韓國 컴퓨터情報學會 論文誌
第11卷 第6號, 2006. 12

2006-11-6-2-9

캠퍼스 망에서의 무선 트래픽 침입 탐지/차단을 위한 Wireless Sensor S/W 개발

최 창 원*, 이 형 우**

Development of the Wireless Sensor S/W for Wireless Traffic Intrusion Detection/Protection on a Campus N/W

Chang-Won Choi *, Hyung-woo Lee **

요 약

무선 네트워크의 확대로 무선 트래픽에 대한 침입 탐지/차단 시스템의 필요성이 강조되고 있다. 본 연구에서는 캠퍼스 망에서 무선망을 통하여 유선망을 공격하는 트래픽들을 탐지하고 분석된 결과를 통합적으로 관리하여 공격 트래픽을 효과적으로 차단하는 시스템을 제안한다. 제안하는 시스템은 무선 트래픽의 침입 탐지를 위해 기존의 W-Sensor 기능을 소프트웨어 형태로 개발하고 탐지된 공격 트래픽을 차단하는 통합 보안 관리 시스템 W-TMS를 개발하여 연동하게 하였다. 개발된 W-Sensor SW를 통해 무선 트래픽의 공격에 대해 효율적인 탐지 기능을 수행하고 변화되는 공격 유형에 대해 신속하게 대응할 수 있다. 또한 노트북 등에 SW를 설치함으로써 기존 AP 기반 시스템에 비해 이동성을 증가시킬 수 있다.

Abstract

As the wireless network is popular and expanded, it is necessary to development the IDS(Intrusion Detection System)/Filtering System from the malicious wireless traffic. We propose the W-Sensor SW which detects the malicious wireless traffic and the W-TMS system which filters the malicious traffic by W-Sensor log in this paper. It is efficient to detect the malicious traffic and adaptive to change the security rules rapidly by the proposed W-Sensor SW. The designed W-Sensor by installing on a notebook supports the mobility of IDS in compare with the existed AP based Sensor.

▸ Keyword : 무선 네트워크 보안(Wireless Network Security), IDS(Intrusion Detection System), Wireless-Sensor, TMS(Threat Management System)

• 제1저자 : 최창원
• 접수일 : 2006.12.08, 심사일 : 2006.12.19, 심사완료일 : 2006. 12.26
* 한신대학교 컴퓨터정보소프트웨어학부 교수, ** 한신대학교 컴퓨터정보소프트웨어학부 부교수
※ 이 논문은 2006년도 한신대학교 학술연구비 지원에 의하여 연구되었음.

Ⅰ. 서론

초고속 무선 인터넷에 대한 요구가 급성장하면서 기존의 무선랜(Wireless Local Area Network) 시스템이 초고속 무선 공중망의 기반구조로서 그 대안이 되고 있다. 노트북과 PDA를 이용하여 사무실 밖에서 업무를 처리하는 이동 근로자(mobile worker)들의 수가 증가하면서 이들을 대상으로 인터넷 접속 서비스를 제공하는 무선랜 서비스 용도로도 활용되고 있다. 또한 가정 및 소규모 사무실의 무선랜 AP 설치 급증하고 있어 일반 가정, 소규모 단독 사무실, 대학 등 사용 환경들도 광범위해지고 있다.

무선랜 사용이 증가되면서 보안 문제도 자연스럽게 대두되고 있으며 특히 무선 인터넷 환경 내에 전문 AP 운영 체계가 미흡하여 무선 AP는 MAC Spoofing 공격, 해킹 및 바이러스 공격 등에 노출되어 있고, 최근 DDoS등 무선랜 AP를 대상으로 하는 바이러스가 급증, 피해사례 속출하고 있다. 이러한 문제들을 해결하기 위해 AP를 기반으로 하는 IDS/IPS 시스템들을 개발하여 무선 트래픽의 침입을 감지하고 차단하는 연구들이 활발하게 진행되어 왔다[2].

무선 랜과 관련된 기술이 발전하고 전송 속도도 빨라지고 있지만 아직까지는 속도 문제나 보안 문제 때문에 많은 대학 캠퍼스망은 유선망과 무선망을 혼용하여 사용하고 있는 것이 현실이다. 특히 무선망에서의 보안상 가장 큰 취약점은 Rogue AP나 AP 기능이 지원되는 무선랜 카드로 인한 접근 통제의 우회 가능성이다[4]. 이 경우 기존의 유선망을 공격하여 안정된 네트워크 운영을 기대할 수 없다.

이러한 문제점들을 해결하기 위해 무선망을 통한 유선망의 공격 탐지 기능을 수행하는 센서(Sensor)를 AP에 탑재하여 침입을 차단하여 왔다. 하지만 새로운 침입 유형이 발견되고 이에 대한 대응 방법이 개발되면 센서가 탐재된 모든 AP에 대해 수정 내용을 반영해야 하며 하드웨어 형태로 AP에 탑재되어 있기 때문에 AP의 교체에 필요한 경제적 비용 또한 무시할 수 없다. 무선망의 사용자가 증가하고 침입 유형도 다양화되면서 AP의 교체 시기는 빨라질 것이며 빈번한 시스템 변경으로 안정된 대학 네트워크 운영을 기대하기 힘들다. 따라서 센서를 하드웨어 형태의 AP 기반으로 운영하기 보다는 노트북이나 PDA와 같은 무선 단말기에 소프트웨어 형태로 운영하게 되면 다양한 침입 유형의 변화에 신속하게 대처할 수 있고 교체 비용도 AP 기반의 방식에 비해 상대적으로 작다. 아울러 노트북이나 PDA에 설치되기 때문에 센서의 이동성을 높일 수 있고 침입 공격이 빈번한 특정 지역에 대한 탐지를 강화할 수 있다.

본 연구는 대학 캠퍼스 망에서 무선망을 통해 유선망을 공격하는 트래픽의 침입 탐지를 위한 Wireless Sensor SW를 설계하고 개발한다. 제안하는 시스템은 무선망에서 Rouge AP나 AP 기능이 지원되는 무선랜 카드를 이용하여 유선망에 접근하는 트래픽들의 공격을 탐지하는 시스템(W-Sensor)과 W-Sensor의 결과를 실시간으로 전송받아 차단하는 시스템(W-TMS : Threat Management System)으로 구성된다. 제안 시스템을 통해 기존 AP 기반의 센서 기능을 수행하면서도 공격 유형의 변화에 대해신속하게 대응하고 센서의 이동성을 높였다.

본 연구는 2장에서 제안 시스템의 필요성과 기존 무선 IDS/IPS 시스템들에 대해 설명하고 대학 캠퍼스 망에 적용할 시 발생되는 문제점들에 대해 분석한다. 3장에서는 제안 시스템의 설명으로 개발한 W-Sonsor 시스템과 W-TMS 시스템의 기능과 구조, 세부 모듈들에 대해 기술한다. 4장에 제안한 시스템들의 무선 트래픽 침입 감지와 차단 기능을 실험을 통해 수행하고 5장 결론에서는 본 연구의 특징과 활용 방안, 향후 연구 내용들을 기술한다.

Ⅱ. 제안 시스템의 필요성

2.1 Wireless Sensor의 필요성

무선 네트워크가 개방형 네트워크로 발전하면서 네트워크의 취약점이 확대되었으며 유무선 네트워크와 운영 체제의 복잡성 등으로 인해 전체적인 시스템의 보안 취약성이 증대하고 있다. 이에 대한 공격 기법도 점차 고도화되고 있는 가운데 취약성을 이용한 내부 및 외부에서의 공격이 급증하고 있어 이에 대한 대응기술 개발이 다양하게 개발되었는데 능동적인 형태의 트래픽 필터링/차단 기능을 제공하는 무선 IDS/IPS 기술이 점차 중요시되고 있다.

최근 많은 대학 캠퍼스 망이 기존의 유선망에무선망을 혼용하여 운영하면서 기존의 유선 트래픽에 대한 침입 탐지/차단 시스템을 무선 트래픽에 대한 시스템으로 확대, 발전시키고 있다. 하지만 유선 트래픽에 대한 침입 탐지/차단 시스템과 무선 트래픽에 대한 침입 탐지/차단 시스템은 별도로 운영되어 무선망을 통한 유선망의 공격이 발생되는 경우 트래픽을 구별하기 힘들며 이에 따른 대응 방안도 어렵다. 공격 트래픽을 분석해 보면 그림 2.1처럼 공격자에 대

한 IP 정보는 분석할 수 있지만 유선망에 대한 공격인지 무선망에 대한 공격인지 구별하기 힘든 것을 알 수 있다.

Class	Attack Count	Packet Count	Percent
203.252.16.9	5,360,680	5,618,220	67.28%
203.252.22.1	781,068	1,355,055	12.72%
203.252.19.62	269,299	877,029	3.81%
203.251.225.118	130,027	295,860	2.12%
203.251.225.119	124,456	264,717	2.09%
Multiple	45,335	53,241	.74%
203.252.18.6	25,761	25,775	.42%
203.252.45.136	22,872	33,390	.37%
203.252.29.120	21,665	43,569	.35%
203.252.34.89	19,639	35,053	.32%

그림 2.1 대학 캠퍼스 망의 트래픽 분석
Fig. 2.1 Traffic Analysis on Campus N/W

이를 위해 기존의 AP에 주변의 공격자들을 탐지하는 센서(Wireless Sensor)를 설치하는데 기존의 AP에 센서를 하드웨어 형태로 내장하는 방식이 많이 사용되고 있다. 대표적인 제품들로는 Airmagnet사의 Distributed[11], Network Chemistry사의 RF Project[13], AirDefense사의 Guard[12] 등이 있다.

Network Chemistry사의 RF protect의 센서들은 모든 무선망 활동을 모니터하고 핵심적인 데이터 요소들의 모든 정보를 분석하고 추출한다. 이 추출하여 얻은 자료는 매우 적은 네트워크 대역폭을 사용하여 실시간으로 서버에 보내진다. 서버 엔진은 모든 센서, 그리고 네트워크 실시간 DB로부터 데이터들 분석하여 모든 탐지 알고리즘들을 수행하며 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 제공한다.

Airmagnet사의 Distributed는 센서들이 분산되어서 데이터를 수집하고 분석하며, 중요한 보안 및 성능 이벤트들을 중앙의 관리 시스템으로 보고해 준다. 분산된 센서들은 SQL DB를 기반으로 무선망 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. 중앙 관리 시스템은 보고된 로그나 기타 정보를 통해 네트워크의 불법적인 침입과 등록되지 않은 AP의 접근을 판별하여 접근을 제한하고 공격들을 차단하는 기능을 수행한다.

AirDefense사의 AirDefense Guard의 원격 센서들은 모든 무선망 상태를 모니터링하고 서버 장비로 보고함으로써 실시간 트래픽 분석을 할 수 있도록 무선 AP 주변에 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. AirDefense에서 제시하는 무선 IPS는 정책 기반 IDS/IPS 시스템으로 네트워크에 대한 관리, 성능 및 안전성을 설정하며 무선 세션에 대한 보안 기능을 제공한다.

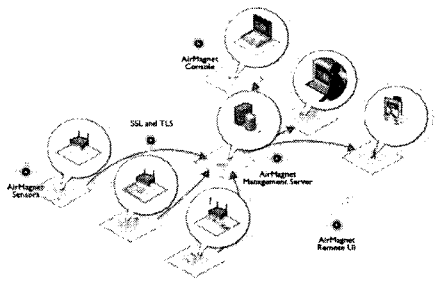

그림 2.3 Airmagnet의 Distributed 시스템
Fig. 2.3 Distributed System(Airmagnet)

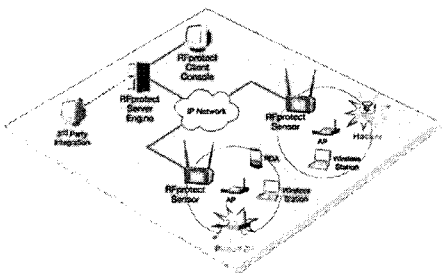

그림 2.2 Network Chemistry사의 RF protect 시스템
Fig. 2.2 RF protect System

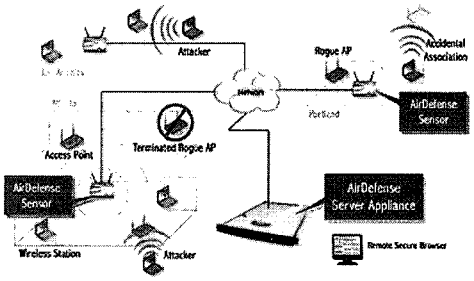

그림 2.4 Airdefense사의 Airdefense Guard 시스템
Fig. 2.4 Guard System(Airdefense)

2.2 기존 연구의 문제점

기존에 연구된 시스템들은 무선망에서만의 트래픽에 대한 침입 감지 및 차단 기능을 제공한다. 또한 센서 기능을 하드웨어 형태로 AP에 탑재하기 때문에 공격 유형의 변화에 대해 능동적으로 대처하기 힘들고 설치된 모든 AP에 대해 변화된 공격 탐지 정보를 변경하여야 하기 때문에 교체 비용 또한 적지 않다. 무선망 사용자가 증가하게 되면 이에 필요한 AP 개수도 증가하게 되는데 기존 시스템으로 센서 기능을 수행하는 경우 안정된 대학 캠퍼스 망을 운영하기 어렵다.

따라서 대학 캠퍼스 망처럼 무선 사용자가 급증하고 다양한 학내 서비스를 제공하기 위해서는 기존 AP에 하드웨어 형태로 센서의 기능을 내장하기 보다는 소프트웨어 형태로 이동성이 높은 노트북이나 PDA에 설치하여 무선 트래픽 공격 변화에 대해 능동적으로 대처하는 시스템 개발이 필요하다.

따라서 본 연구에서는 무선 트래픽 공격의 침입을 AP가 아닌 노트북/PAD 등에서 탐지하는 W-Sensor SW를 개발하고 W-Sensor의 결과를 통해 유해한 무선 트래픽을 차단하는 유무선 통합 보안 관리 시스템(W-TMS)도 함께 개발한다.(그림 2.5)

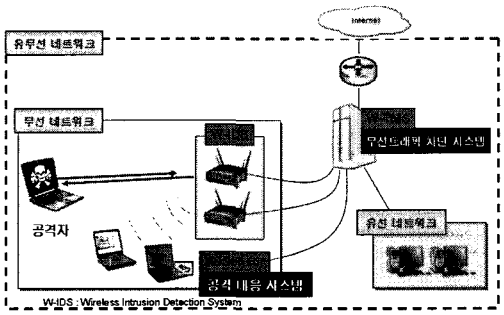

그림 2.5 제안한 무선 트래픽 침입 탐지/차단 시스템
Fig. 2.5 The Proposed W-Sensor/TMS system

III. 제안 시스템 설계 및 개발

3.1 개발 환경

본 연구는 WEP 키를 사용하지 않는 유무선 네트워크에서 무선망을 악용한 해킹 공격을 탐지 및 차단하는데 주 목적이 있다. 핵심 기능으로는 Rogue AP/스테이션 검출 및 격리 기능, DoS 공격 검출 기능, 무선랜 IDS 기능, 무선랜 사용자들을 위한 별도의 접근 통제 기능, Wireless Threat Management로의 센서 기능이다.

센서로서 사용 가능한 무선랜 카드는 Realtek과 Atheros 칩셋을 사용하는 무선랜 카드들로 제한된다. 기존에 리눅스 기반으로 장비화된 무선랜 IDS 시스템들이 있는데 이는 별도의 설치비용과 휴대에 불편한 점이 발생하므로 본 연구는 윈도우즈 기반 시스템에서 구현하였다. 센서가 필요한 대학 연구실이나 사무실에서 기존에 사용하고 있는 시스템에 추가로 무선랜 카드와 소프트웨어만 설치하면 가능하도록 개발하였다.

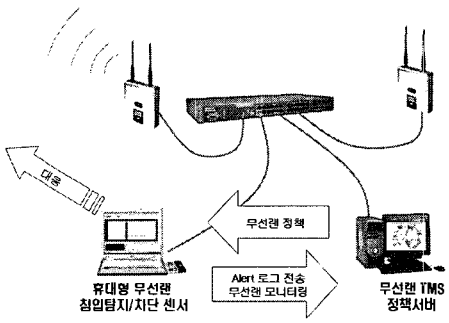

그림 3.1 무선 트래픽 침입 탐지 센서 및 TMS
Fig. 3.1 W-Sensor/TMS system

그림 3.1은 무선 트래픽의 침입탐지/차단 센서 및 TMS의 구성도를 보여주고 있다. 센서는 주위의 무선랜 트래픽을 감시하고 대응하는 역할을 한다. 무선랜 TMS는 기관내에 설치되어 있는 센서들로부터 무선랜을 통한 공격 정보들을 볼 수 있다. 접근 통제 정책을 센서들에게 전달하여 특정 서버로 무선랜을 통한 접근을 차단하도록 하고 있다. 센서들은 stand alone 방식으로도 작동 가능하다.

본 연구에서 개발한 W-Sensor와 W-TMS의 기본적인 침입탐지/차단 엔진 구조는 그림 3.2와 같다.

3.2 Wireless Sensor

3.2.1 시스템 기능 및 구조

Wireless Sensor는 무선 트래픽의 공격에 대응하기 위해 6개의 주요 모듈들로 구성되었다.

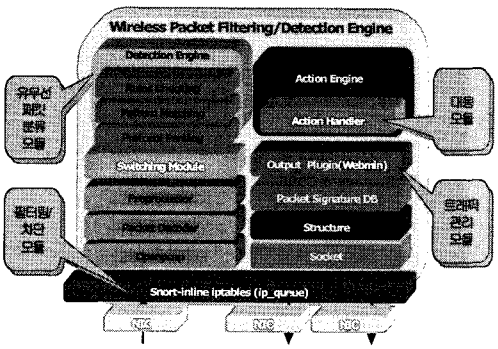

그림 3.2 트래픽 침입탐지/차단 엔진 구조
Fig. 3.2 W-Sensor/TMS Engine Structure

1) 무선랜 패킷 모니터링 모듈

무선랜상의 트래픽을 수집하여 모니터링하는 기능이다. 윈도우즈는 무선랜 프레임을 전달하지 않기 때문에 무선랜 프레임을 수집하기 위해 현재 대부분이 사용 중인 802.11 g를 지원하고 있는 AiroPeek 사의 Peek5.sys 드라이버를 사용하였다. 덤프된 패킷은 802.11 프레임으로 버퍼로 저장된다. 이 버퍼를 이용해서 802.11 헤더를 분석하였다.

2) 무선랜 관리 정보 추출 모듈

덤프된 802.11 헤더를 가지고 관리 프레임, 제어 프레임, 데이터 프레임 등으로 분류하고 관리 프레임과 데이터 프레임을 사용하게 된다. 먼저 모든 패킷들은 AP의 BSSID를 가지고 있으므로 AP의 BSSID를 수집하여 리스트로 정보를 보관하게 된다. 발견된 AP 중에서 Rogue AP 여부도 검사한다. 관리 프레임 패킷을 이용한 DoS 공격도 검출하게 된다. 스테이션 리스트들도 802.11헤더의 정보를 보고 추출한다. 역시 Rogue 스테이션 여부도 검사한다.

3) IP 패킷 공격 탐지 모듈

802.11 헤더 분석 후 남은 IP 패킷을 통해 무선랜을 이용한 유선랜 공격 기법을 검사한다. snort 프로그램을 W-Sensor 프로그램과 같이 컴파일하여 무선랜 카드에서 잡은 IP 패킷을 snort 함수를 호출하여 무선랜 IP 패킷에 대해서만 검사가 가능하도록 하였다. snort도 역시 win32용 소스코드를 사용하였다[1,13].

4) 정책 위반 시스템 격리 모듈

무선 네트워크와 같이 게이트웨이를 우회하여 내부에 침입하는 경우는 In-Line 방식으로는 적용이 불가능하므로 네트워크 말단에 있는 센서에서 수행한다. 하지만 센서는 In-Line이 아니므로 공격 트래픽을 격리하기 위해 상대방에게 TCP RST 패킷을 사용하여 서비스 거부 공격을 수행하였다.

5) 로그 관리 모듈

로그는 로컬 센서에서 발생되는 무선랜 관리와 관련된 로그, 무선랜의 IP 패킷을 IDS로 검사한 로그와 센서와 관련된 로그 등 3 종류로 나누어진다. W-TMS와 연동하기 위해서 선택적으로 원격 로그 기능을 사용할 수 있도록 하였다.

6) 정책 관리 모듈

TMS로부터 처음 실행 시 전달받은 무선랜 접근 통제 정책들을 관리한다. W-Sensor에 접근 통제 정책을 배포하여 실시간으로 접근을 차단하도록 하였다.

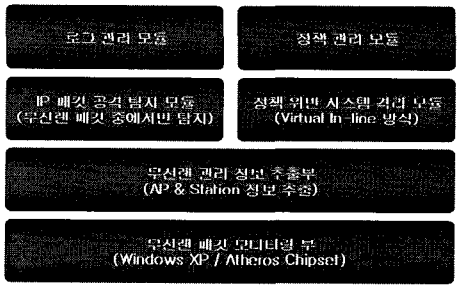

그림 3.3 W-Sensor의 주요 모듈
Fig. 3.3 W-Sensor Modules

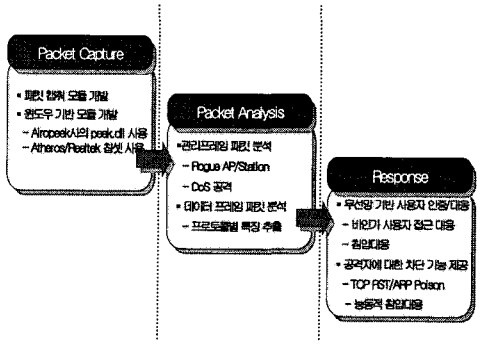

그림 3.4 W-Sensor 시스템 구조
Fig. 3.4 W-Sensor System Structure

그림 3.4는 W-Sensor 시스템의 구조이다. 무선 네트워크상의 패킷들을 수집하여 패킷 분석 단계로 전달된다. 패킷 분석시 수집된 패킷들을 관리 프레임과 데이터 프레임으로 분류하고 관리 프레임인 경우 Rogue AP/스테이션과 DoS 공격인지 판별한다. 데이터 프레임인 경우 프로토콜별로 특징을 추출하여 분석한다. 분석된 패킷별로 무선 네트워크의 유해한 트래픽인 경우 공격에 대한 대응(Response) 기능을 수행한다.

3.2.2 W-Sensor 개발

그림 3.5는 W-Sensor에서 환경 설정 과정이다. 센서 정보를 설정하고 무선랜 어댑터 및 칩셋 설정 기능 등을 수행하게 된다.

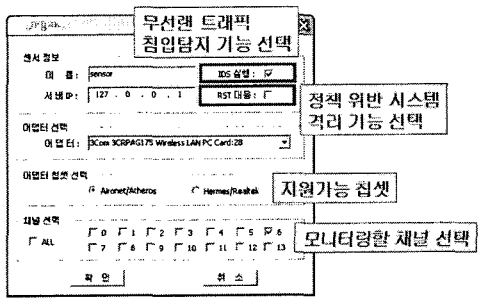

그림 3.5 W-Sensor 환경 설정
Fig. 3.5 Setting W-Sensor Configuration

무선 트래픽에 대한 모니터링은 그림 3.6과 같이 검출된 AP 리스트 출력, 선택된 AP에 대한 실시간 갱신 및 리스트 구성 등을 수행하게 된다. 또한 무선랜 로그 및 침입로그에 대한 표시 기능을 제공한다.

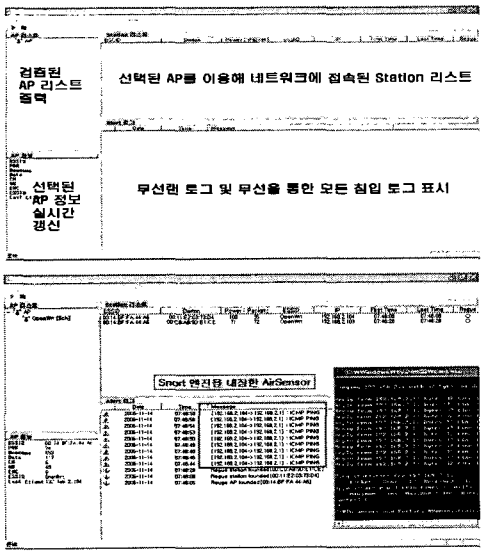

그림 3.6 W-Sensor를 통한 무선 트래픽 탐지
Fig. 3.6 Wireless Traffic Monitoring By W-Sensor

3.3 Wireless TMS

3.3.1 시스템 기능 및 구조

Wireless TMS의 주요 기능은 Policy Manager 기능과 Threat Monitoring 기능이다. Threat Management는 risk를 일정 수준으로 유지하기 위한 제어를 선택하는 것을 의미한다. Policy Manager 기능은 인증 AP 리스트들과 인증 Station 리스트들을 관리하고 무선랜을 통한 접근통제 구역을 설정하는 정책들을 담당한다. 또 센서가 처음 실행될 때 TMS로부터 정책들을 부여받게 된다. Threat Monitoring 기능은 여러 센서들로부터 들어온 무선랜 관리 정보와 침입 탐지된 공격 정보와 센서들의 정보를 네트워크로 전달 받아 화면에 표시한다.

W-TMS의 주요 모듈은 네트워크 모듈과 보안 모듈로 구성된다. 네트워크 모듈에는 Bridging/Route 모듈과 네트워크 모니터링 모듈이 있고, 보안 모듈에는 방화벽 모듈과 IPS 모듈로 구성되어 있다(그림 3.7).

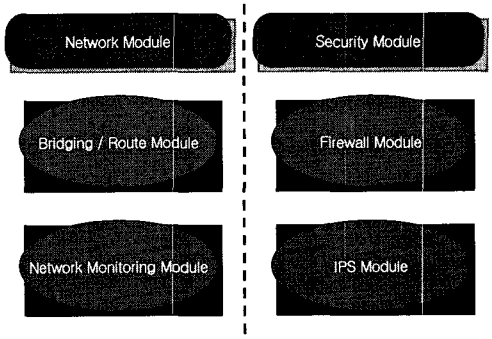

그림 3.7 TMS의 주요 모듈
Fig. 3.7 TMS Modules

1) Bridging / Route 모듈

Bridging/Route 모듈은 네트워크 장비의 가장 기본적인 모듈이다. Bridge와 Route 모드를 동시에 지원할 수 있도록 구성하여 내부 사용자들은 Route 모드로 사설네트워크를 사용하고, 서버들은 Bridge 모드로 NAT 없이 공인 IP를 사용할 수 있도록 하였다. 장비의 포트 위치에 상관없이 공인/사설 네트워크를 사용할 수 있도록 br0 인터페이스로 모든 ethx 인터페이스들을 묶고 br0에 관리용 IP 뿐만 아니라 사설 네트워크의 게이트웨이 IP를 설정하였다.

2) Network Monitoring 모듈

실시간 네트워크 트래픽 정보(TCP/ UDP/ ICMP/CPU /IPS) 제공을 위해 인터페이스에 상관없이 모든 트래픽을 캡쳐하여 대역폭 정보를 관리자의 웹 브라우져로 3초마다 전송한다. 이 프로그램은 TCP/UDP/ICMP 트래픽을 BPS

단위로 누적하는 쓰레드와 3초마다 대역폭 정보를 관리자에게 보내는 쓰레드로 구성되어 있다.

3) 방화벽 모듈

방화벽 모듈은 iptables를 이용하여 시스템의 네트워크 보안을 설정한다. 기본 정책은 INPUT과 FORWARD 체인은 모두 DROP으로 정책을 설정하였다. 사용자 정의 규칙은 br0 인터페이스의 FORWARD 체인에 적용한다. 관리 포인트를 분산하지 않고 한 곳으로 집중하는 방법으로 트래픽 폭주를 막기 위한 대역폭 설정과 IPS 적용까지 규칙 하나로 설정이 가능하도록 하였다. 이는 필요한 경우에만 적용하여 부하를 감소하는 효과도 있다. 기타 기능으로 감사기능과 시간대를 이용한 필터링 기능을 제공한다. 다음은 웹 서비스를 업무시간대(08:00 -21:00)에 3MB로 사용하고자 할 때 적용되는 규칙의 예이다.

```
# /sbin/iptables -I USER_FORWARD 3 -p tcp -s 0.0.0.0/0 --sport
0:65535 -d 0.0.0.0/0 --dport 80 -o br0 -j ACCEPT -m time
--timestart 08:00 --timestop 21:00

# sudo /sbin/tc filter add dev eth0 parent 1:0 protocol ip prio 3
u32 match ip protocol 0x06 0xff match ip dport 80 0xffff flowid
1:7

# sudo /sbin/tc filter add dev eth0 parent 1:0 protocol ip prio 3
u32 match ip protocol 0x06 0xff match ip sport 80 0xffff flowid 1:7
```

4) IPS 모듈

IPS 모듈은 패킷 필터링에서 IPS 검사가 적용된 규칙에 해당하는 패킷에 대해서만 snort_ inline을 이용하여 검사를 수행한다. 현재 적용되는 규칙은 약 3,400여개가 있다. 사용자가 전문적인 지식이 없어서 적용 규칙을 모를 경우를 고려하여 모든 규칙을 하나의 파일로 묶어 해당하는 서비스에 관련된 규칙들만 사용자가 볼 수 있도록 하고 위험도에 따라 분류하였다.

TMS의 구조는 방화벽, 침입 방지, Alert Interface의 세부분으로 구성되어 있다. 방화벽은 수신된 패킷을 IP/ Port, Time에 근거하여 패킷 필터링을 수행한다. 성능 향상을 위하여 IPS 검사가 필요한 차단 규칙에 대해서만 IPS로 패킷을 전달한다. 부가적으로 대역폭 관리기능과 감사기능을 규칙에 적용할 수 있도록 되어 있다.

침입 방지는 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 플래시로 작성된 실시간 로그 뷰어로 전송한다.

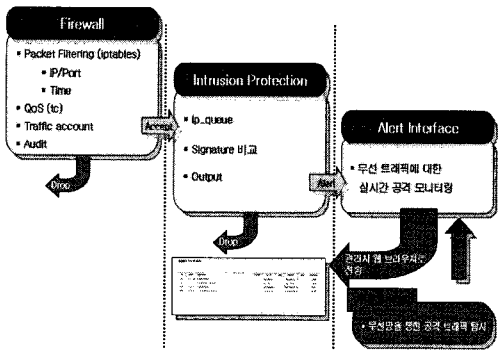

그림 3.8 W-TMS의 구조
Fig. 3.8 W-TMS Structure

3.3.2 W-TMS 개발

W-IDS 및 W-Sensor에 의해 검출된 정보는 W-TMS에게로 전달된다. W-TMS에서는 무선망에 대한 접근 정책을 기반으로 유무선 네트워크에 대한 전체적인 위협관리 및 통합 모니터링 기능을 수행하게 된다. 그림 3.9에서 W-TMS는 Rogue AP에 대한 식별을 위해 인가된 AP에 대한 관리 리스트를 구축하고 있으며 무선랜에 대한 접근 정책을 설정하고 해당 로그를 설정하는 기능을 제공하고 있다.

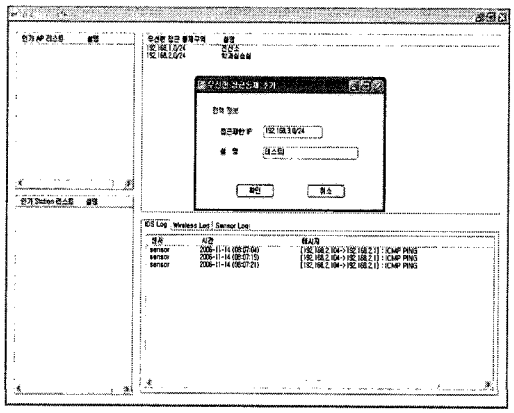

그림 3.9 W-TMS SW
Fig. 3.9 W-TMS SW

〔표 4.1〕 기존 시스템과의 성능 비교 평가
〔Table 4.1〕 Performance Analysis

기능 / 시스템	구성	공격 탐지 방식	공격 탐지 모듈	Rogue AP 탐지	MAC Spoof 탐지	Auth/De auth 탐지	공격 차단 기능	통합형 보안 관리 시스템
AirMagnet Sensor〔10〕	AP, 모니터링 센서, 컨트롤러, 서버	AP→센서→서버 전송 후 탐지	서버	O	-	-	×	-
AirDefense Guard〔11〕	AP, AP 연결 센서, 서버 및 모니터링 툴	AP→연결센서→서버전송/탐지	서버	O	-	-	×	-
RFprotect System〔12〕	AP, 연결 센서, 모니터링 클라이언트 및 통합관리 서버	AP→클라이언트→서버 전송후 탐지	서버	O	O	O	-	O
제안한 시스템	AP, 통합관리 서버	AP탐지→서버 전송→차단	AP 및 서버	O	O	O	O	O

IV. 실험 및 결과 분석

4.1 개발 시스템 실험

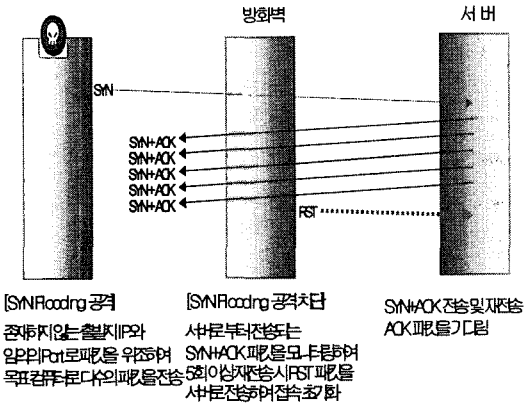

그림 4.1 SYN Flooding 공격에 대한 실험
Fig. 4.1 System Test against SYN Flooding

본 연구에서 제안한 시스템의 침입 탐지 기능과 차단 기능의 효율성 분석을 위해 무선 네트워크에서 SYN Floodin g 패킷을 생성하여 무선 네트워크에 대한 공격을 수행하였고 노트북에 W-Sensor SW를 설치하여 무선 네트워크 공격에 대한 탐지 및 차단 기능을 실험하였다. 실험 결과 W-Sensor가 Rogue AP나 AP 기능을 갖춘 Station들의 공격에 대해 사전 탐지하고 W-TMS와 연동하여 이에 대해 대응하는 것을 확인할 수 있었다. 또한 새로운 공격 유형을 탐지하는 룰들을 신속하게 반영할 수 있었으며 공격 트래픽이 많은 지역에는 여러 개의 W-Sensor를 설치하여 침입 탐지의 성능을 높을 수 있었다.

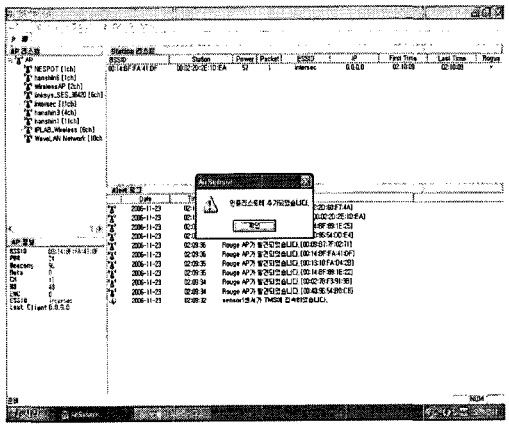

그림 4.2 W-Sensor의 유해 트래픽 탐지
Fig. 4.2 Detection of Malicious Traffic By W-Sensor

4.2 결과 분석

본 연구를 통해 개발한 W-Sensor 시스템과 기존의 IPS 시스템의 성능을 비교하였다〔표 4.1〕. 비교하고자 하는 대상들의 비교 분석은 뉴욕의 Syracuse 대학의 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 "W-Sensor가 내장된 AP->엔진->내부 네트워크"의 총 3단계를 거치므로, 무선 네트워크의 흐름을 더욱 원활하게 할 수 있다. 또한 W-TMS와의 연동을 통해 효율적인 침입 탐지 및 차단을 수행할 수 있었다.

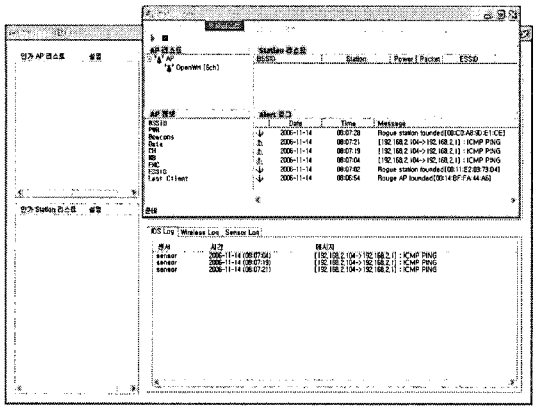

그림 4.3 W-Sensor와 W-TMS의 연동을 통한 트래픽 차단
Fig. 4.3 Traffic Filtering By W-TMS with W-Sensor

V. 결론 및 향후과제

본 연구에서는 유무선 네트워크가 혼재되어 사용하고 있는 대학 캠퍼스 망 환경에서 무선 네트워크를 통해 유선망을 공격할 수 있는 유해 트래픽들의 침입을 탐지하고 효율적으로 차단하는 시스템을 개발하였다. 유해 무선 트래픽의 침입 탐지를 위해 W-Sensor를 개발하여 트래픽 공격에 대응하고 이의 결과를 W-TMS에 연동하여 무선 트래픽을 차단하였다. 개발된 W- Sensor는 소프트웨어 형태로 노트북이나 PDA에 설치되어 공격 유형의 변화에 신속하게 대응하고 기존 AP 기반의 센서 시스템보다 네트워크 운영 비용을 줄일 수 있다. 또한 이동성도 크게 증가되어 공격이 빈번한 지역에서 효과적으로 사용될 수 있다.

제안된 시스템들은 기존의 유선 네트워크와 무선 네트워크를 같이 사용하는 컴퓨팅 환경에 사용될 수 있으며 무선 네트워크의 사용이 증가할수록 많은 분야에서 활용될 수 있다.

향후 공격 유형의 변화를 유기적으로 반영시킬 수 있는 서버 시스템을 개발하여 본 연구에서 제안한 시스템과 연동시킨다면 보다 안정된 대학 캠퍼스 망을 운영할 수 있을 것이다.

참고문헌

[1] 정연서 외, "안전한 인터넷을 위한 보안 관리 시스템 설계," 한국컴퓨터정보학회 논문지, 제 7권 3호, 2002.

[2] 강유, 스노트2.0 마술상자, 에이콘 출판사, 2003.

[3] 정보홍, 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, No2, 2004.

[5] 조현정, "차세대 네트워크 보안기술 기반의 침입방지시스템" 정보과학회지, 제 23권, 제1호, pp.21-26, 2005.

[6] 전용희 , "침입방지시스템(IPS)의 기술분석 및 성능평가 방안" 정보보호학회지, 제 15권, 제 2호, pp.63-73, 2005.

[7] 이창우 외, "분산 환경에서의 침입방지를 위한 통합보안 관리 시스템 설계," 한국컴퓨터정보학회 논문지, 제 11권 2호, 2006.

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

[9] Bruce Potter, "802.11 Security", OReilly, Dec., 2002.

[10] John Wiley & Sons, "Building Secure Wireless Networks with 802.11", Jan., 2003.

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

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

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

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

저 자 소 개

최 창 원
1995년 8월 고려대학교
컴퓨터학과, 이학박사
1996년~ 현재 : 한신대학교
컴퓨터정보소프트웨어학부 교수

이 형 우
1999년 8월 고려대학교
컴퓨터학과, 이학박사
2003년~ 현재 : 한신대학교
컴퓨터정보소프트웨어학부 부교수