(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2014-0075475
(43) 공개일자 2014년06월19일

(51) 국제특허분류(Int. Cl.)
H04L 12/22 (2006.01)
(21) 출원번호 10-2012-0143858
(22) 출원일자 2012년12월11일
심사청구일자 없음
기술이전 희망 : 기술양도, 실시권허여, 기술지도

(71) 출원인
한국전자통신연구원
대전광역시 유성구 가정로 218 (가정동)
(72) 발명자
김정환
대전 유성구 상대남로 26, 918동 2504호 (상대동, 트리풀시티아파트)
윤빈영
대전 유성구 배울1로 119, 1201동 1102호 (용산동, 대덕테크노밸리12단지아파트)
김상기
대전 유성구 지족로 343, 209동 1002호 (지족동, 반석마을2단지아파트)
(74) 대리인
팬코리아특허법인

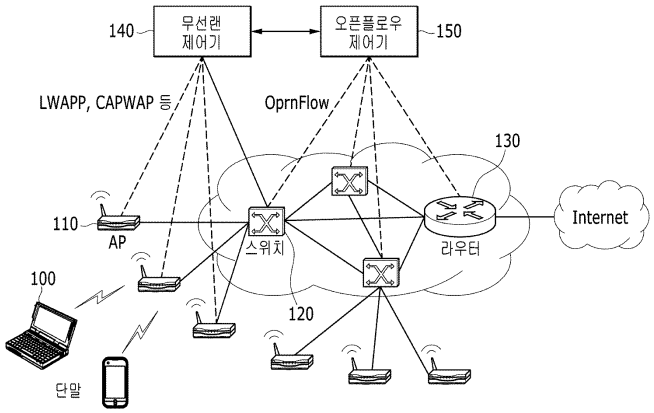
전체 청구항 수 : 총 1 항

(54) 발명의 명칭 **비인가 무선랜 AP의 접근 제어 시스템 및 방법**

(57) 요 약

본 발명에 따른 비인가 무선랜 AP의 접근 제어 방법은 비인가 무선랜 AP의 접근 제어 시스템이 비허가된 무선랜 AP의 접근을 제어하는 방법에 있어서, 무선랜 제어기가 접속이 허용된 AP들의 MAC 주소를 오플플로우 제어기로 전송하고, 상기 오픈플로우 제어기가 상기 MAC 주소를 데이터베이스에 저장하는 단계, 상기 오픈플로우 제어기가 상기 스위치가 상기 MAC 주소를 전송받아 플로우 테이블의 플로우 엔트리에 추가하고, 상기 MAC 주소들의 접속 포트를 상기 오픈플로우 제어기에 보고하는 단계, 비인가 AP가 접속을 시도하여 ARP 요청 메시지가 스위치에 전달되면, 상기 스위치가 상기 플로우 엔트리에 없는 MAC 주소를 통해 접속됨을 인지하여 패킷을 폐지하고, 폐지된 이력을 상기 오픈플로우 제어기로 전송하는 단계, 그리고 상기 오픈플로우 제어기가 상기 무선랜 제어기로 폐지된 상기 이력을 전송하는 단계를 포함한다.

대 표 도



특허청구의 범위

청구항 1

비인가 무선랜 AP의 접근 제어 시스템이 비허가된 무선랜 AP의 접근을 제어하는 방법에 있어서,

무선랜 제어기가 접속이 허용된 AP들의 MAC 주소를 오플플로우 제어기로 전송하고, 상기 오픈플로우 제어기가 상기 MAC 주소를 데이터베이스에 저장하는 단계,

상기 오픈플로우 제어기가 상기 스위치가 상기 MAC 주소를 전송받아 플로우 테이블의 플로우 엔트리에 추가하고, 상기 MAC 주소들의 접속 포트를 상기 오픈플로우 제어기에 보고하는 단계,

비인가 AP가 접속을 시도하여 ARP 요청 메시지가 스위치에 전달되면, 상기 스위치가 상기 플로우 엔트리에 없는 MAC 주소를 통해 접속됨을 인지하여 패킷을 폐지하고, 폐지된 이력을 상기 오픈플로우 제어기로 전송하는 단계, 그리고

상기 오픈플로우 제어기가 상기 무선랜 제어기로 폐지된 상기 이력을 전송하는 단계

를 포함하는

비인가 무선랜 AP의 접근 제어 방법.

명 세 서

기 술 분 야

[0001] 본 발명은 무선랜 AP를 통한 인터넷 접속이 가능한 환경에서 비허가된 무선랜 AP의 접근 제어 방법에 관한 것이다.

배 경 기 술

[0002] 무선랜을 통한 인터넷 접속은 현재 널리 사용되고 있는 방법이다. 하지만, 회사 내에서 불법적으로 설치한 무선랜을 통한 인터넷 접속은 회사기밀 유출 등 심각한 문제를 야기하고 있으며, 공중 무선랜 환경에서도 사용자의 임의적인 무선랜 AP(Access Point) 설치는 무선 사용에 대한 품질을 저하시키는 요인이 되고 있다.

[0003] 최근 엔터프라이즈 환경에서는 이러한 단점을 보완하고, 사내에 설치된 AP에 대한 전체적인 관리 및 제어를 수행하는 무선랜 제어기(WLAN Controller) 기반의 솔루션을 많이 채택하고 있다. 무선랜 제어기 기반의 솔루션은 무선랜 제어기를 통해 무선랜 자원의 효율적인 구성 및 VoIP와 같은 품질 보장형 서비스의 제공이 가능하며, AP의 구성 및 펌웨어 업데이트(firmware update) 등을 수행한다.

[0004] 하지만, 여전히 사내에서의 비인가 된 AP 설치로 인한 네트워크 접속 품질 저하 및 회사 기밀 유출 등에 대한 위험을 안고 있다. 이를 위한 솔루션으로 무선 구간에서의 채널 검색, 탐지를 통한 솔루션들이 있으나, 비용이 비싸고 운영의 어려움도 여전히 존재한다.

[0005] 최근 유선 네트워크에서는, 스위치나 라우터의 기능에서 데이터 경로(data path)와 제어를 분리하여 중앙 집중화된 방식으로 플로우(flow) 제어가 가능한 오픈플로우(OpenFlow) 기술이 대두되고 있다. 오픈플로우 제어기는 스위치나 라우터에 유입되는 패킷의 특성(예를 들어, MAC address, IP address, Port, VLAN tag 등)에 따라 패킷의 흐름을 제어하기 위해 행동들(예를 들어, Forward, Drop 등)을 수행 가능하게 한다. 이러한 상호작용을 위해서 제어기와 스위치 및 라우터 간에 오픈플로우 프로토콜을 사용한다.

발명의 내용

해결하려는 과제

[0006] 따라서, 본 발명의 실시 예에서는, 엔터프라이즈 환경 또는 공중 핫스팟(Hotspot)의 무선랜 AP를 통한 인터넷 접속이 가능한 환경에서 비허가된 무선랜 AP의 접근을 제어하는 방법을 제공하고자 한다.

과제의 해결 수단

[0007] 본 발명의 일 양태에 따른 비인가 무선랜 AP의 접근 제어 방법은 비인가 무선랜 AP의 접근 제어 시스템이 비허가된 무선랜 AP의 접근을 제어하는 방법에 있어서, 무선랜 제어기가 접속이 허용된 AP들의 MAC 주소를 오플플로우 제어기로 전송하고, 상기 오픈플로우 제어기가 상기 MAC 주소를 데이터베이스에 저장하는 단계, 상기 오픈플로우 제어기가 상기 스위치가 상기 MAC 주소를 전송받아 플로우 테이블의 플로우 엔트리에 추가하고, 상기 MAC 주소들의 접속 포트를 상기 오픈플로우 제어기에 보고하는 단계, 비인가 AP가 접속을 시도하여 ARP 요청 메시지가 스위치에 전달되면, 상기 스위치가 상기 플로우 엔트리에 없는 MAC 주소를 통해 접속됨을 인지하여 패킷을 폐지하고, 폐지된 이력을 상기 오픈플로우 제어기로 전송하는 단계, 그리고 상기 오픈플로우 제어기가 상기 무선랜 제어기로 폐지된 상기 이력을 전송하는 단계를 포함한다.

발명의 효과

[0008] 이와 같이, 본 발명의 한 실시예에 따르면, 무선랜 AP를 통한 망 접속 제어를 무선구간에서 채널 검색 등의 방법을 사용하지 않고, 무선랜 AP가 망으로 접속되는 오픈플로우 기반 스위치나 라우터 단에서 불법적인 접근을 효율적으로 제어하고 차단할 수 있다.

[0009] 또한, 본 발명은 무선랜 AP를 통한 접속에 대한 망 접근 제어를 오픈플로우 기반으로 에지(Edge) 스위치 단에서 효율적인 접근 제한 정책 설정 및 제어를 용이하게 할 수 있다.

도면의 간단한 설명

[0010] 도 1은 본 발명의 한 실시예에 따른 무선랜 AP의 접근을 제어하기 전체적인구성을 도시한 도면이다.

도 2는 본 발명의 한 실시예에 따른 비인가된 무선랜 AP의 접근을 제어하는과정을 도시한 흐름도이다.

도 3은 본 발명의 한 실시예에 따른 위조된 MAC을 가진 무선랜 AP를 차단하는 과정을 도시한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0011] 아래에서는 첨부한 도면을 참고로 하여 본 발명의 실시예에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

[0012] 명세서 전체에서, 단말(terminal)은 이동국(mobile station, MS), 이동 단말(mobile terminal, MT), 가입자국(subscriber station, SS), 휴대 가입자국(portable subscriber station, PSS), 접근 단말(access terminal, AT), 사용자 장치(user equipment, UE) 등을 지칭할 수도 있고, 단말, MT, SS, PSS, AT, UE 등의 전부 또는 일부의 기능을 포함할 수도 있다.

[0013] 또한, 기지국(base station, BS)은 노드B(node B), 고도화 노드B(evolved node B, eNodeB), 접근점(access point, AP), 무선 접근국(radio access station, RAS), 송수신 기지국(base transceiver station, BTS), MMR(mobile multihop relay)-BS 등을 지칭할 수도 있고, 노드B, eNodeB, AP, RAS, BTS, MMR-BS 등의 전부 또는 일부의 기능을 포함할 수도 있다.

[0014] 명세서 전체에서, 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다. 또한, 명세서에 기재된 "…부", "…기", "모듈", "블록" 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 하드웨어나 소프트웨어 또는 하드웨어 및 소프트웨어의 결합으로 구현될 수 있다.

[0015] 도 1은 본 발명의 한 실시예에 따른 무선랜 AP의 접근을 제어하기 전체적인구성을 도시한 도면이다.

[0016] 도 1을 참조하면, 본 발명에 따른 비인가 무선랜 AP의 접근 제어 시스템의 전체적인 구성을 볼 수 있다. 엔터프라이즈 환경에서의 무선랜 AP들은 도 1과 같이 무선랜의 구성을 가진다. 무선랜 제어기(WLAN Controller)(140)는 새롭게 조인(join)하거나 빠져나가는 무선랜 AP들을 관리하고, 사내 환경에 맞는 구성을 설정한다.

[0017] 그리고, 무선랜 제어기(140)는 펌웨어 이미지(firmware Image)를 AP에 다운로드하여, 전체적인 환경을 설치하고 구성한다. 이와 관련되어 사용되는 프로토콜에는 LWAPP(Lightweight Access Point Protocol, IETF RFC 5412)나 CAPWAP(Control and Provisioning of Wireless Access Points, IETF RFC 5415)이 있다.

[0018] 오픈플로우(OpenFlow) 기반의 스위치(120) 및 라우터(130) 네트워크 구조는 도 1의 우측과 같은 구성을 가진다. 기존 라우터나 스위치에서는, 동일한 장비 내에서 빠른 패킷 포워딩(fast packet forwarding)(데이터 경로, data path)과 하이 레벨 라우팅 결정(high level routing decision)(제어 경로, control path)을 처리한다. 그러나 오픈플로우 스위치(120)는 이 두가지 기능을 분리한다. 데이터 경로 부분은 스위치(120)에 남고, 제어 경로 부분은 제어기(150)로 분리된다. 오픈플로우 스위치(120)와 제어기(150) 간의 통신은 오픈플로우 프로토콜을 따른다. 오픈플로우 프로토콜은 packet-received, send-packet-out, modify-forwarding 및, get-stats message 들을 정의한다. 오픈플로우 스위치(120)에는 데이터 경로의 흐름을 처리하기 위한 플로우 테이블(flow table)들이 존재한다. 플로우 테이블은 플로우 엔트리(flow entry)로 구성되며, 매칭될 패킷 필드(packet field) 집합과 send-out-port, modify-field 및, 폐기(drop) 같은 행동(action)을 포함한다.

[0019] 예를 들어, 오픈플로우 스위치(120)가 패킷을 받았을 때, 이 패킷이 전에 받았던 적이 없는 패킷이라면, 즉 매칭되는 플로우 엔트리가 없다면 그 패킷을 제어기(150)에게 보낸다. 그러면 제어기(150)는 그 패킷을 처리할 수 있는 규칙이나 로직을 가지고 있어, 패킷 처리에 대한 결정을 한다. 그래서 해당 패킷을 폐기(drop)할 수도 있고, 다음에 유사한 패킷을 포워딩(forwarding)하는 규칙을 플로우 엔트리에 추가하기 위해 스위치(120)에 명령할 수도 있다.

[0020] 따라서 본 구성을 통해서, 무선랜 AP(110)를 거쳐 오픈플로우 스위치(120)로 유입되는 데이터 패킷들의 특성에 따라 서로 다른 행동(Action)을 수행하여 오픈플로우 제어기(150)가 데이터의 흐름을 제어할 수 있는 구조가 갖추어진다.

[0021] 도 2는 본 발명의 한 실시예에 따른 비인가된 무선랜 AP의 접근을 제어하는과정을 도시한 흐름도이다.

[0022] 우선, 무선랜 제어기(WLAN controller)(140)와 오픈플로우 제어기(150) 간의 셋업 과정을 살펴본다.

[0023] 무선랜 제어기(140)는 오픈플로우 제어기(150)의 통신을 위한 연결(connection)을 설정한다. 상기 연결 설정은 TCP나 UDP 프로토콜을 사용하며, 안전한 통신을 위해 SSL를 사용할 수도 있다(S110).

[0024] 무선랜 제어기(140)는 현재 자신이 관리하고 있는 접속 허용된 AP들의 MAC 정보를 오픈플로우 제어기(150)에게 전송하고, 오픈플로우 제어기(150)는 그 내용을 Configuration DB에 저장한다(S120).

[0025] 오픈플로우 제어기(150)는 상기의 MAC 정보들에 대한 정상적인 포워딩(forwarding)을 지시하는 명령을 내리고, 스위치(120)는 해당 MAC 정보를 플로우 테이블의 플로우 엔트리로 추가한다(S130).

[0026] 스위치(120)는 MAC 학습(learning)을 통해 저장된 정보를 바탕으로, MAC 주소들이 어느 포트(port)에 접속되어 있는지 오픈플로우 제어기(150)로 보고하며, 이에 오픈플로우 제어기(150)는 포트 정보와 함께 {포트, MAC 주소 리스트} 형태로 저장하여 최종 화이트 리스트(White list)를 구성한다.

[0027] 다음으로, 등록되지 않은 MAC 주소를 가진 불법의 AP의 접속 차단 과정을 살펴본다.

[0028] 불법 AP(110a)의 연결이 이루어지면, 그 AP(110a)에 단말(100)이 접속하여 외부망으로 연결하려는 시도를 한다. 만약, 허용되지 않는 MAC 주소를 가진 AP(110a)가 스위치(120)에 연결되고, 단말(100)을 통해 통신을 시도할 때, 브로드캐스팅 메시지인 ARP 요청(ARP Request)이 스위치(120)로 전달된다(S150). 오픈플로우 스위치(120)는 전술한 바와 같이, 플로우 엔트리에 없는 MAC을 통한 접속이 연결되었으므로, 패킷을 폐기한다(S160).

[0029] 이때, 폐기된 이력은 오픈플로우 제어기(150)에게 보고되며(S170), 이 사항을 다시 무선랜 제어기(140)에게 전달한다(S180). 이후 무선랜 제어기(140)의 관리자는 비허가된 AP 접속에 대한 오프라인 조치(예를 들어, AP의 위치파악 및 철거)를 취할 수 있다.

[0030] 도 3은 본 발명의 한 실시예에 따른 위조된 MAC을 가진 무선랜 AP를 차단하는 과정을 도시한 흐름도이다.

[0031] 도 3을 참조하면, 위조된 MAC 주소를 가진 AP(110a)를 통해, 망연결을 시도하는 경우, ARP 요청이 스위치에 전송된다(S190).

[0032] 오픈플로우 스위치(120)는 MAC 주소는 동일하나, 접속되는 포트가 다르므로, 이에 대한 처리를 오픈플로우 제어기(150)에게 맡기기 위해 패킷을 포워딩한다(S200). 오픈플로우 제어기(150)는 최근에 관리하고 있는 AP들의 구성에 변경사항이 발생하였는지를 확인하기 위해, 다시 AP MAC 주소의 리스트를 요청하고, 변경사항을 수신하며, 데이터베이스(DB)에 업데이트를 수행한다(S210).

[0033] 비인가 AP(110a)가 포트를 이동한 AP일 경우를 살펴본다.

[0034] 여기서, 데이터베이스에 있는 기존 설정과 비교한 후, 비인가 AP(110a)가 포트를 이동한 AP일 경우에는, 오픈플로우 제어기(150)는 스위치(120)에게 일반적인 스위칭/라우팅 경로로 처리될 수 있도록 정상적인 포워딩 지시를 하며(S220), 이에 따라 스위치(120)는 자신의 MAC 주소를 해당 AP에 회신하고(S230), 이후 스위치(120)는 목적지로의 패킷 포워딩을 수행한다.

[0035] 또한, 오픈플로우 제어기(150)는 변경된 포트, MAC 구성을 반영하기 위해 스위치(120) 내의 플로우 엔트리를 업데이트 한다(S240).

[0036] 다음으로, 위조된 MAC을 가진 AP일 경우를 살펴본다.

[0037] 데이터베이스에 있는 기존 설정과 비교한 후 변경사항이 없는데도, 타 포트에서 허락된 MAC 주소로 망접속을 시도하는 것은, 위조된 AP를 통한 접속이라고 판단하고, 패킷을 일단 폐기(drop)한다(S250).

[0038] 오픈플로우 제어기(150)는 해당 AP(110a)에게 ARP 포이즈닝(poisoning)에 대한 규칙을 설정한다. 여기서, ARP 포이즈닝은 스위치에 대한 가짜 MAC 주소를 ARP 응답에 회신하는 것을 의미한다.

[0039] 이에 의해서, 스위치(120)가 자신의 MAC 주소가 아닌 가짜 MAC 주소를 ARP 응답에 담아서 보냄으로써, 해당 AP(110a)를 통한 망 접속시도는 원천 차단된다(S260).

[0040] 이후, 해당 AP(110a)로부터 지속적으로 ARP 요청이 오게 되면(S270), 스위치(120)의 플로우 엔트리에 의해 패킷은 자동 폐기된다(S280).

[0041] 이와 같이, 본 발명은 무선랜 AP를 통한 망 접속 제어를 무선구간에서 채널 검색 등의 방법을 사용하지 않고, 무선랜 AP가 망으로 접속되는 오픈플로우 기반 스위치나 라우터 단에서 불법적인 접근을 효율적으로 제어하고 차단할 수 있다.

[0042] 또한, 본 발명은 무선랜 AP를 통한 접속에 대한 망 접근 제어를 오픈플로우 기반으로 에지(Edge) 스위치 단에서 효율적인 접근 제한 정책 설정 및 제어를 용이하게 할 수 있다.

[0043] 이상에서 설명한 본 발명의 실시예는 장치 및 방법을 통해서만 구현이 되는 것은 아니며, 본 발명의 실시예의 구성에 대응하는 기능을 실현하는 프로그램 또는 그 프로그램이 기록된 기록 매체를 통해 구현될 수도 있다.

[0044] 이상에서 본 발명의 실시예에 대하여 상세하게 설명하였지만 본 발명의 권리범위는 이에 한정되는 것은 아니고 다음의 청구범위에서 정의하고 있는 본 발명의 기본 개념을 이용한 당업자의 여러 변형 및 개량 형태 또한 본 발명의 권리범위에 속하는 것이다.

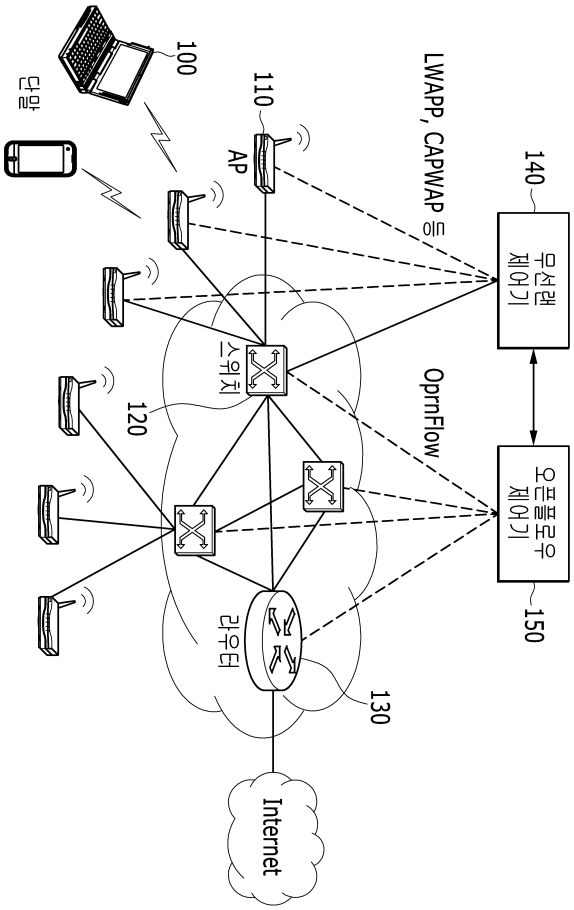
부호의 설명

[0045]

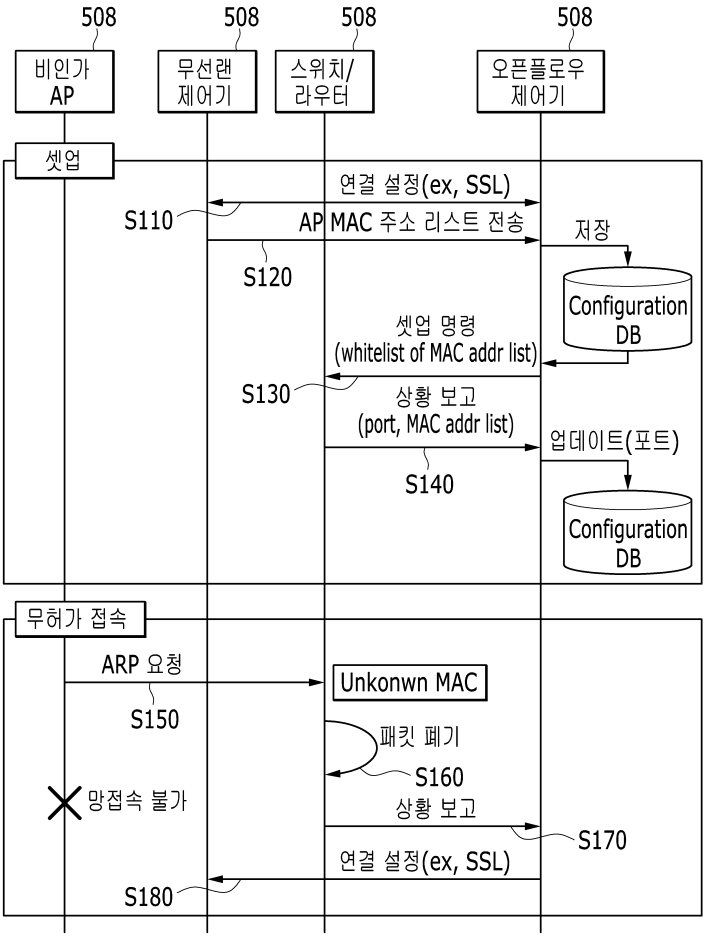
100: 단말	110: AP
120: 스위치	130: 라우터
140: 무선 제어기	150: 오픈플로우 제어기

도면

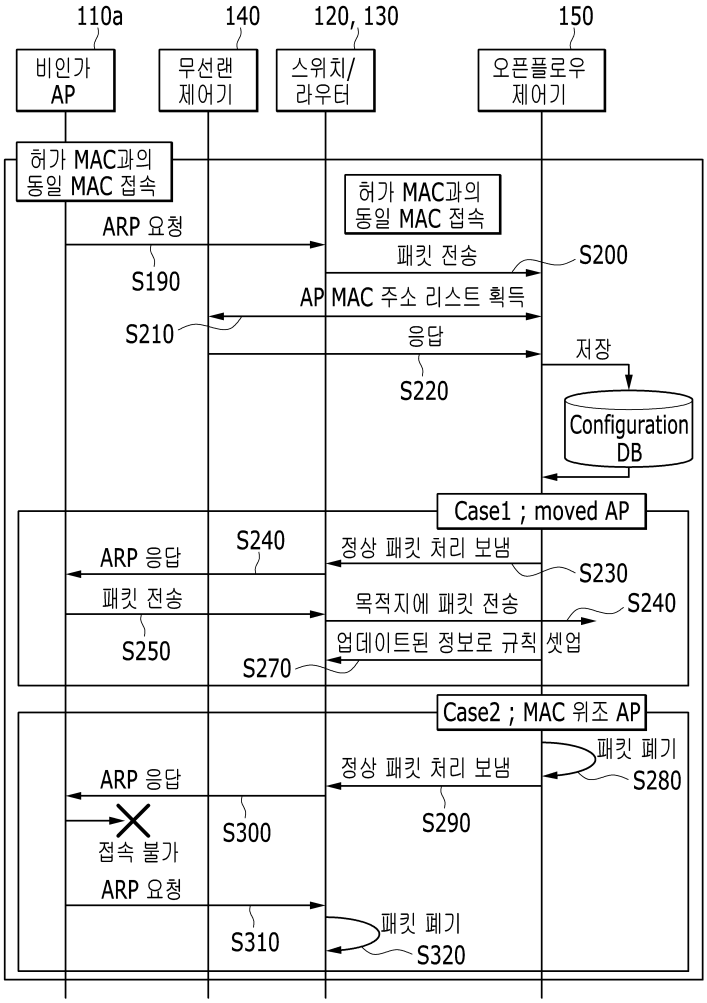
도면1


단말
100
AP
110
LWAPP, CAPWAP 등
140
무선랜
제어기
스위치
120
OprnFlow
오픈플로우
제어기
150
라우터
130
Internet

도면2


508
508
508
508
비인가 AP
무선랜 제어기
스위치/ 라우터
오픈플로우 제어기
셋업
연결 설정(ex, SSL)
S110
AP MAC 주소 리스트 전송
저장
S120
Configuration DB
셋업 명령 (whitelist of MAC addr list)
S130
상황 보고 (port, MAC addr list)
업데이트(포트)
S140
Configuration DB
무허가 접속
ARP 요청
Unkonwn MAC
S150
패킷 폐기
S160
망접속 불가
상황 보고
S170
연결 설정(ex, SSL)
S180

도면3


110a
140
120, 130
150
비인가 AP
무선랜 제어기
스위치/ 라우터
오픈플로우 제어기
허가 MAC과의 동일 MAC 접속
허가 MAC과의 동일 MAC 접속
ARP 요청
S190
패킷 전송
S200
AP MAC 주소 리스트 획득
S210
응답
S220
저장
Configuration DB
Case1 ; moved AP
S240
ARP 응답
정상 패킷 처리 보냄
S230
패킷 전송
S250
목적지에 패킷 전송
S240
업데이트된 정보로 규칙 셋업
S270
Case2 ; MAC 위조 AP
패킷 폐기
S280
ARP 응답
정상 패킷 처리 보냄
S290
S300
접속 불가
ARP 요청
S310
패킷 폐기
S320