(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2010-0117487
(43) 공개일자 2010년11월03일

(51) Int. Cl.
H04L 12/22 (2006.01) *H04W 12/06* (2009.01)
(21) 출원번호 10-2009-0053973
(22) 출원일자 2009년06월17일
심사청구일자 2009년06월17일
(30) 우선권주장
1020090036053 2009년04월24일 대한민국(KR)

(71) 출원인
경희대학교 산학협력단
경기도 용인시 기흥구 서천동 1 경희대학교 국제캠퍼스내
(72) 발명자
홍충선
경기 용인시 수지구 상현동 성원3차상떼빌아파트 233-101
이광현
경기도 부천시 원미구 중2동 꿈마을아파트 1010동 406호
(74) 대리인
서재승

전체 청구항 수 : 총 10 항

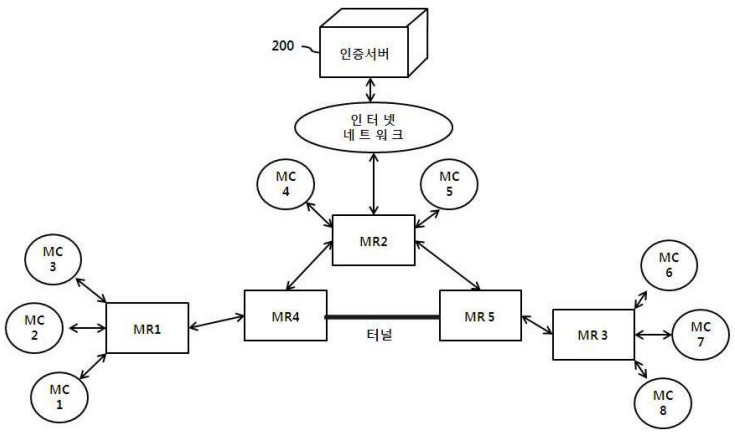
(54) 무선 메쉬 네트워크에서 메쉬 라우터의 인증 방법

(57) 요 약

본 발명은 무선 메쉬 네트워크에서 웜홀 공격을 방지하기 위한 메쉬 라우터의 인증 방법에 관한 것으로, 보다 구체적으로 무선 메쉬 네트워크에 큰 트래픽 부하를 주지 않으면서 높은 보안 레벨을 유지할 수 있는 공개키 기반 방식의 메쉬 라우터 인증 방법에 관한 것이다.

본 발명에 따른 메쉬 라우터의 인증 방법은 인증 서버에 저장되어 있는 메쉬 라우터의 식별자와 공개키를 이용하여 무선 메쉬 네트워크에 접속되어 있는 메쉬 라우터를 인증함으로써 웜홀 공격 라우터를 정확하게 판단할 수 있으며, 메쉬 라우터 단위로 또는 라우팅 경로 상의 모든 메쉬 라우터 단위로 인증을 수행함으로써 무선 메쉬 네트워크의 트래픽 상태에 따라 효율적으로 메쉬 라우터를 인증할 수 있다. 또한, 본 발명에 따른 메쉬 라우터의 인증 방법은 메쉬 라우터의 인증 결과를 반영하여 무선 메쉬 네트워크를 구성하는 모든 메쉬 라우터의 라우팅테이블을 갱신함으로써, 높은 레벨의 보안을 유지할 수 있으며 경제적으로 패킷을 송수신할 수 있다.

대 표 도



특허청구의 범위

청구항 1

무선 메쉬 네트워크에서 웜홀 공격을 방지하기 위한 메쉬 라우터의 인증 방법에 있어서,

(a) 경로설정메시지를 소스 노드에서 목적지 노드로 라우팅하는 상기 메쉬 라우터에서 상기 메쉬 라우터의 개인키로 랜덤 메시지를 암호화하여 서명값을 생성하는 단계;

(b) 상기 생성한 서명값과 상기 서명값을 생성한 메쉬 라우터를 식별하기 위한 식별자를 저장하는 단계;

(c) 상기 서명값과 식별자를 포함하는 인증요청메시지를 생성하고, 상기 생성한 인증요청메시지를 상기 메쉬 무선 네트워크에 접속되어 있는 인증 서버로 송신하는 단계;

(d) 상기 인증 서버는 상기 식별자에 상응하는 메쉬 라우터의 공개키로 상기 서명값을 복호화하고, 상기 식별자 또는 상기 복호화한 서명값에 기초하여 상기 메쉬 라우터가 웜홀 공격 라우터인지를 인증하는 단계; 및

(e) 상기 메쉬 라우터의 식별자와 상기 메쉬 라우터의 인증값을 포함하는 인증확인메시지를 생성하여 상기 인증요청메시지를 생성한 메쉬 라우터로 송신하는 단계를 포함하는 메쉬 라우터의 인증 방법.

청구항 2

제 1 항에 있어서, 상기 인증요청메시지는

상기 인증 서버의 공개키로 암호화되어 상기 인증 서버로 송신되며, 상기 인증 서버는 수신한 인증요청메시지를 인증 서버의 개인키로 복호화하는 것을 특징으로 하는 메쉬 라우터의 인증 방법.

청구항 3

제 2 항에 있어서, 상기 인증확인메시지는

상기 인증요청메시지를 생성한 메쉬 라우터의 공개키로 암호화되어 있는 것을 특징으로 하는 메쉬 라우터의 인증 방법.

청구항 4

제 3 항에 있어서, 상기 (c) 단계에서

상기 인증요청메시지는 상기 목적지 노드의 메쉬 라우터에서 생성되어 상기 소스 노드의 메쉬 라우터로 송신되며, 상기 소스 노드의 메쉬 라우터는 송신된 인증요청메시지를 상기 인증 서버로 송신하는 것을 특징으로 하는 메쉬 라우터의 인증 방법.

청구항 5

제 4 항에 있어서, 상기 (c) 단계는

(c1) 상기 소스 노드에서 목적지 노드로 상기 경로설정메시지를 라우팅하는 모든 메쉬 라우터에서 생성된 서명값과 식별자를 상기 인증 서버의 공개키로 암호화하는 단계;

(c2) 상기 암호화된 서명값과 식별자를 포함하는 인증요청메시지를 생성하는 단계;

(c3) 상기 생성한 인증요청메시지를 상기 소스 서버의 메쉬 라우터로 송신하는 단계; 및

(c4) 상기 소스 서버의 메쉬 라우터에서 상기 인증 서버로 상기 암화화된 인증요청메시지를 송신하는 단계를 포함하는 메쉬 라우터의 인증 방법.

청구항 6

제 3 항에 있어서, 상기 (c) 단계에서

상기 인증요청메시지는 상기 경로설정메시지를 다음 홉 메쉬 라우터로 라우팅하는 이전 메쉬 라우터에서 생성되며, 상기 인증요청정메시지를 생성한 이전 메쉬 라우터는 상기 인증요청메시지를 상기 인증 서버로 송신하는 것

을 특징으로 하는 메쉬 라우터의 인증 방법.

청구항 7

제 6 항에 있어서, 상기 이전 홉 메쉬 라우터는

상기 다음 홉 메쉬 라우터로부터 멀티캐스팅되는 경로설정메시지를 응답시간 내에 수신하지 못하는 경우, 상기 다음 홉 메쉬 라우터를 라우팅 경로에서 제외하는 것을 특징으로 하는 메쉬 라우터의 인증 방법.

청구항 8

제 1 항 내지 제 7 항 중 어느 한 항에 있어서,

(f) 상기 인증확인메시지를 수신한 메쉬 라우터의 개인키로 상기 인증확인메시지를 복호화하는 단계;

(g) 상기 복호화한 인증확인메시지의 인증값에 기초하여 웜홀 공격 라우터로 판단된 메쉬 라우터를 라우팅 테이블에서 삭제하여 라우팅 테이블을 갱신하는 단계; 및

(h) 상기 갱신한 라우팅 테이블에 기초하여 설정된 라우팅 경로를 변경하고, 상기 인증확인메시지를 주변 메쉬 라우터로 브로딩캐스팅하는 단계를 더 포함하는 메쉬 라우터의 인증 방법.

청구항 9

무선 메쉬 네트워크에서 웜홀 공격을 방지하기 위한 메쉬 라우터의 인증 방법에 있어서,

소스 노드에서 목적지 노드로 경로설정메시지를 라우팅하는 모든 메쉬 라우터에서 생성된 서명값과 식별자를 포함하는 인증요청메시지를 수신하는 단계;

상기 인증요청메시지에 구비되어 있는 식별자가 상기 인증 서버에 기저장된 식별자 리스트에 포함되어 있는지 비교 판단하는 단계;

상기 판단한 식별자의 메쉬 라우터에 상응하는 공개키로 상기 인증요청메시지에 구비되어 있는 상기 메쉬 라우터의 서명값을 복호화 가능한지 판단하는 단계; 및

상기 비교 판단 결과와 복호화 가능 판단 결과에 기초하여 상기 메쉬 라우터를 인증하는 단계를 포함하는 메쉬 라우터의 인증 방법.

청구항 10

제 9 항에 있어서, 상기 인증요청메시지는

상기 인증 서버의 공개키로 암호화되어 있어 있는 것을 특징으로 하는 메쉬 라우터의 인증 방법.

명 세 서

발명의 상세한 설명

기 술 분 야

[0001] 본 발명은 무선 메쉬 네트워크에서 웜홀 공격을 방지하기 위한 메쉬 라우터의 인증 방법에 관한 것으로, 보다 구체적으로 무선 메쉬 네트워크에 큰 트래픽 부하를 주지 않으면서 높은 보안 레벨을 유지할 수 있는 공개키 기반 방식의 메쉬 라우터 인증 방법에 관한 것이다.

배 경 기 술

[0002] 기존 무선LAN의 한계를 극복하기 위해 다양한 새로운 기술동향 중 무선 메쉬 네트워크 기술이 등장하였다. 현재 IEEE 802.11에서는 TGs에서 표준화를 다루고 있으며 홈네트워킹 분야의 IEEE 802.15에서는 TG5에서 무선메쉬 네트워크 표준화를 다루고 있다. 무선 메쉬 네트워크는 기존의 점대 점, 점대 다점의 무선통신의 방식과는 달리, 유선망의 메쉬 형태의 네트워크 구조를 무선망에서도 같은 구조를 가짐으로 망의 신뢰도 및 적은 출력을 이

용한 무선망의 확장 등의 장점을 가지는 기술로, 차세대 이동통신, 홈네트워킹, 공공안전과 같은 특수 목적 네트워크 등 다양한 분야에서 활용될 수 있다.

[0003] 무선 메쉬 네트워크의 형태는 크게 기반망(infrastructure) 방식의 무선 메쉬 네트워크, 클라이언트 무선 메쉬 네트워크 및 하이브리드 무선 메쉬 네트워크 3종류로 구분할 수 있다. 도 1 내지 도 3은 3가지 형태의 무선 메쉬 네트워크의 일 예에 대한 구성을 도시하고 있다.

[0004] 도 1을 참고로 기반망 방식의 무선 메쉬 네트워크에 대해 보다 구체적으로 살펴보면, 기반만 방식의 무선 메쉬 네트워크는 다수의 메쉬 라우터(MR)와 각 메쉬 라우터(MR)에 접속되어 있는, Wi-FI, 와이브로(Wibro), 이동 단말기(cellular)와 같은 다수의 메쉬 클라이언트(MC)로 구성되어 있다. 메쉬 라우터(MR) 중 일부는 인터넷 게이트웨이(IGW)의 역활을 수행하며, 인터넷 게이트웨이를 통해 외부의 인터넷 네트워크에 접속된다. 메쉬 클라이언트는 메쉬 라우터(MR)를 통해 메쉬 네트워크 내에서 통신을 수행하거나 인터넷 게이트웨이의 역할을 수행하는 메쉬 라우터(MR)를 통해 외부 인터넷 네트워크와 통신을 수행한다.

[0005] 도 2를 참고로 클라이언트 무선 메쉬 네트워크에 대해 보다 구체적으로 살펴보면, 클라이언트 무선 메쉬 네트워크에는 별도의 메쉬 라우터(MR)가 구비되어 있지 않으며 메쉬 클라이언트(MC) 디바이스 상호 간에 피투피(P2P:peer-2-peer) 통신을 수행한다. 클라이언트 무선 메쉬 네트워크는 실질적으로 애드-혹(ad-hoc) 네트워크와 유사한 방식으로 동작하며 메쉬 클라이언트(MC) 디바이스들은 자율적으로 무선 메쉬 네트워크에 가입하여 상호 간에 데이터를 송수신한다. 그러나 클라이언트 무선 메쉬 네트워크의 메쉬 클라이언트(MC)는 라우팅 기능과 함께 자가구성(self-configuration)의 기능이 있어야 하므로 애드-혹 네트워크를 구성하는 노드보다 높은 성능과 에너지를 요구한다.

[0006] 도 3을 참고로 하이브리드 무선 메쉬 네트워크에 대해 보다 구체적으로 살펴보면, 하이브이드 무선 메쉬 네트워크는 기반망 무선 메쉬 네트워크와 클라이언트 무선 메쉬 네트워크의 형태를 결합한 형태의 네트워크이다. 메쉬 클라이언트(MC)는 자가구성 기능과 라우팅 기능이 있어 피투피 통신 방식으로 상호 간에 통신을 수행하거나, 메쉬 라우터(MR)를 통해 통신을 수행한다. 또한, 메쉬 클라이언트(MC)는 메쉬 라우터(MR)를 통해 외부 인터넷 네트워크에 접속할 수 있다.

[0007] 위에서 살펴본 3가지 형태의 무선 메쉬 네트워크는 공통적으로 무선 메쉬 네트워크와 동일한 무선 인터페이스를 사용하는 외부 이동 노드가 자율적으로 무선 메쉬 네트워크에 접속하여 메쉬 클라이언트와 통신을 할 수 있다는 것이다. 따라서 악의적인 외부 이동 노드가 무선 메쉬 네트워크에 접속하여 메쉬 클라이언트 사이에서 송수신되는 데이터를 조작하거나 메쉬 클라이언트의 데이터를 불법으로 해킹할 수 있다.

[0008] 도 4는 무선 메쉬 네트워크의 대표적인 공격 방법인 웜홀(wormhole) 공격 방식을 설명하기 위한 도면이다.

[0009] 도 4를 참고로 보다 구체적으로 살펴보면, 웜홀 공격 라우터들(AR1, AR2)은 정상적인 노드인 것처럼 무선 메쉬 네트워크에 접속되어 있다. 무선 메쉬 네트워크에 접속되어 있는 웜홀 공격 라우터들(AR1, AR2)은 최적화된 방법으로 웜홀 공격 라우터1(AR1)과 웜홀 공격 라우터2(AR2) 사이에 터널을 형성한다. 이때 터널은 여러 가지 형태로 구성되어 질 수 있는데, 예를 들어 상대적으로 빠른 속도를 보장하는 유선 혹은 정상적인 대역폭 이상의 대역폭을 가지는 터널을 구성하거나, 넓은 지역을 커버할 수 있는 주파수를 사용하여 터널을 구성한다. 혹은 소스 노드(MC1)에서 목적지 노드(MC7)로 송신되는 패킷을 웜홀 공격 라우터1(AR1)과 웜홀 공격 라우터2(AR2) 사이에 형성된 터널에서 캡슐화하여 소스 노드(MC1)에서 목적지 노드(MC7)로 송신할 수 있다.

[0010] 웜홀 공격 라우터들(AR1, AR2)은 이렇게 구성된 터널을 이용하여 주변 메쉬 라우터들로 하여금 터널을 통해서 패킷의 라우팅 경로를 구성하도록 유도한다. 정상적인 라우팅 프로토콜에 의해서 경로가 설정되면, 소스노드(MC1)에서 송신되는 패킷은 소스 메쉬 라우터(MR1)-웜홀 공격 라우터1(AR1)-중간 메쉬 라우터(MR2)-웜홀 공격 라우터메쉬2(AR2)-목적지 메쉬 라우터(MR3)의 경로를 지나서 목적지노드(D)에 도착한다. 그러나 웜홀 공격 라우터들(AR1, AR2)은 정상적인 라우팅 경로보다 최적화된 경로를 제공한다고 주변 메쉬 라우터들에게 알려줌으로써, 패킷의 라우팅 경로를 정상적인 경로가 아닌 비정상적인 경로, 즉 웜홀 공격 라우터1(AR1)과 웜홀 공격 라우터2(AR2) 사이에서 형성된 터널을 통해서 구성하게 된다. 패킷 송신의 비용적인 측면에서 웜홀 공격 라우터(AR1, AR2)가 형성한 터널을 포함하는 라우팅 경로가 유용한 것처럼 보이지만 웜홀 공격 라우터(AR1, AR2)는 형성한 터널을 통해 송수신되는 패킷들을 조작하거나 드롭(drop)하는 등 2차적인 공격이 가능하다.

[0011]

[0012]

발명의 내용

해결 하고자하는 과제

[0013] 위에서 설명한 무선 메쉬 네트워크에서 발생하는 웜홀 공격의 특징은 다른 라우팅 공격과는 다르게 단일 노드의 공격이 아닌 2개 이상의 불법 노드들이 함께 공격한다는 점에서 단일 노드에 비해서 공격탐지가 쉽지 않다. 따라서 무선 메쉬 네트워크에 접속되어 있는 웜홀 노드를 발견하거나 웜홀 노드를 거치지 않는 라우팅 경로의 구성 방법이 필요하다.

[0014] 무선 메쉬 네트워크는 애드-혹 네트워크와 비교하여 메쉬 클라이언트 또는 메쉬 라우터가 하드웨어적으로 높은 성능을 구비하고 있으며 제한되지 않은 에너지 자원을 사용할 수 있어 보다 높은 레벨의 보안 알고리즘을 적용하여 인증받지 않은 악의적인 이동 노드의 접속을 차단할 수 있다.

[0015] 본 발명이 이루고자 하는 목적은 무선 메쉬 네트워크에서 발생하는 웜홀 공격을 방지하기 위한 메쉬 라우터의 인증 방법을 제공하는 것이다.

[0016] 본 발명이 이루고자 하는 다른 목적은 무선 메쉬 네트워크에 큰 트래픽 부하를 주지 않으면서 웜홀 공격을 방지할 수 있는 메쉬 라우터의 인증 방법을 제공하는 것이다.

[0017] 본 발명이 이루고자 하는 또 다른 목적은 발견한 웜홀 노드를 메쉬 라우터의 라우팅 테이블에 반영하여 신뢰있는 라우팅 경로를 설정할 수 있는 메쉬 라우터의 인증 방법을 제공하는 것이다.

과제 해결수단

[0018] 위에서 언급한 본 발명의 목적을 달성하기 위하여, 본 발명에 따른 메쉬 라우터의 인증 방법은 경로설정메시지를 소스 노드에서 목적지 노드로 라우팅하는 메쉬 라우터에서 메쉬 라우터의 개인키로 랜덤 메시지를 암호화하여 서명값을 생성하는 단계와, 생성한 서명값과 서명값을 생성한 메쉬 라우터를 식별하기 위한 식별자를 저장하는 단계와, 서명값과 식별자를 포함하는 인증요청메시지를 생성하고 생성한 인증요청메시지를 메쉬 무선 네트워크에 접속되어 있는 인증 서버로 송신하는 단계 및 인증 서버는 식별자에 상응하는 메쉬 라우터의 공개키로 서명값을 복호화하고, 식별자 또는 복호화한 서명값에 기초하여 메쉬 라우터를 인증하는 단계를 포함한다. 여기서 인증요청메시지를 송신하는 일 예는 목적지 노드에서 생성되어 소스 노드로 송신되며, 소스 노드는 목적지 노드로부터 송신된 인증요청메시지를 인증 서버로 송신한다. 인증요청메시지를 송신하는 다른 예는 경로설정메시지를 다음 홉 메쉬 라우터로 라우팅하는 이전 메쉬 라우터에서 생성되며, 인증요청정메시지를 생성한 이전 메쉬 라우터는 인증요청메시지를 인증 서버로 송신한다.

[0019] 바람직하게, 경로설정메시지를 라우팅하는 모든 메쉬 라우터의 인증 결과를 인증 서버로부터 소스 노드로 송신하거나 또는 다음 홉 메쉬 라우터의 인증 결과를 인증 서버로부터 이전 홉 메쉬 라우터로 송신하고, 인증 결과를 소스 노드 또는 이전 홉 메쉬 라우터의 주변 메쉬 라우터들에게 브로딩캐스팅하여 인증되지 않은 메쉬 라우터를 이전 홉 메쉬 라우터 또는 주변 메쉬 라우터에 저장되어 있는 라우팅 테이블에서 삭제하는 것을 특징으로 한다.

[0020] 또한, 위에서 언급한 본 발명의 목적을 달성하기 위하여, 본 발명에 따른 메쉬 라우터의 인증 방법은 소스 노드에서 목적지 노드로 경로설정메시지를 라우팅하는 모든 메쉬 라우터에서 생성된 서명값과 식별자를 포함하는 인증요청메시지를 수신하는 단계와, 인증요청메시지에 구비되어 있는 식별자가 인증 서버에 기저장된 식별자 리스트에 포함되어 있는지 비교 판단하는 단계와, 판단한 식별자의 메쉬 라우터에 상응하는 공개키로 인증요청메시지에 구비되어 있는 메쉬 라우터의 서명값을 복호화 가능한지 판단하는 단계 및 비교 판단 결과와 복호화 가능 판단 결과에 기초하여 메쉬 라우터를 인증하는 단계를 포함한다.

효 과

[0021] 본 발명에 따른, 무선 메쉬 네트워크에서 웜홀 공격을 방지하기 위한 메쉬 라우터의 인증 방법은 다음과 같은 다양한 효과를 가진다.

[0022] 첫째, 본 발명에 따른 메쉬 라우터의 인증 방법은 인증 서버에 저장되어 있는 메쉬 라우터의 식별자와 공개키를 이용하여 무선 메쉬 네트워크에 접속되어 있는 메쉬 라우터를 인증함으로써, 웜홀 노드를 정확하게 판단할 수

있다.

[0023] 둘째, 본 발명에 따른 메쉬 라우터의 인증 방법은 메쉬 라우터 단위로 또는 라우팅 경로 상의 모든 메쉬 라우터 단위로 인증을 수행함으로써, 무선 메쉬 네트워크의 트래픽 상태에 따라 효율적으로 메쉬 라우터를 인증할 수 있다.

[0024] 셋째, 본 발명에 따른 메쉬 라우터의 인증 방법은 메쉬 라우터의 인증 결과를 반영하여 무선 메쉬 네트워크를 구성하는 모든 메쉬 라우터의 라우팅테이블을 갱신함으로써, 높은 레벨의 보안을 유지할 수 있다.

[0025] 넷째, 본 발명에 따른 메쉬 라우터의 인증 방법은 무선 메쉬 네트워크에서 발생하는 웜홀 공격을 방지함으로써, 경제적으로 패킷을 송수신할 수 있다.

발명의 실시를 위한 구체적인 내용

[0026] 이하 첨부한 도면을 참고로 본 발명에 따른 메쉬 라우터의 인증 방법을 보다 구체적으로 설명한다.

[0027] 도 5는 본 발명의 일 실시예에 따른 무선 메쉬 네트워크를 설명하기 위한 기능 블록도이다.

[0028] 도 5를 참고로 살펴보면, 무선 메쉬 네트워크는 다수의 메쉬 라우터와 각 메쉬 라우터에 접속되어 있는 다수의 메쉬 클라이언트로 구성되어 있다. 메쉬 라우터 중 일부의 메쉬 라우터(MR2)는 인터넷 게이트웨이(IGW)의 역활을 병행하여 수행하며, 인터넷 게이트웨이를 통해 외부의 인터넷 네트워크에 접속된다. 메쉬 클라이언트는 메쉬 라우터를 통해 메쉬 네트워크 내에서 통신을 수행하거나 인터넷 게이트웨이의 역할을 수행하는 메쉬 라우터(MR2)를 통해 외부 인터넷 네트워크와 통신을 수행한다.

[0029] 한편, 인터넷 네트워크에는 인증 서버(200)가 접속되어 있다. 인증 서버(200)는 무선 메쉬 네트워크에 존재하는 메쉬 라우터에게 인증 서버(200)의 공개키를 전송하거나, 각 메쉬 라우터에게 메쉬 라우터 자신의 개인키를 부여한다. 또한, 인증 서버(200)는 무선 메쉬 네트워크를 구성하는 메쉬 라우터의 식별자 리스트를 구비하고 있다. 인증 서버(200)는 각 메쉬 라우터의 개인키로 암호화된 각 메쉬 라우터의 서명값과 메쉬 라우터의 식별자를 이용하여 무선 메쉬 네트워크에서 웜홀 공격을 수행하는 공격 라우터를 판단한다.

[0030] 도 6은 본 발명에 따른 무선 메쉬 네트워크에서 웜홀 공격 라우터(AR)에 의해 발생하는 웜홀 공격을 방지하기 위한 메쉬 라우터의 인증 예를 설명하기 위한 기능 블록도이다.

[0031] 도 6을 참고로 살펴보면, 소스 노드(MC1)에서 목적지 노드(MC7)로 패킷을 송신하기 위하여 소스 노드(MC1)로부터 목적지 노드(MC7)까지의 라우팅 경로를 설정한다. 소스 노드(MC1)가 접속되어 있는 소스 메쉬 라우터(MR1)는 주변의 메쉬 라우터들로 경로설정메시지를 브로딩캐스팅하며, 경로설정메시지를 수신한 주변 메쉬 라우터들은 다시 주변 메쉬 라우터들에게 경로설정메시지를 브로딩캐스팅하여 최종적으로 목적지 노드(MC7)가 접속되어 있는 목적지 메쉬 라우터(MR3)로 송신한다. 목적지 노드(MC7)의 목적지 메쉬 라우터(MR3)는 수신한 경로설정메시지의 라우팅 정보를 이용하여 소스 노드(MC1)의 소스 메쉬 라우터(MR1)로 경로확인메시지를 송신한다. 경로확인메시지에는 소스 노드(MC1)로부터 목적지 노드(MC7)까지의 최적 경로에 대한 라우팅 정보가 포함되어 있다.

[0032] 경로확인메시지에 포함되어 있는 라우팅 정보에 기초하여, 소스 노드(MC1)에서 목적지 노드(MC7)까지의 라우팅 경로가 MR1-AR1-MR2-AR2-MR3로 설정되는 경우, 소스 노드(MC1)는 설정된 라우팅 경로를 통해 패킷을 목적지 노드(MC7)로 설정한다. 그런데, 라우팅 경로에 포함되어 있는 메쉬 라우터들 중에서 메쉬 라우터(AR1)과 메쉬 라우터(AR2)가 웜홀 공격 라우터인 경우 웜홀 공격 라우터(AR1)과 웜홀 공격 라우터(AR2)는 웜홀 공격 라우터(AR1)와 웜홀 공격 라우터(AR2) 사이에 터널을 형성하여 소스 노드(MC1)에서 목적지 노드(MC7) 사이의 최적의 라우팅 경로를 MR1-AR1-AR2-MR3로 변경 설정한다. 웜홀 공격 라우터에 의해 웜홀 공격이 발생하는 경우 웜홀 공격 라우터는 크게 중간 메쉬 라우터를 이용하여 판단하는 방식과 목적지 메쉬 라우터를 이용하여 판단하는 방식, 2가지 방식으로 판단될 수 있다.

[0033] 먼저, 도 7을 참고로 중간 메쉬 라우터를 이용하여 웜홀 공격 라우터를 판단하는 방식을 살펴보면, 소스 노드(MC1)가 목적지 노드(MC7)로 패킷의 송신을 요청하는 경우 소스 메쉬 라우터(MR1)는 주변의 메쉬 라우터들에게 경로설정메시지를 브로딩캐스팅한다(S1). 주변 메쉬 라우터들 중 다음 홉으로 경로설정메시지를 수신하는 메쉬 라우터를 다음 홉 메쉬 라우터라 언급하며, 경로설정메시지를 다음 홉 메쉬 라우터로 송신하는 메쉬 라우터를 이전 홉 메쉬 라우터라 언급한다. 다음 홉 메쉬 라우터는 경로설정메시지를 수신하는 경우, 경로설정메시지의 식별자 필드와 서명값 필드에 각각 다음 홉 메쉬 라우터의 식별자와 랜덤 메시지를 다음 홉 메쉬 라우터의 개인키로 암호화한 서명값을 저장하여 경로설정메시지를 갱신한다. 다음 홉 메쉬 라우터는 갱신한 경로설정메시지

를 이전 홉 메쉬 라우터를 포함하는 주변 메쉬 라우터로 다시 브로딩캐스팅한다(S3).

[0034] 바람직하게, 이전 홉 메쉬 라우터는 소정 응답 시간 내에 다음 홉 메쉬 라우터로부터 갱신한 경로설정메시지를 수신하지 못하는 경우 다음 홉 메쉬 라우터를 자체적으로 웜홀 공격 라우터로 판단한다. 더욱 바람직하게, 이전 홉 메쉬 라우터는 소정 응답 시간 내에 다음 홉 메쉬 라우터로부터 갱신한 경로설정메시지를 수신하지 못하는 경우 경로설정메시지를 반복하여 다음 홉 메쉬 라우터로 송신하며, 소정 응답 시간 내에 다음 홉 메쉬 라우터로부터 갱신한 경로설정메시지를 수신하지 못하는 경우 다음 홉 메쉬 라우터를 자체적으로 웜홀 공격 라우터로 판단한다.

[0035] 다음 홉 메쉬 라우터로부터 경로설정메시지를 수신한 경우, 이전 홉 메쉬 라우터는 다음 홉 메쉬 라우터의 식별자와 서명값을 포함하는 인증요청메시지(RAREQ)를 생성하고 인증요청메시지를 인증서버의 공개키로 암호화하여 인증 서버로 송신한다(S5). 인증 서버는 수신한 인증요청메시지(RAREQ)에 포함되어 있는 다음 홉 메쉬 라우터의 식별자와 서명값에 기초하여 다음 홉 메쉬 라우터가 웜홀 공격 라우터인지 여부를 인증하고 인증확인메시지(RAREP)를 이전 홉 메쉬 라우터로 송신한다(S7).

[0036] 다음으로, 도 8을 참고로 목적지 메쉬 라우터를 이용하여 웜홀 공격 라우터를 판단하는 방식을 살펴보면, 소스 노드(MC1)가 목적지 노드(MC7)로 패킷의 송신을 요청하는 경우 소스 메쉬 라우터(MR1)는 주변의 메쉬 라우터들에게 경로설정메시지를 브로딩캐스팅한다(S11). 다음 홉 메쉬 라우터가 경로설정메시지를 수신하는 경우, 경로설정메시지의 식별자 필드와 서명값 필드에 각각 다음 홉 메쉬 라우터의 식별자와 다음 홉 메쉬 라우터의 개인키로 암호화된 서명값을 추가 저장하여 경로설정메시지를 갱신한다. 경로설정메시지는 계속해서 다음 홉 메쉬 라우터의 주변 메쉬 라우터로 브로딩캐스팅되며(S12), 다음 홉 메쉬 라우터의 다음 홉 메쉬 라우터는 수신한 경로설정메시지의 식별자 필드와 서명값 필드에 각각 자신의 식별값과 서명값을 추가 저장한다. 서명값은 경로설정메시지를 수신한 메쉬 라우터의 개인키로 암호화되어 생성된다.

[0037] 경로설정메시지는 소스 노드(MC1)와 목적지 노드(MC7) 사이의 중간 메쉬 라우터를 경우하여 목적지 메쉬 라우터(M3)로 송신되며(S14), 경로설정메시지를 수신한 목적지 메쉬 라우터(MR3)는 다수의 메쉬라우터들로부터 브로딩캐스팅된 경로설정메시지의 라우터 경로에 기초하여 소스 노드(MC1)와 목적지 노드(MC7) 사이의 라우팅 경로를 설정하여 경로응답메시지(RREP)를 소스 노드로 송신한다(S15). 또한, 목적지 메쉬 라우터(MR3)는 경로설정메시지에 포함되어 있는 라우팅 경로상의 각 메쉬 라우터들의 식별값과 서명값을 인증 서버의 공개키로 암호화하여 생성한 인증요청메시지(RAREQ)를 소스 메쉬 라우터(MR1)로 송신한다(S16).

[0038] 소스 메쉬 라우터(MR1)는 수신한 인증요청메시지를 인증 서버로 송신하며(S17), 인증 서버는 수신한 인증요청메시지를 인증 서버의 개인키로 복호화하여 인증요청메시지(RAREQ)에 포함되어 있는, 라우팅 경로 상의 모든 메쉬 라우터의 식별자와 서명값에 기초하여 라우팅 경로 상의 모든 메쉬 라우터를 인증하고 인증확인메시지(RAREP)를 생성하여 소스 노드로 송신한다(S19).

[0039] 도 9는 본 발명에 따른 경로설정메시지, 인증요청메시지, 인증확인메지시의 일 예를 도시하고 있다.

[0040] 도 9(a)를 참고로 경로설정메시지의 일 예를 살펴보면, 경로설정메시지에는 식별자 필드와 서명값 필드 및 랜덤 메시지 필드를 구비하고 있다. 식별자 필드는 경로설정메시지를 라우팅하는 메쉬 라우터의 식별자가 저장되며, 서명값 필드에는 각 메쉬 라우터의 개인키로 랜덤 메시지를 암호화한 서명값이 저장된다.

[0041] 도 9(b)를 참고로 인증요청메시지의 일 예를 살펴보면, 인증요청메시지에는 식별자 필드와 서명값 필드 및 랜덤 메시지 필드를 구비하고 있다. 경로설정메시지를 라우팅하는 메쉬 라우터의 식별자를 저장하는 식별자 필드와 각 메쉬 라우터의 개인키로 랜덤 메시지를 암호화한 서명값이 저장된 서명값 필드는 인증 서버의 공개키로 암호화되어 있다.

[0042] 도 9(c)를 참고로 인증확인메시지의 일 예를 살펴보면, 식별자 필드와 인증값 필드를 구비하고 있다. 경로설정메시지를 라우팅하는 메쉬 라우터의 식별자를 저장하는 식별자 필드와 각 메쉬 라우터가 웜홀 공격 라우터인지를 인증하는 인증값을 저장하는 인증값 필드는 인증요청메시지를 송신한 메쉬 라우터의 공개키로 암호화되어 있다.

[0043] 도 10은 본 발명에 따른 인증 서버의 일 예를 설명하기 위한 기능 블록도이다.

[0044] 도 10을 참고로 보다 구체적으로 살펴보면, 인증요청메시지를 수신하는 경우 복호화부(205)는 인증 서버의 개인키로 인증요청메시지에 포함되어 있는 식별자 필드와 서명값 필드의 데이터를 복호화한다. 식별자 리스트 DB(210)에는 무선 메쉬 네트워크에 등록되어 있는 모든 메쉬 라우터의 식별자가 저장되어 있으며, 식별자 비교

판단부(230)는 식별자 리스트 DB를 이용하여 인증요청메시지에 기록되어 있는 식별자의 메쉬 라우터들이 무선 메쉬 네트워크에 기등록되어 있는 메쉬 라우터인지를 판단한다. 식별자 비교를 통해 식별자 필드에 기록되어 있는 메쉬 라우터들이 식별자 리스트 DB(210)에 등록되어 있는 메쉬 라우터로 판단되는 경우, 서명값 복호화부(240)는 각 메쉬 라우터의 서명값을 공개키/개인키 DB(220)에 저장되어 있는 메쉬 라우터의 공개키로 복호화한다.

[0045] 식별자 비교 판단부(230)의 비교 결과와 서명값 복호화부의 복호화 결과에 기초하여 인증부(250)는 인증요청메시지에 기록되어 있는 식별자의 메쉬 라우터가 웜홀 공격 라우터인지를 판단한다. 인증요청메시지에 기록되어 있는 식별자의 메쉬 라우터들 중 식별자 리스트 DB(210)에 기등록되어 있지 않은 메쉬 라우터이거나 서명값을 복호화할 수 없는 메쉬 라우터는 웜홀 공격 라우터로 판단된다. 인증확인메시지 생성부(260)는 인증부(250)의 판단 결과에 따라 인증요청메시지에 기록되어 있는 메쉬 라우터들의 식별자와 각 메쉬 라우터의 인증값을 포함하는 인증확인메시지를 생성한다. 인증확인메시지 생성부(260)는 메쉬 라우터의 식별자와 각 메쉬 라우터의 인증값을 인증요청메시지를 송신한 메쉬 라우터의 공개키로 암호화한다.

[0046] 도 11은 본 발명에 따라 인증확인메시지를 수신한 노드에서 라우팅 테이블을 갱신하는 과정을 설명하는 흐름도이다.

[0047] 도 11을 참고로 살펴보면, 인증요청메시지를 인증 서버로 송신한 메쉬 라우터는 인증요청메시지에 응답하여 인증 서버로부터 인증확인메시지를 수신한다(S21). 수신한 인증확인메시지의 식별자 필드와 인증값 필드의 데이터는 인증요청메시지를 송신한 메쉬 라우터의 공개키로 암호화되어 있으며, 메쉬 라우터는 자신의 개인키를 이용하여 식별자 필드와 인증값 필드를 복호화한다(S22). 메쉬 라우터는 복호화한 인증확인메시지의 인증값에 기초하여 라우팅 경로의 메쉬 라우터들 중 웜홀 공격 라우터가 존재하는지 판단한다(S23). 판단 결과 설정된 라우팅 경로 상에 웜홀 공격 라우터가 존재하지 않는 경우 경로확인메시지의 설정된 라우팅 경로로 패킷을 송신한다(S28).

[0048] 반면, 판단 결과 라우팅 경로 상에 웜홀 공격 라우터가 존재하는 경우, 메쉬 라우터는 기저장된 메쉬 라우터의 라우팅 테이블에서 웜홀 공격 라우터로 판단된 메쉬 라우터를 삭제하여 라우팅 테이블을 갱신한다(S24). 메쉬 라우터는 갱신한 라우팅 테이블에 기초하여 설정된 라우팅 경로를 변경하고(S25), 변경한 라우팅 경로로 패킷을 송신한다(S26). 한편, 메쉬 라우터는 주변 메쉬 라우터들에게 인증확인메시지를 브로딩캐스팅하여 주변 메쉬 라우터의 라이팅 테이블에서 웜홀 공격 라우터를 삭제하도록 한다(S27).

[0049] 한편, 상술한 본 발명의 실시 예들은 컴퓨터에서 실행될 수 있는 프로그램으로 작성 가능하고, 컴퓨터로 읽을 수 있는 기록 매체를 이용하여 상기 프로그램을 동작시키는 범용 디지털 컴퓨터에서 구현될 수 있다.

[0050] 상기 컴퓨터로 읽을 수 있는 기록 매체는 마그네틱 저장 매체(예를 들어, 롬, 플로피 디스크, 하드디스크 등), 광학적 판독 매체(예를 들면, 시디롬, 디브이디 등) 및 캐리어 웨이브(예를 들면, 인터넷을 통한 전송)와 같은 저장 매체를 포함한다.

[0051] 본 발명은 도면에 도시된 실시예를 참고로 설명되었으나 이는 예시적인 것에 불과하다. 예를 들어, 웜홀 공격 라우터를 판단하기 위하여 경로설정메시지를 일 예로 설명하였으나, 무선 메쉬 네트워크에서 송수신되는 모든 메시지를 이용하여 웜홀 공격 라우터를 판단할 수 있다. 경로설정메시지는 무선 메쉬 네트워크에서 송수신되는 메시지의 일 예로만 이해하여야 하며, 본 발명이 소스 노드에서 목적지 노드로 송신되는 경로설정메시지에 한정되는 것은 아니다. 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 등록청구범위의 기술적 사상에 의해 정해져야 할 것이다.

도면의 간단한 설명

[0052] 도 1은 기반망 방식의 무선 메쉬 네트워크의 일 예를 설명하기 위한 기능 블록도이다.

[0053] 도 2는 클라이언트 무선 메쉬 네트워크의 일 예를 설명하기 위한 기능 블록도이다.

[0054] 도 3은 하이브리드 무선 메쉬 네트워크의 일 예를 설명하기 위한 기능 블록도이다.

[0055] 도 4는 무선 메쉬 네트워크의 대표적인 공격 방법인 웜홀(wormhole) 공격 방식을 설명하기 위한 도면이다.

[0056] 도 5는 본 발명의 일 실시예에 따른 무선 메쉬 네트워크를 설명하기 위한 기능 블록도이다.

[0057] 도 6은 본 발명에 따른 무선 메쉬 네트워크에서 웜홀 공격 라우터(AR)에 의해 발생하는 웜홀 공격을 방지하기 위한 메쉬 라우터의 인증 예를 설명하기 위한 기능 블록도이다.

[0058] 도 7는 중간 메쉬 라우터를 이용하여 웜홀 공격 라우터를 판단하는 방식을 설명하기 위한 신호의 흐름도를 도시하고 있다.

[0059] 도 8은 목적지 메쉬 라우터를 이용하여 웜홀 공격 라우터를 판단하는 방식을 설명하기 위한 신호의 흐름도를 도시하고 있다.

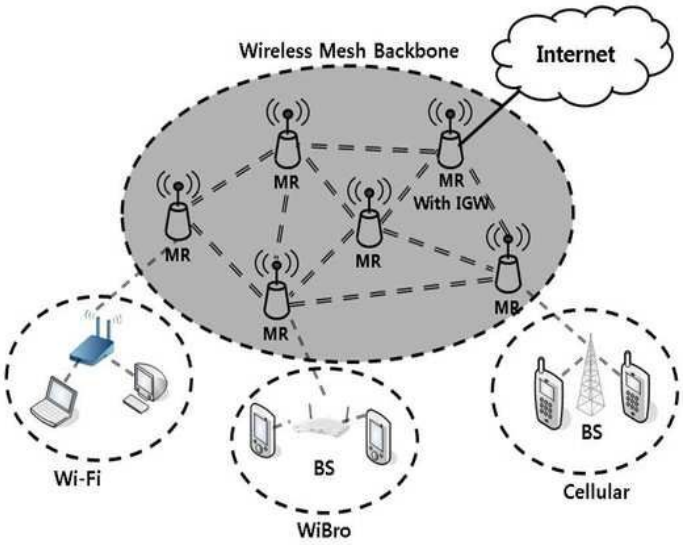
[0060] 도 9는 본 발명에 따른 경로설정메시지, 인증요청메시지, 인증확인메지시의 일 예를 도시하고 있다.

[0061] 도 10은 본 발명에 따른 인증 서버의 일 예를 설명하기 위한 기능 블록도이다.

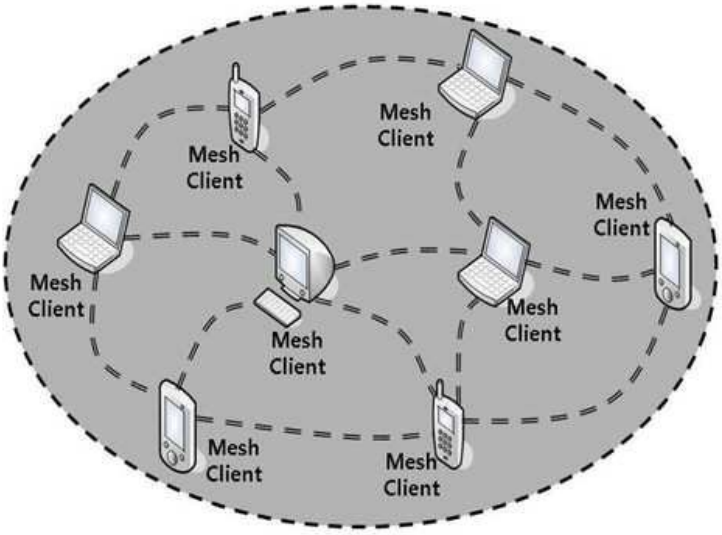
[0062] 도 11은 본 발명에 따라 인증확인메시지를 수신한 노드에서 라우팅 테이블을 갱신하는 과정을 설명하는 흐름도이다.

도면

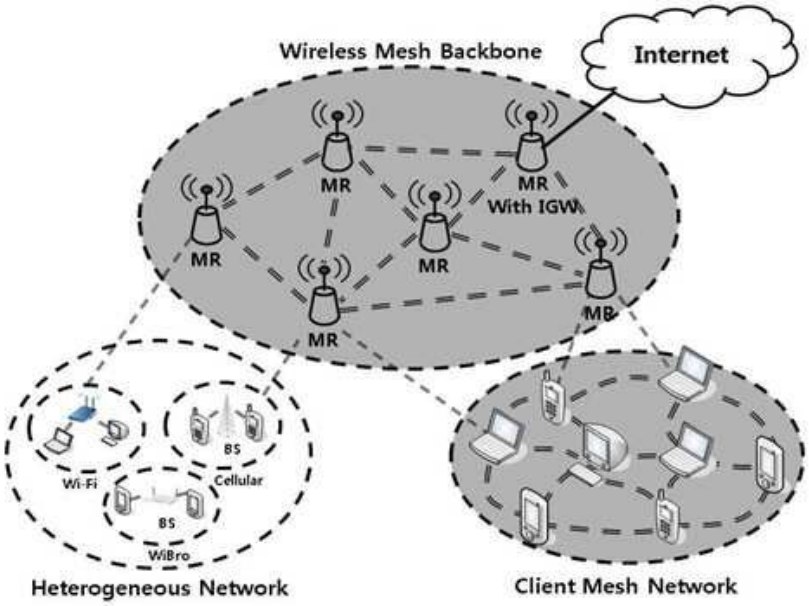
도면1



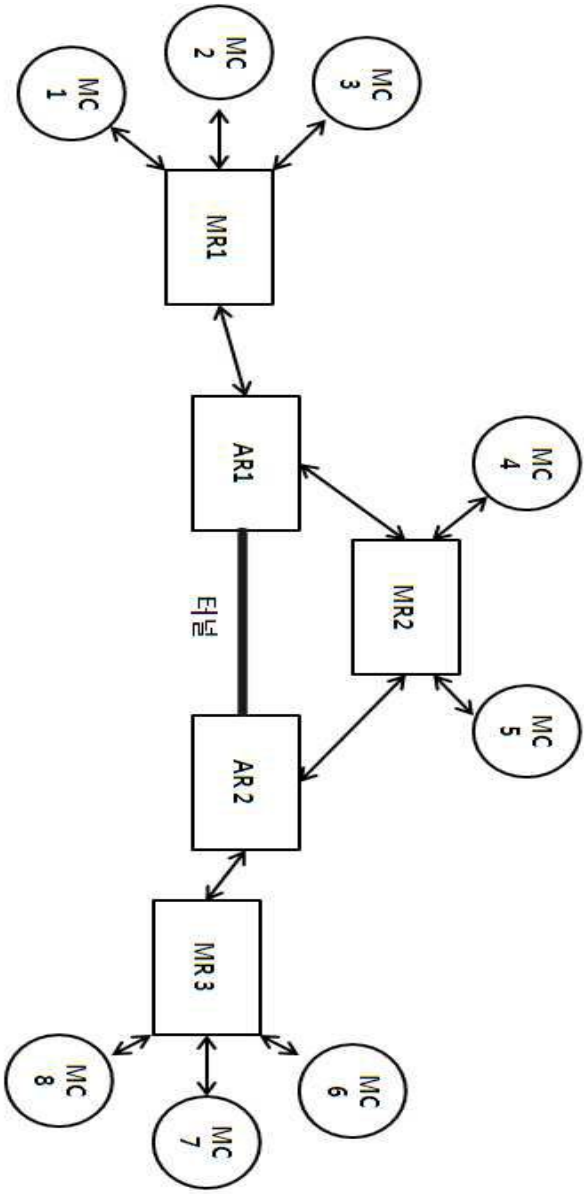
도면2


Mesh Client
Mesh Client
Mesh Client
Mesh Client
Mesh Client
Mesh Client
Mesh Client
Mesh Client

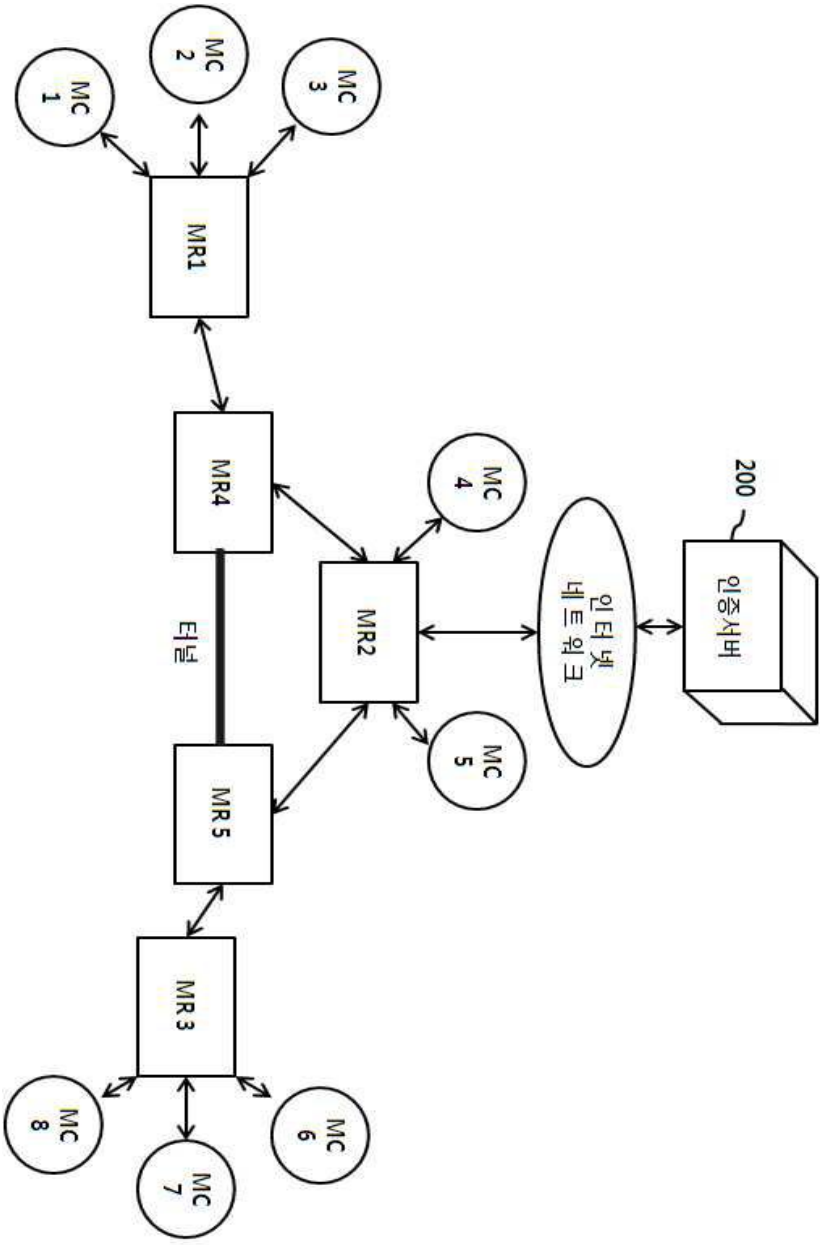
도면3


Wireless Mesh Backbone
Internet
MR
MR
With IGW
MR
MR
MR
MR
Wi-Fi
BS
Cellular
BS
WiBro
Heterogeneous Network
Client Mesh Network

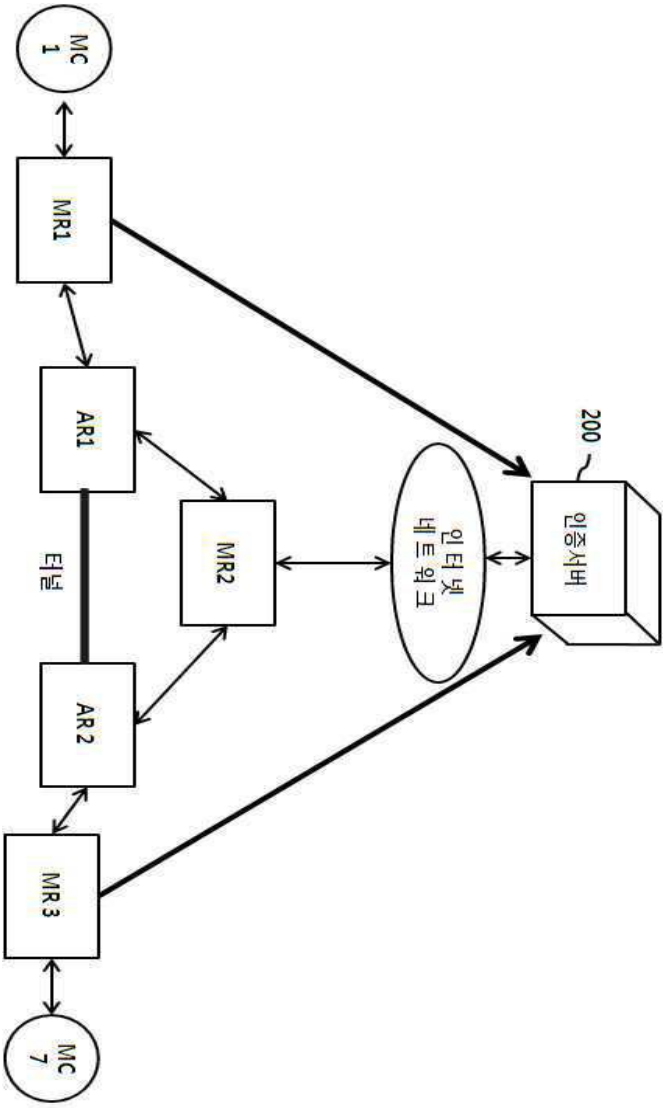
도면4



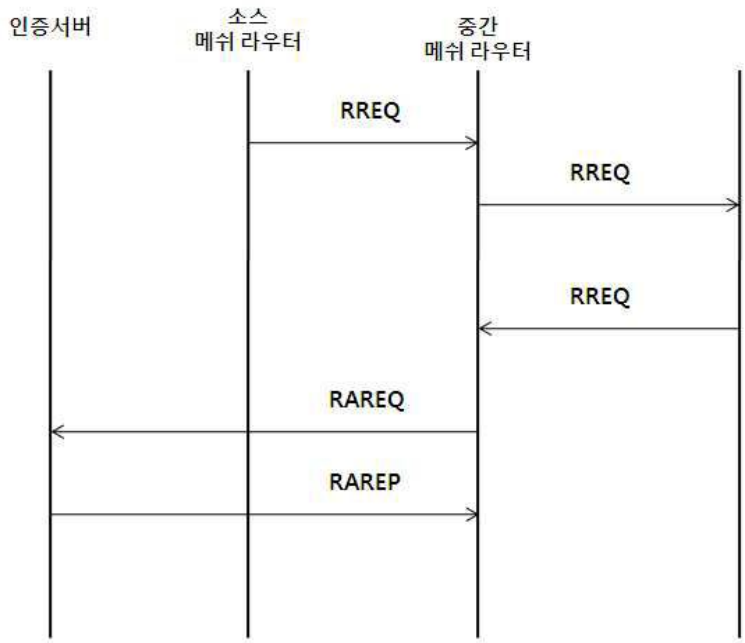
도면5


MC 1
MC 2
MC 3
MR1
MR4
MC 4
MR2
터널
MC 5
MR 5
인터넷 네트워크
200
인증서버
MR 3
MC 8
MC 7
MC 6

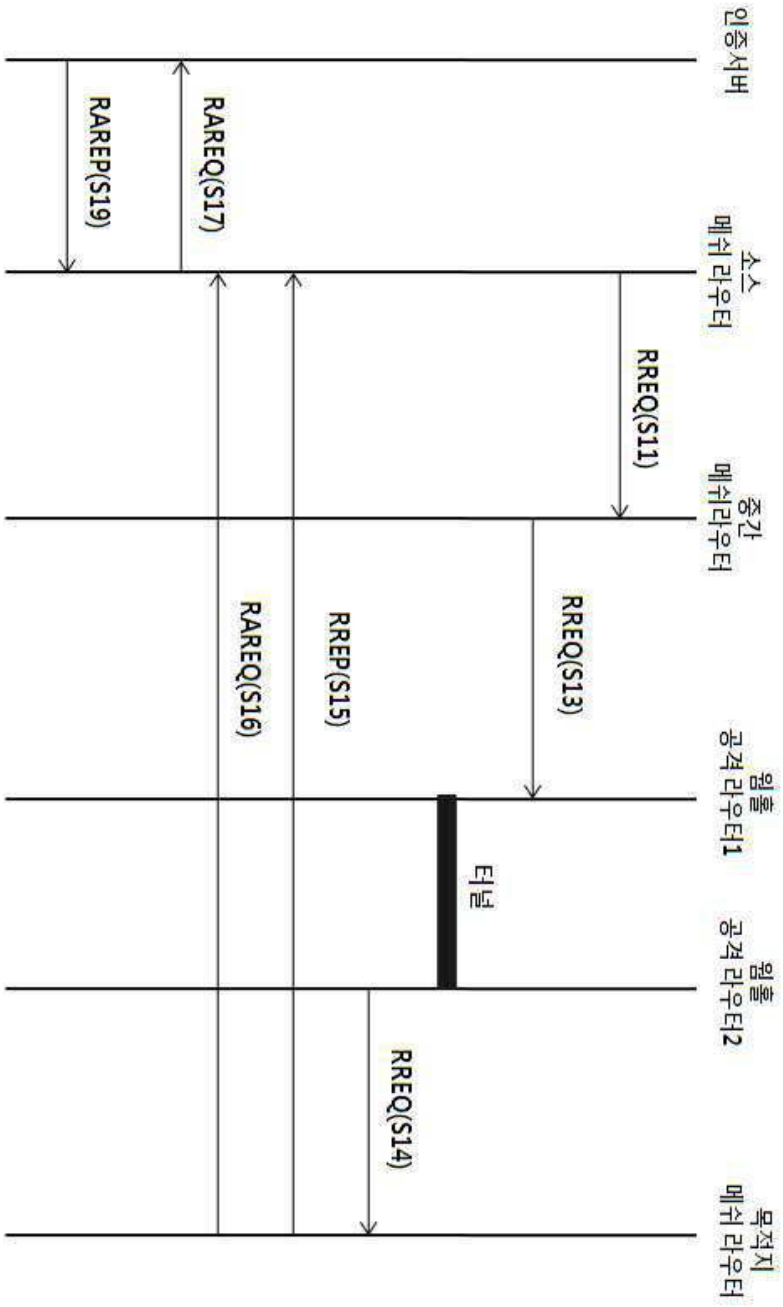
도면6



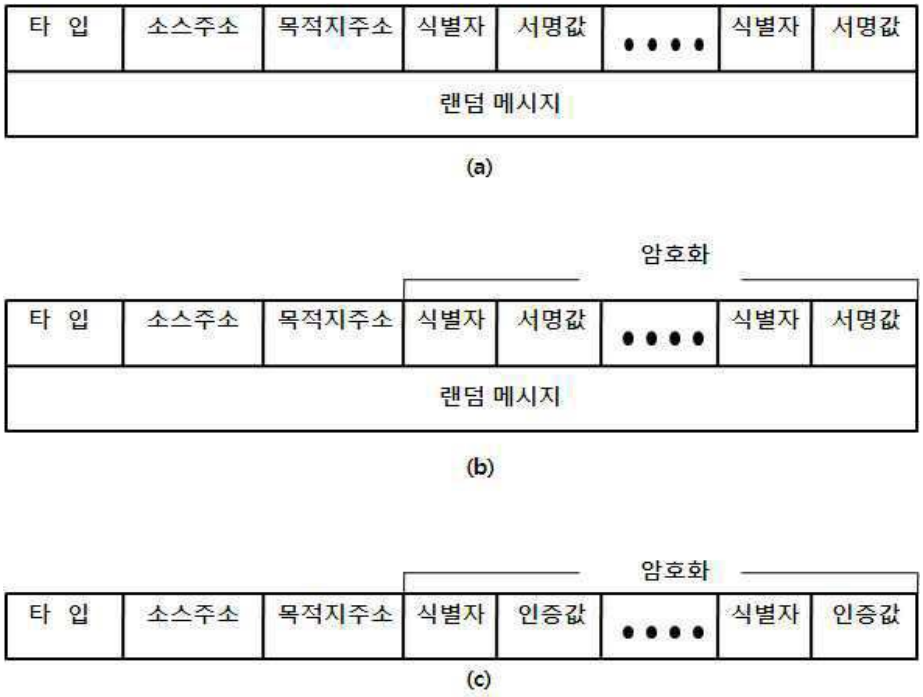
도면7



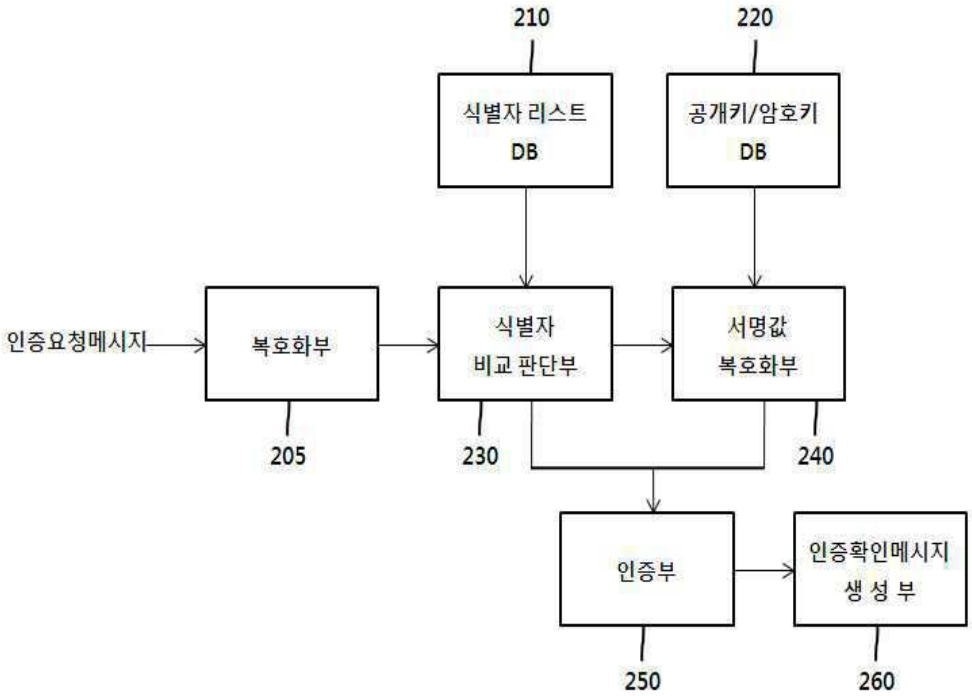
도면8


인증서버
소스 메쉬 라우터
중간 메쉬라우터
웜홀 공격 라우터1
웜홀 공격 라우터2
목적지 메쉬 라우터
RAREP(S19)
RAREQ(S17)
RREQ(S11)
RAREQ(S16)
RREP(S15)
RREQ(S13)
터널
RREQ(S14)

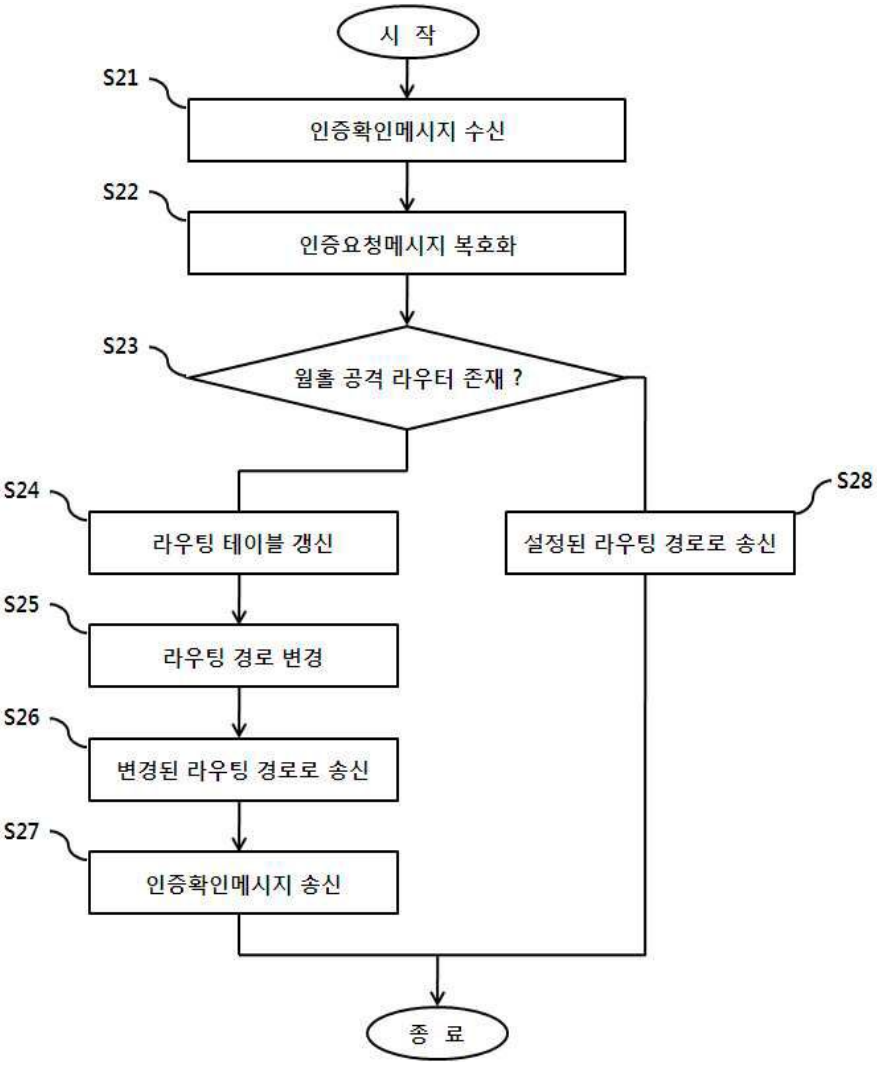
도면9


타 입
소스주소
목적지주소
식별자
서명값
• • • •
식별자
서명값
랜덤 메시지
(a)
암호화
타 입
소스주소
목적지주소
식별자
서명값
• • • •
식별자
서명값
랜덤 메시지
(b)
암호화
타 입
소스주소
목적지주소
식별자
인증값
• • • •
식별자
인증값
(c)

도면10


210
220
식별자 리스트 DB
공개키/암호키 DB
인증요청메시지
복호화부
식별자 비교 판단부
서명값 복호화부
205
230
240
인증부
인증확인메시지 생 성 부
250
260

도면11


시 작
S21
인증확인메시지 수신
S22
인증요청메시지 복호화
S23
웜홀 공격 라우터 존재 ?
S24
라우팅 테이블 갱신
S25
라우팅 경로 변경
S26
변경된 라우팅 경로로 송신
S27
인증확인메시지 송신
S28
설정된 라우팅 경로로 송신
종 료