



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2011-0079408

(43) 공개일자 2011년07월07일

(51) Int. Cl.

H04L 9/08 (2006.01) *H04L 9/16* (2006.01)

(21) 출원번호 10-2010-0006103

(22) 출원일자 2010년01월22일

심사청구일자 2010년01월22일

(30) 우선권주장

1020090135388 2009년12월31일 대한민국(KR)

(71) 출원인

충남대학교산학협력단

대전 유성구 궁동 220 충남대학교

(72) 발명자

최동현

경기도 수원시 장안구 천천동 300 성균관대학교
정보통신공학부

원동호

경기도 수원시 장안구 천천동 300 성균관대학교
정보통신공학부

(뒷면에 계속)

(74) 대리인!

특허법인정직과특허

전체 청구항 수 : 총 11 항

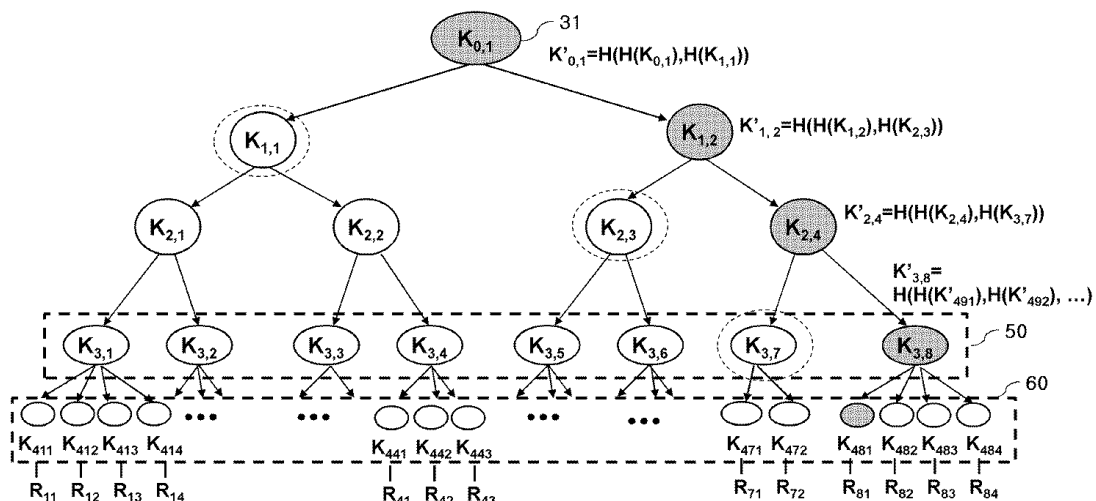
(54) SCADA 시스템 통신 환경에 효율적인 키 관리 방법

(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, 상기 마스터 단말은 그룹키의 공유키들을 트리구조로 생성하되, 상기 트리구조는 상기 마스터 단말에 대응되는 루트노드에서 상기 서브단말에 대응되는 중간노드까지 이진트리로 구성되는 제1 단계; 상기 서브단말은 자신의 중간노드의 하위노드 및 상위노드의 공유키를 저장하는 제2 단계; 중간노드의 공유키가 갱신되면, 갱신되는 중간노드에서 루트노드까지의 경로에 있는 노드(이하 경로상 노드)들의 공유키를 모두 갱신하되, 상기 경로상 노드의 공유키는 자신의 공유키와 경로에 있지 않는 자식노드의 공유키로 갱신되는 제3 단계를 포함하는 구성을 마련한다.

상기와 같은 SCADA 시스템 통신 환경의 공유키 관리방법에 의하여, 메시지를 암호화하여 메시지 브로드캐스팅 또는 멀티캐스팅을 지원하면서 키분배를 위한 연산량을 분산하고 통신량을 줄일 수 있다.

대표도



(72) 발명자

김승주

경기도 수원시 장안구 천천동 300 성균관대학교 정
보통신공학부

류재철

대전광역시 유성구 어은동 한빛아파트 132-801

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,

상기 마스터 단말은 그룹키의 공유키들을 트리구조로 생성하되, 상기 트리구조는 상기 마스터 단말에 대응되는 루트노드에서 상기 서브단말에 대응되는 중간노드까지 이진트리로 구성되는 제1 단계;

상기 서브단말은 자신의 중간노드의 하위노드 및 상위노드의 공유키를 저장하는 제2 단계;

중간노드의 공유키가 갱신되면, 갱신되는 중간노드에서 루트노드까지의 경로에 있는 노드(이하 경로상 노드)들의 공유키를 모두 갱신하되, 상기 경로상 노드의 공유키는 자신의 공유키와 경로에 있지 않는 자식노드의 공유키로 갱신되는 제3 단계를 포함하는 것을 특징으로 하는 SCADA 시스템 통신 환경의 공유키 관리방법.

청구항 2

제1항에 있어서,

상기 제3 단계는, 상기 경로상 노드의 형제노드 각각에 대하여, 상기 형제노드 또는 상기 형제노드의 하위노드에 대응되는 서브단말은 상기 형제노드의 부모노드의 갱신된 공유키를 직접 계산하고, 상기 부모노드의 상위노드의 공유키를 상기 마스터 단말로부터 수신하는 것을 특징으로 하는 SCADA 시스템 통신 환경의 공유키 관리방법.

청구항 3

제1항에 있어서,

제1단계에서, 상기 트리구조는 각 서브단말의 중간노드에서 상기 서브단말에 속하는 원격단말의 리프노드(원격단말에 대응되는 리프노드)까지 n차 트리로 구성되고,

제2단계에서, 상기 원격단말은 자신의 리프노드의 상위노드의 공유키를 저장하는 것을 특징으로 하는 SCADA 시스템 통신 환경의 공유키 관리방법.

청구항 4

제2항에 있어서,

제3단계에서, 상기 경로상 노드의 형제노드 각각에 대하여, 상기 형제노드의 하위노드에 대응되는 원격단말은 상기 형제노드의 부모노드의 갱신된 공유키를 직접 계산하고, 상기 부모노드의 상위노드의 공유키를 상기 마스터 단말 또는 서브단말로부터 수신하는 것을 특징으로 하는 SCADA 시스템 통신 환경의 공유키 관리방법.

청구항 5

제1항 내지 제4항 중 어느 한 항에 있어서,

제2단계에서, 상기 공유키는 상기 마스터 단말로부터 수신되어 저장되는 것을 특징으로 하는 SCADA 시스템 통신 환경의 공유키 관리방법.

청구항 6

제1항 내지 제4항 중 어느 한 항에 있어서,

제3단계에서, 상기 원격단말이 추가 또는 삭제되면, 상기 원격단말을 연결한 서브단말의 중간노드의 공유키가 갱신되는 것을 특징으로 하는 SCADA 시스템 통신 환경의 공유키 관리방법.

청구항 7

제1항 내지 제4항 중 어느 한 항에 있어서,

상기 각 경로상 노드의 공유키는 자신의 공유키와 경로에 있지 않는 자식노드의 공유키를 해시하여 계산되는 것을 특징으로 하는 SCADA 시스템 통신 환경의 공유키 관리방법.

청구항 8

제1항 내지 제4항 중 어느 한 항의 SCADA 시스템 통신 환경의 공유키 관리방법을 기록한 컴퓨터로 읽을 수 있는 기록매체.

청구항 9

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

상기 마스터 단말은 그룹키의 공유키들을 트리구조로 생성하되, 상기 트리구조는 상기 마스터 단말에 대응되는 루트노드에서 상기 서브단말에 대응되는 중간노드까지 이진트리로 구성되는 제1 단계;

상기 서브단말은 자신의 중간노드의 하위노드 및 상위노드의 공유키를 저장하는 제2 단계;

중간노드의 공유키가 갱신되면, 갱신되는 중간노드에서 루트노드까지의 경로에 있는 노드(이하 경로상 노드)들의 공유키를 모두 갱신하되, 상기 경로상 노드의 공유키는 자신의 공유키와 경로에 있지 않는 자식노드의 공유키로 갱신되는 단계; 및

상기 마스터 단말은 상기 트리구조의 노드를 선택하여, 선택한 노드의 하위노드에 대응되는 서브단말 및 원격단말과 통신하기 위한 세션키를 상기 선택한 노드의 공유키로 생성하는 제4 단계를 포함하는 것을 특징으로 하는 SCADA 시스템 통신 환경의 세션키 생성방법.

청구항 10

제9항에 있어서,

제1단계에서, 상기 트리구조는 각 서브단말의 중간노드에서 상기 서브단말에 속하는 원격단말의 리프노드(원격단말에 대응되는 리프노드)까지 n차 트리로 구성되고,

제2단계에서, 상기 원격단말은 자신의 리프노드의 상위노드의 공유키를 저장하고,

제4단계에서, 상기 서브단말은 자신에 속하는 원격단말과 통신을 위한 세션키를 자신의 중간노드의 공유키로 생성하는 것을 특징으로 하는 SCADA 시스템 통신 환경의 세션키 생성방법.

청구항 11

제10항에 있어서,

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

명세서

기술분야

[0001] 본 발명은 마스터 단말(MTU), 다수의 서브단말(SUB-MTU), 다수의 원격단말(RTU)이 순차적인 계층으로 구성된 SCADA(Supervisory Control And Data Acquisition) 시스템에서, 그룹키의 공유키를 트리구조로 생성하고, 원격 단말 또는 서브단말이 자신에 해당하는 노드의 상위노드 및 하위노드의 공유키를 공유하는 SCADA 시스템 통신 환경의 공유키 관리방법 및 세션키 생성방법에 관한 것이다.

[0002] 특히, 본 발명은 SCADA 시스템의 그룹키를 이진트리구조로 생성하되, 중간노드의 공유키가 갱신되면 갱신되는 중간노드에서 루트노드까지의 경로상 노드의 공유키를 모두 갱신하되, 상기 경로상 노드의 공유키는 자신의 공유키와 경로에 있지 않는 자식노드의 공유키로 갱신되는 SCADA 시스템 통신 환경의 공유키 관리방법 및 세션키 생성방법에 관한 것이다.

배경기술

[0003] 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.

[0004] 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.

[0005] 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.

[0006] 이를 해결하고자, 계층구조를 가지는 논리키를 통해 이를 해결하는 SCADA 시스템의 안전한 통신환경을 위하여 개선된 키 관리 기술이 본 출원인에 의하여, [한국특허출원 10-2009-0004213, "SCADA시스템 통신 환경에 효율적인 키 관리 및 통신 방법"] (이하 선행기술 1)에 제시되고 있다.

[0007] 도 5에서 보는 바와 같이, 상기 선행기술 1은 SCADA시스템의 그룹키의 공유키들을 트리구조(1)로 관리한다. 마스터 단말(MTU)에 대응되는 루트노드(2)에서 서브단말(SUB-MTU)에 대응되는 중간노드(3)까지 이진트리구조를 가지는 공유키들을 구성한다. 또, 상기 트리구조는 중간노드(3)에서 리프노드(4)까지 n차 트리로 구성되고, 리프노드(4)는 원격단말에 대응된다.

[0008] 이때, 서브단말(SUB-MTU)의 중간노드(3)의 공유키가 변경되면, 상기 트리구조(1)에서 중간노드(3)에서 루트노드(2)까지의 경로상의 공유키들이 모두 갱신되어야 한다. 예를 들어, 중간노드 $K_{3,8}$ 의 공유키가 변경되면 그 상위 경로의 노드들($K_{0,1}, K_{1,2}, K_{2,4}$)도 모두 변경되어야 한다.

[0009] 이때, 경로상의 각 노드들 $K_{0,1}, K_{1,2}, K_{2,4}, K_{3,8}$ 의 공유키는 자신의 자식노드의 공유키들을 이용하여 갱신된다. 예를 들어, 노드 $K_{1,2}$ 의 공유키는 노드 $K_{2,3}$ 과 노드 $K_{2,4}$ 의 공유키들을 해시하여 계산된다. 이때 노드 $K_{2,4}$ 의 공유키로서 갱신된 공유키인 $K'_{2,4}$ 가 이용된다.

[0010] 그러나 상기 선행기술 1에 의하면, 경로상 이외의 노드들, 예를 들어 도 5의 중간노드 $K_{3,1}, K_{3,2}, K_{3,3}, K_{3,4}$ 또는 이들 중간노드에 속하는 원격단말들은 루트노드(2)의 갱신된 공유키 $K'_{0,1}$ 을 알고 있어야 하고, 중간노드 $K_{3,5}, K_{3,6}$ 에 대응되는 서브단말들도 갱신된 공유키 $K'_{0,1}$ 와 $K'_{1,2}$ 를 알고 있어야 한다. 따라서 마스터 단말(MTU)은 갱신

된 공유키 $K'_{0,1}$ 또는 $K'_{1,2}$ 를 각 원격단말 또는 서브단말로 전송해야 한다. 이때, 마스터 단말(MTU)은 갱신된 공유키를 암호화하여 전송하고 각 원격단말 또는 서브단말은 수신한 공유키들을 복호화해야 한다. 따라서 갱신되는 키분배를 위하여 많은 연산량과 통신량이 소모되는 문제점이 있다.

발명의 내용

해결하려는 과제

- [0011] 본 발명의 목적은 상술한 바와 같은 문제점을 해결하기 위한 것으로, SCADA 시스템의 그룹키를 이진트리구조로 생성하되, 공유키가 변경되는 서브단말 노드에서 루트노드까지의 경로상 노드들의 공유키를 경로의 자식노드의 공유키와 자신의 공유키로 갱신하는 SCADA 시스템 통신 환경의 공유키 관리방법 및 세션키 생성방법을 제공하는 것이다.
- [0012] 또, 본 발명의 목적은 각 경로상 노드의 형제노드 또는 상기 형제노드의 하위노드에 위치하는 서브단말 또는 원격단말들이 상기 형제노드의 부모노드인 경로상 노드의 갱신된 공유키를 직접 계산하는 SCADA 시스템 통신 환경의 공유키 관리방법 및 세션키 생성방법을 제공하는 것이다.

과제의 해결 수단

- [0013] 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 키 관리방법에 관한 것으로서, 상기 마스터 단말은 그룹키의 공유키들을 트리구조로 생성하되, 상기 트리구조는 상기 마스터 단말에 대응되는 루트노드에서 상기 서브단말에 대응되는 중간노드까지 이진트리로 구성되는 제1 단계; 상기 서브단말은 자신의 중간노드의 하위노드 및 상위노드의 공유키를 저장하는 제2 단계; 중간노드의 공유키가 갱신되면, 갱신되는 중간노드에서 루트노드까지의 경로에 있는 노드(이하 경로상 노드)들의 공유키를 모두 갱신하되, 상기 경로상 노드의 공유키는 자신의 공유키와 경로에 있지 않는 자식노드의 공유키로 갱신되는 제3 단계를 포함하는 것을 특징으로 한다.
- [0014] 또, 본 발명은 SCADA 시스템 통신 환경의 공유키 관리방법에 있어서, 상기 제3 단계는, 상기 경로상 노드의 형제노드 각각에 대하여, 상기 형제노드 또는 상기 형제노드의 하위노드에 대응되는 서브단말은 상기 형제노드의 부모노드의 갱신된 공유키를 직접 계산하고, 상기 부모노드의 상위노드의 공유키를 상기 마스터 단말로부터 수신하는 것을 특징으로 한다.
- [0015] 또, 본 발명은 SCADA 시스템 통신 환경의 공유키 관리방법에 있어서, 제1단계에서, 상기 트리구조는 각 서브단말의 중간노드에서 상기 서브단말에 속하는 원격단말의 리프노드(원격단말에 대응되는 리프노드)까지 n 차 트리로 구성되고, 제2단계에서, 상기 원격단말은 자신의 리프노드의 상위노드의 공유키를 저장하는 것을 특징으로 한다.
- [0016] 또, 본 발명은 SCADA 시스템 통신 환경의 공유키 관리방법에 있어서, 제3단계에서, 상기 경로상 노드의 형제노드 각각에 대하여, 상기 형제노드의 하위노드에 대응되는 원격단말은 상기 형제노드의 부모노드의 갱신된 공유키를 직접 계산하고, 상기 부모노드의 상위노드의 공유키를 상기 마스터 단말 또는 서브단말로부터 수신하는 것을 특징으로 한다.
- [0017] 또, 본 발명은 SCADA 시스템 통신 환경의 공유키 관리방법에 있어서, 제2단계에서, 상기 공유키는 상기 마스터 단말로부터 수신되어 저장되는 것을 특징으로 한다.
- [0018] 또, 본 발명은 SCADA 시스템 통신 환경의 공유키 관리방법에 있어서, 제3단계에서, 상기 원격단말이 추가 또는 삭제되면, 상기 원격단말을 연결한 서브단말의 중간노드의 공유키가 갱신되는 것을 특징으로 한다.
- [0019] 또, 본 발명은 SCADA 시스템 통신 환경의 공유키 관리방법에 있어서, 상기 각 경로상 노드의 공유키는 자신의 공유키와 경로에 있지 않는 자식노드의 공유키를 해시하여 계산되는 것을 특징으로 한다.
- [0020] 또한, 본 발명은 SCADA 시스템 통신 환경의 공유키 관리방법을 기록한 컴퓨터로 읽을 수 있는 기록매체에 관한

것이다.

[0021] 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 세션키 생성방법에 관한 것으로서, 상기 마스터 단말은 그룹키의 공유키들을 트리구조로 생성하되, 상기 트리구조는 상기 마스터 단말에 대응되는 루트노드에서 상기 서브단말에 대응되는 중간노드까지 이진트리로 구성되는 제1 단계; 상기 서브단말은 자신의 중간노드의 하위노드 및 상위노드의 공유키를 저장하는 제2 단계; 중간노드의 공유키가 갱신되면, 갱신되는 중간노드에서 루트노드까지의 경로에 있는 노드(이하 경로상 노드)들의 공유키를 모두 갱신하되, 상기 경로상 노드의 공유키는 자신의 공유키와 경로에 있지 않는 자식노드의 공유키로 갱신되는 단계; 및 상기 마스터 단말은 상기 트리구조의 노드를 선택하여, 선택한 노드의 하위노드에 대응되는 서브단말 및 원격단말과 통신하기 위한 세션키를 상기 선택한 노드의 공유키로 생성하는 제4 단계를 포함하는 것을 특징으로 한다.

[0022] 또, 본 발명은 SCADA 시스템 통신 환경의 세션키 생성방법에 있어서, 제1단계에서, 상기 트리구조는 각 서브단말의 중간노드에서 상기 서브단말에 속하는 원격단말의 리프노드(원격단말에 대응되는 리프노드)까지 n차 트리로 구성되고, 제2단계에서, 상기 원격단말은 자신의 리프노드의 상위노드의 공유키를 저장하고, 제4단계에서, 상기 서브단말은 자신에 속하는 원격단말과 통신을 위한 세션키를 자신의 중간노드의 공유키로 생성하는 것을 특징으로 한다.

[0023] 또, 본 발명은 SCADA 시스템 통신 환경의 세션키 생성방법에 있어서, 상기 세션키는, 상기 공유키와, 타임스탬프 및 시퀀스 번호가 결합된 값을 해시하여 생성되는 것을 특징으로 한다.

발명의 효과

[0024] 상술한 바와 같이, 본 발명에 따른 SCADA 시스템 통신 환경의 공유키 관리방법 및 세션키 생성방법에 의하면, 메시지를 암호화하여 메시지 브로드캐스팅 또는 멀티캐스팅을 지원하면서 키분배를 위한 연산량을 분배하고 통신량을 줄일 수 있는 효과가 얻어진다.

[0025] 또, 본 발명에 따른 SCADA 시스템 통신 환경의 공유키 관리방법 및 세션키 생성방법에 의하면, 각 원격단말 또는 서브단말이 마스터 단말로부터 갱신된 공유키를 모두 수신하여 복호화하는 통신 및 연산을 하지 않고, 갱신된 일부 공유키를 간단한 해시함수를 통해 직접 계산함으로써, 성능상 제약을 가지는 원격단말의 계산량을 최소화하는 효과가 얻어진다.

도면의 간단한 설명

[0026] 도 1은 본 발명을 실시하기 위한 SCADA 시스템의 전체 구성을 도시한 도면이다.

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

도 3은 본 발명의 일실시예에 따라 생성한 그룹키의 트리구조를 예시한 도면이다.

도 4는 본 발명의 일실시예에 따라 트리구조의 그룹키의 공유키를 갱신하는 일례를 도시한 도면이다.

도 5는 종래의 발명에 따라 그룹키의 공유키를 갱신하는 트리구조를 예시한 도면이다.

* 도면의 주요 부분에 대한 부호의 설명 *

10 : HMI 단말 21 : 마스터 단말

21 : 마스터 단말

22 : 서브단말 23 : 워격단말

23 : 워격단말

30 : 트리구조 31 : 루트노드

31 : 루트노드

40 : 일반노드 50 : 중간노드

50 : 중간노드

60 : 리프노드

발명을 실시하기 위한 구체적인 내용

- [0027] 이하, 본 발명의 실시를 위한 구체적인 내용을 도면에 따라서 설명한다.
- [0028] 또한, 본 발명을 설명하는데 있어서 동일 부분은 동일 부호를 붙이고, 그 반복 설명은 생략한다.
- [0029] 먼저, 본 발명을 실시하기 위한 SCADA 시스템의 전체 구성의 일례에 대하여 도 1을 참조하여 설명한다.
- [0030] 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.
- [0031] 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.
- [0032] 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.
- [0033] 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.
- [0034] 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.
- [0035] 세션키는 메시지를 송수신하는 특정 세션에서만 이용되는 키로서, 세션을 달리하면 다르게 생성된다. 세션키가 노출되더라도 다른 세션은 안전하다. 그런데 세션키는 각 단말이 공유하는 공유키를 이용하여 생성된다. 즉, 세션키는 공유키에 타임스탬프, 시퀀스 번호, 장치의 식별자 등이 추가되어 생성된다. 따라서 안전한 통신을 위해서는 무엇보다 공유키의 관리가 중요하다.
- [0036] 본 발명에 따른 SCADA 시스템 통신 환경의 공유키 관리방법은 마스터 단말(21)에 의해 전체적으로 하나의 논리 구조로 관리된다. 즉, 본 발명의 일실시예에 따르면, 마스터 단말(21)이 공유키를 생성하여 서브단말(22) 또는 원격단말(23)에 전달된다. 마스터 단말(21)이 전체의 공유키를 주체적으로 관리한다.
- [0037] 한편, SCADA시스템에서 원격단말(23)이 삭제되거나 추가되면, 공유키의 보호를 위해 원격단말(23)과 공유했던 공유키를 모두 갱신해야 한다. 따라서 마스터 단말(21)은 공유키의 일부를 갱신하고, 서브단말(22) 또는 원격단말(23)에 갱신된 공유키를 전달한다. 이때, 서브단말(22) 또는 원격단말(23)은 갱신되는 공유키를 모두 수신하지 않고 일부 공유키를 직접 계산할 수 있다.
- [0038] 다음으로, 본 발명의 일실시예에 따른 SCADA 시스템 통신 환경의 공유키 관리방법을 도 2를 참조하여 설명한다.
- [0039] 도 2에서 보는 바와 같이, 본 발명의 일실시예에 따른 키 관리방법은 공유키를 트리구조로 생성하는 단계(S10), 공유키를 분배하는 단계(S20), 및 공유키의 갱신단계(S30)로 구분된다.
- [0040] 먼저, 상기 마스터 단말(21)은 그룹키의 공유키들을 트리구조(30)로 생성한다(S10). 도 3a에서 보는 바와 같이, 트리구조(30)의 루트노드(31)는 마스터 단말(21)에 대응된다. 또, 중간노드(50)는 서브단말(22)에 대응되고, 리프노드(60)는 원격단말(23)에 대응된다.
- [0041] 한편, 루트노드(31)와 중간노드(50) 사이는 2진 트리구조로 구성된다. 루트(31)와 중간노드(50) 사이의 노드를 "일반노드(40)"라 부르기로 한다.
- [0042] 또, 하나의 서브단말의 중간노드(50)의 자식노드(60)들은 이 서브단말(22)에 연결된 원격단말(23)에 대응되는

노드(60)들로 구성한다. 즉, 중간노드(50)를 정점으로 하는 트리는 n차 트리(n-array tree)로 구성한다.

[0043] 상기 트리구조(30)의 각 노드에는 공유키가 생성된다. 생성되는 방법의 일례는 다음과 같다.

[0044] 먼저, 마스터 단말(21)이 다수의 비밀키를 생성하여 원격단말(23)에 각각 할당한다. 각 원격단말(23)에 할당된 비밀키가 트리구조(30)의 리프노드(60)의 공유키로 정해진다. 예를 들면, 도 3a에서, 트리구조(30)의 리프노드(60)에는 원격단말 $R_1, R_2, \dots, R_{100}$, 에 각각 할당된 비밀키인 $K_{h+1,1}, K_{h+1,2}, \dots, K_{h+1,100}$,을 공유키로 정한다.

[0045] 다음으로, 트리구조(30)의 각 노드의 공유키는 자식노드의 공유키를 이용하여 생성된다. 예를 들어, 각 노드의 공유키는 모든 자식노드의 공유키들을 해시하여 생성된다.

[0046] 중간노드(50)의 공유키는 자신의 자식노드인 리프노드(60)의 공유키를 해시하여 생성된다.

[0047] 즉, 중간노드(50)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 리프노드의 공유키 $K_{i,j}$ if $(1 \leq i \leq \log_n m - 1, 1 \leq j \leq m)$ 을 해시하여 생성된다. 식으로 표현하면, [수학식 1]과 같다.

[0048] [수학식 1]

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

[0049]

[0050] 단, n은 서브단말에 연결하는 원격단말의 수이고, m은 서브단말의 개수이다.

[0051] 예를들어, 도 3a에서 공유키 $K_{h,1}$ 는 $K_{h+1,1}, K_{h+1,2}, \dots, K_{h+1,20}$ 를 해시하여 생성된다.

[0052] 한편, 루트노드(31)와 중간노드(50) 사이는 2진 트리로 생성된다. 2진 트리에서 각 노드의 공유키 값은 2개의 자식 노드의 공유키(또는 해시된 값)들을 해시함으로써 생성된다. 식으로 표현하면, [수학식 2]와 같다.

[0053] [수학식 2]

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

[0054]

[0055] 단, m은 서브단말의 개수이고, $h = 1 + \log_2 m$ 이다.

[0056] 예를 들어, 도 3a에서 공유키 $K_{1,1}$ 은 공유키 $K_{2,1}$ 과 $K_{2,2}$ 를 해시하여 생성된다. 따라서 위의 식을 통해 2진 트리구조의 공유키 구조가 형성되며, 루트노드의 공유키 $K_{0,1}$ 도 생성된다.

[0057]

[0058] 다음으로, 상기 원격단말(23) 또는 서브단말(22)이 자신과 대응되는 노드의 상위노드 및 하위노드의 공유키를 수신하여 저장한다(S20).

[0059] 즉, 서브단말(22)은 트리구조(30)에서 자신의 중간노드(50)의 하위노드 및 상위노드의 공유키를 저장한다. 예를 들어, 도 3b에서 서브단말 $K_{h,2}$ 는 중간노드 $K_{h,2}$ 에 대응된다. 중간노드 $K_{h,2}$ 의 상위노드는 $K_{0,1}, K_{1,1}, K_{2,1}, \dots$, 이고, 중간노드 $K_{h,2}$ 의 하위노드는 $K_{h+1,21}, K_{h+1,22}, \dots, K_{h+1,40}$, 이다. 따라서 서브단말 $K_{h,2}$ 는 자신의 중간노드의 공유키인 $K_{h,2}$ 와, 상위노드의 공유키인 $K_{0,1}, K_{1,1}, K_{2,1}, \dots$, 하위노드의 공유키인 $K_{h+1,21}, K_{h+1,22}, \dots, K_{h+1,40}$, 를 모두 보유한다. 서브단말 $K_{h,2}$ 는 도 3b에서 회색으로 칠한 노드의 공유키들을 모두 보유한다.

[0060] 또, 원격단말(23)은 트리구조(30)에서 자신의 리프노드(50)의 상위노드의 공유키를 저장한다. 원격단말(23)은 하위노드를 가지지 않기 때문에 상위노드의 공유키만을 저장한다. 예를 들어, 도 3b에서 원격단말 $K_{h+1,2}$ 는 리프노드 $K_{h+1,2}$ 에 대응된다. 중간노드 $K_{h+1,2}$ 의 상위노드는 $K_{0,1}, K_{1,1}, K_{2,1}, \dots, K_{h,1}$ 이다. 따라서 원격단말 $K_{h+1,2}$ 는 자신의 리프노드의 공유키인 $K_{h+1,2}$ 와, 상위노드의 공유키인 $K_{0,1}, K_{1,1}, K_{2,1}, \dots, K_{h,1}$ 을 모두 보유한다.

- [0061] 즉, 서브단말(22)의 개수가 m 개 일 경우, $1 + \log_2 m$ 개의 공유키와 자신에 속하는 원격단말(22)의 개수의 공유키를 저장하며, 원격단말(23)은 상위노드의 공유키 개수에서 자신의 공유키(또는 비밀키)를 더한 $2 + \log_2 m$ 개의 공유키를 저장한다.
- [0062] 다음으로, 중간노드의 공유키가 갱신되면, 갱신되는 중간노드에서 루트노드까지의 경로에 있는 노드(이하 경로상 노드)들의 공유키를 모두 갱신하되, 상기 경로상 노드의 공유키는 자신의 공유키와 경로에 있지 않는 자식노드의 공유키로 갱신된다(S30).
- [0063] 일실시예로서, 원격단말(23)이 추가 또는 삭제되면, 상기 원격단말(23)과 연결된 서브단말(22)에 대응되는 중간노드(50) 및 상기 중간노드(50)의 상위노드의 공유키를 갱신한다. 하나의 원격단말(23)이 삭제(탈퇴)되면, 삭제된 원격단말(23)은 트리구조(30)에서 자신에 해당하는 리프노드(60)의 상위노드의 공유키를 모두 알고 있으므로, 이 상위노드의 공유키들이 노출된 것으로 볼 수 있다. 따라서 리프노드(60)의 상위노드의 공유키들을 모두 갱신해야 한다.
- [0064] 또, 원격단말(23)이 추가되면, 마스터 단말(21)로부터 생성된 자신의 비밀키를 수신할 것이다. 그리고 서브단말(상기 원격단말과 연결된 서브단말)에 대응되는 중간노드(50)의 공유키는 추가된 원격단말(23)의 비밀키도 포함하여 다시 갱신될 것이다. 따라서 서브단말의 상위노드들도 서브단말의 공유키 갱신을 반영하여 모두 갱신되어야 한다.
- [0065] 원격단말(23)이 추가 또는 삭제되면, 마스터 단말(21)은 상기 추가 또는 삭제된 원격단말(23)이 연결된 서브단말(22)에 대응되는 노드(50)에서, 상기 추가 또는 삭제된 원격단말에 대응되는 노드(60)를 추가 또는 삭제한다.
- [0066] 중간노드(50)와 리프노드(60)의 트리구조는 n 차원 트리(n -array tree)이므로 중간노드(50)의 자식노드 개수는 여러 개도 가능하다. 따라서 원격단말(23)이 추가 또는 삭제되면, 중간노드(50)에서 리프노드(60)를 추가 또는 삭제한다. 트리구조(30)의 다른 노드를 변경하지 않는다.
- [0067] 예를 들면, 도 3a에서, 원격단말 R_{100} 이 삭제되면, 이에 대응되는 트리구조(30)의 리프노드인 $K_{h+1,100}$ 을 중간노드 $K_{h,m}$ 에서 삭제한다. 또, 도 3a에서 원격단말 R_{101} 이 추가되면, 이에 대응되는 리프노드 $K_{h+1,101}$ 을 중간노드 $K_{h,m}$ 에서 추가한다. 이외에 도 3a에서 트리구조(30)의 구조는 변경되지 않는다.
- [0068] 이때, 공유키를 갱신하는 경우를 원격단말(23)이 추가 또는 삭제되는 경우로 제한하는 것은 아니다. 서브단말이 변경(삭제 또는 추가)되는 경우나, 악의적인 공격자에 의해서 공격을 받았다고 판단되는 경우에도 해당되는 노드의 키를 갱신해야만 한다. 본원발명은 이런 경우도 포함한다.
- [0069] 그리고 추가 또는 삭제된 리프노드에서 루트노드까지의 경로에 있는 노드들의 공유키를 갱신한다.
- [0070] 공유키를 갱신하는 방법을 도 4를 참조하여 보다 구체적으로 설명한다. 도 4는 원격단말 R_{81} 이 탈퇴(삭제)되는 경우에 그룹키의 공유키들이 갱신되는 일례를 예시한 도면이다.
- [0071] 먼저, 원격단말(23)이 추가 또는 삭제되면, 마스터 단말(21)은 상기 원격단말(23)이 속하는 서브단말의 중간노드에서 루트노드까지의 경로에 있는 노드(이하 경로상 노드)들의 공유키를 갱신한다.
- [0072] 이때, 각 경로상 노드의 공유키는 자신의 공유키와 경로에 있지 않는 자식노드의 공유키를 이용하여 계산한다. 예를 들어 다음 [수학식 3]과 같이 해시함수를 이용하여 계산한다.
- [0073] [수학식 3]

$$K_{i-1, \lceil j/2 \rceil} = H(H(K_{i-1, \lceil j/2 \rceil}), H(K_{i,k}))$$

$$\text{if } (1 \leq i \leq h-1, 1 \leq j \leq m, k = j \text{ or } j+1)$$

[0074]

[0075] 단, m 은 서브단말의 개수이고, $h = 1 + \log_2 m$ 이고, $K_{i,k}$ 는 경로에 있지 않는 자식노드($K_{i-1,j/2}$ 의 자식노드)이다.

[0076] 도 4의 예에서, 원격단말 R_{81} 이 삭제되면, 원격단말 R_{81} 에 대응되는 리프노드는 K_{481} 이고, 리프노드는 K_{481} 과 연결되는(속하는) 중간노드는 $K_{3,8}$ 이다. 중간노드 $K_{3,8}$ 에서 루트노드 $K_{0,1}$ 까지의 경로상 노드들 $K_{3,8}$, $K_{2,4}$, $K_{1,2}$, $K_{0,1}$ 의

공유키가 모두 갱신된다.

- [0077] 또한, 상기 원격단말(23) 또는 서브단말(22)은 갱신된 공유키를 직접 계산하거나 수신하여 저장한다. 즉, 경로상 노드의 형제노드 각각에 대하여, 상기 형제노드 또는 상기 형제노드의 하위노드에 대응되는 서브단말(22)은 상기 형제노드의 부모노드의 갱신된 공유키를 직접 계산하고, 상기 부모노드의 상위노드의 공유키를 상기 마스터 단말(21)로부터 수신한다.
- [0078] 또, 상기 경로상 노드의 형제노드 각각에 대하여, 상기 형제노드의 하위노드에 대응되는 원격단말(23)은 상기 형제노드의 부모노드의 갱신된 공유키를 직접 계산하고, 상기 부모노드의 상위노드의 공유키를 상기 마스터 단말(21) 또는 서브단말(22)로부터 수한다.
- [0079] 도 4의 예에서, 경로상 노드 중 하나는 노드 $K_{1,2}$ 이고, 이 노드의 형제노드는 $K_{1,1}$ 이다. 형제노드 $K_{1,1}$ 및 상기 형제노드의 하위노드에 위치하는 서브단말(22)은 $K_{3,1}$, $K_{3,2}$, $K_{3,3}$, $K_{3,4}$ 의 중간노드에 대응되는 서브단말 SUB_1 , SUB_2 , SUB_3 , SUB_4 이다. 또, 형제노드 $K_{1,1}$ 및 상기 형제노드의 하위노드에 위치하는 원격단말(23)은 K_{411} , K_{412} , K_{413} , ..., K_{442} , K_{443} 의 리프노드에 대응되는 원격단말 R_{11} , R_{12} , R_{13} , ..., R_{42} , R_{43} 이다. 상기 서브단말 또는 원격단말은 형제노드 $K_{1,1}$ 의 부모노드인 $K_{0,1}$ 의 갱신된 공유키를 상기 [수학식 3]을 이용하여 직접 계산한다.
- [0080] [수학식 3]에 따르면, 결국, 형제노드와 상기 형제노드의 부모노드를 해시하여 부모노드의 공유키를 구하는 것과 같다. 따라서 각 형제노드 및 상기 형제노드의 하위노드에 대응되는 서브단말 또는 원격단말은 상기 형제노드의 공유키와 상기 부모노드의 갱신된 공유키를 모두 알고 있기 때문에, [수학식 3]을 이용하여 부모노드의 공유키를 계산할 수 있다.
- [0081] 한편, 경로상 노드의 형제노드 및 상기 형제노드에 대응되는 서브단말(22) 또는 원격단말(23)은 상기 형제노드의 부모노드의 상위노드의 공유키를 알 수 없다. 도 4의 예에서, 경로상 노드의 형제노드 중 하나인 노드 $K_{2,3}$ 의 하위노드 $K_{3,5}$ 와 $K_{3,6}$ 에 대응되는 서브단말 SUB_5 , SUB_6 은 자신의 부모노드 $K_{1,2}$ 의 상위노드인 $K_{0,1}$ 의 갱신된 공유키를 직접 계산할 수 없다. $K_{0,1}$ 의 갱신된 공유키는 노드 $K_{1,1}$ 의 공유키를 해시하여 갱신된다. 그러나 서브단말 SUB_5 , SUB_6 은 공유키 $K_{1,1}$ 을 가지고 있지 않기 때문에 노드 $K_{0,1}$ 의 갱신된 공유키를 직접 계산할 수 없다. 따라서 이런 공유키들은 마스터 단말(21)로부터 수신해야 한다.
- [0082] 이때, 마스터 단말(21)은 갱신된 공유키를 갱신된 공유키로 암호화하여 원격단말(23) 또는 서브단말(22)에게 멀티캐스팅하고, 상기 원격단말(23) 또는 서브단말(22)은 암호화된 공유키를 수신하고 복호화하여 저장한다.
- [0083] 상기과 같이, SCADA 시스템 통신 환경에서는 제거되는 사용자 노드(원격단말에 대응되는 노드)에서부터 루트노드까지의 모든 경로에 있는 키를 변경한다. 따라서 원격단말이 탈퇴하더라도 원격단말에 노출된 모든 키를 업데이트함으로써 보안상의 문제점을 막을 수가 있다.
- [0084]
- [0085] 다음으로, 본 발명에 따른 SCADA 시스템 통신 환경의 세션키 생성방법 및 메시지 통신방법을 설명한다.
- [0086] 세션키는 공유키를 이용하여 생성한다. 따라서 공유키의 생성, 저장, 갱신은 앞의 방법을 따른다.
- [0087] 최초 그룹키 분배가 끝나고 각각의 노드는 발전소나 변전소와 같은 원격지에 설치된다. 설치가 끝나고 루트노드인 마스터 단말(MTU)과 해당 노드 원격단말 R_{11} 이 통신을 한다면 다음과 같이 세션키를 생성해서 데이터를 암호화하게 된다.
- [0088] [수학식 4]
- $$S_{0,211} = H(K_{211}, C_{211})$$
- [0089]
- [0090] 우선 [수학식 4]에서처럼 원격단말 R_{11} 의 키인 K_{411} 과 카운터 값인 C_{211} 을 해쉬하여 세션 값을 생성한다. 이러한 과정은 마스터 단말(MTU)과 원격단말 R_{11} 에서 동일하게 진행되어 동일한 세션키를 생성하게 된다. 이렇게 세션키

가 생성되면 해당 세션에서 오고가는 데이터는 [수학식 5]에서처럼 세션키 $S_{0,211}$ 에 의해서 암호화 되어 전송되어진다. 세션이 종료되면 루트노드인 마스터 단말(MTU)과 원격단말 R_{11} 은 [수학식 6]에서처럼 가지고 있는 카운터 값을 1증가시킨다.

[0091] [수학식 5]

$$E_{S_{0,211}}(D)$$

[0093] [수학식 6]

$$C_{211} = C_{211} + 1$$

루트노드인 마스터 단말(MTU)이 어떤 정보를 각 노드에게 브로드캐스팅하려고 한다면, 루트노드는 공유키 $K_{0,1}$ 과 카운터 값 C_0 을 이용하여 브로드캐스팅에 사용할 키를 다음 [수학식 7]과 같이 생성한다.

[0096] [수학식 7]

$$S_{b,0} = H(K_0, C_0)$$

또 다른 일례로서, 마스터 단말(21)은 트리구조(30)의 노드를 선택하여, 선택한 노드의 하위노드에 대응되는 서브단말(22) 및 원격단말(23)과 통신하기 위한 세션키를 상기 선택한 노드의 공유키로 생성한다.

예를 들어, 도 4에서 마스터 단말(21)이 공유키 $K_{1,1}$ 을 이용하여 세션키를 생성하여, 상기 세션키로 암호화한 메시지를 서브단말 SUB_1 , SUB_2 , SUB_3 , SUB_4 와 원격단말 R_{11} , R_{12} , R_{13} , R_{14} ... R_{41} , R_{42} , R_{43} 로 송부한다. 상기 서브단말 및 원격단말은 공유키 $K_{1,1}$ 을 공유하므로, 세션키를 생성하여 상기 메시지를 복호화할 수 있다.

따라서 상기 트리구조(30)의 공유키를 통해, 트리구조에 대응되는 하위 단말들을 그룹화하여 암호화 세션을 설정할 수 있다.

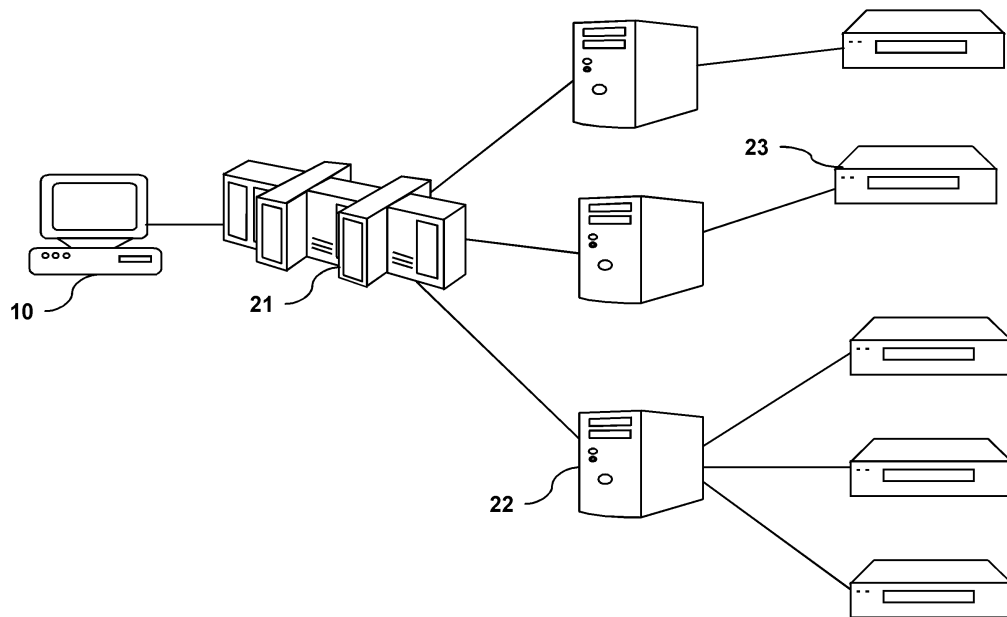
이상, 본 발명자에 의해서 이루어진 발명을 상기 실시 예에 따라 구체적으로 설명하였지만, 본 발명은 상기 실시 예에 한정되는 것은 아니고, 그 요지를 이탈하지 않는 범위에서 여러 가지로 변경 가능한 것은 물론이다.

산업상 이용가능성

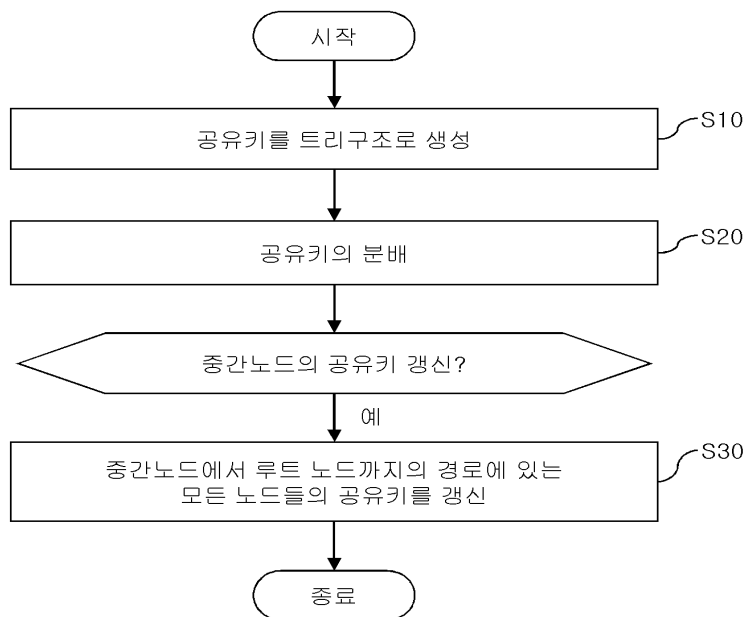
본 발명은 SCADA 시스템에서 암호화 통신으로 메시지를 송수신하는 시스템을 개발하는 데 적용이 가능하다. 특히, 본 발명은 SCADA 시스템에서 암호화 통신을 브로드캐스팅이나 멀티캐스팅 통신으로 할 수 있는 효율적인 암호화 통신시스템을 개발하는 데 유용하다.

도면

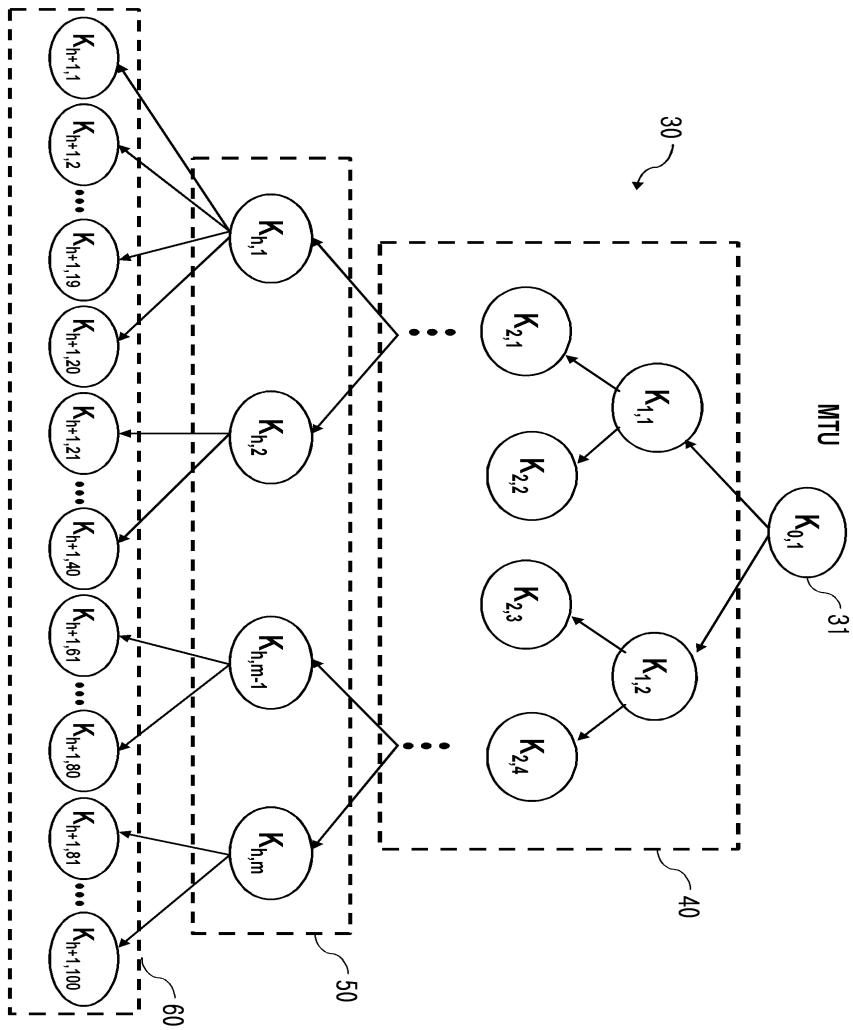
도면1



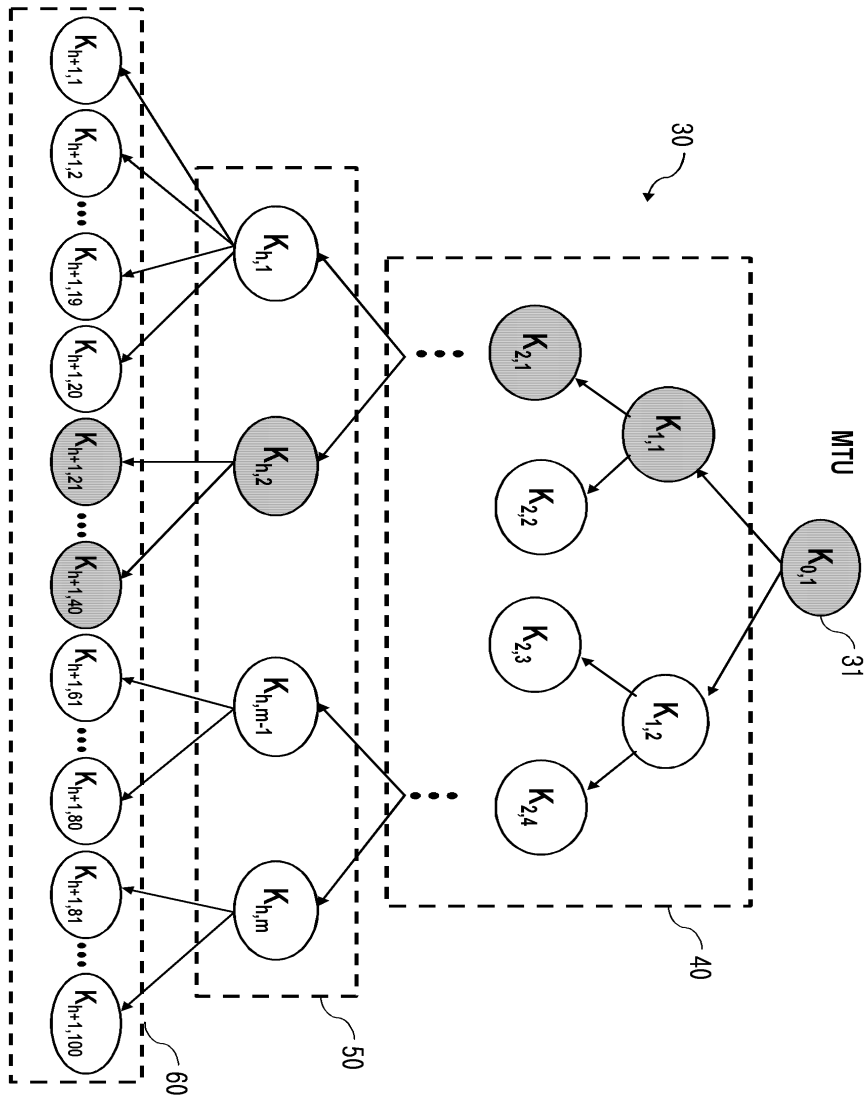
도면2



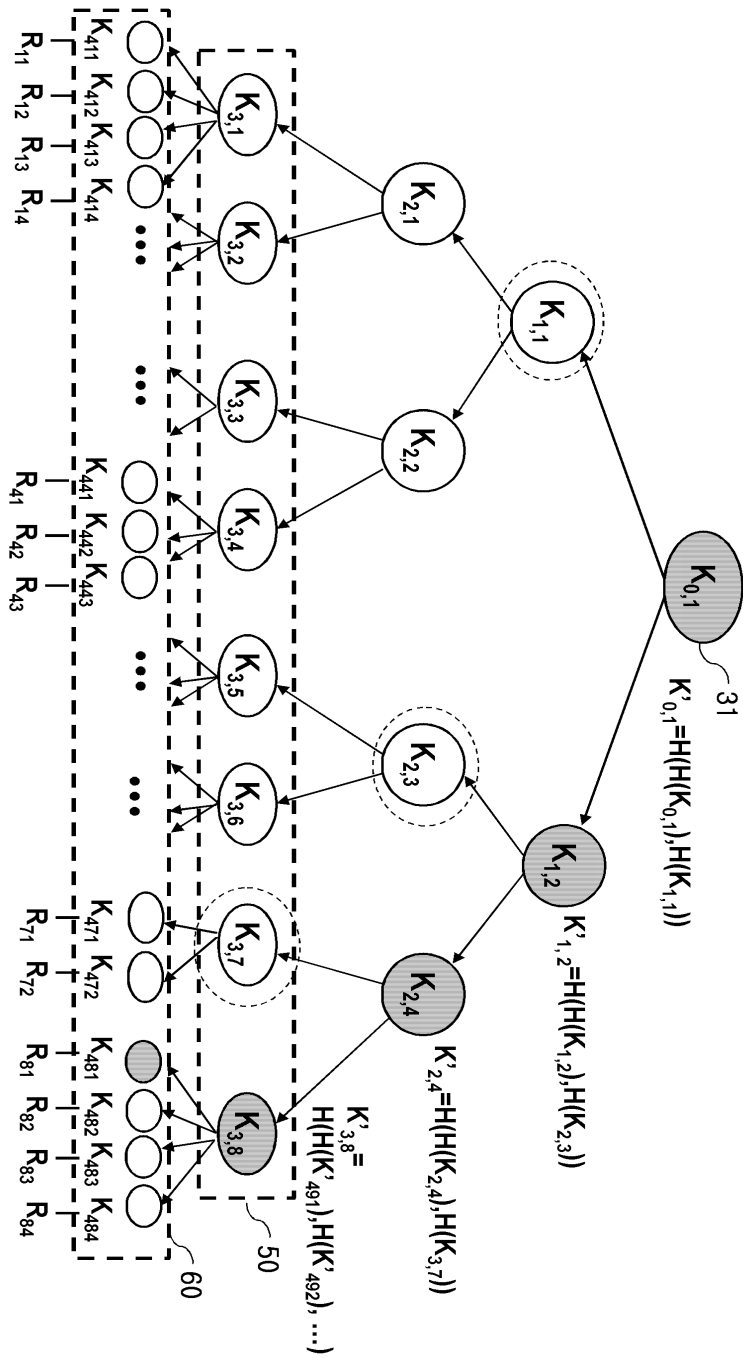
도면3a



도면3b



도면4



도면5

