



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2010-0084854
(43) 공개일자 2010년07월28일

(51) Int. Cl.

H04L 9/08 (2006.01) H04L 9/30 (2006.01)

G06F 15/16 (2006.01)

(21) 출원번호 10-2009-0004213

(22) 출원일자 2009년01월19일

심사청구일자 2009년01월19일

(71) 출원인

충남대학교산학협력단

대전광역시 유성구 공동 220번지 충남대학교

(72) 발명자

이성진

경기도 수원시 장안구 천천동 300 성균관대학교
정보통신공학부

김승주

경기도 수원시 장안구 천천동 300 성균관대학교
정보통신공학부

(뒷면에 계속)

(74) 대리인

특허법인정직과특허

전체 청구항 수 : 총 16 항

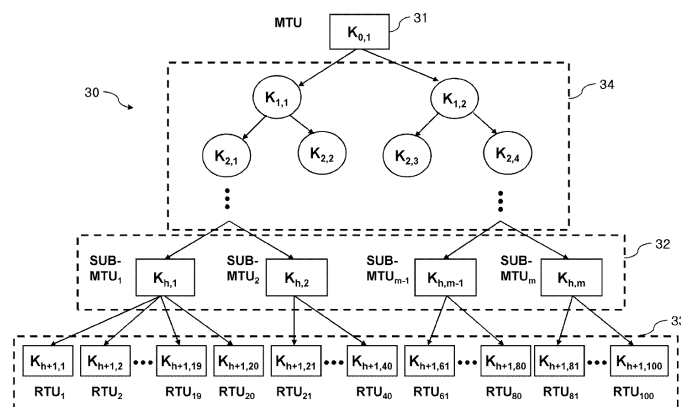
(54) SCADA 시스템 통신 환경에 효율적인 키 관리 방법

(57) 요약

마스터 단말(MTU), 다수의 서브단말(SUB-MTU), 다수의 원격단말(RTU)이 순차적인 계층으로 구성된 SCADA(Supervisory Control And Data Acquisition) 시스템에서의 통신을 위한 그룹키의 공유키를 관리방법에 관한 것으로서, (a) 마스터 단말은 비밀키를 생성하여 원격단말에게 할당하는 단계; (b) 그룹키를 트리구조로 생성하되, 그룹키의 각 노드의 공유키는 모든 자식노드의 공유키들을 해시하여 생성되고, 그룹키의 리프노드의 공유키는 원격단말의 비밀키로 정해지는 단계; (c) 상기 원격단말 또는 서브단말은 자신과 대응되는 노드에서 루트노드까지의 공유키를 수신하여 저장하는 단계; (d) 상기 원격단말 또는 서브단말이 추가 또는 삭제되면, 상기 마스터 단말은 상기 추가 또는 삭제되는 단말에 대응되는 노드에서 루트노드까지의 경로에 있는 노드들의 공유키를 다시 생성하는 단계; (e) 상기 원격단말 또는 서브단말은 다시 생성된 공유키를 수신하여 저장하는 단계를 포함하는 구성을 마련한다.

상기와 같은 SCADA 시스템 통신 환경의 키 관리방법에 의하여, 메시지를 암호화하여 브로드캐스팅 또는 멀티캐스팅 하는 경우, 발생하는 연산량을 줄일 수 있는 효과가 얻어진다.

대표도



(72) 발명자

원동호

경기도 수원시 장안구 천천동 300 성균관대학교 정보통신공학부

최동현

경기 수원시 장안구 천천동 300 성균관대학교 정보통신공학부

이광우

경기도 수원시 장안구 천천동 300 성균관대학교 정보통신공학부

이병희

경기도 수원시 장안구 천천동 300 성균관대학교 정보통신공학부

정한재

경기도 수원시 장안구 천천동 300 성균관대학교 정보통신공학부

전웅렬

경기도 수원시 장안구 천천동 300 성균관대학교 정보통신공학부

허순행

경기도 수원시 장안구 천천동 300 성균관대학교 정보통신공학부

차육재

경기도 수원시 장안구 천천동 300 성균관대학교 정보통신공학부

조성규

경기도 수원시 장안구 천천동 300 성균관대학교 정보통신공학부

박현상

경기도 수원시 장안구 천천동 300 성균관대학교 정보통신공학부

이형섭

경기도 수원시 장안구 천천동 300 성균관대학교 정보통신공학부

이현승

경기도 수원시 장안구 천천동 300 성균관대학교 정보통신공학부

김송이

경기도 수원시 장안구 천천동 300 성균관대학교 정보통신공학부

조영준

경기도 수원시 장안구 천천동 300 성균관대학교 정보통신공학부

특허청구의 범위

청구항 1

마스터 단말(MTU), 다수의 서브단말(SUB-MTU), 다수의 원격단말(RTU)이 순차적인 계층으로 구성되는 SCADA(Supervisory Control And Data Acquisition) 시스템 통신환경의 공유키 관리방법에 있어서,

(a) 상기 마스터 단말은 다수의 비밀키를 생성하여 상기 원격단말에게 각각 할당하는 단계;

(b) 상기 마스터 단말은 그룹키를 트리구조로 생성하되,

상기 트리구조의 리프노드는 각 원격단말과 대응되고, 원격단말에 대응되는 노드의 부모노드는 원격단말이 연결된 서브단말에 대응되고,

상기 그룹키의 각 노드의 공유키는 모든 자식노드의 공유키들을 해시하여 생성되고, 상기 그룹키의 리프노드의 공유키는 상기 원격 단말의 비밀키로 정해지는 단계;

(c) 상기 원격단말 또는 서브단말은 자신과 대응되는 노드에서 루트 노드까지의 공유키를 수신하여 저장하는 단계;

(d) 상기 원격단말 또는 서브단말이 추가 또는 삭제되면, 상기 마스터 단말은 상기 추가 또는 삭제되는 단말에 대응되는 노드에서 루트 노드까지의 경로에 있는 노드들의 공유키를 다시 생성하는 단계;

(e) 상기 원격단말 또는 서브단말은 다시 생성된 공유키를 수신하여 저장하는 단계를 포함하는 것을 특징으로 하는 SCADA 시스템 통신 환경의 공유키 관리방법.

청구항 2

제 1항에 있어서,

상기 (a)단계에서, 상기 마스터 단말은 연결된 원격단말이 없는 서브단말에 비밀키를 생성하여 할당하고,

상기 (b)단계에서, 원격단말이 없는 서브단말은 상기 트리구조의 리프노드에 대응되는 것을 특징으로 하는 SCADA 시스템 통신 환경의 공유키 관리방법.

청구항 3

제 1항에 있어서,

상기 트리구조는 서브단말에 대응되는 노드까지 2진 트리이고, 서브단말에서 원격단말까지는 n차 트리인 것을 특징으로 하는 SCADA 시스템 통신 환경의 공유키 관리방법.

청구항 4

제 3항에 있어서, 상기 (d)단계는,

(d1) 원격단말이 추가 또는 삭제되면, 상기 추가 또는 삭제된 원격단말이 연결된 서브단말에 대응되는 노드에서, 상기 추가 또는 삭제된 원격단말에 대응되는 노드를 추가 또는 삭제하는 단계;

(d2) 서브단말이 추가 또는 삭제되면, 상기 추가 또는 삭제된 서브단말에 대응되는 노드를 상기 그룹키의 트리 구조에서 추가 또는 삭제하고, 상기 그룹키의 트리구조를 2진트리로 재구성하는 단계;

(d3) 상기 추가 또는 삭제된 노드에서 루트노드까지의 경로에 있는 노드들의 공유키를 다시 생성하는 단계를 포함하는 것을 특징으로 하는 SCADA 시스템 통신 환경의 공유키 관리방법.

청구항 5

제 4항에 있어서, 상기 (d2)단계는,

상기 서브단말이 추가되면, 상기 마스터 단말은, 추가된 서브단말에 대응되는 추가노드를 생성하고, 상기 그룹키의 트리구조에서 하나의 리프노드를 제외하고, 상기 추가노드와 상기 제외된 리프노드를 자식노드로 하는 중간노드를 생성하고, 상기 중간노드를 상기 제외된 리프노드가 있었던 위치에 연결하고,

상기 서브단말이 삭제되면, 상기 마스터 단말은, 삭제된 서브단말에 대응되는 노드를 상기 그룹키의 트리구조에서 삭제하고, 상기 삭제된 노드의 형제노드를 상기 삭제된 노드의 부모노드에 대치하는 것을 특징으로 하는 SCADA 시스템 통신 환경의 공유키 관리방법.

청구항 6

제 1항에 있어서, 상기 (e)단계는,

상기 마스터 단말은 다시 생성된 공유키를 다시 생성된 공유키로 암호화하여 서브단말 또는 원격단말에게 멀티캐스팅하고,

상기 서브단말 또는 원격단말은 암호화된 공유키를 수신하고 복호화하여 저장하는 것을 특징으로 하는 SCADA 시스템 통신 환경의 공유키 관리방법.

청구항 7

마스터 단말(MTU), 다수의 서브단말(SUB-MTU), 다수의 원격단말(RTU)이 순차적인 계층으로 구성되는 SCADA(Supervisory Control And Data Acquisition) 시스템 통신환경의 공유키 관리방법에 있어서,

(a) 상기 마스터 단말은 다수의 비밀키를 생성하여 상기 서브 단말에게 각각 할당하고, 상기 서브 단말은 다수의 비밀키를 생성하여 자신에게 속하는 원격 단말에게 각각 할당하는 단계;

(b) 상기 마스터 단말은 상기 서브단말의 그룹키를 트리구조로 생성하고 상기 서브단말은 자신에게 속하는 원격 단말의 그룹키를 트리구조로 생성하되,

상기 트리구조의 리프노드는 각 원격단말 또는 각 서브단말과 대응되고,

상기 그룹키의 각 노드의 공유키는 모든 자식노드의 공유키들을 해시하여 생성되고, 상기 그룹키의 리프노드의 공유키는 상기 원격단말 또는 서브단말의 비밀키로 정해지는 단계;

(c) 상기 서브단말 또는 원격단말은 자신과 대응되는 노드에서 루트 노드까지의 공유키를 수신하여 저장하는 단계;

(d) 상기 서브단말 또는 원격단말이 추가 또는 삭제되면, 상기 마스터 단말 또는 서브단말은 추가 또는 삭제된 단말에 대응되는 노드에서 루트 노드까지의 경로에 있는 노드들의 공유키를 다시 생성하는 단계;

(e) 상기 원격단말 또는 서브단말은 다시 생성된 공유키를 수신하여 저장하는 단계를 포함하는 것을 특징으로 하는 SCADA 시스템 통신 환경의 공유키 관리방법.

청구항 8

제 7항에 있어서,

상기 트리구조는 2진 트리인 것을 특징으로 하는 SCADA 시스템 통신 환경의 공유키 관리방법.

청구항 9

제 8항에 있어서, 상기 (d)단계는,

(d1) 원격단말 또는 서브단말이 추가 또는 삭제되면, 상기 추가 또는 삭제된 원격단말 또는 서브단말에 대응되는 노드를, 상기 그룹키의 트리구조에서 추가 또는 삭제하고, 상기 그룹키의 트리구조를 2진트리로 재구성하는 단계;

(d2) 상기 추가 또는 삭제된 노드에서 루트노드까지의 경로에 있는 노드들의 공유키를 다시 생성하는 단계를 포함하는 것을 특징으로 하는 SCADA 시스템 통신 환경의 공유키 관리방법.

청구항 10

제 9항에 있어서, 상기 (d2)단계는,

상기 서브단말 또는 원격단말이 추가되면, 상기 마스터 단말 또는 서브단말은, 추가된 서브단말 또는 원격단말에 대응되는 추가노드를 생성하고, 상기 그룹키의 트리구조에서 하나의 리프노드를 제외하고, 상기 추가노드와 상기 제외된 리프노드를 자식노드로 하는 중간노드를 생성하고, 상기 중간노드를 상기 제외된 리프노드가 있었던 위치에 연결하고,

상기 서브단말 또는 원격단말이 삭제되면, 상기 마스터 단말 또는 서브단말은, 삭제된 서브단말 또는 원격단말에 대응되는 노드를 상기 그룹키의 트리구조에서 삭제하고, 상기 삭제된 노드의 형제노드를 상기 삭제된 노드의 부모노드에 대치하는 것을 특징으로 하는 SCADA 시스템 통신 환경의 공유키 관리방법.

청구항 11

제 7항에 있어서, 상기 (e)단계는,

상기 마스터 단말 또는 상기 서브단말은 다시 생성된 공유키를 다시 생성된 공유키로 암호화하여 서브단말 또는 원격단말에게 멀티캐스팅하고,

상기 서브단말 또는 원격단말은 암호화된 공유키를 수신하고 생성된 공유키로 복호화하여 저장하는 것을 특징으로 하는 SCADA 시스템 통신 환경의 공유키 관리방법.

청구항 12

제 1항 내지 제 11항 중 어느 한 항의 SCADA 시스템 통신 환경의 공유키 관리방법을 기록한 컴퓨터로 읽을 수 있는 기록매체.

청구항 13

마스터 단말(MTU), 다수의 서브단말(SUB-MTU), 다수의 원격단말(RTU)이 순차적인 계층으로 구성된 SCADA(Supervisory Control And Data Acquisition) 시스템의 통신환경의 세션키 생성방법에 있어서, 제 1항 내지 제 11항 중 어느 한 항의 공유키 관리방법에 의하여 구성된 그룹키를 이용하여 세션키를 생성하는 것을 특징으로 하는 SCADA 시스템 통신 환경의 세션키 생성방법.

청구항 14

제 13항에 있어서, 상기 세션키는,

상기 그룹키와, 타임스탬프 및 시퀀스 번호가 결합된 값을 해시하여 생성되는 것을 특징으로 하는 SCADA 시스템 통신 환경의 세션키 생성방법.

청구항 15

마스터 단말(MTU), 다수의 서브단말(SUB-MTU), 다수의 원격단말(RTU)이 순차적인 계층으로 구성된 SCADA(Supervisory Control And Data Acquisition) 시스템 통신 환경의 메시지 통신방법에 있어서, 제 1항의 공유키 관리방법에 의하여 구성된 그룹키를 이용하여, 마스터 단말과 서브단말의 그룹과, 서브단말과 원격단말의 그룹간에 Iolus 프레임워크에 의해 메시지 통신을 하는 것을 특징으로 하는 SCADA 시스템 통신 환경의 메시지 통신방법.

청구항 16

제 15항에 있어서,

상기 서브단말이 서브단말의 그룹키를 이용한 암호화된 메시지를 수신하면, 그룹키를 이용하여 암호화된 메시지를 복호화하고, 자신에게 속하는 원격단말의 그룹키의 루트노드의 공유키를 이용하여 상기 복호화된 메시지를 암호화하여 자신에게 속하는 원격단말에게 멀티캐스팅하는 것을 특징으로 하는 SCADA 시스템 통신 환경의 메시지 통신방법.

명세서

발명의 상세한 설명

기술 분야

- [0001] 본 발명은 마스터 단말(MTU), 다수의 서브단말(SUB-MTU), 다수의 원격단말(RTU)이 순차적인 계층으로 구성된 SCADA(Supervisory Control And Data Acquisition) 시스템에서, 그룹키를 트리구조로 생성하고, 원격단말 또는 서브단말이 자신에 해당하는 노드에서 루트 노드까지의 그룹키 공유키를 저장하여, 공유키를 통해 통신을 하는 SCADA 시스템 통신 환경의 키 관리방법에 관한 것이다.
- [0002] 특히, 본 발명은 SCADA 시스템의 그룹키를 트리구조로 생성하되, 리프노드와 리프노드의 부모노드를 각각 원격단말과 서브단말에 대응하여 하나의 그룹키를 생성하거나, 마스터 단말과 서브단말, 서브단말과 이와 연결된 원격단말로 분리하여 그룹키를 생성하고, 분리된 그룹간에는 Iolus 프레임워크로 통신을 연계하는 키 관리방법에 관한 것이다.
- [0003] 또, 본 발명은 원격단말 또는 서브단말이 추가 또는 삭제되면, 이에 대응되는 그룹키의 트리구조를 변경하고 변경된 트리구조의 공유키를 갱신하여, 공유키를 재분배하는 키 관리방법에 관한 것이다.

배경 기술

- [0004] 일반적으로 SCADA(Supervisory Control And Data Acquisition) 시스템은 국가 기반시설 등에서 사용되는 산업적인 제어 및 감시 시스템이다. 즉, SCADA 시스템은 수자원 시설, 변전소 또는 발전소 등 에너지 시설, 가스 및 송유관 시설 등의 프로세스를 감시하고 제어하는 컴퓨터 시스템이다.
- [0005] 과거에 SCADA 시스템은 폐쇄적인 환경에서 사용되었기 때문에 보안성에 대한 고려 없이 설계되었다. 하지만, 점차 SCADA 시스템을 개방 네트워크에 연결하려는 요구가 증가함에 따라 SCADA 시스템에 대한 보안이 이슈화 되었다. SCADA 시스템의 보안성을 향상시키기 위해서는 데이터의 암호화 기능과 그에 따른 암호화 키 관리가 필수적이다.
- [0006] 기존에 SCADA 시스템을 위한 키 관리 방법으로 SKE(Key establishment for SCADA systems)와 SKMA(Key management scheme for SCADA systems)가 제안되었지만, 이러한 키 관리 방법들은 브로드캐스팅이나 멀티캐스팅 통신을 지원하지 못한다는 단점이 있었다. 즉, SKE나 SKMA 방식에서는 메시지를 여러 장치에게 보내기 위해서는 각 장치와 공유한 키를 이용하여 메시지를 장치의 수만큼 암호화해야 한다. 이러한 방법은 수 천 개의 장치를

관리하며, 실시간 처리를 해야 하는 SCADA 시스템에 많은 부하를 줄 수 있으며, 적절하지 못한 통신 방법이다.

[0007] 이를 해결하고자, 계층구조를 가지는 논리키를 통해 이를 해결하는 SCADA 시스템의 안전한 통신환경을 위하여 개선된 키 관리 체계가 제시되었다. 그러나 상기 개선된 키 관리 체계는 많은 연산량을 요구한다는 문제점을 가지고 있다. 특히, 이 문제는 실시간 처리를 해야 하는 SCADA 시스템에는 치명적인 약점이다.

발명의 내용

해결 하고자하는 과제

[0008] 본 발명의 목적은 상술한 바와 같은 문제점을 해결하기 위한 것으로, 마스터 단말(MTU), 다수의 서브단말(SUB-MTU), 다수의 원격단말(RTU)이 순차적인 계층으로 구성된 SCADA(Supervisory Control And Data Acquisition) 시스템에서, 그룹키를 트리구조로 생성하고, 원격단말 또는 서브단말이 자신에 해당하는 노드에서 루트 노드까지의 그룹키 공유키를 저장하여, 공유키를 통해 통신을 하는 SCADA 시스템 통신 환경의 키 관리방법을 제공하는 것이다.

[0009] 본 발명의 다른 목적은 SCADA 시스템의 그룹키를 트리구조로 생성하되, 리프노드와 리프노드의 부모노드를 각각 원격단말과 서브단말에 대응하여 하나의 그룹키를 생성하거나, 마스터 단말과 서브단말, 서브단말과 이와 연결된 원격단말로 분리하여 그룹키를 생성하고, 분리된 그룹간에는 Iolus 프레임워크로 통신을 연계하는 키 관리방법을 제공하는 것이다.

[0010] 본 발명의 또 다른 목적은 원격단말 또는 서브단말이 추가 또는 삭제되면, 이에 대응되는 그룹키의 트리구조를 변경하고 변경된 트리구조의 공유키를 갱신하여, 공유키를 재분배하는 키 관리방법을 제공하는 것이다.

과제 해결수단

[0011] 상기 목적을 달성하기 위해 본 발명은 마스터 단말(MTU), 다수의 서브단말(SUB-MTU), 다수의 원격단말(RTU)이 순차적인 계층으로 구성되는 SCADA(Supervisory Control And Data Acquisition) 시스템 통신환경의 공유키 관리방법에 관한 것으로서, (a) 상기 마스터 단말은 다수의 비밀키를 생성하여 상기 원격단말에게 각각 할당하는 단계; (b) 상기 마스터 단말은 그룹키를 트리구조로 생성하되, 상기 트리구조의 리프노드는 각 원격단말과 대응되고, 원격단말에 대응되는 노드의 부모노드는 원격단말이 연결된 서브단말에 대응되고, 상기 그룹키의 각 노드의 공유키는 모든 자식노드의 공유키들을 해시하여 생성되고, 상기 그룹키의 리프노드의 공유키는 상기 원격 단말의 비밀키로 정해지는 단계; (c) 상기 원격단말 또는 서브단말은 자신과 대응되는 노드에서 루트 노드까지의 공유키를 수신하여 저장하는 단계; (d) 상기 원격단말 또는 서브단말이 추가 또는 삭제되면, 상기 마스터 단말은 상기 추가 또는 삭제되는 단말에 대응되는 노드에서 루트 노드까지의 경로에 있는 노드들의 공유키를 다시 생성하는 단계; (e) 상기 원격단말 또는 서브단말은 다시 생성된 공유키를 수신하여 저장하는 단계를 포함하는 것을 특징으로 한다.

[0012] 또, 본 발명은 SCADA 시스템 통신 환경의 공유키 관리방법에 있어서, 상기 (a)단계에서, 상기 마스터 단말은 연결된 원격단말이 없는 서브단말에 비밀키를 생성하여 할당하고, 상기 (b)단계에서, 원격단말이 없는 서브단말은 상기 트리구조의 리프노드에 대응되는 것을 특징으로 한다.

[0013] 또, 본 발명은 SSCADA 시스템 통신 환경의 공유키 관리방법에 있어서, 상기 트리구조는 서브단말에 대응되는 노드까지 2진 트리이고, 서브단말에서 원격단말까지는 n차 트리인 것을 특징으로 한다.

[0014] 또, 본 발명은 SSCADA 시스템 통신 환경의 공유키 관리방법에 있어서, 상기 (d)단계는, (d1) 원격단말이 추가 또는 삭제되면, 상기 추가 또는 삭제된 원격단말이 연결된 서브단말에 대응되는 노드에서, 상기 추가 또는 삭제된 원격단말에 대응되는 노드를 추가 또는 삭제하는 단계; (d2) 서브단말이 추가 또는 삭제되면, 상기 추가 또는 삭제된 서브단말에 대응되는 노드를 상기 그룹키의 트리구조에서 추가 또는 삭제하고, 상기 그룹키의 트리구조를 2진트리로 재구성하는 단계; (d3) 상기 추가 또는 삭제된 노드에서 루트노드까지의 경로에 있는 노드들의 공유키를 다시 생성하는 단계를 포함하는 것을 특징으로 한다.

[0015] 또, 본 발명은 SSCADA 시스템 통신 환경의 공유키 관리방법에 있어서, 상기 (d2)단계는, 상기 서브단말이 추가 되면, 상기 마스터 단말은, 추가된 서브단말에 대응되는 추가노드를 생성하고, 상기 그룹키의 트리구조에서 하

나의 리프노드를 제외하고, 상기 추가노드와 상기 제외된 리프노드를 자식노드로 하는 중간노드를 생성하고, 상기 중간노드를 상기 제외된 리프노드가 있었던 위치에 연결하고, 상기 서브단말이 삭제되면, 상기 마스터 단말은, 삭제된 서브단말에 대응되는 노드를 상기 그룹키의 트리구조에서 삭제하고, 상기 삭제된 노드의 형제노드를 상기 삭제된 노드의 부모노드에 대치하는 것을 특징으로 한다.

[0016] 또, 본 발명은 SSCADA 시스템 통신 환경의 공유키 관리방법에 있어서, 상기 (e)단계는, 상기 마스터 단말은 다시 생성된 공유키를 다시 생성전 공유키로 암호화하여 서브단말 또는 원격단말에게 멀티캐스팅하고, 상기 서브단말 또는 원격단말은 암호화된 공유키를 수신하고 복호화하여 저장하는 것을 특징으로 한다.

[0017] 또한, 본 발명은 마스터 단말(MTU), 다수의 서브단말(SUB-MTU), 다수의 원격단말(RTU)이 순차적인 계층으로 구성되는 SCADA(Supervisory Control And Data Acquisition) 시스템 통신환경의 공유키 관리방법에 관한 것으로서, (a) 상기 마스터 단말은 다수의 비밀키를 생성하여 상기 서브 단말에게 각각 할당하고, 상기 서브 단말은 다수의 비밀키를 생성하여 자신에게 속하는 원격 단말에게 각각 할당하는 단계; (b) 상기 마스터 단말은 상기 서브단말의 그룹키를 트리구조로 생성하고 상기 서브단말은 자신에게 속하는 원격단말의 그룹키를 트리구조로 생성하되, 상기 트리구조의 리프노드는 각 원격단말 또는 각 서브단말과 대응되고, 상기 그룹키의 각 노드의 공유키는 모든 자식노드의 공유키들을 해시하여 생성되고, 상기 그룹키의 리프노드의 공유키는 상기 원격단말 또는 서브단말의 비밀키로 정해지는 단계; (c) 상기 서브단말 또는 원격단말은 자신과 대응되는 노드에서 루트 노드까지의 공유키를 수신하여 저장하는 단계; (d) 상기 서브단말 또는 원격단말이 추가 또는 삭제되면, 상기 마스터 단말 또는 서브단말은 추가 또는 삭제된 단말에 대응되는 노드에서 루트 노드까지의 경로에 있는 노드들의 공유키를 다시 생성하는 단계; (e) 상기 원격단말 또는 서브단말은 다시 생성된 공유키를 수신하여 저장하는 단계를 포함하는 것을 특징으로 한다.

[0018] 또, 본 발명은 SSCADA 시스템 통신 환경의 공유키 관리방법에 있어서, 상기 트리구조는 2진 트리인 것을 특징으로 한다.

[0019] 또, 본 발명은 SSCADA 시스템 통신 환경의 공유키 관리방법에 있어서, 상기 (d)단계는, (d1) 원격단말 또는 서브단말이 추가 또는 삭제되면, 상기 추가 또는 삭제된 원격단말 또는 서브단말에 대응되는 노드를, 상기 그룹키의 트리구조에서 추가 또는 삭제하고, 상기 그룹키의 트리구조를 2진트리로 재구성하는 단계; (d2) 상기 추가 또는 삭제된 노드에서 루트노드까지의 경로에 있는 노드들의 공유키를 다시 생성하는 단계를 포함하는 것을 특징으로 한다.

[0020] 또, 본 발명은 SSCADA 시스템 통신 환경의 공유키 관리방법에 있어서, 상기 (d2)단계는, 상기 서브단말 또는 원격단말이 추가되면, 상기 마스터 단말 또는 서브단말은, 추가된 서브단말 또는 원격단말에 대응되는 추가노드를 생성하고, 상기 그룹키의 트리구조에서 하나의 리프노드를 제외하고, 상기 추가노드와 상기 제외된 리프노드를 자식노드로 하는 중간노드를 생성하고, 상기 중간노드를 상기 제외된 리프노드가 있었던 위치에 연결하고, 상기 서브단말 또는 원격단말이 삭제되면, 상기 마스터 단말 또는 서브단말은, 삭제된 서브단말 또는 원격단말에 대응되는 노드를 상기 그룹키의 트리구조에서 삭제하고, 상기 삭제된 노드의 형제노드를 상기 삭제된 노드의 부모노드에 대치하는 것을 특징으로 한다.

[0021] 또, 본 발명은 SSCADA 시스템 통신 환경의 공유키 관리방법에 있어서, 상기 (e)단계는, 상기 마스터 단말 또는 상기 서브단말은 다시 생성된 공유키를 다시 생성전 공유키로 암호화하여 서브단말 또는 원격단말에게 멀티캐스팅하고, 상기 서브단말 또는 원격단말은 암호화된 공유키를 수신하고 생성전 공유키로 복호화하여 저장하는 것을 특징으로 한다.

[0022] 또한, 본 발명은 상기 SSCADA 시스템 통신 환경의 공유키 관리방법을 기록한 컴퓨터로 읽을 수 있는 기록매체에 관한 것이다.

[0023] 또한, 본 발명은 마스터 단말(MTU), 다수의 서브단말(SUB-MTU), 다수의 원격단말(RTU)이 순차적인 계층으로 구성된 SCADA(Supervisory Control And Data Acquisition) 시스템에서, 상기 SSCADA 시스템 통신 환경의 공유키 관리방법에 의하여 구성된 그룹키를 이용하여 세션키를 생성하는, SCADA 시스템 통신 환경의 세션키 생성방법에 관한 것이다.

[0024] 또, 본 발명은 SCADA 시스템 통신 환경의 세션키 생성방법에 있어서, 상기 세션키는, 상기 그룹키와, 타임스탬프 및 시퀀스 번호가 결합된 값을 해시하여 생성되는 것을 특징으로 한다.

[0025] 또한, 본 발명은 마스터 단말(MTU), 다수의 서브단말(SUB-MTU), 다수의 원격단말(RTU)이 순차적인 계층으로 구성된 SCADA(Supervisory Control And Data Acquisition) 시스템에서, 상기 SSCADA 시스템 통신 환경의 공유키 관리방법에 의하여 구성된 그룹키를 이용하여, 마스터 단말과 서브단말의 그룹과, 서브단말과 원격단말의 그룹 간에 Iolus 프레임워크에 의해 메시지 통신을 하는, SCADA 시스템 통신 환경의 메시지 통신방법에 관한 것이다.

[0026] 또, 본 발명은 SCADA 시스템 통신 환경의 메시지 통신방법에 있어서, 상기 서브단말은 서브단말의 그룹키를 이용한 암호화된 메시지를 수신하면, 그룹키를 이용하여 암호화된 메시지를 복호화하고, 자신에게 속하는 원격단말의 그룹키의 루트노드의 공유키를 이용하여 상기 복호화된 메시지를 암호화하여 자신에게 속하는 원격단말에게 멀티캐스팅하는 것을 특징으로 한다.

효 과

[0027] 상술한 바와 같이, 본 발명에 따른 SCADA 시스템 통신 환경의 키 관리방법에 의하면, SCADA 시스템에서 메시지를 암호화하여 브로드캐스팅 또는 멀티캐스팅 하는 경우, 발생하는 연산량을 줄일 수 있는 효과가 얻어진다.

[0028] 또, 본 발명에 따른 SCADA 시스템 통신 환경의 키 관리방법에 의하면, 메모리 공간과 연산능력이 제한적인 SCADA 시스템 통신 장치의 암호화 통신 수행 시, 브로드캐스팅이나 멀티캐스팅 통신을 위한 암호화 연산량이 줄어들어 실시간 처리를 요하는 SCADA 시스템에 효율적일 뿐만 아니라, 저장해야 할 키의 수가 적어 효율적으로 키를 관리할 수 있는 효과가 얻어진다.

발명의 실시를 위한 구체적인 내용

[0029] 이하, 본 발명의 실시를 위한 구체적인 내용을 도면에 따라서 설명한다.

[0030] 또한, 본 발명을 설명하는데 있어서 동일 부분은 동일 부호를 붙이고, 그 반복 설명은 생략한다.

[0031] 먼저, 본 발명을 실시하기 위한 SCADA 시스템의 전체 구성의 일례에 대하여 도 1을 참조하여 설명한다.

[0032] 도 1에서 보는 바와 같이, 본 발명을 실시하기 위한 SCADA 시스템은 관리자 단말(HMI, Human-Machine Interface)(10), 마스터 단말(MTU, Master Terminal Unit)(21), 서브단말(SUB-MTU, SUB Master Terminal Unit)(22), 원격단말(RTU, Remote Terminal Unit)(23)로 구성된다. 특히, 마스터 단말(21), 서브단말(22), 원격단말(23)은 순차적으로 계층적 구조를 갖는다.

[0033] 관리자 단말(10)은 기반시설의 프로세스 데이터를 관리자에게 보여주는 장치로서, 관리자가 이를 통해 기반시설을 모니터링하고 제어하는 단말 장치이다. 이를 위해, 관리자 단말(10)은 컴퓨팅 기능을 가진 단말장치로 구성된다.

[0034] 원격단말(23)은 기반시설에 직접 설치되어 프로세스 데이터를 수집하여 전송하거나 제어명령에 따라 수행하는 단말장치이다. 일반적으로 SCADA시스템에 적용되는 기반시설은 지역적으로 넓게 분포되어 있기 때문에, 원격단말(23)들도 지역적으로 흩어져 있다.

[0035] 서브단말(22)은 특정한 원격단말(23)과 통신하고 이들을 제어한다. 마스터 단말(21)은 전체적으로 프로세스 데이터를 수집하고 제어하는 장치이다. 즉, 마스터 단말(21)은 서브단말(22)을 제어하고 서브단말(22)을 통해 원격단말(23)을 모니터링하고 제어한다.

[0036] 마스터 단말(21), 서브단말(22), 원격단말(23)들이 서로 암호화된 통신을 하기 위해서는 세션키를 이용한다. 즉, 송신하는 단말과 수신하는 단말 사이에서 세션키를 생성하여 서로 나누어 갖는다. 그리고 송신 단말은 보내려는 메시지를 세션키로 암호화하여 전송하고, 수신 단말은 암호화된 메시지를 수신하여 세션키로 복호화한다.

[0037] 세션키는 메시지를 송수신하는 특정 세션에서만 이용되는 키로서, 세션을 달리하면 다르게 생성된다. 세션키가

노출되더라도 다른 세션은 안전하다. 그런데 세션키를 만들기 위해서 사용되는 비밀키가 공유키이다. 즉, 세션키는 공유키에 타임스탬프, 시퀀스 번호, 장치의 식별자 등이 추가되어 생성된다. 따라서 안전한 통신을 위해서는 무엇보다 공유키의 관리가 중요하다.

- [0038] 본 발명에 따른 SCADA 시스템 통신 환경의 공유키 관리방법은 마스터 단말(21)에 의해 전체적으로 하나의 논리구조로 관리하는 제1 실시예와, 마스터 단말(21) 또는 서브단말(22)이 각각 별도의 논리구조로 나누어 관리하는 제2 실시예로 나뉜다.
- [0039] 즉, 본 발명의 제1 실시예에 따르면, 마스터 단말(21)이 공유키를 생성하여 서브단말(22) 또는 원격단말(23)에 전달된다. 즉, 마스터 단말(21)이 전체의 공유키를 주체적으로 관리한다. 그리고 공유키는 전체적으로 공유된다.
- [0040] 본 발명의 제2 실시예에 따르면, 마스터 단말(21)이 공유키를 생성하여 자신이 관리하는 서브단말(22)에 전달하고, 서브단말(22)도 공유키를 생성하여 자신이 관리하는 원격단말(23)에 전달한다. 즉, 마스터 단말(21)과 서브단말(22)이 2개의 계층으로 공유키를 나누어 관리한다. 또, 공유키는 마스터 단말(21)과 서브단말(22), 서브단말(22)과 원격단말(23)로 구분되어 공유된다.
- [0041] 이때, 마스터 단말(21)과 이에 속하는 서브단말(22)을 "마스터 계층 그룹"이라고 칭하고, 서브단말(22)과 이에 속하는 원격단말(23)을 "서브계층 그룹"으로 부르기로 한다.
- [0042] 이 경우, 서브단말(22)은 마스터 계층 그룹 내에서 통신을 할 때는 마스터 계층 그룹에서 만들어지는 세션키를 이용하고, 서브 계층 그룹 내에서 통신을 할 때는 서브 계층 그룹에서 만들어지는 세션키를 이용한다. 또, 세션키는 각 그룹에서 생성되고 관리되는 공유키에 의해 생성된다.
- [0043] 한편, 마스터 계층 그룹과 서브계층 그룹 간의 메시지 통신은 Iolus 프레임워크에 의해 연계된다. 즉, 마스터 계층 그룹에서 서브계층 그룹으로 메시지를 전달하는 경우, 서브단말(22)은 마스터 계층 그룹에서 만들어진 세션키로 수신된 메시지를 복호화하고, 서브계층 그룹에서 만들어진 세션키로 다시 암호화하여 서브계층 그룹으로 전달한다. 반대로 서브계층 그룹에서 마스터 계층 그룹으로 전송하는 경우, 서브단말(22)은 그 반대로 작업을 수행한다.
- [0044] 한편, SCADA시스템에서 서브단말(22) 또는 원격단말(23)이 삭제되거나 추가되면, 도 1과 같은 SCADA시스템의 구조가 변경된다. SCADA시스템의 구조가 변경되면, 이에 따라 공유키도 변경된다.
- [0045] 즉, 제1 실시예에 따르면 마스터 단말(21)이, 제2 실시예에 따르면 마스터 단말(21) 또는 서브단말(22)이 변경된 SCADA시스템의 구조에 따라 공유키를 갱신하고, 서브단말(22) 또는 원격단말(23)에 갱신된 공유키를 전달한다.
- [0046] 다음으로, 본 발명의 제1 실시예에 따른 SCADA 시스템 통신 환경의 공유키 관리방법을 도 2를 참조하여 설명한다.
- [0047] 도 2에서 보는 바와 같이, 본 발명의 제 1의 실시예에 따른 키 관리방법은 (a) 마스터 단말은 비밀키를 생성하여 원격단말에게 할당하는 단계(S10); (b) 그룹키를 트리구조로 생성하되, 그룹키의 각 노드의 공유키는 모든 자식노드의 공유키들을 해시하여 생성되고, 그룹키의 리프노드의 공유키는 원격단말의 비밀키로 정해지는 단계(S20); (c) 상기 원격단말 또는 서브단말은 자신과 대응되는 노드에서 루트 노드까지의 공유키를 수신하여 저장하는 단계(S30); (d) 상기 원격단말 또는 서브단말이 추가 또는 삭제되면, 상기 마스터 단말은 상기 추가 또는 삭제되는 단말에 대응되는 노드에서 루트 노드까지의 경로에 있는 노드들의 공유키를 다시 생성하는 단계(S40); (e) 상기 원격단말 또는 서브단말은 다시 생성된 공유키를 수신하여 저장하는 단계(S50)로 구성된다.
- [0048] 상기 (a)단계는 마스터 단말(21)이 다수의 비밀키를 생성하여 원격단말(23)에게 각각 할당하는 단계이다(S10). 또, 상기 마스터 단말(21)은 연결된 원격단말(23)이 없는 서브단말(22)에 비밀키를 생성하여 할당한다.
- [0049] 따라서 마스터 단말(21)은 SCADA 시스템의 계층구조에서 제일 말단, 즉, 리프노드에 해당하는 서브단말(22) 또는 원격단말(23) 모두에 비밀키를 생성하여 할당한다.
- [0050] 상기 (b)단계에서, 상기 마스터 단말(21)은 그룹키를 트리구조로 생성하되, 상기 트리구조의 리프노드는 각 원격단말(23)과 대응되고, 원격단말(23)에 대응되는 노드의 부모노드는 원격단말(23)이 연결된 서브단말(22)에 대응되고, 상기 그룹키의 각 노드의 공유키는 모든 자식노드의 공유키들을 해시하여 생성되고, 상기 그룹키의 리

프노드의 공유키는 상기 원격 단말(23)의 비밀키로 정해지는 단계(S20)이다.

[0051] 특히, 상기 그룹키의 트리구조는 서브단말(22)에 대응되는 노드까지 2진 트리이고, 서브단말(22)에서 원격단말(23)까지는 n차 트리이다.

[0052] 본 발명의 제1 실시예에 따른 그룹키(30)의 트리구조를 도 3을 참조하여 보다 자세히 설명한다.

[0053] 도 3에서 보는 바와 같이, 그룹키(30)는 SCADA시스템에 대응되는 트리구조를 가진다. 그룹키(30)의 루트노드(31)는 마스터 단말(21)에 대응되고, 리프노드(33)는 원격단말(23)에 대응된다. 이를 각각 "마스터 단말 노드(31)", "원격단말 노드(32)"라 부르기로 한다.

[0054] 또, 리프노드(33)의 부모노드(32)는 서브단말(22)에 대응된다. 이를 "서브단말 노드(32)"라 부르기로 한다. 특히, 하나의 서브단말 노드(32)의 자식노드(33)들은 이 서브단말(22)에 연결된 원격단말(23)에 대응되는 노드(33)들이다. 따라서 서브단말 또는 원격단말에 대응되는 노드들의 구조는 SCADA시스템의 계층구조와 동일하다. 또, 서브단말(22)에는 다수의 원격단말(23)이 연결될 수 있으므로, 서브단말(22)에 대응되는 노드를 루트로 하는 트리는 n차 트리(n-array tree)이다.

[0055] 한편, 마스터 단말 노드(31)와 서브단말 노드(32) 사이는 2진 트리구조로 만들어진다. 마스터 단말 노드(31)와 서브단말 노드(32) 사이의 노드를 "중간노드(34)"라 부르기로 한다.

[0056] 따라서 마스터 단말 노드(31)를 정점(루트노드)으로 하여 서브단말 노드(32)까지의 트리는 2진 트리구조이고, 서브단말 노드(32)를 정점으로 하는 트리는 n차 트리(n-array tree)이다.

[0057] 상기 그룹키(31)의 트리구조의 각 노드에는 공유키가 생성된다. 생성되는 방법은 다음과 같다.

[0058] 먼저, 앞서 (a)단계에서 각 원격단말(23)에 할당된 비밀키가 그룹키(30)의 리프노드(33)(또는 원격단말 노드)의 공유키로 정해진다. 원격단말이 없는 서브단말(22)에 대응되는 서브단말 노드(32)에도 상기 서브단말(23)에 할당된 비밀키가 공유키로 정해진다. 즉, 그룹키(30)의 트리구조의 리프노드에 비밀키가 공유키로 정해진다. 예를 들면, 도 3에서, 그룹키(30)의 리프노드에는 원격단말 RTU₁, RTU₂, ..., RTU₁₀₀, 에 각각 할당된 비밀키인 K_{h+1,1}, K_{h+1,2}, ..., K_{h+1,100}, 이 공유키로 정해진다.

[0059] 다음으로, 그룹키(30)의 각 노드의 공유키는 모든 자식노드의 공유키들을 해시하여 생성된다.

[0060] 특히, 서브단말 노드(32)의 공유키는 서브단말(22)에 연결된 모든 원격단말(23)의 비밀키를 해시하여 생성한다. 서브단말 노드(32)의 공유키 $K_{i+1, \lceil j/n \rceil}$ if $(1 \leq i \leq \log_n m - 1, 1 \leq j \leq m)$ 는 m개의 원격단말의 비밀키 $K_{i,j}$ if $(1 \leq i \leq \log_n m - 1, 1 \leq j \leq m)$ 를 해시하여 생성된다. 식으로 표현하면, [수식 1]과 같다.

[0061] [수식 1]

$$K_{i-1, \lceil j/n \rceil} = H(H(K_{i,j}), H(K_{i,j+1}), \dots, H(K_{i,j+n-1}))$$

$$\text{if } (1 \leq i \leq \log_n m - 1, 1 \leq j \leq m)$$

[0062]

[0063] 단, n은 서브단말에 연결하는 원격단말의 수,

[0064] m은 원격단말의 개수

[0065] 한편, 마스터 단말 노드(31)와 서브단말 노드(32) 사이는 2진 트리 형태로 공유키 구조가 생성된다. 2진 트리구조에서 각 노드의 공유키 값은 자식 노드의 두 공유키(또는 해시된 값)를 해시함으로써 생성된다. 식으로 표현하면, [수식 2]와 같다.

[0066] [수식 2]

$$K_{i-1, \lceil j/2 \rceil} = H(H(K_{i,j}), H(K_{i,j+1})) \text{ if } (1 \leq i \leq h-1, 1 \leq j \leq m)$$

[0067]

[0068] 단, m은 원격단말의 개수

- [0069] $h = 1 + \log_2 m$
- [0070] 따라서 위의 식을 통해 2진 트리구조의 공유키 구조가 형성되며, 루트노드의 공유키 $K_{0,1}$ 이 생성된다.
- [0071]
- [0072] 상기 (c)단계는 상기 원격단말(23) 또는 서브단말(22)이 자신과 대응되는 노드에서 루트 노드까지의 공유키를 수신하여 저장하는 단계이다(S30).
- [0073] 앞서 (b)단계에서 설명된 그룹키 구조에서 서브단말(22)은 자신의 노드부터 루트 노드까지의 경로에 있는 모든 노드의 키 값을 저장한다. 즉, 서브단말(22)의 개수가 m 개 일 경우, $1 + \log_2 m$ 개의 공유키를 저장하며, 원격단말(23)은 서브단말(22)의 공유키 개수에서 자신의 공유키(또는 비밀키)를 더한 $2 + \log_2 m$ 개의 공유키를 저장한다.
- [0074] 상기 (d)단계는 상기 원격단말(23) 또는 서브단말(22)이 추가 또는 삭제되면, 상기 마스터 단말(21)이 상기 추가 또는 삭제되는 단말에 대응되는 노드에서 루트 노드까지의 경로에 있는 노드들의 공유키를 다시 생성하는 단계(S40)이다.
- [0075] 상기 (d)단계를 도 4를 참조하여 상세히 설명한다.
- [0076] 도 4에서 보는 바와 같이, 상기 (d)단계는 (d1) 원격단말(23)이 추가 또는 삭제되면 그룹키(30)를 변경하는 단계(S41), (d2) 서브단말(22)이 추가 또는 삭제되면 그룹키(30)를 변경하는 단계(S42), (d3) 그룹키(30)의 변경에 따라 노드들의 공유키를 재생성하는 단계(S43)으로 나뉜다.
- [0077] 상기 (d1)단계는, 원격단말(23)이 추가 또는 삭제되면, 상기 추가 또는 삭제된 원격단말(23)이 연결된 서브단말에 대응되는 노드(32)에서, 상기 추가 또는 삭제된 원격단말에 대응되는 노드(33)를 추가 또는 삭제하는 단계(S41)이다.
- [0078] 서브단말(22)과 원격단말(23)의 구조는 그룹키(30)에서 서브단말 노드(32)와 원격단말 노드(33)의 구조가 동일하다. 또, 서브단말 노드(32)와 원격단말 노드(33)의 트리구조는 n 차원 트리(n -array tree)이므로 서브단말 노드(23)의 자식노드 개수는 몇 개도 가능하다. 따라서 원격단말(23)이 추가 또는 삭제되면, 서브단말 노드(32)에서 원격단말 노드(33)를 추가 또는 삭제한다. 그룹키(30)의 다른 노드를 변경하지 않는다.
- [0079] 예를 들면, 도 3에서, 원격단말 RTU_{100} 이 삭제되면, 이에 대응되는 그룹키(30)의 노드인 $K_{h+1,100}$ 을 서브단말 노드 $K_{h,m}$ 에서 삭제한다. 또, 도 3에서 원격단말 RTU_{101} 이 추가되면, 이에 대응되는 노드 $K_{h+1,101}$ 을 서브단말 노드 $K_{h,m}$ 에서 추가한다. 이외에 도 3에서 변경되는 그룹키(30)의 구조는 없다.
- [0080] 상기 (d2)단계는, 서브단말(22)이 추가 또는 삭제되면, 상기 추가 또는 삭제된 서브단말(22)에 대응되는 노드를 상기 그룹키(30)의 트리구조에서 추가 또는 삭제하고, 상기 그룹키(30)의 트리구조를 2진 트리로 재구성하는 단계(S42)이다.
- [0081] 앞서 원격단말(23)이 추가 또는 삭제되는 것과는 달리, 서브단말(22)이 추가 또는 삭제되면, 마스터 단말 노드(31)에서 서브단말(32)까지의 노드들을 2진 트리로 재구성해야 한다. 이를 도 5와 도 6을 참조하여 설명한다.
- [0082] 도 5에서 보는 바와 같이, 상기 (d2)단계에서, 상기 서브단말(22)이 추가되면, 상기 마스터 단말(21)은, 추가된 서브단말(22)에 대응되는 추가노드를 생성하고, 상기 그룹키(30)의 트리구조에서 하나의 리프노드를 제외하고, 상기 추가노드와 상기 제외된 리프노드를 자식노드로 하는 중간노드를 생성하고, 상기 중간노드를 상기 제외된 리프노드가 있었던 위치에 연결한다.
- [0083] 도 5에서, 추가되는 서브단말(22)에 대응되는 추가노드는 $K_{4,2}$ 이고, 추가하려고 하는 위치는 서브단말 노드인 $K_{3,8}$ 이다. 추가노드 $K_{4,2}$ 를 추가하여 2진 트리를 만들기 위해서는, 서브단말 노드 $K_{3,8}$ 의 위치에 새로운 중간노드 $K'_{3,8}$ 을 추가하고, 서브단말 노드 $K_{3,8}$ 과 추가노드 $K_{4,2}$ 를 새로운 중간노드 $K'_{3,8}$ 의 자식노드로 추가한다. 따라서 표기상 서브단말 노드 $K_{3,8}$ 은 서브단말 노드 $K_{4,1}$ 로 표기된다.

- [0084] 한편, 도 6에서 보는 바와 같이, 상기 (d2)단계에서, 상기 서브단말(22)이 삭제되면, 상기 마스터 단말(21)은, 삭제된 서브단말(22)에 대응되는 노드를 상기 그룹키(30)의 트리구조에서 삭제하고, 상기 삭제된 노드의 형제노드를 상기 삭제된 노드의 부모노드에 대치한다.
- [0085] 도 6에서, 삭제되는 서브단말(22)에 대응되는 삭제노드는 $K_{4,2}$ 이다. 삭제노드 $K_{4,2}$ 를 삭제하면, 중간노드 $K_{3,8}$ 의 자식노드가 서브단말 노드 $K_{4,1}$ 한 개만 남는다. 따라서 혼자 남은 서브단말 노드 $K_{4,1}$ 을 중간노드 $K_{3,8}$ 의 위치로 대치한다. 표기상 대치된 서브단말 노드 $K_{4,1}$ 은 $K'_{3,8}$ 로 표기된다.
- [0086] 앞서 서브단말(22)이 삭제 또는 추가될 때, 삭제 또는 추가되는 서브단말(22)에 연결된 원격단말(23)은 그대로 상기 서브단말(22)에 연결된다. 따라서 서브추가 또는 삭제되는 서브단말 노드(32)의 자식노드들인 원격단말 노드(33)들도 그대로 연결된다. 도 5와 도 6에서 서브단말 노드(32)의 자식노드는 표시하지 않았으나, 자식노드는 그대로 서브단말 노드(32)를 따라 이동된다.
- [0087] 상기 (d3)단계는, 상기 추가 또는 삭제된 노드에서 루트노드까지의 경로에 있는 노드들의 공유키를 다시 생성하는 단계(S43)이다.
- [0088] 그룹키(30)의 트리구조가 변경되면, 변경된 것에 따라 각 노드의 공유키를 다시 생성한다. 생성방법은 앞서 (b)단계와 유사하다. 다만, 공유키를 재생성하는 노드는 추가 또는 삭제된 노드에서 루트노드까지의 경로에 있는 노드들이다. 각 노드는 모든 자식노드의 공유키를 해시하기 때문이다.
- [0089] 예를 들면, 도 5 또는 도 6에서 중간노드 공유키인 $K_{1,1}$ 의 자식노드들의 공유키는 변함이 없으므로, 갱신할 필요가 없다. 그러나 공유키 $K_{1,1}$, $K_{1,2}$, $K_{2,4}$, 등 루트노드까지의 경로상의 공유키는 갱신된다.
- [0090] 상기 (e)단계는, 상기 원격단말(23) 또는 서브단말(22)은 다시 생성된 공유키를 수신하여 저장하는 단계이다 (S50). 특히, 상기 (e)단계에서, 상기 마스터 단말(21)은 다시 생성된 공유키를 다시 생성된 공유키로 암호화하여 원격단말(23) 또는 서브단말(22)에게 멀티캐스팅하고, 상기 원격단말(23) 또는 서브단말(22)은 암호화된 공유키를 수신하고 복호화하여 저장한다.
- [0091] 마스터 단말(21)은 갱신된 공유키를 그 키의 이전 공유키로 암호화하여 멀티캐스팅 한다. 그리고 갱신된 공유키들을 새로운 노드의 공유키와 새로운 노드의 형제 노드의 공유키로 각각 암호화하여 새로 추가된 서브단말(22) 또는 원격단말(23)과 그 형제 노드에게 유니캐스팅 한다.
- [0092] 다음으로, 본 발명의 제2 실시예에 따른 SCADA 시스템 통신 환경의 공유키 관리방법을 도 7을 참조하여 설명한다.
- [0093] 도 7에서 보는 바와 같이, 본 발명의 제2 실시예에 따른 키 관리방법은 (a) 마스터 단말 또는 서브단말은 비밀키를 생성하여 서브단말 또는 원격단말에게 할당하는 단계(S60); (b) 마스터 계층 그룹과 서브계층 그룹 각각의 그룹키를 트리구조로 생성하되, 그룹키의 각 노드의 공유키는 모든 자식노드의 공유키들을 해시하여 생성되고, 그룹키의 리프노드의 공유키는 서브단말 또는 원격단말의 비밀키로 정해지는 단계(S70); (c) 상기 원격단말 또는 서브단말은 자신과 대응되는 노드에서 루트 노드까지의 공유키를 수신하여 저장하는 단계(S80); (d) 상기 원격단말 또는 서브단말이 추가 또는 삭제되면, 상기 마스터 단말 또는 서브단말은 상기 추가 또는 삭제되는 단말에 대응되는 노드에서 루트 노드까지의 경로에 있는 노드들의 공유키를 다시 생성하는 단계(S90); (e) 상기 원격단말 또는 서브단말은 다시 생성된 공유키를 수신하여 저장하는 단계(S100)로 구성된다.
- [0094] 앞서 본 바와 같이, 본 발명에 따른 제2 실시예는 마스터 단말(21)과 이에 속하는 서브단말(22)의 그룹인 "마스터 계층 그룹"과, 서브단말(22)과 이에 속하는 원격단말(23)의 그룹인 "서브계층 그룹"으로 나누어 공유키를 관리한다.
- [0095] 마스터 계층 그룹에서는 마스터 단말(21)이 주체적으로 공유키를 관리하고, 서브계층 그룹에서는 서브단말(22)이 주체적으로 공유키를 관리한다. 각 그룹에서 그룹키의 공유키를 관리하는 방식은 동일하다. 또한, 그룹키의 관리방식은 제1 실시예의 마스터 단말 노드에서 서브단말 노드까지의 트리구조를 관리하는 방식과 거의 유사하다. 따라서 이하에서, 앞서 설명된 제1 실시예를 참조하여 설명한다.
- [0096] 상기 (a)단계는, 상기 마스터 단말(21)이 다수의 비밀키를 생성하여 상기 서브 단말(22)에게 각각 할당하고, 상기 서브 단말(22)은 다수의 비밀키를 생성하여 자신에게 속하는 원격 단말(23)에게 각각 할당하는 단계이다

(S60).

- [0097] 상기 (b)단계는, 마스터 단말(21)이 서브단말(22)의 그룹키를 트리구조로 생성하고 상기 서브단말(22)도 자신에게 속하는 원격단말(23)의 그룹키를 트리구조로 생성하는 단계이다(S70). 다만, 상기 트리구조의 리프노드는 각 원격단말(23) 또는 각 서브단말(22)과 대응되고, 상기 그룹키의 각 노드의 공유키는 모든 자식노드의 공유키들을 해시하여 생성되고, 상기 그룹키의 리프노드의 공유키는 상기 원격단말(23) 또는 각 서브단말(22)의 비밀키로 정해지는 단계이다(S70).
- [0098] 이때, 트리구조는 2진 트리이다. 상기 계층 그룹으로 분리된 그룹키의 트리구조가 도 8에 도시되고 있다.
- [0099] 도 8에서 보는 바와 같이, 마스터 단말 노드 $K_{0,1}$ 을 루트노드(41)로 하는 마스터 계층 그룹키(40)와, 서브단말 노드 $K_{0,1}^1, K_{0,1}^2, \dots, K_{0,1}^m$ 을 각각 루트노드(52)로 하는 서브계층 그룹키(50)로 분리된다. 서브계층 그룹키(50)는 서브단말(22)의 개수만큼 만들어진다.
- [0100] 그룹키를 생성하는 방법은 다음과 같다. 앞서 (a)단계에서 마스터 단말(21)은 모든 서브단말(22)에게 비밀키를 할당하며, 각 서브단말(22)은 자신의 비밀키를 알고 있다. 이 비밀키 구조에서 다른 노드의 공유키 값 $K_{i+1, \lceil j/2 \rceil}$ if $(1 \leq i \leq h-1, 1 \leq j \leq m)$ 은 상기 [수식 2]와 같이 자식 노드의 두 해시값(공유키)을 해시함으로써 생성된다. 따라서 위의 식에 따라 이진 트리 형태의 키 구조가 형성되며 루트노드의 공유키 $K_{0,1}$ 가 생성된다.
- [0101] 서브단말(22)과 원격단말(23) 사이의 그룹키 구조도 위의 방법과 동일하게 형성된다. 앞서 (a)단계에서 서브단말(22)은 각 원격단말(23)에게 비밀키를 할당하며, 각 원격단말(23)은 자신의 키를 알고 있다. 서브단말(22)과 원격단말(23) 사이의 공유키 구조는 2진 트리를 형성하며, 각 노드의 공유키 값 $K_{i+1, \lceil j/2 \rceil}$ if $(1 \leq i \leq h-1, 1 \leq j \leq m)$ 은 상기 [수식 2]와 같이 자식 노드의 두 공유키(해시값)을 해시함으로써 생성된다.
- [0102] 상기 (c)단계는 상기 서브단말(22) 또는 원격단말(23)은 자신과 대응되는 노드에서 루트 노드까지의 공유키를 수신하여 저장하는 단계이다(S80).
- [0103] 제2 실시예에 따른 공유키 구조에서 서브단말(22)은 자신의 노드부터 마스터 단말 노드(41)인 루트 노드까지의 경로에 있는 모든 노드의 공유키 값과 자신이 관리하는 모든 원격단말(23)의 공유키를 저장하게 된다. 즉, 서브단말(22)의 개수가 m개이고, 하나의 서브단말(22)이 관리하는 원격단말(23)의 개수가 n개일 경우, $1 + n + \log_2 m$ 개의 공유키를 저장한다. 원격단말(23)은 자신의 관리하는 서브단말(22)의 노드인 루트 노드까지의 경로에 있는 모든 노드의 공유키 값을 저장한다. 즉, 하나의 서브단말(22)이 관리하는 원격단말(23)의 개수가 n개 일 경우, $1 + \log_2 n$ 개의 공유키를 저장하게 된다.
- [0104] 상기 (d)단계는, 서브단말(22) 또는 원격단말(23)이 추가 또는 삭제되면, 상기 마스터 단말(21) 또는 서브단말(22)은 추가 또는 삭제된 단말에 대응되는 노드에서 루트 노드까지의 경로에 있는 노드들의 공유키를 다시 생성하는 단계이다(S90).
- [0105] 특히, 상기 (d)단계는, (d1) 원격단말(23) 또는 서브단말(22)이 추가 또는 삭제되면, 상기 추가 또는 삭제된 원격단말(23) 또는 서브단말(22)에 대응되는 노드를, 상기 그룹키(40, 50)의 트리구조에서 추가 또는 삭제하고, 상기 그룹키(40, 50)의 트리구조를 2진트리로 재구성하는 단계와, (d2) 상기 추가 또는 삭제된 노드에서 루트노드까지의 경로에 있는 노드들의 공유키를 다시 생성하는 단계로 나뉜다.
- [0106] 한편, 제2 실시예에서, 서브단말(22) 또는 원격단말(23)이 추가 또는 삭제될 때, 그룹키의 공유키를 재생성하는 방법은 앞서 설명한 제1 실시예에서 서브단말(22)이 추가 또는 삭제될 때의 공유키 재생성 방법과 동일하다.
- [0107] 즉, 상기 (d2)단계에서, 상기 서브단말(22) 또는 원격단말(23)이 추가되면, 상기 마스터 단말(21) 또는 서브단말(22)은, 추가된 서브단말(22) 또는 원격단말(23)에 대응되는 추가노드를 생성하고, 상기 그룹키의 트리구조에서 하나의 리프노드를 제외하고, 상기 추가노드와 상기 제외된 리프노드를 자식노드로 하는 중간노드를 생성하고, 상기 중간노드를 상기 제외된 리프노드가 있었던 위치에 연결한다.
- [0108] 또, 상기 (d2)단계에서, 상기 서브단말(22) 또는 원격단말(23)이 삭제되면, 상기 마스터 단말(21) 또는 서브단말(22)은, 삭제된 서브단말(22) 또는 원격단말(23)에 대응되는 노드를 상기 그룹키의 트리구조에서 삭제하고,

상기 삭제된 노드의 형제노드를 상기 삭제된 노드의 부모노드에 대치한다.

[0109] 상기 (e)단계도, 제1 실시예와 마찬가지로, 상기 마스터 단말(21) 또는 서브단말(22)은 다시 생성된 공유키를 다시 생성전 공유키로 암호화하여 서브단말(22) 또는 원격단말(23)에게 멀티캐스팅하고, 상기 서브단말(22) 또는 원격단말(23)은 암호화된 공유키를 수신하고 생성전 공유키로 복호화하여 저장한다.

[0110] 다음으로, 본 발명에 따른 SCADA 시스템 통신 환경의 세션키 생성방법 및 메시지 통신방법을 설명한다.

[0111] 본 발명에 따른 메시지 통신방법은 다수의 장치로 메시지를 전송할 경우, 다수의 장치가 그룹키 계층 구조를 통해 공유한 키를 통해 세션키를 생성하고, 그 세션키로 메시지를 암호화 하여 전송한다. 세션키는 기본적으로 타임스탬프와 시퀀스 번호가 결합된 TVP와 그룹키 구조에서 통신하는 장치들 간의 공유한 키를 이용하여 생성된다. TVP는 재생 공격으로부터 세션키를 보호하기 위해 사용된다. 송신 장치 i 가 다수의 수신장치 그룹 j 와 통신할 경우, 세션키 $SK_{i,j}$ 는 [수식 3]과 같이 공유한 키 $K_{u,v}$ 와 TVP를 해시함으로써 생성된다.

[0112] [수식 3]

[0113] $SK_{i,j} = H(K_{u,v}, TVP)$

[0114] 송신 장치 i 가 하나의 수신 장치 j 와 통신할 경우, 세션키 $SK_{i,j}$ 는 위의 식과 구별 되도록 각 장치의 ID를 추가 하여 [수식 4]와 같이 공유한 키 $K_{u,v}$ 와 TVP, 송신 장치의 ID, 수신 장치의 ID를 해시함으로써 생성된다.

[0115] [수식 4]

[0116] $SK_{i,j} = H(K_{u,v}, ID_i, ID_j, TVP)$

[0117] 본 발명에 따른 세션키 생성 방법은 [수식 3]과 [수식 4]에 제한적이지 않으며, 추가적인 요소가 더해져서 생성될 수 있다.

[0118] 본 발명에 따른 메시지 통신방법은 Iolus 프레임워크를 적용할 수 있다. Iolus 프레임워크를 적용할 경우, 메시지 암호화를 위한 연산량을 줄일 수 있다. Iolus 프레임워크를 적용한 통신 방법은 다음과 같다. 먼저 마스터 단말(21)은 GSC(Group Security Controller)의 역할을 담당하게 되고, 서브단말(22)은 GSI(Group Security Intermediary) 역할을 담당하게 된다.

[0119] 따라서 모든 전송 메시지는 서브단말(22)을 통해서 전송된다. 송신 장치는 메시지를 랜덤한 키로 암호화 하고, 그 랜덤한 암호화 키는 송신 장치와 서브단말(22)이 공유한 세션키로 암호화 하여 서브단말(22)로 전송한다. 서브단말(22)은 암호화된 메시지와 암호화된 키를 수신한 뒤, 송신 장치와 공유한 세션키로 암호화된 키를 복호화 하고, 그 키를 수신 장치와 공유한 세션키로 재암호화 하여 수신 장치로 전송한다. 이 때, 세션키가 그룹키 계층 구조를 통해 특정 다수의 수신 장치와 공유한 세션키인 경우, 해당 수신 장치만 암호화된 키를 복호화 하고, 그 키로 메시지를 복호화 할 수 있다.

[0120] 다음으로, 본 발명에 따른 공유키 관리방법과 이를 이용한 메시지 통신방법의 효과를 도 9를 참조하여 설명한다.

[0121] 본 발명에 따른 키 관리 방법 및 통신 방법을 사용할 경우, 도면 9a와 도면 9b와 같이 SKE나 SKMA 방식 보다 더 높은 효율성을 갖게 된다. 도면 9a와 도면 9b에서 C_E 는 하나의 메시지를 암호화하는데 드는 연산량이며, C_{Ek} 는 하나의 키를 암호화하는데 드는 연산량, p 는 멀티캐스팅 메시지를 받을 서브단말(22)의 개수, q 는 멀티캐스팅 메시지를 받을 원격단말(23)의 개수, X 는 $1 \leq X \leq \min(m/2, p)$ 인 마스터 단말(21)이 멀티캐스팅 메시지 암호화에 사용할 키의 개수, Y 는 $1 \leq Y \leq \min(n/2, q)$ 인 서브단말(22)이 멀티캐스팅 메시지 암호화에 사용할 키의 개수이다.

[0122] 이상, 본 발명자에 의해서 이루어진 발명을 상기 실시 예에 따라 구체적으로 설명하였지만, 본 발명은 상기 실시 예에 한정되는 것은 아니고, 그 요지를 이탈하지 않는 범위에서 여러 가지로 변경 가능한 것은 물론이다.

산업이용 가능성

[0123] 본 발명은 SCADA 시스템에서 암호화 통신으로 메시지를 송수신하는 시스템을 개발하는 데 적용이 가능하다. 특히, 본 발명은 SCADA 시스템에서 암호화 통신을 브로드캐스팅이나 멀티캐스팅 통신으로 할 수 있는 효율적인 암호화 통신시스템을 개발하는 데 유용하다.

도면의 간단한 설명

[0124] 도 1은 본 발명을 실시하기 위한 SCADA 시스템의 전체 구성을 도시한 도면이다.

[0125] 도 2는 본 발명의 제1 실시예에 따른 SCADA 시스템 통신 환경의 공유키 관리방법을 설명한 흐름도이다.

[0126] 도 3은 본 발명의 제1 실시예에 따라 생성한 그룹키의 트리구조를 예시한 도면이다.

[0127] 도 4는 본 발명의 제1 실시예에 따라 원격단말 또는 서브단말이 추가 또는 삭제될 때의 공유키 재생성 단계를 설명하는 흐름도이다.

[0128] 도 5는 본 발명의 제1 실시예에 따라 서브단말이 추가될 때, 그룹키의 트리구조를 재구성하는 일례를 도시한 도면이다.

[0129] 도 6은 본 발명의 제1 실시예에 따라 서브단말이 삭제될 때, 그룹키의 트리구조를 재구성하는 일례를 도시한 도면이다.

[0130] 도 7은 본 발명의 제2 실시예에 따른 SCADA 시스템 통신 환경의 공유키 관리방법을 설명한 흐름도이다.

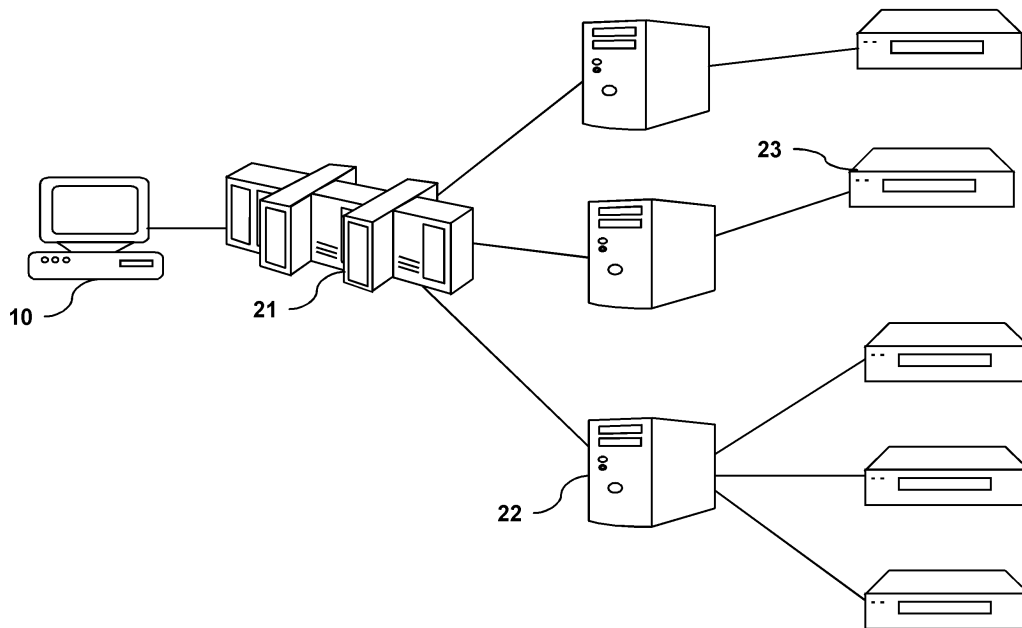
[0131] 도 8은 본 발명의 제2 실시예에 따라 생성한 그룹키의 트리구조를 예시한 도면이다.

[0132] * 도면의 주요 부분에 대한 부호의 설명 *

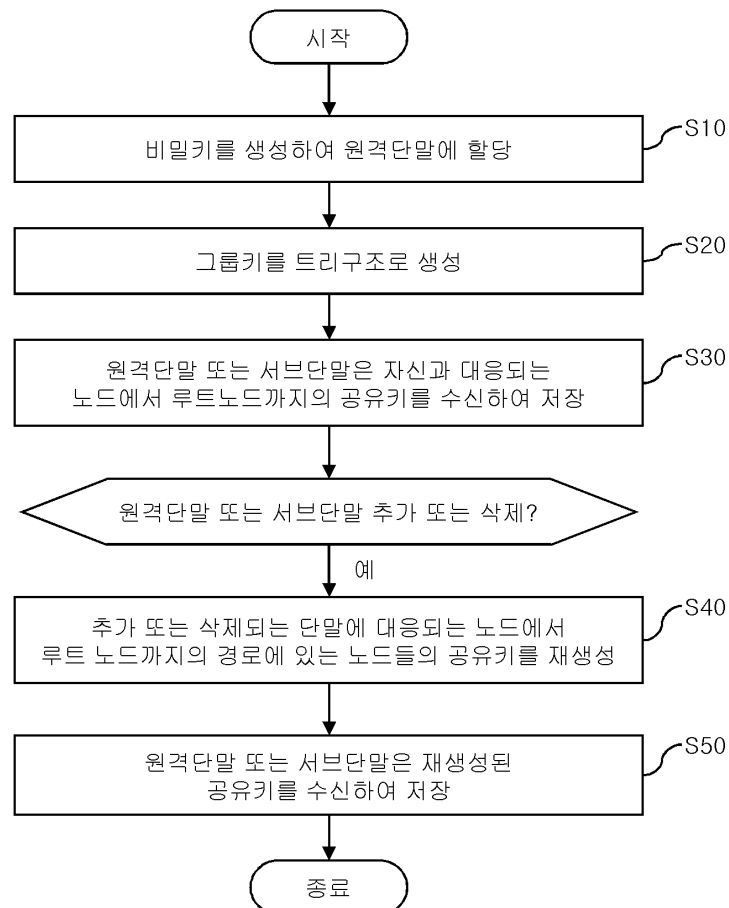
[0133]	10 : HMI 단말	21 : 마스터 단말
[0134]	22 : 서브 단말	23 : 원격 단말
[0135]	30 : 그룹키	31, 41 : 마스터 단말 노드
[0136]	32, 42, 52 : 서브 단말 노드	33, 53 : 원격 단말 노드
[0137]	34, 44, 54 : 중간노드	

도면

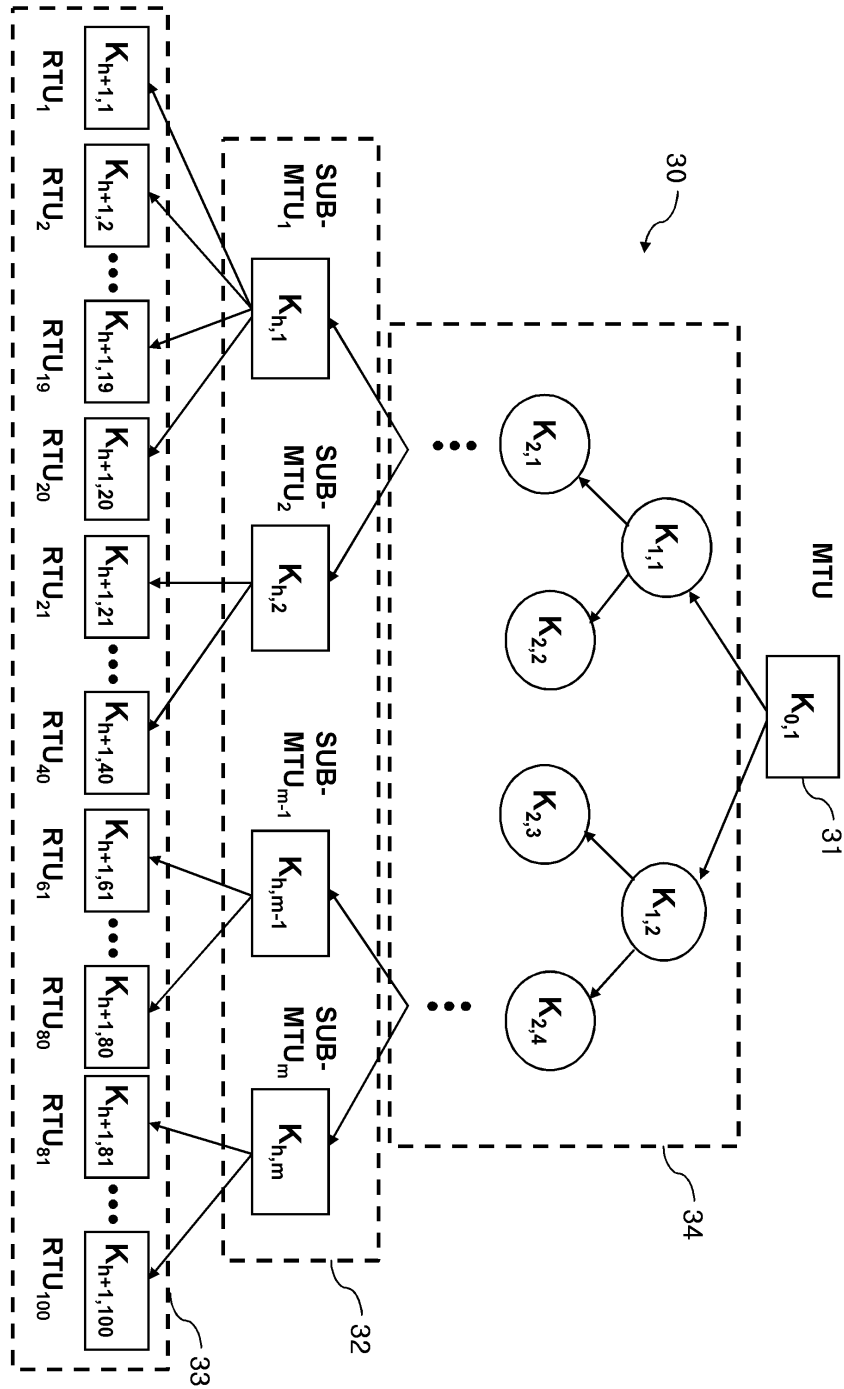
도면1



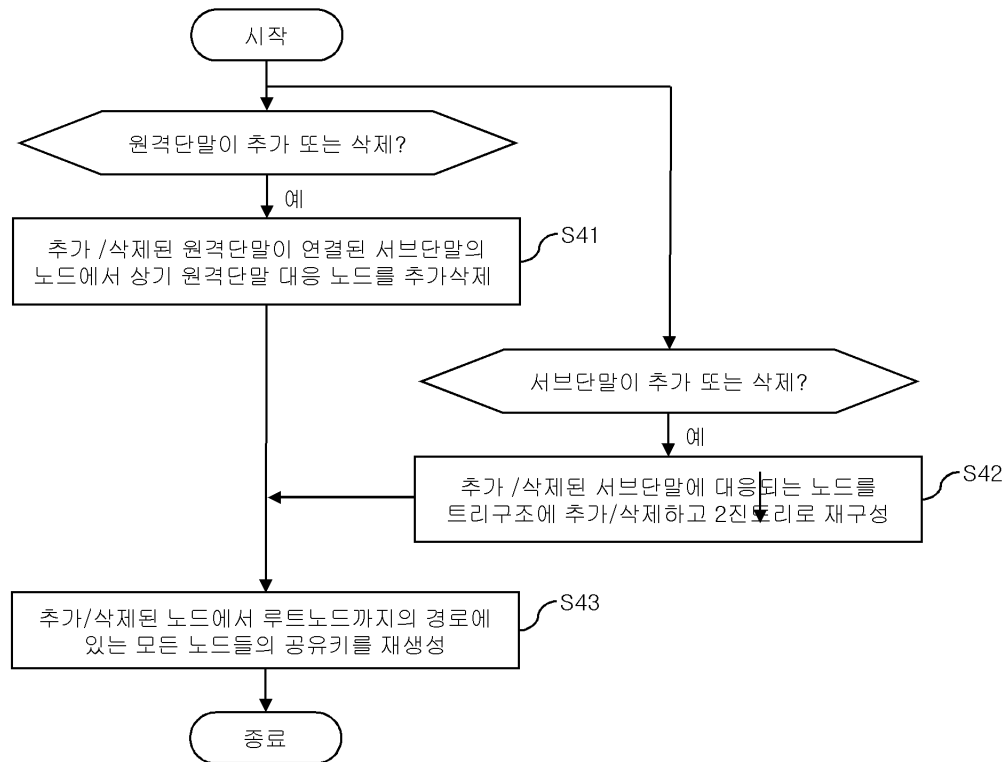
도면2



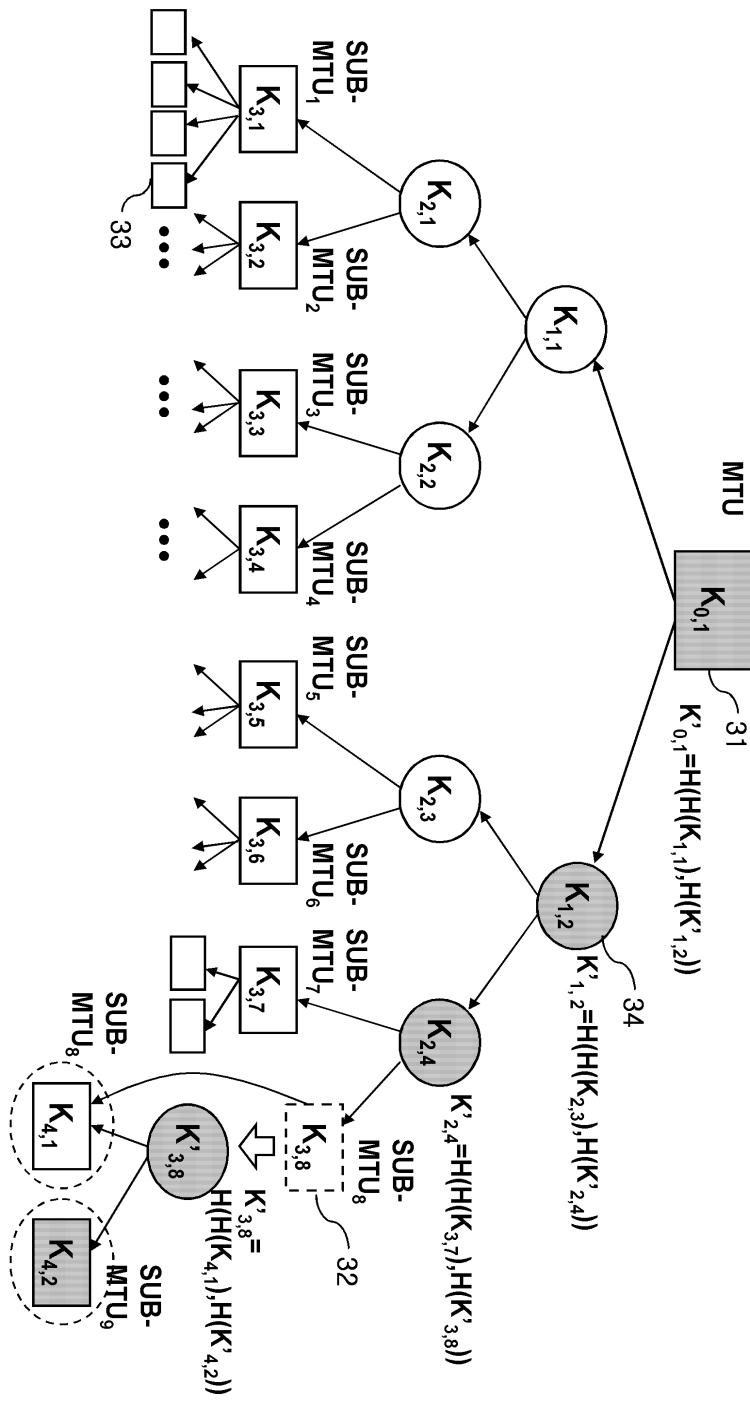
도면3



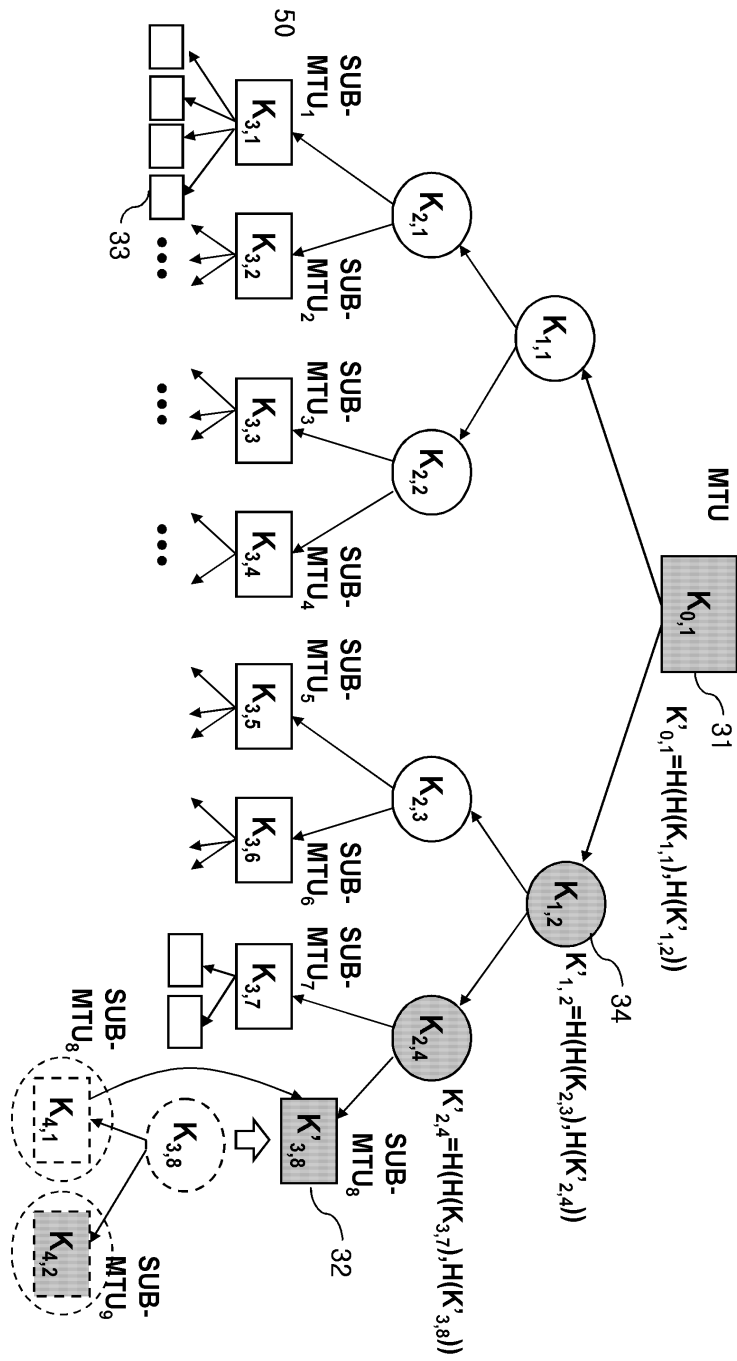
도면4



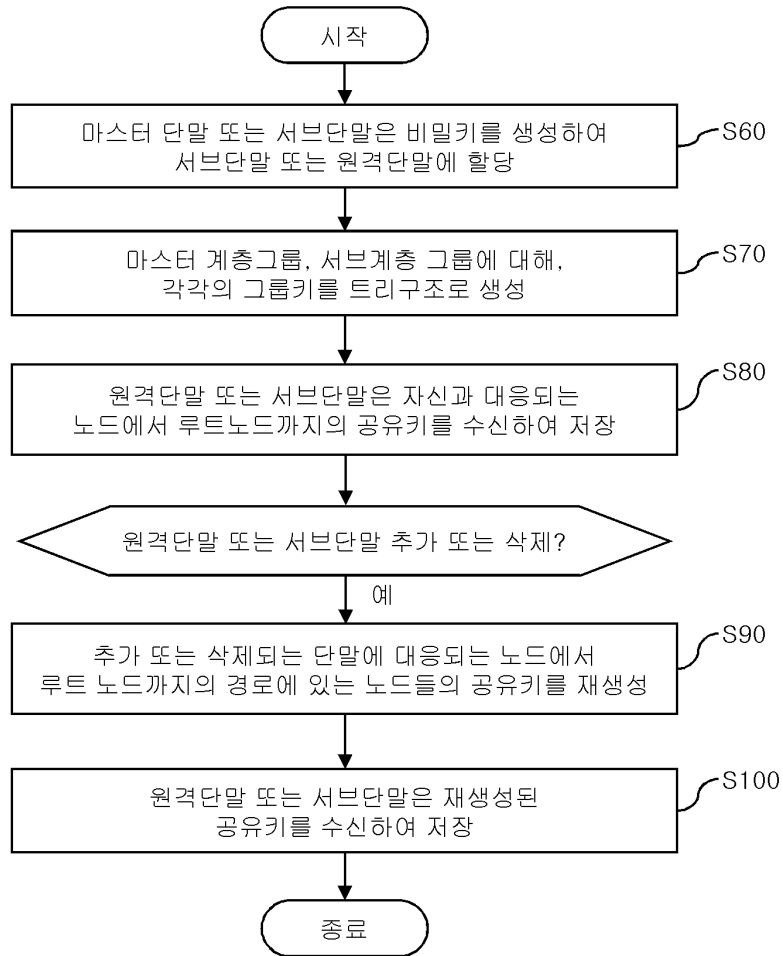
도면5



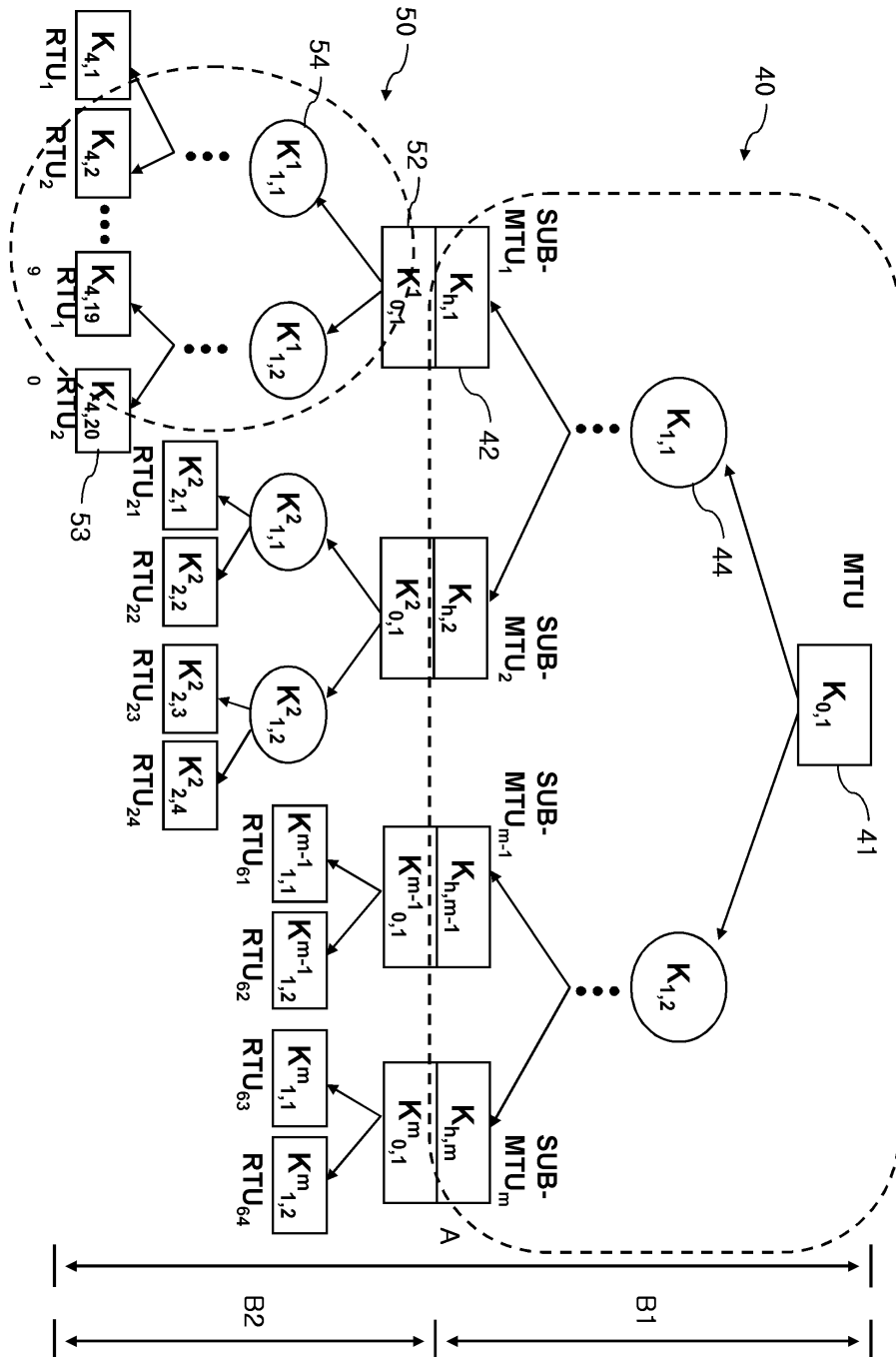
도면6



도면7



도면8



도면9a

멀티캐스팅 통신 시 MTU와 SUB-MTU에서의 연산량

	SKE 또는 SKMA	방법 1 (Iolus 프레임워크 사용 없음)	방법 2 (Iolus 프레임워크 사용)
MTU	pC_E	XC_E	$C_E + XC_{E_K}$
SUB-MTU	qC_E	$(q \bmod (n-1))C_E$	$(Y+1)C_{E_K}$

C_E : 하나의 메시지를 암호화하는데 드는 연산량

C_{E_K} : 하나의 키를 암호화하는데 드는 연산량

m : MTU에 연결된 SUB-MTU의 총 개수

n : 하나의 SUB-MTU에 연결된 RTU의 총 개수

p : 멀티캐스팅 메시지를 받을 SUB-MTU 장치의 개수

q : 멀티캐스팅 메시지를 받을 RTU 장치의 개수

X : MTU가 멀티캐스팅 메시지 암호화에 사용할 키의 개수, $1 \leq X \leq \min(m/2, p)$

Y : SUB-MTU가 멀티캐스팅 메시지 암호화에 사용할 키의 개수, $1 \leq Y \leq \min(n/2, q)$

도면9b

MTU와 SUB-MTU, RTU에서 저장하는 키의 수

	SKE 또는 SKMA	방법 1 (Iolus 프레임워크 사용 없음)	방법 2 (Iolus 프레임워크 사용)
MTU	mn	$2m-1+mn$	m
SUB-MTU	$1+n$	$1+\log_2 m$	$1+n+\log_2 m$
RTU	1	$2+\log_2 m$	$1+\log_2 n$