(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2015년04월23일
(11) 등록번호 10-1513508
(24) 등록일자 2015년04월14일

(51) 국제특허분류(Int. Cl.)
H04L 9/28 (2006.01)
(21) 출원번호 10-2014-0052362
(22) 출원일자 2014년04월30일
심사청구일자 2014년04월30일
(56) 선행기술조사문헌
최진춘 외 3인, "멀티 홉 Unattended WSN에서 가변 키 슬롯 기반 μTESLA의 운영", 한국통신학회 논문지 제39권 제3호(융합기술) (2014.03)

(73) 특허권자
인하대학교 산학협력단
인천광역시 남구 인하로 100, 인하대학교 (용현동)
(72) 발명자
양대헌
서울 서초구 서초중앙로 200, 13동 1407호 (서초동, 삼풍아파트)
강전일
인천광역시 남구 인하로 100 인하대학교 하이테크센터 307호 정보보호연구실
최진춘
인천 남동구 소래역로 93, 909동 2102호 (논현동, 냇마을신영지웰)
(74) 대리인
이원희

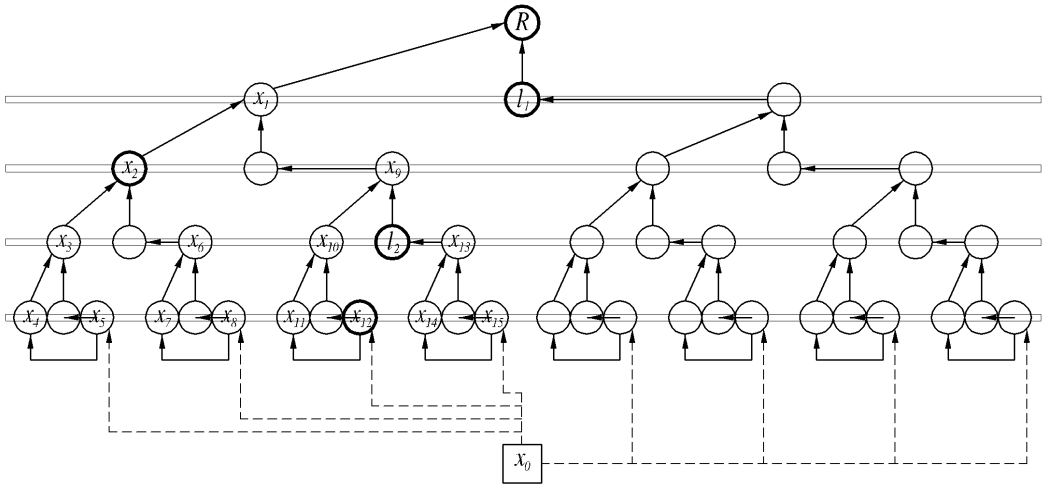
전체 청구항 수 : 총 8 항 심사관 : 문형섭

(54) 발명의 명칭 **해시 트리 기반의 브로드캐스트 메시지 인증 방법 및 장치**

(57) 요 약

해시 트리 기반의 브로드캐스트 메시지 인증 방법 및 장치가 개시된다. 베이스 스테이션에서 브로드캐스트된 메시지 및 키를 이용하여 MAC을 생성하는 단계, 생성된 MAC 및 메시지를 센서 노드에 전송하는 단계, MAC 및 메시지가 전송된 센서 노드에서 해시 연산하는 단계, 해시 연산의 결과값과 해시 트리의 루트 값이 동일한지 판단하는 단계 및 메시지를 인증하는 단계를 포함하고, 해시 연산을 수행하는 단계는, 해시 트리에서 우측 리프(leaf)에 연결된 트리 노드 사이에 링크(link)를 생성한다.

대 표 도 - 도1



명 세 서

청구범위

청구항 1

베이스 스테이션(Base Station, BS)에서 브로드캐스트된 메시지 및 키를 이용하여 메시지 인증 코드(Message Authentication Code, MAC)을 생성하는 단계;

상기 생성된 메세지 및 상기 메시지를 센서 노드에 전송하는 단계;

상기 MAC 및 메시지가 전송된 센서 노드에서 해시 연산하는 단계;

상기 해시 연산의 결과값과 해시 트리의 루트 값이 동일한지 판단하는 단계; 및

상기 메시지를 인증하는 단계;를 포함하고,

상기 해시 연산을 수행하는 단계는,

상기 해시 트리에서 우측 리프(leaf)에 연결된 트리 노드 사이에 링크(link)를 생성하는 것을 특징으로 하는 해시 트리 기반의 브로드캐스트 메시지 인증 방법.

청구항 2

제 1항에 있어서,

상기 해시 트리의 루트(root) 값을 설정하는 단계;를 더 포함하는 것을 특징으로 하는 해시 트리 기반의 브로드캐스트 메시지 인증 방법.

청구항 3

제 1항에 있어서,

상기 센서 노드는 상기 해시 트리의 루트 값을 상기 베이스 스테이션과 공유하는 것을 특징으로 하는 해시 트리 기반의 브로드캐스트 메시지 인증 방법.

청구항 4

제 1항에 있어서,

상기 해시 트리의 트리 노드들은 씨드(seed)로부터 각각 다른 형태로 패딩(padding)된 값을 포함하는 것을 특징으로 하는 해시 트리 기반의 브로드캐스트 메시지 인증 방법.

청구항 5

제 1항에 있어서,

상기 링크는,

해시 연산을 이용하여 생성된 적어도 하나의 트리 노드를 포함하는 것을 특징으로 하는 해시 트리 기반의 브로드캐스트 메시지 인증 방법.

청구항 6

제 1항에 있어서,

상기 해시 연산을 수행하는 단계는,

현재 해시 연산이 수행되는 트리 노드가 우측 리프에 연결된 트리 노드이면 상기 링크의 값을 형제 트리 노드에 전송하고,

현재 해시 연산이 수행되는 트리 노드가 좌측 리프에 연결된 트리 노드이면 기 설정된 트리 노드의 값을 형제 트리 노드에 전송하는 것을 특징으로 하는 해시 트리 기반의 브로드캐스트 메시지 인증 방법.

청구항 7

메시지를 센서 노드로 브로드캐스트(broadcast)하는 입력부;

상기 브로드캐스트된 메시지를 센서 노드에서 해시 연산을 수행하고, 상기 해시 연산의 결과값과 기 설정된 루트 값의 동일여부를 판단하며, 상기 메시지를 인증하는 제어부;를 포함하고,

상기 제어부는,

상기 해시 트리에서 우측 리프(leaf)에 연결된 트리 노드 사이에 링크(link)를 생성하는 것을 특징으로 하는 해시 트리 기반의 브로드캐스트 메시지 인증 장치.

청구항 8

제 7항에 있어서,

상기 제어부는,

현재 해시 연산이 수행되는 트리 노드가 우측 리프에 연결된 트리 노드이면 상기 링크의 값을 형제 트리 노드에 전송하고,

현재 해시 연산이 수행되는 트리 노드가 좌측 리프에 연결된 트리 노드이면 기 설정된 트리 노드의 값을 형제 트리 노드에 전송하는 것을 특징으로 하는 해시 트리 기반의 브로드캐스트 메시지 인증 장치.

발명의 설명

기 술 분 야

[0001] 본 발명은 브로드캐스트 메시지 인증 방법 및 장치에 관한 것으로, 보다 상세하게는 UWSN에서 해시 트리 기반의 브로드캐스트 메시지 인증 방법 및 장치에 관한 것이다.

배 경 기 술

[0002] 상주하지 않는 무선 센서 네트워크(Unattended Wireless Sensor Network, UWSN)는 센서 네트워크에 베이스 스테이션(Base Station, BS)가 상주하지 않고, 일정 주기에 따라 베이스 스테이션이 네트워크를 방문하여 센서 노드들의 데이터를 수집해 가는 환경이다. 이 때, 베이스 스테이션이 센서 노드들에게 메시지를 전달하는 방법 중 하나로 브로드캐스트 메시지를 사용한다. 특히, 브로드캐스트는 그 특성상 공격자가 엿듣거나 브로드캐스트 메시지를 위조 또는 변조하여 재전송하기 쉽다. 이러한 공격에 대응하는 방법으로 μTESLA가 있다.

[0003] μTESLA는 해시 체인을 이용한 대칭키를 이용하여 비대칭적 메시지 인증 기법을 구현한 것으로, 이는 해시 체인을 이용하여 이전 메시지 인증에 사용한 키(key)를 생성할 수 있는 값으로 일정 시간이 지난 후 노출시킴으로써 동작하게 된다. 하지만 μTESLA는 키 슬롯 길이를 짧게 하여 운영하는 경우, 해시 체인이 극단적으로 길어질 수 있다. 이런 문제점을 해결하기 위한 방법 중 하나로 멀티레벨-μTESLA가 있다.

[0004] 멀티레벨-μTESLA는 Long-term 키 체인과 Short-term 키 체인을 따로 운영하여 키 체인의 길이가 길어지는 경우 유용하게 사용된다.

[0005] 그러나 μTESLA나 멀티레벨-μTESLA에서는 베이스 스테이션으로부터 MAC(Message Authentication Code)을 받고 바로 인증하지 못하고 키 슬롯시간을 기다린 뒤 베이스 스테이션이 전송해준 키를 이용하여 인증할 수 있다. 특히, 인증 지연시간을 이용하여 공격자는 DoS공격(Denial of Service Attack)을 할 수 있다.

[0006] 이러한 종래 방법들은 키가 해시 체인으로 묶여있는 방법으로, 모든 센서 노드에 대해 전송되는 원소들(elements)의 수가 많아지는 문제가 있다. 이는 베이스 스테이션이 보낸 메시지를 다른 센서 노드에게 범람(flooding)해서 전달해야 하는 WSN의 특성상 큰 부담으로 적용될 수 있으며, 또한 이런 방법을 사용하여 메시지를 전송할 때 보내야 하는 평균 원소의 개수는 고정되기 때문에 네트워크의 상황에 맞춰 유연하게 운영하기에는 무리가 있다.

[0007] 한국 공개특허 제2012-0052305호는 무선 센서 네트워크에서 데이터의 안전한 브로드캐스트를 보장하기 위한 것으로, WSN의 센서 노드들의 물리적 제한들을 고려하면서 안전한 방식으로 방송중인 소프트웨어를 업데이트하기 위한 방법을 제공한다.

[0008] 논문 정보보호학회 논문지, 17권 1호는 무선센서 네트워크 환경에서 서명 기반 브로드캐스트 인증에 관한 것으로 기존 키 체인을 사용한 μTESLA방식의 인증 시간 지연의 문제점을 해결하고, 리킹(re-keying) 문제가 없는 효율적인 브로드캐스트 인증 기법을 제공한다.

발명의 내용

해결하려는 과제

[0009] 본 발명이 이루고자 하는 기술적 과제는 브로드캐스트 메시지 인증에 사용하는 원소의 개수를 줄일 수 있는 해시 트리 기반의 브로드캐스트 메시지 인증 방법 및 장치를 제공한다.

[0010] 본 발명이 이루고자 하는 다른 기술적 과제는 원소의 개수를 줄임으로써 네트워크에서 사용되는 패킷의 평균 개수를 줄일 수 있는 해시 트리 기반의 브로드캐스트 메시지 인증 방법 및 장치를 제공한다.

[0011] 본 발명이 이루고자 하는 또 다른 기술적 과제는 네트워크에서 센서 노드에게 전송되는 원소와 해시 함수 수행 횟수와의 트레이드오프(trade-off) 관계를 형성할 수 있는 해시 트리 기반의 브로드캐스트 메시지 인증 방법 및 장치를 제공한다.

과제의 해결 수단

[0012] 해시 트리 기반의 브로드캐스트 메시지 인증 방법은,

[0013] 베이스 스테이션(Base Station, BS)에서 브로드캐스트할 메시지 및 키를 이용하여 메시지 인증 코드(Message Authentication Code, MAC)을 생성하는 단계, 상기 생성된 MAC 및 상기 메시지를 해시 트리의 루트 값과 상기 베이스 스테이션이 공유하는 센서 노드에 전송하는 단계, 상기 MAC 및 메시지가 전송된 센서 노드에서 해시 연산하는 단계, 상기 해시 연산의 결과값과 해시 트리의 루트 값이 동일한지 판단하는 단계 및 상기 메시지를 인증하는 단계를 포함하고,

[0014] 상기 해시 연산을 수행하는 단계는, 상기 해시 트리에서 우측 리프(leaf)에 연결된 트리 노드 사이에 링크(link)를 생성한다.

[0015] 해시 트리의 루트(root) 값을 설정하는 단계를 더 포함한다.

[0016] 상기 센서 노드는 상기 해시 트리의 루트 값을 상기 베이스 스테이션과 공유한다.

[0017] 상기 해시 트리의 트리 노드들은 상기 씨드로부터 각각 다른 형태로 패딩(padding)된 값을 포함한다.

[0018] 상기 링크는, 해시 연산을 이용하여 생성된 트리 노드고, 적어도 하나를 포함한다.

[0019] 상기 해시 연산을 수행하는 단계는, 현재 해시 연산이 수행되는 트리 노드가 우측 리프에 연결된 트리 노드이면 상기 링크의 값을 형제 트리 노드에 전송하고, 현재 해시 연산이 수행되는 트리 노드가 좌측 리프에 연결된 트리 노드이면 기 설정된 트리 노드의 값을 형제 트리 노드에 전송한다.

[0020] 해시 트리 기반의 브로드캐스트 메시지 인증 장치는,

[0021] 메시지를 센서 노드로 브로드캐스트(broadcast)하는 입력부,

[0022] 상기 브로드캐스트된 메시지를 상기 센서 노드에서 해시 연산을 수행하고, 상기 해시 연산의 결과값과 기 설정된 루트 값의 동일여부를 판단하며, 상기 메시지를 인증하는 제어부를 포함하고,

[0023] 상기 제어부는, 상기 해시 트리에서 우측 리프(leaf)에 연결된 트리 노드 사이에 링크(link)를 생성한다.

[0024] 상기 제어부는, 현재 해시 연산이 수행되는 트리 노드가 우측 리프에 연결된 트리 노드이면 상기 링크의 값을 형제 트리 노드에 전송하고, 현재 해시 연산이 수행되는 트리 노드가 좌측 리프에 연결된 트리 노드이면 기 설정된 트리 노드의 값을 형제 트리 노드에 전송한다.

발명의 효과

[0025] 본 발명에 따른 해시 트리 기반의 브로드캐스트 메시지 인증 방법 및 장치는 브로드캐스트 메시지 인증에 사용하는 원소의 개수를 줄일 수 있다.

[0026] 또한 원소의 개수를 줄임으로써 네트워크에서 사용되는 패킷의 평균 개수를 줄일 수 있다.

[0027] 또한 네트워크에서 센서 노드에게 전송되는 원소와 해시 함수 수행 횟수와의 트레이드오프(trade-off) 관계를 형성할 수 있다.

[0028] 또한 종래에는 노출되는 형제 트리 노드들 때문에 전체 트리 노드의 절반만 키로 사용할 수 있던 것을 본 발명은 전체 트리 노드의 2/3까지 키로 사용할 수 있다.

도면의 간단한 설명

[0029] 도 1은 본 발명의 일 실시예에 따른 해시 트리 기반의 브로드캐스트 메시지 인증을 설명하기 위한 도면이다.

도 2는 본 발명의 다른 실시예에 따른 해시 트리 기반의 브로드캐스트 메시지 인증을 설명하기 위한 도면이다.

도 3은 본 발명의 일 실시예에 따른 브로드캐스트 메시지 인증 방법을 설명하기 위한 순서도이다.

도 4는 본 발명의 단계 S120을 보다 상세하게 설명하기 위한 순서도이다.

도 5는 본 발명의 일 실시예에 따른 브로드캐스트 메시지 인증 장치를 설명하기 위한 블록도이다.

도 6은 본 발명의 일 실시예에 따른 브로드캐스트 메시지 인증 방법과 종래 방법의 평균 원소 개수를 비교한 그래프이다.

발명을 실시하기 위한 구체적인 내용

[0030] 이하 본 발명의 실시예를 첨부된 도면들을 참조하여 상세히 설명할 수 있다. 우선 각 도면의 구성요소들에 참조부호를 부가함에 있어서, 동일한 구성요소들에 대해서는 비록 다른 도면상에 표시되더라도 가능한 한 동일한 부호를 가지도록 하고 있음에 유의해야 할 수 있다. 또한 본 발명을 설명함에 있어, 관련된 공지 구성 또는 기능에 대한 구체적인 설명이 당업자에게 자명하거나 본 발명의 요지를 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명은 생략할 수 있다.

[0031] 여기서, 후술되는 베이스 스테이션(Base Station, BS), 센서 노드(Sensor Node) 및 트리 노드(Tree Node)를 정의한다. 베이스 스테이션은 센서 네트워크에서 센서 노드들이 수집한 데이터를 수거하거나, 명령을 내리는 센터 역할을 수행한다. 센서 노드는 센서 네트워크에 분산되어 있으며, 센서 노드들이 가지고 있는 센서를 이용하여 주변 데이터를 수집하고, 베이스 스테이션가 요청시 데이터를 전송한다. 본 발명에서 사용되는 트리 노드는 센서 노드와는 구별되어, 해시 트리 등 트리 구조에서 하나의 개체를 의미한다. 예를 들면, 도 1에서 x_1, x_2 등이 트리 노드이며, 특히 맨 아래에 있는 노드들은 리프 트리 노드(Leaf Node)라도 한다.

[0032] 도 1은 본 발명의 일 실시예에 따른 해시 트리 기반의 브로드캐스트 메시지 인증을 설명하기 위한 도면이고, 도 2는 본 발명의 다른 실시예에 따른 해시 트리 기반의 브로드캐스트 메시지 인증을 설명하기 위한 도면이다.

[0033] 도 1 및 도 2를 참조하면, 브로드캐스트 메시지 인증은 머클 해시 트리(Merkle Hash Tree)를 이용하여 인증할 수 있다. 특히, 본 발명의 해시 트리는 해시 트리의 우측 가지에 연결되어 있는 트리 노드 사이에 링크를 생성하여 추가한다.

[0034] 해시 트리의 트리 노드 값인 키(key)를 이용하여 브로드캐스트 메시지를 전송할 때, 해시 트리에서 R을 산출할 수 있는 형제 트리 노드 값을 함께 전송한다. 해시 트리의 루트 값인 R은 센서 노드들이 베이스 스테이션으로부터 전송받은 키를 인증할 때 이용하는 값이다. 특히, 센서 노드들은 상기 값들을 초기에 분배받아 저장된다.

[0035] 해시 트리의 리프 트리 노드들은 x_0를 씨드(seed)로 하여 각기 다른 형태로 패딩(padding)한 값을 이용하여 형성된다. 상기 씨드는 초기값을 사용하는 상수이고, 상기 패딩은 레코드나 블록의 맨 나중에 공백이나 의미가 없는 기호를 부가하여 고정길이로 만드는 것이다. 특히, 패딩은 고정 길이 레코드나 고정 블록이 사용되는 경우에 이용하며, 길이가 짧은 데이터의 처리도 가능하다. 또한 도 2와 같이 x_0와 y_0를 각각 해시 트리의 리프 트리 노드를 형성하기 위한 씨드 값으로 이용할 수 있다.

[0036] 만약 x_{12}를 키 값으로 이용한다면, 베이스 스테이션은 $\{x_{12},\ l_2,\ x_2,\ l_1\}$를 전송하고, x_{12}를 받은 센서 노드는 $H(H(x_2||H(H(H(x_{12})||H(x_{12}))||l_2))||l_1)$을 하여 센서 노드가 가지고 있는 R값을 비교하여 일치하는지 여부를 확인하면 된다.

[0037] 즉, 리프 트리 노드 중에서 x_{12}값을 키로 이용하기 위해서는 x_{12}, x_{12}의 형제 트리 노드를 해시하여 나온 결과 값(l_2), l_2의 형제 트리 노드인 x_2 및 x_2의 형제 트리 노드를 해시하여 나온 결과 값(l_1)을 베이스 스테이션에서 전송받을 수 있다.

[0038] 링크는 적어도 1개를 생성할 수 있으며, 만약 링크를 1개로 메시지 인증을 수행을 하면 종래 방법에 비해 이용되는 평균 원소의 개수를 줄일 수 있다. 즉, 전체 해시 트리에서 이용할 수 있는 트리 노드의 수가 많아지기 때문에 해시 트리의 높이를 낮출 수 있다. 이는 센서 네트워크에서 전송되는 원소들의 수를 줄일 수 있다는 것을 의미한다.

[0039] 도 3은 본 발명의 일 실시예에 따른 브로드캐스트 메시지 인증 방법을 설명하기 위한 순서도이다.

[0040] 도 3을 참조하면, 브로드캐스트 메시지 인증 방법은 해시 트리의 루트 값을 설정하는 단계(S100), MAC을 생성하는 단계(S110), 센서 노드가 해시 연산하는 단계(S120), 해시 연산의 결과값과 루트 값이 동일한지 판단하는 단계(S130) 및 메시지를 인증하는 단계(S140)을 포함한다.

[0041] 해시 트리의 루트 값을 설정하는 단계(S100)는 루트 값을 기 설정한다. 루트 값인 R은 각각 센서 노드들이 미리

가지고 있는 값이다. 특히, 루트값은 센서 노드가 받은 키가 베이스 스테이션으로부터 전송받은 키와 동일한지 인증할 때 이용된다.

[0042] MAC을 생성하는 단계(S110)는 베이스 스테이션에서 브로드캐스트된 메시지 및 키를 이용하여 MAC을 생성하는 단계이다. MAC은 컴퓨터 보안에서 메시지의 내용, 작성자, 발신처 등 속성의 정당성을 검증하기 위해 메시지와 함께 전송되는 임의의 값이다. 따라서 MAC을 생성함으로써 메시지 인증에 대한 신뢰성을 높일 수 있다.

[0043] 또한 생성된 MAC과 브로드캐스트된 메시지를 센서 노드에 전송한다. 또한 해시 트리를 형성할 때 사용되는 초기 값인 씨드를 설정할 수 있다. 즉, 해시 트리의 센서 노드들은 상기 씨드로부터 각각 다른 형태로 패딩된 값을 전송 받을 수 있다. 특히, 씨드는 베이스 스테이션으로부터 키 값으로 이용하려는 센서 노드에 대한 정보를 수신받을 수 있다.

[0044] MAC 및 메시지가 전송된 센서 노드가 해시 연산하는 단계(S120)는 상기 베이스 스테이션으로부터 수신된 키 값으로 이용되는 트리 노드에 관한 해시 연산을 수행한다. 상기 키 값으로 이용되는 트리 노드는 해시 연산을 하면서 그에 해당하는 형제 트리 노드 값을 함께 전송할 수 있다.

[0045] 해시 연산의 결과값과 기 설정된 루트 값의 동일여부를 판단하는 단계(S130)는 베이스 스테이션으로부터 받은 메시지의 키 값과 기 설정된 루트 값의 동일여부를 판단한다. 이를 통해 해시 트리는 브로드캐스트된 메시지가 기 설정된 메시지와 동일한 메시지인지를 판단할 수 있다.

[0046] 메시지를 인증하는 단계(S140)는 메시지의 키 값과 루트 값이 동일하면 기 설정된 메시지이므로 메시지에 대한 인증을 한다. 메시지 인증은 브로드캐스트 중 기 설정된 메시지를 수신 받았다는 것을 의미한다.

[0047] 도 4는 본 발명의 단계 S120을 보다 상세하게 설명하기 위한 순서도이다.

[0048] 도 4를 참조하면, MAC 및 메시지가 전송된 센서 노드가 해시 연산하는 단계는 보다 상세하게 개시할 수 있다.

[0049] 단계 S120는 기 설정된 센서 노드로 메시지의 키 값을 전송하는 단계(S200), 해시 트리에서 우측 리프(leaf)에 연결된 트리 노드 사이에 링크를 생성하는 단계(S210), 우측 리프에 연결된 트리 노드는 링크의 값을 형제 트리 노드에 전송하고, 좌측 리프에 연결된 트리 노드는 원래 트리 노드의 값을 형제 트리 노드에 전송하는 단계(S220)를 포함한다. 또한 현재 트리 노드가 루트인지를 판단하고 만약 루트가 아니면 단계 S220을 반복할 수 있다(S230).

[0050] 기 설정된 센서 노드로 메시지의 키 값을 전송하는 단계(S200)는 센서 노드에 수신된 키 값으로 이용하려는 트리 노드에 메시지의 키 값을 전송한다. 키 값은 메시지에 포함되어 있으며 키 값을 통하여 기 설정된 메시지인지를 판단할 수 있다.

[0051] 해시 트리에서 우측 리프에 연결된 트리 노드 사이에 링크를 생성하는 단계(S210)는 해시 트리의 우측 리프에 연결된 트리 노드에만 해시 연산을 이용하여 링크를 생성하는 단계이다. 또한 링크는 적어도 하나를 생성할 수 있다. 무선 센서 네트워크의 상황에 따라, 링크는 하나 이상일 될 수 있다.

[0052] 본 발명의 해시 트리는 링크의 생성으로 인한 트리 노드 추가로, 전체 트리 노드의 2/3까지 키로 이용할 수 있다. 즉, 해시 트리에서는 시간의 흐름에 따라 트리의 트리 노드가 키로 이용되면서, 노출되는 형제 트리 노드들이 이용될 수 없게 되기 때문에 종래에는 전체 트리 노드의 절반만이 키로 이용할 수 있었다.

[0053] 하지만 본 발명의 해시 트리는 링크를 생성함으로써 형제 트리 노드들을 노출시키는 대신 링크를 노출시키므로써 키로 이용할 수 있는 트리 노드의 수를 보다 많이 확보할 수 있다.

[0054] 트리 노드의 값을 전송하는 단계(S220)는 현재 해시 연산을 수행하는 트리 노드의 위치에 따라 트리 노드를 선택하여 전송한다. 현재 해시 연산을 수행하는 트리 노드가 해시 트리 중 우측 리프에 연결된 트리 노드이면, 수행 중인 트리 노드의 링크 값을 형제 트리 노드에 전송할 수 있다. 또한 현재 해시 연산을 수행하는 트리 노드가 해시 트리 중 좌측 리프에 연결된 트리 노드이면, 수행 중인 트리 노드의 원래 값을 형제 트리 노드에 전송할 수 있다.

[0055] 이를 통해 무선 센서 네트워크에서 센서 노드에게 전송되는 원소들과 해시 함수 수행 횟수와의 트레이드오프(trade-off) 관계를 형성할 수 있다. 또한 각 무선 센서 네트워크의 상황에 접합하도록 센서 노드에 대해 전송해야 하는 원소들의 수를 조절할 수 있다.

[0056] 도 5는 본 발명의 일 실시예에 따른 브로드캐스트 메시지 인증 장치를 설명하기 위한 블록도이다.

[0057] 도 5를 참조하면, 브로드캐스트 메시지 인증 장치(1)는 머클 해시 트리를 이용하여 메시지 인증한다. 브로드캐스트 메시지 인증 장치(1)는 해시 트리의 우측 가지에 연결되어 있는 트리 노드 사이에 링크를 생성하여 추가할 수 있다. 브로드캐스트 메시지 인증 장치(1)는 입력부(110), 제어부(120), 출력부(130) 및 저장부(140)를 포함한다.

[0058] 입력부(110)는 베이스 스테이션으로부터 메시지를 수신한다. 상기 메시지는 키를 포함할 수 있다. 상기 키는 이용하려는 센서 노드에 대한 정보가 포함될 수 있다.

[0059] 제어부(120)는 베이스 스테이션으로부터 수신된 키 값으로 이용되는 트리 노드에 관한 해시 연산을 수행한다. 제어부(120)는 해시 연산을 하면서 그에 해당하는 형제 트리 노드 값을 함께 전송할 수 있다. 또한 제어부(120)는 해시 연산의 결과값과 기 설정된 루트 값의 동일여부를 판단할 수 있다. 이를 통해 제어부(120)는 메시지가 기 설정된 메시지인지 아닌지를 확인할 수 있다.

[0060] 상세하게는, 제어부(120)는 기 설정된 센서 노드로 메시지의 키 값을 전송하고, 해시 트리에서 우측 리프에 연결된 트리 노드 사이에 링크를 생성할 수 있다. 제어부(120)는 우측 리프에 연결된 트리 노드는 링크의 값을 형제 트리 노드에 전송하고, 좌측 리프에 연결된 트리 노드는 원래 트리 노드의 값을 형제 트리 노드에 전송할 수 있다. 또한 제어부(120)는 현재 트리 노드가 루트인지를 판단하고, 만약 루트가 아니면 해시 연산을 반복하고, 루트이면 해시 연산의 결과값과 루트 값을 비교한다.

[0061] 제어부(120)는 해시 트리에서 우측 리프에 연결된 트리 노드 사이에 링크를 생성한다. 제어부(120)는 상기 링크를 적어도 하나를 생성할 수 있다. 특히, 제어부(120)는 무선 센서 네트워크의 상황에 따라, 링크를 하나 이상 생성할 수 있다.

[0062] 이를 통해 제어부(120)는 해시 트리에서 전체 트리 노드의 2/3까지 키로 이용할 수 있다. 즉, 시간의 흐름에 따라 트리의 트리 노드가 키로 이용되면서, 노출되는 형제 트리 노드들이 이용될 수 없게 되기 때문에 종래에는 전체 트리 노드의 절반만이 키로 이용할 수 있었다. 하지만 제어부(120)는 해시 트리에 링크를 생성함으로써 형제 트리 노드들을 노출시키는 대신 링크를 노출시키므로써 키로 이용할 수 있는 트리 노드의 수를 보다 많이 확보할 수 있다.

[0063] 제어부(120)는 현재 해시 연산을 수행하는 트리 노드의 위치에 따라 트리 노드를 선택하여 전송한다. 제어부(120)는 현재 해시 연산을 수행하는 트리 노드가 해시 트리 중 우측 리프에 연결된 트리 노드이면, 수행 중인 트리 노드의 링크 값을 형제 트리 노드에 전송할 수 있다. 또한 제어부(120)는 현재 해시 연산을 수행하는 트리 노드가 해시 트리 중 좌측 리프에 연결된 트리 노드이면, 수행 중인 트리 노드의 원래 값을 형제 트리 노드에 전송할 수 있다.

[0064] 제어부(120)는 현재 해시 연산이 수행 중인 트리 노드가 루트인지 확인할 수 있다. 특히 제어부(120)는 현재 수행 중인 트리 노드가 루트가 아니면 해시 연산을 계속 수행하고, 루트이면 해시 연산의 결과값과 루트 값을 비교한다.

[0065] 즉, 제어부(120)는 해시 연산의 결과값과 기 설정된 루트 값의 동일여부를 판단할 수 있다. 이를 통해 제어부(120)는 해시 트리에 브로드캐스트된 메시지가 기 설정된 메시지와 동일한 메시지인지 판단할 수 있다.

[0066] 출력부(130)는 제어부(120)에서 메시지의 키 값과 루트 값이 동일하다고 판단하면 브로드캐스트된 메시지가 기 설정된 메시지와 동일함으로 메시지에 대한 인증을 한다. 즉, 메시지 인증은 브로드캐스트 중 기 설정된 메시지를 수신 받았다는 것을 의미한다.

[0067] 저장부(140)는 기 설정된 루트 값 및 각 트리 노드의 값이 저장된다. 특히 루트 값은 센서 노드가 받은 키가 베이스 스테이션으로부터 전송받은 키와 동일한지 인증할 때 이용된다. 저장부(140)는 해시 연산을 통해서 산출된 각 트리 노드마다 결과값이 저장될 수 있다. 또한 저장부(140)는 최종적으로 해시 연산으로 산출된 결과값이 저장될 수 있다.

[0068] 도 6은 본 발명의 일 실시예에 따른 브로드캐스트 메시지 인증 방법과 종래 방법의 평균 원소 개수를 비교한 그래프이다.

[0069] 도 6을 참조하면, 브로드캐스트 메시지 인증 방법과 종래 방법이 사용하는 평균 원소 개수를 확인할 수 있다.

[0070] 본 발명에 따른 브로드캐스트 메시지 인증 방법은 링크를 1개 생성하고 메시지 인증을 수행한 것이다. 종래 방법은 Liu, D., Ning, P., Zhu, S. 및 Jajodia, S.의 "Practical broadcast authentication in sensor networks." Mobile and Ubiquitous Systems: Networking and Services, 2005. MobiQuitous 2005. The Second Annual International Conference on(pp. 118-129). IEEE. Jul, 2005에 개시된 방법(LNZJ05)으로 메시지 인증을 수행한 것이다.

[0071] 도 6에 도시된 것 같이, 브로드캐스트 메시지 인증 방법은 종래 방법보다 원소의 개수가 3개가 적다. 이는 한 번에 전송할 수 있는 패킷의 크기가 제한적인 무선 센서 네트워크에서 보내는 패킷의 개수를 줄일 수 있는 장점이 있다는 것을 의미한다.

[0072] 다시 말하면, 본 발명에 따른 해시 트리 기반의 브로드캐스트 메시지 인증 방법 및 장치는 브로드캐스트 메시지 인증에 사용하는 원소의 개수를 줄임으로써 네트워크에서 사용되는 패킷의 평균 개수를 줄일 수 있다.

[0073] 또한 네트워크에서 센서 노드에게 전송되는 원소와 해시 함수 수행 횟수와의 트레이드오프(trade-off) 관계를 형성할 수 있다.

[0074] 또한 종래에는 노출되는 형제 트리 노드들 때문에 전체 트리 노드의 절반만 키로 사용할 수 있던 것을 본 발명은 전체 트리 노드의 2/3까지 키로 사용할 수 있다.

[0075] 본 발명은 또한 컴퓨터로 읽을 수 있는 기록매체에 컴퓨터가 읽을 수 있는 코드로서 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 장치에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록장치를 포함한다. 컴퓨터가 읽을 수 있는 기록매체의 예로는 하드디스크, ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광데이터 저장장치 등이 있으며, 또한 캐리어 웨이브(예를 들어 인터넷을 통한 전송)의 형태로 구현되는 것도 포함한다. 이상에서 본 발명의 바람직한 실시예에 대해 도시하고 설명하였으나, 본 발명은 상술한 특정의 바람직한 실시예에 한정되지 아니하며, 청구범위에서 청구하는 본 발명의 요지를 벗어남이 없이 당해 발명이 속하는 기술분야에서 통상의 지식을 가진 자라면 누구든지 다양한 변형 실시가 가능한 것은 물론이고, 그와

같은 변경은 청구범위 기재의 범위 내에 있게 된다.

부호의 설명

[0076] 1: 브로드캐스트 메시지 인증 장치

110: 입력부

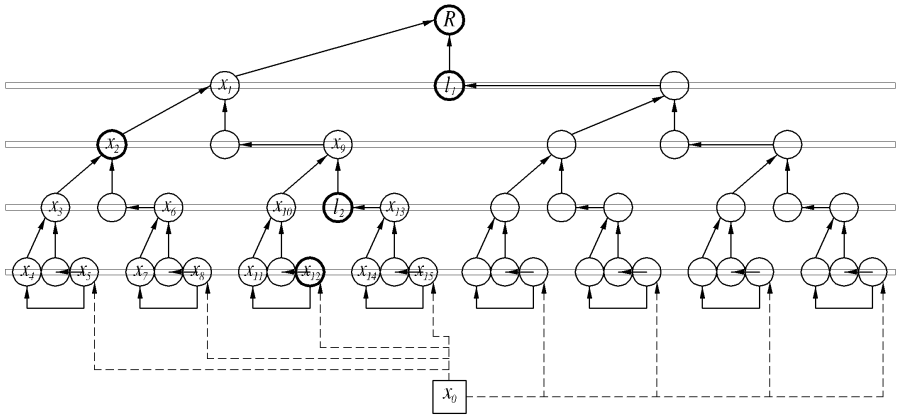
120: 제어부

130: 출력부

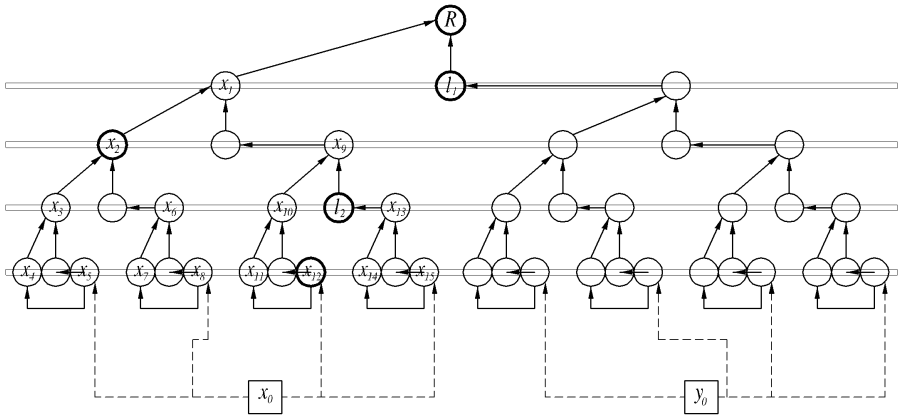
140: 저장부

도면

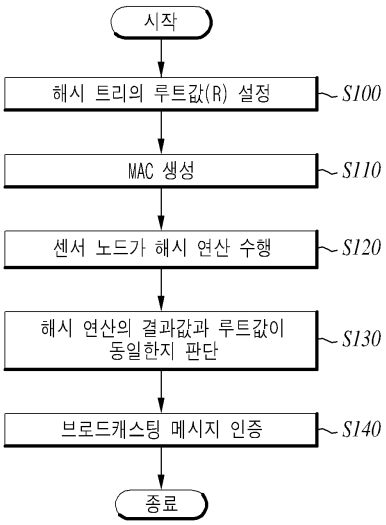
도면1



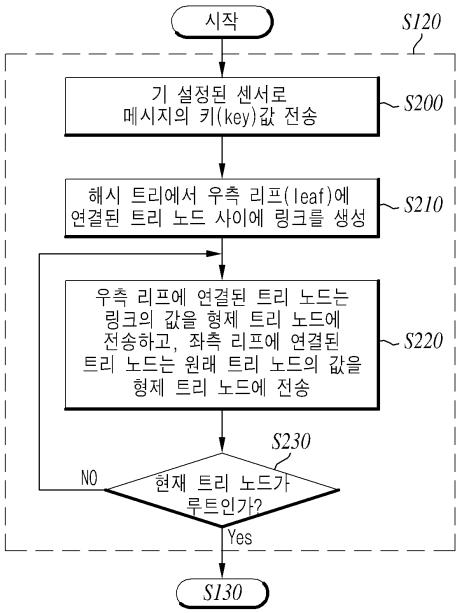
도면2



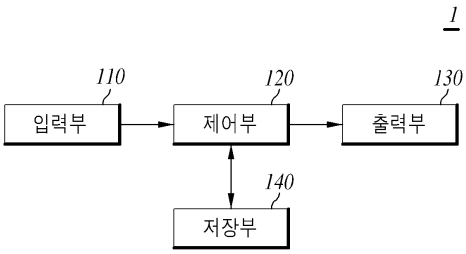
도면3


시작
해시 트리의 루트값(R) 설정
S100
MAC 생성
S110
센서 노드가 해시 연산 수행
S120
해시 연산의 결과값과 루트값이 동일한지 판단
S130
브로드캐스팅 메시지 인증
S140
종료

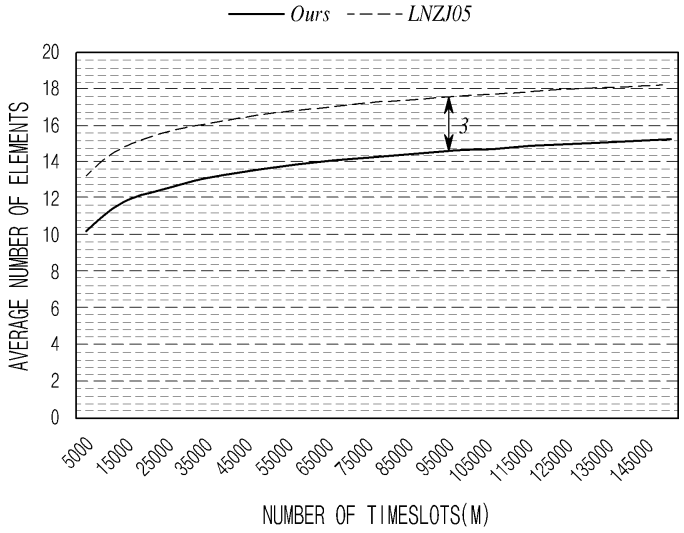
도면4


시작
S120
기 설정된 센서로 메시지의 키(key)값 전송
S200
해시 트리에서 우측 리프(leaf)에 연결된 트리 노드 사이에 링크를 생성
S210
우측 리프에 연결된 트리 노드는 링크의 값을 형제 트리 노드에 전송하고, 좌측 리프에 연결된 트리 노드는 원래 트리 노드의 값을 형제 트리 노드에 전송
S220
S230
현재 트리 노드가 루트인가?
NO
Yes
S130

도면5


1
110
입력부
120
제어부
130
출력부
140
저장부

도면6


Ours
LNZJ05
AVERAGE NUMBER OF ELEMENTS
NUMBER OF TIMESLOTS(M)
3
0
2
4
6
8
10
12
14
16
18
20
5000
15000
25000
35000
45000
55000
65000
75000
85000
95000
105000
115000
125000
135000
145000