(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2009년01월15일
(11) 등록번호 10-0879083
(24) 등록일자 2009년01월09일

(51) Int. Cl.
H04L 9/32 (2006.01) *H04L 9/14* (2006.01)
(21) 출원번호 10-2006-0124715
(22) 출원일자 2006년12월08일
심사청구일자 2006년12월08일
(65) 공개번호 10-2008-0052930
(43) 공개일자 2008년06월12일
(56) 선행기술조사문헌
US20040114672 A1
KR1020060031257 A
JP2005191805 A
전체 청구항 수 : 총 6 항

(73) 특허권자
인하대학교 산학협력단
인천 남구 용현동 253 인하대학교
(72) 발명자
양대헌
서울 서초구 서초4동 삼풍아파트 3동 405호
(74) 대리인
이원희

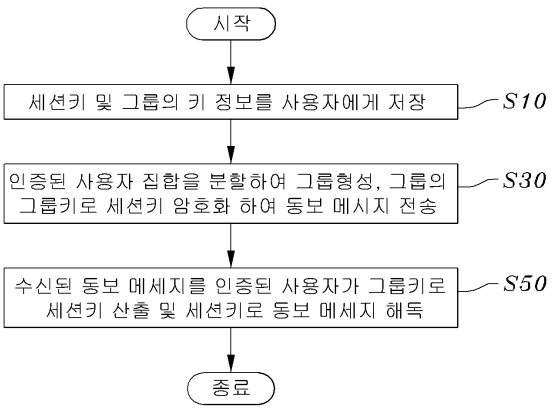
심사관 : 양종필

(54) 2 부분 차집합을 이용한 동보 메세지 암호화 방법

(57) 요 약

본 발명은 2 부분 차집합을 이용한 동보 메세지 암호화 방법에 관한 것으로서, 동보 메세지를 인증되지 않은 사용자는 해독할 수 없도록 암호화시켜 전송하는 방법으로, 사용자를 이진 트리에 배열시키고, 인증되지 않은 사용자가 제거되도록 부분 차집합을 이용함으로써, 동보 메세지 암호화 과정에서 인증 사용자의 그룹을 최소화시켜 헤더 길이를 감소시키며, 이에 따라 그룹의 수에 비례하는 전송 부하가 감소되며, 상기 사용자 그룹키를 루트 노드와 제외되는 트리의 루트 노드 간 XOR(Exclusive OR) 연산으로 추가적인 저장 공간 부하 및 네트워크의 전송 부하를 감소시킬 수 있어 효율적인 전송이 이루어지는 2 부분 차집합을 이용한 동보 메세지 암호화 방법을 제공하기 위한 것으로서, 그 기술적 구성은 컨텐츠를 포함하는 동보 메세지를 송신자가 암호화하여 인증 사용자만이 상기 동보 메세지를 수신 및 복조할 수 있도록 전송하는 방법에 있어서, 통신 중 상기 송신자와 사용자 간에 상기 동보 메세지를 암호화하기 위하여 이용되는 세션키와, 상기 전체 사용자 그룹의 키 정보를 상기 사용자에게 저장시키는 초기설정단계; 상기 전체 사용자 중에서 비인증 사용자를 제외시키고, 인증 사용자를 분할하여 그룹을 형성시키며, 상기 그룹의 그룹키로 상기 송신자가 생성시킨 세션키를 암호화하여 상기 동보 메세지를 전송하는 암호화단계; 상기 동보 메세지를 수신한 인증 사용자는 상기 그룹키로 세션키를 산출하고, 상기 산출된 세션키로 상기 동보 메세지를 해독하는 복호화단계; 를 포함하여 이루어지는 것을 특징으로 한다.

대 표 도 - 도1



특허청구의 범위

청구항 1

통신 중 송신자와 인증 사용자 간에 동보 메세지를 암호화하기 위하여 이용되는 세션키와, 상기 인증 사용자가 포함될 그룹의 키 정보를 상기 인증 사용자에게 저장시키는 초기설정단계;

전체 사용자 중에서 비인증 사용자를 제외시키고, 인증 사용자를 분할하여 그룹을 형성시키며, 상기 인증 사용자를 분할하여 형성한 그룹의 그룹키로 상기 송신자가 생성시킨 세션키를 암호화하여 상기 동보 메세지를 전송하는 암호화단계;

상기 동보 메세지를 수신한 상기 인증 사용자는 상기 그룹키로 세션키를 산출하고, 상기 산출된 세션키로 상기 동보 메세지를 해독하는 복호화단계;

를 포함하여 이루어지는 것을 특징으로 하는 2 부분 차집합을 이용한 동보 메세지 암호화 방법.

청구항 2

제1항에 있어서,

상기 초기설정단계는

상기 전체 사용자를 트리의 최하위 노드에 해당하는 리프(leaf) 노드에 위치시켜 이진 트리를 구성하는 단계;

상기 구성된 이진 트리의 루트(root) 노드에서부터 각 노드에 레벨을 할당하는 단계;

상기 이진 트리(30)에서 상기 루트 노드의 좌, 우측 자식 노드이면서, 트리의 최하위 노드에 해당하는 리프 노드의 부모가 아닌 노드의 레벨을 저장하는 단계;

를 포함하여 이루어져 차후에 해당하는 그룹의 키를 얻는 것을 특징으로 하는 2 부분 차집합을 이용한 동보 메세지 암호화 방법.

청구항 3

제2항에 있어서,

상기 암호화단계는

상기 전체 사용자 중에서 인증되지 않은 비인증 사용자와 상기 루트 노드로 스테이너 트리를 구성하여 상기 비인증 사용자를 포함하는 노드 2개(33,35)를 선택하는 단계;

상기 선택된 두 노드(33,35)의 상위 노드에 해당하는 최소의 공통 부모 노드(31)를 검색하는 단계;

상기 최소의 공통 부모 노드(31)의 좌, 우측 자식 노드와 상기 선택된 두 노드(33,35)가 다르면 하나의 그룹으로 형성시키는 단계;

상기 하나의 그룹은 상기 최소의 공통 부모 노드(31)를 루트(root)로 하는 부분 트리에서 상기 선택된 두 노드를 각각 루트로 하는 부분 트리를 제외시키는 단계;

를 포함하여 이루어져, 인증 사용자를 그룹으로 분류하는 것을 특징으로 하는 2 부분 차집합을 이용한 동보 메세지 암호화 방법.

청구항 4

제3항에 있어서,

상기 하나의 그룹으로 형성시키는 단계에서, 상기 하나의 그룹에는 상기 비인증 사용자를 포함하는 부분트리(20′,20″)가 최대 2개까지 포함되도록 구성하는 것을 특징으로 하는 2 부분 차집합을 이용한 동보 메세지 암호화 방법.

청구항 5

제3항에 있어서,

세션키를 암호화하는데 필요한 각 그룹의 키는

해당부분 트리에서의 상기 최소의 공통 부모 노드(31)와 제외되는 한 부분 트리의 루트 노드(33)간의 차집합으로 결정되는 부분 차집합의 키;

해당부분 트리에서의 상기 최소의 공통 부모 노드(31)와 제외되는 다른 부분 트리의 루트 노드(35)간의 차집합으로 결정되는 부분 차집합의 키;

를 XOR 연산하여 얻어질 수 있는 것을 특징으로 하는 2 부분 차집합을 이용한 동보 메세지 암호화 방법.

청구항 6

제1항에 있어서,

상기 복호화단계는

상기 동보 메세지를 수신한 인증 사용자가 상기 동보 메세지의 헤더로 자신이 속한 그룹을 검색하는 단계;

상기 검색된 그룹의 그룹키로 세션키를 산출하는 단계;

를 포함하여 이루어져, 상기 세션키로 상기 동보 메세지를 해독하는 것을 특징으로 하는 2 부분 차집합을 이용한 동보 메세지 암호화 방법.

명 세 서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

<14> 본 발명은 2 부분 차집합을 이용한 동보 메세지 암호화 방법에 관한 것으로, 더욱 상세하게는 동보 메세지를 인증되지 않은 사용자는 해독할 수 없도록 암호화시켜 전송하는 방법으로, 사용자를 이진 트리에 배열시키고, 인증되지 않은 사용자가 제거되도록 부분 차집합을 이용함으로써, 동보 메세지 암호화 과정에서 인증 사용자의 그룹을 최소화시켜 헤더 길이를 감소시키며, 이에 따라 그룹의 수에 비례하는 전송 부하가 감소되며, 상기 사용자 그룹키를 루트 노드와 제외되는 트리의 루트 노드 간 XOR(Exclusive OR) 연산으로 추가적인 저장 공간 부하 및 네트워크의 전송 부하를 감소시킬 수 있어 효율적인 전송이 이루어지는 2 부분 차집합을 이용한 동보 메세지 암호화 방법에 관한 것이다.

<15> 일반적으로, 동보 메세지 암호화(Broadcast Encryption)는 송신자가 미디어를 인터넷 또는 케이블로 저작권이 있는 미디어를 이용하는 전체 사용자 중에서 인증된 수신자인 사용자(Authenticated User)들에게만 정보를 전달하는 방법으로서, 불법 사용자 또는 기간이 만료된 사용자를 배제(Revocation)시키는 기능을 가진다.

<16> 여기서, 컨텐츠 생산자는 오디오 또는 비디오 데이터를 비롯한 각종 유용한 데이터를 생산하며, 생산된 데이터를 서비스 제공자에게 제공하는데, 상기 서비스 제공자는 컨텐츠 사용자로부터 제공받은 데이터를 각종 유무선 통신 네트워크를 통하여 해당 데이터에 대한 비용을 지불한 인증 사용자에게 동보 메세지를 전달하고, 해당 데이터에 대한 정당한 비용을 지불하지 않은 불법 사용자가 데이터를 이용하지 못하도록 하기 위하여 동보 메세지 암호화로 데이터를 암호화(Encryption)를 하게 된다.

<17> 그리고, 상기 동보 메세지 암호화는 통신 세션 중에만 통신을 하는 송, 수신자 간에 임시적으로 사용되는 세션키를 계산하기 위한 키를 각 사용자에게 저장시키는 초기설정단계와, 세션키를 생성하여 인증 사용자 그룹의 키로 상기 세션키를 암호화된 동보 메세지가 전송되는 암호화단계와, 인증 사용자는 상기 그룹키를 이용하여 세션키를 산출하고, 상기 세션키로 상기 동보 메세지를 해독하는 복호화단계를 포함하여 이루어진다.

<18> 그러나, 사용자 중에서 인증받은 사용자를 분할시켜 그룹으로 형성할 때, 동보 메세지의 헤더 길이가 증가함으로 전송 부하가 높아지고, 상기 전송 부하를 증가시키기 위하여 분할되는 그룹의 수를 감소시키면, 상기 감소된 그룹의 키가 복잡해지므로 저장 공간 부하가 증가하는 등의 문제점이 있었다.

발명이 이루고자 하는 기술적 과제

<19> 본 발명은 상기한 문제점을 해결하기 위하여 안출한 것으로, 동보 메세지를 인증되지 않은 사용자는 해독할 수 없도록 암호화시켜 전송하는 방법으로, 사용자를 이진 트리에 배열시키고, 인증되지 않은 사용자가 제거되도록 부분 차집합을 이용함으로써, 동보 메세지 암호화 과정에서 인증 사용자의 그룹을 최소화시켜 헤더 길이를 감소시키며, 이에 따라 그룹의 수에 비례하는 전송 부하가 감소되며, 상기 사용자 그룹키를 루트 노드와 제외되는 트리의 루트 노드 간 XOR(Exclusive OR) 연산으로 추가적인 저장 공간 부하 및 네트워크의 전송 부하를 감소시킬 수 있어 효율적인 전송이 이루어지는 2 부분 차집합을 이용한 동보 메세지 암호화 방법을 제공하는 것을 목적으로 한다.

발명의 구성 및 작용

<20> 상기한 바와 같은 목적을 달성하기 위하여 본 발명은 컨텐츠를 포함하는 동보 메세지를 송신자가 암호화하여 인증 사용자만이 상기 동보 메세지를 수신 및 복조할 수 있도록 전송하는 방법에 있어서, 통신 중 상기 송신자와 사용자 간에 상기 동보 메세지를 암호화하기 위하여 이용되는 세션키와, 상기 전체 사용자 그룹의 키 정보를 상기 사용자에게 저장시키는 초기설정단계; 상기 전체 사용자 중에서 비인증 사용자를 제외시키고, 인증 사용자를 분할하여 그룹을 형성시키며, 상기 그룹의 그룹키로 상기 송신자가 생성시킨 세션키를 암호화하여 상기 동보 메세지를 전송하는 암호화단계; 상기 동보 메세지를 수신한 인증 사용자는 상기 그룹키로 세션키를 산출하고, 상기 산출된 세션키로 상기 동보 메세지를 해독하는 복호화단계; 를 포함하여 이루어지는 것을 특징으로 한다.

<21> 그리고, 상기 초기설정단계는 상기 전체 사용자를 트리의 최하위 노드에 해당하는 리프(leaf) 노드에 위치시켜 이진 트리를 구성하는 단계; 상기 구성된 이진 트리의 루트 노드에서부터 각 노드에 레벨을 할당하는 단계; 상기 이진 트리에서 상기 루트 노드의 자식 노드이면서, 리프 노드의 부모가 아닌 노드의 레벨을 저장하는 단계; 를 포함하여 이루어져, 상기 저장된 각 노드의 레벨로 상기 전체 사용자 그룹의 키를 얻는 것을 특징으로 한다.

<22> 또한, 상기 암호화단계는 상기 전체 사용자 중에서 인증되지 않은 비인증 사용자와 상기 루트 노드로 스테이너 트리를 구성하여 상기 비인증 사용자를 포함하는 노드를 선택하는 단계; 상기 비인증 사용자를 포함하는 노드의 최소공통 부모 노드를 검색하는 단계; 상기 최소공통 부모 노드의 좌, 우측 자식 노드와 상기 비인증 사용자를 포함하는 노드가 다르면 하나의 그룹으로 형성시키는 단계; 상기 하나의 그룹은 상기 최소공통 부모 노드를 뿌리로 하는 트리에서 상기 비인증 사용자를 포함하는 노드를 뿌리로 하는 트리를 제외시키는 단계; 를 포함하여 이루어져, 인증 사용자를 그룹으로 분류하는 것을 특징으로 한다.

<23> 상기 하나의 그룹으로 형성시키는 단계에서, 상기 하나의 그룹에는 상기 비인증 사용자를 포함하는 부분트리(20′,20″)가 최대 2개까지 포함되도록 구성한다.

<24> 여기서, 상기 그룹키는 상기 사용자 그룹 트리의 루트 노드와, 상기 비인증 사용자 그룹을 포함하는 노드 간의 차집합으로 결정되는 부분 차집합의 키; 상기 사용자 그룹 트리의 루트 노드와, 상기 다른 비인증 사용자를 포함하는 노드 간의 차집합으로 결정되는 부분 차집합의 키; 를 XOR 연산하여 얻어질 수 있는 것을 특징으로 한다.

<25> 그리고, 상기 복호화단계는 상기 동보 메세지를 수신한 인증 사용자가 상기 동보 메세지의 헤더로 자신이 속한 그룹을 검색하는 단계; 상기 검색된 그룹의 그룹키로 세션키를 산출하는 단계; 를 포함하여 이루어져, 상기 세션키로 상기 동보 메세지를 해독하는 것을 특징으로 한다.

<26> 이하, 본 발명에 따른 실시예를 첨부된 예시도면을 참고로 하여 상세하게 설명한다.

<27> 도 1은 본 발명에 따른 2 부분 차집합을 이용한 동보 메세지 암호화 방법에 따른 개략적인 흐름도이다. 도면에 도시된 바와 같이, 저작권이 있는 음악, 영화, 책 등의 미디어 컨텐츠(Media Contents)를 포함하는 동보 메세지(Broadcast Message)를 방송국, 정보 제공자 등의 송신자는 상기 동보 메세지를 암호화시켜 인증된 사용자만이 상기 동보 메세지를 수신 및 복조할 수 있도록 전송하는 방법에 관한 것이다.

<28> 그리고, 본 발명에 따른 2 부분 차집합을 이용한 동보 메세지 암호화 방법은 초기설정단계와 암호화단계와 복호화단계를 포함하여 이루어진다.

<29> 여기서, 상기 초기설정단계는 상기 동보 메세지를 전송하는 송신자와 상기 동보 메세지를 수신하는 수신자 간의 통신 연결로부터 연결 해제인 통신 세션 동안에 상기 동보 메세지를 암호화시키기 위하여 임시적으로 사용되는 세션키와, 상기 전체 사용자 그룹의 키 정보를 상기 사용자에게 저장시킨다.

<30> 이때, 상기 그룹의 키 정보는 상기 세션키를 암호화시키기 위하여 할당된다.

<31> 또한, 상기 암호화단계는 상기 전체 사용자 중에서 비인증 사용자를 제외시키며, 상기 전체 사용자 중에서 인증된 사용자인 인증 사용자 그룹을 분할하여 그룹을 형성시키고, 상기 인증 사용자 그룹의 키인 그룹키로 상기 송신자가 생성시킨 세션키를 암호화시켜 상기 동보 메세지를 인증 사용자에게 전송한다.

<32> 그리고, 상기 복호화단계는 상기 동보 메세지를 수신한 인증 사용자는 상기 그룹키로 세션키를 산출해내고, 상기 산출된 세션키로 상기 동보 메세지를 해독하여 영화, 음악, 책 등의 저작권이 있는 미디어 컨텐츠에 대하여 열람이 가능하며, 한편, 비인증 사용자는 상기 동보 메세지를 수신하더라도 암호를 복호시킬 수 있는 키가 없기 때문에 미디어 컨텐츠에 대하여 열람이 불가능하다.

<33> 도 2는 본 발명에 따른 2 부분 차집합을 이용한 동보 메세지 암호화 방법의 초기설정단계에 대한 개략적인 흐름도이고, 도 3은 본 발명에 따른 사용자 그룹의 이진 트리에 대한 도이다. 도면에서 도시된 바와 같이, 상기 초기설정단계는 인증 사용자(10a)와 비인증 사용자(20)를 트리의 최하위 노드인 리프 노드에 위치시켜 이진 트리(30)를 형성시킨다(S10-1).

<34> 그리고, 상기 구성된 이진 트리(30)의 상위 스텝인 루트 노드(31)에서부터 각 노드마다 기 정해진 레벨을 할당한다(S10-2).

<35> 또한, 상기 이진 트리(30)에서 상기 루트 노드의 하위 좌, 우측 자식 노드이면서, 트리의 최하위 노드에 해당하는 리프 노드의 부모가 아닌 노드의 레벨을 저장한다(S10-3).

<36> 상기 단계(S10-1, S10-2, S10-3)를 통하여 각 노드의 레벨을 저장하여 상기 전체 사용자 그룹(10, 20', 20'')의 키를 얻을 수 있다.

<37> 도 4는 본 발명에 따른 2 부분 차집합을 이용한 동보 메세지 암호화 방법의 암호화단계에 대한 개략적인 흐름도이고, 도 5는 본 발명에 따른 스테이터 트리를 개략적으로 나타낸 도이고, 도 6은 본 발명에 따른 인증 사용자 그룹과 비인증 사용자 그룹을 개략적으로 도시한 도이다. 도면에서 도시하고 있는 바와 같이, 비인증 사용자를 포함하는 부분트리(20', 20'')를 최대 2개까지 포함시키도록 구성되는데, 이를 위하여 상기 암호화단계는 하기와 같이 이루어진다.

<38> 상기 전체 사용자 중에서, 인증되지 않은 비인증 사용자(20)와, 상위 스텝인 루트 노드로 스테이너 트리(Steiner Tree)를 구성하여, 상기 비인증 사용자를 포함하는 노드(33, 35)를 선택한다(S30-1).

<39> 그리고, 상기 비인증 사용자(20)를 포함하는 노드의 최소의 공통 부모 노드(31)를 검색한다(S30-2).

<40> 또한, 상기 최소의 공통 부모 노드(31)의 하위 노드인 좌, 우측 자식 노드와, 상기 비인증 사용자를 포함하는 노드(33, 35)가 다르다면 하나의 그룹으로 형성시킨다(S30-3).

<41> 여기서, 형성된 상기 하나의 그룹은 상기 최소의 공통 부모 노드(31)를 뿌리로 하는 트리에서 상기 비인증 사용자를 포함하는 노드(33, 35)를 제외시키는 것으로 전체 사용자 중에서 인증 사용자(10a)를 그룹으로 분류해낸다(S30-4).

<42> 한편, 상기 그룹키는 상기 사용자 그룹 트리의 루트 노드(31)와 상기 비인증 사용자 그룹을 포함하는 노드(33) 간의 차집합으로 결정되는 부분 차집합의 키와, 상기 사용자 그룹 트리의 루트 노드(31)와 상기 다른 비인증 사용자를 포함하는 노드(35) 간의 차집합으로 결정되는 부분 차집합의 키를 XOR(eXclusive OR) 연산자를 이용하여 얻을 수 있다.

<43> 이때, XOR는 배타적 논리합(排他的論理合, Exclusive OR)으로서, 부울 연산자 중의 하나이며, 2 개의 피 연산자 중 하나가 참이고, 다른 하나가 거짓일 시에만 연산의 결과는 참이 된다.

<44> 상기한 바와 같이, 한 그룹에서 최대 2개의 비인증 사용자 그룹(20', 20'')을 포함함으로써, 생성되는 전체 그룹의 수가 감소하여 그룹의 수에 비례하는 메세지 헤더의 길이가 감소됨과 동시에 전송 부하가 감소하며, 그룹의 키를 2개의 부분 차집합 키를 XOR 연산하여 이용함으로써, 저장공간의 부하가 증가되지 않는다.

<45> 여기서, 동보 메세지 암호화 기법은 전송 부하, 저장 공간 부하, 그리고 계산량 부하의 3가지 측면에서 효율성을 측정하는데, 상기 전송 부하는 메세지의 본체와 같으므로, 메세지의 헤더 길이에 따라 증감되고, 메세지의 헤더 길이는 권한이 있는 사용자들을 어떻게 그룹을 구성하였는지에 따라 결정되며, 인증 사용자(10a)를 가능한 적은 수의 그룹으로 분할함이 관건이다.

<46> 또한, 상기 저장 공간 부하는 상기 초기설정단계에서 각 사용자에게 저장되는 키의 수에 따라 증감되는데, 그룹키를 어떻게 구성되었는지에 따라 판별된다.

<47> 그리고, 상기 계산량 부하는 중앙에서 전송된 암호화된 메세지를 받은 사용자가 메세지를 해독하기 위하여 구비되는 세션키를 계산하는데 필요한 계산량에 따라 증감되는데, 그룹키를 어떻게 구성되었는지에 따라 판별된다.

<48> 상기한 바와 같이, 본 발명에 따른 2 부분 차집합을 이용한 동보 메세지 암호화 방법은 r의 전송 부하, $O(\log^2(n))$의 저장 공간 부하, 2log(n)의 계산량 부하를 가진다.

<49> 도 7은 본 발명에 따른 2 부분 차집합을 이용한 동보 메세지 암호화 방법의 복호화단계에 대한 개략적인 흐름도이며, 도 3을 참조하여 설명한다. 도면에서 도시한 바와 같이, 상기 복호화단계는 상기 동보 메세지를 수신한 인증 사용자(10a)가 상기 동보 메세지의 그룹의 정보에 의하여 설정되는 메세지 헤더로 자신이 속한 그룹을 검색한다(S50-1).

<50> 그리고, 상기 검색된 그룹의 그룹키로 세션키를 산출한다(S50-2).

<51> 마지막으로, 상기 그룹키로 산출된 세션키로 상기 동보 메세지를 인증 사용자(10a)만이 해독하여 열람할 수 있다(S50-3).

<52> 이상에서는 본 발명의 바람직한 실시예를 예시적으로 설명하였으나, 본 발명의 범위는 이같은 특정 실시예에만 한정되지 않으며 해당 분야에서 통상의 지식을 가진자라면 본 발명의 특허 청구 범위내에 기재된 범주 내에서 적절하게 변경이 가능 할 것이다.

발명의 효과

<53> 이상에서 설명한 바와 같이 상기와 같은 구성을 갖는 본 발명은 동보 메세지를 인증되지 않은 사용자는 해독할 수 없도록 암호화시켜 전송하는 방법으로, 사용자를 이진 트리에 배열시키고, 인증되지 않은 사용자가 제거되도록 부분 차집합을 이용함으로써, 동보 메세지 암호화 과정에서 인증 사용자의 그룹을 최소화시켜 헤더 길이를 감소시키며, 이에 따라 그룹의 수에 비례하는 전송 부하가 감소되며, 상기 사용자 그룹키를 루트 노드와 제외되는 트리의 루트 노드 간 XOR(Exclusive OR) 연산으로 추가적인 저장 공간 부하 및 네트워크의 전송 부하를 감소시킬 수 있어 효율적인 전송이 이루어지는 등의 효과를 거둘 수 있다.

도면의 간단한 설명

<1> 도 1은 본 발명에 따른 2 부분 차집합을 이용한 동보 메세지 암호화 방법에 따른 개략적인 흐름도.

<2> 도 2는 본 발명에 따른 2 부분 차집합을 이용한 동보 메세지 암호화 방법의 초기설정단계에 대한 개략적인 흐름도.

<3> 도 3은 본 발명에 따른 사용자 그룹의 이진 트리에 대한 도.

<4> 도 4는 본 발명에 따른 2 부분 차집합을 이용한 동보 메세지 암호화 방법의 암호화단계에 대한 개략적인 흐름도.

<5> 도 5는 본 발명에 따른 스테이터 트리를 개략적으로 나타낸 도.

<6> 도 6은 본 발명에 따른 인증 사용자 그룹과 비인증 사용자 그룹을 개략적으로 도시한 도.

<7> 도 7은 본 발명에 따른 2 부분 차집합을 이용한 동보 메세지 암호화 방법의 복호화단계에 대한 개략적인 흐름도.

<8> <도면의 주요 부분에 대한 도면 부호의 설명>

<9> 10: 인증 사용자 그룹 10a: 인증 사용자

<10> 20', 20'': 비인증 사용자 그룹 20: 비인증 사용자

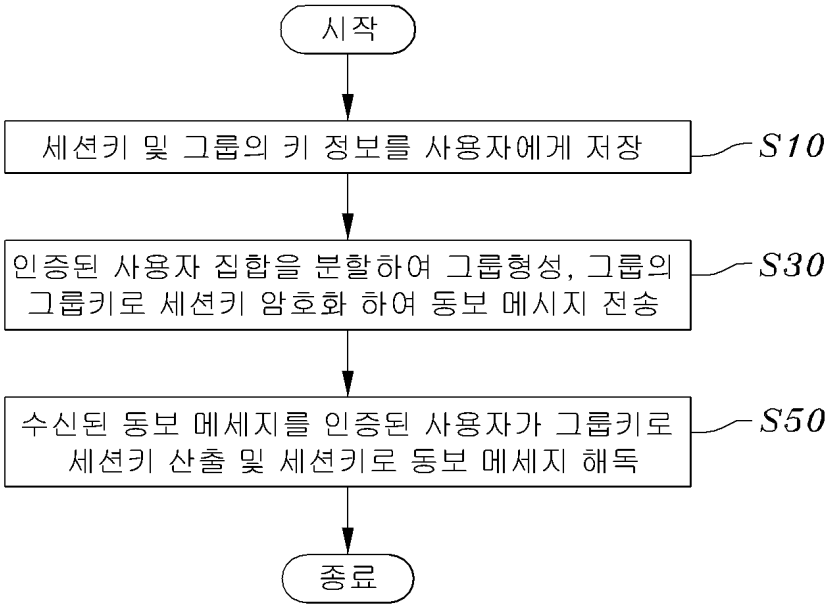
<11> 30: 이진 트리 30': 스테이너 트리

<12> 31: 루트 노드

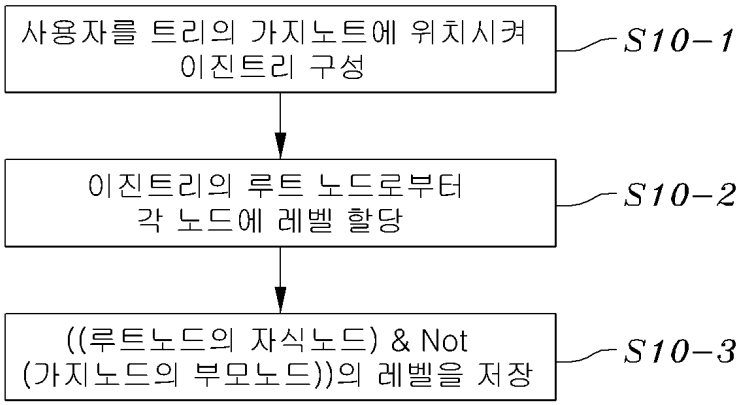
<13> 33, 35: 비인증 사용자를 포함하는 노드

도면

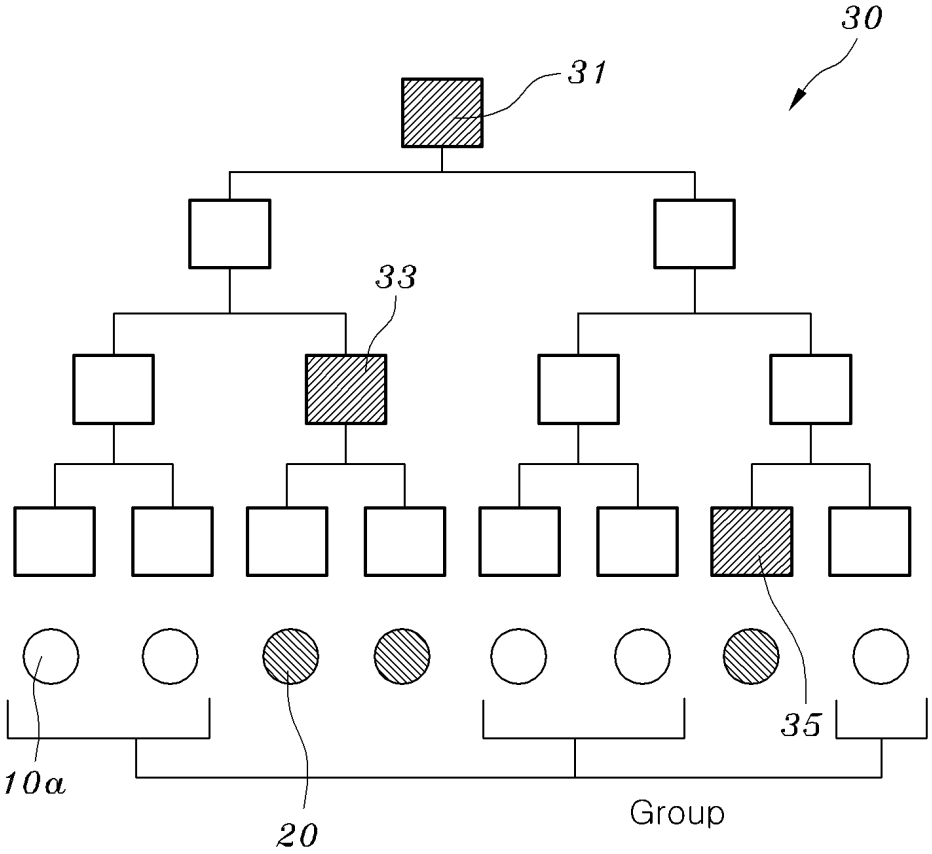
도면1


시작
세션키 및 그룹의 키 정보를 사용자에게 저장
S10
인증된 사용자 집합을 분할하여 그룹형성, 그룹의 그룹키로 세션키 암호화 하여 동보 메시지 전송
S30
수신된 동보 메세지를 인증된 사용자가 그룹키로 세션키 산출 및 세션키로 동보 메세지 해독
S50
종료

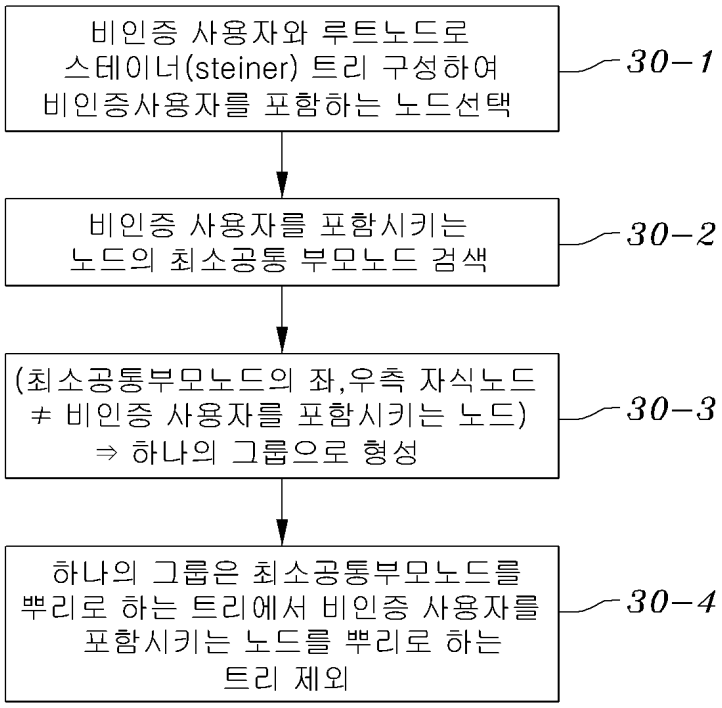
도면2


사용자를 트리의 가지노트에 위치시켜 이진트리 구성
S10-1
이진트리의 루트 노드로부터 각 노드에 레벨 할당
S10-2
((루트노드의 자식노드) & Not (가지노드의 부모노드))의 레벨을 저장
S10-3

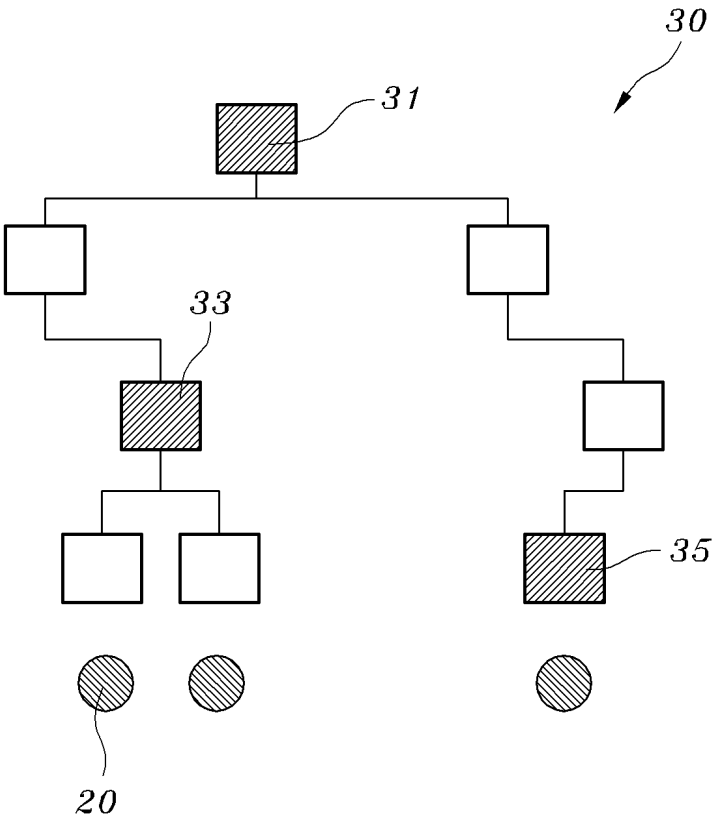
도면3



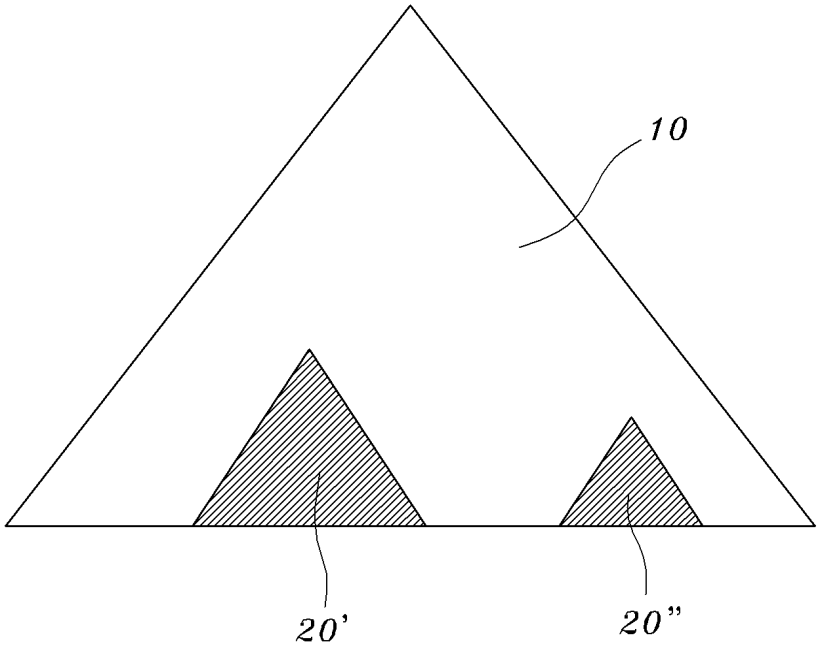
도면4


비인증 사용자와 루트노드로
스테이너(steiner) 트리 구성하여
비인증사용자를 포함하는 노드선택
30-1
비인증 사용자를 포함시키는
노드의 최소공통 부모노드 검색
30-2
(최소공통부모노드의 좌,우측 자식노드
≠ 비인증 사용자를 포함시키는 노드)
⇒ 하나의 그룹으로 형성
30-3
하나의 그룹은 최소공통부모노드를
뿌리로 하는 트리에서 비인증 사용자를
포함시키는 노드를 뿌리로 하는
트리 제외
30-4

도면5



도면6



도면7