구항 17

제15항에 있어서,

상기 제1 데이터는,

상기 헤더 노드의 공개키 및 상기 제1 노드의 개인키를 이용하여 생성한 제1 비밀값과, 상기 제1 비밀값을 이용하여 생성한 제1 서브택 메시지인 데이터 암호화 전송 노드.

청구항 18

제15항에 있어서,

상기 프로세서는,

상기 제2 데이터를 인증하여 완료되면, 상기 제2 데이터와 상기 제1 노드의 개인키를 이용하여 상기 공유 비밀키를 생성하고, 상기 암호문을 상기 공유 비밀키로 복호화하여 상기 암호문의 원문 메시지를 획득하는 데이터 암호화 전송 노드.

청구항 19

제15항에 있어서,

상기 데이터 송수신부는,

상기 제2 데이터와 상기 제2 노드의 아이디와 임의의 값인 제2 난스값을 상기 제2 노드로부터 수신하고, 상기 제2 데이터로서, 제2 비밀값과 상기 제2 비밀값을 이용하여 상기 제2 노드에 의하여 생성된 제2 서브택 메시지를 상기 제2 노드로부터 수신하는 데이터 암호화 전송 노드.

청구항 20

데이터 암호화 전송 노드에 있어서,

제1 노드의 개인키와, 상기 제1 노드에 연결된 상기 데이터 암호화 전송 노드인 제2 노드의 클러스터의 헤더 노드의 공개키를 이용하여, 상기 제1 노드에 의하여 생성된 제1 데이터를 상기 제1 노드로부터 수신하는 데이터 송수신부, 및

상기 데이터 암호화 전송 노드인, 제2 노드의 공개키 및 제2 노드의 개인키를 생성하는 프로세서를 포함하되,

상기 데이터 송수신부는,

상기 제2 노드의 개인키와 상기 헤더 노드의 공개키를 이용하여 상기 프로세서가 생성한, 제2 데이터를 상기 제1 노드로 전송하고, 상기 제1 데이터와 상기 제2 노드의 개인키를 이용하여 상기 프로세서가 생성한 공유 비밀키로 암호화된 암호문을 상기 제1 노드로 전송하는 데이터 암호화 전송 노드.

청구항 21

제20항에 있어서,

상기 데이터 송수신부는,

상기 제1 데이터와 상기 제1 노드의 아이디와 임의의 값인 제1 난스값을 수신하는 데이터 암호화 전송 노드.

청구항 22

제20항에 있어서,

상기 제1 데이터는,

상기 헤더 노드의 공개키 및 상기 제1 노드의 개인키를 이용하여, 상기 제1 노드에 의하여 생성된 제1 비밀값과, 상기 제1 비밀값을 이용하여 상기 제1 노드에 의하여 생성된 제1 서브맥 메시지를 데이터 암호화 전송 노드.

청구항 23

제20항에 있어서,

상기 프로세서는,

상기 제1 데이터를 인증하여 완료되면, 상기 제1 데이터와 상기 제2 노드의 개인키를 이용하여 상기 공유 비밀키를 생성하고, 상기 암호문의 원문 메시지를 상기 공유 비밀키로 암호화하고,

상기 데이터 송수신부는,

상기 암호문을 전송하는 데이터 암호화 전송 노드.

청구항 24

제20항에 있어서,

상기 데이터 송수신부는,

상기 제2 데이터와 상기 제2 노드의 아이디와 임의의 값인 제2 난스값을 상기 제1 노드로 전송하고, 상기 제2 데이터로서, 제2 비밀값과 상기 제2 비밀값을 이용하여 상기 프로세서가 생성한 제2 서브맥 메시지를 상기 제1 노드로 전송하는 데이터 암호화 전송 노드.

청구항 25

삭제

청구항 26

삭제

청구항 27

삭제

청구항 28

삭제

청구항 29

제1항 내지 제10항 중 어느 한 항의 방법을 실행하기 위한 프로그램이 기록된 컴퓨터에서 판독 가능한 기록 매

체.

발명의 설명

기술 분야

[0001] 본 발명은, 데이터 암호화 전송 방법 및 노드 및 컴퓨터에서 관독 가능한 기록 매체에 관한 것이다.

배경 기술

[0002] 스마트 그리드(Smart Grid) 시장은 지속적인 성장을 하고 있으며, 스마트 배전시스템 전기차 충전인프라, AMI(Advanced Metering Infrastructure) 시스템 등의 기술 개발이 꾸준히 이뤄지고 있다.

[0003] 특히, 미국의 경우, 2000년 전력대란, 2001년 대규모 정전사태, 2003년 중동부지역 정전사태의 경험으로 인하여 이에 대응할 솔루션을 획득하기 위하여, 꾸준한 연구가 진행되고 있다.

[0004] 스마트 그리드는 전력망에 정보통신 기술을 접목한 새로운 형태의 전력 공급시스템이다. 스마트 그리드는 전력 공급을 위해서 전력공급시스템과 사용자가 양방향으로 의사 소통하는 시스템이다.

[0005] 스마트 그리드 환경에서는 각 가정과 건물이 실시간으로 에너지 사용량을 확인할 수 있어 언제 사용량이 폭증하며 어느 시간 때에 사용량이 줄어드는 지를 확인할 수 있다.

[0006] 이로 인한 편리성과 효율성은 향상되었지만, 더불어 다루어지는 정보들의 중요성으로 인하여, 이 정보들을 안전하게 저장하고 전송하는 것이 필요하다.

[0007] 스마트 그리드 환경의 취약성을 이용해서 중요 정보 및 개인 정보를 취득하여 이를 악용한 다양한 공격들이 발생하고 있다. 작게는 홈이나 빌딩 하나에서부터 스마트 그리드 시스템 전체까지 시스템 중단을 통해 엄청난 규모의 가용성침해를 통한 경제적 및 사회적 큰 문제가 발생하여 혼란을 야기할 수 있는 공격까지 발생하고 있다.

[0008] 이러한 공격 기법들로 인한 피해를 방지할 수 있으며, 스마트 그리드 환경에서 에너지를 더욱 절감하기 위한 기술을 제안한다.

발명의 내용

해결하려는 과제

[0009] 본 발명은 상술한 문제점을 모두 해결하는 것을 목적으로 한다.

[0010] 본 발명은, 전송 데이터를 효율적으로 전송하고 데이터 송신 및 수신에 사용되는 에너지를 감소시켜 에너지 절감을 제공하는 것을 다른 목적으로 한다.

[0011] 본 발명은, 비밀키를 사용해서 메시지를 암호화해서 전송함으로써 안전한 데이터 전송을 제공하는 것을 또 다른 목적으로 한다.

[0012] 본 발명은, 스마트 미터기의 에너지 사용량을 감소시키는 것을 또 다른 목적으로 한다.

과제의 해결 수단

[0013] 상기한 바와 같은 본 발명의 목적을 달성하고, 후술하는 본 발명의 특징적인 효과를 실현하기 위한, 본 발명의 특징적인 구성은 하기와 같다.

[0014] 일실시예에 따른, 제1 노드가 수행하는 데이터 암호화 전송 방법에 있어서,

[0015] 제1 노드의 공개키 및 제1 노드의 개인키를 생성하는 단계; 상기 제1 노드와 상기 제1 노드에 연결된 제2 노드의 클러스터의 헤더 노드로부터 전송 받은 헤더 노드의 공개키와, 상기 제1 노드의 개인키를 이용하여, 생성한 제1 데이터를 상기 제2 노드로 전송하는 단계; 및 상기 헤더 노드의 공개키와, 상기 제2 노드에 의하여 생성된 제2 노드의 개인키를 이용하여, 상기 제2 노드에 의하여 생성된 제2 데이터를 상기 제2 노드로부터 수신하고, 상기 제1 데이터와 상기 제2 노드의 개인키를 이용하여 상기 제2 노드에 의하여 생성된, 공유 비밀키로 암호화된 암호문을 상기 제2 노드로부터 수신하는 단계;를 포함할 수 있다.

[0016] 다른 실시예에 따른, 상기 전송하는 단계는, 상기 제1 데이터와 상기 제1 노드의 아이디와 임의의 값인 제1 난

스값을 전송하는 것을 포함할 수 있다.

- [0017] 또 다른 실시예에 따른, 상기 제1 데이터는, 상기 헤더 노드의 공개키 및 상기 제1 노드의 개인키를 이용하여 생성한 제1 비밀값과, 상기 제1 비밀값을 이용하여 생성한 제1 서브맥 메시지를 포함할 수 있다.
- [0018] 또 다른 실시예에 따른, 상기 수신하는 단계는, 상기 제2 데이터를 인증하여 완료되면, 상기 제2 데이터와 상기 제1 노드의 개인키를 이용하여 상기 공유 비밀키를 생성하고, 상기 암호문을 상기 공유 비밀키로 복호화하여 상기 암호문의 원문 메시지를 획득하는 것을 포함할 수 있다.
- [0019] 또 다른 실시예에 따른, 상기 수신하는 단계는, 상기 제2 데이터와 상기 제2 노드의 아이디와 임의의 값인 제2 난스값을 상기 제2 노드로부터 수신하고, 상기 제2 데이터로서, 제2 비밀값과 상기 제2 비밀값을 이용하여 상기 제2 노드에 의하여 생성된 제2 서브맥 메시지를 상기 제2 노드로부터 수신하는 것을 포함할 수 있다.
- [0020] 일실시예에 따른, 제2 노드가 수행하는 데이터 암호화 전송 방법에 있어서,
- [0021] 제1 노드의 개인키와, 상기 제1 노드에 연결된 제2 노드의 클러스터의 헤더 노드의 공개키를 이용하여, 상기 제1 노드에 의하여 생성된 제1 데이터를 상기 제1 노드로부터 수신하는 단계;와 제2 노드의 공개키 및 제2 노드의 개인키를 생성하는 단계; 및 상기 제2 노드의 개인키와 상기 헤더 노드의 공개키를 이용하여 생성한, 제2 데이터를 상기 제1 노드로 전송하고, 상기 제1 데이터와 상기 제2 노드의 개인키를 이용하여 생성한 공유 비밀키로 암호화된 암호문을 상기 제1 노드로 전송하는 단계;를 포함할 수 있다.
- [0022] 다른 실시예에 따른, 상기 수신하는 단계는, 상기 제1 데이터와 상기 제1 노드의 아이디와 임의의 값인 제1 난스값을 수신하는 것을 포함할 수 있다.
- [0023] 또 다른 실시예에 따른, 상기 제1 데이터는,
- [0024] 상기 헤더 노드의 공개키 및 상기 제1 노드의 개인키를 이용하여, 상기 제1 노드에 의하여 생성된 제1 비밀값과, 상기 제1 비밀값을 이용하여 상기 제1 노드에 의하여 생성된 제1 서브맥 메시지를 포함할 수 있다.
- [0025] 또 다른 실시예에 따른, 상기 전송하는 단계는, 상기 제1 데이터를 인증하여 완료되면, 상기 제1 데이터와 상기 제2 노드의 개인키를 이용하여 상기 공유 비밀키를 생성하고, 상기 암호문의 원문 메시지를 상기 공유 비밀키로 암호화하여 상기 암호문을 전송하는 것을 포함할 수 있다.
- [0026] 또 다른 실시예에 따른, 상기 전송하는 단계는, 상기 제2 데이터와 상기 제2 노드의 아이디와 임의의 값인 제2 난스값을 상기 제1 노드로 전송하고, 상기 제2 데이터로서, 제2 비밀값과 상기 제2 비밀값을 이용하여 생성한 제2 서브맥 메시지를 상기 제1 노드로 전송하는 것을 포함할 수 있다.
- [0027] 일실시예에 따른, 헤더 노드가 수행하는 데이터 암호화 전송 방법에 있어서, 상기 헤더 노드가 상기 헤더 노드와 연결된 네트워크에서 클러스터의 헤더 노드로 결정되고, 상기 클러스터의 복수의 노드들의 통신 경로를 설정하여 클러스터링하는 단계; 상기 헤더 노드의 공개키를 상기 클러스터의 멤버 노드들로 전송하는 단계; 및 상기 헤더 노드의 공개키와 상기 멤버 노드의 개인키를 이용하여 암호화된 메시지를 상기 멤버 노드들로부터 수신하는 단계;를 포함하고, 상기 수신하는 단계는, 기설정된 조건에 의하여 상기 암호화된 메시지를 수신하는 시간이 변경되고, 상기 암호화된 메시지를 복호화하여 상기 멤버 노드의 수치 정보를 획득하는 것을 포함할 수 있다.
- [0028] 다른 실시예에 따른, 상기 클러스터링하는 단계는, 상기 헤더 노드와 연결된 네트워크에 포함된 복수의 노드들과 베이스 스테이션 간의 거리 및 상기 네트워크에 포함된 복수의 노드들 각각의 에너지를 고려하여 상기 네트워크에 포함된 복수의 노드들 중 클러스터의 헤더 노드로 결정하는 것을 포함할 수 있다.
- [0029] 또 다른 실시예에 따른, 상기 클러스터링하는 단계는, 상기 헤더 노드와 상기 베이스 스테이션 간의 거리, 상기 헤더 노드의 에너지값, 및 상기 헤더 노드가 클러스터의 헤더 노드가 될 확률을 이용하여 제1 임계값을 계산하고, 상기 제1 임계값과 상기 헤더 노드가 선택한 랜덤값을 비교하여, 상기 헤더 노드가 선택한 랜덤값이 상기 제1 임계값보다 작으면, 상기 노드를 헤더 노드로 결정하는 것을 포함할 수 있다.
- [0030] 또 다른 실시예에 따른, 상기 에너지값은, 상기 헤더 노드의 현재 보유 에너지 및 상기 헤더 노드의 최대 보유 에너지를 포함할 수 있다.
- [0031] 일실시예에 따른, 데이터 암호화 전송 노드에 있어서, 상기 데이터 암호화 전송 노드인, 제1 노드의 공개키 및 제1 노드의 개인키를 생성하고, 상기 제1 노드 및 상기 제1 노드에 연결된 제2 노드의 클러스터의 헤더 노드로부터 전송 받은 헤더 노드의 공개키와, 상기 제1 노드의 개인키를 이용하여, 생성한 제1 데이터를 생성하는 프

로세서, 및 상기 제1 데이터를 상기 제1노드와 연결된 제2 노드로 전송하는 데이터 송수신부를 포함하되, 상기 데이터 송수신부는, 상기 헤더 노드의 공개키와, 상기 제2 노드에 의하여 생성된 제2 노드의 개인키를 이용하여, 상기 제2 노드에 의하여 생성된 제2 데이터를 상기 제2 노드로부터 수신하고, 상기 제1 데이터와 상기 제2 노드의 개인키를 이용하여 상기 제2 노드에 의하여 생성된, 공유 비밀키로 암호화된 암호문을 상기 제2 노드로부터 수신하는 것을 포함할 수 있다.

- [0032] 다른 실시예에 따른, 상기 데이터 송수신부는, 상기 제1 데이터와 상기 제1 노드의 아이디와 임의의 값인 제1 난스값을 전송하는 것을 포함할 수 있다.
- [0033] 또 다른 실시예에 따른상기 제1 데이터는, 상기 헤더 노드의 공개키 및 상기 제1 노드의 개인키를 이용하여 생성한 제1 비밀값과, 상기 제1 비밀값을 이용하여 생성한 제1 서브맥 메시지를 포함할 수 있다.
- [0034] 또 다른 실시예에 따른, 상기 프로세서는, 상기 제2 데이터를 인증하여 완료되면, 상기 제2 데이터와 상기 제1 노드의 개인키를 이용하여 상기 공유 비밀키를 생성하고, 상기 암호문을 상기 공유 비밀키로 복호화하여 상기 암호문의 원문 메시지를 획득하는 것을 포함할 수 있다.
- [0035] 또 다른 실시예에 따른, 상기 데이터 송수신부는, 상기 제2 데이터와 상기 제2 노드의 아이디와 임의의 값인 제2 난스값을 상기 제2 노드로부터 수신하고, 상기 제2 데이터로서, 제2 비밀값과 상기 제2 비밀값을 이용하여 상기 제2 노드에 의하여 생성된 제2 서브맥 메시지를 상기 제2 노드로부터 수신하는 것을 포함할 수 있다.
- [0036] 일실시예에 따른, 데이터 암호화 전송 노드에 있어서, 제1 노드의 개인키와, 상기 제1 노드에 연결된 상기 데이터 암호화 전송 노드인 제2 노드의 클러스터의 헤더 노드의 공개키를 이용하여, 상기 제1 노드에 의하여 생성된 제1 데이터를 상기 제1 노드로부터 수신하는 데이터 송수신부, 및 상기 데이터 암호화 전송 노드인, 제2 노드의 공개키 및 제2 노드의 개인키를 생성하는 프로세서를 포함하되, 상기 데이터 송수신부는,상기 제2 노드의 개인키와 상기 헤더 노드의 공개키를 이용하여 상기 프로세서가 생성한, 제2 데이터를 상기 제1 노드로 전송하고, 상기 제1 데이터와 상기 제2 노드의 개인키를 이용하여 상기 프로세서가 생성한 공유 비밀키로 암호화된 암호문을 상기 제1 노드로 전송하는 것을 포함할 수 있다.
- [0037] 다른 실시예에 따른, 상기 데이터 송수신부는, 상기 제1 데이터와 상기 제1 노드의 아이디와 임의의 값인 제1 난스값을 수신하는 것을 포함할 수 있다.
- [0038] 또 다른 실시예에 따른, 상기 제1 데이터는, 상기 헤더 노드의 공개키 및 상기 제1 노드의 개인키를 이용하여, 상기 제1 노드에 의하여 생성된 제1 비밀값과, 상기 제1 비밀값을 이용하여 상기 제1 노드에 의하여 생성된 제1 서브맥 메시지인 데이터를 포함할 수 있다.
- [0039] 또 다른 실시예에 따른, 상기 프로세서는, 상기 제1 데이터를 인증하여 완료되면, 상기 제1 데이터와 상기 제2 노드의 개인키를 이용하여 상기 공유 비밀키를 생성하고, 상기 암호문의 원문 메시지를 상기 공유 비밀키로 암호화하고, 상기 데이터 송수신부는, 상기 암호문을 전송하는 것을 포함할 수 있다.
- [0040] 또 다른 실시예에 따른, 상기 데이터 송수신부는, 상기 제2 데이터와 상기 제2 노드의 아이디와 임의의 값인 제2 난스값을 상기 제1 노드로 전송하고, 상기 제2 데이터로서, 제2 비밀값과 상기 제2 비밀값을 이용하여 상기 프로세서가 생성한 제2 서브맥 메시지를 상기 제1 노드로 전송하는 것을 포함할 수 있다.
- [0041] 일 실시예에 따른, 데이터 암호화 전송 노드에 있어서, 상기 데이터 암호화 전송 노드인, 헤더 노드가 상기 헤더 노드와 연결된 네트워크에서 클러스터의 헤더 노드로 결정하고, 상기 클러스터의 복수의 노드들의 통신 경로를 설정하여 클러스터링하는 클러스터링 관리부,와 상기 헤더 노드의 공개키를 상기 클러스터의 멤버 노드들로 전송하고, 상기 헤더 노드의 공개키와 상기 멤버 노드의 개인키를 이용하여 암호화된 메시지를 상기 멤버 노드들로부터 수신하는 데이터 송수신부, 및
- [0042] 기설정된 조건에 의하여 상기 암호화된 메시지를 수신하는 시간이 변경되고, 상기 암호화된 메시지를 복호화하여 상기 멤버 노드의 수치 정보를 획득하는 암호화 제어부를 포함할 수 있다.
- [0043] 다른 실시예에 따른, 상기 클러스터링 관리부는, 상기 헤더 노드와 연결된 네트워크에 포함된 복수의 노드들과 베이스 스테이션 간의 거리 및 상기 네트워크에 포함된 복수의 노드들 각각의 에너지를 고려하여 상기 네트워크에 포함된 복수의 노드들 중 클러스터의 헤더 노드로 결정하는 것을 포함할 수 있다.
- [0044] 또 다른 실시예에 따른, 상기 클러스터링 관리부는, 상기 헤더 노드와 상기 베이스 스테이션 간의 거리, 상기 헤더 노드의 에너지값, 및 상기 헤더 노드가 클러스터의 헤더 노드가 될 확률을 이용하여 제1 임계값을 계산하

고, 상기 제1 임계값과 상기 헤더 노드가 선택한 랜덤값을 비교하여, 상기 헤더 노드가 선택한 랜덤값이 상기 제1 임계값보다 작으면, 상기 노드를 헤더 노드로 결정하는 것을 포함할 수 있다.

[0045] 또 다른 실시예에 따른, 상기 에너지값은, 상기 헤더 노드의 현재 보유 에너지 및 상기 헤더 노드의 최대 보유 에너지를 포함할 수 있다.

[0046] 일 실시예에 따른, 데이터 암호화 전송 방법을 실행하기 위한 프로그램이 기록된 컴퓨터에서 판독 가능한 기록 매체를 포함할 수 있다.

발명의 효과

[0047] 본 발명은, 위치를 기반으로 해서 거리를 측정 후 가까운 미터기로의 경로 설정을 할 수 있다. 그러므로, 본 발명은, 미터기들간 데이터 전송의 효율성을 높일 수 있는 효과가 있다.

[0048] 본 발명은, 헤더들 간의 전송 거리가 줄어들 수 있다. 그러므로, 본 발명은, 데이터의 소실율이나 에러율이 적게 되고, 전송 및 수신 시 클러스터 헤더들이 사용하는 에너지도 감소하는 효과가 있다.

[0049] 본 발명은, 클러스터 헤더 노드들 간의 경로 설정도, 베이스 스테이션들과 이웃 클러스터 헤더 노드들과의 거리를 고려해서 전송 경로를 설정할 수 있다. 그러므로, 본 발명은, 데이터 전송 에러율이나 재전송률을 줄이는 효과가 있다.

[0050] 본 발명은, 안전한 데이터 전송을 제공하며, 스마트 미터기들이 사용하는 에너지를 절감한다는 효과가 있다.

도면의 간단한 설명

[0051] 도 1은 일실시예에 따른 데이터 전송을 위한 클러스터링 방법의 흐름을 나타내는 것이다.

도 2는 일실시예에 따른 노드 전송 구조를 나타내는 것이다.

도 3은 일실시예에 따른 노드 전송 경로를 나타내는 흐름도이다.

도 4는 일실시예에 따른 노드 동기화를 나타내는 것이다.

도 5는 일실시예에 따른 스마트 홈 네트워크 구조를 나타내는 것이다.

도 6은 일실시예에 따른 데이터 전송을 위한 클러스터링 방법을 시뮬레이션한 결과를 나타내는 것이다.

도 7은 일실시예에 따른 데이터 전송을 위한 클러스터 제어 서버로서, 클러스터 제어 서버를 나타내는 블록도이다.

도 8은 일실시예에 따른 데이터 퓨전 전송 방법의 흐름을 나타내는 것이다.

도 9는 일실시예에 따른 시간적 연관성에 의한 데이터 퓨전 전송 방법을 나타내는 것이다.

도 10은 일실시예에 따른 공간적 연관성에 의한 데이터 퓨전 전송 방법을 나타내는 것이다.

도 11은 일실시예에 따라서 시간 및 공간적 연관성에 의한 데이터 퓨전 전송 방법의 시뮬레이션 결과를 나타내는 것이다.

도 12는 일실시예에 따른 수신 모드에서 임계값에 따른 소모 에너지 변화를 나타내는 것이다.

도 13은 일실시예에 따른 데이터 퓨전 전송 노드를 나타내는 블록도이다.

도 14는 일실시예에 따른 데이터 암호화 전송 방법의 흐름을 나타내는 것이다.

도 15는 일실시예에 따른 키 생성 과정을 나타내는 것이다.

도 16a는 일실시예에 따른 데이터 암호화 전송 방법을 시뮬레이션할 경우, 전송시 에너지 소모량을 나타내는 것이다.

도 16b는 일실시예에 따른 데이터 암호화 전송 방법을 시뮬레이션할 경우, 수신시 에너지 소모량을 나타내는 것이다.

도 16c는 일실시예에 따른 데이터 암호화 전송 방법을 시뮬레이션할 경우, 남은 배터리 용량을 나타내는 것이다.

도 17은 일실시예에 따른 데이터 암호화 전송 노드를 나타내는 블록도이다.

발명을 실시하기 위한 구체적인 내용

- [0052] 이하, 본 발명의 실시예를 첨부된 도면을 참조하여 상세하게 설명한다. 본 발명은, 네트워크 상의 노드를 이용한 기술로서, 상기 노드는 컴퓨팅 기기일 수도 있으며, 스마트 미터기일 수도 있으며, 네트워크 기기일 수도 있다.
- [0053] 본 발명의 이해를 위하여, 상기 노드를 전력 미터기 관련 기술로 설명하였으나, 이에 한정된 것은 아니다.
- [0054] 도 1은 일실시예에 따른 데이터 전송을 위한 클러스터링 방법의 흐름을 나타내는 것이다.
- [0055] 단계(S101)에서, 클러스터 제어 서버가, 네트워크에 포함된 복수의 노드들과 베이스 스테이션 간의 거리 및 복수의 노드들 각각의 에너지를 고려하여 복수의 노드들 중 클러스터의 헤더 노드를 결정할 수 있다. 이때, 클러스터 제어 서버는 네트워크에 포함된 노드들 중 하나일 수도 있으며, 베이스 스테이션일 수도 있으나, 이에 한정되는 것은 아니며, 외부에서 상기 네트워크에 연결된 서버일 수도 있다.
- [0056] 구체적으로, 클러스터 제어 서버는, 노드와 베이스 스테이션 간의 거리, 노드의 에너지값, 및 노드가 헤더 노드가 될 확률을 이용하여 제1 임계값을 계산할 수 있다. 또한, 클러스터 제어 서버는, 제1 임계값과 노드가 선택한 랜덤값을 비교하여 헤더 노드를 결정할 수 있다.
- [0057] 예를 들어, 클러스터 제어 서버는, 노드가 선택한 랜덤값이 제1 임계값보다 작으면, 노드를 헤더 노드로 결정할 수 있다. 물론, 에너지값은, 노드의 현재 보유 에너지 및 클러스터의 노드의 최대 보유 에너지일 수 있다.
- [0058] 또한, 클러스터 제어 서버는, 결정한 헤더 노드의 현재 보유 에너지 및 최대 보유 에너지의 비가 기설정된 제2 임계값보다 작을 경우, 헤더 노드를 다시 결정할 수도 있다.
- [0059] 다음으로, 클러스터 제어 서버가, 클러스터의 헤더 노드에 기초하여 네트워크에 포함된 복수의 노드들의 통신 경로를 설정할 수 있으며, 하기와 같다.
- [0060] 단계(S102)에서, 클러스터 제어 서버가, 클러스터의 헤더 노드로부터 네트워크에 포함된 복수의 노드들 중 적어도 하나의 노드로 헤더 노드가 헤더 노드로 설정되었음을 나타내는 메시지를 브로드캐스팅할 수 있다. 물론, 상기 헤더 노드가 메시지를 브로드캐스팅할 수도 있으며, 이때, 클러스터 제어 서버가 브로드캐스팅을 지원할 수도 있다.
- [0061] 단계(S103)에서, 클러스터 제어 서버가, 메시지를 수신한 노드들을, 클러스터 헤더 노드의 멤버 노드로 확정할 수 있다.
- [0062] 단계(S104)에서, 클러스터 제어 서버가, 헤더 노드와 멤버 노드들 간의 거리에 기초하여, 헤더 노드를 중심으로 한 트리 형태의 통신 경로를 설정할 수 있다.
- [0063] 경우에 따라서, 수신한 노드들이 메시지를 복수로 획득할 수 있다. 이 경우에, 클러스터 제어 서버는, 메시지 획득시 신호 세기 및 상기 수신한 노드부터 상기 헤더 노드까지의 거리를 이용하여, 상기 수신한 노드의 헤더 노드를 확정할 수 있다. 또한, 클러스터 제어 서버는, 헤더 노드를 중심으로 한 트리 형태의 통신 경로를 설정할 수 있다.
- [0064] 단계(S105)에서, 클러스터 제어 서버는, 설정된 통신 경로를 이용하여, 클러스터의 노드가 클러스터의 다른 노드로 데이터를 전송하는 것을 지원할 수도 있다.
- [0065] 구체적으로, 클러스터 제어 서버는, 기설정된 스케줄을 기초로 하여, 브로드캐스팅하여 데이터를 전송하는 것을 지원할 수 있다. 또한, 클러스터 제어 서버는, 데이터로서 에너지 사용 정보를 노드가 선택된 헤더 노드로 전송할 수 있다.
- [0066] 도 2는 일실시예에 따른 노드 전송 구조를 나타내는 것이다.
- [0067] 먼저, 도 2를 참조하면, 클러스터(210, 220, 230, 240) 내의 멤버 노드들의 전송 효율성을 위해 클러스터 헤더(211, 221, 231, 241)로의 데이터 전송 경로를 트리 형태로 구성하여, 한 홉 이상을 거쳐 전송되도록 구성할 수 있다. 이때, 클러스터 헤더와의 거리를 계산해서 위치에 기반한 트리 구성을 할 수 있다.
- [0068] 노드 i 와 노드 j , 상기 노드 I 및 노드 j 의 클러스터 헤더 노드 H 가 있을 때, $d(i, H)$ 는 노드 i 에서 클러스터 헤더 H 까지의 거리라고 가정하면, $d(i, H) > d(j, H)$ 이고 $d(i, H) > d(i, j)$ 이면 노드 i 는 노드 j 에게 전송

하도록 구성할 수 있다.

- [0069] 물론, 거리가 비슷한 경우에는 신호세기를 비교하여 신호세기가 더 큰 헤더 노드를 상기 노드의 헤더 노드로 결정할 수 있다.
- [0070] 가령, 거리가 비슷하거나 거리가 가깝더라도 각 가정이나 건물에 설치된 스마트 미터기들은 여러 장애요소들에 의해 통신이 원활하게 이루어지지 않는 경우도 발생할 수 있다.
- [0071] 이런 경우에도, CTP(Collection Tree Protocol)에서 제안한 방식을 이용해 최적의 노드 전송 경로를 선정할 수 있다. CTP는 센서 네트워크에서의 라우팅 프로토콜로 데이터를 주고받고자 하는 두 노드들이 예상 전송수(expected transmission count; ETX)를 라우팅 측정 기준으로 사용해서 더 적은 값을 가지는 노드를 경로로 설정하는 방식이다.
- [0072] 예를 들어서, 헤더 노드들(211, 221, 231, 241)은 자신이 트리의 루트가 되어서 광고 메시지를 보내고 이 메시지를 받은 인근에 위치한 각 노드들은 응답 메시지를 보내는데, 가장 근접한 트리 루트로의 작은 ETX 값만 유지할 수 있다.
- [0073] 또한, 클러스터 헤더들(211, 221, 231, 241) 간의 전송 경로 설정 시에도 거리가 비슷한 경우엔 신호 세기를 비교해서 더 큰 클러스터 헤더 노드 쪽으로 결정할 수 있다. 클러스터 헤더들 사이에서도 건물이나 다른 장애요소들이 있을 수 있으므로 CTP를 이용해 최적의 전송 경로를 설정할 수 있다.
- [0074] 가령, 베이스 스테이션(201)으로부터 멀리 위치한 클러스터 헤더들(221,231)이 베이스 스테이션으로 직접 전송하는 것이 아니라, 근거리의 클러스터 헤더(211)로 전송을 할 수 있다.
- [0075] 전송 받은 이웃 클러스터 헤더(211)가 자신의 정보와 함께 전송해 줌으로써 한 홉이 아닌 트리 구성에 의하여 여러 홉을 거쳐서 전송할 수 있다. 이러한 전송 경로 설정을 통해 전송 효율성과 안전성 및 에너지 절약의 효과를 볼 수 있다.
- [0076] 도 3은 일실시예에 따른 노드 전송 경로를 나타내는 것이다.
- [0077] 도 3을 참조하면, 클러스터(300) 설정이 모두 완료되면, 클러스터 제어 서버(미도시) 및 클러스터 헤더(310)가 보낸 스케줄링에 따라서 데이터 전송을 시작할 수 있다.
- [0078] 예를 들면, 전력 사용량을 전송하는 전송 주기가 한 시간마다 전송하도록 스케줄링 되어 있다면, 클러스터 내 전송 경로 트리의 리프에 해당하는 노드들(321, 331, 332, 333, 334, 335)부터 한 시간이 되면 데이터를 전송할 수 있다.
- [0079] 이때, 리프 노드들의 한단계 상위 부모 노드들(322, 323)은 이를 전송 받아 데이터 퓨전을 하여 생성된 데이터를 전송해서 루트 노드인 클러스터 헤더 노드(310)까지 전송되도록 할 수 있다. 물론, 여러 단계를 거쳐서 상위 부모 노드가 있을 수도 있다.
- [0080] 클러스터 헤더 노드들(310)의 전송 경로 트리의 리프에 해당하는 노드는 상기와 동일하게 퓨전 데이터들이 도착하면, 한 단계 상위 부모 헤더 노드로 퓨전 데이터를 전송할 수 있다.
- [0081] 또한 상기 퓨전 데이터를 전송 받은 부모 헤더 노드들은, 이 정보를 자신의 퓨전 데이터와 함께 다시 상위 부모 헤더 노드로 전송하고, 베이스 스테이션까지 모든 헤더 노드들의 퓨전 데이터가 전달되도록 할 수도 있다.
- [0082] 도 4는 일실시예에 따른 노드 동기화를 나타내는 것이다.
- [0083] 도 4를 참조하면, 노드 간의 동기화를 위해 사용한 기법(400)을 토대로 시간 및 공간 연관성을 고려한 데이터 퓨전 간의 동기화를 진행할 수 있다.
- [0084] 각 클러스터 생성 주기마다 생성된 클러스터의 내부 전송 경로의 트리 깊이(depth)만큼 타임 슬롯을 생성하고, 정해진 전송 주기가 되면, 최하위 리프 노드들부터 수면 상태에서 깨어나서 데이터를 전송할 수 있다.
- [0085] 이때, 그 상위 노드는 리스닝하며 대기하고, 그 위 클러스터 헤더 노드까지의 조상 노드들은 수면 상태를 유지할 수 있다.
- [0086] 또한, 클러스터 헤더 노드(421)까지 전송이 완료되면, 다음 전송 주기가 될 때까지 모든 노드들은 수면 상태로 될 수 있다.
- [0087] 예를 들어, 정해진 전송 주기가 한 시간인 경우, 한 시간마다 첫 번째 슬롯에서 노드 E(425), 노드 F(426)는 데

이터를 전송하기 위해 깨어나서 데이터 전송 여부를 결정한 후 데이터를 전송해야 하는 경우이면 데이터를 전송할 수 있다.

[0088] 이때, 노드 C(423), 노드 D(424)는 데이터를 수신하기 위해 깨어 있으며, 나머지 상위 노드 A(421), 노드 B(422)는 수면 상태를 유지할 수 있다.

[0089] 또한, 두 번째 슬롯에서는 노드 C(423), 노드 D(424)가 데이터를 퓨전하여서 전송하고 노드 B(422)는 깨어 있으며 리스닝 상태를 유지하고 노드 A(421), 노드 E(425), 노드 F(426)는 수면 상태일 수 있다.

[0090] 또한, 그 다음의 세 번째 슬롯에서는 노드 B(422)가 전송 받은 데이터와 자신의 데이터를 퓨전하여서 전송하고, 노드 A(421)는 리스닝 상태에 있으며, 노드 C(423), 노드 D(424), 노드 E(425), 노드 F(426)는 수면 상태를 유지할 수 있다.

[0091] 최대한 노드들의 깨어있는 상태를 줄이고 수면 상태를 늘임으로 인해 노드들의 에너지 사용량을 줄이는 효과를 볼 수 있다.

[0092] 도 5는 일실시예에 따른 스마트 홈 네트워크 구조를 나타내는 것이다.

[0093] 도 5를 참조하면, 데이터 전송을 위한 클러스터링 방법으로 구축된 스마트 홈 네트워크 구조(500)를 알 수 있다.

[0094] 각 가정이나 빌딩, 학교 등 건물에 설치된 스마트 미터기에서 전력 사용량을 주기적으로 클러스터 헤더(531, 532, 533, 534)에게 전송할 수 있다. 또한, 클러스터 헤더(532, 534)는 이를 다시 클러스터 헤더들(533, 531) 간 경로를 거치고 필요한 경우 중간 라우터들(520)을 경유해서 베이스 스테이션(510)으로 전송할 수 있다. 물론, 클러스터는 건물 단위로 될 수도 있으며, 마을 단위로 될 수도 있다.

[0095] 도 6은 일실시예에 따른 데이터 전송을 위한 클러스터링 방법을 시뮬레이션한 결과를 나타내는 것이다.

[0096] 도 6을 참조하면, 데이터 전송을 위한 클러스터링 방법으로 5,000라운드 실행한 결과(600)는, 베이스 스테이션을 중심으로 인근에 위치한 노드들이 먼저 에너지가 고갈되어서 데드 노드가 됨을 알 수 있다.

[0097] 상기에서 언급하였듯이, 클러스터 헤더 노드 결정시, 베이스 스테이션과 가까운 곳에 위치한 노드들이 헤더로 선택될 확률이 높기 때문이다.

[0098] 또한, 클러스터 헤더를 기준으로 클러스터 멤버 노드들은, 클러스터 헤더에서 먼 노드부터 가까운 노드로 트리 구조로 데이터 전송 경로 설정이 될 수 있다. 클러스터 헤더 노드에 가까이 위치한 노드들이 또한 에너지를 더 소모할 수 있기 때문이다.

[0099] 또한, 5,000라운드씩 100회 실행할 경우, 평균적으로, 25노드가 에너지를 다 사용하여 데드 노드가 되고 75노드가 살아있는 노드가 된다. 100회 실행에서 최대 32노드, 최소 17노드가 데드 노드가 된다.

[0100] 5,000라운드 실행 시에도 에너지 사용량이 적으므로, 많은 노드들이 보유 에너지를 가지고 있어 살아 있는 노드 상태가 됨을 알 수 있다.

[0101] 도 7은 일실시예에 따른 데이터 전송을 위한 클러스터 제어 서버로서, 클러스터 제어 서버를 나타내는 블록도이다.

[0102] 먼저, 도 7을 참조하면, 데이터 전송을 위한 클러스터 제어 서버(700)는, 헤더 노드 결정부(710), 통신 경로 설정부(720)로 구성되며, 경우에 따라서, 데이터 전송 지원부(730)등을 더 포함할 수도 있다. 헤더 노드 결정부(710), 통신 경로 설정부(720), 데이터 전송 지원부(730)는 제어 시스템, 프로세서, 센서의 제어 유닛, 메모리, 데이터 송수신기 중 하나를 포함할 수도 있으며, 그 자체가 될 수도 있으나 이에 한정되는 것은 아니다.

[0103] 헤더 노드 결정부(710)는, 네트워크에 포함된 복수의 노드들과 베이스 스테이션 간의 거리 및 복수의 노드들 각각의 에너지를 고려하여 복수의 노드들 중 클러스터의 헤더 노드를 결정할 수 있다.

[0104] 구체적으로, 헤더 노드 결정부(710)는, 노드와 베이스 스테이션 간의 거리, 노드의 에너지값, 및 노드가 헤더 노드가 될 확률을 이용하여 제1 임계값을 계산하고, 제1 임계값과 노드가 선택한 랜덤값을 비교하여 헤더 노드를 결정할 수 있다.

[0105] 예를 들어, 헤더 노드 결정부(710)는, 노드가 선택한 랜덤값이 제1 임계값보다 작으면, 노드를 헤더 노드로 결정할 수 있다. 물론, 에너지값은, 노드의 현재 보유 에너지 및 클러스터의 노드의 최대 보유 에너지일 수 있다.

- [0106] 또한, 헤더 노드 결정부(710)는, 결정한 헤더 노드의 현재 보유 에너지 및 최대 보유 에너지의 비가 기설정된 제2 임계값보다 작을 경우, 헤더 노드를 다시 결정할 수도 있다.
- [0107] 통신 경로 설정부(720)는, 클러스터의 헤더 노드에 기초하여 네트워크에 포함된 복수의 노드들의 통신 경로를 설정할 수 있다.
- [0108] 구체적으로, 통신 경로 설정부(720)는, 클러스터의 헤더 노드로부터 네트워크에 포함된 복수의 노드들 중 적어도 하나의 노드로 헤더 노드가 헤더 노드로 설정되었음을 나타내는 메시지를 브로드캐스팅할 수 있다.
- [0109] 또한, 통신 경로 설정부(720)는, 메시지를 수신한 노드들을, 클러스터 헤더 노드의 멤버 노드로 확정할 수 있다.
- [0110] 또한, 통신 경로 설정부(720)는, 헤더 노드와 멤버 노드들 간의 거리에 기초하여, 헤더 노드를 중심으로 한 트리 형태의 통신 경로를 설정할 수 있다.
- [0111] 예를 들어, 통신 경로 설정부(720)는, 수신한 노드들이 메시지를 복수로 획득한 경우, 메시지 획득시 신호 세기 및 수신한 노드부터 헤더 노드까지의 거리를 이용하여, 수신한 노드의 헤더 노드를 확정할 수 있다. 또한, 통신 경로 설정부(720)는, 헤더 노드를 중심으로 한 트리 형태의 통신 경로를 설정할 수 있다.
- [0112] 데이터 전송 지원부(730)는, 설정된 통신 경로를 이용하여, 클러스터의 노드가 클러스터의 다른 노드로 데이터를 전송하는 것을 지원할 수 있다.
- [0113] 구체적으로, 데이터 전송 지원부(730)는, 기설정된 스케줄을 기초로 하여, 브로드캐스팅하여 데이터를 전송하는 것을 지원할 수 있다. 또한, 데이터 전송 지원부(730)는, 데이터로서 에너지 사용 정보를 노드가 선택된 헤더 노드로 전송하는 것을 지원할 수도 있다.
- [0114] 도 8은 일실시예에 따른 데이터 퓨전 전송 방법의 흐름을 나타내는 것이다.
- [0115] 단계(S801)에서, 제1 노드가, 전송 시점의 제1 노드의 수치 데이터와 제1 노드의 전송 시점의 이전 전송 시점의 수치 데이터의 차를 계산하여 수치 정보를 생성할 수 있다.
- [0116] 단계(S802)에서, 제1 노드가, 제1 노드와 네트워크로 연결된 이웃하는 제2 노드로 수치 정보를 전송할 수 있다.
- [0117] 구체적으로, 기설정된 일정 주기마다 제1 노드가 전송 시점의 제1 노드의 수치 데이터를 제2 노드로 전송할 수 있다. 이때, 제1 노드가 수치 정보를 기설정된 임계값과 비교하여, 수치 정보가 임계값보다 크면, 제2 노드로 수치 정보를 전송할 수 있다. 물론, 수치 데이터는, 제1 노드에서 수치로 측정되거나 입력되는 전력 사용량일 수 있다.
- [0118] 단계(S803)에서, 현재 시점의 제1 노드의 수치 데이터와 제1 노드의 이전 시점의 수치 데이터의 차로 계산된 제1 수치 정보를 제1 노드로부터 제2 노드가 수신할 수 있다. 물론, 수치 데이터는, 제1 노드 및 제2 노드에서 수치로 측정되거나 입력되는 전력 사용량일 수 있다.
- [0119] 단계(S804)에서, 제2 노드가, 현재 시점의 제2 노드의 수치 데이터와 제2 노드의 이전 시점의 수치 데이터의 차로 계산한 수치 정보와 제1 수치 정보를 합산하여 제2 수치 정보를 생성할 수 있다.
- [0120] 단계(S805)에서, 제2 노드가, 제2 노드와 네트워크로 연결된 이웃하는 제3 노드로 제2 수치 정보를 전송할 수 있다. 이때, 제1 노드는 제2 노드와 함께 구성된 트리 구조의 네트워크에서 제2 노드의 자식 노드이고, 제3 노드는 제2 노드의 부모 노드일 수 있다.
- [0121] 또한, 다른 일 실시예에 따라서, 제1 노드가 연결된 네트워크 상에서 클러스터가 구축될 수 있다. 이 때, 제1 노드의 클러스터의 헤더 노드는, 헤더 노드와 연결된 네트워크에 포함된 복수의 노드들과 베이스 스테이션 간의 거리 및 네트워크에 포함된 복수의 노드들 각각의 에너지를 고려하여 클러스터의 헤더 노드로 결정할 수 있다. 또한, 헤더 노드의 클러스터의 멤버 노드인 복수의 노드들의 통신 경로를 설정할 수도 있다.
- [0122] 또한, 일 실시예에 따라서, 헤더 노드가 수행하는 데이터 퓨전 전송 방법은 하기와 같다.
- [0123] 먼저, 헤더 노드는, 데이터 퓨전 전송 노드인 헤더 노드와 연결된 복수의 노드들로부터 수치 정보를 수신할 수 있다. 이때, 헤더 노드는, 기설정된 주기마다 복수의 노드들로부터 수치 정보를 수신할 수 있다.
- [0124] 다음으로, 헤더 노드는, 복수의 노드들로부터 데이터의 합산값을 수신할 수 있다. 이때, 헤더 노드는, 기설정된 제2 임계값과 비교된 데이터가 제2 임계값보다 클 경우, 복수의 노드들로부터 데이터를 수신할 수도 있다.

- [0125] 다음으로, 헤더 노드는, 수치 정보와 데이터의 합산값을 비교할 수 있다. 또한, 노드들에게 데이터의 재전송을 요청할 수도 있다. 물론, 수치 정보와 데이터의 합산값이 일치하지 않으면, 헤더 노드는, 복수의 노드들에게 데이터의 재전송을 요청할 수 있다.
- [0126] 또한, 일 실시예에 따라서, 헤더 노드는, 이전 주기에서 헤더 노드와 연결된 복수의 노드로부터 제1 데이터를 수신할 수 있다. 물론, 제1 노드는 복수의 노드 중 하나의 노드일 수 있다.
- [0127] 다음으로, 헤더 노드는, 현재 주기에서 복수의 노드로부터 제2 데이터를 수신할 수 있다. 구체적으로, 헤더 노드는, 현재 주기에서 기설정된 제2 임계값과 비교하여 제2 데이터가 제2 임계값보다 클 경우, 복수의 노드로부터 제2 데이터를 수신할 수 있다.
- [0128] 다음으로, 헤더 노드는, 제1 데이터와 제2 데이터의 합산한 결과와 다음 주기에서 복수의 노드로부터 수신한 제3 데이터와 비교할 수 있다. 이때, 제1 데이터와 제2 데이터의 합산한 결과와 제3 데이터가 다른 경우, 헤더 노드는, 복수의 노드들에게 데이터의 재전송을 요청할 수도 있다.
- [0129] 도 9는 일 실시예에 따른 시간적 연관성에 의한 데이터 퓨전 전송 방법을 나타내는 것이다.
- [0130] 도 9를 참조하면, 시간적인 연관성을 고려하여 새로운 데이터를 전송시 이전 전송 데이터와 비교해서 정해진 임계값보다 작으면 전송을 하지 않고, 임계값보다 크면, 데이터를 전송할 수 있다. 이에 따라서, 데이터 전송량을 줄이고, 네트워크의 효율성을 향상시킬 수 있다.
- [0131] 전송 횟수를 줄임으로써 사용하는 전기량을 줄이고, 전기 사용량 노출을 최소화함으로써 보안성까지 높일 수 있다. 일반적으로 매15분마다 전송을 하는 경우라면, 이 주기를 길게 해서 예를 들면 한 시간마다 전송할 데이터를 체크하도록 할 수 있다.
- [0132] 노드(910, 920, 930, 940)의 새로 전송할 사용량(V_n), 이전 전송한 사용량 데이터(V_{n-1})의 차가 임계값보다 크면, 이 차이값 $|V_n - V_{n-1}|$ 을 전송할 수 있다.
- [0133] 이때, 시작 시 사용량 데이터를 전송하고, 정해진 주기마다 사용량 데이터를 보낼 수 있다. 물론, 경우에 따라서, 사용량 데이터인 전기량 데이터를 전송하도록 정하는 주기는, 하루 또는 일주일 등으로 정할 수도 있다.
- [0134] 예를 들어, 초기 시작 시점인 0시에는 모든 미터기들이 전력 사용량을 그대로 전송할 수 있다. 또한, 1시에는 각 미터들에서 0시에 전송한 데이터와 값을 비교하여 기설정된 임계값보다 작으면 데이터를 전송하지 않고, 임계치보다 크면 차이값($|V_n - V_{n-1}|$)만 전송할 수 있다.
- [0135] 예를 들어, 임계값이 10이라고 하면, 노드(920)는 1시에 데이터를 전송하지 않고, 다른 노드(930)는 차이값 13을 전송할 수 있다.
- [0136] 도 10은 일 실시예에 따른 공간적 연관성에 의한 데이터 퓨전 전송 방법을 나타내는 것이다.
- [0137] 도 10을 참조하면, 공간적 연관성을 고려한 데이터 전송의 방법을 알 수 있다.
- [0138] 예를 들어, 클러스터 내의 각 미터기는 정해진 전송 경로에 따라 자신의 데이터를 전송 시에 전송 받은 합계값에 자신의 값을 더해서 전송하는 데이터들에 덧붙여서 전송할 수 있다. 이를 전송 받은 클러스터 헤더는 전송 받은 모든 데이터들과 합계값을 비교해서 데이터의 정확성을 검증할 수 있다.
- [0139] 또한, 그룹 2(1031)의 말단(1040)의 스마트 미터기가 1시에 차이값 9와 합계값 9를 전송하고, 이를 수신한 상위(1030) 스마트 미터기가 자신의 차이값 6과 수신한 값 9를 더해서 합계값 15를 부모 노드(1010)로 전송할 수 있다.
- [0140] 또한, 예를 들어, 그룹 1(1021)에 있는 말단(1020) 스마트 미터기가 차이값 7과 합계값 7을 전송할 수 있다. 또한, 상위(1010) 스마트 미터기는, 그룹 2(1031)의 미터기에서 수신한 합계값 15와 그룹 1(1021)의 미터기로부터 수신한 값 7을 더해서 합계값 22를 각 노드(1010, 1020, 1030, 1040)의 미터기들의 전송값과 더불어 부모 노드로 전송할 수 있다.
- [0141] 또한, 클러스터 헤더(미도시)가 모든 데이터를 수신하면, 수신한 차이값들과 수신한 합계값을 비교하여, 전송 받은 데이터의 정확성을 다시 한번 검증할 수 있다.
- [0142] 도 11은 일 실시예에 따라서 시간 및 공간적 연관성에 의한 데이터 퓨전 전송 방법의 시뮬레이션 결과를 나타내

는 것이다.

- [0143] 도 11을 참조하면, 시간 및 공간적 연관성에 의한 데이터 퓨전 전송 방법의 시뮬레이션 결과(1100), 임계값이 증가함에 따라서 전송되는 패킷의 양이 현저히 줄어들고 있음을 알 수 있다.
- [0144] 네트워크 전송량을 줄임으로써 네트워크 효율성을 높이고, 네트워크 전송시 사용되는 에너지의 사용량도 감소한다. 노드가 네트워크 전송시 사용하는 에너지는, 계산 등의 경우에 사용하는 에너지보다 훨씬 더 많이 소모됨을 알 수 있다.
- [0145] 도 12는 일실시예에 따른 수신 모드에서 임계값에 따른 소모 에너지 변화를 나타내는 것이다.
- [0146] 도 12를 참조하면, 수신시 소모 에너지 변화(1200)에서도 전송시와 비슷한 결과를 보임을 알 수 있다. 임계값(t)이 커질수록 전송 횟수가 줄어들기 때문에 수신 모드에서도 사용되는 에너지량은 점점 감소한다.
- [0147] 전송시 및 수신시 모두 사용되는 에너지는 임계치가 커질수록 감소하며, 임계값이 0일 때를 기준으로 대비하여, 그 감소율이 현저히 차이가 생기고, 임계값이 커질수록 사용되는 에너지량이 급격히 감소함을 알 수 있다.
- [0148] 데이터 전송 횟수가 감소함에 따라서, 노드들이 실제로 사용하는 에너지가 줄어드는 것을 시뮬레이션 결과로 확인할 수 있다.
- [0149] 도 13은 일실시예에 따른 데이터 퓨전 전송 노드를 나타내는 블록도이다.
- [0150] 먼저, 도 13을 참조하면, 데이터 퓨전 전송 노드(1300)는, 프로세서(1310), 정보 송수신부(1320)로 구성된다. 데이터 퓨전 전송 노드(1300)는, 센서 네트워크 내의 하나의 센서일 수도 있으며, 스마트 미터기, 컴퓨팅 기기일 수도 있으나, 이에 한정되지는 않는다.
- [0151] 프로세서(1310)는, 데이터 퓨전 전송 노드인 제1 노드의 전송 시점의 수치 데이터와 제1 노드의 전송 시점의 이전 전송 시점의 수치 데이터의 차를 계산하여 수치 정보를 생성할 수 있다.
- [0152] 정보 송수신부(1320)는, 수치 정보를 제1 노드에서 제1 노드와 네트워크로 연결된 이웃하는 제2 노드로 전송할 수 있다.
- [0153] 구체적으로, 정보 송수신부(1320)는, 기설정된 일정 주기마다 제1 노드가 전송 시점의 제1 노드의 수치 데이터를 제2 노드로 전송할 수 있다.
- [0154] 또한, 정보 송수신부(1320)는, 수치 정보를 기설정된 임계값과 비교하여, 수치 정보가 임계값보다 크면, 수치 정보를 전송할 수 있다. 물론, 수치 데이터는, 제1 노드에서 수치로 측정되거나 입력되는 전력 사용량일 수도 있다.
- [0155] 다른 일 실시예에 따르면, 데이터 퓨전 전송 노드(1300)는, 정보 송수신부(1320), 프로세서(1310), 및 제어부(1330, 미도시), 클러스터링 관리부(1340, 미도시)로 구성될 수 있다. 물론, 언급하였듯이, 데이터 퓨전 전송 노드(1300)는, 센서 네트워크 내의 하나의 센서일 수도 있으며, 스마트 미터기, 컴퓨팅 기기일 수도 있으나, 이에 한정되지는 않는다.
- [0156] 정보 송수신부(1320)는, 헤더 노드와 연결된 복수의 노드로부터 이전 주기에서 제1 데이터를 수신하고, 현재 주기에서 복수의 노드로부터 제2 데이터를 수신할 수 있다.
- [0157] 구체적으로, 정보 송수신부(1320)는, 현재 주기에서 기설정된 제2 임계값과 비교하여 제2 데이터가 제2 임계값보다 클 경우, 복수의 노드로부터 제2 데이터를 수신할 수 있다.
- [0158] 프로세서(1310)는, 제1 데이터와 제2 데이터의 합산한 결과와 다음 주기에서 복수의 노드로부터 수신한 제3 데이터와 비교할 수 있다.
- [0159] 제어부(1330, 미도시)는, 제1 데이터와 제2 데이터의 합산한 결과와 제3 데이터가 다른 경우, 복수의 노드들에게 데이터의 재전송을 요청할 수 있다.
- [0160] 클러스터링 관리부(1340, 미도시)는, 헤더 노드와 연결된 네트워크에 포함된 복수의 노드들과 베이스 스테이션 간의 거리 및 네트워크에 포함된 복수의 노드들 각각의 에너지를 고려하여, 헤더 노드를 클러스터의 헤더 노드로 결정할 수 있다.
- [0161] 또한, 클러스터링 관리부(1340, 미도시)는, 복수의 노드들의 통신 경로를 설정할 수 있다.

- [0162] 또 다른 일 실시예에 따르면, 데이터 퓨전 전송 노드(1300)는, 정보 송수신부(1320), 합산값 수신부(미도시), 데이터 비교부(미도시), 제어부(미도시), 클러스터링 관리부(1340, 미도시)로 구성될 수도 있다.
- [0163] 정보 송수신부(1320)는, 데이터 퓨전 전송 노드인 헤더 노드와 연결된 복수의 노드들로부터 수치 정보를 수신할 수 있다. 또한, 정보 송수신부(1320)는, 기설정된 주기마다 복수의 노드들로부터 수치 정보를 수신할 수 있다.
- [0164] 합산값 수신부(미도시)는, 복수의 노드들로부터 데이터의 합산값을 수신할 수 있다. 이때, 합산값 수신부(미도시)는, 기설정된 제2 임계값과 비교된 데이터가 제2 임계값보다 클 경우, 복수의 노드들로부터 데이터를 수신할 수 있다.
- [0165] 데이터 비교부(미도시)는, 수치 정보와 데이터의 합산값을 비교할 수 있다.
- [0166] 제어부(미도시)는, 비교 결과에 따라 복수의 노드들에게 데이터의 재전송을 요청할 수 있다. 물론, 제어부(미도시)는, 수치 정보와 데이터의 합산값이 일치하지 않으면, 복수의 노드들에게 데이터의 재전송을 요청할 수 있다.
- [0167] 클러스터링 관리부(1340, 미도시)는, 헤더 노드와 연결된 네트워크에 포함된 복수의 노드들과 베이스 스테이션 간의 거리 및 네트워크에 포함된 복수의 노드들 각각의 에너지를 고려하여, 네트워크에 포함된 복수의 노드들 중 헤더 노드를 클러스터의 헤더 노드로 결정하고, 복수의 노드들의 통신 경로를 설정할 수 있다.
- [0168] 또 다른 일 실시예에 따르면, 데이터 퓨전 전송 노드(1300)는, 정보 송수신부(1320), 프로세서(1310)로 구성될 수 있다. 물론, 언급하였듯이, 데이터 퓨전 전송 노드(1300)는, 센서 네트워크 내의 하나의 센서일 수도 있으며, 스마트 미터기, 컴퓨팅 기기일 수도 있으나, 이에 한정되지는 않는다.
- [0169] 정보 송수신부(1320)는, 현재 시점의 제1 노드의 수치 데이터와 제1 노드의 이전 시점의 수치 데이터의 차로 계산된 제1 수치 정보를 제1 노드로부터 수신할 수 있다. 물론, 수치 데이터는, 제1 노드 및 제2 노드에서 수치로 측정되거나 입력되는 전력 사용량일 수도 있다.
- [0170] 프로세서(1310)는, 데이터 퓨전 전송 노드인 제2 노드의 현재 시점의 수치 데이터와 제2 노드의 이전 시점의 수치 데이터의 차로 계산한 수치 정보와 제1 수치 정보를 합산하여 제2 수치 정보를 생성할 수 있다. 이때, 정보 송수신부(1320)는, 제2 노드와 네트워크로 연결된 이웃하는 제3 노드로 제2 수치 정보를 전송할 수도 있다.
- [0171] 물론, 제1 노드는 제2 노드와 함께 구성된 트리 구조의 네트워크에서 제2 노드의 자식 노드이고, 제3 노드는 제2 노드의 부모 노드일 수 있다.
- [0172] 도 14는 일실시예에 따른 데이터 암호화 전송 방법의 흐름을 나타내는 것이다.
- [0173] 단계(S1401)에서, 제1 노드는, 제1 노드의 공개키 및 제1 노드의 개인키를 생성할 수 있다.
- [0174] 단계(S1402)에서, 제1 노드는, 제1 노드와 제1 노드에 연결된 제2 노드의 클러스터의 헤더 노드로부터 전송 받은 헤더 노드의 공개키와, 제1 노드의 개인키를 이용하여, 생성한 제1 데이터를 제2 노드로 전송할 수 있다. 또한, 제1 노드는, 제1 데이터와 제1 노드의 아이디와 임의의 값인 제1 난스값을 전송할 수 있다.
- [0175] 이때, 제1 데이터는, 헤더 노드의 공개키 및 제1 노드의 개인키를 이용하여 생성한 제1 비밀값과, 제1 비밀값을 이용하여 생성한 제1 서브맥 메시지일 수 있다.
- [0176] 단계(S1403)에서, 제2 노드는, 제1 노드의 개인키와, 제1 노드에 연결된 제2 노드의 클러스터의 헤더 노드의 공개키를 이용하여, 제1 노드에 의하여 생성된 제1 데이터를 제1 노드로부터 수신할 수 있다. 또한, 제2 노드는, 제1 데이터와 제1 노드의 아이디와 임의의 값인 제1 난스값을 수신할 수 있다.
- [0177] 물론, 제1 데이터는, 헤더 노드의 공개키 및 제1 노드의 개인키를 이용하여, 제1 노드에 의하여 생성된 제1 비밀값과, 제1 비밀값을 이용하여 제1 노드에 의하여 생성된 제1 서브맥 메시지일 수 있다.
- [0178] 다음으로, 제2 노드는, 제2 노드의 공개키 및 제2 노드의 개인키를 생성할 수 있다. 물론 단계(S1403) 이전에서, 제2 노드는, 공개키 및 개인키를 생성할 수도 있다.
- [0179] 단계(S1404)에서, 제2 노드는, 제2 노드의 개인키와 헤더 노드의 공개키를 이용하여 생성한, 제2 데이터를 제1 노드로 전송할 수 있다. 또한, 제2 노드는, 제1 데이터와 제2 노드의 개인키를 이용하여 생성한 공유 비밀키로 암호화된 암호문을 제1 노드로 전송할 수 있다.
- [0180] 이때, 제1 데이터를 인증하여 완료되면, 제2 노드는, 제1 데이터와 제2 노드의 개인키를 이용하여 공유 비밀키

를 생성하고, 암호문의 원문 메시지를 공유 비밀키로 암호화하여 암호문을 전송할 수 있다.

- [0181] 또한, 제2 노드는, 제2 데이터와 제2 노드의 아이디와 임의의 값인 제2 난스값을 제1 노드로 전송하고, 제2 데이터로서, 제2 비밀값과 제2 비밀값을 이용하여 생성한 제2 서브맥 메시지를 제1 노드로 전송할 수 있다.
- [0182] 단계(S1405)에서, 제1 노드는, 헤더 노드의 공개키와, 제2 노드에 의하여 생성된 제2 노드의 개인키를 이용하여, 제2 노드에 의하여 생성된 제2 데이터를 제2 노드로부터 수신할 수 있다. 또한, 제1 노드는, 제1 데이터와 제2 노드의 개인키를 이용하여 제2 노드에 의하여 생성된, 공유 비밀키로 암호화된 암호문을 제2 노드로부터 수신할 수 있다.
- [0183] 이때, 제2 데이터를 인증하여 완료되면, 제1노드는, 제2 데이터와 제1 노드의 개인키를 이용하여 공유 비밀키를 생성하고, 암호문을 공유 비밀키로 복호화하여 암호문의 원문 메시지를 획득할 수 있다.
- [0184] 또한, 제1노드는, 제2 데이터와 제2 노드의 아이디와 임의의 값인 제2 난스값을 제2 노드로부터 수신하고, 제2 데이터로서, 제2 비밀값과 제2 비밀값을 이용하여 제2 노드에 의하여 생성된 제2 서브맥 메시지를 제2 노드로부터 수신할 수 있다.
- [0185] 일 실시예에 따라서, 헤더 노드는, 헤더 노드가 헤더 노드와 연결된 네트워크에서 클러스터의 헤더 노드로 결정되고, 클러스터의 복수의 노드들의 통신 경로를 설정하여 클러스터링할 수 있다.
- [0186] 이때, 헤더 노드는, 헤더 노드와 연결된 네트워크에 포함된 복수의 노드들과 베이스 스테이션 간의 거리 및 네트워크에 포함된 복수의 노드들 각각의 에너지를 고려하여 복수의 노드들 중 클러스터의 헤더 노드로 결정할 수 있다.
- [0187] 또한, 헤더 노드는, 헤더 노드와 베이스 스테이션 간의 거리, 헤더 노드의 에너지값, 및 헤더 노드가 클러스터의 헤더 노드가 될 확률을 이용하여 제1 임계값을 계산할 수 있다. 물론, 에너지값은, 헤더 노드의 현재 보유 에너지 및 헤더 노드의 최대 보유 에너지일 수 있다.
- [0188] 또한, 헤더 노드는, 제1 임계값과 헤더 노드가 선택한 랜덤값을 비교하여, 헤더 노드가 선택한 랜덤값이 제1 임계값보다 작으면, 노드를 헤더 노드로 결정할 수 있다.
- [0189] 다음으로, 헤더 노드는, 헤더 노드의 공개키를 클러스터의 멤버 노드들로 전송할 수 있다.
- [0190] 다음으로, 헤더 노드는, 헤더 노드의 공개키와 멤버 노드의 개인키를 이용하여 암호화된 메시지를 멤버 노드들로부터 수신할 수 있다.
- [0191] 이때, 기설정된 조건에 의하여 메시지를 수신하는 시간이 변경되고, 통신 경로가 트리 구조이면, 상위 노드에 의하여 하위 노드의 메시지의 원문 메시지 상의 수치의 합산된 값을 메시지의 복호화로 획득할 수 있다.
- [0192] 또한, 일 실시예에 따른, 헤더 노드가 수행하는 데이터 암호화 전송 방법은 하기와 같다.
- [0193] 먼저, 헤더 노드가 헤더 노드와 연결된 네트워크에서 클러스터의 헤더 노드로 결정되고, 헤더 노드는, 클러스터의 복수의 노드들의 통신 경로를 설정하여 클러스터링 할 수 있다.
- [0194] 다음으로, 헤더 노드는, 헤더 노드의 공개키를 클러스터의 멤버 노드들로 전송할 수 있다.
- [0195] 다음으로, 헤더 노드는, 헤더 노드의 공개키와 멤버 노드의 개인키를 이용하여 암호화된 메시지를 멤버 노드들로부터 수신할 수 있다. 이때, 기설정된 조건에 의하여 암호화된 메시지를 수신하는 시간이 변경되고, 헤더 노드는, 암호화된 메시지를 복호화하여 멤버 노드의 수치 정보를 획득할 수도 있다.
- [0196] 도 15는 일실시예에 따른 키 생성 과정을 나타내는 것이다.
- [0197] 도 15를 참조하면, 전체 시스템(1500)은 제1 노드(1510)와 제2 노드(1020), 및 클러스터의 헤더 노드(미도시)로 구성된다.
- [0198] 클러스터 헤더 노드의 공개키 Y를 받은 제1 노드(1510)와 제2 노드(1020)는 공유하는 공유 비밀키를 생성할 수 있다.
- [0199] 먼저, 제1 노드(1510)는, 자신의 공개키와 개인키를 생성할 수 있다. 또한, 제1 노드(1510)는, 클러스터 헤더 노드의 공개키 Y, 자신의 개인키를 이용하여 제1 비밀값을 계산한 후, 생성한 비밀값을 이용하여 제1 서브맥 메시지를 생성할 수 있다.

- [0200] 다음으로, 제1 노드(1510)는, 제1 노드(1510)에 연결된 제2 노드(1020)로 제1 노드(1510)의 아이디, 제1 비밀값, 제1 난스값, 제1 서버맥 메시지를 전송할 수 있다.
- [0201] 다음으로, 제2 노드(1020)는, 제1 노드(1510)로부터, 제1 노드(1510)의 아이디, 제1 비밀값, 제1 난스값, 제1 서버맥 메시지를 수신할 수 있다. 또한, 제2 노드(1020)는, 자신의 공개키와 개인키를 생성할 수 있다. 물론, 제2 노드(1020)는 자신의 공개키와 개인키를 제1 노드(1510)로부터 데이터를 수신하기 이전에 생성할 수도 있다.
- [0202] 다음으로, 제2 노드(1020)는, 전송 받은 메시지의 무결성과 인증을 하기 위해 제1 서버맥 메시지를 검증할 수 있다.
- [0203] 검증이 완료되면, 제2 노드(1020)는, 제2 비밀값을 계산하고, 제2 비밀값을 이용하여 키 K' 를 생성하고, 해쉬 함수를 이용하여 공유 비밀키 K 를 생성하여, 공유 비밀키를 이용하여서 보낼 메시지 m 을 암호화하여 암호문 C 을 생성할 수 있다.
- [0204] 다음으로, 제2 노드(1020)는, 제1 노드(1510)로 제2 노드(1020)의 아이디, 제2 비밀값, 제2 난스값, 제2 서버맥 메시지, 암호문 C 를 전송할 수 있다.
- [0205] 다음으로, 제1 노드(1510)는, 제2 노드(1020)로부터, 제2 노드(1020)의 아이디, 제2 비밀값, 제2 난스값, 제2 서버맥 메시지, 암호문 C 를 수신할 수 있다.
- [0206] 다음으로, 제1 노드(1510)는, 전송 받은 메시지의 무결성과 인증을 하기 위해 제2 서버맥 메시지를 검증할 수 있다.
- [0207] 검증이 완료되면, 제1 노드(1510)는, 제2 비밀값과 자신의 개인키를 이용하여 키 K' 를 생성하고, 해쉬 함수를 이용하여 공유 비밀키 K 를 생성하여, 공유 비밀키를 이용하여서 암호문 C 를 복호화하여 원문 메시지 m 을 획득할 수 있다. 또한, 수신한 제2 난스값을 확인할 수 있다.
- [0208] 클러스터 내부에 있는 미터기들끼리 공유 비밀키를 각각 만들어서 메시지를 전송할 때 공유 비밀키를 이용해 메시지를 암호화해서 전송함으로써 보안성을 향상시킬 수 있다.
- [0209] 또한, 키 생성을 위해서 주고 받는 메시지의 노출과 공격의 위험성을 방지하고, 탐지하기 위해서 서버맥 메시지를 이용함으로써 전송 메시지의 부하를 줄이고, 보안성은 높이는 효과가 있다.
- [0210] 도 16a는 일실시예에 따른 데이터 암호화 전송 방법을 시뮬레이션할 경우, 전송시 에너지 소모량을 나타내는 것이다.
- [0211] 랙넷 시뮬레이터를 이용해 두 노드간에 키 설정 과정을 통해 비밀키를 생성하는데 소요되는 시간과 각 노드가 사용하는 에너지량을 측정한 결과이다.
- [0212] 시뮬레이션 결과, 키 생성 과정은, 전체 수행 시간이 0.006835861초로 아주 짧은 시간만 소요되며, 다수회 반복 수행도 동일한 결과를 보인다.
- [0213] 새로운 주기마다 클러스터 헤더를 선정하고, 그 다음으로, 클러스터 헤더가 자신의 공개키를 브로드캐스트하고, 두 노드(미터기)가 공유 비밀키를 생성해도, 소요 시간은 1초에 훨씬 못 미치는 시간이 걸린다.
- [0214] 도 16a를 참조하면, 두 노드에서 각각 데이터를 전송 시 사용하는 에너지는 0.038 mWh이다.
- [0215] 도 16b는 일실시예에 따른 데이터 암호화 전송 방법을 시뮬레이션할 경우, 수신시 에너지 소모량을 나타내는 것이다.
- [0216] 도 16b를 참조하면, 데이터 수신시 노드가 사용한 에너지는 0.0034mWh임을 알 수 있다.
- [0217] 예를 들어, 알카라인 배터리 AA를 사용하는 경우와 비교해보면, 알카라인 배터리 AA가 2.8Ahr 이고, 이때 AA 배터리의 공식 전압이 1.5 볼트이므로 전기량은 $2.8Ahr \times 1.5V = 4.2Wh$ 이다.
- [0218] 4.2Wh에 비해서, 노드가 전송시 사용하는 전기량은 0.0009%이고, 노드가 수신시 사용하는 전기량은 0.00008%이다. 아주 적은 양으로도, 한 라운드 실행시 마다 키를 생성하는 경우, 또는 일주일 및 한달 등의 정해진 기간마다 키를 생성하는 경우, 한번씩 소모되는 에너지이므로 더욱 미미할 수 있다.
- [0219] 도 16c는 일실시예에 따른 데이터 암호화 전송 방법을 시뮬레이션할 경우, 남은 배터리 용량을 나타내는

것이다.

- [0220] 도 16c를 참조하면, 예를 들어, 알카라인 배터리 AA를 사용하는 경우에, 제안하는 키 생성 과정을 수행하며 소모한 에너지의 결과를 알 수 있다. 이때, 소모한 에너지는 0.16 mAh이다. 남은 배터리 용량은 거의 2,800 mAh로 거의 전체가 남는다. 물론, 전송시 및 수신시뿐만 아니라 미터기의 키생성을 하는 동안 다른 프로세스도 구동하며 소모한 에너지를 포함한다.
- [0221] 도 17은 일실시예에 따른 데이터 암호화 전송 노드를 나타내는 블록도이다.
- [0222] 먼저, 도 17을 참조하면, 데이터 암호화 전송 노드(1700)는, 프로세서(1710), 데이터 송수신부(1720)로 구성된다. 물론, 언급하였듯이, 데이터 암호화 전송 노드(1700)는, 센서 네트워크 내의 하나의 센서일 수도 있으며, 스마트 미터기, 컴퓨팅 기기일 수도 있으나, 이에 한정되지는 않는다.
- [0223] 프로세서(1710)는, 데이터 암호화 전송 노드인, 제1 노드의 공개키 및 제1 노드의 개인키를 생성할 수 있다. 또한, 프로세서(1710)는, 제1 노드 및 제1 노드에 연결된 제2 노드의 클러스터의 헤더 노드로부터 전송 받은 헤더 노드의 공개키와, 제1 노드의 개인키를 이용하여, 생성한 제1 데이터를 생성할 수 있다.
- [0224] 데이터 송수신부(1720)는, 제1 데이터를 제1노드와 연결된 제2 노드로 전송할 수 있다. 제1 데이터는, 헤더 노드의 공개키 및 제1 노드의 개인키를 이용하여 생성한 제1 비밀값과, 제1 비밀값을 이용하여 생성한 제1 서브맥 메시지일 수 있다.
- [0225] 또한, 데이터 송수신부(1720)는, 제1 데이터와 제1 노드의 아이디와 임의의 값인 제1 난스값을 전송할 수 있다.
- [0226] 또한, 데이터 송수신부(1720)는, 헤더 노드의 공개키와, 제2 노드에 의하여 생성된 제2 노드의 개인키를 이용하여, 제2 노드에 의하여 생성된 제2 데이터를 제2 노드로부터 수신할 수 있다. 또한, 데이터 송수신부(1720)는, 제1 데이터와 제2 노드의 개인키를 이용하여 제2 노드에 의하여 생성된, 공유 비밀키로 암호화된 암호문을 제2 노드로부터 수신할 수 있다.
- [0227] 이때, 프로세서(1710)는, 제2 데이터를 인증하여 완료되면, 제2 데이터와 제1 노드의 개인키를 이용하여 공유 비밀키를 생성하고, 암호문을 공유 비밀키로 복호화하여 암호문의 원문 메시지를 획득할 수 있다.
- [0228] 또한, 데이터 송수신부(1720)는, 제2 데이터와 제2 노드의 아이디와 임의의 값인 제2 난스값을 제2 노드로부터 수신할 수 있다. 또한, 데이터 송수신부(1720)는, 제2 데이터로서, 제2 비밀값과 제2 비밀값을 이용하여 제2 노드에 의하여 생성된 제2 서브맥 메시지를 제2 노드로부터 수신할 수 있다.
- [0229] 일 실시예에 따라서, 데이터 암호화 전송 노드(1700)는, 프로세서(1710), 데이터 송수신부(1720)로 구성된다. 물론, 언급하였듯이, 데이터 암호화 전송 노드(1700)는, 센서 네트워크 내의 하나의 센서일 수도 있으며, 스마트 미터기, 컴퓨팅 기기일 수도 있으나, 이에 한정되지는 않는다.
- [0230] 데이터 송수신부(1720)는, 제1 노드의 개인키와, 제1 노드에 연결된 데이터 암호화 전송 노드인 제2 노드의 클러스터의 헤더 노드의 공개키를 이용하여, 제1 노드에 의하여 생성된 제1 데이터를 제1 노드로부터 수신할 수 있다.
- [0231] 프로세서(1710)는, 데이터 암호화 전송 노드인, 제2 노드의 공개키 및 제2 노드의 개인키를 생성할 수 있다.
- [0232] 또한, 데이터 송수신부(1720)는, 제2 노드의 개인키와 헤더 노드의 공개키를 이용하여 프로세서(1710)가 생성한, 제2 데이터를 제1 노드로 전송할 수 있다. 또한, 데이터 송수신부(1720)는, 제1 데이터와 제2 노드의 개인키를 이용하여 프로세서(1710)가 생성한 공유 비밀키로 암호화된 암호문을 제1 노드로 전송할 수 있다.
- [0233] 물론, 데이터 송수신부(1720)는, 제1 데이터와 제1 노드의 아이디와 임의의 값인 제1 난스값을 수신할 수 있다.
- [0234] 이때, 제1 데이터는, 헤더 노드의 공개키 및 제1 노드의 개인키를 이용하여, 제1 노드에 의하여 생성된 제1 비밀값과, 제1 비밀값을 이용하여 제1 노드에 의하여 생성된 제1 서브맥 메시지일 수 있다.
- [0235] 또한, 프로세서(1710)는, 제1 데이터를 인증하여 완료되면, 제1 데이터와 제2 노드의 개인키를 이용하여 공유 비밀키를 생성하고, 암호문의 원문 메시지를 공유 비밀키로 암호화하고, 데이터 송수신부(1720)는, 암호문을 전송할 수 있다.
- [0236] 또한, 데이터 송수신부(1720)는, 제2 데이터와 제2 노드의 아이디와 임의의 값인 제2 난스값을 제1 노드로 전송할 수 있다. 또한, 데이터 송수신부(1720)는, 제2 데이터로서, 제2 비밀값과 제2 비밀값을 이용하여 프로세서

(1710)가 생성한 제2 서브맥 메시지를 제1 노드로 전송할 수 있다.

- [0237] 일 실시예에 따라서, 데이터 암호화 전송 노드(1700)는, 프로세서(1710), 데이터 송수신부(1720), 클러스터링 관리부(1730, 미도시), 암호화 제어부(1740, 미도시)로 구성된다. 경우에 따라서, 프로세서(1710)은 클러스터링 관리부 또는 암호화 제어부에 포함될 수도 있다. 물론, 언급하였듯이, 데이터 암호화 전송 노드(1700)는, 센서 네트워크 내의 하나의 센서일 수도 있으며, 스마트 미터기, 컴퓨팅 기기일 수도 있으나, 이에 한정되지는 않는다.
- [0238] 클러스터링 관리부(1730, 미도시)는, 데이터 암호화 전송 노드인, 헤더 노드가 헤더 노드와 연결된 네트워크에서 클러스터의 헤더 노드로 결정하고, 클러스터의 복수의 노드들의 통신 경로를 설정하여 클러스터링할 수 있다.
- [0239] 또한, 클러스터링 관리부(1730, 미도시)는, 헤더 노드와 연결된 네트워크에 포함된 복수의 노드들과 베이스 스테이션 간의 거리 및 네트워크에 포함된 복수의 노드들 각각의 에너지를 고려하여 클러스터의 헤더 노드를 결정할 수 있다.
- [0240] 또한, 클러스터링 관리부(1730, 미도시)는, 헤더 노드와 베이스 스테이션 간의 거리, 헤더 노드의 에너지값, 및 헤더 노드가 클러스터의 헤더 노드가 될 확률을 이용하여 제1 임계값을 계산할 수 있다.
- [0241] 이때, 클러스터링 관리부(1730, 미도시)는, 제1 임계값과 헤더 노드가 선택한 랜덤값을 비교하여, 헤더 노드가 선택한 랜덤값이 제1 임계값보다 작으면, 노드를 헤더 노드로 결정할 수 있다.
- [0242] 물론, 에너지값은, 헤더 노드의 현재 보유 에너지 및 헤더 노드의 최대 보유 에너지일 수 있다.
- [0243] 데이터 송수신부(1720)는, 헤더 노드의 공개키를 클러스터의 멤버 노드들로 전송하고, 헤더 노드의 공개키와 멤버 노드의 개인키를 이용하여 암호화된 메시지를 멤버 노드들로부터 수신할 수 있다.
- [0244] 암호화 제어부(1740, 미도시)는, 기설정된 조건에 의하여 메시지를 수신하는 시간이 변경되고, 통신 경로가 트리 구조이면, 상위 노드에 의하여 하위 노드의 메시지의 원문 메시지 상의 수치의 합산된 값을 메시지의 복호화로 획득할 수 있다.
- [0245] 또한, 일 실시예에 따라서, 데이터 암호화 전송 노드(1700)는, 데이터 송수신부(1720), 클러스터링 관리부(1730, 미도시), 암호화 제어부(1740, 미도시)로 구성된다. 또한, 경우에 따라서, 프로세서가 클러스터링 관리부 또는 암호화 제어부에 포함될 수도 있다.
- [0246] 클러스터링 관리부(1730, 미도시)는, 데이터 암호화 전송 노드인, 헤더 노드가 헤더 노드와 연결된 네트워크에서 클러스터의 헤더 노드로 결정하고, 클러스터의 복수의 노드들의 통신 경로를 설정하여 클러스터링할 수 있다.
- [0247] 데이터 송수신부(1720)는, 헤더 노드의 공개키를 클러스터의 멤버 노드들로 전송하고, 헤더 노드의 공개키와 멤버 노드의 개인키를 이용하여 암호화된 메시지를 멤버 노드들로부터 수신할 수 있다.
- [0248] 암호화 제어부(1740, 미도시)는, 기설정된 조건에 의하여 암호화된 메시지를 수신하는 시간이 변경되고, 암호화된 메시지를 복호화하여 멤버 노드의 수치 정보를 획득할 수 있다.
- [0249] 이상에서 설명된 장치는 하드웨어 구성요소, 소프트웨어 구성요소, 및/또는 하드웨어 구성요소 및 소프트웨어 구성요소의 조합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치 및 구성요소는, 예를 들어, 프로세서, 컨트롤러, ALU(arithmetic logic unit), 디지털 신호 프로세서(digital signal processor), 마이크로컴퓨터, FPA(field programmable array), PLU(programmable logic unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수 목적 컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 애플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(processing element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 컨트롤러를 포함할 수 있다. 또한, 병렬 프로세서(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.
- [0250] 소프트웨어는 컴퓨터 프로그램(computer program), 코드(code), 명령(instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나

처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성요소(component), 물리적 장치, 가상 장치(virtual equipment), 컴퓨터 저장 매체 또는 장치, 또는 전송되는 신호 파(signal wave)에 영구적으로, 또는 일시적으로 구체화(embodiment)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.

[0251]

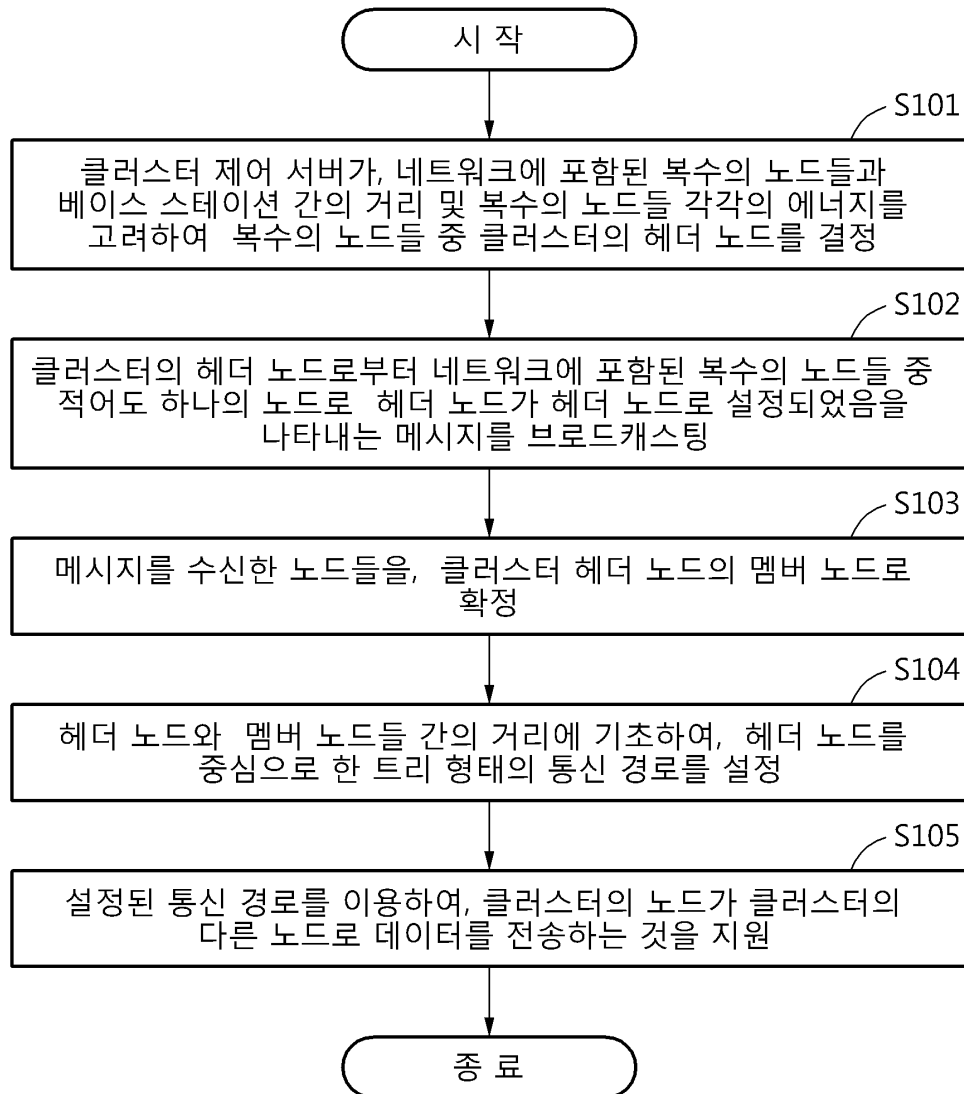
실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 실시예의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0252]

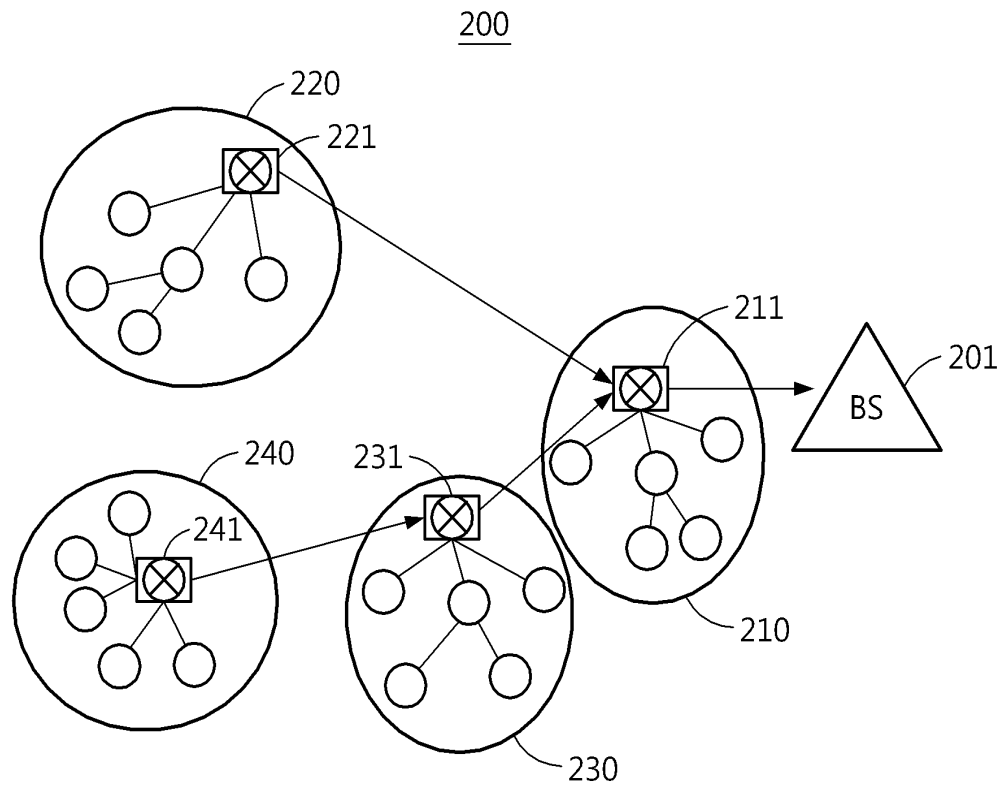
이상과 같이 실시예들이 비록 한정된 실시예와 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기의 기재로부터 다양한 수정 및 변형이 가능하다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다. 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

도면

도면1

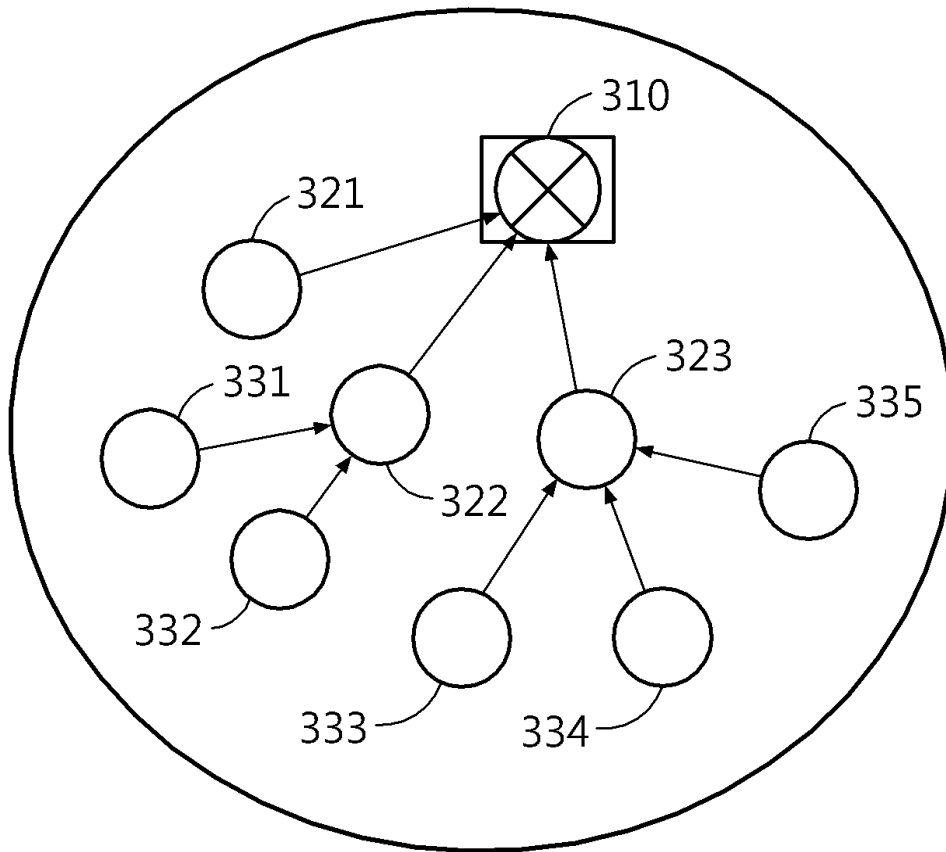


도면2

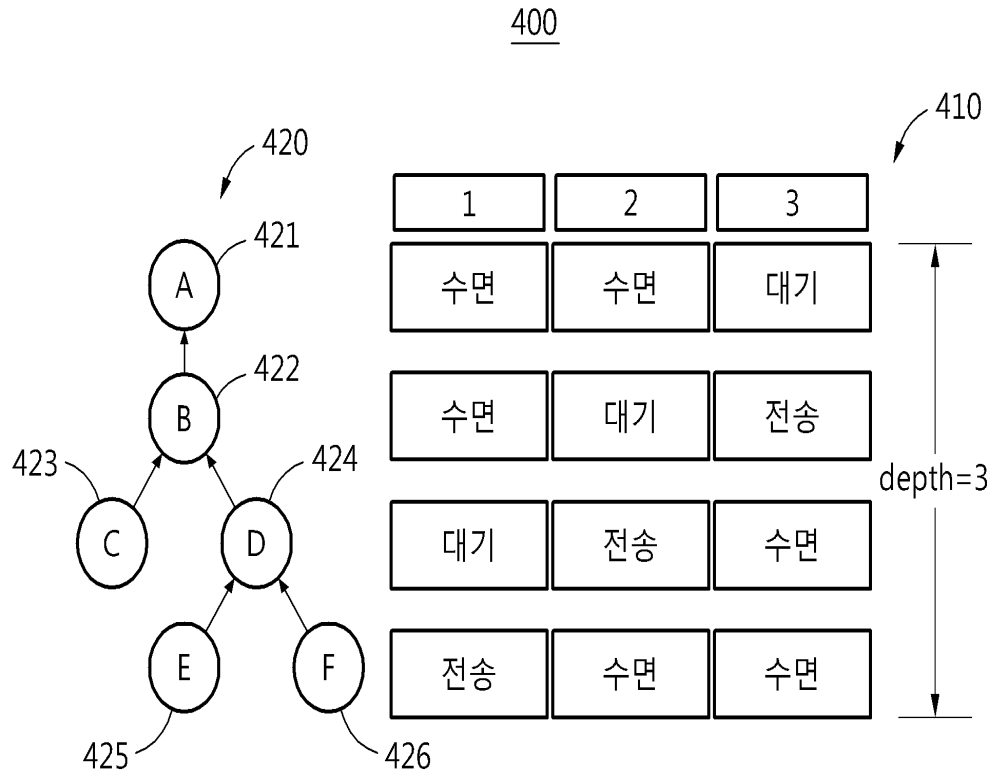


도면3

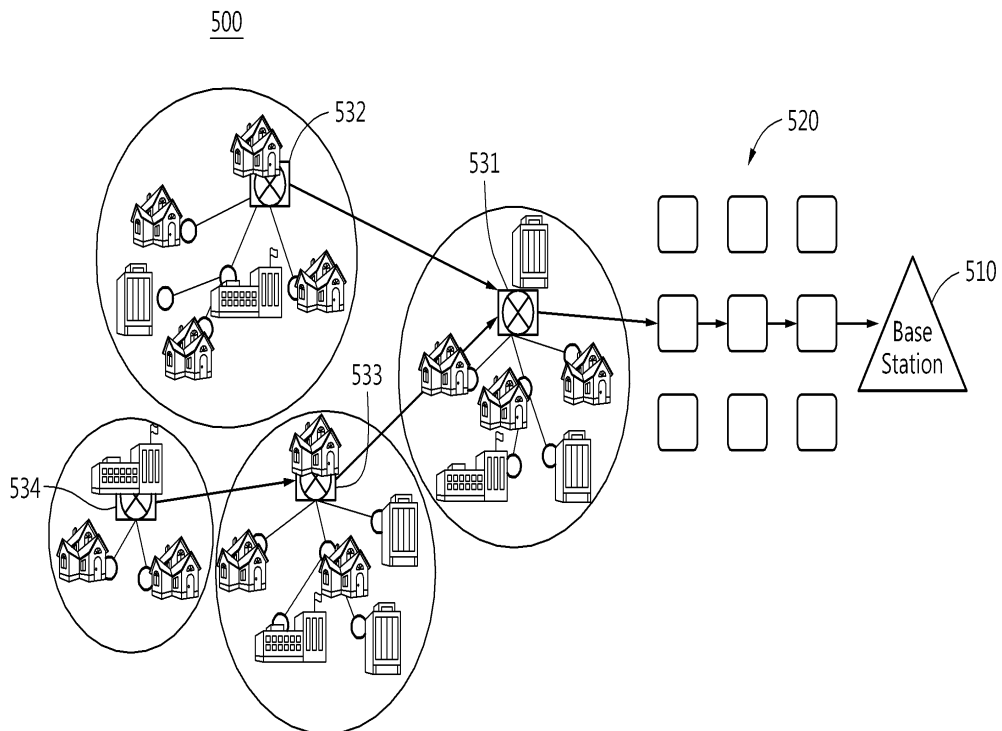
300



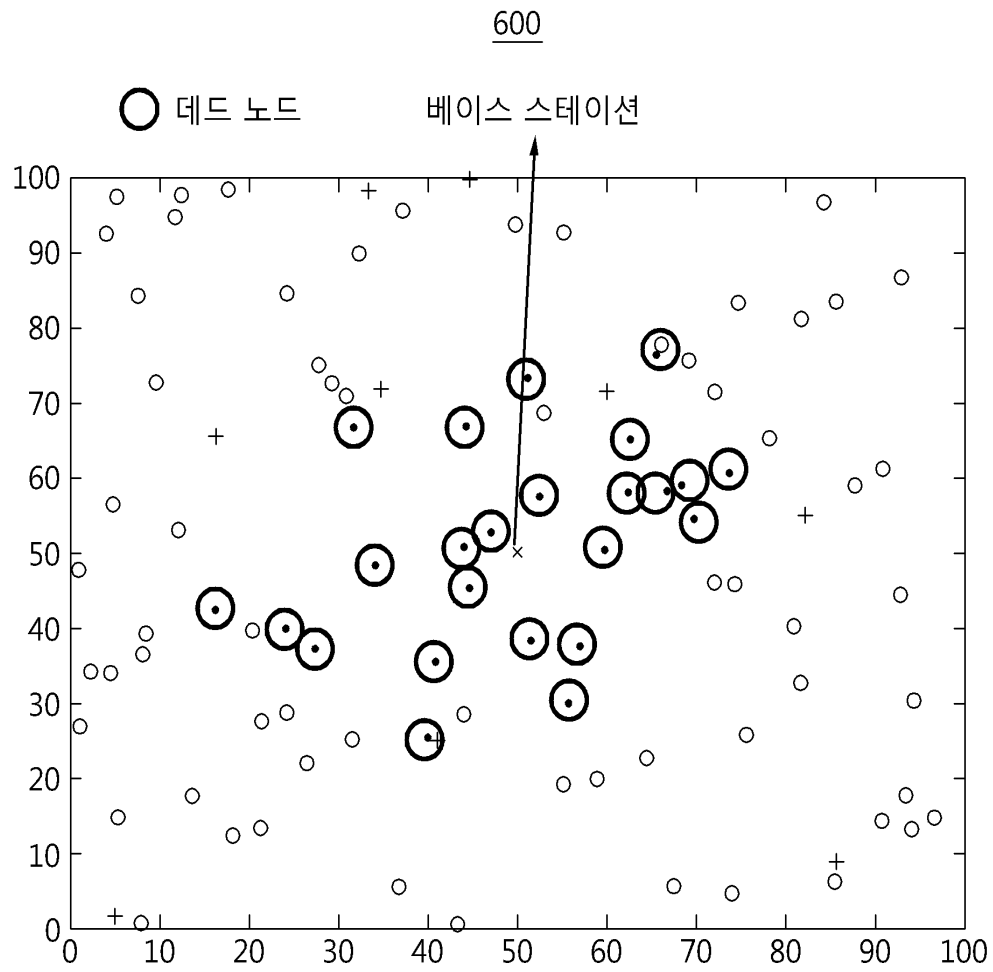
도면4



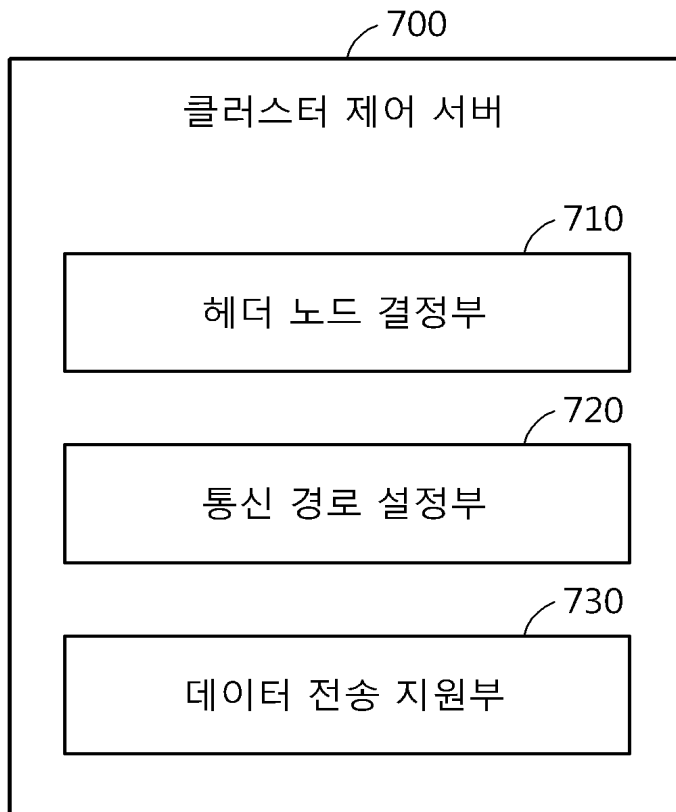
도면5



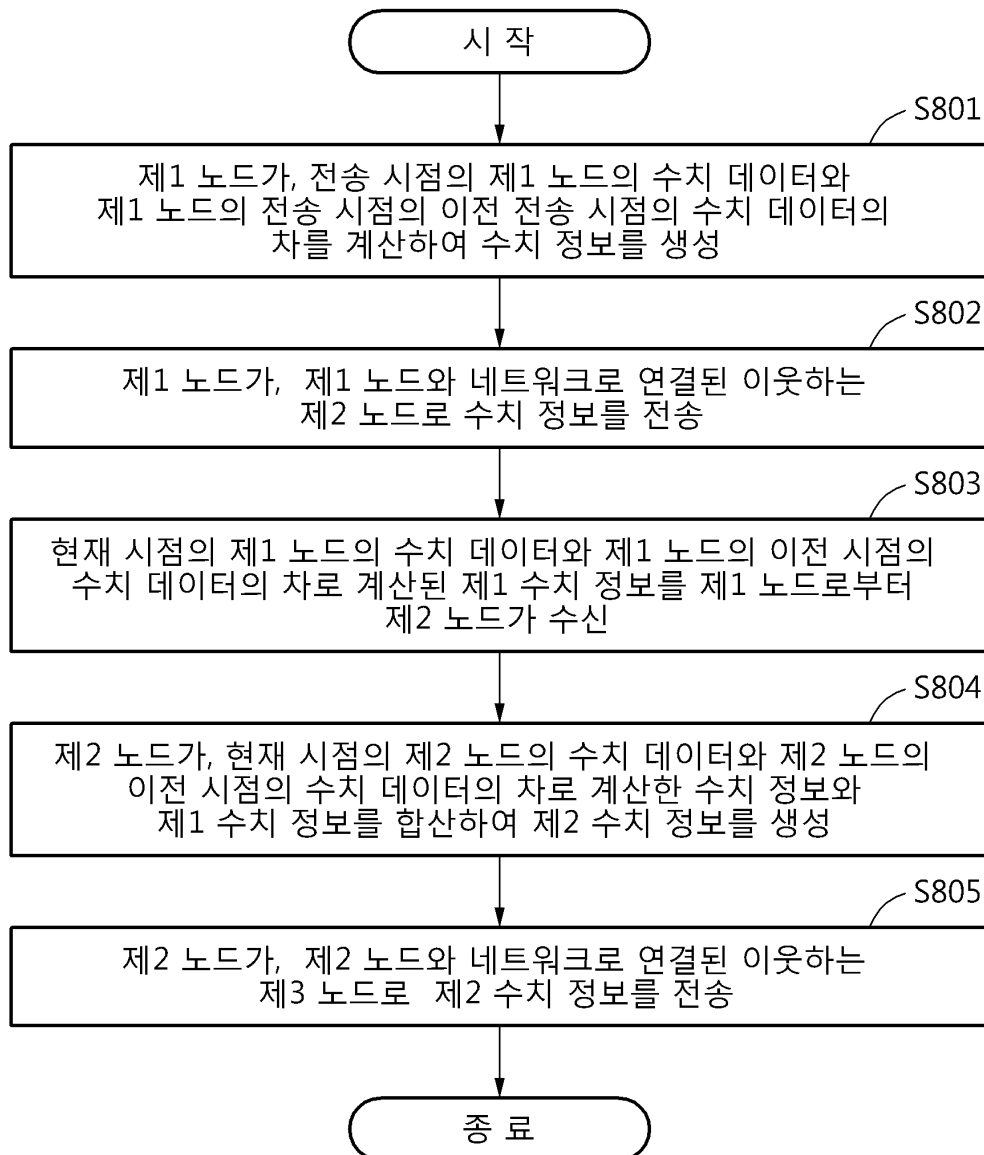
도면6



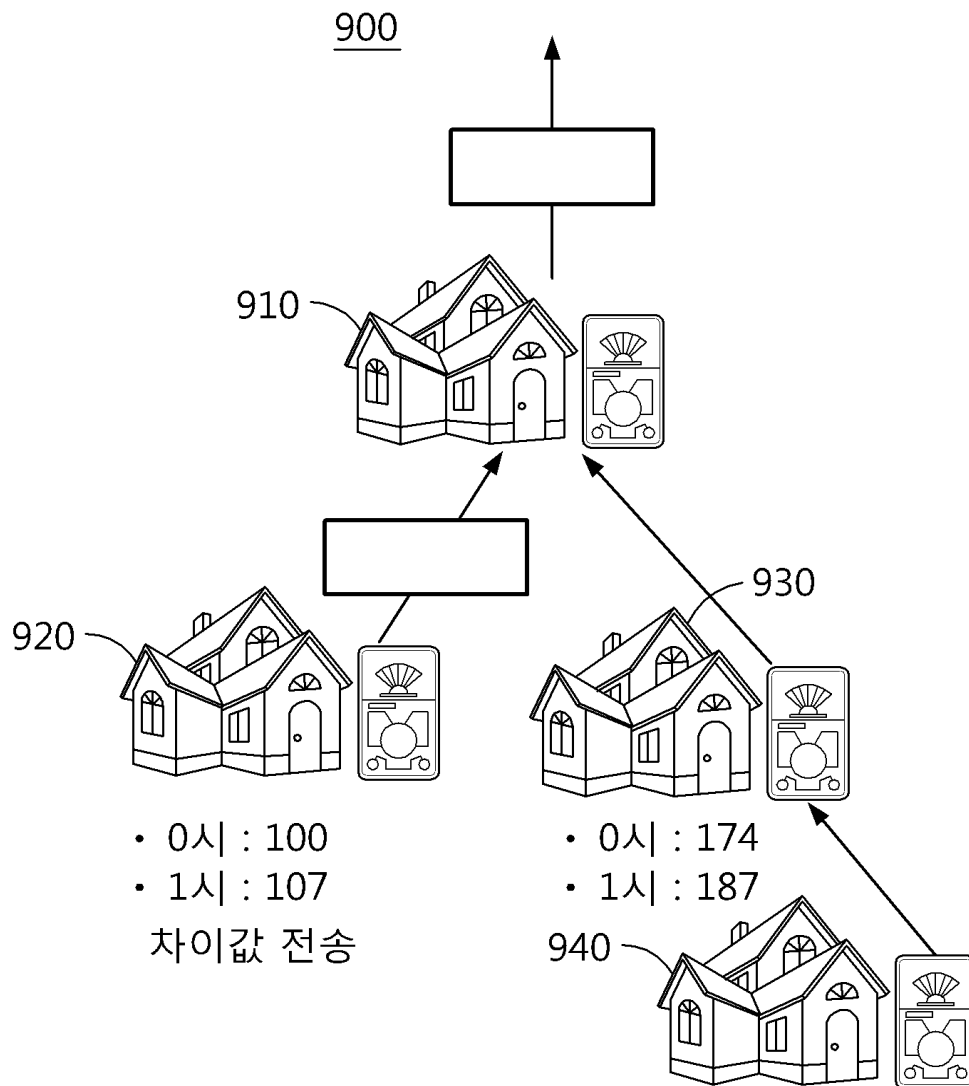
도면7



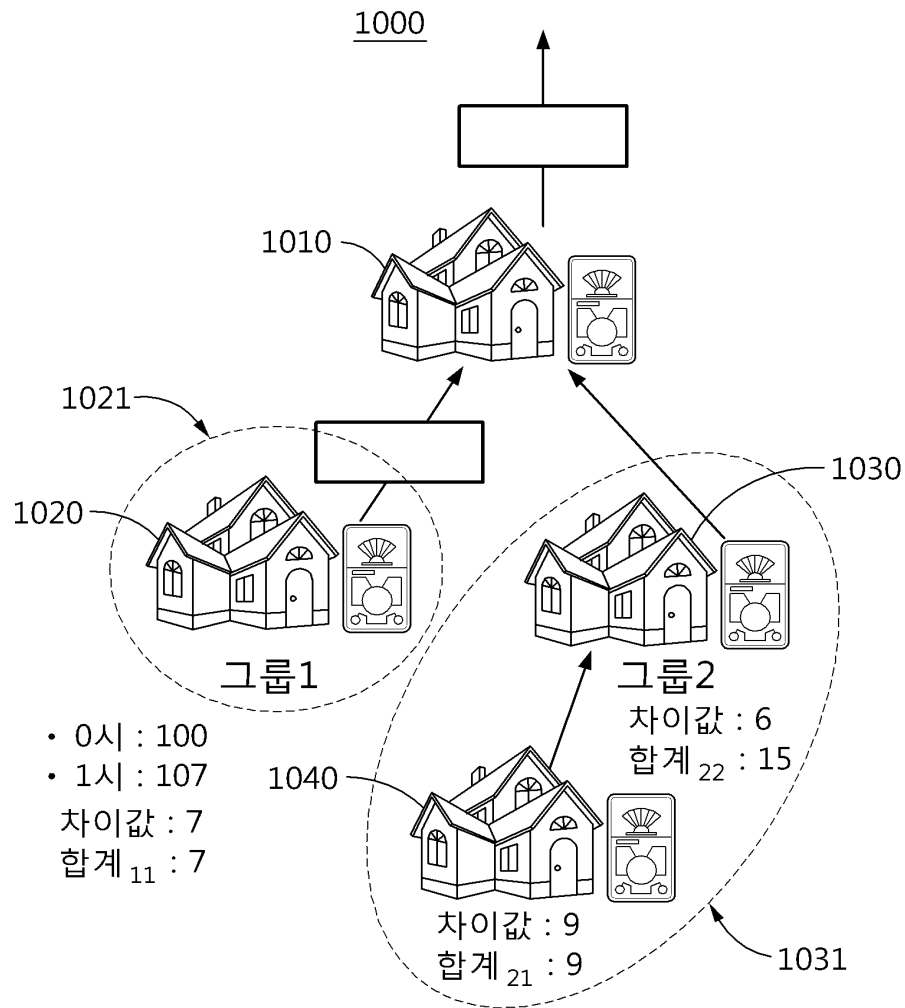
도면8



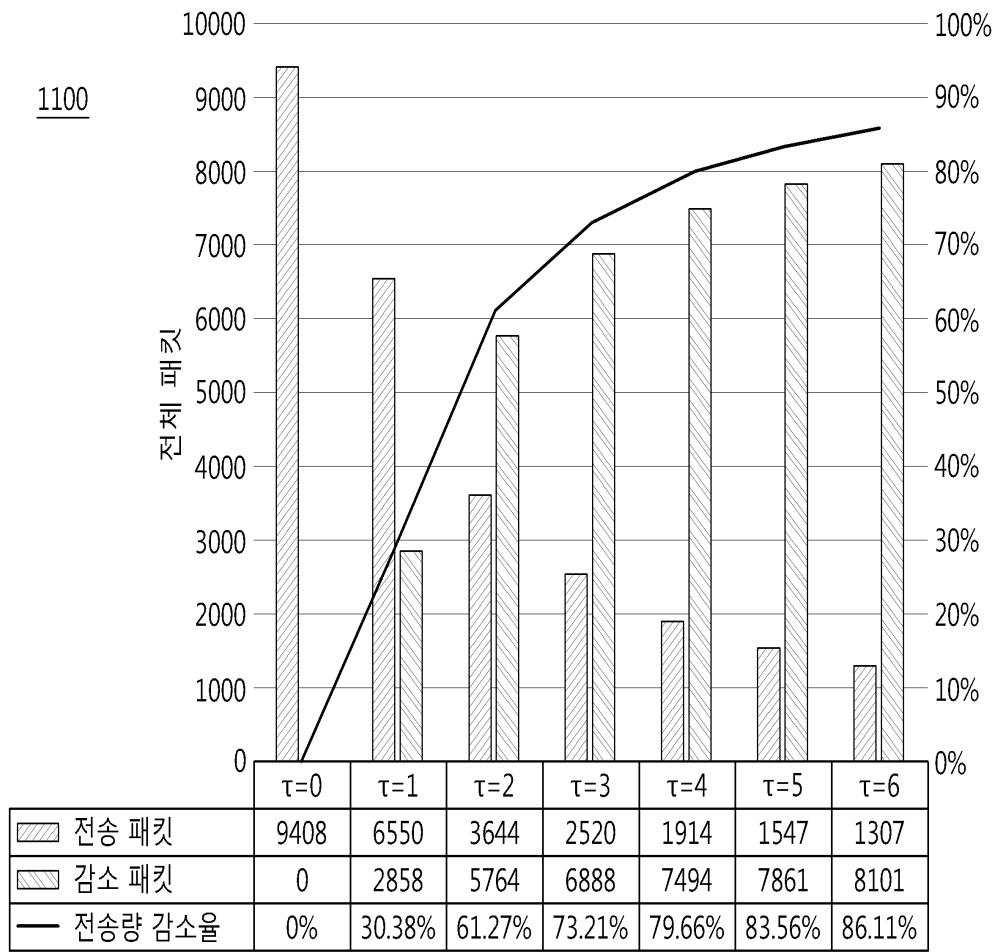
도면9



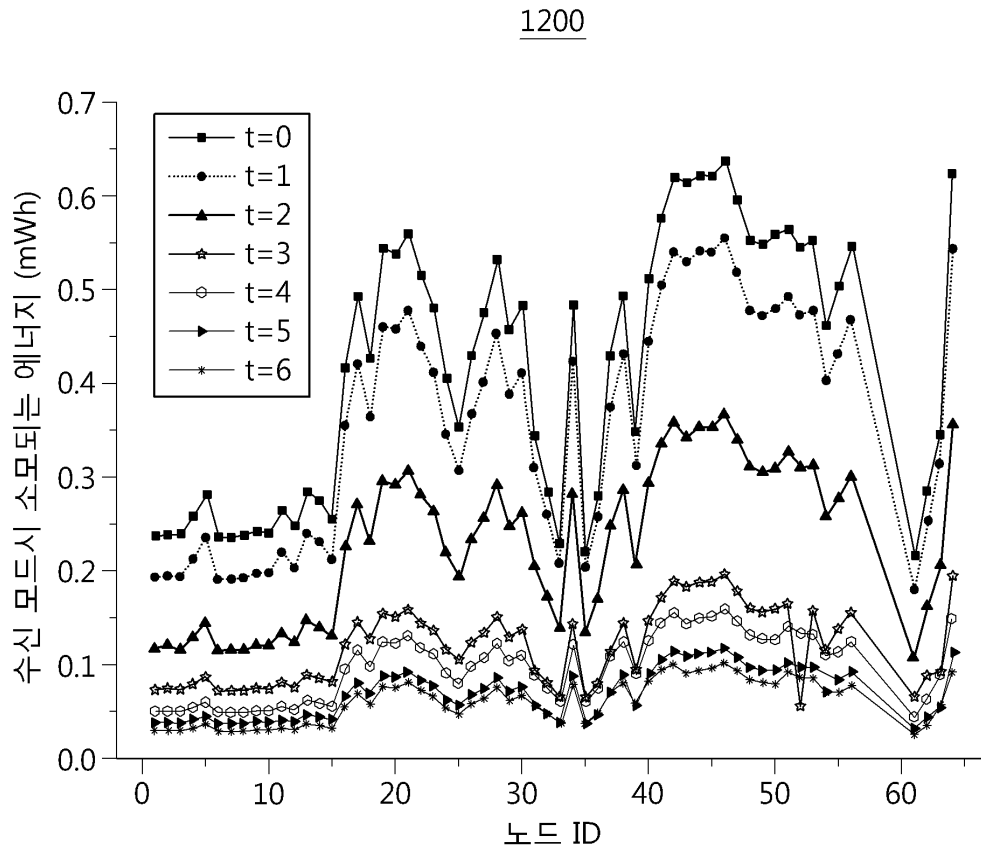
도면10



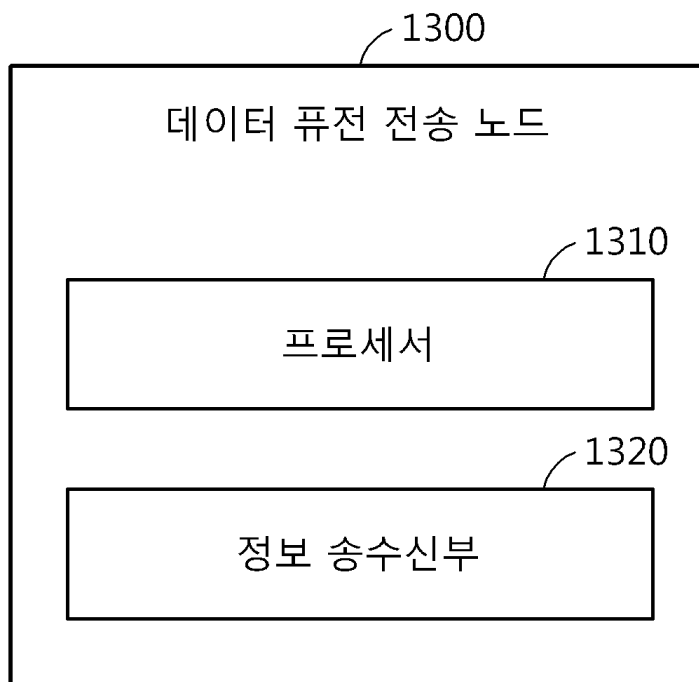
도면11



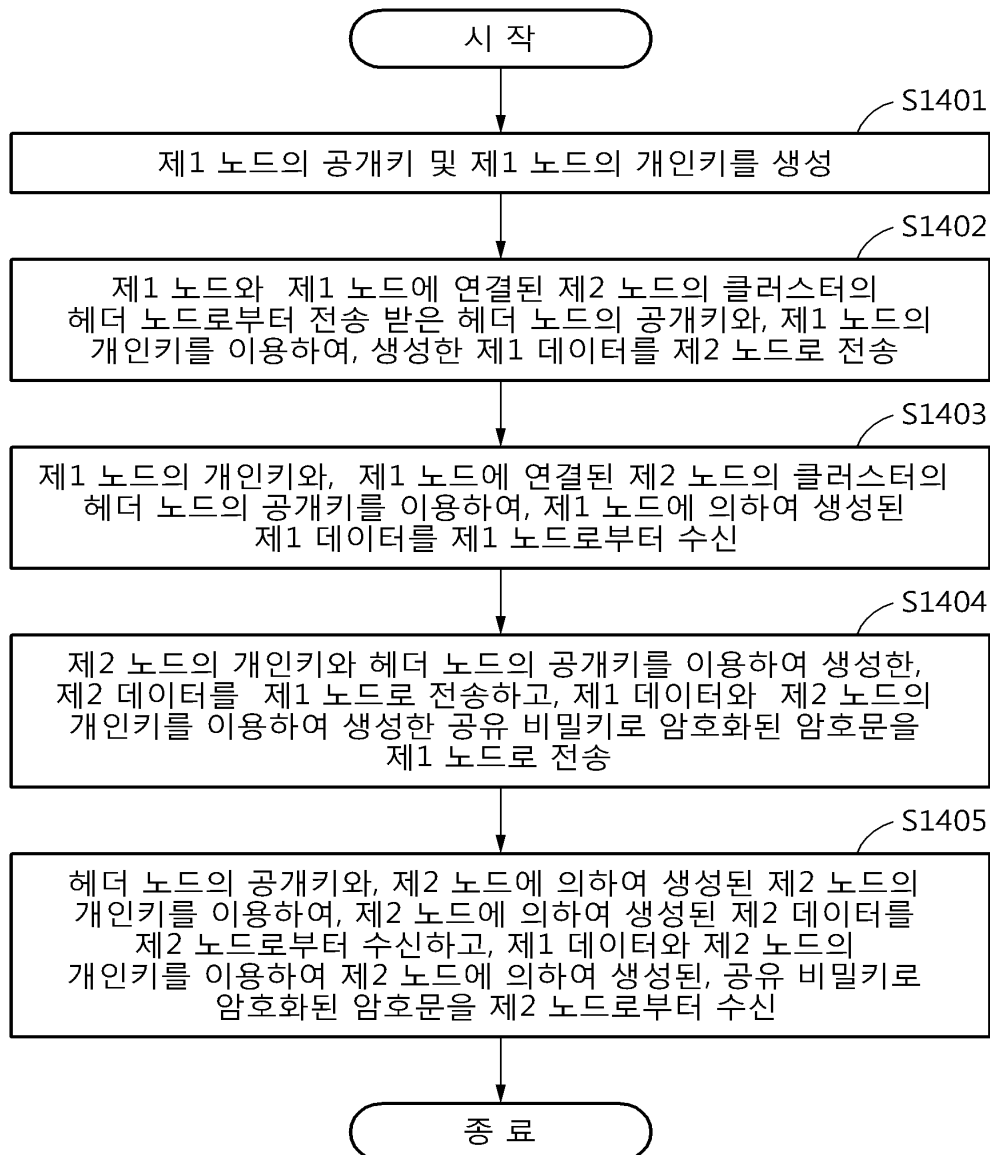
도면12



도면13

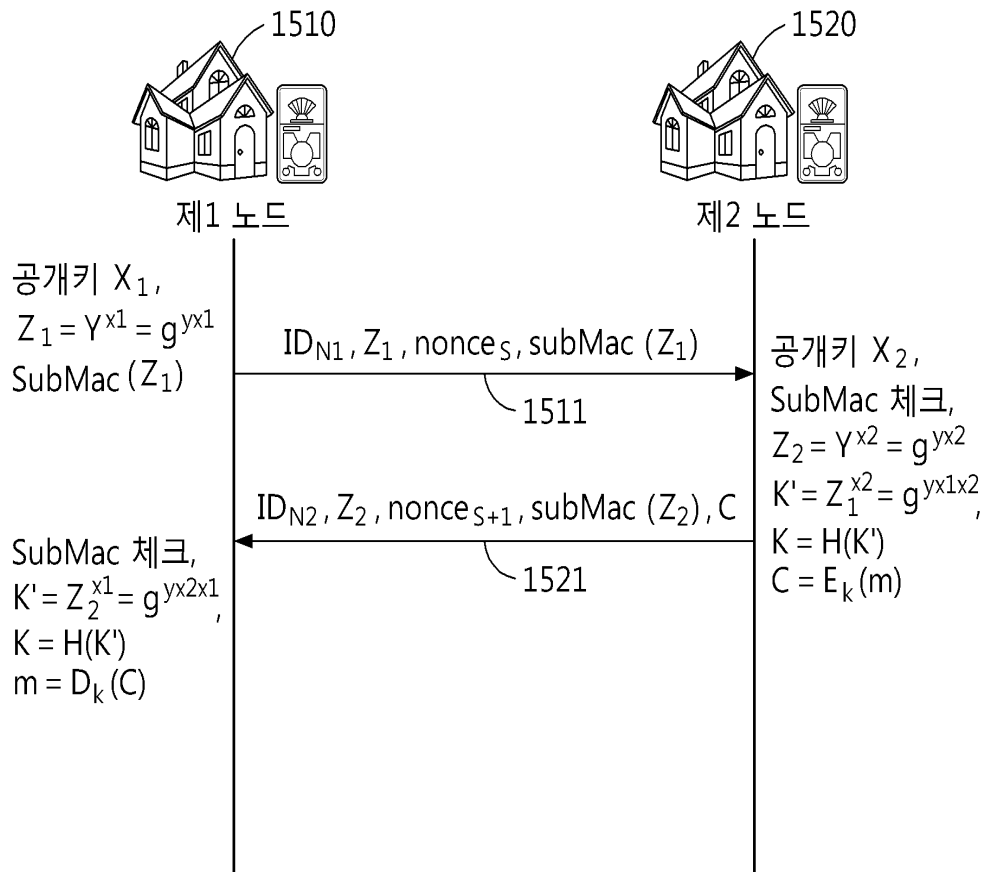


도면14

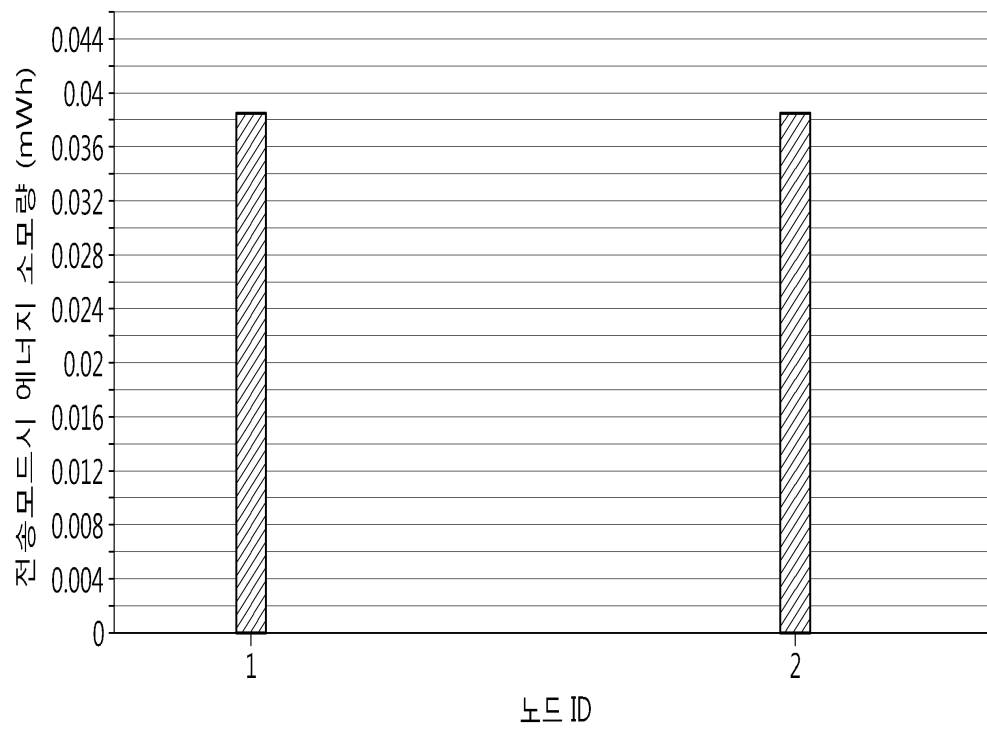


도면15

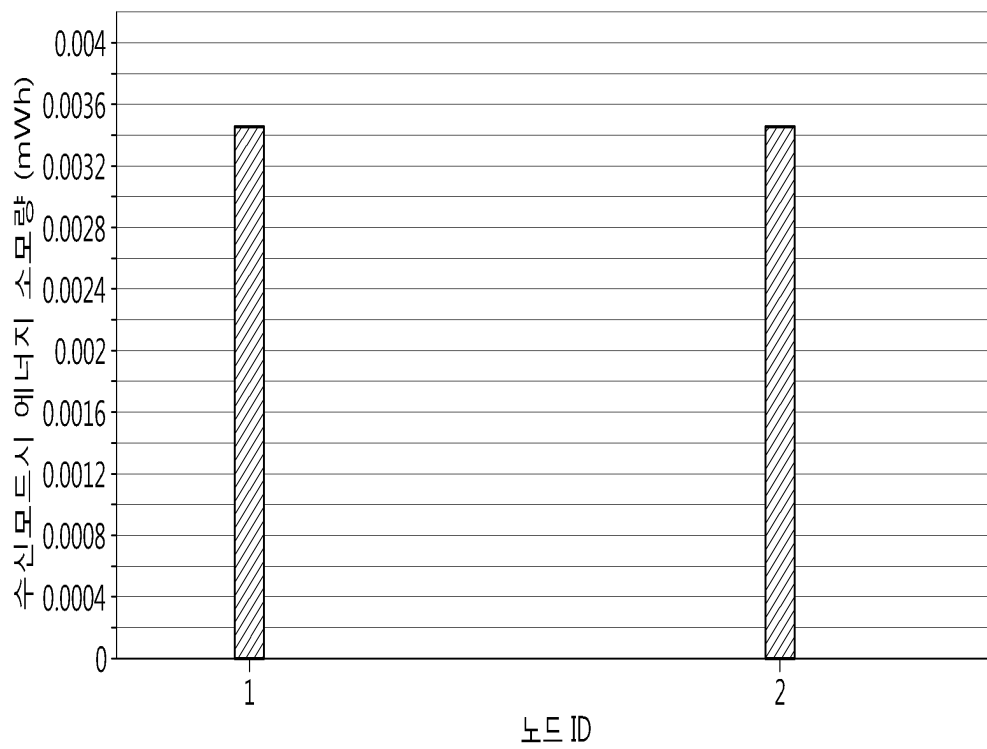
1500



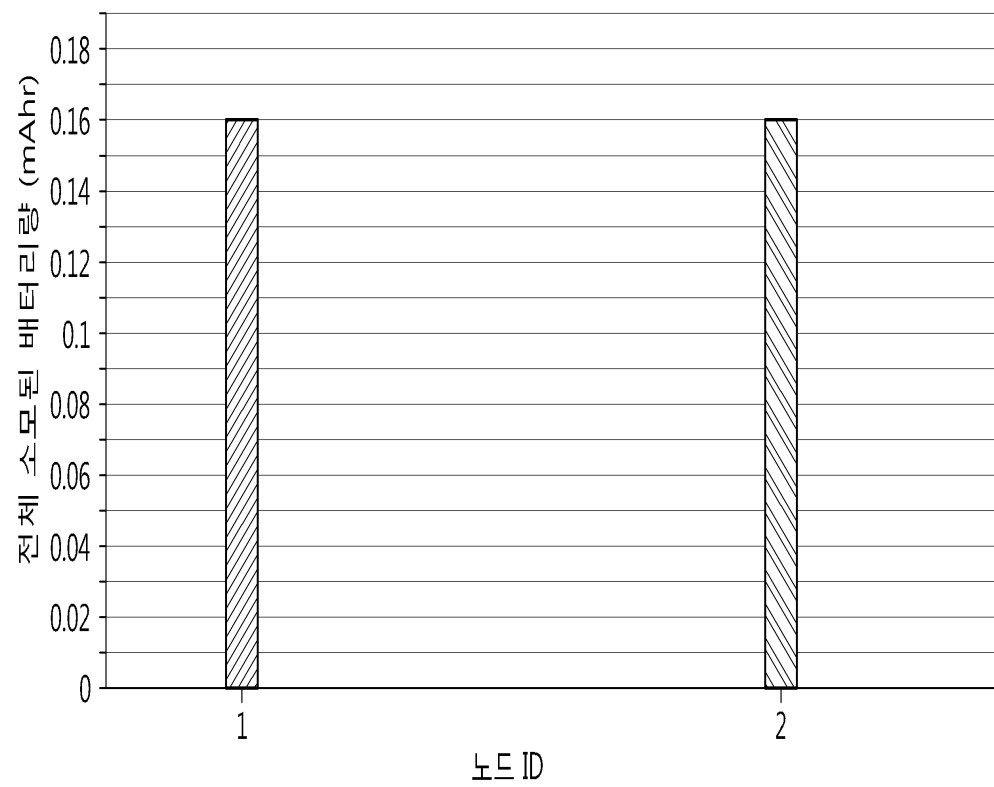
도면16a



도면16b



도면16c



도면17

