(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2009-0072892
(43) 공개일자 2009년07월02일

(51) Int. Cl.
H04L 9/30 (2006.01) *H04L 9/08* (2006.01)
H04L 9/32 (2006.01)
(21) 출원번호 10-2007-0141147
(22) 출원일자 2007년12월29일
심사청구일자 2007년12월29일

(71) 출원인
인하대학교 산학협력단
인천 남구 용현동 253 인하대학교
(72) 발명자
양대헌
서울 서초구 서초동 삼풍 ATP 3동 405호
맹영재
서울 광진구 자양1동 226-12호
아지즈
대전시 유성구 관평동 668 대덕테크노밸리 중앙아파트 305-604
(74) 대리인
김건우

전체 청구항 수 : 총 9 항

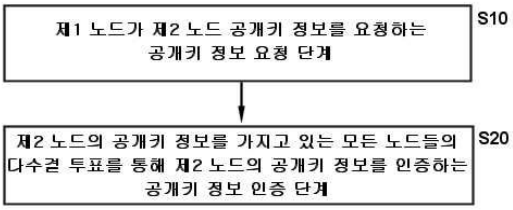
(54) 무선 센서 네트워크에서의 공개키 인증 방법

(57) 요 약

본 발명은 무선 센서 네트워크에서의 협력적인 공개키 인증 방법에 관한 것이다. 본 발명에 따른 무선 센서 네트워크에서의 공개키 인증 방법은, 임의의 제1 노드가 임의의 제2 노드의 공개키를 인증하기 위한 공개키 인증 방법으로서, (1) 상기 제1 노드가 상기 제2 노드에 대하여 상기 제2 노드의 공개키 정보를 요청하는 공개키 정보 요청 단계; 및 (2) 상기 제2 노드의 상기 공개키 정보를 가지고 있는 모든 노드들의 다수결 투표를 통해 상기 제2 노드의 공개키 정보를 인증하는 공개키 정보 인증 단계를 포함하는 것을 그 구성상의 특징으로 한다.

본 발명에서 제안하고 있는 무선 센서 네트워크에서의 공개키 인증 방법에 따르면, 무선 센서 네트워크 내의 임의의 제1 노드가 임의의 제2 노드에 대하여 공개키 정보를 요청하면, 제2 노드의 공개키 정보를 가지고 있는 모든 노드들의 다수결 투표를 통해 제2 노드의 공개키 정보를 어떠한 암호학적 연산 없이도 분산적이고 협력적인 방식으로 인증함으로써, 제한된 자원의 무선 센서 네트워크에서 연결성과 탄력성이 우수한 공개키 암호화 시스템을 이용할 수 있다. 이것은 무선 센서 네트워크에서의 공개키 인증과 관련된 문제를 해결하여 보안성이 높은 무선 센서 네트워크를 구성하는 데 도움이 될 것으로 기대된다.

대 표 도 - 도1



특허청구의 범위

청구항 1

무선 센서 네트워크에서, 임의의 제1 노드가 임의의 제2 노드의 공개키를 인증하기 위한 공개키 인증 방법으로서,

(1) 상기 제1 노드가 상기 제2 노드에 대하여 상기 제2 노드의 공개키 정보를 요청하는 공개키 정보 요청 단계; 및

(2) 상기 제2 노드의 상기 공개키 정보를 가지고 있는 모든 노드들의 다수결 투표를 통해 상기 제2 노드의 공개키 정보를 인증하는 공개키 정보 인증 단계

를 포함하는 방법.

청구항 2

제1항에 있어서, 상기 공개키 정보 인증 단계는,

a. 상기 제1 노드가 상기 제2 노드의 공개키 정보와 관련하여 자신에게 수신되는 응답의 수를 카운트하는 카운트 단계;

b. 상기 카운트 단계의 카운트 결과, 도착한 응답의 수와 상기 제2 노드의 공개키 정보를 가지고 있는 모든 노드들의 수와의 차이가 오차 임계치 이내일 경우, 다수결 투표를 실시하는 다수결 투표 단계; 및

c. 상기 카운트 단계의 카운트 결과, 도착한 응답의 수와 상기 제2 노드의 공개키 정보를 가지고 있는 모든 노드들의 수와의 차이가 오차 임계치보다 클 경우, 수신된 응답을 무시하고 요청 단계를 다시 실행하는 공개키 정보 재요청 단계

를 포함하는 방법.

청구항 3

제2항에 있어서,

상기 다수결 투표 단계는, 다수결 투표 후 상기 제2 노드의 공개키 정보를 가지고 있는 모든 노드들이 상기 제2 노드의 공개키 정보를 자신의 메모리에서 삭제하는 공개키 정보 삭제 단계를 더 포함하는 방법.

청구항 4

제1항에 있어서,

상기 공개키 인증 단계 이후에, 동전 던지기의 확률을 통해 상기 제2 노드의 공개키 정보를 저장하는 공개키 정보 저장 단계를 더 포함하는 방법.

청구항 5

제1항에 있어서,

상기 공개키 정보 요청 단계 이전에, 각각의 노드에 대하여, 소정 개수의 노드를 무작위로 선택하여 상기 각각의 노드의 공개키 정보를 저장하는 초기화 단계를 더 포함하는 방법.

청구항 6

제1항에 있어서,

상기 공개키 정보는 공개키의 해시 값인 것을 특징으로 하는 방법.

청구항 7

제1항에 있어서,

상기 공개키 정보는 인증 라운드 정보를 더 포함하며,

상기 공개키 정보 인증 단계는, 상기 제2 노드의 상기 공개키 정보를 가지고 있는 노드들 중 현재 인증 라운드에 해당하는 인증 라운드 정보를 가지고 있는 노드들만의 다수결 투표를 통해 상기 제2 노드의 공개키 정보를 인증하는 방법.

청구항 8

제7항에 있어서,

상기 공개키 정보 인증 단계 이후, 다음 라운드의 공개키 정보 인증을 위해 인증 라운드 정보를 1만큼 증가시키는 방법.

청구항 9

제1항에 있어서,

상기 공개키 정보는 시리얼 정보를 더 포함하고,

상기 공개키 정보 요청 단계는, 요청 시리얼 정보를 함께 전송하며,

상기 공개키 정보 인증 단계는, 상기 제2 노드의 상기 공개키 정보를 가지고 있는 노드들 중 시리얼 정보가 상기 요청 시리얼 정보와 동일한 노드들만의 다수결 투표를 통해 상기 제2 노드의 공개키 정보를 인증하는 방법.

명 세 서

발명의 상세한 설명

기 술 분 야

<1> 본 발명은 무선 센서 네트워크에서의 협력적인 공개키 인증 방법에 관한 것으로서, 무선 센서 네트워크 내의 임의의 제1 노드가 임의의 제2 노드에 대하여 공개키 정보를 요청하면, 제2 노드의 공개키 정보를 가지고 있는 모든 노드들의 다수결 투표를 통해 제2 노드의 공개키 정보를 어떠한 암호학적 연산 없이도 분산적이고 협력적인 방식으로 인증함으로써, 제한된 자원의 무선 센서 네트워크에서 연결성과 탄력성이 우수한 공개키 암호화 시스템을 이용할 수 있도록 하는 공개키 인증 방법에 관한 것이다.

배 경 기 술

<2> 무선 센서 네트워크(Wireless Sensor Network; WSN)는 마이크로 전자 공학, 반도체, 네트워크, 신호처리 등 다양한 기술들의 복합체이며, 자원이 제한된 센서 노드들은 감지된 데이터를 목적지까지 협력적으로 전달하는데 그 목적이 있다. 센서들은 MITM(Man In The Middle), Sybil, 노드 복제와 같은 공격들이 가능한 공개된 환경에서 peer-to-peer 방법으로 통신한다. 이와 같이 안전하지 않은 환경에서의 보안의 필요성 때문에 WSN의 보안 연구는 센서 노드의 제한된 자원을 이유로 제한된 연결성과 탄력성, 키 선분배의 필요성에도 불구하고 적은 자원의 사용과 빠른 속도를 보이는 대칭키를 이용한 기법이 주로 연구되어 왔다.

<3> 활발하게 연구가 진행된 대칭키와는 달리, 공개키는 필요로 하는 자원이 센서 노드에서 부담이 되어 좀처럼 연구가 진행되지 않았지만 기존의 센서 노드 플랫폼에서 공개키 프로토콜을 시험한 최근의 연구들은 적절한 연산 효율 보여 WSN에서의 공개키 사용 가능성을 보였다. 만약 WSN에서 공개키(ECC, RSA)가 사용될 수 있다면 대칭키에서 문제시되었던 확장성과 연결성과 관련한 문제는 더 이상 존재하지 않을 것이다. 공개키 사용에 있어서 가장 문제시되는 것은 Alice가 요청하여 수신된 Bob의 공개키가 Bob의 것이 옳은가에 대한 것(즉, 공개키의 인증의 문제)인데, 이 문제를 해결하기 위하여 각 노드가 자신을 제외한 모든 노드들의 공개키에 해당하는 (N-1) * P 비트(N: 네트워크 사이즈, P: 공개키의 길이)를 저장하고 수신된 공개키의 인증을 원할 때 키 목록에서 $\log_2 N$ 번의 비교로 검색하는 방법이 있다. 공개키의 키 크기를 고려하여 각 노드가 공개키 대신에 공개키의 해시 값에 해당하는 (N-1) * L 비트(L은 해시된 키의 길이)를 저장하는 방법이 있을 수 있지만 두 방법 모두 메모리 효율 측면에서 좋은 방법은 아니다.

<4> Du등이 연구한 WSN에서의 공개키 인증 기법에서는 Merkle 해시 트리를 이용한다. 이 기법에서 각각의 노드는 $\log_2 N + 1$ 개의 해시 값(트리의 노드에서부터 루트까지)을 가지고 있다. Alice가 Bob의 키를 인증하려 할 때 Alice는 Bob에게서부터 Bob의 해시 값과 공개키를 받는다. Alice는 받은 것을 SHA1 해시한 값이 그녀의 루트와

같은지 비교하는 것으로 수신된 키가 진짜인지 가짜인지 구분해낼 수 있다. 분배 기법을 이용하여 Merkle 트리는 서브트리(Merkle 숲)로 나뉘어 각 노드의 메모리를 줄일 수 있다. 그러므로 각 나뭄은 요구되는 메모리를 키 하나 정도의 크기로 줄일 수 있다.

<5> 그러나 앞서 언급한 모든 종래의 연구들은, 여전히 메모리 효율 측면에서의 한계가 있으며 또한 상당한 암호학적 연산을 요구한다는 문제점이 있다.

발명의 내용

해결 하고자하는 과제

<6> 본 발명은 기존에 제안된 방법들의 상기와 같은 문제점들을 해결하기 위해 제안된 것으로서, 무선 센서 네트워크 내의 임의의 제1 노드가 임의의 제2 노드에 대하여 공개키 정보를 요청하면, 제2 노드의 공개키 정보를 가지고 있는 모든 노드들의 다수결 투표를 통해 제2 노드의 공개키 정보를 어떠한 암호학적 연산 없이도 분산적이고 협력적인 방식으로 인증함으로써, 제한된 자원의 무선 센서 네트워크에서 연결성과 탄력성이 우수한 공개키 암호화 시스템을 이용할 수 있도록 하는 공개키 인증 방법을 제공하는 것을 그 목적으로 한다.

과제 해결수단

<7> 상기한 목적을 달성하기 위한 본 발명의 특징에 따른 무선 센서 네트워크에서의 공개키 인증 방법은,

<8> 임의의 제1 노드가 임의의 제2 노드의 공개키를 인증하기 위한 공개키 인증 방법으로서,

<9> (1) 상기 제1 노드가 상기 제2 노드에 대하여 상기 제2 노드의 공개키 정보를 요청하는 공개키 정보 요청 단계; 및

<10> (2) 상기 제2 노드의 상기 공개키 정보를 가지고 있는 모든 노드들의 다수결 투표를 통해 상기 제2 노드의 공개키 정보를 인증하는 공개키 정보 인증 단계를 포함하는 것을 그 구성상의 특징으로 한다.

<11> 바람직하게는, 상기 공개키 정보 인증 단계는,

<12> a. 상기 제1 노드가 상기 제2 노드의 공개키 정보와 관련하여 자신에게 수신되는 응답의 수를 카운트하는 카운트 단계;

<13> b. 상기 카운트 단계의 카운트 결과, 도착한 응답의 수와 상기 제2 노드의 공개키 정보를 가지고 있는 모든 노드들의 수와의 차이가 오차 임계치 이내일 경우, 다수결 투표를 실시하는 다수결 투표 단계; 및

<14> c. 상기 카운트 단계의 카운트 결과, 도착한 응답의 수와 상기 제2 노드의 공개키 정보를 가지고 있는 모든 노드들의 수와의 차이가 오차 임계치보다 클 경우, 수신된 응답을 무시하고 요청 단계를 다시 실행하는 공개키 정보 재요청 단계를 포함할 수 있다.

<15> 또한 바람직하게는, 상기 다수결 투표 단계는, 다수결 투표 후 상기 제2 노드의 공개키 정보를 가지고 있는 모든 노드들이 상기 제2 노드의 공개키 정보를 자신의 메모리에서 삭제하는 공개키 정보 삭제 단계를 더 포함할 수 있다.

<16> 바람직하게는, 상기 공개키 인증 단계 이후에, 동전 던지기의 확률을 통해 상기 제2 노드의 공개키 정보를 저장하는 공개키 정보 저장 단계를 더 포함할 수 있다.

<17> 바람직하게는, 상기 공개키 정보 요청 단계 이전에, 각각의 노드에 대하여, 소정 개수의 노드를 무작위로 선택하여 상기 각각의 노드의 공개키 정보를 저장하는 초기화 단계를 더 포함할 수 있다.

<18> 바람직하게는, 상기 공개키 정보는 공개키의 해시 값일 수 있다.

<19> 바람직하게는, 상기 공개키 정보는 인증 라운드 정보를 더 포함하며, 상기 공개키 정보 인증 단계는, 상기 제2 노드의 상기 공개키 정보를 가지고 있는 노드들 중 현재 인증 라운드에 해당하는 인증 라운드 정보를 가지고 있는 노드들만의 다수결 투표를 통해 상기 제2 노드의 공개키 정보를 인증할 수 있다.

<20> 또한 바람직하게는, 상기 공개키 정보 인증 단계 이후, 다음 라운드의 공개키 정보 인증을 위해 인증 라운드 정보를 1만큼 증가시킬 수 있다.

<21> 바람직하게는, 상기 공개키 정보는 시리얼 정보를 더 포함하고, 상기 공개키 정보 요청 단계는, 요청 시리얼 정

보를 함께 전송하며, 상기 공개키 정보 인증 단계는, 상기 제2 노드의 상기 공개키 정보를 가지고 있는 노드들 중 시리얼 정보가 상기 요청 시리얼 정보와 동일한 노드들만의 다수결 투표를 통해 상기 제2 노드의 공개키 정보를 인증할 수 있다.

효 과

<22> 본 발명에서 제안하고 있는 무선 센서 네트워크에서의 공개키 인증 방법에 따르면, 무선 센서 네트워크 내의 임의의 제1 노드가 임의의 제2 노드에 대하여 공개키 정보를 요청하면, 제2 노드의 공개키 정보를 가지고 있는 모든 노드들의 다수결 투표를 통해 제2 노드의 공개키 정보를 어떠한 암호학적 연산 없이도 분산적이고 협력적인 방식으로 인증함으로써, 제한된 자원의 무선 센서 네트워크에서 연결성과 탄력성이 우수한 공개키 암호화 시스템을 이용할 수 있다. 이것은 무선 센서 네트워크에서의 공개키 인증과 관련된 문제를 해결하여 보안성이 높은 무선 센서 네트워크를 구성하는 데 도움이 될 것으로 기대된다.

발명의 실시를 위한 구체적인 내용

<23> 이하에서는 첨부된 도면들을 참조하여, 본 발명에 따른 실시예에 대하여 상세하게 설명하기로 한다.

<24> 도 1은 본 발명의 일 실시예에 따른 무선 센서 네트워크에서의 공개키 인증 방법의 구성을 나타내는 도면이다. 도 1에 도시된 바와 같이, 본 발명에서 제안하고 있는 공개키 인증 방법은, 제1 노드가 제2 노드의 공개키 정보를 요청하는 공개키 정보 요청 단계(S10), 및 제2 노드의 공개키 정보를 가지고 있는 모든 노드들의 다수결 투표를 통해 제2 노드의 공개키 정보를 인증하는 공개키 정보 인증 단계(S20)를 포함한다. 각 단계들에 대한 상세한 설명은 아래에서 다루기로 한다.

<25> 먼저 본 발명에서 제안하고 있는 공개키 인증 방법이 적용될 무선 센서 네트워크에 대한 기본적인 가정들을 설명하기로 한다.

<26> 1. 네트워크 모델에 대한 가정

<27> A.1 모든 센서 노드들(또는 같은 클러스터에 속한 노드들)은 같은 주파수 범위를 사용한다. 네트워크의 크기는 물리적 레이어가 아닌 MAC 레이어에 의존하도록 한다.

<28> A.2 네트워크의 노드들(또는 인증에 도움이 될 수 있는 정보를 가진 같은 클러스터에 속한 노드들)은 주어진 시간 내에 노드들의 모든 통신을 도청할 수 있다. 보통의 경우 이 도청은 프레임의 중계 여부를 결정하는데 사용된다. WSN에서의 도청 작업은 애드 혹 네트워크의 것과는 다르므로 정해진 시간에 동작하는 노드가 인증 작업을 도와 유효한 인증 결과를 주는데 충분하다고 가정한다.

<29> A.3 공격자가 지리적으로 같은 영역에 있거나 같은 주파수 범위 안에 있어도 정적 데이터는 한 노드에서부터 다른 노드까지 전송 가능하다.

<30> A.4 공격자는 단일 홉의 전송시간 내에 어떤 노드가 전송할지를 알고 있을 때, 프레임의 차단이나 수정이 가능하다.

<31> A.5 공격자는 인증 작업 동안에 인증 결과에 영향을 줄 수 있는 위조된 프레임을 삽입할 수 있다.

<32> 2. 기본 프로토콜

<33> (1) MAC 프레임 수정

<34> 상기 설명한 네트워크에 대한 가정을 기반으로 두고, 센서 노드에 요구되는 자원을 줄이는 것과 동시에 플러딩 공격을 방지하기 위해 수정한 MAC 프레임을 설명한다.

<35> * 보통 프레임과 인증 프레임을 구별하기 위해 인증을 위한 1비트의 플래그 AC(Authentication Flag)를 기존의 프레임에 추가한다. 이 비트는 k보다 많은 프레임의 수신을 무효화할 때에도 사용된다.

<36> * 인증 프레임은 노드로부터의 인증 요청, 인증 응답 프레임 또는 도우미 노드로부터의 인증 응답 프레임이 될 수 있다. 그러므로 위와 같은 서로 다른 인증 프레임을 구분하기 위해, 2비트의 ARR(Authentication Request Response bits)을 추가한다. 이는 MAC 레이어에서의 플러딩 공격을 방지하기 위함이다.

<37> 도 2는 본 발명의 일 실시예에 따라 수정된 MAC 프레임의 일례를 나타내는 도면이며, 도 3은 본 발명의 일 실시예에 따른 AC와 ARR 비트의 의미를 설명하기 위한 도면이다. 수정된 MAC 프레임은 전체적인 MAC 프로토콜 디자

인에 영향을 주지 않고 소프트웨어 구현 단계에서 선택적으로 사용될 수 있다. 또한, 수정된 MAC 프레임은 경쟁과 스케줄 기반의 MAC 프로토콜에서도 사용될 수 있다. 본 발명에서 제안하고 있는 공개키 인증 방법에서의 프로토콜은 크게 초기화와 온라인 프로시저로 구분된다. 다음에서 본 프로토콜의 초기화를 보인다.

<38> (2) 프로토콜 초기화

<39> 본 발명에서 제안하고 있는 공개키 인증 방법에 따른 프로토콜에서 각 노드는 동전 던지기를 통해 앞면이 선택될 확률(p)을 통하여 키 인증 과정에 참여할지 여부를 결정한다. 네트워크의 각 센서 노드 i는 아래 프로시저를 실행하여 센서 노드의 ID로 묶인 공개키 정보를 설치한다.

<40> 1. TA(Trusted Authority)는 k개의 노드를 무작위로 선택한다.

<41> 2. TA는 노드 i의 공개키 정보인 K_i를 무작위로 선택된 k개의 노드들에게 전송하여 저장시킨다.

<42> K_i = hash(Node i public key|Node i ID)

<43> (3) 온라인 프로시저의 인증 프로토콜

<44> 본 발명의 일 실시예에 따르면, 노드 j가 노드 i의 공개키 정보인 K_i를 얻으려고 할 경우, 아래와 같은 단계들을 실행한다.

<45> 1. 노드 j는 노드 i에게 노드 i의 공개키 정보 K_i를 요청하는 프레임을 보낸다. 2절의 가정에서와 같이 모든 노드들은 이를 도청할 수 있다.

<46> 2. K_i를 가진 모든 노드(노드 i 포함)들은 K_i를 노드 j에게 송신한다. 센서 노드 i는 자신의 공개키를 함께 보낸다.

<47> 3. 노드 j는 첫 번째 응답을 받은 후 한계치의 응답을 받을 때까지 응답 프레임의 수를 카운트한다. 한계치 이상의 응답이 수신되면 노드 j는 이후에 도착하는 같은 키에 대한 모든 응답을 무시한다.

<48> 4. k'를 노드 j에 도착한 응답의 수, e(k의 편차)를 오류 한계치라고 하면,

<49> a. $|k'-k| \leq e$ 일 경우:

<50> (1) 노드 j는 K_i를 정하기 위해 다수결 투표를 한다.

<51> (2) K_i를 가진 모든 노드는 자신의 메모리에서 K_i를 지운다.

<52> b. $|k'-k|>e$ 일 경우: 공격을 뜻하므로 센서 노드는 요청을 다시 하기 위해 수신된 프레임들을 모두 무효화한다.

<53> 5. j를 제외한 모든 노드들은 4단계를 실행하고(가정 A.2만큼의 자원 소모), 4.a의 경우, 즉 $|k'-k| \leq e$ 일 경우에는 아래와 같이 추가로 실행한다.

<54> a. 동전 던지기를 실행한다.

<55> b. 앞면이 나왔을 경우에만 K_i를 저장한다. p(K_i를 유지하는 것과 같은 확률)를 앞면이 나올 확률, N을 네트워크의 노드의 수, k를 평균적으로 K_i를 가지는 노드의 수라 했을 때 p=k/N이다.

<56> 인증이 실행된 후에 도우미 그룹은 공격을 힘들게 하기 위해 오래된 그룹은 공개키 정보를 지우고 무작위 동전 던지기를 통해 새로운 그룹을 생성할 것이다. 다음으로 위에서 언급한 동전 던지기의 편차에 대해 알아본다.

<57> (4) 동전 던지기(Tossing) 편차 제어

<58> 동전 던지기의 확률을 p=k/N라고 할당한다 하여도 노드 i의 공개키 정보 K_i를 가지는 노드들의 수는 평균적으로 k개 정도이다. 이와 같은 프로세스의 확률은 이항 분포를 가진다. 네트워크의 크기를 N이라 하고 k를 평균이라 했을 때 다음 수학식 1과 같은 동전 던지기의 표준 편차를 얻을 수 있다.

수학식 1

$$\sigma = \sqrt{k(1-\frac{k}{N})}$$

<59>

<60> 인증 노드들 k의 평균을 줄이더라도 작은 규모의 네트워크에서 표준 편차는 크게 나타난다. 따라서 수신자는 그 차이가 공격자에게서부터 왔는지 또는 큰 규모의 동전 던지기 편차와 통신 잡음에서 왔는지 구별하기가 쉽지 않다. 큰 규모의 네트워크(예컨대, 노드의 수가 1000 개 이상)의 경우 인증을 돕는 그룹 k의 사이즈에 비하여 편차가 작게 나타나기 때문에 인증은 성공적으로 이루어질 것이다. 아래에서는 작은 규모의 네트워크에서 편차가 크게 나타나는 단점을 보완하기 위한 두 가지 수정된 공개키 인증 방법을 제안한다.

<61> 3. 수정된 공개키 인증 방법

<62> 작은 규모의 네트워크에서 나타나는 큰 편차를 극복하기 위해서 다음 두 가지 수정된 공개키 인증 방법을 추가로 제안한다.

<63> (1) c-rounds 프로토콜: 제한된 수명과 선택적인 보안

<64> 센서 네트워크는 정적으로 동작하므로 분배하기 전에 정확한 공개키 분포 정보를 알 수 있다. 이 프로토콜은 아래와 같이 초기화 단계와 온라인 프로토콜 단계로 나뉜다.

<65> a. 초기화 단계

<66> K_i를 가진 각 노드는 아래와 같이 초기화를 실행한다.

<67> 1. TA는 WSN에서 임의로 k사이즈의 c개의 그룹을 선택한다.

<68> 2. 공개키 정보는 <r, K_i>로 묶인다. 여기서, r은 시리얼을 뜻하며, $0<r\leq c$이다. 다른 쌍들은 해당되는 노드 그룹들에 로드된다. 즉, 같은 그룹의 노드들은 똑같은 시리얼을 가지게 된다.

<69> b. 온라인 인증 단계

<70> 온라인 인증 단계는 다음과 같다.

<71> 1. 노드 j는 노드 i의 공개키 정보를 요청한다.

<72> 2. 노드 i의 공개키 정보를 가지고 있는 다른 노드들은 주어진 키로 인증에 참여할지 여부를 결정하기 위해 현재의 인증 단계를 나타내는 시리얼 r을 유지한다. 이 단계는 키 정보 쌍의 값과 현재 카운터 값에 대한 키 정보를 단순 비교하는 것으로 수행될 수 있다.

<73> 3. 노드 i뿐만 아니라 <r, K_i>를 가진 다른 모든 노드들은 요청에 응답한다(r은 현재의 인증 라운드를 뜻한다). 인증에 참여하는 모든 노드들은 네트워크 트래픽을 도청할 수 있으므로 모든 K_i의 복사본을 가질 수 있다.

<74> 4. 노드 j는 첫 번째 응답을 받자마자 키 정보 프레임 응답의 수를 한계 값까지 카운트하며 저장한다. 노드 i는 한계 값 이후에 도착한 모든 프레임을 버린다.

<75> 5. 노드 j에 대해서 다수결 투표가 실행되고 그룹 구성원들은 K_i를 승낙할지 여부를 결정한다.

<76> 6. 만약 다수결 투표가 K_i를 승낙하면 각각의 노드들은 인증 그룹 안의 모든 K_i의 복사본과 현재의 인증 라운드 r을 자신의 메모리에서 삭제한다.

<77> 7. 다음 라운드에서 다음 인증 그룹이 K_i를 인증하는 것을 돕기 위해 인증 라운드 카운터를 1만큼 증가시킨다.

<78> 위에서 설명한 수정된 공개키 인증 방법은, 다음번 인증 라운드를 예상하기 위해 동전 던지기를 요구하지 않지만 편차 0에 보증하는 공개키 정보의 선 분배에 의존한다. 게다가 이 프로토콜은 어떤 키 K_i에 대해서도 c번의 인증 라운드로 제한되어 있다. 또한 키 인증 프로세스가 시작되면 각 노드는 AC와 ARR 비트 값에 따라 모든 수신중인 프레임을 식별할 수 있어야 하며 인증 프로세스의 현재 상태를 보고 각 노드는 수신된 인증 프레임을 상위 레이어로의 전송 여부 역시 결정할 수 있어야 한다.

<79> (2) Long Living 프로토콜

<80> 앞서 설명한 수정된 공개키 인증 방법에 따른 프로토콜에서 주목해야 할 문제점은 제한된 수명이다. 공격자는 프로토콜의 수명을 단축시키기 위하여 위조된 프레임을 삽입할 수 있다. 이를 해결하기 위하여, 보안 수준을 약간 낮추는 대신 프로토콜의 수명을 연장시키는 또 다른 수정된 공개키 인증 방법(프로토콜)을 추가로 다음과 같이 제안한다.

<81> 1. 노드 j는 <r, req>를 전송하여 공개키 K_i에 대한 인증을 요구한다. 여기서, r은 $o<r\leq c$를 만족하는 무작위의 정수이다.

<82> 2. K_i와 r을 가지고 있는 모든 노드는 요청에 응답한다. 예외적으로 노드 i는 자신의 공개키도 함께 보낸다.

<83> 3. 앞의 프로토콜처럼 노드 i는 응답이 한계치만큼 올 때까지 수신된 K_i의 복사본을 카운트한다. 응답의 수가 한계치를 넘으면 j는 공개키 K_i에 대한 인증을 위한 나머지 모든 프레임을 버린다.

<84> 4. 다수결 투표를 실행한 후에 인증 라운드에 참여한 노드들의 내용은 지우지 않는다.

<85> 5. 같은 키에 대해서 인증이 다시 필요하게 되면 r이 임의로 선택되고 요청이 진행된다.

<86> 6. 공격자는 r과 인증 그룹을 τ 시간 이전에 알아낼 수 있는 경우에만 공격에 성공할 수 있다.

<87> 이상 설명한 본 발명은 본 발명이 속한 기술분야에서 통상의 지식을 가진 자에 의하여 다양한 변형이나 응용이 가능하며, 본 발명에 따른 기술적 사상의 범위는 아래의 특허청구범위에 의하여 정해져야 할 것이다.

도면의 간단한 설명

<88> 도 1은 본 발명의 일 실시예에 따른 무선 센서 네트워크에서의 공개키 인증 방법의 구성을 나타내는 도면.

<89> 도 2는 본 발명의 일 실시예에 따라 수정된 MAC 프레임의 일예를 나타내는 도면.

<90> 도 3은 본 발명의 일 실시예에 따른 AC와 ARR 비트의 의미를 설명하기 위한 도면.

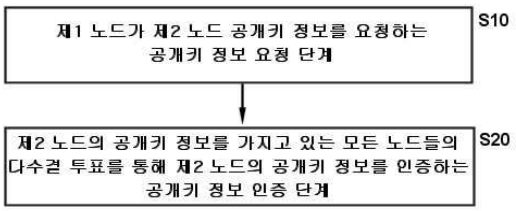
<91> <도면 중 주요 부분에 대한 부호의 설명>

<92> S10: 제1 노드가 제2 노드의 공개키 정보를 요청하는 공개키 정보 요청 단계

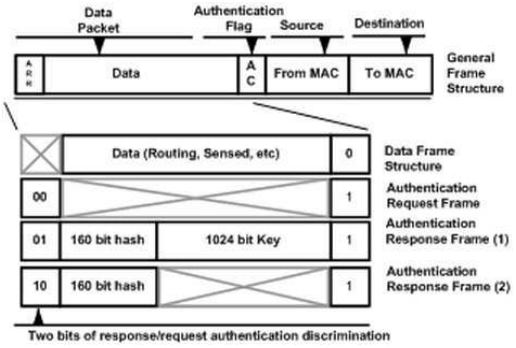
<93> S20: 제2 노드의 공개키 정보를 가지고 있는 모든 노드들의 다수결 투표를 통해 제2 노드의 공개키 정보를 인증하는 공개키 정보 인증 단계

도면

도면1



도면2



도면3

필드 값	의미 (인증)
ARR(00)	요청 프레임
ARR(01)	관련 노드로부터의 응답 프레임
ARR(10)	협조 노드로부터의 응답 프레임
ARR(11)	사용되지 않음
AC(0)	일반 프레임
AC(1)	인증 프레임