무선 LAN Access Point에서 임베디드 형태의 유해 트래픽 침입탐지/차단 시스템 개발

Development of Malicious Traffic Detection and Prevention System by Embedded Module on Wireless LAN Access Point

이형우, 최창원
한신대학교 컴퓨터정보소프트웨어학부

Hyung-Woo Lee(hwlee@hs.ac.kr), Chang-Won Choi(won@hs.ac.kr)

요약

네트워크의 급속한 성장과 더불어 유무선 서비스 및 사용자들이 급증하고 있는 가운데 IEEE 802.1x 기반 WLAN 환경에서 Session hijacking 및 DoS 공격 등 취약점으로 인해 다양한 공격이 시도되고 있어 무선 네트워크에 대한 침입탐지/차단 시스템 개발이 시급하다. 본 연구에서는 AP(Access Point)에서 임베디드 형태로 무선 패킷에 대한 모니터링 및 유해 트래픽 침입탐지/차단 기능을 제공하며 무선 네트워크에 대한 통합 보안 관리 기능을 제공하는 시스템을 개발하였다. 개발한 시스템은 기존의 무선망 보안 관리 시스템보다 경량화된 형태로 개발되었으며 무선 트래픽에 대한 능동적인 보안 관리 기능을 제공하여 대학 캠퍼스망과 같이 최근 급속도로 확산되고 있는 무선랜 기반 네트워크 환경에서의 개선된 보안관리 기능을 제공할 수 있었다.

■ 중심어 : □액세스 포인트□침입탐지□침입방지□무선랜□통합 보안관리□

Abstract

With the increasing popularity of the wireless network, the vulnerability issue on IEEE 802.1x Wireless Local Area Network (WLAN) are more serious than we expected. Security issues range from mis-configured wireless Access Point(AP) such as session hijacking to Denial of Service(DoS) attack. We propose a new system based on intrusion detection or prevention mechanism to protect the wireless network against these attacks. The proposed system has a security solution on AP that includes an intrusion detection and protection system(IDS/IPS) as an embedded module. In this paper, we suggest integrated wireless IDS/IPS module on AP with wireless traffic monitoring, analysis and packet filtering module against malicious wireless attacks. We also present that the system provides both enhanced security and performance such as on the university wireless campus network.

■ keyword : □Access Point□Intrusion detection□Intrusion Prevention□Wireless LAN□Integrated Wireless Security System□

* 본 연구는 2008년 한신대학교 교내 특별연구비 지원으로 수행되었습니다.

접수번호 : #081127-002
접수일자 : 2008년 11월 27일
심사완료일 : 2008년 12월 19일
교신저자 : 이형우, e-mail : hwlee@hs.ac.kr

I. 서 론

네트워크에서 침입이란 컴퓨터 자원의 무결성, 비밀성, 가용성을 방해하는 모든 행위들의 집합을 의미한다. 또 다른 의미로는 컴퓨터의 보안 정책을 파괴하는 행위를 말하기도 한다. 이러한 침입의 형태와 기술은 시간과 비례하여 그 다양성이 나날이 증가되고 있으며 공격 시도 및 침입에 성공하는 공격의 횟수도 증가하고 있다. 네트워크 보안의 1세대 솔루션인 방어정책을 설정하여 침입을 차단하는 방화벽(Firewall)과 방화벽을 우회한 공격에 대해 분석하고 탐지하는 2세대 솔루션인 침입탐지 시스템(IDS : Intrusion Detection System)이 등장하였다. 이들은 네트워크 위협을 최소화하고 공격을 완화하는데 중요한 역할을 하지만 각각의 취약성으로 인해 또 다른 위협을 야기하기 때문에 이들의 취약성을 해결하고 공격에 보다 능동적인 대응이 가능한 침입차단시스템(IPS : Intrusion Prevention System)이 나오게 되었다[1-3].

IPS는 IDS와 마찬가지로 데이터 소스에 따라 호스트 기반 IPS와 네트워크 기반의 IPS으로 나눠진다. 네트워크 기반의 IPS는 기술적으로 실시간 패킷 처리와 오탐지를 최소화, 변형 공격과 오용공격의 탐지기술, 그리고 각 상황에 맞는 실시간 반응 기술이 요구된다[2]. 또한 IPS는 탐지 모델에 따라 시그너처(Signature) 기반 IPS와 비정상행위(Anomaly behavior) 기반 IPS로 구분되며, 시그너처 방법은 공격자와 피해자 중에서 공격자에 초점을 맞춘 것으로 해당 공격의 규칙을 바탕으로 네트워크 트래픽에서 해당 규칙을 찾아내어 이를 차단하는 방식이다. 비정상행위 방법은 기존 및 신종 공격에 대한 사전 대응을 위하여 피해자에 초점을 맞춘 것으로 피해자의 취약점을 악용할 수 있는 행위를 사전에 차단하는 방식이다[1-3]. 일반적으로 비정상행위 IPS인 경우 과거의 경험적인 자료로부터 침입을 탐지하기 때문에 자료의 양과 질에 의존적이다. 또한 탐지 할 수 있는 가능성을 증명하는 것에 의의가 있을 뿐 탐지율이 낮다는 단점을 갖기 때문에 상대적으로 탐지율이 높은 시그너처 기반의 IPS가 널리 사용되고 있다[3][4]. 공개 소프트웨어 형태인 Snort[5]를 기반으로 IDS 및 IPS 기능을 제공하는 시스템이 개발되고 있다.

이와 같이 기존의 유선망(Wired Network)에서의 네트워크 침해대응(Network Intrusion Response) 기술은 점차 능동적이면서 지능적인 형태로 발전하고 있다. 이는 최근 이슈가 되고 있는 무선망(Wireless Network)에서도 안전한 통신 서비스를 위해서 반드시 요구되는 사항들이다. 따라서 최근 급속도로 확산되고 있는 무선 LAN(WLAN : Wireless Local Area Network) 기반 네트워크 환경에서의 침입탐지/차단 기능을 제공하는 시스템 개발이 필요한 시점이다.

특히 최근 무선 LAN을 통한 새로운 형태의 공격 방법들이 출현하고 있다. 기존의 인터넷 사용은 모두 유선으로만 이뤄져 있어 물리적으로 침입 위치를 확보해야만 하는 문제가 있었다. 하지만 무선 랜을 사용할 경우 전파가 도달 가능한 거리에 있는 위치라면 어디에서든지 스니핑과 침입 공격이 가능하며, 정보를 빼내어가거나 웜과 바이러스 등의 전파로 네트워크를 마비시키는 등의 무선 LAN에 대한 공격에 취약하다[1].

무선 LAN을 통한 공격 방법으로는 멍키 잭(Monkey Jack)이나 키스메트(KISMET) 기반 공격, 웰른라이터(Wellenreiter), 보이드(Void) 11, 에어잭(AirJack), 호스트 AP(Host AP), ASLEAP, Ttcp WiFi, Associate Flood, Auth Flood, De-auth Flood, FakeAP Flood 등 매우 다양한 공격 기법이 있다[2].

현재까지 유선 네트워크를 중심으로 침해사고를 예방하고 효과적인 대응법을 마련하기 위한 침입탐지 시스템이 개발되었으며, 또한 유선망에서의 유해 트래픽에 대한 차단 기능까지 더하여진 침입차단 시스템이 개발이 되었다. 하지만 무선 LAN을 통한 공격에 대해서는 대응 시스템 구축이 미비한 실정이다. 따라서 무선 네트워크에 대한 침입 대응 시스템 개발이 매우 필요한 시점이다.

본 연구는 기존의 유선 네트워크 기반 침입차단시스템을 무선 네트워크 기반 침입차단 시스템(Wireless IPS)으로 확장하기 위한 연구를 수행하였으며, 현재 개발된 국외의 주요 침입차단 시스템을 분석하고 본 연구에서 개발하고자 하는 침입차단 시스템과의 비교를 통해 무선 LAN에서의 액세스 포인트(AP : Access Point) 기반 임베디드 형태의 침입탐지/차단 시스템을 개발하였으며

통합 보안 관리 형태로 모니터링 할 수 있는 시스템을 개발하였다. 개발한 시스템은 대학 캠퍼스망과 같이 최근 급속도로 확산되고 있는 무선 LAN 환경에서의 안전성을 확보할 수 있으며 효율적인 통합 보안 관리 기능을 제공한다.

2장에서는 기존 무선 LAN 공격에 대해 분석하고 3장에서는 기존 시스템에 대해 고찰하였다. 4장에서는 제안한 시스템에 대한 구조 및 개발 결과를 제시하였으며, 5장에서는 실험 결과와 성능에 대한 비교 평가를 수행하였다.

II. 무선 LAN 공격에 대한 대응방안

1. 무선 LAN의 취약성

무선 LAN은 AP와 무선랜 네트워크 어댑터(WNIC : Wireless Network Interface Card)로 구성된다. AP는 유선 네트워크에 접속되어 무선 사용자들의 트래픽을 중계하는 역할을 담당하는 장비이고 WNIC은 해당 노드(STA : Station Node)에서 AP로 접속하기 위한 네트워크 인터페이스를 담당하는 장비이다. 무선망 보안상의 문제점은 바로 AP와 WNIC간에서 발생한다. AP와 WNIC간 통신은 위에서 언급한 대로 무선 구간을 이용하기 때문에 전파 도달 거리에 있는 모든 무선랜 장치들은 해당 전파를 수신할 수 있게 된다[7].

Wireless LAN 환경의 취약점은 많은 문제점을 안고 있다. Wired LAN에서는 물리적으로 연결된 단말들이 CSMA/CA 방식으로 무선 매체에 대한 접근 제어 기능을 수행하지만, Wireless LAN을 통한 IEEE 802.1x 프레임은 기본적으로 브로트 캐스팅 망이므로 AP의 비콘(beacon) 수신영역 내에 있는 모든 단말들은 다른 사람의 송수신 데이터 내용을 청취할 수 있다. 즉, 무선망 공격자는 일단 접속할 AP를 찾은 경우 해당 AP로의 접속은 별도의 절차 없이 이뤄진다[8].

따라서 AP에 접속한 후 Ethereal이나 Kismet Wireless 등과 같이 인터넷상에서 쉽게 구할 수 있는 패킷 스니퍼 프로그램 등을 이용해 ARP 패킷이나 DHCP 패킷 등을 스니핑할 수 있다. ARP 패킷을 분석하면 현재 해당 AP에서 사용하는 사용자들의 IP 주소가 보이게 되므로 이를 이용해 IP를 도용할 수 있다.

그림 1. 무선망에서의 패킷 스니핑 방법

위 [그림 1]은 무선망에서 패킷을 스니핑하는 방법을 보인다. 불법적인 AP를 설치하여 트래픽에 대한 수집 과정을 수행할 수 있다. 무선 패킷 스니핑을 하기 위해서는 AiroPeek 등의 공개 소프트웨어를 사용할 수 있다. 패킷 스니핑을 통해 암호화를 하지 않는 응용 프로그램들(예를 들어 웹 사이트 로그인 데이터, 웹 메일 로그인, 혹은 POP3 이메일 계정 등)의 ID와 패스워드를 알아 낼 수 있다. 만일 암호화가 이뤄진 경우라도 취약점이 알려진 경우라면 수집한 패킷을 이용해 오프라인에서 전수공격(Brute-Force Attack)이나 사전 공격(Dictionary Attack) 등을 통해 ID와 패스워드를 알아 낼 수도 있다.

IEEE 802.1x 기반 무선 LAN에서는 동일한 AP에 접속되어 있는 무선 클라이언트에 대해서 유선 네트워크를 통하지 않고서도 접속 또는 공격이 가능하다. AP의 역할은 일종의 허브와 비슷한 역할을 수행하는데 동일 AP에 접속된 클라이언트끼리의 통신은 AP에서 바로 중계하는 경우가 많아서 직접적인 공격의 대상이 될 수 있다. 또한 일반적으로 서버보다는 클라이언트에 대한 방어가 허술한 경우가 많아 개인 정보 유출이 쉽게 이뤄질 수 있다.

무선 LAN 공격 기법에 대한 고찰을 통해 취약점을 보완할 수 있는 기법을 도출할 수 있다.

2. 무선 LAN 공격 기법

악의적인 사용자들에 의해서 사이버 공격 기법은 날로 다양해고 있으며, 해킹 기법의 발달로 자동화, 지능화 된 해킹 툴이 공개적으로 유포되어 국내외 해킹 발생빈도는 급격히 증가하고 있는 추세이다. 특히 네트워크의 취약

점이 지속적으로 증가하고 있으며 웜바이러스와 같은 치명적인 공격에 의해 네트워크 서비스를 마비시킬 수 있는 DDoS 공격이 급증하고 있는 가운데 무선 네트워크상에서의 무선랜 공격은 아래 [그림 2]와 같이 수동적 공격(Passive Attack), 능동적 공격(Active Attack) 및 불법 AP(Rogue AP)를 통한 공격으로 분류할 수 있다.

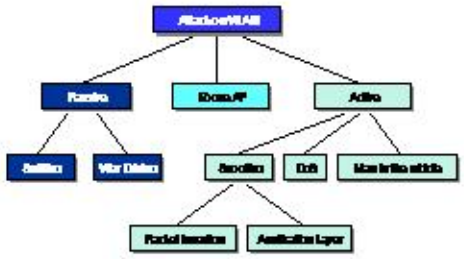

그림 2. 무선랜 공격 유형

2.1 Passive 공격

Passive 공격의 목적은 AP의 MAC, SSID, Channel, 제조사, WEP 설정여부, 설치 위치 정보를 얻기 위함이다. 3가지 방식의 프로그램들이 있는데 패킷을 캡쳐하는 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 시스템이 있다.

2.2 Rogue AP를 통한 공격

Rogue AP란 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 신경쓰지 않은 채 AP를 연결하여 Ad-hoc 네트워크를 구성한다면 더욱 위험하게 되고 비인가자에 의한 네트워크 대역폭 낭비를 불러올 수도 있다.

2.3 Active 공격

Active 공격의 목적은 정보 수집 보다는 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 유도할 수도 있다. 또한 아래 [그림 3]과 같이 WLAN-Jack 기법을 통해 공격자는 피해시스템의 MAC 주소로 스푸핑하여 세션을 가로채는 기법을 보이고 있다.

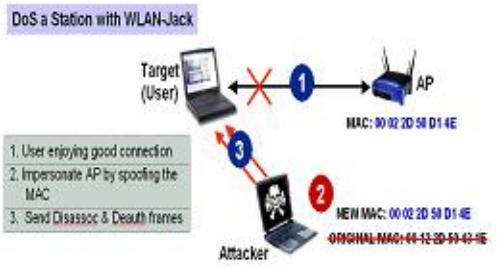

그림 3. WLAN-Jack 기반 세션 가로채기 기법

3. 대응방안 : Wireless IDS/IPS

Wireless IDS/IPS 기능을 제공하기 위해 수행된 기존의 관련 연구 결과는 AirMagnet[10], AirDefense[11] 등이 있다. Airmagnet 센서는 SQL DB를 기반으로 WLAN 관리 및 모니터링 기능을 수행한다. Rogue AP 탐지 및 추적 기능을 제공하며 DoS 공격에 대한 대응을 통해 무선 네트워크에 대한 안전성 확보를 목적으로 하고 있다.

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. 또한 일반적으로 리눅스 운영체제를 기반으로 공개 소프트웨어 형태로 개발되어 현재 활발한 연구가 진행되고 있다. 현재까지 개발된 기존의 주요 시

스템에 대해 고찰하면 다음과 같다.

III. 기존 시스템에 대한 고찰

1. Airmagnet Sensor

Airmagnet사의 Distributed는 현재 나와 있는 것들 중에 최고의 분산 무선 모니터링 시스템으로 무선 센서들이 공중에서 데이터를 캡처해서 분석하며, 중요한 보안 및 성능 이벤트들을 중앙의 관리 시스템으로 보고해 준다[5]. [그림 4]와 같이 Airmagnet 기반 중앙 관리 시스템은 보고된 로그나 기타 정보를 통해 네트워크의 불법적인 침입과 등록되지 않은 AP의 접근을 판별하여 접근을 제한하고 공격들을 차단한다[10].

그림 4. Airmagnet의 Distributed 구조

2. AirDefence Guard

AirDefense사의 AirDefense Guard는 분포된 센서와 서버 설비들로 이루어져 있다. 원격 센서들은 모든 WLAN 활동을 모니터하고 서버 장비로 보고함으로써 실시간 트래픽 분석을 할 수 있도록 802.11 AP 근처에 위치한다. 센서들로부터 보고된 실시간 트래픽 분석을 통해 불법적인 침입에 대한 탐지와 차단기능이 가능하고, 보고된 로그정보를 가지고 침입이라 판단되는 유사한 트래픽의 접근을 막음으로써 내부의 네트워크를 보호할 수 있다[11]. [그림 5]와 같이 AirDefense에서 제시하는 Wireless IPS는 정책 기반 IDS/IPS 시스템으로 네트워크에 대한 관리, 성능 및 안전성을 설정하며 WLAN 세션에 대한 보안 기능을 제공한다.

그림 5. Airdefense사의 Airdefense Guard 구조

3. RFprotect

Network Chemistry사의 RFprotect의 Sensor들은 모든 WLAN 활동을 모니터하고, 이후에 핵심적인 데이터 요소들의 모든 정보를 분석하고 추출한다. 이 추출하여 얻은 자료는 매우 적은 네트워크 대역폭을 사용하여 실시간으로 서버 엔진에 보내진다[12].

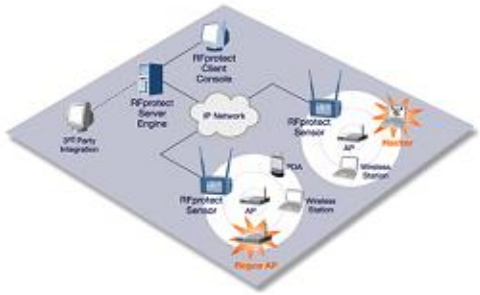

그림 6. Network Chemistry사의 RFprotect 구조

[그림 6]에서 RFprotect 기반 서버 엔진은 모든 센서, 그리고 전체 네트워크(WLAN)의 실시간 데이터베이스로부터 자료를 연관지어가며, 그 후에 모든 탐지 알고리즘들을 수행하는 것으로 안전과 이행 변칙을 식별하게 된다. 공격탐지 또는 운용상의 경보(alarm)가 되는 새로운 경고(alert)들은 각 센서의 하부가 아닌 서버 위에 단순히 로드시키고 이러한 과정을 통해 높은 범위성과, 정확성을 보장하고, 관리자의 편리를 도모할 수 있게 된다.

4. 기존 시스템의 문제점

기존 시스템들은 공통적으로 무선 네트워크 환경에서 별도의 인증을 위해 RADIUS 서버를 필요로 한다. 개별

적으로 안전성을 확보하기 위해 VPN을 필요로 하기도 하며, 이기종간의 AP들에 대한 연결 및 관리 방식을 지원하지 않는다. 또한 무선 네트워크에 대한 모니터링을 위해 AP와 서버간 네트워크의 잦은 연결 설정이 필요할 수도 있다. 따라서 무선 트래픽에 대한 효율적인 침입탐지 및 대응에 문제점을 보인다.

아래 [그림 7]과 같이 기존 시스템에서 AP의 기능은 각 스테이션들로부터 무선을 통한 연결만을 설정할 뿐이고, 차단기능은 AP와 서버사이에 위치하는 IPS 시스템에서 하도록 되어 있다. 기존의 AP와 별도로 무선 트래픽에 대한 센서 기능을 수행하는 시스템을 두고 여기에서 수집된 정보를 서버로 전송하는 구조이기 때문에 무선 공격에 대한 실시간 모니터링 및 효율적이면서 능동적인 대응을 보이지 못하고 있어서 이에 대한 개선이 필요하다.

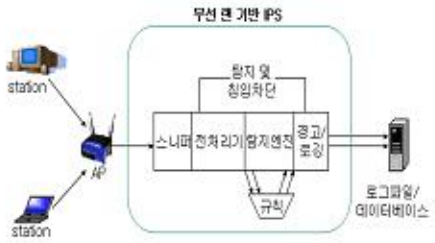

그림 7. 기존의 무선랜 기반 IPS

5. AP 기반 경량화된 Wireless IDS 필요

본 연구에서 제안한 시스템은 IPS의 일부 기능을 AP로 이전하여 AP를 통해 전달되는 트래픽에 대한 실시간 모니터링을 지원한다. AP에 과부하로 인한 침입 차단기능의 저하를 막기 위해 AP에 Snort_inline 기반의 IPS 모듈 중에서 인증과정과 관련된 전처리기 과정을 수행하도록 설계할 필요가 있다. 무선 환경에서 침입자들의 내부 네트워크로의 접근을 위해 우선시 되어질 수 있는 공격으로 DoS 공격의 일종인 Auth/De-auth flood attack과 MAC Spoofing Attack으로 인한 불법적인 침입에 대한 공격을 차단하기 위해 경량형 모듈을 내장하도록 하여야 한다.

아래 [그림 9]과 같이 AP를 통하여 유입되는 패킷에 대한 분석은 우선 중앙의 IPS 엔진에서 처리하게 되며, IPS 엔진은 AP로부터의 데이터와 로그정보를 이용하여 침입에 대한 관리 및 대응 기능을 제공하도록 설계 및 구현되어야 한다.

그림 8. 경량화된 IPS 기능을 탑재한 AP

IV. 제안한 무선 AP 기반 임베디드 형태의 유해 트래픽 침입탐지/차단 시스템

제안하는 시스템은 네트워크상에서 전송되는 트래픽에 대한 모니터링 기능을 수행하게 된다. 특히 AP를 통해 전송되는 트래픽에 대한 모니터링 기능을 통해 패킷 필터링 및 차단 기능을 제공하는 것을 목적으로 한다. 따라서 Wireless IPS 시스템 구성을 위해서는 AP가 직접 IPS 센서(Sensor) 기능을 수행하여 무선 트래픽에 대한 모니터링 기능을 수행하게 된다.

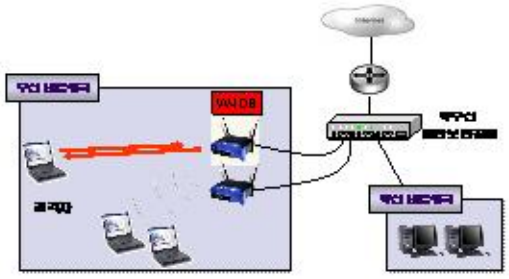

그림 9. W-IDS 시스템 구성도

무선 패킷에 대한 스니핑, 변조 및 조작 등을 탐지하고, AirJack 등의 DDoS 공격에 대해 AP 단에서 사전에 탐지/차단하는 기술을 제공해야한다. 구체적으로 패킷 스니핑, 룰 기반 침입탐지/차단 기능을 제공하는 임베디드 형태의 AP 통합형 IPS 시스템을 개발하였다. 또한 AP는 유무선 통합형 보안 장비와 직간접으로 연결 되어

있으며, 무선 네트워크 상의 트래픽을 분석하여 트래픽 정보와 alert 정보를 유무선 통합형 보안장비로 전송한다. 전체적인 시스템 구성도는 아래 그림과 같다.

1. 개발 시스템 환경

현재 대부분의 네트워크 환경에서 무선이 도입되었지만, AP(Access Point) 에서 해킹 공격을 탐지하지는 않는다. 따라서 본 연구에서는 최근 점차적으로 무선랜과 관련된 공격들이 증가되고 있는 시점에서 무선 AP 기능에 패킷 필터링과 네트워크 침입탐지 기능을 내장한 AP를 설계하고자한다.

무선랜 공격 프레임은 무선 AP에서만 탐지할 수 있으므로 아래 [그림 9]와 같이 firmware가 공개되어 있는 Linksys WRT54G(S) 장비를 선택하여 기능을 추가하는 방법을 사용하였다.

그림 10. 무선 AP(Linksys WRT54G(S))

기본 linksys firmware가 설치되어 있는 경우는 웹관리화면으로 접속하여 OpenWRT firmware (linux 2.4.30)를 설치하였다.

유무선 통합 장비에서 무선 관련 모든 네트워크 트래픽을 모니터링할 수 있도록 W-IDS에서 발생한 802.11 b/g level 2 frame 로그를 유무선 통합형 보안 장비로 전송한다.

2. 개발 시스템 구조

W-IDS 시스템의 내부 구조는 아래 [그림 11]과 같이 Listener, Real-time Analysis 및 Alert Interface 등 크게 세부분으로 구성된다. Listener는 802.11 b/g channel을 hopping 하여 모든 네트워크의 패킷을 수집한다. 그리고, Level 2의 무선 트래픽을 모니터링하고 유무선 통합장비로 네트워크 트래픽 정보를 전송한다. Listener에서 수집된 무선 패킷들은 real-time analysis 부분에서 침입과 연관된 패킷여부를 실시간 분석을 수행한다. 만약 alert가 발생하면 alert interface에서 유무선 통합형 보안 시스템으로 로그를 전송한다.

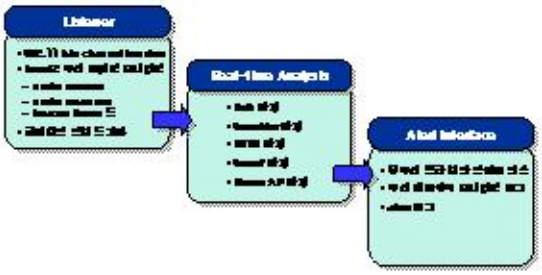

그림 11. W-IDS 소프트웨어 구조

무선랜 공격 프레임은 무선 AP에서만 탐지할 수 있으므로 firmware 가 공개되어 있는 Linksys WRT54G(S) 장비를 선택하여 기능을 추가하는 방법을 사용하였다. 무선 관련 모든 네트워크 트래픽을 모니터링할 수 있도록 W-IDS에서 발생한 802.11 b/g level 2 frame 로그를 유무선 통합형 보안 장비로 전송하는 기능을 수행한다.

AP에 임베디드 형태로 개발된 무선 유해 트래픽 침입탐지/차단 모듈 구성은 아래 [그림 12]와 같다. 제안한 AP 시스템에서는 무선 패킷를 수신하게 되면 패킷에 대한 분석을 통해 트래픽에 대한 유해 여부를 확인하게 된다. 그리고 공격 트래픽에 대해서는 Alert 메시지를 생성하여 통합 모듈로 전송하는 기능을 수행한다.

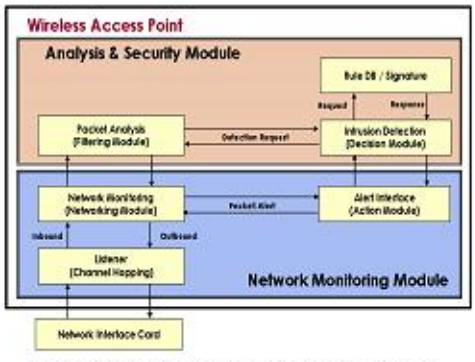

그림 12. 침입탐지 기능을 제공하는 AP 구조

3. W-IDS 내부 공격 탐지 모듈

W-IDS 모듈은 네트워크 모듈과 보안 모듈로 구분 짓는다. 네트워크 모듈에는 네트워크 모니터링 모듈이 있고 보안 모듈에는 rogue AP 탐지 모듈과 spoof/DoS/Stumbler/MITM 탐지 모듈로 구성되어 있다.

3.1 네트워크 모니터링 모듈

네트워크 모니터링 모듈은 passive 형태의 sniffiing을 수행하고 모든 네트워크 패킷을 탐지하는 monitoring mode로 802.11 b/g 패킷을 수집한다. SSID beacon frame을 전송하지 않는 숨겨진 AP 네트워크는 클라이언트의 AP 접속 시 SSID를 모니터링 하여 탐지한다. 수집된 패킷들은 보안 모듈로 전달한다. 주기적으로 유무선 통합장비의 무선관련 환경설정 변경을 검사하여 동기화 시킨다.

3.2 Rogue AP 탐지 모듈

Rogue AP 탐지 모듈은 네트워크 모니터링 모듈로부터 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 탐지 되면 alert 로그를 유무선 통합장비로 전송한다.

3.3 Spoof/DoS/Stumbler/MITM 탐지 모듈

Spoof/DoS/Stumbler/MITM 탐지 모듈은 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. Man-in-the-middle 공격 탐지는 AP의 channel 변경여부를 확인하여 탐지한다. 이렇게 탐지된 alert 로그들은 유무선 통합장비로 전송한다.

4. 무선 AP 통합 보안 관리 시스템 구조

유무선 통합형 보안 시스템은 [그림 13]과 같이 유무선 네트워크로 유입되는 일반적 해킹 공격에 대한 차단과 무선 네트워크에만 존재하는 해킹 공격에 대한 알람을 제공하는 시스템으로 방화벽의 일반적인 기능인 패킷 필터링 기능을 수행하고 이를 통과한 패킷에 대하여 inline 방식으로 해킹 패턴을 검사하고 차단하는 IPS 기능을 구현하였다.

W-IDS로부터 수신된 alert 및 무선 네트워크 트래픽 로그를 웹에서 실시간 로그를 볼 수 있으며 W-IDS 환경설정 정보를 관리하는 기능을 구현하였다.

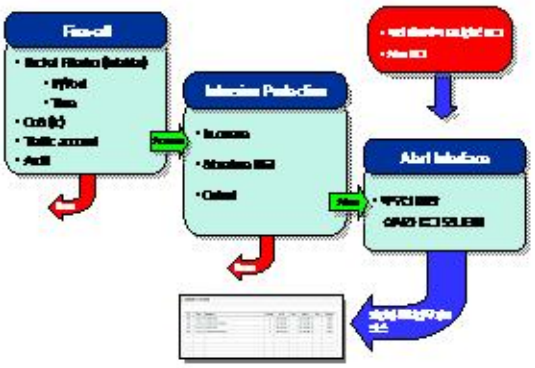

그림 13. 무선 AP 통합 보안 관리 시스템 구조

유무선 통합형 보안시스템 모듈은 네트워크 모듈과 보안 모듈로 구분 짓는다. 네트워크 모듈에는 Bridging/Route 모듈과 네트워크 모니터링 모듈이 있고, 보안 모듈에는 Firewall 모듈과 IPS 모듈로 구성되어 있다.

Firewall은 수신된 패킷을 IP/Port, Time에 근거하여 패킷 필터링을 수행한다. 성능향상을 위하여 IPS 검사가 필요한 filtering 규칙에 대해서만 IPS로 패킷을 전달한다. 부가적으로 대역폭 관리기능과 감사기능을 규칙에 적용할 수 있도록 되어 있다.

Intrusion Protection은 패킷 필터링으로부터 전달된 패킷을 signature 규칙과 비교하여 경고를 발생하거나 차단한다. 발생된 로그는 Alert Interface에 의해서 처리된다.

Alert Interface는 IPS alert 로그, W-IDS의 alert 로그, 무선네트워크 트래픽 로그정보를 분석 및 가공하여 관리자의 웹페이지에 있는 Flash로 작성된 실시간 로그 뷰어로 전송한다.

5. 전체 개발 시스템 구조

앞에서 제시한 AP에서의 침입탐지 모듈과 이에 대한 통합 형태의 관리 구조에 대해 전체적으로 제시하면 아래 그림과 같다.

본 연구에서 개발한 시스템인 경우 AP 기반 무선랜에서 급속도로 확산되고 있는 무선 공격에 대한 관리 및 모니터링 기능을 제공하며, 통합 보안 관리 시스템을 통해 전체 망에 대한 보안 관리 기능을 제공하게 된다.

아래 [그림 14]는 크게 (a) AP를 중심으로 무선 트래픽에 대한 침입탐지 기능을 수행하는 부분과 (b) 웹 중심의 통합 유무선 관리 시스템으로 구성된다.

(a) 부분과 관련해서는 4.2절의 [그림 12]에서 제시한 바와 같이 AP에서는 트래픽에 대한 모니터링 및 분석 기능을 수행하고 만일 공격에 해당하는 트래픽이 있을 경우 이를 유무선 통합 시스템으로 전송하는 기능을 수행한다. AP 부분은 네트워크 모니터일 부분과 침입탐지 모듈로 나뉘어 무선 트래픽에 대한 모니터링을 수행하게 된다.

(b) 부분과 관련해서는 4.4절의 [그림 13]에서 제시한 바와 같이 AP로부터 전달받은 정보와 기존의 유선 트래픽에 대해 필터링 및 침입탐지/차단 기능을 수행하는 부분으로 시스템 관리자 및 사용자는 웹 인터페이스를 이용하여 AP로부터 전송받은 로그 정보를 사용하여 실시간으로 네트워크 트래픽을 모니터링하는 시스템 구조를 보인다.

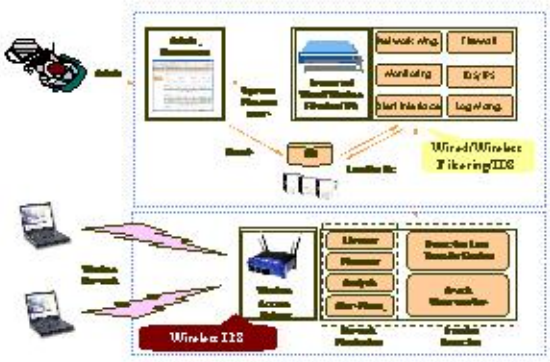

그림 14. 전체 시스템 구조

V. 실험 및 결과 분석

1. 개발 시스템 실험 결과

본 연구에서는 [그림 15]와 같이 우선 무선랜 환경에서 SYN Flooding 패킷을 생성하여 네트워크에 대한 공격을 모의 실험하였고 본 연구를 통해 개발한 시스템을 통해 무선 네트워크 공격이 탐지 및 차단되는지를 실험하였다. 실험 결과 무선랜을 통한 공격을 사전탐지하고 이에 대해 대응하는 것을 확인할 수 있었다.

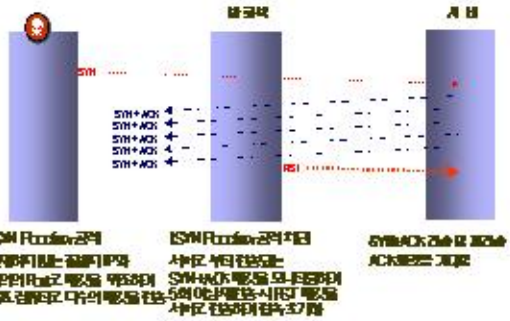

그림 15. SYN Flooding 공격에 대한 실험

SYN Flooding 공격 뿐만아니라 본 연구에서는 아래 [그림 16]과 같이 통합보안시스템을 통해 무선망에 대한 침입탐지/차단 정책 설정을 통해 무선망에 대한 침입탐지/차단 기능을 제공할 수 있었다.

그림 16. 무선 LAN 보안 정책 설정

제안한 시스템을 통해 무선망에 대한 침입탐지/차단 결과를 모니터링 할 수 있었다. 아래 [그림 17]과 같이 대

학 캠퍼스망에 구축된 AP에 대한 관리 및 침입탐지 기능을 수행하여 보다 안전한 대학내 캠퍼스망을 구축할 수 있었다.

실험 결과 대학 무선 캠퍼스망에서 발생하는 트래픽에 대한 모니터일 뿐만아니라 무선 트래픽에 대한 공격 탐지 및 차단 기능을 수행하는 것을 확인할 수 있었다.

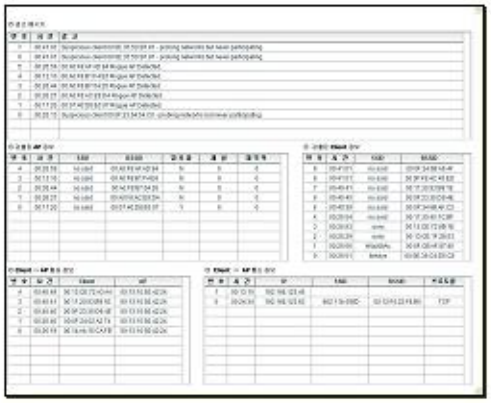

그림 17. 무선 AP에 대한 침입탐지/차단

2. 비교 분석

[표 1]과 같이 본 연구를 통해 개발한 IPS 시스템과 기존의 IPS 시스템의 성능의 비교를 예측치로 비교하였다. 비교하고자 하는 대상들의 비교 분석은 뉴욕의 Syracuse University의 리얼월드 랩에서 진행된 자료를 기반으로 작성하였다[9]. 기존 시스템들의 경우는 AP를 연결하기 위한 센서라는 부분이 존재하고, 스테이션들은 "AP->센서->엔진->내부 네트워크"의 4단계를 거쳐 네트워크로의 연결이 된다. 하지만 제안한 시스템의 경우는 "IPS 탑재한 AP->엔진->내부 네트워크"의 총 3단계를 거치므로, 무선 네트워크의 흐름을 더욱 원활하게 할 수 있다.

또한 [표 1]에 제시된 것과 같이 본 연구에서 제시한 시스템은 기존 연구와 비교한 결과 불법 AP에 대한 탐지 결과를 제시하며, MAC 스푸핑 공격 및 Auth-Flooding 공격 등에 대해 대응하는 것을 확인할 수 있었으며, AP는 통합 장비와 연계되어 있어서 무선을 통한 네트워크 공격이 발생할 경우 이를 차단할 수 있었다.

결국 본 연구에서 개발한 시스템을 기존의 시스템과 비교하였을 경우에 공격 차단 기능을 제공하였으며 AP를 기반으로 유무선 네트워크에 대한 모니터링 기능을 제공하였다. 따라서 최근 급속도로 확산되고 있는 무선망에 대한 효율적인 보안 관리 기능을 제공할 수 있었다.

VI. 결 론

본 연구에서는 임베디드 형태의 침입탐지/차단 시스템을 AP(Access pointer)에 탑재하여 이상 무선 트래픽에 대하여 탐지 및 차단할 수 있는 통합형 무선 침입탐지/차단 시스템을 설계 및 구현하였다. 또한 AP를 관리하는 서버로 구성되는 유무선 통합형 보안시스템을 제안함으로써 유무선 공격 시그니처 기반으로 유해 트래픽을 탐지/차단할 수 있으며, 이는 단순히 공격을 차단하는 것뿐

표 1. 기존 시스템과의 성능 비교 평가

기능 / 시스템	구성	공격 탐지 방식	공격 탐지 모듈	Rogue AP 탐지	MAC Spoof 탐지	Auth/Deauth 탐지	공격 차단 기능	AP 기반 트래픽 모니터링	통합형 보안 관리 시스템
AirMagnet Sensor[10]	AP, 모니터링 센서, 컨트롤러, 서버	AP□센서□서버 전송후 탐지	서버	□	-	-	□	□	-
AirDefense Guard[11]	AP, AP 연결 센서, 서버 및 모니터링 툴	AP□연결센서□서버 전송/탐지	서버	□	-	-	□	□	-
RFprotect System[12]	AP, 연결 센서, 모니터링 클라이언트 및 통합관리 서버	AP□클라이언트□서버전송후 탐지	서버	□	□	□	-	□	□
제안한 시스템	AP, 통합관리 서버	AP탐지□서버 전송□차단	AP 및 서버	□	□	□	□	□	□

□ : 지원함 - : 명확히 판단할 수 없음 □ : 지원하지 않음

만 아니라 탐지 결과들을 통하여 잠재적인 위험 요소를 분석하여 이를 관리자에게 알려주어 대학내 무선 캠퍼스망을 보다 안전한 네트워크 형태로 구성 가능하였다.

참 고 문 헌

[1] 전용희, "침입방지시스템(IPS)의 기술분석 및 성능평가 방안", 정보보호학회지, 제15권, 제2호, pp.63-73, 2005.

[2] 조현정, "차세대 네트워크 보안기술 기반의 침입방지시스템", 정보과학회지, 제23권, 제1호, pp.21-26, 2005.

[3] 정보흥, 김정녀, 손승원, "침입방지시스템 기술 현황 및 전망", ETRI IT정보센터, 주간기술동향 1098호, 2003.

[4] 전원용, 김은희, 신문선, 류근호, "점진적 연관 규칙을 이용한 침입탐지 시스템의 오경보 패턴 분석 프레임워크 설계", 한국정보과학회, Vol.31, No.2, 2004.

[5] http://www.enterpriseitplanet.com/security

[6] 강유, *스노트2.0 마술상자*, 에이콘 출판사, 2003.

[7] Matthew Gast, *802.11 Wireless Networks: The Definitive Guide*, OReilly, Apr, 2002.

[8] Bruce Potter, *802.11 Security*, OReilly, Dec., 2002.

[9] Jo, Wiley and Sons, *Building Secure Wireless Networks with 802.11*, Jan, 2003.

[10] http://www.airmagnet.com

[11] http://www.airdefense.com

[12] http://www.networkchemistry.com

[13] http://snort-wireless.org/

[14] http://www.snort.org/

저 자 소 개

이 형 우(Hyung-Woo Lee) 정회원

- 1994년 2월 : 고려대학교 컴퓨터학과 (이학학사)
- 1996년 2월 : 고려대학교 컴퓨터학과 (이학석사)
- 1999년 2월 : 고려대학교 컴퓨터학과 (이학박사)
- 1999년 3월 ~ 2003년 2월 : 천안대학교 정보통신학부 교수
- 2003년 3월 ~ 현재 : 한신대학교 컴퓨터정보소프트웨어학부 교수

<관심분야> : 정보보호, 네트워크보안, 무선랜, 침입탐지/차단, 컨텐츠 보호

최 창 원(Chang-Won Choi) 정회원

- 1990년 2월 : 고려대학교 컴퓨터학과 (이학학사)
- 1992년 2월 : 고려대학교 컴퓨터학과 (이학석사)
- 1995년 8월 : 고려대학교 컴퓨터학과 (이학박사)
- 1996년 3월 ~ 현재 : 한신대학교 컴퓨터정보소프트웨어학부 교수

<관심분야> : 네트워크, 네트워크보안, 멀티미디어, 네트워크 성능평가