



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2018-0052346
(43) 공개일자 2018년05월18일

(51) 국제특허분류(Int. Cl.)
H04L 29/12 (2006.01) H04L 9/32 (2006.01)
(52) CPC특허분류
H04L 61/103 (2013.01)
H04L 61/6022 (2013.01)
(21) 출원번호 10-2016-0149550
(22) 출원일자 2016년11월10일
심사청구일자 2016년11월10일

(71) 출원인
인하대학교 산학협력단
인천광역시 남구 인하로 100, 인하대학교 (용현동)
(72) 발명자
양대현
서울특별시 서초구 서초중앙로 200, 17동 901호(서초동, 삼풍아파트)
(74) 대리인
양성보

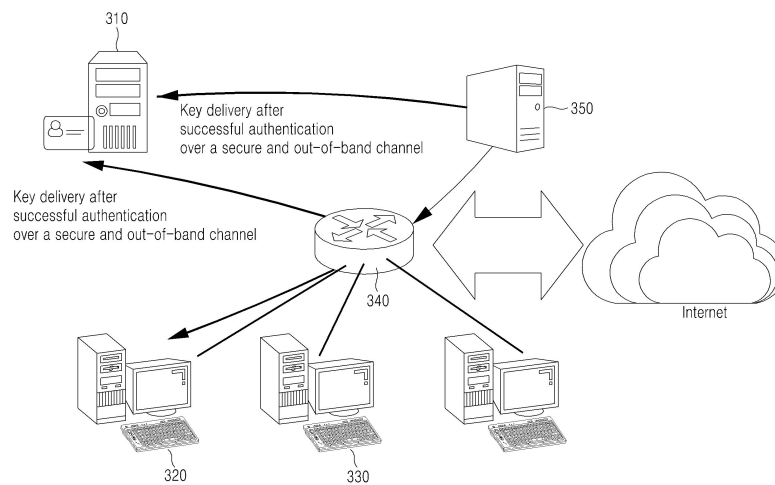
전체 청구항 수 : 총 10 항

(54) 발명의 명칭 암호화하여 생성된 MAC 주소와 SDN 어플리케이션을 이용한 레이어 2 액세스 제어 방법 및 시스템

(57) 요약

일 실시예에 따른 제1 단말과 제2 단말 간의 통신 방법은, 상기 제1 단말에서, 상기 제2 단말 각각의 IP 주소를 해시함수를 사용하여 해시한 값에 기반하여 상기 제 2 단말의 MAC 주소를 획득하는 단계; 상기 제1 단말에서, 상기 획득된 MAC 주소를 포함하는 MAC 프레임을 생성하고, 상기 제2 단말로 전송하는 단계; 및 상기 제2 단말에서, 상기 제1 단말로부터 상기 MAC 프레임을 수신하는 단계를 포함할 수 있다.

대표도



(52) CPC특허분류
H04L 9/3236 (2013.01)

명세서

청구범위

청구항 1

제1 단말과 제2 단말 간의 통신 방법에 있어서,

상기 제1 단말에서, 상기 제2 단말 각각의 IP 주소를 해시함수를 사용하여 해시한 값에 기반하여 상기 제2 단말의 MAC 주소를 획득하는 단계;

상기 제1 단말에서, 상기 획득된 MAC 주소를 포함하는 MAC 프레임을 생성하고, 상기 제2 단말로 전송하는 단계; 및

상기 제2 단말에서, 상기 제1 단말로부터 상기 MAC 프레임을 수신하는 단계를 포함하는 통신 방법.

청구항 2

제1항에 있어서,

상기 제1 단말에서, 상기 제1 단말의 IP 주소를 상기 해시함수를 사용하여 해시한 값에 기반하여, 상기 제1 단말의 MAC 주소를 계산하는 단계

를 더 포함하고,

상기 생성된 MAC 프레임은 상기 제1 단말의 MAC 주소를 소스 주소로서 포함하고,

상기 제2 단말에서, 상기 제1 단말의 IP 주소를 상기 해시함수를 사용하여 해시한 값에 기반하여, 상기 수신된 MAC 프레임의 소스 주소를 검증하는 단계

를 더 포함하는 통신 방법.

청구항 3

제1항에 있어서,

인증 서버로부터, 상기 제1 단말 및 상기 제2 단말에 고유 키를 제공하는 단계

를 더 포함하고,

상기 제2 단말의 MAC 주소를 획득하는 단계에서,

상기 제2 단말의 MAC 주소는 상기 제2 단말의 IP 주소 및 상기 고유 키를 상기 해시함수를 사용하여 해시한 값에 기반하여 획득되는 통신 방법.

청구항 4

제3항에 있어서,

상기 고유 키는, 상기 제1 단말 및 상기 제2 단말의 각각으로부터의 식별 정보에 기초하여 상기 제1 단말 및 상기 제2 단말의 각각이 상기 인증 서버에 대해 인증됨에 따라, 상기 제1 단말 및 상기 제2 단말의 각각으로 제공되는 통신 방법.

청구항 5

제1항에 있어서,

상기 제2 단말은 라우터이고, 상기 제2 단말의 MAC 주소는 상기 라우터의 MAC 주소로서 생성되고,

상기 제1 단말로부터 상기 라우터로 아웃바운드(outbound) 트래픽을 전송하는 단계

를 더 포함하는 통신 방법.

청구항 6

제2항에 있어서,

인증 서버로부터, 상기 제1 단말 및 상기 제2 단말에 고유 키를 제공하는 단계

를 더 포함하고,

상기 제 1 단말의 MAC 주소를 계산하는 단계에서,

상기 제 1 단말의 MAC 주소는 상기 제1 단말의 IP 주소 및 상기 고유 키를 상기 해시함수를 사용하여 해시한 값에 기반하여 계산되는 통신 방법.

청구항 7

제2항에 있어서,

상기 제1 단말은 라우터이고, 상기 제 1 단말의 MAC 주소는 상기 라우터의 MAC 주소로서 생성되고,

상기 제2 단말에서, 상기 소스 주소를 상기 라우터의 MAC 주소로서 검증하고, 상기 라우터로부터 인바운드(inbound) 트래픽을 수신하는 단계

를 더 포함하는 통신 방법.

청구항 8

제3항에 있어서,

상기 인증 서버에서 상기 고유 키를 갱신하는 단계;

상기 인증 서버로부터, SDN 컨트롤러로 상기 갱신된 고유 키를 브로드캐스트하도록 요청하는 단계;

상기 SDN 컨트롤러에서, 상기 갱신된 고유 키를 브로드캐스트하는 단계; 및

상기 갱신된 고유 키가 수신된 상기 제1 단말 및 상기 제2 단말 간의 통신을 종료하는 단계

를 더 포함하는 통신 방법.

청구항 9

다른 단말과의 통신 방법에 있어서,

자신의 IP 주소를 해시함수를 사용하여 해시한 값에 기반하여 자신의 MAC 주소를 계산하는 단계;

상기 다른 단말의 IP 주소를 해시함수를 사용하여 해시한 값에 기반하여 상기 다른 단말의 MAC 주소를 획득하는 단계; 및

상기 계산된 자신의 MAC 주소 및 상기 획득된 다른 단말의 MAC 주소를 포함하는 MAC 프레임을 생성하고, 상기 다른 단말로 전송하는 단계

를 포함하는 통신 방법.

청구항 10

다른 단말과의 통신 방법에 있어서,

자신의 IP 주소를 해시함수를 사용하여 해시한 값에 기반하여 자신의 MAC 주소를 변경하는 단계;

상기 다른 단말로부터 상기 변경된 MAC 주소를 목적지(destination) 주소로 하는 MAC 프레임을 수신하는 단계; 및

상기 다른 단말의 IP 주소를 상기 해시함수를 사용하여 해시한 값에 기반하여, 상기 수신된 MAC 프레임의 소스 주소가 상기 다른 단말의 MAC 주소에 해당하는지를 검증하는 단계

를 포함하는 통신 방법.

발명의 설명

기술 분야

[0001] 아래의 설명은 통신 기술에 관한 것으로, ARP Poisoning 공격에 대응하는 네트워크 보안 방법 및 장치에 관한 것이다.

배경 기술

[0002]도 1을 참고하면, ARP(Address Resolution Protocol)를 설명하기 위한 것으로 ARP는 IP 네트워크 상에서의 이더넷(Ethernet) 주소와 IP주소를 서로 연결시켜주는 DNS 역할을 하는 프로토콜을 지칭한다. LAN 네트워크 통신에서는 IP 주소가 아닌 MAC 주소에 의하여 통신이 이루어지게 된다. 실제 통신을 위하여 사용자가 사용하는 IP 주소와 물리적인 MAC 주소와의 매핑 과정이 필요하게 되며, 상대 단말의 IP 주소에 대한 MAC 주소를 파악하는데 있어서, ARP 프로토콜이 이용된다.

[0003]예를 들면, 단말 A는 단말 B와 통신을 하기 위하여 MAC 주소를 알아야 한다. 이때, MAC 주소를 파악하기 위하여 단말 B의 IP 주소에 해당하는 MAC 주소를 묻는 ARP 패킷을 로컬 네트워크에 브로드캐스팅(Broadcasting)할 수 있다. ARP 패킷을 수신한 단말 B는 단말 B의 MAC 주소를 요청하고 있음을 인지하여 자신의 MAC 주소를 포함한 정보를 ARP 패킷에 포함하여 ARP 응답 패킷을 단말 A로 전송할 수 있다.

[0004]단말 A는 단말 B로부터 전송된 ARP 응답 패킷 내에서 단말 B의 MAC 주소를 확인한 후, 통신이 개시될 수 있다. 이때, 단말 A는 단말 B의 IP 주소 및 MAC 주소를 테이블로 생성하여 캐시에 저장할 수 있다. 이후, 단말 A가 단말 B와 통신할 경우, ARP 과정을 거치지 않고 캐시에 저장된 테이블을 참조하여 통신을 수행하게 된다.

[0005]하지만 이러한 통신 방법은, 최근 들어 웹 서버가 전혀 해킹을 당하지 않았음에도 웹 서버로부터 악성코드 등이 다운로드되는 경우가 발생한다는 문제점이 있다. 이는 공격자가 웹 서버와 동일한 IP 세그먼트 내의 다른 서버를 해킹한 후 웹 서버와 관련된 웹 트래픽을 가로채 악성코드를 삽입함으로써 발생한다.

[0006]이에 따라 무선 네트워크에서 ARP Poisoning 공격이 발생하는 것을 방지하기 위한 기술에 요구되고 있다.

발명의 내용

해결하려는 과제

[0007]IP 주소에 대하여 해시함수를 사용하여 해시한 값에 기반하여 MAC 주소를 획득하고, MAC 주소를 포함하는 MAC 프레임을 상대방 단말로 전송하여 MAC 프레임을 검증하도록 함으로써 ARP Poisoning을 방지하는 방법을 제공할 수 있다.

과제의 해결 수단

[0008]일 실시예에 따르면, 제1 단말과 제2 단말 간의 통신 방법은, 상기 제1 단말에서, 상기 제2 단말 각각의 IP 주소를 해시함수를 사용하여 해시한 값에 기반하여 상기 제2 단말의 MAC 주소를 획득하는 단계; 상기 제1 단말에서, 상기 획득된 MAC 주소를 포함하는 MAC 프레임을 생성하고, 상기 제2 단말로 전송하는 단계; 및 상기 제2 단말에서, 상기 제1 단말로부터 상기 MAC 프레임을 수신하는 단계를 포함할 수 있다.

[0009]상기 통신 방법은, 상기 제1 단말에서, 상기 제1 단말의 IP 주소를 상기 해시함수를 사용하여 해시한 값에 기반하여, 상기 제1 단말의 MAC 주소를 계산하는 단계를 더 포함하고, 상기 생성된 MAC 프레임은 상기 제1 단말의 MAC 주소를 소스 주소로서 포함하고, 상기 제2 단말에서, 상기 제1 단말의 IP 주소를 상기 해시함수를 사용하여 해시한 값에 기반하여, 상기 수신된 MAC 프레임의 소스 주소를 검증하는 단계를 더 포함할 수 있다.

- [0010] 인증 서버로부터, 상기 제1 단말 및 상기 제2 단말에 고유 키를 제공하는 단계를 더 포함하고, 상기 제 2 단말의 MAC 주소를 획득하는 단계에서, 상기 제 2 단말의 MAC 주소는 상기 제2 단말의 IP 주소 및 상기 고유 키를 상기 해시함수를 사용하여 해시한 값에 기반하여 획득될 수 있다.
- [0011] 상기 고유 키는, 상기 제1 단말 및 상기 제2 단말의 각각으로부터의 식별 정보에 기초하여 상기 제1 단말 및 상기 제2 단말의 각각이 상기 인증 서버에 대해 인증됨에 따라, 상기 제1 단말 및 상기 제2 단말의 각각으로 제공될 수 있다.
- [0012] 상기 제2 단말은 라우터이고, 상기 제 2 단말의 MAC 주소는 상기 라우터의 MAC 주소로서 생성되고, 상기 제1 단말로부터 상기 라우터로 아웃바운드(outbound) 트래픽을 전송하는 단계를 더 포함할 수 있다.
- [0013] 인증 서버로부터, 상기 제1 단말 및 상기 제2 단말에 고유 키를 제공하는 단계를 더 포함하고, 상기 제 1 단말의 MAC 주소를 계산하는 단계에서, 상기 제 1 단말의 MAC 주소는 상기 제1 단말의 IP 주소 및 상기 고유 키를 상기 해시함수를 사용하여 해시한 값에 기반하여 계산될 수 있다.
- [0014] 상기 제1 단말은 라우터이고, 상기 제 1 단말의 MAC 주소는 상기 라우터의 MAC 주소로서 생성되고, 상기 제2 단말에서, 상기 소스 주소를 상기 라우터의 MAC 주소로서 검증하고, 상기 라우터로부터 인바운드(inbound) 트래픽을 수신하는 단계를 더 포함할 수 있다.
- [0015] 상기 통신 방법은, 상기 인증 서버에서 상기 고유 키를 갱신하는 단계; 상기 인증 서버로부터, SDN 컨트롤러로 상기 갱신된 고유 키를 브로드캐스트하도록 요청하는 단계; 상기 SDN 컨트롤러에서, 상기 갱신된 고유 키를 브로드캐스트하는 단계; 및 상기 갱신된 고유 키가 수신된 상기 제1 단말 및 상기 제2 단말 간의 통신을 종료하는 단계를 더 포함할 수 있다.
- [0016] 일 실시예에 따르면, 다른 단말과의 통신 방법은, 자신의 IP 주소를 해시함수를 사용하여 해시한 값에 기반하여 자신의 MAC 주소를 계산하는 단계; 상기 다른 단말의 IP 주소를 해시함수를 사용하여 해시한 값에 기반하여 상기 다른 단말의 MAC 주소를 획득하는 단계; 및 상기 계산된 자신의 MAC 주소 및 상기 획득된 다른 단말의 MAC 주소를 포함하는 MAC 프레임을 생성하고, 상기 다른 단말로 전송하는 단계를 포함할 수 있다.
- [0017] 일 실시예에 따르면, 다른 단말과의 통신 방법은, 자신의 IP 주소를 해시함수를 사용하여 해시한 값에 기반하여 자신의 MAC 주소를 변경하는 단계; 상기 다른 단말로부터 상기 변경된 MAC 주소를 목적지(destination) 주소로 하는 MAC 프레임을 수신하는 단계; 및 상기 다른 단말의 IP 주소를 상기 해시함수를 사용하여 해시한 값에 기반하여, 상기 수신된 MAC 프레임의 소스 주소가 상기 다른 단말의 MAC 주소에 해당하는지를 검증하는 단계를 포함할 수 있다.

발명의 효과

- [0018] LAN에서 ARP 프로토콜 주소를 제거하여 ARP Poisoning 공격이 불가능하도록 제공할 수 있고, LAN 에서 ARP 트래픽의 높은 볼륨이 제거되어 네트워크 처리량이 증가할 것이다.
- [0019] 또한, LAN에서 ARP 프로토콜 주소를 제거하여 기업 네트워크에서 중앙 집중식 관리가 가능하도록 제공함으로써 SDN 컨트롤러에 의하여 중앙에서 단말들이 네트워크에 연결되도록 관리할 수 있고, 네트워크에서 비가입 및 가입을 동적으로 지원할 수 있고, 스위치의 포트에 플러그인됨으로써 물리적으로 연결된 외부인이 네트워크에서 어떠한 패킷을 보내거나 엿볼 수 없게 된다.

도면의 간단한 설명

- [0020] 도 1은 ARP(Address Resolution Protocol)를 설명하기 위한 도면이다.
- 도 2는 ARP Poisoning 공격을 설명하기 위한 도면이다.
- 도 3은 일 실시예에 있어서, 각각의 장치들이 네트워크 통신을 수행하기 위한 동작을 설명하기 위한 도면이다.
- 도 4는 일 실시예에 있어서, 네트워크에서 통신하는 과정을 설명하기 위한 흐름도이다.
- 도 5는 일 실시예에 있어서, 인터넷 통신을 수행하는 과정을 설명하기 위한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

- [0021] 이하, 실시예를 첨부한 도면을 참조하여 상세히 설명한다.
- [0022] 도 2는 ARP Poisoning 공격을 설명하기 위한 도면이다.
- [0023] A 호스트(210)(IP 주소: 192.168.1.1, MAC 주소: 000000000001) 및 B 호스트(220)(IP 주소: 192.168.1.2, MAC 주소: 000000000002)가 L2 스위치에 의하여 연결되어 서로 패킷을 송수신한다고 가정하자.
- [0024] A 호스트의 ARP 캐쉬 테이블(ARP Cache Table)에는 동일 네트워크 내의 다른 호스트인 B 호스트의 IP 주소 및 IP 주소에 대응되는 MAC 주소가 저장되고, B 호스트의 ARP 캐쉬 테이블(ARP Cache Table)에는 A 호스트의 IP 주소 및 IP 주소에 대응되는 MAC 주소가 저장될 수 있다. 또한, L2 스위치의 라우트 테이블에는 A 호스트 및 B 호스트로의 패킷 라우팅을 위하여 A 호스트 및 B 호스트의 MAC 주소가 저장될 수 있다.
- [0025] 이때, 공격자(230)(Sniffer, IP 주소: 192.168.1.10, MAC 주소: 000112233445)는 ARP 포이즈닝(스푸핑)을 위하여 A 호스트 및 B 호스트로 자신의 MAC 주소를 포함하는 ARP 메시지를 전송할 수 있다. ARP 메시지는 ARP 응답 메시지로써, 예를 들면, 공격자는 ARP 응답 메시지의 송신 IP 주소에 B 호스트의 IP 주소를 부가하고, 송신 MAC 주소에는 자신(공격자)의 MAC 주소를 부가하여 A 호스트로 전송할 수 있다. 마찬가지로, 공격자는 ARP 응답 메시지의 송신 IP 주소에 A 호스트의 IP 주소를 부가하고, 송신 MAC 주소에 자신(공격자)의 MAC 주소를 부가하여 B 호스트로 전송할 수 있다.
- [0026] ARP 프로토콜의 특성에 따르면, 네트워크 내에 존재하는 각 호스트들은 자신이 ARP 요청 메시지를 송신하지 않았는데 ARP 응답 메시지만이 수신되는 경우에도 자신의 ARP 캐쉬 테이블을 업데이트하도록 구성될 수 있다. A 호스트 및 B 호스트는 수신되는 ARP 응답 메시지에 대응하여 자신의 ARP 캐쉬 테이블을 도 2에 도시된 것과 같이 공격자의 MAC 주소로 업데이트하게 된다. 다시 말해서, A 호스트 및 B 호스트는 각각 상대방의 MAC 주소를 공격자의 MAC 주소로 변경하여 ARP 캐쉬 테이블에 저장하며, 이후 A 호스트 및 B 호스트 간 모든 트래픽은 L2 스위치에 의하여 공격자 측으로 라우팅될 수 있다. 이에 따라 공격자는 ARP 프로토콜의 허점을 이용하여, A 호스트 및 B 호스트 간의 패킷을 훔쳐보거나 변조할 수 있게 된다.
- [0027] 이에 따라 LAN에서 ARP 프로토콜 주소를 제거하여 LAN에서 ARP 프로토콜 주소를 제거하여 ARP Poisoning 공격이 불가능하도록 하고, 기업 네트워크에서 중앙 집중식 관리가 가능하도록 하는 방법을 설명하기로 한다. 아래의 실시예들은 IP 주소가 해시함수로 암호화되어 생성된 MAC 주소와 SDN 어플리케이션을 이용한 레이어 2 또는 레이어 3를 액세스 제어하기 위한 방법을 상세하게 설명하기로 한다.
- [0028] 도 3은 일 실시예에 있어서, 각각의 장치들이 네트워크 통신을 수행하기 위한 동작을 설명하기 위한 도면이다.
- [0029] 단말들(320, 330)은 윈도우, 리눅스 등으로 운영되는 PC와 노트북들로서, 컴퓨터 장치로 구현되는 고정형 단말이거나 이동형 단말일 수 있다. 단말들(320, 330)의 예를 들면, 스마트폰(smart phone), 휴대폰, 내비게이션, 컴퓨터, 노트북, 디지털 방송용 단말, PDA(Personal Digital Assistants), PMP(Portable Multimedia Player), 태블릿 PC 등이 해당될 수 있다. 단말들(320, 330)은 ARP 기능을 비활성화할 수 있다. 단말들(320, 330)은 IP 주소를 해시함수로 암호화하거나, IP 주소 및 키를 해시함수로 암호화하여 목적지 단말의 MAC 주소를 계산할 수 있다.
- [0030] 디폴트 라우터(Default Router)(340)는 외부 인터넷으로부터 IP 패킷을 전달할 수 있도록 하기 위하여 SDN 컨트롤러(350)에 의해 고유키를 제공받을 수 있다.
- [0031] 인증 서버(Authentication Server)(310)는 먼저 단말의 식별 정보(예를 들면, 아이디, 패스워드)를 인증할 수 있고, 고유키(K)를 보안 채널(예를 들면, SSL)을 통하여 제공할 수 있다. 마찬가지로, SDN 컨트롤러(350)는 인증 서버로부터 인증을 성공적으로 수행한 후, 고유키를 수신할 수 있다.
- [0032] SDN 컨트롤러(350)는 인증 서버(310)로부터 제공되는 라우터의 키 값을 설정하고 갱신할 수 있다.
- [0033] 우선적으로, 레이어(Layer 2) 통신을 위하여, 제1 단말(320)과 제2 단말(330)이 네트워크에서 통신을 수행하기 위한 과정을 설명하기로 한다. 제1 단말 및 제2 단말은 각각의 IP 주소를 가지고 있다. 제1 단말 및 제2 단말은 서로의 IP 주소를 알고 있다고 가정한다.
- [0034] 예를 들면, 제1 단말의 IP 주소는 IPA, 제2 단말의 IP 주소는 IPB라고 가정하자. 제1 단말은 제2 단말로 통신

할 것을 요청할 수 있다. 제1 단말은 레이어 2 프레임을 구성하기 위하여 제2 단말의 MAC 주소가 필요하고, 제2 단말의 MAC 주소는 목적지 MAC 주소로 사용될 수 있다.

[0035] 제1 단말은 제1 단말 고유의 MAC 주소를 계산하고, 제1 단말의 IP 주소를 해시함수로 암호화할 수 있고, 제2 단말의 IP 주소를 해시함수로 암호화할 수 있다.

[0036] $MAC = Hash_48(IPA)$

[0037] 이때, 해시함수는, SHA1 또는 SHA256과 같은 암호화된 보안 해시 함수로부터 48 비트를 출력할 수 있다. Hash_48(IPA)는 제1 단말의 IP 주소인 IPA를 해시함수를 사용하여 해시한 값을 의미할 수 있으며, 해시한 값에 기반하여 MAC 주소를 계산할 수 있다.

[0038] 제1 단말은 제1 단말의 IP 주소를 해시함수로 해시한 값에 기반하여 제1 단말의 MAC 주소, 제2 단말의 IP 주소를 해시함수로 해시한 값에 기반하여 제2 단말의 MAC 주소를 획득하고, 획득된 MAC 주소를 포함하는 각각 MAC 프레임으로 구성하여 제2 단말로 전송할 수 있다.

[0039] 제2 단말은 MAC 프레임을 수신함에 따라 제1 단말의 MAC 주소가 소스 단말의 MAC 주소와 일치하는지 확인함으로써 MAC 프레임을 검증할 수 있다. 이때, 제2 단말은 해시함수로 암호화된 제1 단말의 IP 주소를 해시함수를 사용하여 해시한 값과 MAC 프레임 내의 소스 어드레스 값을 비교할 수 있다. 만약, 제2 단말은 해시함수로 암호화된 제1 단말의 IP 주소를 계산함에 따른 해시한 값과 MAC 프레임 내의 소스 어드레스 값이 일치하지 않을 경우, 제1 단말의 MAC 주소가 유효하지 않음을 판단할 수 있고, MAC 프레임을 폐기하고 관리자에게 통보할 수 있다.

[0040] 또 다른 예로서, 제1 단말은 제1 단말의 IP 주소 및 고유키를 해시함수를 사용하여 해시한 값에 기반하여 제1 단말의 MAC 주소를 획득하고, 제2 단말의 IP 주소 및 고유키를 해시함수를 이용하여 해시한 값에 기반하여 MAC 주소를 획득할 수 있다.

[0041] $MAC = Hash_48(IPA, K)$

[0042] 이때, 해시함수는, SHA1 또는 SHA256과 같은 암호화된 보안 해시 함수로부터 48 비트를 출력할 수 있다. Hash_48(IPA, K)는 제1 단말의 IP 주소인 IPA 및 고유키를 해시함수를 사용하여 해시한 값을 의미할 수 있으며, 해시한 값에 기반하여 MAC 주소를 계산할 수 있다.

[0043] 제1 단말은 제1 단말 고유의 MAC 주소를 계산하고, 제1 단말의 IP 주소 및 고유키를 해시함수로 암호화할 수 있고, 제2 단말의 IP 주소 및 고유키를 해시함수로 암호화할 수 있다. 이때, 키는 각각의 단말의 식별 정보에 기초하여 인증이 성공적으로 이루어질 경우 부여하는 고유키로서, 예를 들면, 각각의 단말은 서버 또는 관리자로부터 키를 제공받을 수 있다.

[0044] 이에 따라 제1 단말은 제1 단말의 IP 주소 및 고유키를 해시함수를 이용하여 해시한 값에 기반하여 제1 단말의 MAC 주소, 제2 단말의 IP 주소 및 고유키를 해시함수를 이용하여 해시한 값에 기반하여 제2 단말의 MAC 주소를 획득하고, 획득된 MAC 주소를 포함하는 각각 MAC 프레임으로 구성하여 제2 단말로 전송할 수 있다.

[0045] 제2 단말은 제1 단말의 IP 주소 및 키를 해시함수로 암호화된 제1 단말의 MAC 주소가 소스 단말의 MAC 주소와 일치하는지 확인함으로써 MAC 프레임을 검증할 수 있다. 이때, 제2 단말은 고유키까지 해시함수로 암호화된 제1 단말의 IP 주소를 해시함수를 사용하여 해시한 값과 소스 어드레스 값을 비교할 수 있다. 만약, 제2 단말은 키까지 해시함수로 암호화된 제1 단말의 IP 주소를 해시한 값과, MAC 프레임 내의 소스 어드레스 값이 일치하지 않을 경우, 제1 단말의 MAC 주소가 유효하지 않음을 판단하여, MAC 프레임을 폐기하고 관리자에게 통보할 수 있다.

[0046] 다른 실시예로, Layer 3 통신을 위하여, 인터넷 통신을 위한 과정을 설명하기로 한다.

[0047] 앞서 설명한 것과 마찬가지로, MAC 주소를 생성함에 있어서, IP 주소를 해시함수로 암호화하여 MAC 주소를 생성할 수 있고, IP 주소 및 키를 해시함수로 암호화하여 MAC 주소를 생성할 수도 있다.

[0048] 아웃바운드 트래픽에 대하여, 제1 단말은 디폴트 라우터의 MAC 주소를 목적지 MAC 주소로 설정할 수 있다. 디폴트 라우터는 MAC 프레임을 검사하고, MAC 프레임의 유효성을 검증할 수 있다. 이때, MAC 프레임이 유효하다면, 레이어 3 통신을 시작할 수 있다. 제1 단말은 라우터로 아웃바운드 트래픽을 전송할 수 있다.

[0049] 제1 단말의 IP 주소가 인바운드 트래픽일 경우, 디폴트 라우터는 제1 단말의 IP 주소에 대한 MAC 주소를 계산할

수 있어야 한다. 제1 단말의 MAC 주소를 계산하기 위하여 키가 필요하며, SDN 컨트롤러로부터 고유키를 제공받을 수 있다.

- [0050] 인증 서버는 제1 단말 및 제2 단말에 고유키를 제공할 수 있다. 여기서, 제2 단말은 라우터일 수 있다. 이때, 고유키는 제1 단말 및 제2 단말의 각각으로부터의 식별 정보에 기초하여 제1 단말 및 제2 단말의 각각이 인증 서버에 인증됨에 따라 제1 단말 및 제2 단말의 각각으로 제공될 수 있다. 이때, 인증 서버에서 각각의 단말의 식별 정보에 기초하여 인증이 수행됨에 따라 SDN 컨트롤러로부터 고유키를 각각의 단말로 전달하도록 제공할 수 있다.
- [0051] 디폴트 라우터는 제1 단말의 IP 주소를 해시함수를 사용하여 해시한 값에 기반하여 제1 단말의 MAC 주소를 계산할 수 있다. 디폴트 라우터는 제1 단말의 MAC 주소를 포함하는 MAC 프레임을 제1 단말로 전송할 수 있다.
- [0052] 제1 단말이 MAC 프레임을 수신할 경우, 소스 MAC 주소와 제1 단말의 해시함수로 암호화된 IP 주소를 계산한 해시한 값을 비교하여 MAC 프레임의 유효성을 검증할 수 있다.
- [0053] 새로운 단말이 네트워크에 참여할 경우, 새로운 단말은 물리적 네트워크 스위치 포트에 연결되는 경우에도 고유키를 가지고 있지 않기 때문에 통신을 수행할 수 없다. 인증 서버로부터 유효키를 획득하기 위하여, 대역의 채널을 통하여 인증 서버로 연결될 수 있다. OOC는 네트워크에 유효한 MAC 주소를 가지고 있지 않더라도 인증 서버에서 모든 인증 패킷(예를 들면, Extensible Authentication Protocol:EAP)을 전송함으로써 구현될 수 있다. 이때, EAP는 아이디와 패스워드와 같은 인증에 필요한 정보를 제공할 수 있다.
- [0054] 성공적으로 인증이 수행됨에 따라 새로운 단말은 인증 서버로부터 고유키를 수신할 수 있다. 이때, 인증 및 키 전달 채널은 SSL에 의해 보호될 수 있다. 그러면, 새로운 단말은 고유키를 가지게 되고, 네트워크에 연결될 수 있다.
- [0055] 단말의 네트워크를 종료하는 것에 대하여 설명하기로 하자. SDN 컨트롤러는 해당 포트를 사용하지 않을 수 있다. 인증 서버는 키를 갱신할 수 있고, SDN 컨트롤러에게 네트워크에 고유키를 브로드캐스트하도록 요청할 수 있다. 이때, 브로드캐스트되어 수신한 모든 단말들은 업데이트된 고유키를 수신할 수 있다. 그러면, 단말의 네트워크가 철회되어, 통신이 불가능해진다.
- [0056] 도 4는 일 실시예에 있어서, 네트워크에서 통신하는 과정을 설명하기 위한 흐름도이다.
- [0057] 제1 단말(410)의 IP 주소는 IPA, 제2 단말(420)의 IP 주소는 IPB이고, 제1 단말은 제2 단말로 통신할 것을 요청할 수 있다. 제1 단말은 레이어 2 프레임을 구성하기 위하여 제2 단말의 MAC 주소가 필요하고, 제2 단말의 MAC 주소는 목적지 MAC 주소로 사용될 수 있다.
- [0058] 제1 단말은 자신의 IP 주소를 해시함수를 사용하여 해시한 값에 기반하여 MAC 주소를 계산할 수 있다. 또한, 제1 단말은 다른 단말의 IP 주소를 해시함수를 사용하여 해시한 값에 기반하여 다른 단말의 MAC 주소를 획득할 수 있다. 이때, 제1 단말은 계산된 자신의 MAC 주소, 획득된 다른 단말의 MAC 주소를 포함하는 MAC 프레임을 생성하고, 다른 단말로 전송할 수 있다.
- [0059] 제1 단말은 제1 단말 고유의 MAC 주소를 계산하고, 제1 단말의 IP 주소를 해시함수를 사용하여 해시한 값에 기반하여 제1 단말의 MAC 주소를 계산하고, 제2 단말의 IP 주소를 해시함수를 사용하여 해시한 값에 기초하여 제2 단말의 MAC 주소를 획득할 수 있다. 이때, 제1 단말은 제1 단말의 IP 주소를 해시함수를 사용하여 암호화할 수 있고 또는 제1 단말의 IP 주소 및 고유키를 해시함수로 사용하여 암호화할 수 있다. 또한, 마찬가지로, 제1 단말은 제2 단말의 IP 주소를 해시함수를 사용하여 암호화할 수 있고, 제2 단말의 IP 주소 및 고유키를 해시함수를 사용하여 암호화할 수 있다.
- [0060] 이에 따라 제1 단말은 제1 단말의 MAC 주소, 제2 단말의 MAC 주소를 포함하는 MAC 프레임을 생성하여 제2 단말로 전송할 수 있다(430). 제2 단말은 제1 단말로부터 변경된 MAC 주소를 목적지 주소로 하는 MAC 프레임을 수신할 수 있다(432). 이때, 제2 단말의 IP 주소를 해시함수를 사용하여 해시한 값에 기초하여 제2 단말의 MAC 주소가 변경될 수 있다. 제2 단말은 제1 단말의 IP 주소를 해시함수를 사용하여 해시한 값에 기반하여 계산된 MAC 주소가 MAC 프레임 내의 소스 어드레스 값과 비교함으로써 MAC 프레임을 검증할 수 있다(433, 434). 이때, 제2 단말은 해시함수로 암호화된 제1 단말의 IP 주소를 계산하여 제1 단말의 MAC 주소를 계산할 수 있다. 만약, 제2 단말은 해시함수로 암호화된 제1 단말의 IP 주소를 계산한 제1 단말의 MAC 주소가 유효하지 않을 경우, MAC 프레임을 폐기하고 MAC 주소가 유효하지 않음을 통보할 수 있다.

- [0061] 도 5는 일 실시예에 있어서, 인터넷 통신을 수행하는 과정을 설명하기 위한 흐름도이다.
- [0062] MAC 주소를 생성함에 있어서, IP 주소를 해시함수를 사용하여 해시한 값에 기반하여 MAC 주소를 획득할 수 있고, IP 주소 및 키를 해시함수를 사용하여 해시한 값에 기반하여 MAC 주소를 획득할 수도 있다. 도 5에서는 IP 주소 및 키를 해시함수를 사용하여 해시한 값에 기반하여 MAC 주소를 생성함으로써 인터넷 통신을 수행하는 과정을 설명하기로 한다.
- [0063] 아웃바운드 트래픽에 대하여, 제1 단말(510)은 디폴트 라우터(520)의 MAC 주소를 목적지 MAC 주소로 설정할 수 있다(541). 제1 단말은 MAC 프레임을 디폴트 라우터로 전송함으로써 디폴트 라우터는 MAC 프레임을 수신할 수 있다(542). 디폴트 라우터는 MAC 프레임을 검사하고, MAC 프레임의 유효성을 검증할 수 있다(543). 이때, MAC 프레임이 유효하다면, 레이어 3 통신을 시작할 수 있다(543). 제1 단말로부터 라우터로 아웃바운드 트래픽을 전송할 수 있게 된다.
- [0064] 제1 단말의 IP 주소가 인바운드 트래픽일 경우, 디폴트 라우터는 제1 단말의 IP 주소에 대한 MAC 주소를 계산할 수 있어야 한다. 제1 단말의 MAC 주소를 계산하기 위하여 고유키가 필요하며, SDN 컨트롤러(530)로부터 고유키를 제공받을 수 있다(544). 디폴트 라우터는 제1 단말의 IP 주소 및 고유키를 해시함수를 사용하여 해시한 값에 기반하여 제1 단말의 MAC 주소를 계산할 수 있다(545). 디폴트 라우터는 제1 단말의 MAC 주소를 포함하는 MAC 프레임을 생성하여 제1 단말로 전송할 수 있다.
- [0065] 제1 단말이 MAC 프레임을 수신할 경우, 소스 MAC 주소와 제1 단말의 키까지 해시함수로 암호화된 IP 주소를 계산한 해시한 값을 비교하여 MAC 프레임의 유효성을 검증할 수 있다(546).
- [0066] 이상에서 설명된 장치는 하드웨어 구성요소, 소프트웨어 구성요소, 및/또는 하드웨어 구성요소 및 소프트웨어 구성요소의 조합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치 및 구성요소는, 예를 들어, 프로세서, 컨트롤러, ALU(arithmetic logic unit), 디지털 신호 프로세서(digital signal processor), 마이크로컴퓨터, FPGA(field programmable gate array), PLU(programmable logic unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수 목적 컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 애플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(processing element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 컨트롤러를 포함할 수 있다. 또한, 병렬 프로세서(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.
- [0067] 소프트웨어는 컴퓨터 프로그램(computer program), 코드(code), 명령(instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성요소(component), 물리적 장치, 가상장치(virtual equipment), 컴퓨터 저장 매체 또는 장치에 영구적으로, 또는 일시적으로 구체화(embodiment)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.
- [0068] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 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(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 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.
- [0069] 이상과 같이 실시예들이 비록 한정된 실시예와 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가

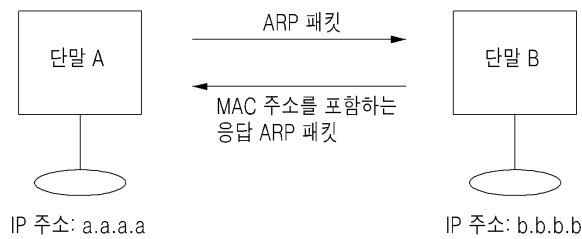
진 자라면 상기의 기재로부터 다양한 수정 및 변형이 가능하다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다.

[0070]

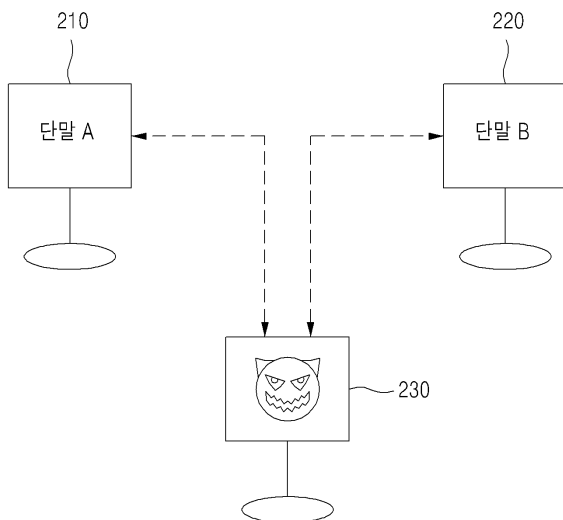
그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

도면

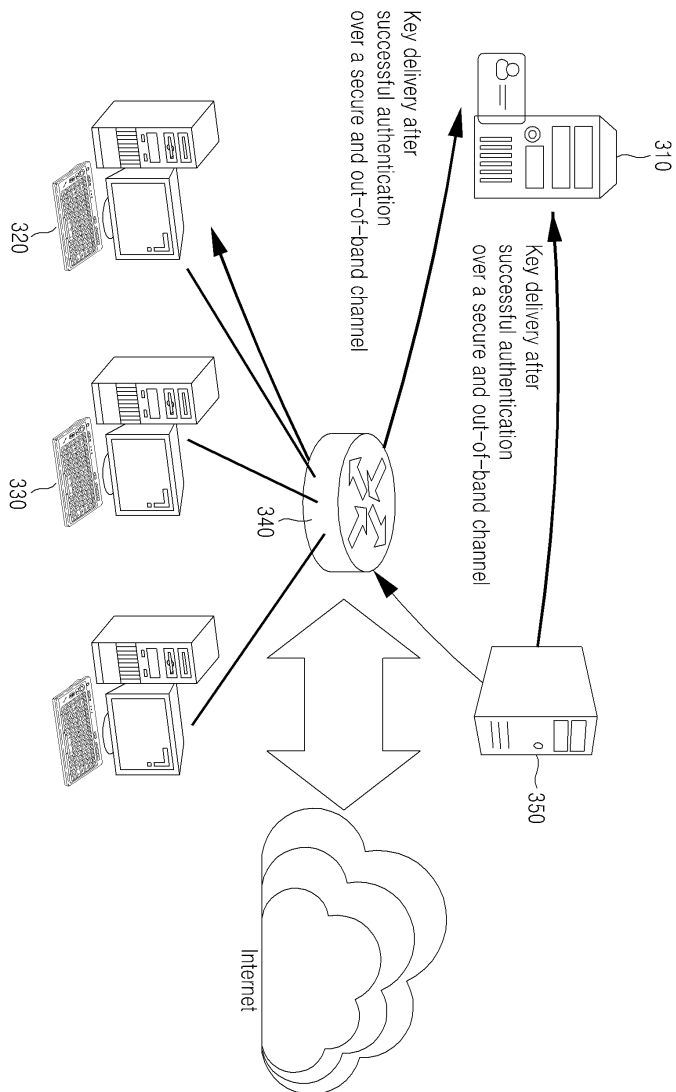
도면1



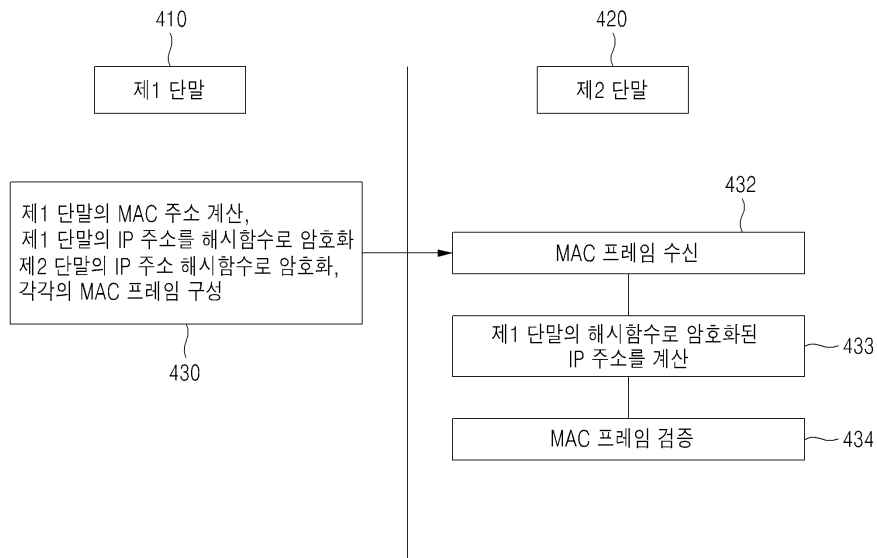
도면2



도면3



도면4



도면5

