(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2012-0004715
(43) 공개일자 2012년01월13일

(51) Int. Cl.
H04L 9/14 (2006.01) *H04L 9/32* (2006.01)
H04L 12/28 (2006.01)
(21) 출원번호 10-2010-0065358
(22) 출원일자 2010년07월07일
심사청구일자 2010년07월07일

(71) 출원인
충남대학교산학협력단
대전광역시 유성구 대학로 99 (궁동, 충남대학교)
(72) 발명자
염흥열
충청남도 아산시 신창면 읍내리 순천향대학교 M114
류재철
대전광역시 유성구 어은로 57, 132동 801호 (어은동, 한빛아파트)
(뒷면에 계속)
(74) 대리인
특허법인정직과특허

전체 청구항 수 : 총 16 항

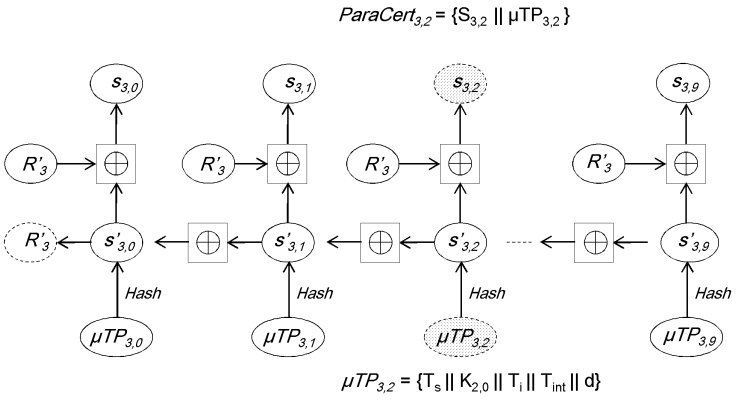
(54) XOR체인을 이용한 트리기반 센서 네트워크 인증 시스템 및 방법

(57) 요 약

중앙서버, 송신노드, 수신노드로 구성되는 센서 네트워크에서 송신노드와 수신노드 사이를 인증하는 XOR체인을 이용한 트리기반 센서 네트워크 인증 시스템 및 방법에 있어서, 다수의 송신노드; 각 송신노드에 대하여 송신노드의 제1 및 제2 키체인 파라미터열 및 인증정보를 생성하여 송신노드로 전송하되, 최초키에 해쉬함수를 반복 적용하여 송신노드의 키체인을 형성하고 송신노드의 키체인으로부터 제1 키체인 파라미터열을 생성하고, 제1 키체인 파라미터열을 모두 XOR 연산하여 인증정보를 생성하고, 제1 키체인 파라미터열의 각 파라미터(이하 제1 파라미터)와 동일한 열에 대응되는 파라미터(이하 제2 파라미터)로 구성하여 제2 키체인 파라미터열을 생성하고, 인증정보에 제1 파라미터를 XOR 연산하여 제2 파라미터를 생성하는 중앙서버; 및 송신노드의 인증정보를 수신하고, 송신노드로부터 메시지와 함께 제1 및 제2 파라미터를 수신하여, 제1 및 제2 파라미터를 XOR 연산하고, XOR 연산 결과와 인증정보를 대비하여 메시지를 인증하는 수신노드를 포함하는 구성을 마련한다.

상기와 같은 시스템 및 방법에 의하여, 수신노드에서 XOR 연산이 증가하기는 하지만 고효율의 인증 연산을 지원하고, 송신노드와 장기간의 통신 두절이 발생하더라도 수신노드는 언제든 즉시 인증을 할 수 있다.

대 표 도 - 도5



(72) 발명자

장재훈

충청남도 아산시 신창면 읍내리 순천향대학교 M114

최현우

충청남도 아산시 신창면 읍내리 순천향대학교 M114

여돈구

충청남도 아산시 신창면 읍내리 순천향대학교 M114

이동희

충청남도 아산시 신창면 읍내리 순천향대학교 M114

이상래

충청남도 아산시 신창면 읍내리 순천향대학교 M114

정영곤

충청남도 아산시 신창면 읍내리 순천향대학교 M114

특허청구의 범위

청구항 1

중앙서버, 송신노드, 수신노드로 구성되는 센서 네트워크에서 송신노드와 수신노드 사이를 인증하는 XOR체인을 이용한 트리기반 센서 네트워크 인증방법에 있어서,

(a) 상기 송신노드는 상기 중앙서버로부터 최초키를 수신하여 자신의 제1 및 제2 키체인 파라미터열 및 인증정보를 생성하되,

(a1) 상기 최초키에 해쉬함수를 반복 적용하여 송신노드의 키체인을 형성하고 상기 송신노드의 키체인으로부터 상기 제1 키체인 파라미터열을 생성하는 단계,

(a2) 상기 제1 키체인 파라미터열을 모두 XOR 연산하여 상기 인증정보를 생성하는 단계, 및

(a3) 상기 제1 키체인 파라미터열의 각 파라미터(이하 제1 파라미터)와 동일한 열에 대응되는 파라미터(이하 제2 파라미터)로 구성하여 상기 제2 키체인 파라미터열을 생성하되, 상기 인증정보에 상기 제1 파라미터를 XOR 연산하여 상기 제2 파라미터를 생성하는 단계를 포함하는 단계;

(b) 상기 수신노드는 상기 송신노드의 인증정보를 수신하는 단계;

(c) 상기 송신노드는 상기 제1 및 제2 키체인 파라미터열에서 순차적으로 동일한 열의 제1 및 제2 파라미터를 메시지와 함께 상기 수신노드로 전송하는 단계;

(d) 상기 수신노드는 상기 제1 및 제2 파라미터를 XOR 연산하고, XOR 연산결과와 상기 인증정보를 대비하여 상기 메시지를 인증하는 단계를 포함하는 것을 특징으로 하는 XOR체인을 이용한 트리기반 센서 네트워크 인증방법.

청구항 2

중앙서버, 송신노드, 수신노드로 구성되는 센서 네트워크에서 송신노드와 수신노드 사이를 인증하는 XOR체인을 이용한 트리기반 센서 네트워크 인증방법에 있어서,

(a) 상기 중앙서버는 각 송신노드에 대하여 상기 송신노드의 제1 및 제2 키체인 파라미터열 및 인증정보를 생성하여 상기 송신노드로 전송하되,

(a1) 최초키에 해쉬함수를 반복 적용하여 송신노드의 키체인을 형성하고 상기 송신노드의 키체인으로부터 상기 제1 키체인 파라미터열을 생성하는 단계,

(a2) 상기 제1 키체인 파라미터열을 모두 XOR 연산하여 상기 인증정보를 생성하는 단계, 및,

(a3) 상기 제1 키체인 파라미터열의 각 파라미터(이하 제1 파라미터)와 동일한 열에 대응되는 파라미터(이하 제2 파라미터)로 구성하여 상기 제2 키체인 파라미터열을 생성하되, 상기 인증정보에 상기 제1 파라미터를 XOR 연산하여 상기 제2 파라미터를 생성하는 단계를 포함하는 단계;

(b) 상기 수신노드는 상기 송신노드의 인증정보를 수신하는 단계;

(c) 상기 송신노드는 상기 제1 및 제2 키체인 파라미터열에서 순차적으로 동일한 열의 제1 및 제2 파라미터를 메시지와 함께 상기 수신노드로 전송하는 단계;

(d) 상기 수신노드는 상기 제1 및 제2 파라미터를 XOR 연산하고, XOR 연산결과와 상기 인증정보를 대비하여 상기 메시지를 인증하는 단계를 포함하는 것을 특징으로 하는 XOR체인을 이용한 트리기반 센서 네트워크 인증방법.

청구항 3

제1항 또는 제2항에 있어서,

상기 (a1)단계에서,

상기 최초키를 시드키로 하여 제1 및 제2 해쉬함수를 반복 적용하여 일련의 부분 키체인들을 생성하되, 시드키에 제1 해쉬함수를 반복 적용하여 부분 키체인을 형성하고 부분 키체인의 두 번째 키를 제2 해쉬함수로 해쉬하여 구한 키를 직전 부분 키체인의 시드키로 정하고,

상기 일련의 부분 키체인들의 각 부분 키체인의 초기키를 부분 키체인들의 순서대로 구성하여 상기 송신노드의 키체인으로 생성하는 것을 특징으로 하는 XOR체인을 이용한 트리기반 센서 네트워크 인증방법.

청구항 4

제1항 또는 제2항에 있어서,

상기 (a1)단계에서, 상기 송신노드의 키체인의 각 키에 타임스탬프를 포함하여 상기 제1 키체인 파라미터열의 파라미터를 구하는 것을 특징으로 하는 XOR체인을 이용한 트리기반 센서 네트워크 인증방법.

청구항 5

제1항 또는 제2항에 있어서,

상기 제1 파라미터는 XOR 연산을 할 때 해쉬되어 해쉬된 값으로 연산되는 것을 특징으로 하는 XOR체인을 이용한 트리기반 센서 네트워크 인증방법.

청구항 6

제1항 또는 제2항에 있어서,

상기 중앙서버는 인증서들을 트리구조로 생성하되, 상기 트리구조의 리프노드는 상기 송신노드 각각에 대응되고, 상기 리프노드의 인증서는 대응되는 송신노드의 인증정보를 해쉬한 값으로 정하고, 상기 트리구조의 각 노드는 모든 자식노드의 인증서를 결합하여 해쉬한 값으로 정하는 것을 특징으로 하는 XOR체인을 이용한 트리기반 센서 네트워크 인증방법.

청구항 7

제6항에 있어서,

상기 수신노드는 상기 루트노드의 인증서 및 상기 송신노드의 인증서들을 수신하고 상기 송신노드의 인증서들로부터 루트노드의 인증서를 연산하여 수신한 루트노드의 인증서와 비교하여 상기 송신노드를 인증하되, 상기 송신노드의 인증서는 상기 송신노드에 대응되는 리프노드의 모든 조상노드의 형제노드의 인증서인 것을 특징으로 하는 XOR체인을 이용한 트리기반 센서 네트워크 인증방법.

청구항 8

제7항에 있어서,

상기 수신노드는 하위노드의 인증서와 하위노드의 형제노드의 인증서를 결합하고 해쉬하여 상위노드의 인증서를 생성하고, 상위노드의 인증서를 생성하는 과정을 반복하여 루트노드의 인증서를 연산하는 것을 특징으로 하는 XOR체인을 이용한 트리기반 센서 네트워크 인증방법.

청구항 9

제6항에 있어서,

상기 송신노드는 상기 루트노드의 인증서 및 상기 송신노드의 인증서들을 수신하고 상기 송신노드의 인증서들로부터 루트노드의 인증서를 연산하여 수신한 루트노드의 인증서와 비교하여 상기 중앙서버를 인증하되, 상기 송신노드의 인증서는 상기 송신노드에 대응되는 리프노드의 모든 조상노드의 형제노드의 인증서인 것을 특징으로 하는 XOR체인을 이용한 트리기반 센서 네트워크 인증방법.

청구항 10

제6항에 있어서,

상기 트리구조는 이진트리인 것을 특징으로 하는 XOR체인을 이용한 트리기반 센서 네트워크 인증방법.

청구항 11

제1항 또는 제2항의 방법을 수행하는 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

청구항 12

센서 네트워크에서 XOR체인을 이용한 트리기반 센서 네트워크 인증 시스템에 있어서,

다수의 송신노드;

각 송신노드에 대하여 상기 송신노드의 제1 및 제2 키체인 파라미터열 및 인증정보를 생성하여 상기 송신노드로 전송하되, 최초키에 해쉬함수를 반복 적용하여 송신노드의 키체인을 형성하고 상기 송신노드의 키체인으로부터 상기 제1 키체인 파라미터열을 생성하고, 상기 제1 키체인 파라미터열을 모두 XOR 연산하여 상기 인증정보를 생성하고, 상기 제1 키체인 파라미터열의 각 파라미터(이하 제1 파라미터)와 동일한 열에 대응되는 파라미터(이하 제2 파라미터)로 구성하여 상기 제2 키체인 파라미터열을 생성하고, 상기 인증정보에 상기 제1 파라미터를 XOR 연산하여 상기 제2 파라미터를 생성하는 중앙서버; 및

상기 송신노드의 인증정보를 수신하고, 상기 송신노드로부터 메시지와 함께 제1 및 제2 파라미터를 수신하여, 상기 제1 및 제2 파라미터를 XOR 연산하고, XOR 연산결과와 상기 인증정보를 대비하여 상기 메시지를 인증하는 수신노드를 포함하는 것을 특징으로 하는 XOR체인을 이용한 트리기반 센서 네트워크 인증 시스템.

청구항 13

센서 네트워크에서 XOR체인을 이용한 트리기반 센서 네트워크 인증 시스템에 있어서,

최초키를 생성하여 전송하는 중앙서버;

상기 최초키를 수신하여 제1 및 제2 키체인 파라미터열 및 인증정보를 생성하되, 상기 최초키에 해쉬함수를 반복 적용하여 송신노드의 키체인을 형성하고 상기 송신노드의 키체인으로부터 상기 제1 키체인 파라미터열을 생성하고, 상기 제1 키체인 파라미터열을 모두 XOR 연산하여 상기 인증정보를 생성하고, 상기 제1 키체인 파라미터열의 각 파라미터(이하 제1 파라미터)와 동일한 열에 대응되는 파라미터(이하 제2 파라미터)로 구성하여 상기 제2 키체인 파라미터열을 생성하고, 상기 인증정보에 상기 제1 파라미터를 XOR 연산하여 상기 제2 파라미터를 생성하는 다수의 송신노드; 및

상기 송신노드의 인증정보를 수신하고, 상기 송신노드로부터 메시지와 함께 제1 및 제2 파라미터를 수신하여, 상기 제1 및 제2 파라미터를 XOR 연산하고, XOR 연산결과와 상기 인증정보를 대비하여 상기 메시지를 인증하는 수신노드를 포함하고,

상기 중앙서버는 상기 송신노드 각각에 대하여 서로 다른 최초키를 생성하여 전송하는 것을 특징으로 하는 XOR

체인을 이용한 트리기반 센서 네트워크 인증 시스템.

청구항 14

제12항 또는 제13항에 있어서,

상기 송신노드는 상기 제1 및 제2 키체인 파라미터열에서 열의 순서에 따라 순차적으로 동일한 열의 제1 및 제2 파라미터를 선정하여 메시지와 함께 상기 수신노드로 전송하는 것을 특징으로 하는 XOR체인을 이용한 트리기반 센서 네트워크 인증 시스템.

청구항 15

제12항 또는 제13항에 있어서,

상기 중앙서버는 상기 인증서들을 트리구조로 생성하되, 상기 트리구조의 리프노드는 상기 송신노드 각각에 대응되고, 상기 리프노드의 인증서는 대응되는 송신노드의 인증정보를 해쉬한 값으로 정하고, 상기 트리구조의 각 노드는 모든 자식노드의 인증서를 결합하여 해쉬한 값으로 정하는 것을 특징으로 하는 XOR체인을 이용한 트리기반 센서 네트워크 인증방법.

청구항 16

제15항에 있어서,

상기 수신노드는 상기 루트노드의 인증서 및 상기 송신노드의 인증서들을 수신하고 상기 송신노드의 인증서들로부터 루트노드의 인증서를 연산하여 수신한 루트노드의 인증서와 비교하여 상기 송신노드를 인증하되, 상기 송신노드의 인증서는 상기 송신노드에 대응되는 리프노드의 모든 조상노드의 형제노드의 인증서인 것을 특징으로 하는 XOR체인을 이용한 트리기반 센서 네트워크 인증방법.

명 세 서

기 술 분 야

[0001] 본 발명은 중앙서버, 송신노드, 수신노드로 구성되는 센서 네트워크에서 수신노드가 인증서의 파라미터들을 XOR 연산하여 인증정보와 비교하여 송신노드를 인증하는 XOR체인을 이용한 트리기반 센서 네트워크 인증 시스템 및 방법에 관한 것이다.

[0002] 특히, 본 발명은 키체인으로부터 제1 키체인 파라미터열을 생성하고, 이를 모두 XOR 연산하여 인증정보를 생성하고, 인증정보에 제1 키체인 파라미터열의 파라미터들을 XOR 연산하여 제2 키체인 파라미터열을 생성하고, 상기 제1 및 제2 키체인 파라미터열 및 인증정보를 이용하여 인증하는 XOR체인을 이용한 트리기반 센서 네트워크 인증 시스템 및 방법에 관한 것이다.

배 경 기 술

[0003] 일반적으로, 센서 네트워크(Sensor Network)는 주변 환경 정보를 수집하는 수신자(또는 수신노드, Sensor Node)와 수신자를 컨트롤하며 수신자로부터 수집된 정보를 모으고 센서 네트워크 외부와 통신할 수 있는 송신자(또는 송신노드, Base Station)로 구성된다. 센서 네트워크의 특징 중 하나는 수신자의 파워, 저장, 연산 능력이 제약적이라는 것이다. 이러한 특징은 센서 네트워크 전체의 수명에도 영향을 미치게 되기 때문에, 송ㅇ수신자간 통신 중 수신자의 부하를 최대한 줄이려는 연구가 활발하게 진행되어왔다.

[0004] 센서 네트워크에서는 송신자(송신노드)와 수신자(수신노드) 간에 메시지 전달에 있어 무선 통신 기술을 이용한다. 무선 통신에 사용되는 브로드캐스트 방식은 송신자의 전파 범위 안에 있는 수신자라면 누구든지 메시지를

획득할 수 있다. 이러한 통신 방식은 광범위한 센서 네트워크에서의 센서 노드들을 관리하는데 있어 효율적이다. 다만, 브로드캐스트된 메시지들을 인증하는데 있어 센서 네트워크의 낮은 대역폭, 무선 통신의 간헐적인 통신 두절, 센서 노드의 자원 제약적인 특징 등이 제약사항으로 작용한다. 그렇기 때문에 기존의 유선 네트워크에서 사용하던 브로드캐스트 방식에서의 인증 방식이나, 기존 보안 프로토콜들을 센서 네트워크에 그대로 적용할 수가 없다.

[0005] SPIN(Security Protocol for Sensor Networks)은 일반 PC급에서 디지털 서명을 이용한 브로드캐스트 인증 방식을 지원하는 TESLA(the Timed, Efficient, Streaming, Loss-tolerant, Authentication) 프로토콜을 센서 네트워크에 적용한 μTESLA(또는 오리지날 μTESLA)를 선보였다. 인증을 위해 송신자의 디지털 서명 기법을 이용하기 때문에, 자원이 제약적이고 무선을 이용하는 센서 네트워크에 적용하기에는 부적합하다.

[0006] 오리지날 μTESLA는 해쉬 함수를 이용하여 해쉬 체인을 만들고, 체인이 생성된 방향과 반대 방향으로 생성된 키를 브로드캐스트 한다. 즉, 전체 센서 네트워크의 생명 주기를 Interval$\triangle_0$ 길이의 n개의 구간으로 서로 다른 인증키(K_j)를 할당한다. 인증키(K_j)는 해쉬 체인의 생성된 방향과 반대 방향으로 순차적으로 할당한다.

[0007] 송신자는 n 구간마다 전달되는 메시지에 인증키 값(K_j)을 포함하여 전달하고, 수신자는 이를 수신하였다가 수신한 인증키 값(K_j)을 해쉬하여 그 이전에 수신한 인증키 값(K_i)과 대비하여 인증한다. 값이 동일하면 인증된 것으로 판단하여 수신한 메시지를 저장한다. 즉, 수신자는 현재 구간($Interval_i$)에 수신한 인증키(K_j)의 검증을 위해 해쉬함수에 인증키(K_j)를 입력 값으로 하여 (j-i)회 반복 연산한다. 결과 값이 가장 최근($Interval_i$)에 이용하였던 인증키(K_i)값과 동일한지 확인한다. 만약, 값이 동일하다면 올바른 인증키로 믿고 인증키를 K_j로 대체한다.

[0008] 결과적으로 송신자가 수신한 메시지에 이전에 전달했던 인증키 값(K_i)이 있을 경우에만 메시지를 저장하게 된다. 한번 공개된 키는 다음 키가 공개되기 이전 시점까지만 사용함으로서 비대칭 키와 유사한 특징을 갖는다. 하지만, 하나의 키 체인으로 센서 네트워크의 수명을 포함(cover)하기에는 키 체인의 각 구간(Interval$\triangle_0$)이 상당히 길어지기 때문에 인증지연 문제가 발생한다.

[0009] 이후, 다수의 짧은 구간의 키 체인을 계층적으로 연결하여 인증지연 시간을 줄인 다층(Multi-Level) μTESLA 프로토콜를 비롯하여, 광범위한 센서 네트워크에서 다수의 송신자를 고려한 트리기반(Tree-based) μTESLA 프로토콜 등이 제안되었다.

[0010] 다층(Multi-Level) μTESLA에서는 Original μTESLA를 좀 더 큰 규모의 센서 네트워크에 적용할 수 있도록 개선하였다. 그 특징으로 첫째, 동일한 μTESLA 파라메타의 경우 사전결정 방법을 이용하여 전달할 데이터의 양을 줄였다. 둘째, 상위 레벨에 구간이 긴 키 체인을 두고, 구간이 짧은 키 체인을 하위 레벨에 두고 서로를 계층적으로 연결함으로써 인증키의 갱신 주기를 줄였다. 셋째, 메시지 손실과 DoS(Denial of Service) 공격의 피해를 줄이기 위해 메시지를 반복 전송하는 방법과 메시지 인증 지연을 줄이기 위해 다음 구간의 인증키를 현재 구간의 분배 메시지(CDM_i)에 추가하는 방법을 이용하였다.

[0011] 즉. 다층(Multi-Level) μTESLA는 상위레벨의 n개의 긴 구간을 m개의 짧은 구간(Interval$\triangle_1$)으로 나누어 메시지 인증지연 시간을 줄이고, 인증키의 갱신 주기를 줄였다. 분배 메시지(CDM_i)는 다음 구간($Interval_i$)에서 사용될 인증키($K_{i+1,0}$)의 이미지 값을 담고 있으므로, 현재 분배 메시지(CDM_i)를 수신하고 $H(K_{i+1,0})$를 연산하여 값이 동일하면 이전 분배 메시지(CDM_{i-1})를 인증하게 된다. 이후 이전 분배 메시지(CDM_{i-1})의 무결성 검사를 위해서 현재 분배 메시지(CDM_i)의 마지막 파라메타인 K_{i-1}을 이용한다. i번째 구간의 하위 레벨 키 체인의 마지막 키($K_{i-1,n}$)의 분실시 복구가 가능하도록 상위 레벨 키 체인과 하위 레벨 키 체인을 해쉬함수로 서로 연결하였다.

[0012] 그러나 오리지날 μTESLA 및 다층(Multi-Level) μTESLA는 센서 네트워크에 하나의 유선 혹은 무선으로 연결된 단일 송신자가 있는 경우에 적합하다. 센서 네트워크에 송신자가 하나만 위치한 경우, 다수의 수신자들로부터 전달되는 데이터로 인하여 병목현상이 발생하며 송신자 인근에 배치된 중계 노드들의 에너지 소모가 많아지게 된다. 결과적으로 센서 네트워크의 수명을 짧아지게 만든다.

[0013] 트리기반(Tree-based) μTESLA는 하나의 센서 네트워크에 다수의 송신자를 고려함으로써 병목현상을 줄일 수 있으며 광범위한 센서 네트워크에 적용 가능하다.

[0014] 트리기반(Tree-based) μTESLA는 센서 네트워크에 다수의 송신자를 고려하기 위하여 각 송신자 j에 대한 인증서(s_j)와 i번째 구간에 대한 송신자 j의 키 체인에 대한 인증서($s_{j,i}$)를 생성하고, 이를 연산할 수 있는 인증서 파라메타($ParaCert_j$, $ParaCert_{j,i}$)를 수신자에게 전달한다. 트리의 각 노드는 이웃한 하위 레벨 트리 2개를 연접하고 해쉬 함수를 적용함으로써 생성된다.

[0015] 트리기반(Tree-based) μTESLA는 짧은 구간(Interval$\triangle_1$)의 키 체인을 이용하여 메시지 인증지연 시간을 줄이고, 사전 분배된 상위 트리의 루트 값($Root_R$)을 이용하여 송신자로부터 인증서 파라메타($ParaCert_j$, $ParaCert_{j,i}$)를 수신할 경우, 즉시인증이 가능하다. 또한, 송신자를 위해 상위 레벨의 트리 기반 인증서 구조를 이용함으로써 센서 네트워크에 다수의 송신자를 설치할 수 있는 장점이 있다.

[0016] 하지만, 송신자의 수나 소유하는 키 체인의 수가 많은 경우, 트리 높이가 증가하기 때문에 전달해야 하는 $ParaCert_{j,i}$의 데이터 량이 증가하게 된다. 따라서 송○수신자 사이의 통신량 및 연산량이 증가하게 되는 단점을 가지고 있다.

[0017]

[0018] μTPCT-based μTESLA 프로토콜은 트리기반(Tree-based) μTESLA 프로토콜에서 송신자가 소유하는 키 체인의 수가 늘어남에 따라 센서 노드에서의 연산량이 증가하는 문제를 해결하였다. 이 기법은 ITU-T와 ISO/IEC에서 국제표준화로 추진 중인 USN (Ubiquitous Sensor Network)을 위한 보안 프레임워크(X.usnsec-1)에서 센서 네트워크에서의 브로드캐스트 인증 기법으로 채택되었다.

[0019] 트리기반(Tree-based) μTESLA의 하위 트리의 구조를 μTPC(μTESLA Parameter Chain)라 불리는 해쉬 체인 구조로 변경하여, 수신자 측에서의 메시지 인증시 연산에 필요한 인증서 파라메타($ParaCert_{j,i}$)의 데이터양을 줄임으로써 통신량과 수신자의 연산량을 고정적으로 줄이는 효과를 가져왔다. 그러나 μTPCT-based μTESLA 프로토콜의 해쉬 체인 구조는 긴 2구간 이상의 통신 두절시 더 이상 메시지 인증이 불가능하다는 문제점이 있다.

[0020] 요약하면, 트리 기반 인증서 구조는 트리 높이가 높아질 경우 통신량과 연산량이 증가하는 문제점을 가지고 있다. 해쉬 체인 기반 인증서 구조는 트리 기반 인증서 구조의 문제를 해결했지만, 장기간의 통신 두절이 발생할 경우에는 인증이 불가능하다는 문제점이 발생한다.

발명의 내용

해결하려는 과제

[0021] 본 발명의 목적은 상술한 바와 같은 문제점을 해결하기 위한 것으로, 센서 네트워크에서 수신노드가 인증서의 파라미터들을 수신하여 인증하되, 장기간 통신 두절 이후 언제라도 인증서 파라메타를 수신하면 인증할 수 있는 XOR체인을 이용한 트리기반 센서 네트워크 인증 시스템 및 방법을 제공하는 것이다.

[0022] 또한, 본 발명은 순서성을 가진 키체인으로부터 제1 및 제2 키체인 파라미터열을 생성하여 이의 파라미터를 이용하여 인증하되, 키 체인의 수와 관계없이 적은양의 고정된 연산만으로 송신노드(송신자)와 메시지를 인증할 수 있는 XOR체인을 이용한 트리기반 센서 네트워크 인증 시스템 및 방법을 제공하는 것이다.

[0023] 또한, 본 발명은 만들어진 키와 인증서의 값은 각 구간마다 서로 상이해야 하고, 공개되지 않은 키에 대한 정보를 유추할 수 없어야 하는 XOR체인을 이용한 트리기반 센서 네트워크 인증 시스템 및 방법을 제공하는 것이다.

과제의 해결 수단

[0024] 상기 목적을 달성하기 위해 본 발명은 중앙서버, 송신노드, 수신노드로 구성되는 센서 네트워크에서 송신노드와 수신노드 사이를 인증하는 XOR체인을 이용한 트리기반 센서 네트워크 인증방법에 관한 것으로서, (a) 상기 송신노드는 상기 중앙서버로부터 최초키를 수신하여 자신의 제1 및 제2 키체인 파라미터열 및 인증정보를 생성하되,

(a1) 상기 최초키에 해쉬함수를 반복 적용하여 송신노드의 키체인을 형성하고 상기 송신노드의 키체인으로부터 상기 제1 키체인 파라미터열을 생성하는 단계, (a2) 상기 제1 키체인 파라미터열을 모두 XOR 연산하여 상기 인증정보를 생성하는 단계, 및 (a3) 상기 제1 키체인 파라미터열의 각 파라미터(이하 제1 파라미터)와 동일한 열에 대응되는 파라미터(이하 제2 파라미터)로 구성하여 상기 제2 키체인 파라미터열을 생성하되, 상기 인증정보에 상기 제1 파라미터를 XOR 연산하여 상기 제2 파라미터를 생성하는 단계를 포함하는 단계; (b) 상기 수신노드는 상기 송신노드의 인증정보를 수신하는 단계; (c) 상기 송신노드는 상기 제1 및 제2 키체인 파라미터열에서 순차적으로 동일한 열의 제1 및 제2 파라미터를 메시지와 함께 상기 수신노드로 전송하는 단계; (d) 상기 수신노드는 상기 제1 및 제2 파라미터를 XOR 연산하고, XOR 연산결과와 상기 인증정보를 대비하여 상기 메시지를 인증하는 단계를 포함하는 것을 특징으로 한다.

[0025] 또한, 본 발명은 중앙서버, 송신노드, 수신노드로 구성되는 센서 네트워크에서 송신노드와 수신노드 사이를 인증하는 XOR체인을 이용한 트리기반 센서 네트워크 인증방법에 관한 것으로서, (a) 상기 중앙서버는 각 송신노드에 대하여 상기 송신노드의 제1 및 제2 키체인 파라미터열 및 인증정보를 생성하여 상기 송신노드로 전송하되, (a1) 최초키에 해쉬함수를 반복 적용하여 송신노드의 키체인을 형성하고 상기 송신노드의 키체인으로부터 상기 제1 키체인 파라미터열을 생성하는 단계, (a2) 상기 제1 키체인 파라미터열을 모두 XOR 연산하여 상기 인증정보를 생성하는 단계, 및, (a3) 상기 제1 키체인 파라미터열의 각 파라미터(이하 제1 파라미터)와 동일한 열에 대응되는 파라미터(이하 제2 파라미터)로 구성하여 상기 제2 키체인 파라미터열을 생성하되, 상기 인증정보에 상기 제1 파라미터를 XOR 연산하여 상기 제2 파라미터를 생성하는 단계를 포함하는 단계; (b) 상기 수신노드는 상기 송신노드의 인증정보를 수신하는 단계; (c) 상기 송신노드는 상기 제1 및 제2 키체인 파라미터열에서 순차적으로 동일한 열의 제1 및 제2 파라미터를 메시지와 함께 상기 수신노드로 전송하는 단계; (d) 상기 수신노드는 상기 제1 및 제2 파라미터를 XOR 연산하고, XOR 연산결과와 상기 인증정보를 대비하여 상기 메시지를 인증하는 단계를 포함하는 것을 특징으로 한다.

[0026] 또, 본 발명은 XOR체인을 이용한 트리기반 센서 네트워크 인증방법에 있어서, 상기 (a1)단계에서, 상기 최초키를 시드키로 하여 제1 및 제2 해쉬함수를 반복 적용하여 일련의 부분 키체인들을 생성하되, 시드키에 제1 해쉬함수를 반복 적용하여 부분 키체인을 형성하고 부분 키체인의 두 번째 키를 제2 해쉬함수로 해쉬하여 구한 키를 직전 부분 키체인의 시드키로 정하고, 상기 일련의 부분 키체인들의 각 부분 키체인의 초기키를 부분 키체인들의 순서대로 구성하여 상기 송신노드의 키체인으로 생성하는 것을 특징으로 한다.

[0027] 또, 본 발명은 XOR체인을 이용한 트리기반 센서 네트워크 인증방법에 있어서, 상기 (a1)단계에서, 상기 송신노드의 키체인의 각 키에 타임스탬프를 포함하여 상기 제1 키체인 파라미터열의 파라미터를 구하는 것을 특징으로 한다.

[0028] 또, 본 발명은 XOR체인을 이용한 트리기반 센서 네트워크 인증방법에 있어서, 상기 제1 파라미터는 XOR 연산을 할 때 해쉬되어 해쉬된 값으로 연산되는 것을 특징으로 한다.

[0029] 또, 본 발명은 XOR체인을 이용한 트리기반 센서 네트워크 인증방법에 있어서, 상기 중앙서버는 인증서들을 트리구조로 생성하되, 상기 트리구조의 리프노드는 상기 송신노드 각각에 대응되고, 상기 리프노드의 인증서는 대응되는 송신노드의 인증정보를 해쉬한 값으로 정하고, 상기 트리구조의 각 노드는 모든 자식노드의 인증서를 결합하여 해쉬한 값으로 정하는 것을 특징으로 한다.

[0030] 또, 본 발명은 XOR체인을 이용한 트리기반 센서 네트워크 인증방법에 있어서, 상기 수신노드는 상기 루트노드의 인증서 및 상기 송신노드의 인증서들을 수신하고 상기 송신노드의 인증서들로부터 루트노드의 인증서를 연산하여 수신한 루트노드의 인증서와 비교하여 상기 송신노드를 인증하되, 상기 송신노드의 인증서는 상기 송신노드에 대응되는 리프노드의 모든 조상노드의 형제노드의 인증서인 것을 특징으로 한다.

[0031] 또, 본 발명은 XOR체인을 이용한 트리기반 센서 네트워크 인증방법에 있어서, 상기 수신노드는 하위노드의 인증서와 하위노드의 형제노드의 인증서를 결합하고 해쉬하여 상위노드의 인증서를 생성하고, 상위노드의 인증서를 생성하는 과정을 반복하여 루트노드의 인증서를 연산하는 것을 특징으로 한다.

[0032] 또, 본 발명은 XOR체인을 이용한 트리기반 센서 네트워크 인증방법에 있어서, 상기 송신노드는 상기 루트노드의 인증서 및 상기 송신노드의 인증서들을 수신하고 상기 송신노드의 인증서들로부터 루트노드의 인증서를 연산하여 수신한 루트노드의 인증서와 비교하여 상기 중앙서버를 인증하되, 상기 송신노드의 인증서는 상기 송신노드에 대응되는 리프노드의 모든 조상노드의 형제노드의 인증서인 것을 특징으로 한다.

[0033] 또, 본 발명은 XOR체인을 이용한 트리기반 센서 네트워크 인증방법에 있어서, 상기 트리구조는 이진트리인 것을

특징으로 한다.

[0034] 또한, 본 발명은 상기 방법을 수행하는 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체에 관한 것이다.

[0035] 또한, 본 발명은 센서 네트워크에서 XOR체인을 이용한 트리기반 센서 네트워크 인증 시스템에 관한 것으로서, 다수의 송신노드; 각 송신노드에 대하여 상기 송신노드의 제1 및 제2 키체인 파라미터열 및 인증정보를 생성하여 상기 송신노드로 전송하되, 최초키에 해쉬함수를 반복 적용하여 송신노드의 키체인을 형성하고 상기 송신노드의 키체인으로부터 상기 제1 키체인 파라미터열을 생성하고, 상기 제1 키체인 파라미터열을 모두 XOR 연산하여 상기 인증정보를 생성하고, 상기 제1 키체인 파라미터열의 각 파라미터(이하 제1 파라미터)와 동일한 열에 대응되는 파라미터(이하 제2 파라미터)로 구성하여 상기 제2 키체인 파라미터열을 생성하고, 상기 인증정보에 상기 제1 파라미터를 XOR 연산하여 상기 제2 파라미터를 생성하는 중앙서버; 및 상기 송신노드의 인증정보를 수신하고, 상기 송신노드로부터 메시지와 함께 제1 및 제2 파라미터를 수신하여, 상기 제1 및 제2 파라미터를 XOR 연산하고, XOR 연산결과와 상기 인증정보를 대비하여 상기 메시지를 인증하는 수신노드를 포함하는 것을 특징으로 한다.

[0036] 또한, 본 발명은 센서 네트워크에서 XOR체인을 이용한 트리기반 센서 네트워크 인증 시스템에 관한 것으로서, 최초키를 생성하여 전송하는 중앙서버; 상기 최초키를 수신하여 제1 및 제2 키체인 파라미터열 및 인증정보를 생성하되, 상기 최초키에 해쉬함수를 반복 적용하여 송신노드의 키체인을 형성하고 상기 송신노드의 키체인으로부터 상기 제1 키체인 파라미터열을 생성하고, 상기 제1 키체인 파라미터열을 모두 XOR 연산하여 상기 인증정보를 생성하고, 상기 제1 키체인 파라미터열의 각 파라미터(이하 제1 파라미터)와 동일한 열에 대응되는 파라미터(이하 제2 파라미터)로 구성하여 상기 제2 키체인 파라미터열을 생성하고, 상기 인증정보에 상기 제1 파라미터를 XOR 연산하여 상기 제2 파라미터를 생성하는 다수의 송신노드; 및 상기 송신노드의 인증정보를 수신하고, 상기 송신노드로부터 메시지와 함께 제1 및 제2 파라미터를 수신하여, 상기 제1 및 제2 파라미터를 XOR 연산하고, XOR 연산결과와 상기 인증정보를 대비하여 상기 메시지를 인증하는 수신노드를 포함하고, 상기 중앙서버는 상기 송신노드 각각에 대하여 서로 다른 최초키를 생성하여 전송하는 것을 특징으로 한다.

[0037] 또, 본 발명은 XOR체인을 이용한 트리기반 센서 네트워크 인증 시스템에 있어서, 상기 송신노드는 상기 제1 및 제2 키체인 파라미터열에서 열의 순서에 따라 순차적으로 동일한 열의 제1 및 제2 파라미터를 선정하여 메시지와 함께 상기 수신노드로 전송하는 것을 특징으로 한다.

[0038] 또, 본 발명은 XOR체인을 이용한 트리기반 센서 네트워크 인증 시스템에 있어서, 상기 중앙서버는 상기 인증서들을 트리구조로 생성하되, 상기 트리구조의 리프노드는 상기 송신노드 각각에 대응되고, 상기 리프노드의 인증서는 대응되는 송신노드의 인증정보를 해쉬한 값으로 정하고, 상기 트리구조의 각 노드는 모든 자식노드의 인증서를 결합하여 해쉬한 값으로 정하는 것을 특징으로 한다.

[0039] 또, 본 발명은 XOR체인을 이용한 트리기반 센서 네트워크 인증 시스템에 있어서, 상기 수신노드는 상기 루트노드의 인증서 및 상기 송신노드의 인증서들을 수신하고 상기 송신노드의 인증서들로부터 루트노드의 인증서를 연산하여 수신한 루트노드의 인증서와 비교하여 상기 송신노드를 인증하되, 상기 송신노드의 인증서는 상기 송신노드에 대응되는 리프노드의 모든 조상노드의 형제노드의 인증서인 것을 특징으로 한다.

발명의 효과

[0040] 상술한 바와 같이, 본 발명에 따른 XOR체인을 이용한 트리기반 센서 네트워크 인증 시스템 및 방법에 의하면, 키체인으로부터 제1 및 제2 키체인 파라미터열을 생성하여 이들 파라미터열의 동일한 열의 파라미터를 XOR 연산하여 인증함으로써, 장기간 통신 두절 이후 언제라도 인증서 파라메타를 수신하면 인증할 수 있고, 키 체인의 수와 관계없이 적은양의 고정된 연산만으로 인증할 수 있는 효과가 얻어진다.

[0041] 또한, 본 발명에 따른 XOR체인을 이용한 트리기반 센서 네트워크 인증 시스템 및 방법에 의하면, 제1 및 제2 키체인 파라미터열에서 구간마다 한 쌍의 파라미터를 순차적으로 선정하고 해쉬한 값을 통해 인증함으로써, 만들어진 키와 인증서의 값은 각 구간마다 서로 상이하고 공개되지 않은 키에 대한 정보를 유추할 수 없어 보안성을 높이는 효과가 얻어진다.

도면의 간단한 설명

[0042] 도 1은 본 발명을 실시하기 위한 전체 센서 네트워크 구성의 일례를 도시한 도면이다.

도 2와 도 3은 본 발명의 일실시예에 따른 센서 네트워크 인증방법을 설명하는 흐름도이다.

도 4는 본 발명의 일실시예에 따른 키체인의 구조를 도시한 도면이다.

도 5는 본 발명의 일실시예에 따른 파라미터의 구조를 도시한 도면이다.

도 6은 본 발명의 일실시예에 따른 인증서의 구성을 도시한 것이다.

도 7은 본 발명을 종래 기술의 효율성을 대비한 표이다.

* 도면의 주요 부분에 대한 부호의 설명 *

10 : 중앙서버 20 : 송신노드

30 : 수신노드 50 : 인증서의 트리구조

51 : 루트노드 52 : 중간노드

53 : 리프노드

발명을 실시하기 위한 구체적인 내용

[0043] 이하, 본 발명의 실시를 위한 구체적인 내용을 도면에 따라서 설명한다.

[0044] 또한, 본 발명을 설명하는데 있어서 동일 부분은 동일 부호를 붙이고, 그 반복 설명은 생략한다.

[0045] 먼저, 본 발명을 실시하기 위한 전체 센서 네트워크 구성의 일례를 도 1을 참조하여 설명한다.

[0046] 도 1에서 도시한 바와 같이, 본 발명을 실시하기 위한 센서 네트워크는 중앙서버(10), 송신노드(20), 및 수신노드(30)로 구성된다.

[0047] 수신노드(30)는 주변 환경 정보를 수집하는 센서장치로서, 수집하는 정보에 따라 필요한 센서를 장착하여 정보를 수집한다. 수신노드(30)는 수집된 정보를 자신이 속하는 송신노드(20)로 전송한다.

[0048] 송신노드(20)는 수신노드(30)에서 수집된 정보들을 취합하는 컴퓨팅 장치이다. 송신노드(20)는 적어도 2개 이상 다수로 구성된다. 각 송신노드(20)는 자신에게 속하는 수신노드(30)로부터 데이터를 취합하고 취합된 정보를 중앙서버(10)로 전송한다.

[0049] 중앙서버(10)는 센서 네트워크에서 수집된 모든 데이터를 모으는 컴퓨팅 장치이다. 즉, 수신노드(30)에서 수집된 정보들은 송신노드(20)를 통해 중앙서버(10)에서 모두 취합된다.

[0050] 다음으로, 본 발명의 일실시예에 따른 XOR체인을 이용한 트리기반 센서 네트워크 인증방법을 도 2 내지 도 6을 참조하여 설명한다. 도 2와 도 3은 본 발명의 일실시예에 따른 센서 네트워크 인증방법을 설명하는 흐름도이다. 도 4는 본 발명의 일실시예에 따른 키체인의 구조를 도시한 것이고, 도 5는 본 발명의 일실시예에 따른 파라미터의 구조를 도시한 것이다. 도 6은 본 발명의 일실시예에 따른 인증서의 구성을 도시한 것이다.

[0051] 도 2에서 보는 바와 같이, 본 발명의 일실시예에 따른 센서 네트워크 인증방법은 (a) 송신노드(20)는 중앙서버(10)로부터 최초키를 수신하여 자신의 제1 및 제2 키체인 파라미터열 및 인증정보를 생성하는 단계(S10); (b) 수신노드(30)는 송신노드(20)의 인증정보를 수신하는 단계(S20); (c) 송신노드(20)는 제1 및 제2 키체인 파라미터열에서 순차적으로 동일한 열의 제1 및 제2 파라미터를 메시지와 함께 수신노드(30)로 전송하는 단계(S30); (d) 수신노드(30)는 제1 및 제2 파라미터를 XOR 연산하고, XOR 연산결과와 인증정보를 대비하여 메시지를 인증하는 단계(S40)로 구성된다.

[0052] 또한, 도 3에서 보는 바와 같이, 상기 (a)단계는, (a1) 최초키에 해쉬함수를 반복 적용하여 송신노드의 키체인

을 형성하고 상기 송신노드의 키체인으로부터 제1 키체인 파라미터열을 생성하는 단계, (a2) 제1 키체인 파라미터열을 모두 XOR 연산하여 인증정보를 생성하는 단계, 및 (a3) 제1 키체인 파라미터열의 각 파라미터(이하 제1 파라미터)와 동일한 열에 대응되는 파라미터(이하 제2 파라미터)로 구성하여 제2 키체인 파라미터열을 생성하되, 인증정보에 제1 파라미터를 XOR 연산하여 제2 파라미터를 생성하는 단계로 구분된다.

[0053] 보다 구체적으로 설명하면 다음과 같다.

[0054] 먼저, 송신노드(20)는 중앙서버(10)로부터 최초키를 수신하여 최초키를 시드키(seed key)에 해쉬함수를 반복 적용하여 송신노드의 키체인을 형성하고 상기 송신노드의 키체인으로부터 제1 키체인 파라미터열을 생성한다(S11).

[0055] 예를 들어, 도 4a에서 보는 바와 같이, 최초키를 $K_{9,4}$라고 하면, 송신노드(20)는 최초키 $K_{9,4}$를 수신하여 이를 시드키(seed key)로 하여 제1 해쉬함수 $F_1()$을 반복 적용하여 마지막 부분 키체인을 형성한다. 이때, 제1 해쉬함수를 이용하여 부분 키체인을 형성하는 수식은 다음 [수학식 1]과 같다.

[0056] [수학식 1]

[0057] $$K_{i,t-1} = F_1(K_{i,t}),\ (1 \le t \le m-1)$$

[0058] 단, $F_1()$은 제1 해쉬함수이고, m은 부분 키체인의 수이다.

[0059] 이때 부분 키체인(또는 작은 키체인)의 수를 $Interval_0$, $\triangle_0$라고도 표시한다.

[0060] 도 4a에서, 시드키 $K_{9,4}$를 제1 해쉬함수 $F_1()$의 입력 값으로 하여 4 회(m-1회) 반복 연산하여 1개의 부분 키체인(또는 짧은 키체인) { $K_{9,0}$, $K_{9,1}$, $K_{9,2}$, $K_{9,3}$, $K_{9,4}$ }를 만든다.

[0061] 이때, 마지막 부분 키체인의 초기키로 $K_{9,0}$ 이 선정된다.

[0062] 다음으로, 다음 [수학식 2]를 이용하여, 부분 키체인의 초기키의 다음 키(또는 2번째 키)를 제2 해쉬함수로 해쉬한다. 그리고 해쉬하여 구한 키를 다음(next) 부분 키체인의 시드키로 정한다.

[0063] [수학식 2]

[0064] $$K_{t-1,m-1} = F_{01}(K_{t,1}),(0 \le t \le n)$$

[0065] 즉, 도 4a에서, 마지막 부분 키체인의 2번째 키 $K_{9,1}$을 제2 해쉬함수 $F_{01}()$로 해쉬하여 구한 키 $F_{01}(K_{9,1})$을 직전 부분 키체인의 시드키 $K_{8,4}$로 정한다.

[0066] 앞서와 마지막 부분 키체인을 생성하는 것과 같이, [수학식 1]을 이용하여, 마지막 직전(또는 8번째) 부분 키체인을 { $K_{8,0}$, $K_{8,1}$, $K_{8,2}$, $K_{8,3}$, $K_{8,4}$ } 을 생성한다. 그리고 8번째 부분 키체인의 초기값으로 $K_{8,0}$을 선택한다.

[0067] 상기 [수학식 1]과 [수학식 2]를 반복적으로 적용하여, 일련의 부분 키체인들을 생성한다. 그리고 일련의 부분 키체인들의 각 부분 키체인의 초기키를 부분 키체인들의 순서대로 구성하여 송신노드의 키체인으로 생성한다.

[0068] 앞서의 예제의 과정을 반복하면, 모두 10개의 부분 키체인을 생성할 수 있다. 마지막으로 구해지는 첫 번째 키체인은 { $K_{0,0}$, $K_{0,1}$, $K_{0,2}$, $K_{0,3}$, $K_{0,4}$ }이다. 따라서 일련의 부분 키체인들의 각 부분 키체인의 초기키는 $K_{0,0}$, $K_{1,0}$, $K_{2,0}$, ..., $K_{8,0}$, $K_{9,0}$이다.

[0069] 상기 초기키들을 부분 키체인들의 순서대로 구성하여 송신노드의 키체인을 구한다. 즉, 앞서의 예제에서, 송신노드(20)의 키체인은 { $K_{0,0}$, $K_{1,0}$, $K_{2,0}$, ..., $K_{8,0}$, $K_{9,0}$ }이다.

[0070] 다음으로, 송신노드의 키체인으로부터 제1 키체인 파라미터열을 생성한다(S11). 특히, 상기 송신노드의 키체인의 각 키에 타임스탬프를 포함하여 상기 제1 키체인 파라미터열의 파라미터를 구한다.

[0071] 즉, 송신노드 j의 제1 키체인 파라미터열 { $\mu TP_{j,i}$ }$_i$는 다음 [수학식 3]에 의해 구한다.

[0072] [수학식 3]

[0073] $$\mu TP_{j,i} = \{T_s || K_{i,0} || T_i || T_{int} || d\}$$

[0074] 단, T_s, T_i, T_{int}는 각각 현재 시간, 시작 시간, 동기화 구간 크기이고, d는 지연 시간이다. 즉, T_s는 센서 네트워크의 송ㅇ수신노드 간에 시간 동기화를 위한 현재 시간이고, T_i는 전달된 초기 키 값이 이용되는 시작 시간을 의미하고, T_{int}는 키 체인의 동기화 구간 크기를 나타낸다. d는 메시지 키 노출 지연 시간으로, 분배된 $K_{j,i}$는 d 구간만큼 지연된 이후에 사용된다.

[0075] 이때 파리미터를 μTESLA 파라미터라고도 한다.

[0076] 앞서의 예에서, 송신노드 j의 키체인은 { $K_{0,0}$, $K_{1,0}$, $K_{2,0}$, ..., $K_{8,0}$, $K_{9,0}$ }이고, 상기 키체인의 각 키로부터 [수학식 3]을 적용하여 파라미터 $\mu TP_{j,i}$를 생성한다. 즉, 파라미터열 { $\mu TP_{j,0}$, $\mu TP_{j,1}$, $\mu TP_{j,2}$, ..., $\mu TP_{j,8}$, $\mu TP_{j,9}$ }를 생성한다. 이때의 파라미터열을 제1 키체인 파라미터열이라 하고, 파라미터열의 각 파라미터를 제1 파라미터라 부르기로 한다.

[0077] 한편, 공개되는 키의 방향은 키 체인 생성방향과 반대방향이다. 즉, 상기 송신노드의 키체인 또는 제1 키체인 파라미터열에서 공개되는 키 또는 파라미터는 열의 순서대로 공개된다. 예를 들어, 송신노드의 키체인의 각 키들은 $K_{9,0}$, $K_{8,0}$, $K_{7,0}$, ..., $K_{1,0}$, $K_{0,0}$ 의 순서대로 생성되나, 각 키들은 $K_{0,0}$, $K_{1,0}$, $K_{2,0}$, ..., $K_{8,0}$, $K_{9,0}$ 으로 공개된다.

[0078] 다음으로, XORC(XOR 체인) 기반의 제2 파라미터 생성 과정을 설명한다. 즉, 제1 키체인 파라미터열을 모두 XOR 연산하여 송신노드의 인증정보를 생성한다(S12). 특히, 제1 파라미터는 XOR 연산을 할 때 해쉬되어 해쉬된 값으로 연산한다.

[0079] 즉, 송신노드 j의 인증정보 R'_j는 다음 [수학식 4]에 의해 구한다.

[0080] [수학식 4]

[0081] $$R'_j = \{H(\mu TP_{j,0}) \oplus H(\mu TP_{j,1}) \oplus \cdots \oplus H(\mu TP_{j,n-2}) \oplus H(\mu TP_{j,n-1})\}$$

[0082] 단, H는 제3 해쉬함수이다.

[0083] 다음으로, 제1 키체인 파라미터열의 각 파라미터(이하 제1 파라미터)와 동일한 열에 대응되는 파라미터(이하 제2 파라미터)로 구성하여 상기 제2 키체인 파라미터열을 생성하되, 송신노드의 인증정보에 상기 제1 파라미터를 XOR 연산하여 상기 제2 파라미터를 생성한다(S13). 특히, 제1 파라미터는 XOR 연산을 할 때 해쉬하여 해쉬된 값으로 연산하는 것이 바람직하다.

[0084] 즉, 다음 [수학식 5]에 따라, 송신노드 j의 인증정보 R'_j를 이용하여, 송신노드 j의 i번째 부분 키체인(또는 짧은 체인)의 μTESLA 파라미터 값에 대한 제2 파라미터 $S_{j,i}$를 생성한다.

[0085] [수학식 5]

[0086] $$S_{j,i} = \{R'_j \oplus H(\mu TP_{j,i})\}$$

[0087] 이때, H는 제3 해쉬함수이다.

[0088] 도 5는 앞서 설명한 송신노드의 인증정보 및 제2 키체인 파라미터열을 구하는 회로의 구성도를 도시한 것이다.

[0089] 한편, 앞서 설명한 실시예는 송신노드(20)는 중앙서버(10)로부터 최초키를 수신하여 자신의 제1 및 제2 키체인 파라미터열 및 인증정보를 생성한다. 그러나 다른 실시예로서, 중앙서버(10)가 최초키를 이용하여 각 송신노드의 제1 및 제2 키체인 파라미터열 및 인증정보를 생성하여 각 송신노드로 전송한다. 전자의 실시예는 중앙서버

(10)에서 송신노드(20)로 데이터를 전송하는 전송량은 적으나 송신노드(20)의 컴퓨팅 계산량이 많다는 문제점이 있고, 후자의 실시예는 송신노드(20)의 계산 부하량은 적으나 데이터 전송량이 많다는 문제점이 있다.

[0090]

[0091] 한편, 수신노드(30)는 송신노드(20)의 인증정보(또는 인증서)를 사전에 수신한다(S20). 즉, 수신노드(30)는 자신이 속하는 송신노드 j의 인증정보 R'_j(또는 인증서 S_j)를 수신하여 저장하여 둔다.

[0092] 바람직하게는 수신노드(30)는 송신노드(20)의 인증정보와 ID를 연접하여 구성한 인증서를 수신한다. 송신노드 j의 인증서는 송신노드 j의 인증정보 R'_j와 송신노드 j의 ID_j 를 연접하여 구성된다. 즉, 송신노드 j의 인증서 S_j는 다음 [수학식 7]과 같이 $\{R'_j \| ID_j\}$ 이다.

[0093] [수학식 6]

[0094] $$S_j = \{R'_j \| ID_j\}$$

[0095] 그리고 송신노드(20)는 상기 제1 및 제2 키체인 파라미터열에서 순차적으로 동일한 열의 제1 및 제2 파라미터를 메시지와 함께 상기 수신노드(30)로 전송한다(S30).

[0096] 즉, 송신노드 j는 수신노드(30)에게 자신이 소유한 키 $K_{i,0}$ 을 알리기 위해, 다음 [수학식 7]에 의해, 제1 파라미터(μTESLA 파라미터)와 제2 파라미터로 구성된 제1 인증서 파라미터 $ParaCert_{j,i}$를 주기적으로 브로드캐스트한다.

[0097] [수학식 7]

[0098] $$ParaCert_{j,i} = \{S_{j,i} \| \mu TP_{j,i}\}$$

[0099] 이때, 제1 인증서 파라미터 $ParaCert_{j,i}$는 제1 및 제2 키체인 파라미터열의 파라미터들을 순서대로 순차적으로 한 쌍으로 연접하여 전송한다. 예를 들어, 앞서 도 5의 예에서, $\{S_{j,0} \| \mu TP_{j,0}\}$, $\{S_{j,1} \| \mu TP_{j,1}\}$, $\{S_{j,1} \| \mu TP_{j,1}\}$, ..., $\{S_{j,1} \| \mu TP_{j,1}\}$ 순으로 전송한다.

[0100] 다음으로, 수신노드(30)는 상기 제1 및 제2 파라미터를 XOR 연산하고, XOR 연산결과와 상기 인증정보를 대비하여 상기 메시지를 인증한다(S40).

[0101] 즉, 수신노드(30)는 송신노드 j의 제1 및 제2 파라미터 $\{S_{j,i} \| \mu TP_{j,i}\}$를 수신하여, 이들을 XOR 연산한다. 이때, 제1 파라미터는 XOR 연산을 할 때 해쉬하여 해쉬된 값으로 연산한다. 그리고 다음 [수학식 8]과 같이 대비하여 동일여부로 메시지를 인증한다.

[0102] [수학식 8]

[0103] $$R'_j = H(\mu TP_{j,i}) \oplus S_{j,i}$$

$$S_j \stackrel{?}{=} R'_j \| ID_j$$

[0104] 도 5의 예에서, 송신노드 3이 메시지를 보내는 경우, 수신노드(30)는 제1 인증서 파라미터 $ParaCert_{3,2}$를 수신하여, [수학식 8]에 의해 계산한 R'_3을 송신노드 3의 ID_3과 연접하고, 연접한 값이 송신노드 3의 인증서 값 S_3과 동일한지 검사한다. 일치할 경우, 수신했던 데이터를 저장한다.

[0105] 다음으로, 트리구조의 인증서를 설명한다.

[0106] 중앙서버(10)는 인증서들을 트리구조(50)로 생성하되, 상기 트리구조의 리프노드는 상기 송신노드(20) 각각에 대응되고, 상기 리프노드의 인증서는 대응되는 송신노드의 인증정보를 해쉬한 값으로 정하고, 상기 트리구조의 각 노드는 모든 자식노드의 인증서를 결합하여 해쉬한 값으로 정한다.

[0107] 앞서 [수학식 6]에서 본 바와 같이, 송신노드 j의 인증서(S_j)는 키체인의 초기키 값들의 정보(R'_3)와 송신노드 j의 식별자(ID_j)로 구성된다. 바람직하게는 상기 송신노드의 인증서(S_j)를 외부에 노출되지 않도록 다음 [수학식 9]를 이용하여 해쉬한다.

[0108] [수학식 9]

[0109] $$K_j = H(S_j)$$

[0110] 도 6에서 보는 바와 같이, 상기 송신노드 j의 해쉬된 인증서(K_j)가 트리구조(50)에서의 리프노드(53)에 해당한다. 이때 트리구조(50)에서 해쉬된 인증서(K_j)의 리프노드(53)를 "송신노드 j와 대응된다"라고 표시한다.

[0111] 트리구조(50)에서 리프노드(53)가 아닌 중간노드(52) 및 루트노드(51)들은 자신의 자식노드들의 인증서들을 모두 연접(concatenation)하고 해쉬하여 노드 자신의 인증서를 만든다.

[0112] 특히, 도 6의 트리구조는 이진트리이므로, 중간노드(52) 및 루트노드(51)들은 2개의 자식노드들을 가지고 있다. 따라서 [수학식 10]을 이용하여, 2개의 자식노드들의 인증서들을 연접하고 해쉬하여 자신의 인증서를 생성한다.

[0113] [수학식 10]

[0114] $$K_{ab} = H(K_a \| K_b)$$

[0115] 단, 노드 ab는 자식노드 a와 b를 갖는다.

[0116] 상기와 같은 연산을 통해 트리구조의 높이가 올라감에 따라, 노드의 수가 1/2 씩 줄게 된다. 따라서 이진트리의 높이인 L_N회를 반복하면 루트노드(51)의 인증서($Root_R$)를 생성할 수 있다. 루트노드(51)의 인증서($Root_R$)는 센서 네트워크에 참여하고 있는 모든 송신노드 또는 수신노드에게 사전 분배된다.

[0117] 또한, 중앙서버(10)는 송신노드 j에게 전달하려는 정보가 있을 경우, 송신노드 j의 제2 인증서 파라미터를 함께 전달한다. 송신노드 j의 제2 인증서 파라미터 $ParaCert_j$는 다음 [수학식 11]와 같이 구한다.

[0118] [수학식 11]

[0119] $$ParaCert_j = \left\{ S_j \| K_{s(j,1)} \| K_{s(j,2)} \| \ \ldots \ \| K_{s(j,L_N)} \right\}$$

[0120] 단, $K_{s(j,k)}$는 높이 k에 위치하는 리프노드 K_j의 형제노드 또는 리프노드 K_j의 조상노드의 형제노드이다.

[0121] 즉, 송신노드 j의 제2 인증서 파라미터는 자신의 인증서를 포함하고, 그 외에 상기 송신노드 j에 대응되는 리프노드 K_j의 형제노드 및 리프노드 K_j의 모든 조상노드의 형제노드의 인증서들을 더 포함하여 구성된다.

[0122] 도 6의 예에서, 송신노드 3의 제2 인증서 파라미터 $ParaCert_3$은 { $S_3 \| K_4 \| K_{12} \| K_{58}$ }이다. 즉, K_4는 리프노드 K_3의 형제노드이고, K_{12}, K_{58}은 각각 K_3의 조상노드인 K_{34}, K_{14}의 형제노드들이다.

[0123] 다음으로, 송신노드(20)의 메시지 인증 과정을 설명한다.

[0124] 중앙서버(10)로부터 송신노드(20)가 메시지를 수신한 경우, 메시지와 함께 자신의 제2 인증서 파라미터를 함께 수신한다. 도 6의 예에서, 송신노드 3은 메시지 및 제2 인증서 파라미터, 즉, $DATA \| ParaCert_3 = \{ S_3 \| K_4 \| K_{12}$

$\| K_{58} \}$ 을 수신한다.

[0125] 송신노드(20)는 사전분배 받은 루트노드(51)의 인증서($Root_R$)를 이용하여, [수학식 12]에 의해 인증서 파라미터의 연산결과($Root'_R$)와 동일한지 검사한다. 일치할 경우, 수신했던 데이터를 저장한다.

[0126] [수학식 12]

$$Root'_R = \left\{ H(H(K_{12} \| H(H(S_3) \| K_4)) \| K_{58}) \right\}$$

[0127] $$Root_R \stackrel{?}{=} Root'_R$$

[0128] 다음으로, 수신노드(30)의 메시지 인증 과정을 설명한다.

[0129] 수신노드(30)가 송신노드(20)로부터 메시지를 수신한 경우, 다음과 같이, 메시지와 함께 송신노드의 제1 및 제2 인증서 파라미터를 수신한다.

[0130] 그리고 수신노드(30)는 제1 인증서 파라미터를 이용하여 [수학식 12]에 의해, 올바른 송신노드인지를 확인하고, [수학식 9]에서 계산한 R'_j을 이용하여 송신노드 j의 ID_j와 연접한 값이 송신노드 j의 인증서 값 S_j과 동일한지 검사한다. 일치할 경우, 수신했던 데이터를 저장한다.

[0131] 본 발명의 실시예들은 다양한 컴퓨터로 구현되는 동작을 수행하기 위한 프로그램 명령을 포함하는 컴퓨터 판독 가능 매체를 포함한다. 컴퓨터 판독 가능 매체는 프로그램 명령, 로컬 데이터 파일, 로컬 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 매체는 본 발명을 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, CD-ROM, DVD와 같은 광기록 매체, 플롭티컬 디스크와 같은 자기-광 매체, 및 롬, 램, 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.

[0132] 다음으로, 본 발명의 일실시예에 따른 발명의 효과를 도 7을 참조하여 보다 구체적으로 설명한다.

[0133] 본 발명의 효율성을 확인하기 위해서 각 기법에서의 저장, 통신, 연산 오버헤드 및 메시지 복원력과 제안한 인증서 구조의 안전성에 대해 분석하였다. 본 발명(XOR Chain-based μTESLA)과 대비한 기술은 트리기반(Tree-based) μTESLA 와 μTPCT-based μTESLA이다. 센서 네트워크에 N명의 송신노드(20)는 각각 n개의 긴 키 체인을 소유하고 있다고 가정한다.

[0134] 효율성 분석의 결과는 도 7a에서와 같다. 즉, 중앙서버의 연산량에 의한 효율성을 비교하자면 μTPCT-based μTESLA > 본 발명(XOR Chain-based μTESLA) > 트리기반 μTESLA기법 순이다.

[0135] 송신노드의 저장 오버헤드에 의한 효율성을 비교하면, μTPCT-based μTESLA = 본 발명(XOR Chain-based μTESLA) > 트리기반 μTESLA기법 순이다.

[0136] 중앙서버와 송신노드 간의 통신량, 송신자의 연산량, 수신자의 저장량에 의한 효율성을 비교하면, 3 방법 모두 동일하다.

[0137] 송신노드와 수신노드 간의 통신량에 의한 효율성을 비교하면, μTPCT-based μTESLA = 본 발명(XOR Chain-based μTESLA) > 트리기반 μTESLA기법 순이다.

[0138] 수신노드 측면에서의 연산량에 의한 효율성을 비교하면, μTPCT-based μTESLA > 본 발명(XOR Chain-based μTESLA) > 트리기반 μTESLA기법 순이다.

[0139] 한편, 도 7a와 같이, 본 발명은 1회의 XOR 연산만을 추가함으로써 μTPCT-based μTESLA의 방식처럼 수신노드 측면에서 효율적인 메시지 인증 연산량을 갖는다.

[0140] 본 발명 및 트리기반 μTESLA기법에서는 모든 송수신노드가 신뢰하는 루트의 인증서를 전달하기 위해 사전분배 기법을 이용하였다. 따라서 네트워크 상태가 장기간 끊어지더라도, 메시지 인증을 위해 제1 및 제2 인증서 파라미터만 수신한다면 언제라도 메시지 인증이 가능하다.

[0141] μTPCT-based μTESLA에서는 모든 송수신노드가 신뢰하는 루트의 인증서 $Root_R$ 을 사전분배 받음으로써 적은 양의 데이터만을 수신하여 즉시 인증이 가능하다. 하지만, 순서성을 갖는 해쉬 함수 체인를 이용하기 때문에 연속된 입력 값을 알지 못하는 경우 출력 값을 알 수 없다. 그러므로 2구간($2\triangle_0$)간 이상 제1 인증서 파라미터를 수신하지 못하면 이후 수신한 메시지를 모두 인증할 수 없는 문제점이 발생하게 된다.

[0142] 도 7b는 각 기법에서 최대 복구 가능한 분실 기간을 표로 정리한 것이다. 트리기반 μTESLA도 분실 기간에 상관없이 메시지 인증이 가능하지만, 키 체인의 개수에 따라 통신량이 증가하는 단점이 있다. 본 발명은 적은 양의 데이터 통신만으로 언제든 메시지 인증이 가능함을 확인할 수 있다.

[0143] 상기 방법들에서 송신노드 인증을 위해 동일한 상위 트리 기반 인증서 구조를 이용하고, 트리 기반 인증서 구조는 해쉬함수의 안전성에 기반을 둔다. 마찬가지로 각 기법이 이용하는 하위 레벨의 인증서 구조 또한 해쉬함수의 안전성에 기반을 두고 있다. 다만, 본 발명의 경우 XOR 체인을 이용함에 있어, 해쉬함수를 이용하였다. 각 기법 모두에서 n비트의 출력이 발생하는 해쉬 연산을 이용하고 있으므로 모든 기법에서 해쉬 함수를 공격하여 인증서를 위조할 확률은 $2^{n/2}$이다.

[0144] 제안하는 XOR 체인 구조에서는 모두를 XOR 연산한 결과를 기반으로 인증서 또는 인증서 파라미터를 생성하게 된다. 이 과정에서 XOR만을 이용하게 될 경우, 상기 값들이 노출될 수 있는 취약점이 발생한다. 이런 문제점을 해결하기 위해 XOR 체인 연산에 해쉬 연산을 추가하였다. 해쉬 연산을 추가한 XOR 체인 구조가 공개되지 않은 파라미터의 노출 문제를 해결할 수 있음이 증명된다.

[0145] 센서 네트워크에서 수신자의 자원 제약적인 측면은 센서 네트워크의 전체적인 수명에 크게 영향을 미치기 때문에 송신자와 수신자 간에 전달되는 메시지의 양을 최대한 줄여야 하며, 전달된 메시지를 인증하기 위해 소모되는 연산량 또한 최소화시켜야 한다. 더욱이 대부분의 센서 네트워크에서 통신으로 이용하는 브로드캐스트 방식은 수신을 보장할 수 없으므로 반복적인 전송을 기본으로 하고 있다. 손실률이 높은 무선 네트워크라도 수신한 메시지에 대한 인증은 보장되어야 한다.

[0146] 트리 기반 인증서 구조는 트리 높이가 높아질 경우 통신량과 연산량이 증가하는 문제점을 가지고 있다. 해쉬 체인 기반 인증서 구조는 트리 기반 인증서 구조의 문제를 해결했지만, 장기간의 통신 두절이 발생할 경우에는 인증이 불가능하다는 문제점이 발생한다. 본 발명은 이러한 문제를 해결하면서 트리 기반 인증서 구조의 장점과 체인 기반 인증서 구조의 장점을 고루 갖춘 XORC 생성을 위해 XOR 연산과 해쉬 연산을 이용하였다.

[0147] 또한, XOR 연산은 보안상 취약한 요소로 작용할 수 있다. 이를 보완하기 위해서 XORC 생성 이전에 1회의 해쉬 연산을 추가하였다

[0148] 따라서 본 발명은 수신자 측면에서 1회의 XOR 연산이 증가하기는 하지만 고효율의 인증 연산을 지원하고, 장기간의 통신 두절이 발생하더라도 언제든 즉시인증이 가능하다. 2-레벨의 XOR 체인 기반 인증서 구조를 이용하면 상위 레벨 트리 인증서 구조가 가지는 저장, 연산, 통신 오버헤드를 획기적으로 줄일 수 있을 것으로 예상된다.

[0149]

[0150] 이상, 본 발명자에 의해서 이루어진 발명을 실시 예에 따라 구체적으로 설명하였지만, 본 발명은 실시 예에 한정되는 것은 아니고, 그 요지를 이탈하지 않는 범위에서 여러 가지로 변경 가능한 것은 물론이다.

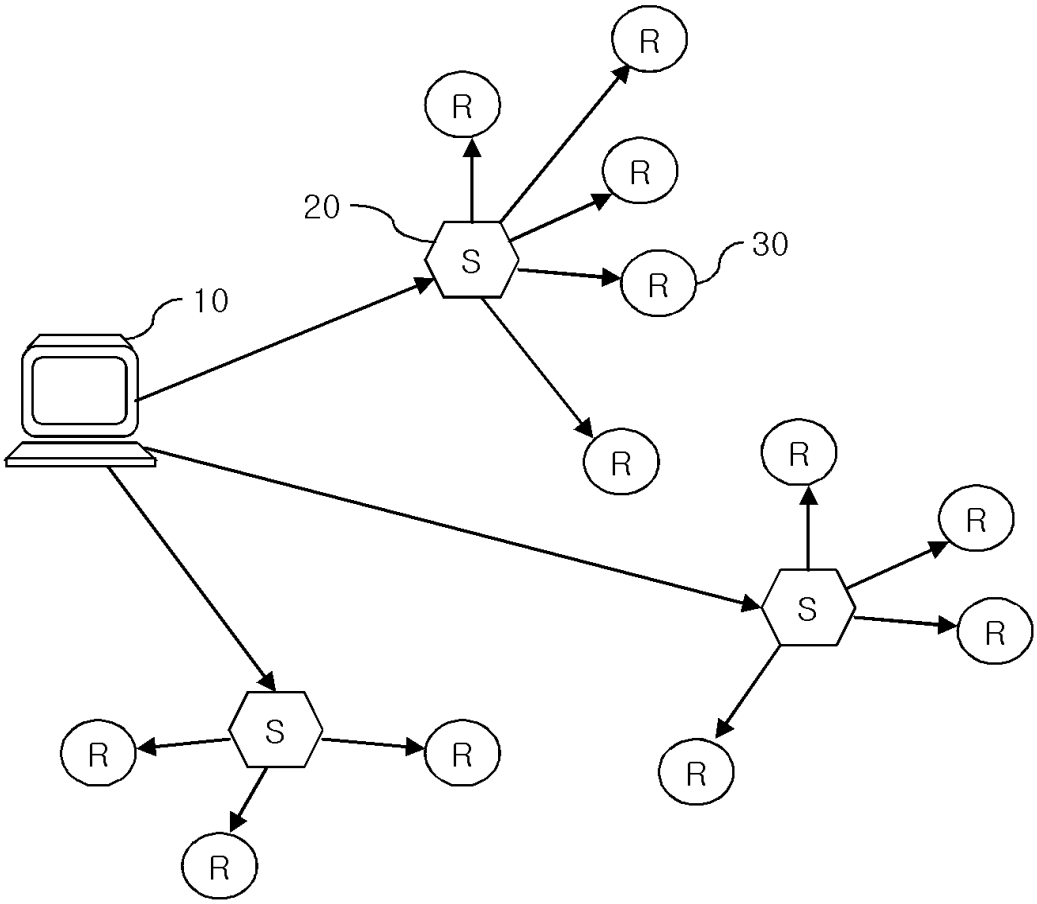
[0151]

산업상 이용가능성

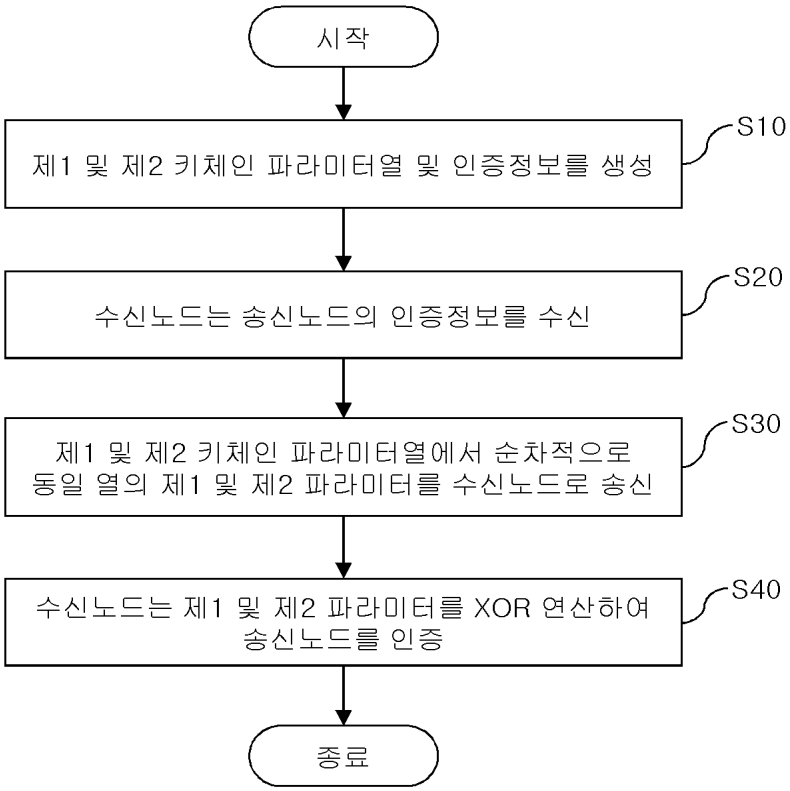
[0152] 본 발명은 I중앙서버, 송신노드, 수신노드로 구성되는 센서 네트워크에서 수신노드가 인증서의 파라미터들을 XOR 연산하여 인증정보와 비교하여 송신노드를 인증하는 XOR체인을 이용한 트리기반 센서 네트워크 인증 시스템을 개발하는 데 적용이 가능하다.

도면

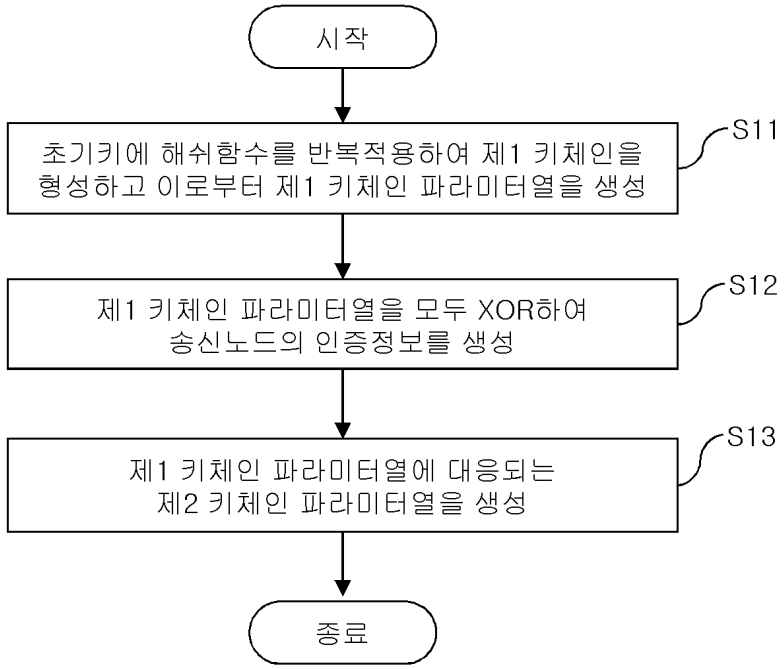
도면1



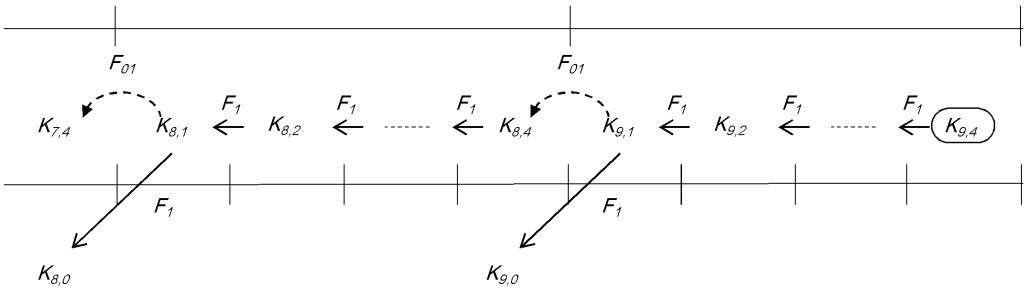
도면2


시작
제1 및 제2 키체인 파라미터열 및 인증정보를 생성
S10
수신노드는 송신노드의 인증정보를 수신
S20
제1 및 제2 키체인 파라미터열에서 순차적으로
동일 열의 제1 및 제2 파라미터를 수신노드로 송신
S30
수신노드는 제1 및 제2 파라미터를 XOR 연산하여
송신노드를 인증
S40
종료

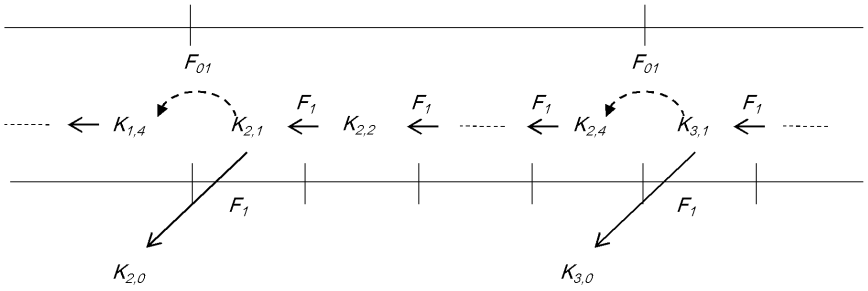
도면3


시작
초기키에 해쉬함수를 반복적용하여 제1 키체인을
형성하고 이로부터 제1 키체인 파라미터열을 생성
S11
제1 키체인 파라미터열을 모두 XOR하여
송신노드의 인증정보를 생성
S12
제1 키체인 파라미터열에 대응되는
제2 키체인 파라미터열을 생성
S13
종료

도면4



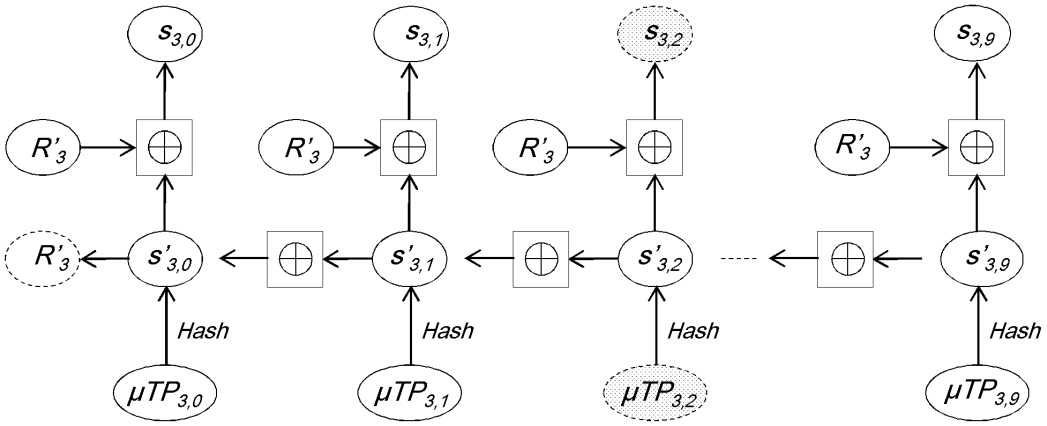
(a)



(b)

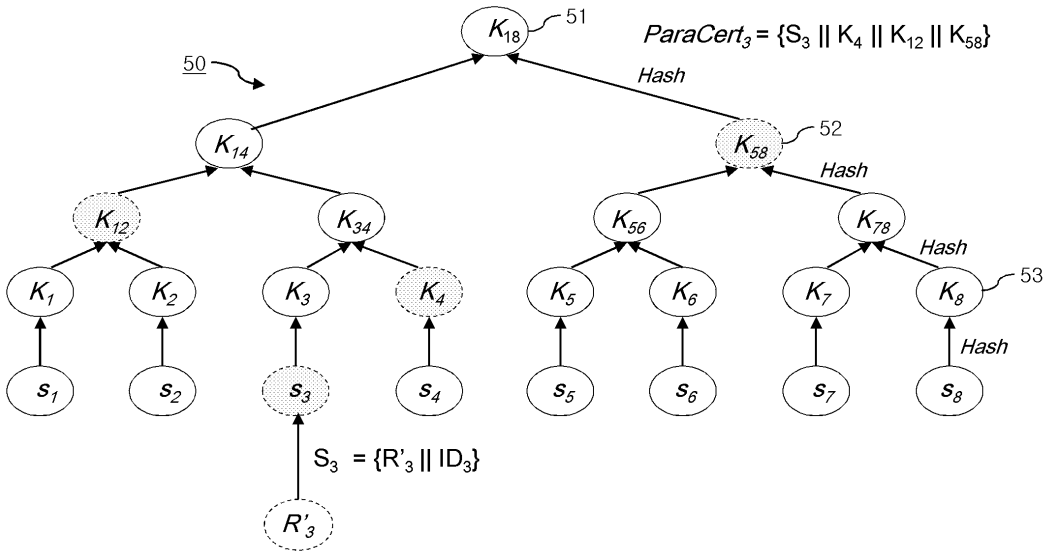
도면5

$$ParaCert_{3,2} = \{S_{3,2} \,||\, \mu TP_{3,2}\}$$



$$\mu TP_{3,2} = \{T_s \,||\, K_{2,0} \,||\, T_i \,||\, T_{int} \,||\, d\}$$

도면6



도면7a

(단위: $|HASH| = |PCert| = |S| = 8bytes, |\mu TP| \geq 8bytes$)

		Tree-based μTESLA(1)	μTPCT-based μTESLA(2)	XORC-based μTESLA(3)
CS	인증서 연산량	$(2^{L_N}-1)h + (2^{L_n}-1)h$	$(2^{L_N}-1)h + nh$	$(2^{L_N}-1)h + nh + (2n-1)x$
BS	저장량	$\|HASH\| + (2^{L_n}-1)\|PCert\|$	$\|HASH\| + n\|PCert\|$	$\|HASH\| + n\|PCert\|$
	CS-BS 통신량	$(L_N-1)\|PCert\| + \|S\|$	$(L_N-1)\|PCert\| + \|S\|$	$(L_N-1)\|PCert\| + \|S\|$
	인증 연산량	$(1+log_2 N)h$	$(1+log_2 N)h$	$(1+log_2 N)h$
SN	저장량	$HASH$	$2HASH$	$HASH$
	BS-CS 통신량	$(L_N-1)\|PCert\| + \|S\| + (L_n-1)\|PCert\| + \|\mu TP\|$	$(L_N-1)\|PCert\| + \|S\| + \|PCert\| + \|\mu TP\|$	$(L_N-1)\|PCert\| + \|S\| + \|PCert\| + \|\mu TP\|$
	인증 연산량	$((log_2 Nn)+2)h$	$((log_2 N)+2)h$	$((log_2 N)+2)h + x$

도면7b

구분	최대 구간	인증 기준	데이터 통신량
Tree	-	$Root_R$	$(L_n-1)PCert + 1\mu TP$
μTPC	1	$U_{j,m-1}$	$1PCert + 1\mu TP$
XORC	-	$Root_R$	$1PCert + 1\mu TP$

*최대 구간 : 인증이 가능한 최대 메시지 손실 구간 기간

*인증기준 : 수신자가 m번째 메시지 인증을 위해 신뢰하고 있는 신뢰하는 값.

*데이터 통신량 : 메시지 인증을 위해 전달되어야 하는 최소한의 데이터 통신량