



(19) 대한민국특허청(KR)

(12) 등록특허공보(B1)

(45) 공고일자 2015년08월05일

(11) 등록번호 10-1540343

(24) 등록일자 2015년07월23일

(51) 국제특허분류(Int. Cl.)

H04W 12/12 (2009.01)

(21) 출원번호 10-2013-0106843

(22) 출원일자 2013년09월05일

심사청구일자 2013년09월05일

(65) 공개번호 10-2015-0028139

(43) 공개일자 2015년03월13일

(56) 선행기술조사문헌

Somayeh Nikbakhsh 외 1인, "A Novel Approach for Rogue Access Point Detection on the Client-Side", WAINA 2012 26th International Conference, IEEE, 2012.03.

Diogo Monica 외 1인, "WiFiHop-Mitigating the Evil Twin Attack through Multi-hop Detection", Computer Security - ESORICS 2011, pp21-39, 2011.09.

(73) 특허권자

승실대학교산학협력단

서울특별시 동작구 상도로 369 (상도동)

주식회사 안랩

경기도 성남시 분당구 판교역로 220 (삼평동)

(72) 발명자

정수환

서울특별시 동작구 상도로 369 승실대학교 형남공학관 1105호

임권택

서울특별시 동작구 상도로 369 승실대학교 형남공학관 1102호

박정수

서울특별시 동작구 상도로 369 승실대학교 형남공학관 1102호

(74) 대리인

특허법인엠에이피에스

전체 청구항 수 : 총 9 항

심사관 : 이상윤

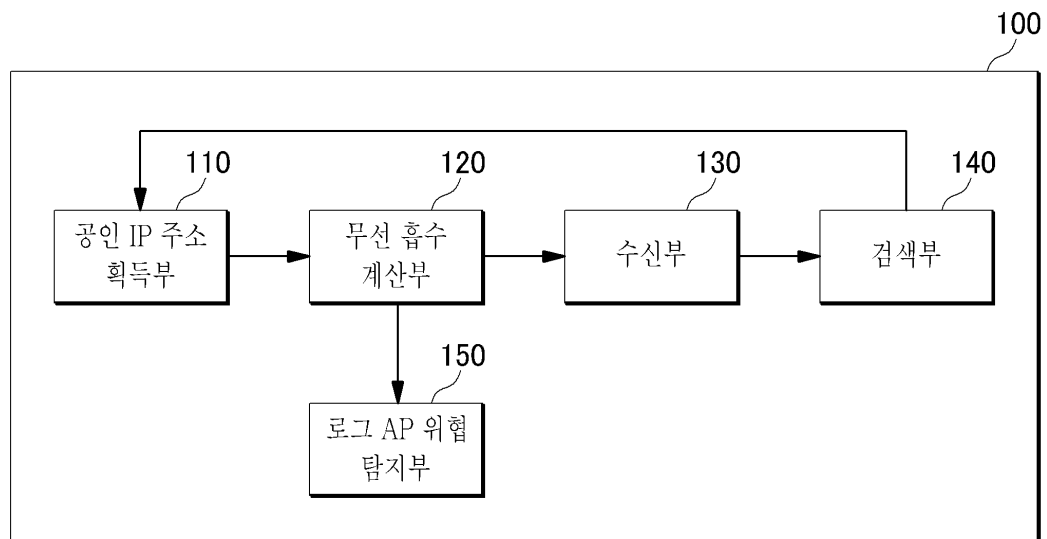
(54) 발명의 명칭 로그 AP 탐지 시스템 및 방법

(57) 요약

본 발명인 로그 AP(Access Point) 탐지 시스템은 사용자 단말과 현재 접속 중인 최초 접속 AP 및 정상 AP의 공인 IP 주소를 획득하는 공인 IP 주소 획득부, 상기 사용자 단말을 기준으로 상기 최초 접속 AP 및 상기 정상 AP의 무선 홉 수를 계산하는 무선 홉 수 계산부, 상기 최초 접속 AP의 무선 홉 수가 1 이상인 경우, 상기 최초 접속

(뒷면에 계속)

대표도 - 도1



AP의SSID, MAC, IP 주소 및 인증방식 정보를 수신하는 수신부, 상기 최초 접속 AP의 연결을 종료한 후, 상기 최초 접속 AP와 동일한 SSID를 가지고, 상기 최초 접속 AP와 상이한 MAC 주소를 가지는 상기 정상 AP를 검색하는 검색부 및 상기 최초 접속 AP의 무선 홉 수와 상기 정상 AP의 무선 홉 수 중 더 많은 무선 홉 수를 가진 AP를 로그 AP의 위협을 받고 있는 것으로 탐지하는 로그 AP 위협 탐지부를 포함하되, 상기 무선 홉 수 계산부는 상기 최초 접속 AP의 공인 IP 주소와 상기 정상 AP의 공인 IP 주소가 동일할 경우, 상기 정상 AP의 무선 홉 수를 계산한다.

이 발명을 지원한 국가연구개발사업

과제고유번호 1415128814

부처명 미래창조과학부

연구관리전문기관 정보통신산업진흥원

연구사업명 정보통신기술인력양성

연구과제명 클라우드 환경의 스마트 기기와 서비스 보안 기술개발 및 연구 인력양성

기 여 율 1/1

주관기관 숭실대학교산학협력단

연구기간 2013.01.01 ~ 2013.12.31

명세서

청구범위

청구항 1

로그 AP(Access Point) 탐지 시스템에 있어서,

사용자 단말과 현재 접속 중인 최초 접속 AP 및 상기 최초 접속 AP와 동일한 SSID를 가지고, 상이한 MAC 주소를 가지는 주변 AP의 공인 IP 주소를 획득하는 공인 IP 주소 획득부,

상기 사용자 단말을 기준으로 상기 최초 접속 AP 및 상기 주변 AP의 무선 홉 수를 계산하는 무선 홉 수 계산부,

상기 최초 접속 AP의 무선 홉 수가 1 이상인 경우, 상기 최초 접속 AP의 SSID, MAC, IP 주소 및 인증방식 정보를 수신하는 수신부,

상기 최초 접속 AP의 연결을 종료한 후, 상기 주변 AP를 검색하는 검색부 및

상기 최초 접속 AP의 무선 홉 수와 상기 주변 AP의 무선 홉 수 중 더 많은 무선 홉 수를 가진 AP를 로그 AP로 탐지하는 로그 AP 위협 탐지부를 포함하되,

상기 무선 홉 수 계산부는 상기 최초 접속 AP의 공인 IP 주소와 상기 주변 AP의 공인 IP 주소가 동일할 경우, 상기 주변 AP의 무선 홉 수를 계산하는 로그 AP 탐지 시스템.

청구항 2

제 1 항에 있어서,

상기 최초 접속 AP의 무선 홉 수가 0인 경우 로그 AP의 위협이 없는 것으로 탐지하는 로그 AP 탐지 시스템.

청구항 3

제 1 항에 있어서,

상기 최초 접속 AP의 공인 IP 주소와 상기 주변 AP의 공인 IP 주소가 상이한 경우 로그 AP의 위협이 없는 것으로 탐지하는 로그 AP 탐지 시스템.

청구항 4

제 1 항에 있어서,

상기 최초 접속 AP 및 상기 주변 AP의 무선 홉 수는 스텐(STUN) 프로토콜 및 인터넷 제어 메시지 프로토콜(ICMP)에 기초하여 계산하는 로그 AP 탐지 시스템.

청구항 5

제 1 항에 있어서,

상기 최초 접속 AP와 동일한 SSID를 가지고, 상기 최초 접속 AP와 상이한 MAC 주소를 가지는 주변 AP는 비콘 프레임 스캐닝에 기초하여 검색하는 로그 AP 탐지 시스템.

청구항 6

로그 AP(Access Point) 탐지 방법에 있어서,

사용자 단말과 접속 중인 최초 접속 AP의 공인 IP 주소를 획득하는 단계,

상기 사용자 단말을 기준으로 상기 최초 접속 AP의 무선 홉 수를 계산하는 단계,

상기 최초 접속 AP의 무선 홉 수가 1 이상인 경우, 상기 최초 접속 AP의 SSID, MAC, IP 주소 및 인증방식 정보를 수신하는 단계,

상기 최초 접속 AP의 연결을 종료하는 단계,

상기 최초 접속 AP와 동일한 SSID를 가지고, 상기 최초 접속 AP와 상이한 MAC 주소를 가지는 주변 AP를 검색하는 단계,

상기 검색된 주변 AP에 각각 접속하여 공인 IP 주소를 획득하는 단계,

상기 최초 접속 AP의 공인 IP 주소와 상기 주변 AP의 공인 IP 주소가 동일할 경우, 상기 사용자 단말을 기준으로 상기 주변 AP의 무선 홉 수를 계산하는 단계 및

상기 최초 접속 AP의 무선 홉 수와 상기 주변 AP의 무선 홉 수 중 더 많은 무선 홉 수를 가진 AP를 로그 AP로 탐지하는 단계를 포함하는 로그 AP 탐지 방법.

청구항 7

제 6 항에 있어서,

상기 최초 접속 AP의 무선 홉 수가 0인 경우 로그 AP의 위협이 없는 것으로 탐지하는 로그 AP 탐지 방법.

청구항 8

제 6 항에 있어서,

상기 최초 접속 AP의 공인 IP 주소와 상기 주변 AP의 공인 IP 주소가 상이한 경우 로그 AP의 위협이 없는 것으로 탐지하는 로그 AP 탐지 방법.

청구항 9

제 6 항에 있어서,

상기 최초 접속 AP와 동일한 SSID를 가지고, 상기 최초 접속 AP와 상이한 MAC 주소를 가지는 주변 AP는 비콘 프레임 스캐닝에 기초하여 검색하는 로그 AP 탐지 방법.

발명의 설명

기술 분야

[0001] 본 발명은 로그 AP 탐지 시스템 및 방법에 관한 것이다.

배경 기술

[0002] 최근 스마트기기를 통한 무선인터넷의 수요가 높아지면서 무선랜 사용이 확산되고 있으며, 그에 따라 무선랜 보안 기술의 요구도 더욱 중요시되고 있다. 무선랜은 공기를 전송매체로 사용하는 서비스의 특성상 많은 취약점이 존재한다. 불특정 다수의 신호 수신이 가능하므로 도청이 가능하고, 무선 전파를 전송하는 무선 장비에 대한 공격이 가능하다.

[0003] 현재 무선랜 보안 위협 중 사용자들의 무선랜 사용 빈도가 높은 공항, 카페 등 공공 무선랜 환경에서 가장 취약한 보안 위협이 바로 로그 AP(Rogue AP)이다. 로그 AP는 공격자가 불법으로 AP를 설치하여 사용자들의 전송 데이터를 수집하는 것으로 로그 AP의 설치 유무나 정확한 위치를 탐지하는 것은 쉽지 않다.

[0004] 한편, 무선랜 환경에서 로그 AP는 두 가지의 형태로 설치될 수 있다. 첫 번째는 일반적인 라우터나 이더넷 스위치와 같이 유선 포트에 로그 AP가 직접 연결되는 형태이며, 이러한 로그 AP는 주로 기업 등과 같이 관리되는 무선랜(Managed WLAN) 환경에서 불법 침입자 및 악의적 내부 사용자에게 의해 설치되어 기업 내부의 중요한 정보 유출을 야기한다. 두 번째는 두 개의 무선 인터페이스를 가진 노트북을 이용하여 무선랜 영역을 악의적으로 확장하여 사용자의 접속을 유도하는 로그 AP로 Evil Twin AP라고 한다. Evil Twin AP는 유선으로 설치된 로그 AP에 비해 어떠한 환경에서든 설치가 가능하므로 사용자에게 더 취약한 공격이 될 수 있다. 이러한 공격은 주로 관리되지 않은 공공 무선랜(Unmanaged WLAN) 환경에서 접속 사용자의 개인정보 유출이 일어난다. 이러한 로그 AP는 정상 AP의 SSID(Service Set Identifier)/MAC 주소를 도용하고, 강한 신호 세기를 가진 AP에 접속하는 무선랜 디바이스 특성을 이용하여 접속을 유도한다. 또한, 접속 사용자에게 다양한 형태의 중간자 공격(Man-In-The-Middle attack)이 가능하기 때문에 사용자의 개인정보 탈취 등의 정보유출이 가능하다.

[0005] 이와 관련하여, 한국공개특허공보 제2012-0129741호(발명의 명칭: 무선 액세스 포인트 장치 및 비인가 무선 랜 노드 탐지 방법)는 특정 통신 사업자 또는 특정인이 사용하는 AP의 SSID와 동일한 SSID를 송출하는 비정상/비인가의 WIFI 디바이스들을 탐지할 수 있는 방법을 개시하고 있다.

[0006] 또한, 한국공개특허공보 제2011-0020072호(발명의 명칭: 무선 네트워크 보안 장치 및 그 방법)는 미리 인가된 AP에 관한 인가 AP를 저장하고, 복수의 AP에 접속하여 AP 정보를 추출하고, 추출된 AP 정보와 인가 AP 정보를 비교하여 비인가 AP 정보를 추출한 후 사용자 단말기로 전송하여 인가된 AP에 접속을 유도하는 기술을 개시하고 있다.

[0007] 다만, 위 선행기술과 더불어 기존의 로그 AP 탐지 기법은 주로 단말 중심의 탐지가 아닌 특정 로컬 영역의 서버 및 탐지를 위한 센서를 통해 로그 AP의 식별과 접속을 제한하고 있다. 이러한 방법은 대규모 네트워크 환경에 적합하지만 비용이 비싸다는 단점이 있고, 일반적인 공항, 커피숍, 도서관 등의 공공환경에서의 탐지는 불가능하므로, 이와 같은 단점이 보완된 단말 중심의 로그 AP 탐지 기법이 필요하다.

발명의 내용

해결하려는 과제

[0008] 본 발명은 진술한 종래 기술의 문제점을 해결하기 위한 것으로서, 본 발명의 일부 실시예는 접속 중인 AP의 무선 홉 수를 계산하고, 정상 AP와 공인 IP 주소를 비교하여 로그 AP의 위협 유무를 탐지할 수 있는 로그 AP 탐지 시스템 및 방법을 제공하는 것을 그 목적으로 한다.

과제의 해결 수단

[0009] 상술한 기술적 과제를 달성하기 위한 기술적 수단으로서, 본 발명의 제 1 측면에 따른 로그 AP(Access Point) 탐지 시스템은 사용자 단말과 현재 접속 중인 최초 접속 AP 및 정상 AP의 공인 IP 주소를 획득하는 공인 IP 주소 획득부, 상기 사용자 단말을 기준으로 상기 최초 접속 AP 및 상기 정상 AP의 무선 홉 수를 계산하는 무선 홉 수 계산부, 상기 최초 접속 AP의 무선 홉 수가 1 이상인 경우, 상기 최초 접속 AP의 SSID, MAC, IP 주소 및 인증 방식 정보를 수신하는 수신부, 상기 최초 접속 AP의 연결을 종료한 후, 상기 최초 접속 AP와 동일한 SSID를 가지고, 상기 최초 접속 AP와 상이한 MAC 주소를 가지는 상기 정상 AP를 검색하는 검색부 및 상기 최초 접속 AP의 무선 홉 수와 상기 정상 AP의 무선 홉 수 중 더 많은 무선 홉 수를 가진 AP를 로그 AP의 위협을 받고 있는 것으로 탐지하는 로그 AP 위협 탐지부를 포함하되, 상기 무선 홉 수 계산부는 상기 최초 접속 AP의 공인 IP 주소와 상기 정상 AP의 공인 IP 주소가 동일할 경우, 상기 정상 AP의 무선 홉 수를 계산한다.

[0010] 또한, 본 발명의 제 2 측면에 따른 로그 AP(Access Point) 탐지 방법은 사용자 단말과 접속 중인 최초 접속 AP의 공인 IP 주소를 획득하는 단계, 상기 사용자 단말을 기준으로 상기 최초 접속 AP의 무선 홉 수를 계산하는 단계, 상기 최초 접속 AP의 무선 홉 수가 1 이상인 경우, 상기 최초 접속 AP의 SSID, MAC, IP 주소 및 인증 방식 정보를 수신하는 단계, 상기 최초 접속 AP의 연결을 종료하는 단계, 상기 최초 접속 AP와 동일한 SSID를 가지고, 상기 최초 접속 AP와 상이한 MAC 주소를 가지는 주변 AP를 검색하는 단계, 상기 검색된 정상 AP에 각각 접속하여 공인 IP 주소를 획득하는 단계, 상기 최초 접속 AP의 공인 IP 주소와 상기 정상 AP의 공인 IP 주소가 동일할 경우, 상기 사용자 단말을 기준으로 상기 정상 AP의 무선 홉 수를 계산하는 단계 및 상기 최초 접속 AP의 무선 홉 수와 상기 정상 AP의 무선 홉 수 중 더 많은 무선 홉 수를 가진 AP를 로그 AP의 위협을 받고 있는 것으로 탐지하는 단계를 포함한다.

발명의 효과

[0011] 전술한 본 발명의 과제 해결 수단에 의하면, 이동 가능한 사용자 단말에서 로그 AP의 위협 유무를 탐지할 수 있다.

[0012] 또한, 기존의 센서를 통해 수행하던 로그 AP의 식별 및 접속 제한을 이동 가능한 사용자 단말에서 수행할 수 있어 비용을 절감할 수 있으며, 개인 단말을 이용함으로써 시스템 구축이 용이하다.

[0013] 또한, 특정 서버를 이용한 AP의 블랙리스트 또는 화이트리스트를 이용하지 않으므로 관리가 용이하다.

도면의 간단한 설명

[0014] 도 1은 본 발명의 일 실시예에 따른 로그 AP 탐지 시스템의 블록도이다.

도 2는 본 발명에 따른 무선 홉 수 계산부에서의 무선 홉 수 계산 방법을 설명하기 위한 도면이다.

도 3은 로그 AP를 탐지하기 위한 과정을 도시한 도면이다.

도 4는 본 발명의 일 실시예에 따른 로그 AP 탐지 방법의 순서도이다.

도 5 내지 도 6은 본 발명에 따른 로그 AP 탐지 시스템 및 방법을 테스트한 결과를 도시한 도면이다.

발명을 실시하기 위한 구체적인 내용

- [0015] 아래에서는 첨부한 도면을 참조하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 본 발명의 실시예를 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.
- [0016] 명세서 전체에서, 어떤 부분이 다른 부분과 "연결"되어 있다고 할 때, 이는 "직접적으로 연결"되어 있는 경우뿐 아니라, 그 중간에 다른 소자를 사이에 두고 "전기적으로 연결"되어 있는 경우도 포함한다. 또한 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. 본원 명세서 전체에서 사용되는 정도의 용어 "~(하는) 단계" 또는 "~의 단계"는 "~를 위한 단계"를 의미하지 않는다.
- [0017] 도 1은 본 발명의 일 실시예에 따른 로그 AP 탐지 시스템(100)의 블록도이다.
- [0018] 본 발명의 일 실시예에 따른 로그 AP 탐지 시스템은 공인 IP 주소 획득부(110), 무선 홉 수 계산부(120), 수신부(130), 검색부(140) 및 로그 AP 위협 탐지부(150)를 포함한다.
- [0019] 참고로, 본 발명의 실시예에 따른 도 1에 도시된 구성 요소들은 소프트웨어 또는 FPGA(Field Programmable Gate Array) 또는 ASIC(Application Specific Integrated Circuit)와 같은 하드웨어 구성 요소를 의미하며, 소정의 역할들을 수행한다.
- [0020] 그렇지만 '구성 요소들'은 소프트웨어 또는 하드웨어에 한정되는 의미는 아니며, 각 구성 요소는 어드레싱할 수 있는 저장 매체에 있도록 구성될 수도 있고 하나 또는 그 이상의 프로세서들을 재생시키도록 구성될 수도 있다.
- [0021] 따라서, 일 예로서 구성 요소는 소프트웨어 구성 요소들, 객체지향 소프트웨어 구성 요소들, 클래스 구성 요소들 및 태스크 구성 요소들과 같은 구성 요소들과, 프로세스들, 함수들, 속성들, 프로시저들, 서브루틴들, 프로그램 코드의 세그먼트들, 드라이버들, 펌웨어, 마이크로 코드, 회로, 데이터, 데이터베이스, 데이터 구조들, 테이블들, 어레이들 및 변수들을 포함한다.
- [0022] 구성 요소들과 해당 구성 요소들 안에서 제공되는 기능은 더 작은 수의 구성 요소들로 결합되거나 추가적인 구성 요소들로 더 분리될 수 있다.
- [0023] 공인 IP 주소 획득부(110)는 사용자 단말과 현재 접속 중인 최초 접속 AP 및 정상 AP의 공인 IP 주소를 획득한다. 먼저, 공인 IP 주소 획득부(110)는 사용자 단말과 현재 접속 중인 최초 접속 AP의 공인 IP 주소를 획득한다. 그리고 아래에서 설명하는 바와 같이, 검색부(140)에서 검색된 정상 AP의 공인 IP 주소를 획득한다. 이때, 최초 접속 AP의 공인 IP 주소와 정상 AP의 공인 IP 주소가 상이한 경우 로그 AP의 위협이 없는 것으로 탐지할 수 있다.
- [0024] 무선 홉 수 계산부(120)는 사용자 단말을 기준으로 최초 접속 AP 및 정상 AP의 무선 홉 수를 계산한다. 이때 최초 접속 AP 및 정상 AP의 무선 홉 수는 스턴(STUN) 프로토콜 및 인터넷 제어 메시지 프로토콜(ICMP)에 기초하여 계산할 수 있다.
- [0025] 무선 홉 수 계산부(120)는 공인 IP 주소 획득부(110)에서 최초 접속 AP의 공인 IP 주소를 획득한 다음 최초 접속 AP의 무선 홉 수를 계산한다. 그리고, 검색부(140)에서 검색된 정상 AP의 무선 홉 수를 계산하며, 이에 기초하여 로그 AP의 위협 유무를 탐지할 수 있다. 이때, 무선 홉 수 계산부(120)는 최초 접속 AP의 공인 IP 주소와 정상 AP의 공인 IP 주소가 동일할 경우, 정상 AP의 무선 홉 수를 계산한다.
- [0026] 한편, 무선 홉 수 계산부(120)에서 계산한 최초 접속 AP의 무선 홉 수가 0일 경우 로그 AP의 위협이 없는 것으로 탐지할 수 있다. 이하에서는 도 2를 참조하여 무선 홉 수 계산부(120)에서의 무선 홉 수를 계산하는 방법을 설명하도록 한다.

- [0027] 도 2 는 본 발명에 따른 무선 홉 수 계산부(120)에서의 무선 홉 수 계산 방법을 설명하기 위한 도면이다.
- [0028] 사용자 단말은 표준에 정의된 스텐(STUN, Simple Traversal of User UDP through NATs) 프로토콜 및 인터넷 제어 메시지 프로토콜(ICMP, Internet Control Message Protocol)을 이용하여 사용자 단말의 무선구간 홉 수를 검사하고 불필요한 무선구간을 포함하는 AP를 찾는다. 이때 공공 스텐 서버(Public STUN server)는 서버에 가장 근접한 NAT 디바이스의 공인 IP 주소를 사용자 단말에 제공하는 특성을 가지고 있다. 이는 일반적인 무선랜 환경에서 정상 AP가 할당 받은 공인 IP 주소에 해당되며, 그렇지 않을 경우 NAT 기능을 가지고 있는 로그 AP의 IP 주소를 알려준다.
- [0029] 사용자 단말은 다음 단계로 ICMP 패킷의 TTL(Time-To-Live) 값을 변화하여 단말로부터 연결되어 있는 AP, 게이트웨이, 라우터 등의 로컬 IP 정보를 얻을 수 있다. 이 정보는 윈도우 환경에서 Tracert, 리눅스에서는 Traceroute 명령어를 통해 얻을 수 있으며, TTL 값을 1부터 순차적으로 증가시켜 AP의 디폴트 게이트웨이 IP와 AP가 포함되는 서브넷 영역의 게이트웨이/라우터 IP 등을 알 수 있다.
- [0030] 스텐/ICMP 프로토콜을 이용하여 얻은 IP 정보를 통해 사용자 단말은 현재 접속 중인 AP의 무선 홉 수를 계산할 수 있다. 스텐 응답 패킷으로부터 얻은 공인 IP 주소와 ICMP를 통해 얻은 IP 주소를 비교하고, 각 IP 주소에 대한 서브넷 마스크를 적용하면 두 IP가 동일한 값을 가진다. 이 경우 ICMP의 TTL 값을 통하여 무선 홉 수를 계산할 수 있다. 이때, TTL 값은 현재 무선 홉 수보다 1이 큰 값이므로 현재의 무선 홉 수 $WH_n = TTL - 1$ 이 된다. 아래의 알고리즘은 무선 홉 수를 탐지하기 위한 수도코드이다.
- [0031] Connect and associate with AP_n
- [0032] Get a Public IP address of AP_n using STUN protocol
- [0033] IP_n = Public IP address of AP_n
- [0034] for i=1 do
- [0035] Traceroute()=Send the ICMP packet increasing TTL=i
- [0036] GIP_i = Local gateway address of Subnet $\otimes$ SubnetMask
- [0037] PIP_n = $IP_n \otimes$ SubnetMask
- [0038] if $GIP_i == PIP_n$ then
- [0039] Compute Number of Wireless Hops WH_n
- [0040] $WH_n = TTL - 1$
- [0041] end if
- [0042] end for
- [0043] 무선 홉 수 탐지기법을 이용하면 무선랜 환경에 관계없이 빠르고 정확하게 로그 AP를 탐지할 수 있다는 장점이 있다. 기존에 제안된 기법들에 비해, 모든 AP에 대한 주기적인 모니터링이 요구되지 않기 때문에 스마트 폰과 같은 모바일 단말에 적용이 용이하다.
- [0044] 일반적으로 로그 AP는 사용자의 접속을 유도하고 원활한 무선 네트워크 환경을 제공하기 위해서 DHCP(Dynamic Host Configuration Protocol)와 NAT 기능을 가지고 있다. 따라서, 로그 AP에 접속한 단말이라면 정상 AP가 NAT 기능을 포함하지 않은 경우에도 무선 홉 수 탐지에 의한 WH_n 값은 1 이상이 된다.
- [0045] 또한, 학교, 회사, 통신서비스 제공 사업자와 같은 관리되는 무선 네트워크 환경에서의 접속 단말은 공인 IP 주소를 바로 할당받게 되어 AP는 NAT 기능을 수행하지 않으며, 유선구간을 무선구간으로 전이하는 기능만을 수행하는 경우가 있다. 이 경우, 단말이 로그 AP에 접속하였음에도 NAT 디바이스의 개수를 1로 인식하고, 무선 홉 수를 1로 판단하게 된다.
- [0046] 이와 더불어, AP를 제외한 유선망 내부에 NAT 스위치와 같은 또 다른 NAT 디바이스가 존재할 경우, 무선 홉 수

가 변하게 되는 문제가 생기므로 정상 AP에 접속했음에도 불구하고 로그 AP로 판단하는 오류가 발생할 수도 있다.

[0047] 따라서, 본 발명에 따른 로그 AP 탐지 시스템(100)은 현재 접속 AP의 무선 홉 수 WH_n 이 0보다 큰 경우, 로그 AP의 위협이 있는지 여부를 정확하게 판단할 수 있다.

[0048] 다시 도 1을 참조하면, 수신부(130)는 최초 접속 AP의 무선 홉 수가 1 이상인 경우, 최초 접속 AP의 SSID, MAC, IP 주소 및 인증방식 정보를 수신한다. 위에서 설명한 바와 같이, 무선 홉 수가 0인 경우에는 로그 AP의 위협이 없는 것으로 판단하기 때문에 무선 홉 수가 1 이상인 경우에만 최초 접속 AP의 SSID, MAC, IP 주소 및 인증방식 정보를 수신한다. 이와 같은 정보를 이용하여 아래에서 설명할 검색부(140)에서 최초 접속 AP와 동일한 SSID를 가지고 상이한 MAC 주소를 가지는 정상 AP를 검색하게 된다.

[0049] 검색부(140)는 최초 접속 AP의 연결을 종료한 후, 최초 접속 AP와 동일한 SSID를 가지고, 최초 접속 AP와 상이한 MAC 주소를 가지는 정상 AP를 검색한다. 이때, 최초 접속 AP와 동일한 SSID를 가지고, 최초 접속 AP와 상이한 MAC 주소를 가지는 정상 AP는 비콘 프레임 스캐닝에 기초하여 검색할 수 있다.

[0050] 로그 AP 위협 탐지부(150)는 최초 접속 AP의 무선 홉 수와 정상 AP의 무선 홉 수 중 더 많은 무선 홉 수를 가진 AP를 로그 AP의 위협을 받고 있는 것으로 탐지한다. 이하에서는 도 3을 참조하여 로그 AP 탐지 과정을 설명하도록 한다.

[0051] 도 3은 로그 AP를 탐지하기 위한 과정을 도시한 도면이다.

[0052] 최초에 로그 AP(AP_1)에 접속한 단말은 무선 홉 수 계산(WH_1)을 수행한 후, WH_1 이 0보다 큰 경우, 현재 접속 중인 최초 접속 AP와의 접속을 끊고, 주변의 정상 AP(AP_2 , AP_3)들에 접속을 시도한다. 이 과정에서 사용자 단말이 정상 AP(AP_2 , AP_3)를 찾는 과정은 사용자 단말 주변에 로그 AP(AP_1)와 동일한 SSID를 사용하는 AP_{n+1} 에 모두 접속을 시도하고, 각 AP에 이전 과정과 동일하게 무선 홉 수 계산부(110)를 통하여 무선 홉 수를 계산한다.

[0053] 주변의 정상 AP(AP_2 , AP_3)인 AP_{n+1} 에 대한 공인 IP 주소인 IP_{n+1} 값을 얻은 후 검색부(140)는 최초 접속 AP와 동일한 공인 IP 주소를 가지는 정상 AP를 검색한다. 도 3에서 동일한 공인 IP 주소를 가지는 두 AP 중 하나는 로그 AP, 나머지 하나는 정상 AP가 된다. 두 개의 AP 중 어떤 AP가 로그 AP인지를 판단하기 어렵기 때문에 로그 AP 위협 탐지부(150)는 각 AP로부터 수행한 무선 홉 수를 비교하여 로그 AP의 위협 여부를 정확하게 탐지할 수 있다. 아래의 알고리즘은 무선 홉 수 계산 과정 후 로그 AP 위협을 탐지하기 위한 수도코드이다.

[0054] Connect and associate with AP_n

[0055] Compute WH_n of AP_n (through Algorithm 1)

[0056] if ($WH_n > 0$) then

[0057] for $n=1$ do

[0058] $n=n+1$

[0059] Algorithm 1

[0060] if ($IP_1 == IP_n$) then

[0061] if ($WH_1 > WH_n$) then

[0062] AP_1 is an Evil Twin AP

[0063] else

[0064] AP_n is an Evil Twin AP

[0065] end if

[0066] else if then

- [0067] Doesn' t exist Evil Twin AP
- [0068] end if
- [0069] end for
- [0070] else if then
- [0071] Doesn' t exist Evil Twin AP
- [0072] end if
- [0073] 위와 같은 알고리즘을 이용하여 로그 AP 위협 탐지부(150)는 더 많은 무선 홉 수를 가지는 AP를 로그 AP의 위협이 있는 것으로 탐지하고, 더 적은 무선 홉 수를 가지는 AP를 정상 AP로 판단한다.
- [0074] 도 4는 본 발명의 일 실시예에 따른 로그 AP 탐지 방법의 순서도이다.
- [0075] 본 발명에 따른 로그 AP 탐지 방법은 먼저, 사용자 단말과 접속 중인 최초 AP의 공인 IP 주소를 획득한다(S410).
- [0076] 다음으로 사용자 단말을 기준으로 최초 접속중인 AP의 무선 홉 수를 계산한다(S420). 이때, 최초 접속 AP의 무선 홉 수 및 아래에서 설명할 정상 AP의 무선 홉 수는 스텐(STUN) 프로토콜 및 인터넷 제어 메시지 프로토콜(ICMP)에 기초하여 계산할 수 있다.
- [0077] 다음으로, 최초 접속 AP의 무선 홉 수가 1 이상인 경우(S430), 최초 접속 AP의 SSID, MAC, IP 주소 및 인증방식 정보를 수신한다(S440). 이때, 최초 접속 AP의 무선 홉 수가 0인 경우 로그 AP의 위협이 없는 것으로 탐지할 수 있다. 한편, 무선 홉 수를 계산하는 방법은 도 2에서 자세히 설명하였으므로 이하에서는 생략하도록 한다.
- [0078] 다음으로, 최초 접속 AP의 연결을 종료하고(S450), 최초 접속 AP와 동일한 SSID를 가지고, 최초 접속 AP와 상이한 MAC 주소를 가지는 정상 AP를 검색한 후(S460), 검색된 정상 AP에 각각 접속하여 공인 IP 주소를 획득한다(S470). 이때, 최초 접속 AP와 동일한 SSID를 가지고, 상이한 MAC 주소를 가지는 정상 AP는 비콘 프레임 스캐닝에 기초하여 검색할 수 있다.
- [0079] 다음으로, 최초 접속 AP의 공인 IP 주소와 정상 AP의 공인 IP 주소가 동일할 경우, 사용자 단말을 기준으로 정상 AP의 무선 홉 수를 계산한다(S480). 이때, 최초 접속 AP의 공인 IP 주소와 정상 AP의 공인 IP 주소가 상이한 경우 로그 AP의 위협이 없는 것으로 탐지할 수 있다.
- [0080] 다음으로, 최초 접속 AP의 무선 홉 수와 정상 AP의 무선 홉 수 중 더 많은 무선 홉 수를 가진 AP를 로그 AP의 위협을 받고 있는 것으로 탐지한다(S490).
- [0081] 이와 같은, 로그 AP 탐지 시스템 및 방법을 적용하면, 이동 가능한 사용자 단말에서 로그 AP의 위협 유무를 탐지할 수 있으며, AP의 블랙 리스트 또는 화이트리스트를 이용하고 있지 않아, 관리가 용이하다.
- [0082] 또한, 기존의 센서를 통해 수행하던 로그 AP의 식별 및 접속 제한을 이동 가능한 사용자 단말에서 수행할 수 있어 비용을 절감할 수 있으며, 개인 단말을 이용하고 있어 시스템 구축이 용이하다.
- [0083] 한편, 본 발명에 따른 로그 AP 탐지 시스템(100) 및 방법에서의 사용자 단말은 네트워크를 통해 접속할 수 있는 컴퓨터나 휴대용 단말기로 구현될 수 있다. 여기서, 컴퓨터는 예를 들어, 웹 브라우저(WEB Browser)가 탑재된 노트북, 데스크톱(desktop), 랩톱(laptop) 등을 포함하고, 휴대용 단말기는 예를 들어, 휴대성과 이동성이 보장되는 무선 통신 장치로서, PCS(Personal Communication System), GSM(Global System for Mobile communications), PDC(Personal Digital Cellular), PHS(Personal Handyphone System), PDA(Personal Digital Assistant), IMT(International Mobile Telecommunication)-2000, CDMA(Code Division Multiple Access)-2000, W-CDMA(W-Code Division Multiple Access), Wibro(Wireless Broadband Internet) 단말 등과 같은 모든 종류의 핸드헬드(Handheld) 기반의 무선 통신 장치를 포함할 수 있다.
- [0084] 도 5 내지 도 6은 본 발명에 따른 로그 AP 탐지 시스템(100) 및 방법을 테스트한 결과를 도시한 도면이다. 이와 같은 테스트 결과를 도 3을 함께 참조하여 설명하도록 한다.
- [0085] 도 5는 로그 AP의 위협이 없는 경우의 탐지 결과를 도시한 도면이다.
- [0086] 사용자 단말은 초기에 강한 신호 세기의 AP(AP₃)에 접속한 후, 무선 홉 수를 계산하고, 동일한 SSID를 가지는

AP₂에 접속하여 공인 IP 주소 획득 및 무선 홉 수를 계산한다.

[0087] 테스트 결과, 사용자 단말에는 현재 접속 중인 AP로부터 획득한 공인 IP 주소와 AP의 MAC, 공인 IP 주소 등의 정보가 표시되고, 무선 홉 수 계산 결과도 함께 표시된다. 또한, SSID를 동일하게 사용하는 주변의 AP 정보를 함께 제공받는다. 현재 무선 홉 수가 1이므로 주변 AP를 검색한 후, 획득한 공인 IP 주소인 220.70.2.157이 AP의 공인 IP 주소인 220.70.2.37과 다르기 때문에 로그 AP의 위협이 없는 것으로 판단하게 된다.

[0088] 도 6은 로그 AP의 위협이 있는 경우의 탐지 결과를 도시한 도면이다.

[0089] 정상 AP(AP₂)보다 강한 신호를 전파해 무선랜 사용자의 접속을 유도한 로그 AP에 접속한 사용자 단말은 로그 AP로부터 로컬 IP 주소인 192.168.0.46을 할당받았다. 로그 AP 위협 여부 탐지를 위해 무선 홉 수 검사과정을 수행하여, 현재 단말이 가지는 무선 홉 수(WH_n)가 2임을 확인할 수 있다. 또한, 접속한 AP의 공인 IP 주소가 220.70.2.157임을 알 수 있다. 이때, 무선 홉 수(WH_n)가 0보다 큰 값을 가지므로, 사용자 단말은 주변 AP를 스캐닝하여, 동일한 SSID를 사용하며, MAC 주소가 상이한 다른 AP를 검색한다. 이 과정은 정상 AP를 탐지하기 위한 과정이고, 정상 AP로 검색된 AP₂과 AP₃에 각각 접속하는 과정을 수행한다.

[0090] AP₂에 접속한 단말은 접속한 AP의 공인 IP 주소인 220.70.2.157을 얻고, 최초로 접속한 로그 AP로부터 얻은 공인 IP 주소인 220.70.2.157과 같음을 확인할 수 있다. 공인 IP 주소가 같다는 것은 두 AP 중 로그 AP가 존재한다는 것이고, 어떤 AP가 로그 AP인지 확인하기 위하여 현재 접속한 AP₂에 대해서도 무선 홉 수 검사를 수행한다. 그 다음, 로그 AP와 정상 AP인 AP₂으로부터 수행한 홉 수를 비교하여 더 많은 무선 홉 수를 가지는 AP를 로그 AP로 판단한다. 마찬가지로 또 다른 AP(AP₃)에도 접속하여 공인 IP 주소인 220.70.2.37을 얻지만, 동일한 공인 IP 주소가 아니므로 또 다른 정상 AP로 판단한다. 도 8에 도시된 바와 같이, 로그 AP 공격 위협을 안드로이드 토스트 형태로 경고를 할 수 있으며, 로그 AP의 MAC 주소를 파악하여 위협 여부를 정확하게 탐지할 수 있다.

[0091] 본 발명의 일 실시예는 컴퓨터에 의해 실행되는 프로그램 모듈과 같은 컴퓨터에 의해 실행 가능한 명령어를 포함하는 기록 매체의 형태로도 구현될 수 있다. 컴퓨터 판독 가능 매체는 컴퓨터에 의해 액세스될 수 있는 임의의 가용 매체일 수 있고, 휘발성 및 비휘발성 매체, 분리형 및 비분리형 매체를 모두 포함한다. 또한, 컴퓨터 판독가능 매체는 컴퓨터 저장 매체 및 통신 매체를 모두 포함할 수 있다. 컴퓨터 저장 매체는 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터와 같은 정보의 저장을 위한 임의의 방법 또는 기술로 구현된 휘발성 및 비휘발성, 분리형 및 비분리형 매체를 모두 포함한다. 통신 매체는 전형적으로 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈, 또는 반송파와 같은 변조된 데이터 신호의 기타 데이터, 또는 기타 전송 매커니즘을 포함하며, 임의의 정보 전달 매체를 포함한다.

[0092] 본 발명의 방법 및 시스템은 특정 실시예와 관련하여 설명되었지만, 그것들의 구성 요소 또는 동작의 일부 또는 전부는 범용 하드웨어 아키텍처를 갖는 컴퓨터 시스템을 사용하여 구현될 수 있다.

[0093] 전술한 본 발명의 설명은 예시를 위한 것이며, 본 발명이 속하는 기술분야의 통상의 지식을 가진 자는 본 발명의 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 쉽게 변형이 가능하다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적이 아닌 것으로 이해해야만 한다. 예를 들어, 단일형으로 설명되어 있는 각 구성 요소는 분산되어 실시될 수도 있으며, 마찬가지로 분산된 것으로 설명되어 있는 구성 요소들도 결합된 형태로 실시될 수 있다.

[0094] 본 발명의 범위는 상기 상세한 설명보다는 후술하는 특허청구범위에 의하여 나타내어지며, 특허청구범위의 의미 및 범위 그리고 그 균등 개념으로부터 도출되는 모든 변경 또는 변형된 형태가 본 발명의 범위에 포함되는 것으로 해석되어야 한다.

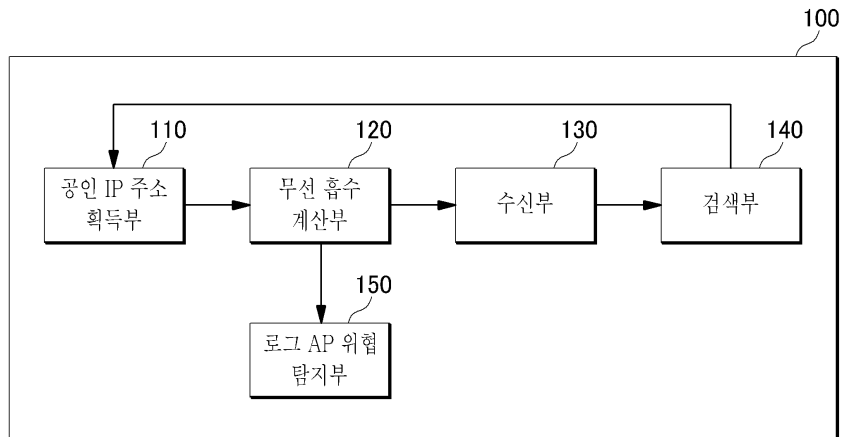
부호의 설명

[0095]

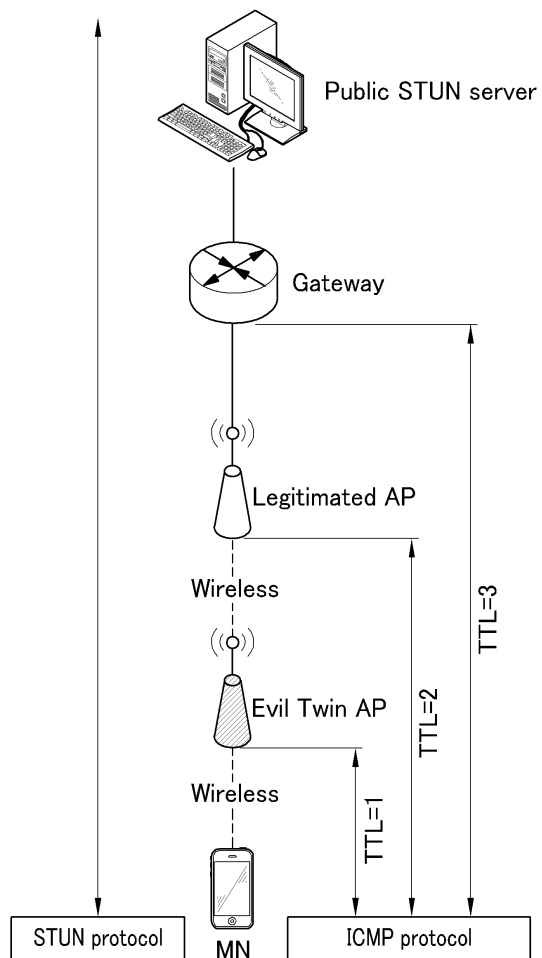
100: 로그 AP 탐지 시스템	110: 공인 IP 주소 획득부
120: 무선 홉 수 계산부	130: 수신부
140: 검색부	150: 로그 AP 위협 탐지부

도면

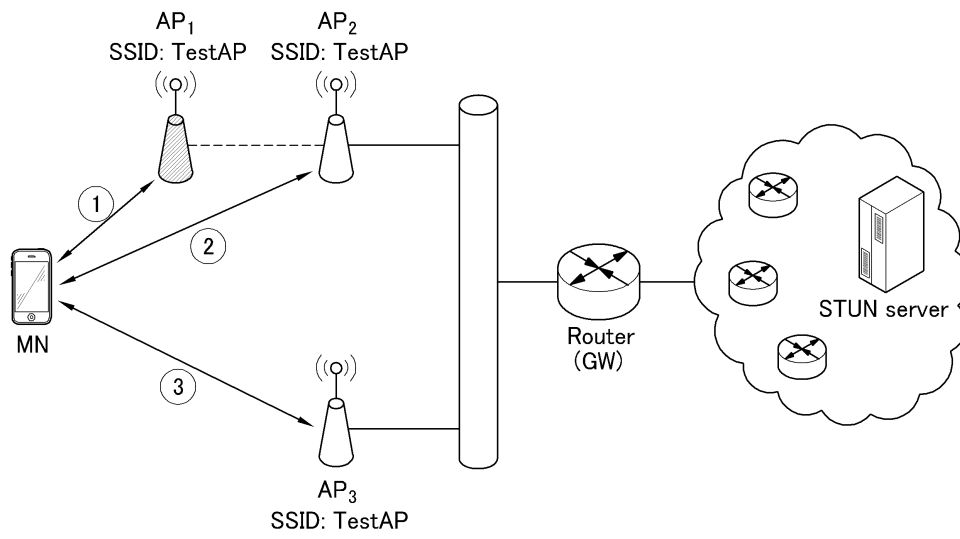
도면1



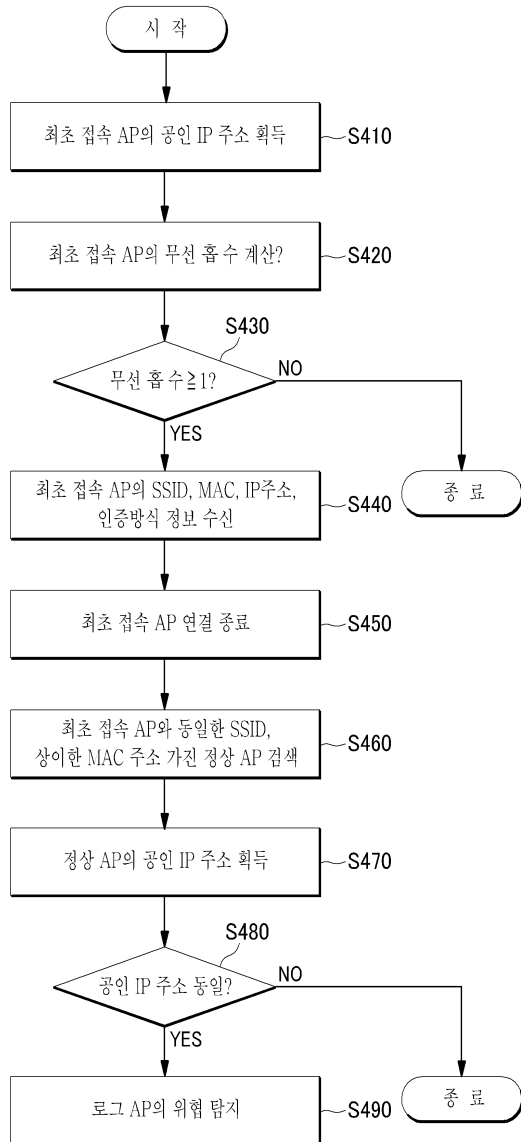
도면2



도면3



도면4



도면5



도면6

