(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl.
H04L 12/28 (2006.01)
H04L 12/22 (2006.01)
H04L 9/32 (2006.01)
H04L 12/56 (2006.01)

(11) 공개번호 10-2007-0054067
(43) 공개일자 2007년05월28일

(21) 출원번호 10-2005-0112061
(22) 출원일자 2005년11월22일
심사청구일자 없음

(71) 출원인 충남대학교산학협력단
대전광역시 유성구 궁동 220번지 충남대학교
이형우
경기도 용인시 기흥구 중동 성산마을서해그랑블 3101동 501호
최창원
서울 구로구 신도림동 645 동아3차아파트 307-1701
한신대학교 산학협력단
경기 오산시 양산동 한신대학교내

(72) 발명자 이형우
경기도 용인시 기흥구 중동 성산마을서해그랑블 3101동 501호
최창원
서울 구로구 신도림동 645 동아3차아파트 307-1701

(74) 대리인 이선우

전체 청구항 수 : 총 8 항

(54) 무선 액세스 포인트 장치 및 그를 이용한 네트워크 트래픽침입탐지 및 차단방법

(57) 요약

본 발명은 무선 액세스 포인트 장치에서 무선으로 입력되는 트래픽들에 대한 침입을 탐지하고 차단할 수 있도록 함으로써 무선 네트워크에서의 보안 서비스의 질을 향상시킬 수 있는 무선 액세스 포인트 장치 및 그를 이용한 네트워크 트래픽 침입탐지 및 차단방법에 관한 것이다

본 발명에 따른 무선 액세스 장치는 사용자와 무선으로 연동하여 무선 신호를 송수신 중계하고 공격자부터의 무선 네트워크 트래픽 신호를 탐지 및 차단하는 무선 액세스 포인트 장치(100)에 있어서, 네트워크 인터페이스 카드(101)를 포함하고 공격자의 공격 트래픽을 접수하고 탐지하는 네트워크 모니터링 모듈(112) 및 공격자에게 경고메시지를 전송하도록 제어하는 경고 인터페이스 모듈(116)을 포함하는 네트워크 모듈(110)과; 상기 네트워크 모니터링 모듈(112)로부터 전송된 공격 트래픽을 필터링하는 패킷 분석모듈(122) 및 상기 패킷 분석모듈(122)로부터의 필터링된 패킷이 네트워크 공격패킷인지를 규칙 DB/서명모듈(126)과 연동하여 판단하여 그 결과를 상기 패킷분석모듈(122) 및 상기 경고 인터페이스 모듈

(116)에 전송하는 침입탐지모듈(124)을 포함하는 분석 및 보안모듈(120);로 이루어지는 것을 특징으로 하여 해당 공격트래픽을 필터링하여 탐지하고 일차적으로 경고메시지를 전송하며 이차적으로는 해당 수신자의 접속을 끊는 신호를 전송함으로써 확실하게 무선 네트워크 트래픽 침입을 탐지하고 차단할 수 있는 효과가 있다.

대표도

도 9

특허청구의 범위

청구항 1.

사용자와 무선으로 연동하여 무선 신호를 송수신 중계하고 공격자부터의 무선 네트워크 트래픽 신호를 탐지 및 차단하는 무선 액세스 포인트 장치(100)에 있어서,

네트워크 인터페이스 카드(101)를 포함하고 공격자의 공격 트래픽을 접수하고 탐지하는 네트워크 모니터링 모듈(114) 및 공격자에게 경고메시지를 전송하도록 제어하는 경고 인터페이스 모듈(116)을 포함하는 네트워크 모듈(110)과;

상기 네트워크 모니터링 모듈(114)로부터 전송된 공격 트래픽을 필터링하는 패킷 분석모듈(122) 및 상기 패킷 분석모듈(122)로부터의 필터링된 패킷이 네트워크 공격패킷인지를 규칙 DB/서명모듈(126)과 연동하여 판단하여 그 결과를 상기 패킷분석모듈(122) 및 상기 경고 인터페이스 모듈(116)에 전송하는 침입탐지모듈(124)을 포함하는 분석 및 보안모듈(120);로 이루어지는 것을 특징으로 하는 무선 액세스 포인트 장치(100).

청구항 2.

제 1 항에 있어서, 상기 네트워크 모듈(110)은 802.11 b/g 패킷을 채널 호핑(channel hopping)하며, 환경설정 정보를 동기화시키고, level 2 무선 트래픽을 모니터링하며, probe request, probe response, beacon frame을 전송하는 상기 채널 호핑 모듈(112)을 더 포함하여 이루어지는 것을 특징으로 하는 무선 액세스 포인트 장치(100).

청구항 3.

제 1 항에 있어서, 상기 네트워크 모니터링 모듈(114)은 수동적(passive) 형태의 sniffing을 수행하고 모든 네트워크 패킷을 탐지하는 monitoring mode이고, 상기 채널 호핑 모듈(112)을 통해 수집된 802.11 b/g 패킷을 수집하고, SSID beacon frame을 전송하지 않는 숨겨진 AP 네트워크는 클라이언트의 AP 접속시 SSID를 모니터링 하여 탐지하는 것을 특징으로 하는 무선 액세스 포인트 장치(100).

청구항 4.

제 1 항에 있어서, 상기 경고 인터페이스 모듈(116)은 네트워크 공격 패킷 전송자의 접속을 끊는 deauth 신호를 전송하는 것을 특징으로 하는 무선 액세스 포인트 장치(100).

청구항 5.

제 1 항에 있어서, 상기 침입 탐지 모듈(124)은 상기 네트워크 모니터링 모듈(114)로부터 전달된 AP 정보를 사전에 관리자에 의해서 입력된 인가된 AP 리스트와 비교를 수행하는 불법 AP(Rogue AP) 탐지 모듈(124-1)과, sequence 번호를 추적하여 MAC spoofing 공격을 탐지하고 DoS의 deauth flooding 공격은 브로드캐스트 disassociate/deauthenticate

frame 발생 여부를 확인하여 탐지하고, Stumbler 공격 탐지를 위해서 stumbler 별로 존재하는 fingerprint를 패킷과 비교하여 탐지하고, Man-in-the-middle 공격 탐지는 AP의 channel 변경 여부를 확인하여 탐지하는 Spoof/DoS/Stumbler/MITM 탐지 모듈(124-2)를 포함하여 이루어진 것을 특징으로 하는 무선 액세스 포인트 장치(100).

청구항 6.

무선 액세스 포인트 장치(100)를 통해 무선 네트워크 공격 트래픽을 탐지하고 차단하는 무선 액세스 포인트 장치(100)를 이용한 무선 네트워크 침입탐지 및 차단방법에 있어서,

접수된 무선 트래픽을 분석하고 전송하는 단계와;

전송된 무선 트래픽을 필터링하는 단계와;

필터링된 패킷이 네트워크 공격패킷 인지를 규칙 DB/서명 모듈(126)과 연동하여 판단하는 단계와;

상기 판단결과, 필터링된 패킷이 네트워크 공격 패킷인 경우에는 그 결과를 경고 메시지로 공격자에게 전달하는 단계로 이루어진 것을 특징으로 하는 무선 액세스 포인트 장치(100)를 이용한 무선 네트워크 침입탐지 및 차단방법.

청구항 7.

제 6 항에 있어서,

상기 경고메시지 전달단계 이후에 수신자가 확인을 하였는지를 판단하는 단계와;

만약, 수신자가 확인한 경우에는 해당 데이터를 버리는 단계;를 더 포함하여 이루어진 것을 특징으로 하는 무선 액세스 포인트 장치(100)를 이용한 무선 네트워크 침입탐지 및 차단방법.

청구항 8.

제 6 항에 있어서, 만약 필터링된 패킷이 네트워크 공격 패킷인 경우에, 경고메시지 전송시 수신자의 접속을 끊는 deauth 데이터를 전송하는 것을 특징으로 하는 무선 액세스 포인트 장치(100)를 이용한 무선 네트워크 침입탐지 및 차단방법.

명세서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 무선 액세스 포인트 장치 및 그를 이용한 네트워크 트래픽 침입탐지 및 차단방법에 관한 것으로, 더욱 상세하게는 무선 액세스 포인트 장치에서 무선으로 입력되는 트래픽들에 대한 침입을 필터링하여 탐지하고 차단할 수 있도록 함으로써 무선 네트워크에서의 보안 서비스의 질을 향상시킬 수 있는 무선 액세스 포인트 장치 및 그를 이용한 네트워크 트래픽 침입탐지 및 차단방법에 관한 것이다.

일반적으로 무선 인터넷 통신을 위하여 액세스 포인트(AP:Access Point) 장치라는 장비를 설치하여 사용하고 있다. 그러나, 현재까지 개발된 엑세스 포인트 장치는 무선 트래픽에 대한 전송, 네트워크 지원 기능만을 제공하거나 또한 추가적인 기능 등이 포함된 것으로는 패킷에 대한 필터링 기능등을 수행하는 제품이 있다.

현재까지 개발된 종래의 엑세스 포인트 장치 중, 3Com Access Point 사양을 살펴보면,

* 사용자 지원: 최대 253명까지 동시 접속 가능,

* 준수 표준: Wi-Fi 인증, IEEE 802.11g, IEEE 802.11a (업그레이드 키트 이용),

* 데이터 전송속도: 54, 48, 36, 24, 18, 11, 9, 5.5, 2, 1 Mbps,

* 주파수 대역: 2.4 GHz,

* 무선 매체: OFDM 및 DSSS (802.11b와의 역호환을 위한 Barker 코딩 및 CCK 포함),

* 매체 접근 통신규약: CSMA/CA, 운영 채널: 1 - 11 (미국 및 캐나다), 1 - 13 (전세계; 사용 채널 범위는 현지 법규에 의거하여 결정됨.),

* 작동 범위: 최대 100미터 (328피트), 송수신,

* 전송전력 설정: 17 dBm (비트율에 따라 결정됨),

* 전력 소비: 평균 7.1W, 최대 8.4W,

* 수신감도: 1 Mbps: -96 dBm,

* 2 Mbps: -94 dBm,

* 5.5 Mbps: -92 dBm,

* 11 Mbps: -88 dBm,

* 12 Mbps: -86 dBm,

* 24 Mbps: -85 dBm,

* 36 Mbps: -80 dBm,

* 54 Mbps: -73 dBm,

* 보안: 40/64비트 및 128/154비트 WEP 암호화; WPA AES 256비트 암호화, Dynamic Security Link 128비트 암호화; 802.11x (RADIUS 서버 인증 방식); EAP-MD5, EAP-TLS, EAP-TTLS 및 PEAP 인증; ESSID 브로드캐스트 제어, 로컬 MAC 인증; 서버 접근제어목록, Dynamic Session Key 관리 및 TKIP, 동적 VLAN 할당, CC(client-to-client) 및 업링크 필터링,

* 성능: 클리어 채널 선택(Clear Channel Select), 자동 네트워크 연결, 동적 속도 전환(dynamic rate shifting),

* 네트워크 관리: 사이트 검색 툴, Wireless Infrastructure Device Manager, Wireless LAN Discovery Tool, 3NS, SNMP이다.

즉, 종래의 액세스 포인트 장치는 패킷에 대한 안정성을 보장하기 위해 아래와 같이 보안 모듈만을 탑재하고 있다.

* 보안: 40/64비트 및 128/154비트 WEP 암호화; WPA AES 256비트 암호화, Dynamic Security Link 128비트 암호화; 802.11x (RADIUS 서버 인증 방식); EAP-MD5, EAP-TLS, EAP-TTLS 및 PEAP 인증; ESSID 브로드캐스트 제어, 로컬 MAC 인증; 서버 접근제어목록, Dynamic Session Key 관리 및 TKIP, 동적 VLAN 할당, CC(client-to-client) 및 업링크 필터링.

그러나, 종래의 엑세스 포인트 장치에 대해서 다양한 공격이 가능하며 이에 대한 대응 기능을 포함하고 있는 장비는 개발되지 않은 상태이다.

이하에서는 현재까지 공개된 엑세스 포인터에 대한 공격방법에 대하여 설명한다.

네트워크 공격 기술 개요

* 무선 네트워크 공격

악의적인 사용자들에 의해서 사이버 공격 기법은 날로 다양해고 있으며, 해킹 기법의 발달로 자동화, 지능화된 해킹 툴이 공개적으로 유포되어 국내외 해킹 발생빈도는 급격히 증가하고 있는 추세이다. 특히 네트워크의 취약점이 지속적으로 증가하고 있으며 웜바이러스와 같은 치명적인 공격에 의해 네트워크 서비스를 마비시킬 수 있는 서비스거부(DDoS) 공격이 급증하고 있는 가운데 무선 네트워크상에서의 무선랜 공격은 도 1에 도시된 바와 같이 수동적(passive), 능동적(active), 로그 에이피 (rogue AP) 공격으로 분류할 수 있다.

가. 수동적(Passive) 공격

수동적 공격의 목적은 액세스 포인트 장치 MAC, SSID, 채널, 제조사, WEP 설정여부, 설치 위치 정보를 얻기 위함이다. 3가지 방식의 프로그램들이 있는데 패킷을 캡쳐하는 스니퍼(sniffer) 방식, 정보를 얻기 위해서 query 하는 stumbler 방식 그리고, 전송되는 패킷이 존재하지 않고 어떤 네트워크에도 속하지 않아 모든 네트워크 패킷을 수집할 수 있는 passive monitor 가 있다.

대표적인 sniffer 프로그램으로 airopeek, ethereal, tcpdump 가 있고, stumbler 프로그램은 netstumbler, passive monitor 프로그램은 kismet이 있다.

나. 불법 AP(Rogue AP) 공격

불법 AP(Rogue AP)란 사용자의 편의를 목적으로 유선 네트워크에 설치된 비인가 AP, 또는 공격자에 의해서 고의로 설치된 AP를 말한다. 이는 상당한 위협요소가 되는데 회사 내의 보안 정책을 거치지 않고 내부 유선망에 침입할 수 있으므로 rogue AP를 반드시 제거하여야 한다. 만약 사용자의 부주의로 보안을 신경 쓰지 않은 채 AP를 연결하여 Ad-hoc 네트워크를 구성한다면 더욱 위험하게 되고 비인가자에 의한 네트워크 대역폭 낭비를 불러올 수도 있다.

다. 능동적(Active) 공격

능동적 공격의 목적은 정보 수집보다는 서비스 거부와 같은 공격적인 면이 강하다. 공격기법으로는 spoofing, DoS, MITM 등이 있다. 각각 살펴보면 spoofing 공격은 MAC/IP/Frame을 변조하여 인증을 통과하기 위한 목적으로 사용되고, 서비스 거부 공격에도 사용된다. DoS 공격으로는 반복적으로 위조된 disassociation / deauthentication 프레임을 전송하는 deauth flooding과 주파수대가 비슷한 장비의 잡음을 이용하는 jamming 기법이 있다. disassociation 기법은 rogue AP 격리를 위한 기법으로 활용되기도 한다. Man-in-the- middle과 session hijack 공격은 기존 접속을 해제시켜 공격자의 AP로 유도하거나 mac을 spoofing 하여 세션을 가로채는 기법이다. 또한 도 2에 도시된 바와 같이 서비스거부(DDoS) 공격이 가능하기 때문에 이에 대한 대응 기술이 제공되어야 한다.

따라서 상기한 바와 같은 다양한 공격에 대하여 대응 기술/대응 모듈에 대한 제안이 필요한 실정이다.

현재 무선 아이디에스/아이피에스(Wireless IDS/IPS) 기능을 제공하기 위해 수행된 연구 결과는 AirMagnet(Borque, Lyne, " Wi-Fi Security Review: AirMagnet", http://www.enterpriseitplanet.com/security, 2004), AirDefense (http://www.airdefense.com) 등이 있다.

Airmagnet 센서는 SQL DB를 기반으로 WLAN 관리 및 모니터링 기능을 수행하는데, 이에 따르면, Rogue AP 탐지 및 추적 기능을 제공하며 DoS 공격에 대한 대응을 통해 무선 네트워크에 대한 안전성 확보를 목적으로 하고 있다.

도 3은 무선 아이피에스 시스템 구조도(AirDefense 참조)이다.

도 3을 참조하면, AirDefense 시스템은 wireless AP 센서와 자바 기반 웹 콘솔 시스템으로 구성된 Red Hat 리눅스 서버로 구성되어 있다. AirDefense 웹 콘솔과 AP 센서는 서버와 안전한 무선 통신을 통해 트래픽에 대한 관리 및 차단 기능을 수행한다.

AirDefense에서 제시하는 Wireless IPS는 정책 기반 IDS/IPS 시스템으로 네트워크에 대한 관리, 성능 및 안전성을 설정하며 WLAN 세션에 대한 보안 기능을 제공한다. 또한 일반적으로 리눅스 운영체제를 기반으로 공개 소프트웨어 형태로 개발되어 현재 활발한 연구가 진행되고 있으며 현재 Snort-Wireless 및 WIDZ와 같은 코드가 제시되고 있다.

그러나, 상기한 바와 같은 구조에 따르면 에어디펜스 시스템은 공격에 대한 탐지 기능만을 제공하고 있으며, 외부 공격에 대해 수동적 대응만을 제공하고 있으므로 사용자 능동적으로 공격침입을 탐지하고 차단할 수 있는 기술이 절실히 요구되고 있는 실정이다.

발명이 이루고자 하는 기술적 과제

본 발명의 목적은 상기한 바와 같은 종래 기술에서의 문제점을 해결하고자 제안된 것으로서, 외부로부터의 공격을 탐지하고 및 차단할 수 있도록 하는 무선 액세스 포인트 장치를 제공하고자 한다.

본 발명의 또 다른 목적은 액세스 포인트 장치 이상 트래픽에 대한 판별 기능을 제공하는 모듈을 추가하여 무선 네트워크에서의 보안 서비스의 질을 향상시킬 수 있는 무선 액세스 포인트 장치를 제공함에 있다.

본 발명의 또 다른 목적은 무선 액세스 포인트 장치를 이용하여 이상 트래픽을 탐지하여, 액세스 포인트 장치에서 서비스 거부 공격 등과 같은 네트워크 공격이 있을 경우 이를 탐지할 수 있는 방법을 제공함에 있다.

본 발명의 또 다른 목적은 무선 액세스 포인트 장치를 이용하여 탐지된 이상 트래픽의 공격을 차단할 수 있는 방법을 제공함에 있다.

본 발명의 또 다른 목적은 무선 액세스 포인트 장치를 이용하여 공격침입이 탐지된 네트워크에 대해서는 해당 트래픽 연결을 끊을 수 있는 방법을 제공하는 데 있다.

본 발명의 또 다른 목적은 무선 액세스 포인트 장치를 이용하여 액세스 포인트 장치에서 De-Auth flooding 패킷을 해당 호스트에 전송하여 공격자 시스템에 대한 연결을 끊을 수 있는 방법을 제공하는 데 있다.

발명의 구성

상기한 바와 같은 목적을 달성하기 위한 본 발명의 바람직한 실시 예에 따르면, 사용자와 무선으로 연동하여 무선 신호를 송수신 중계하고 공격자부터의 무선 네트워크 트래픽 신호를 탐지 및 차단하는 무선 액세스 포인트 장치에 있어서, 네트워크 인터페이스 카드를 포함하고 공격자의 공격 트래픽을 접수하고 탐지하는 네트워크 모니터링 모듈 및 공격자에게 경고 메시지를 전송하도록 제어하는 경고 인터페이스 모듈을 포함하는 네트워크 모듈과; 상기 네트워크 모니터링 모듈로부터 전송된 공격 트래픽을 필터링하는 패킷 분석모듈 및 상기 패킷 분석모듈로부터의 필터링된 패킷이 네트워크 공격패킷인지를 규칙 DB/서명모듈과 연동하여 판단하여 그 결과를 상기 패킷분석모듈 및 상기 경고 인터페이스 모듈에 전송하는 침입탐지모듈을 포함하는 분석 및 보안모듈;로 이루어지는 것을 특징으로 하는 무선 액세스 포인트 장치가 제공된다.

바람직하게는, 상기 네트워크 모듈은 802.11 b/g 패킷을 채널 호핑(channel hopping)하고, 기타 환경설정 정보를 동기화시키고, level 2 무선 트래픽을 모니터링하며, probe request, probe response, beacon frame을 전송하는 상기 채널 호핑 모듈을 더 포함하여 이루어지는 것을 특징으로 한다.

또한 바람직하게는, 상기 네트워크 모니터링 모듈은 passive 형태의 sniffing을 수행하고 모든 네트워크 패킷을 탐지하는 monitoring mode이고, 상기 채널 호핑 모듈을 통해 수집된 802.11 b/g 패킷을 수집하고, SSID beacon frame을 전송하지 않는 숨겨진 AP 네트워크는 클라이언트의 AP 접속시 SSID를 모니터링 하여 탐지하는 것을 특징으로 한다.

또한 바람직하게는, 상기 경고 인터페이스 모듈은 네트워크 공격 패킷 전송자의 접속을 끊는 deauth 신호를 전송하는 것을 특징으로 한다.

또한 바람직하게는, 상기 침입 탐지 모듈은 상기 네트워크 모니터링 모듈로부터 전달된 AP 정보를 사전에 관리자에 의해서 입력된 인가된 AP 리스트와 비교를 수행하는 Rogue AP 탐지 모듈과, sequence 번호를 추적하여 MAC spoofing 공격을 탐지하고 DoS의 deauth flooding 공격은 브로드캐스트 disassociate/deauthenticate frame 발생 여부를 확인하여 탐지하고, Stumbler 공격 탐지를 위해서 stumbler 별로 존재하는 fingerprint를 패킷과 비교하여 탐지하고, Man-in-the-middle 공격 탐지는 AP의 channel 변경여부를 확인하여 탐지하는 Spoof/DoS/Stumbler/MITM 탐지 모듈을 포함하여 이루어진 것을 특징으로 한다.

본 발명의 또 다른 측면에 따르면, 무선 액세스 포인트 장치를 통해 무선 네트워크 공격트래픽을 탐지하고 차단하는 무선 액세스 포인트 장치를 이용한 무선 네트워크 침입탐지 및 차단방법에 있어서, 접수된 무선 트래픽을 분석하고 전송하는 단계와; 전송된 무선 트래픽을 필터링하는 단계와; 필터링된 패킷이 네트워크 공격패킷 인지를 규칙 DB/서명 모듈과 연동하여 판단하는 단계와; 상기 판단결과, 필터링된 패킷이 네트워크 공격 패킷인 경우에는 그 결과를 경고 메시지로 공격자에게 전달하는 단계로 이루어진 것을 특징으로 하는 무선 액세스 포인트 장치를 이용한 무선 네트워크 침입탐지 및 차단방법이 제공된다.

바람직하게는, 상기 경고메시지 전달단계 이후에 수신자가 확인을 하였는지를 판단하는 단계와; 만약, 수신자가 확인한 경우에는 해당 데이터를 버리는 단계;를 더 포함하여 이루어진 것을 특징으로 한다.

또한 바람직하게는, 만약 필터링된 패킷이 네트워크 공격 패킷인 경우에, 경고메시지 전송시 수신자의 접속을 끊는 deauth 데이터를 전송하는 것을 특징으로 한다.

본 발명은 종래 802.1x 기반 WLAN은 손쉽게 공격 가능하다는 취약점을 보이고 있어, 무선 패킷에 대한 스니핑, 변조 및 조작 등을 탐지하고, AirJack 등의 DDoS 공격에 대해 AP 단에서 사전에 탐지/차단하는 것을 특징으로 한다.

즉, 종래 대부분의 네트워크 환경에서 무선이 도입되었지만, AP(Access Point) 에서 해킹 공격을 탐지하지는 않는 반면, 본 발명에서는 최근 점차적으로 무선랜과 관련된 공격들이 증가되고 있는 시점에서 무선 AP 기능에 패킷 필터링과 네트워크 침입탐지 기능을 내장한 임베디드 리눅스 기반 무선 AP를 개발한 점에 특징이 있다.

이하 본 발명에 따른 무선 액세스 포인트 장치 및 그를 이용한 무선 네트워크 시스템의 공격 침입 탐지 및 차단방법을 첨부 도면을 참고로 상세히 설명한다.

도 4는 본 발명에 따른 무선 액세스 포인트 장치를 이용한 유무선 통합형 보안시스템의 개략적인 구성도이다.

본 발명에 따른 유무선 통합형 보안시스템(1000)에 있어서, 무선 아이디에스(IDS) 장치(100)(무선 액세스 포인트 장치, 이하 'AP'장치라 함)는 무선 네트워크상에서 전송되는 트래픽에 대한 모니터링 기능을 수행하며, 특히 Wi-Fi 장치(113)(도 8 참조)를 통해 전송되는 트래픽에 대한 모니터링 기능을 통해 패킷 필터링 및 차단 기능을 제공한다.

도 4를 참조하면, 아이피에스(IPS) 센서(Sensor) 역할을 하는 상기 무선 AP 장치(100)를 유무선 네트워크 사이에 구축하여 무선 트래픽에 대한 모니터링 기능을 수행한 점에 본 발명의 특징이 있다.

즉, 본 발명에 따른 패킷 스니핑, 룰 기반 침입탐지/차단 기능을 제공하는 임베디드 형태의 AP 통합형 고성능 IPS 시스템은 이후에 설명되는 바와 같이, 무선 아이디에스 장치(W-IDS)와 유무선 통합형 보안장치(200)(서버)로 이루어진다.

탐지를 위한 무선 아이디에스(W-IDS) 장비는 유무선 통합형 보안 장비와 직간접으로 연결되어 있으며, 무선 네트워크상의 트래픽을 분석하여 트래픽 정보와 경고(alert) 정보를 유무선 통합형 보안장비로 전송한다.

상기 무선 AP 장치(100)는 사용자 컴퓨터로부터의 무선 신호를 송수신 중계하고 공격자로부터의 무선 네트워크 공격 패킷을 탐지하여 차단하는 기능을 수행한다.

상기 시스템을 통해 유무선에 상관없이 통합형으로 공격 패킷을 탐지하여 차단할 수 있다.

본 발명에 따르면, 무선랜 공격 프레임은 무선 AP에서만 탐지할 수 있으므로 펌웨어(firmware)가 공개되어 있는 업체의 장비를 선택하여 기능을 추가하는 방법을 사용하였다. 만약 제품화하여 대량 생산이 필요하다면 적합한 AP 개발용 임베디드 보드를 선정해야할 것이다.

도 5는 도 4에서의 무선 액세스 포인트(AP:Access Pointer) 장치(100)를 나타낸 외관사시도 및 부품이 장착된 내부인쇄회로기판을 나타낸 도면이다. 도 6은 본 발명에서 사용된 링크시스템 펌웨어 장비의 내부 시스템 구성을 개략적으로 나타낸 개념도이다.

실무적으로 본 발명에서는 공개된 여러 펌웨어(firmware)중 최소 기능만 포함하는 OpenWRT를 포팅하고 침입탐지 기능을 추가한다. 무선과 관련된 공격이 아닌 경우는 무선 AP에 연결되어 있다고 할지라도 유무선 통합 장치(200)에서 탐지 및 차단한다.

본 발명에 따르면, 유무선 통합 장비에서 무선 관련 모든 네트워크 트래픽을 모니터링할 수 있도록 상기 무선 AP 장치(100)에서 발생한 802.11 b/g level 2 frame 로그를 유무선 통합형 보안 장치(200)로 전송한다.

도 7은 본 발명에서 사용된 시스템 보드를 개략적으로 나타낸 구성도이다.

도 7을 참조하면, 무선 AP 기반 W-IDS 구조 즉 무선 AP 장치(100)를 실제로 다음과 같은 사양의 무선 AP 장치에 관련 소프트웨어를 임베디드 방식으로 탑재하였다.

상기 장치(100)의 하드웨어 사양은 Linksys WRT54GS를 하드웨어로 사용한다. 이 장치(100)는 MIPS CPU 200MHz, flash 8MB, RAM 32MB, LAN 4Port, WAN 1Port 그리고, Wifi로 구성되어 있다. MIPS는 little-endian과 big-endian 모두 지원하는데 OpenWRT firmware는 little-endian 방식의 MIPSEL을 사용한다.

상기 장치(100)는 4개의 LAN 포트와 1개의 WAN 포트, 안테나를 지원하기 때문에 이를 통해 외부와 연계할 수 있으며, 임베디드 형태의 프로그래밍을 지원하기 위해 RAM과 Flash Memory를 갖추고 있다. 본 발명에서는 펌웨어(firmware)형태로 필터링 모듈을 컴파일하여 AP 시스템 내부에 임베딩한다.

도 8은 본 발명에 따른 무선 AP 장치 네트워크 인터페이스를 나타낸 개념도이다.

즉, 무선 AP 장치(100)에서 제어부(140), WiFi 안테나(130), 스위치(150)의 연계를 나타내고 있다. 본 시스템에 snort 형태의 패킷 필터링, sniffing 모듈을 적용하여 무선 트래픽에 대한 제어 기능을 제공할 수 있다.

상기 무선 AP 장치(100)의 사용에 있어서, 참고적으로 소프트웨어에 관한 사항을 설명하면, openWRT 포팅 및 toolchain 구성은 다음과 같다. 기본 linksys firmware가 설치되어 있는 경우는 웹관리화면으로 접속하여 OpenWRT firmware (linux 2.4.30)를 설치하면 된다. 또는, NVRAM 값을 초기화 시킨 뒤 tftp로 firmware를 설치할 수 있다. 설치가 끝난 뒤 telnet을 이용하여 192.168.1.1로 접속가능하다. 만약 ssh를 사용하기 위해서는 root에 패스워드를 부여하면 된다. 리눅스가 설치된 PC에서 MIPSEL toolchain을 구성하여 개발 플랫폼을 구축한다.

도 9는 본 발명에 따른 무선 액세스 포인트 장치의 개략적인 기능블럭도이다.

도 9를 참조하면, 무선 액세스 포인트 장치(100)는 크게 네트워크 모듈(110)과 분석 및 보안모듈(120) 및 네트워크 인터페이스 카드(101)를 포함하여 이루어진다.

상기 네트워크 모듈(110)은 채널 호핑 모듈(112), 네트워크 모니터링 모듈(114) 및 경고 인터페이스 모듈(116)로 이루어진다.

상기 채널 호핑 모듈(112)은 802.11 b/g 패킷을 채널 호핑(channel hopping)한다. 기타 환경설정 정보를 동기화시킨다. 또한 level 2 무선 트래픽을 모니터링하며, 구체적으로 probe request, probe response, beacon frame을 전송한다.

상기 네트워크 모니터링 모듈(114)은 passive 형태의 sniffing을 수행하고 모든 네트워크 패킷을 탐지하는 monitoring mode로서 상기 채널 호핑 모듈(112)을 통해 수집된 802.11 b/g 패킷을 수집한다. 또한, SSID beacon frame을 전송하지 않는 숨겨진 AP 네트워크는 클라이언트의 AP 접속시 SSID를 모니터링 하여 탐지한다. 또한, 수집된 패킷들은 이후의 보안 모듈(120)로 전달된다. 또한, 주기적으로 유무선 통합장비의 무선관련 환경설정 변경을 검사하여 동기화시킨다.

상기 네트워크 모니터링 모듈(114)은 AP 장치에서의 모든 네트워크 패킷을 수집한다.

상기 경고 인터페이스 모듈(116)은 유무선 통합장치(200)로 전송하는 역할을 수행하며, 무선 네트워크 모니터링을 로그하고, 경고(alert)를 로그하는 일종의 액션 모듈(action module)이다. 또한 무선 네트워크를 공격하는 공격 경고를 생성할 수 있다.

상기 분석 및 보안모듈(120)은 패킷 분석모듈(122), 침입탐지 모듈(124) 및 규칙 DB/서명 모듈(126)로 이루어진다.

상기 패킷 분석모듈(122)은 일종의 무선 트래픽 필터링 모듈로서, 상기 네트워크 모니터링 모듈(114)로부터 전송된 네트워크 패킷을 캡춰하고, 공격 트래픽을 검출한다.

상기 침입 탐지 모듈(124)은 불법 AP(rogue AP) 탐지 모듈(124-1)과 spoof/DoS/Stumbler/MITM 탐지 모듈(124-2)로 이루어지며 일종의 판단 모듈이다.

상기 불법 AP(rogue AP) 탐지 모듈(124-1)은 상기 네트워크 모니터링 모듈(114)로부터 전달된 AP 정보를 사전에 관리자에 의해서 입력된 인가된 AP 리스트와 비교를 수행한다. 이때 비교하는 정보는 MAC/SSID/Vendor/Media type (802.11 b/a/g)/Channel 등을 비교한다. 비인가 AP로 탐지되면 alert 로그를 유무선 통합장치(200)로 전송한다.

상기 Spoof/DoS/Stumbler/MITM 탐지 모듈(124-2)은 sequence 번호를 추적하여 MAC spoofing 공격을 탐지하고 DoS의 deauth flooding 공격은 브로드캐스트 disassociate/deauthenticate frame 발생여부를 확인하여 탐지한다. Stumbler 공격 탐지를 위해서 stumbler 별로 존재하는 fingerprint를 패킷과 비교하여 탐지한다. 대표적인 netstumbler 3.2.3 의 경우는 query 시 “All your 802.11b are belong to us" 문자열을 포함한다. Man-in-the-middle 공격 탐지는 AP의 channel 변경 여부를 확인하여 탐지한다. 이렇게 탐지된 alert 로그들은 유무선 통합장비로 전송한다.

상기 규칙 데이터베이스/서명모듈(126)은 상기 침입탐지모듈(124)과 연동하여 작동되며, 서명과 규칙을 검색할 수 있다.

참조부호 101은 네트워크 인터페이스카드를 나타낸 것으로서 각종 무선 패킷들의 송수신 통로가 된다.

도 10은 본 발명에 따른 무선 액세스 포인트 장치를 통한 무선 네트워크 침입탐지 및 차단과정을 나타낸 흐름도이다.

도 10을 참조하면, 먼저 무선 액세스 포인트 장치(100)의 네트워크 모듈(110)의 채널 호핑 모듈(112) 및 네트워크 모니터링 모듈(114)을 통해 무선 트래픽을 접수한다(ST-2).

이후 접수된 무선 트래픽은 네트워크 모니터링 모듈(114)에서 분석되고 패킷 분석모듈(122)로 전송된다(ST-4).

이후 전송된 무선 트래픽은 상기 패킷 분석모듈(122)에서 필터링되고 이후 침입탐지모듈(124)로 전송된다(ST-6).

상기 침입탐지모듈(124)은 필터링된 패킷이 네트워크 공격패킷인지를 규칙 DB/서명 모듈(126)과 연동하여 판단한다(ST-8). 상기 단계 ST-8의 판단결과, 만약 네트워크 공격 패킷이 아닌 경우에는 그 결과를 패킷 분석모듈(122) 및 경고 인터페이스 모듈(116)에 알려준다. 결과적으로 해당 데이터는 바이패스 된다.

만약 상기 단계 ST-8의 판단결과, 필터링된 패킷이 네트워크 공격 패킷인 경우에는 그 결과를 패킷 분석모듈(122) 및 경고 인터페이스 모듈(116)에 알려준다. 상기 경고 인터페이스 모듈(116)은 경고 메시지를 상기 네트워크 모니터링 모듈(114)에 전송하여 경고메시지가 수신자에게 전달되도록 한다(ST-10). 한편, 상기 단계 ST-10에서는, 경고메시지와 함께 수신된 데이터가 전달되도록 할 수도 있다.

이후, 상기 네트워크 모니터링 모듈(114)은 상기 경고메시지(혹은 경고메시지+ 데이터)를 받은 수신자가 확인을 하였는지를 판단한다(ST-12). 만약 상기 단계 ST-12의 판단결과, 수신자가 확인한 경우에는 해당 데이터를 버린다(ST-14).

한편 도시되지는 않았지만, 만약 상기 단계 ST-8에서 필터링된 패킷이 네트워크 공격 패킷인 경우에, 상기 단계 ST-10에서 경고메시지 전송을 하지 않고 수신자의 접속을 끊는 deauth 데이터를 전송할 수도 있다.

발명의 효과

상기한 바와 같이 본 발명에 따른 무선 액세스 포인트 장치 및 그를 이용한 무선 네트워크 트래픽 침입탐지 및 차단방법에 의하면, 종래에 단순히 공격 트래픽의 기본적인 사항만을 체크하던 상태에서 발전하여 본 발명에서는 해당 공격 트래픽을 필터링하여 탐지하고 일차적으로 경고메시지를 전송하며 이차적으로는 해당 수신자의 접속을 끊는 신호를 전송함으로써 확실하게 무선 네트워크 트래픽 침입을 탐지하고 차단할 수 있는 효과가 있다.

본 발명은 상기 실시 예를 중심으로 설명하였지만 본 발명의 범위는 이에 제한되는 것은 아니며, 본 발명의 기술분야에 익숙한 기술자는 상기 실시 예에 기술된 내용을 토대로 이후에 기술되는 본 발명의 특허청구범위내에서 다양하게 변형실시가 가능할 것이다.

도면의 간단한 설명

도 1은 일반적인 무선랜에서의 공격 유형을 나타낸 개념도이다.

도 2는 종래 기술에 따른 무선랜 서비스거부(DDos) 공격 기법을 나타낸 개념도이다.

도 3은 무선 아이피에스(IPS) 시스템 구조를 개략적으로 나타낸 개념도이다.

도 4는 본 발명에 따른 무선 아이디에스 시스템의 개략적인 구성도이다.

도 5는 도 4에서의 무선 액세스 포인트 장치(AP:Access Point) 장치를 나타낸 외관사시도 및 부품이 장착된 내부인쇄회로기판을 나타낸 도면이다.

도 6은 본 발명에서 사용된 링크시스템 펌웨어 장비의 내부 시스템 구성을 개략적으로 나타낸 개념도이다.

도 7은 본 발명에서 사용된 시스템 보드를 개략적으로 나타낸 구성도이다.

도 8은 본 발명에 따른 무선 아이피에스 시스템의 네트워크 인터페이스를 나타낸 개념도이다.

도 9는 본 발명에 따른 무선 액세스 포인트 장치의 개략적인 기능블럭도이다.

도 10은 본 발명에 따른 무선 액세스 포인트 장치를 통한 무선 네트워크 침입탐지 및 차단과정을 나타낸 흐름도이다.

* 도면의 주요 부분에 대한 부호의 설명 *

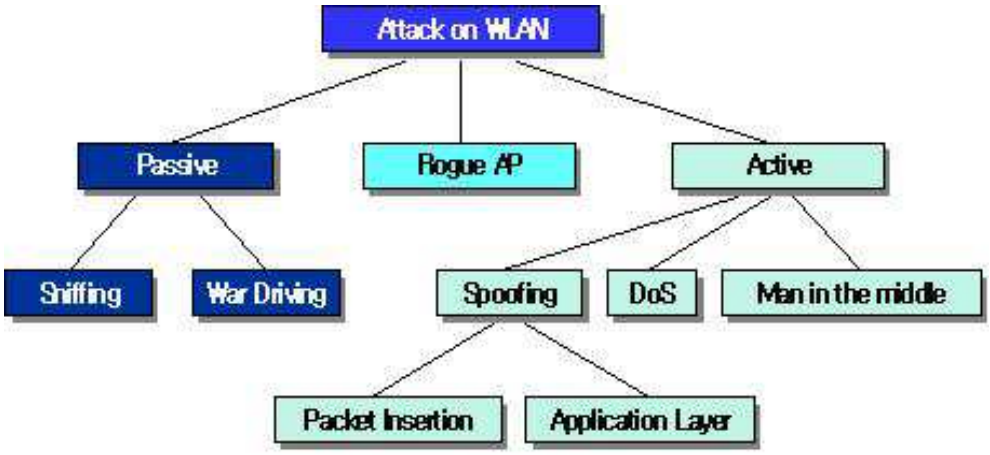
100: 무선 액세스 장치

110: 네트워크 모듈

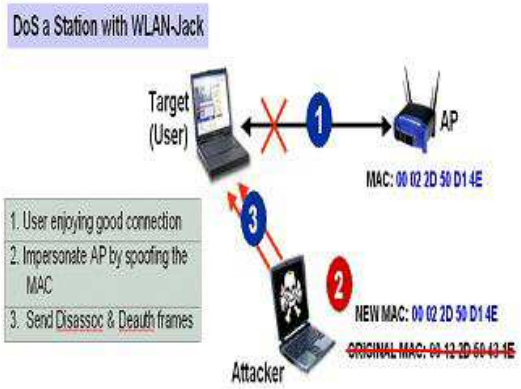
120: 분석 및 보안모듈

도면

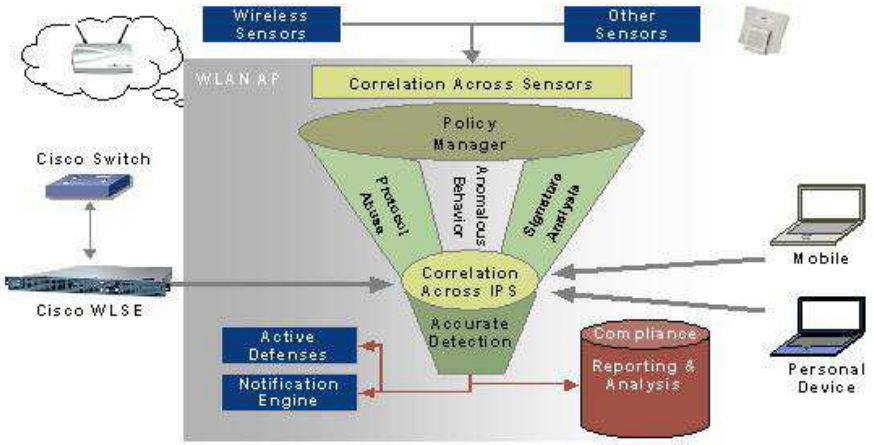
도면1


Attack on WLAN
Passive
Rogue AP
Active
Sniffing
War Driving
Spoofing
DoS
Man in the middle
Packet Insertion
Application Layer

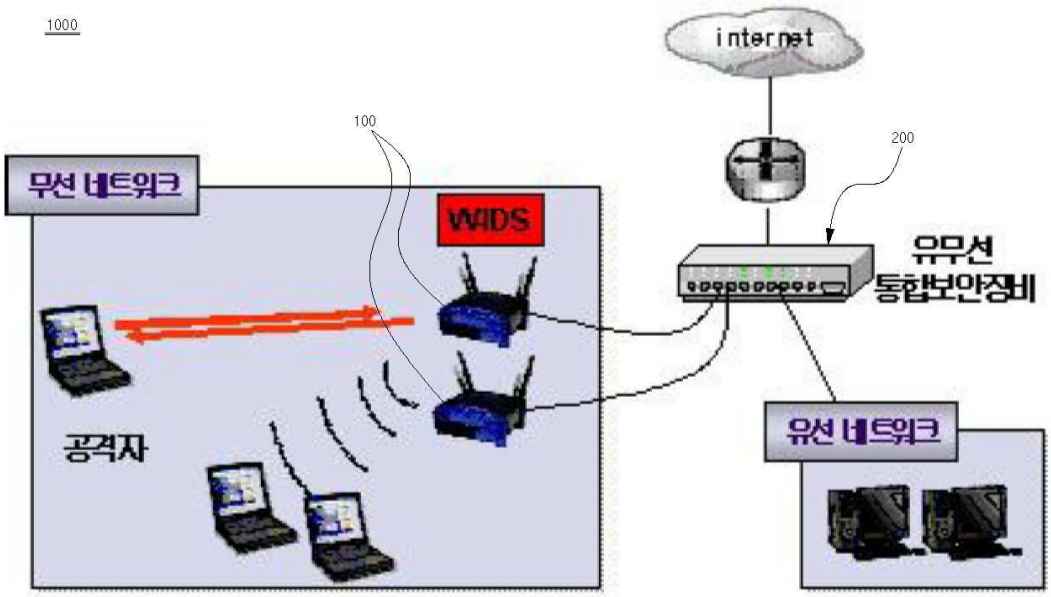
도면2


DoS a Station with WLAN-Jack
Target (User)
AP
MAC: 00 02 2D 50 D1 4E
1. User enjoying good connection
2. Impersonate AP by spoofing the MAC
3. Send Disassoc & Deauth frames
NEW MAC: 00 02 2D 50 D1 4E
Attacker

도면3


Wireless Sensors
Other Sensors
WLAN AP
Correlation Across Sensors
Policy Manager
Protocol Abuse
Anomalous Behavior
Signature Analysis
Cisco Switch
Cisco WLSE
Correlation Across IPS
Accurate Detection
Active Defenses
Notification Engine
Compliance
Reporting & Analysis
Mobile
Personal Device

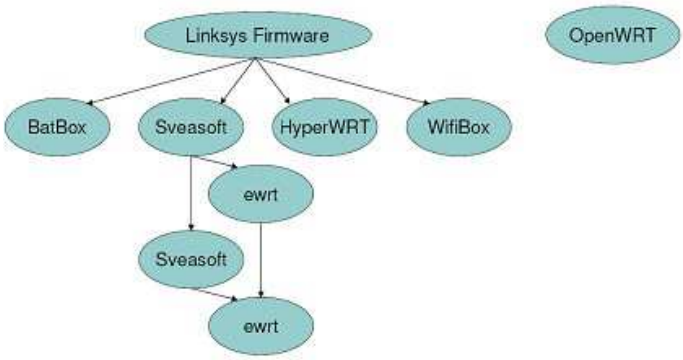
도면4


1000
internet
100
200
무선 네트워크
WDS
유무선
통합보안장비
공격자
유선 네트워크

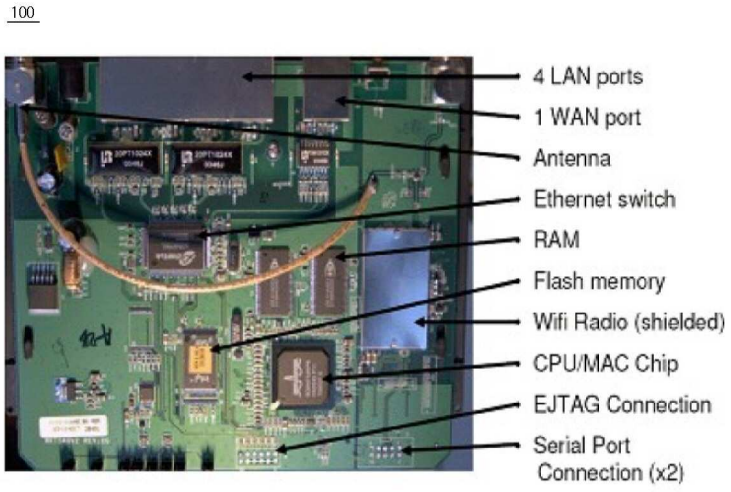
도면5


100
LINKSYS

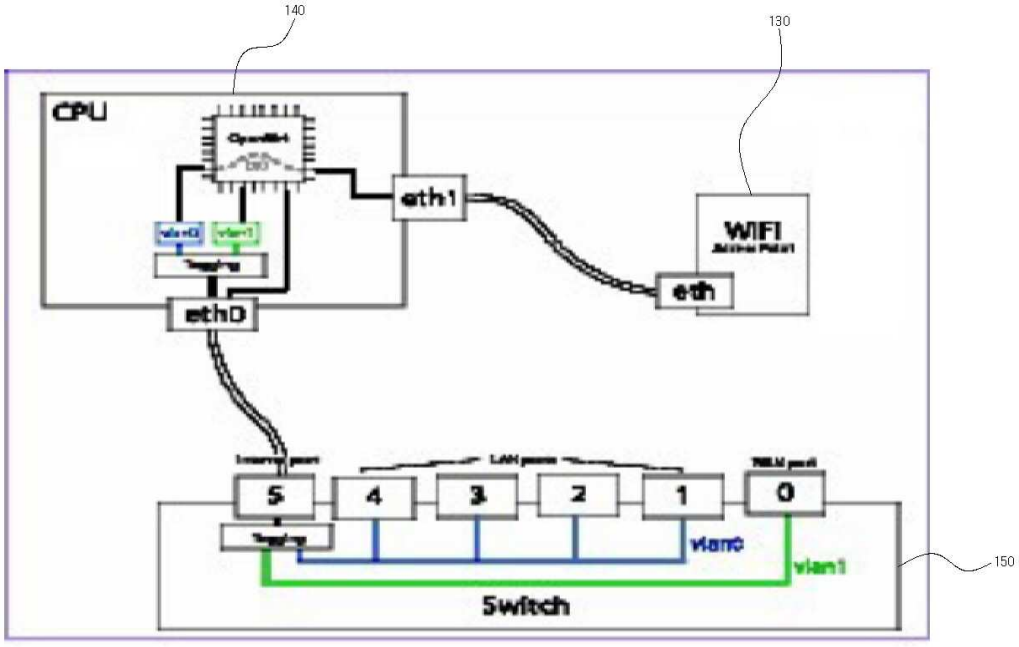
도면6


Linksys Firmware
OpenWRT
BatBox
Sveasoft
HyperWRT
WifiBox
ewrt
Sveasoft
ewrt

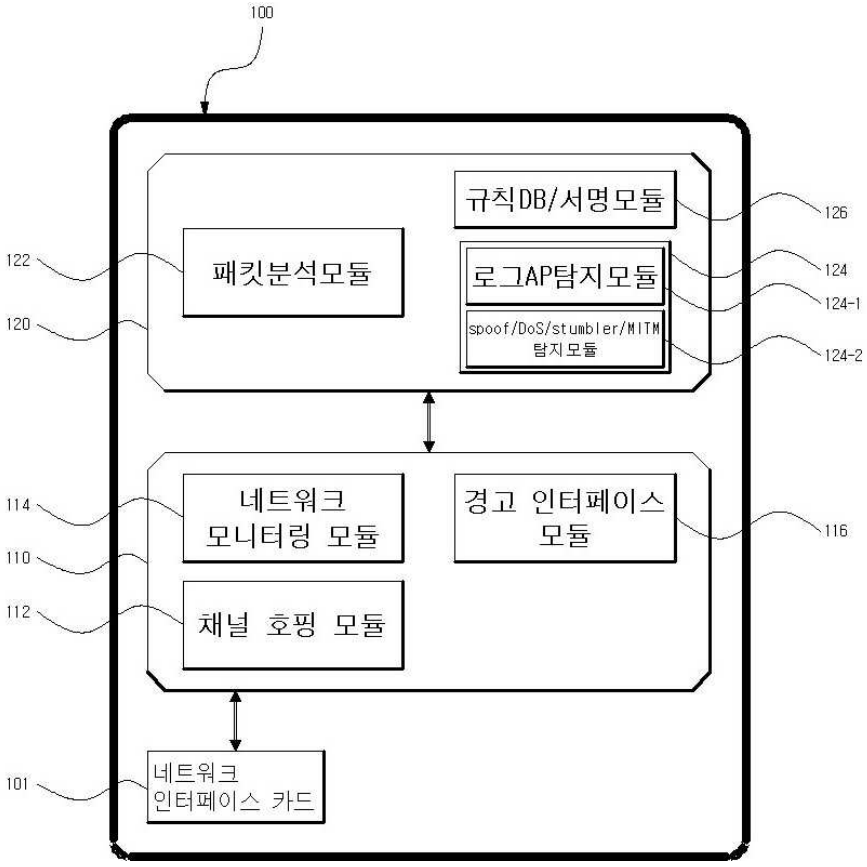
도면7


100
4 LAN ports
1 WAN port
Antenna
Ethernet switch
RAM
Flash memory
Wifi Radio (shielded)
CPU/MAC Chip
EJTAG Connection
Serial Port
Connection (x2)

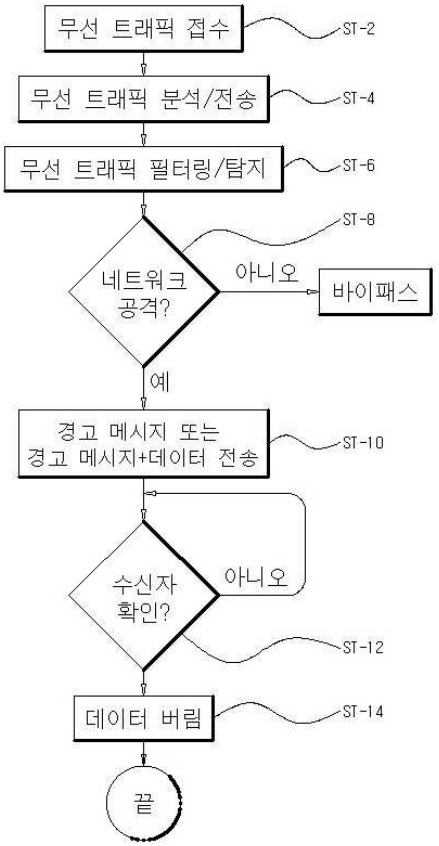
도면8


140
130
CPU
eth1
WIFI
eth
eth0
5
4
3
2
1
0
vlan0
vlan1
Switch
150

도면9


100
규칙DB/서명모듈
126
패킷분석모듈
122
로그AP탐지모듈
124
124-1
120
spoof/DoS/stumbler/MITM
탐지모듈
124-2
네트워크
모니터링 모듈
114
경고 인터페이스
모듈
116
110
채널 호핑 모듈
112
네트워크
인터페이스 카드
101

도면10


무선 트래픽 접수
ST-2
무선 트래픽 분석/전송
ST-4
무선 트래픽 필터링/탐지
ST-6
ST-8
네트워크
공격?
아니오
바이패스
예
경고 메시지 또는
경고 메시지+데이터 전송
ST-10
수신자
확인?
아니오
ST-12
데이터 버림
ST-14
끝