韓國컴퓨터情報學會 論文誌
第16卷 第12號, 2011. 12.

2011-16-12-4-2

Wi-Fi 환경에서 패킷 분석을 위한 모니터링 시스템

서 희 석*, 김 희 완**, 안 우 영***

Monitoring system for packet analysis on Wi-Fi environment

Hee-Suk Seo*, Hee-Wan Kim**, Woo-Young Ahn***

요 약

노트북 컴퓨터, 스마트폰 및 기타 단말기 등 네트워크를 제공하는 모바일 기기가 증가함에 따라 무선 인터넷에 대한 많은 기술들이 발전하고 있다. IEEE 802.11은 흔히 무선랜, 와이파이라고 부르는 좁은 지역을 위한 컴퓨터 무선 네트워크에 사용되는 기술로 일상생활에서 쉽게 접할 수 있으며 액세스 포인트(AP)와 네트워킹이 가능하지만 무선랜은 보안에 취약하고 제 3자가 AP에 불법으로 접속하여 패킷을 조작하거나 정보를 빼낼 가능성이 있어 주의가 필요하다. AP (Access Point)는 무선 환경을 제공하는 기기로써 카페와 같은 공공장소에 설치되고 있다. AP는 무선인터넷을 더 편리하게 사용할 수 있게 한다. 하지만 IEEE 802.11 가진 많은 취약점 때문에 공격자는 AP와의 통신을 쉽게 도청할 수 있다. 따라서 본 논문에서는 무선랜 환경에서 패킷 분석을 위한 모니터링 시스템을 설계하고 구현한 것으로서 최근 스마트폰의 보급 확대에 따른 모바일상의 보안문제가 크게 대두되고 있는 시점에서 주변에 어떤 AP와 스테이션이 통신을 하며, AP의 정보를 캡처하여 보안상의 취약점을 알아내고 분석할 수 있는 무선 네트워크 패킷을 분석을 위한 모니터링 시스템을 개발하고자 하였다.

▸ Keyword : 무선 네트워크, IEEE 802.11, 패킷 분석, 모니터링

Abstract

Many technologies for wireless internet are increasing as more and more laptop computers, net books, smart phone and other terminals, which provide wireless network, are created. IEEE 802.11 is computer wireless network technology that used in small area, called wireless LAN or

• 제1저자 : 서희석 • 교신저자 : 안우영
• 투고일 : 2011. 11. 14, 심사일 : 2011. 11. 30, 게재확정일 : 2011. 12. 09.
* 한국기술교육대학교 컴퓨터공학부(Dept. of Computer Science, Korea University of Technology and Education)
** 삼육대학교 컴퓨터학부(Dept. of Computer Science, SahmYook University)
*** 대전보건대학 바이오정보과(School of Bio-infomation, Daejeon Health Sciences College)

Wi-Fi. IEEE 802.11 is a set of standards for implementing wireless local area network (WLAN) computer communication in the 2.4, 3.6 and 5 GHz frequency bands. They are created and maintained by the IEEE LAN/MAN Standards Committee (IEEE 802). AP (Access Point) is installed at cafes and public places providing wireless environment. It is more convenient to use wireless internet, however, It can be seen easily around us and possible to communicate with AP. IEEE 802.11 has many vulnerability, such as packet manipulation and information disclosure, so we should pay more attention when using IEEE 802.11. Therefore this paper developing monitoring system which can find out AP and Stations that connect with it, and capturing AP's information to find out vulnerability. This paper suggests monitoring system which traffic analysis in wireless environment.

▸ Keyword : Wireless Networt, IEEE 802.11, Packet Analysis, Monitoring

I. 서 론

인터넷 사용이 보편화됨에 따라 노트북과 휴대용 이동 통신 기기들이 널리 사용되면서 사용자들은 일반 컴퓨팅 환경에서도 보다 편리한 이동성과 원격성을 요구하고 있다. 이러한 시점에서 Wi-Fi[1](Wireless-Fidelity, 802.11, 무선 랜)는 사용자들에게 특정지역 내에서 어디에서든지 자유롭게 접속할 수 있는 이동성을 보장해 주며, 사업자들에게는 케이블링이 필요 없어 빠른 시간 내에 네트워크 구축이 용이하게 하고, 재배치 및 확장 시 추가적인 비용이 적고, 다양한 형태의 네트워크 구축을 용이하게 해준다.

차세대 무선 네트워킹을 주도하고 있는 무선 랜은 그동안 유선 선로를 포설하기 어렵거나 이동이 잦은 업무 환경에서 극히 제한적으로 사용되었다. 이처럼 무선 랜은 그 활용이 증가하고 있는 반면 그에 비해 사용자의 안전한 사용을 보장할 만한 보안 솔루션은 상대적으로 취약한 편이다.[2]

우리 주위에서 흔히 사용되는 무선 랜은 보안상 매우 취약하고 보통 우리가 사용하는 무선 공유기(Access Point)의 설정은 보안에 취약하며 암호화조차 되어 있지 않다. 이는 악의적으로 누군가가 AP에 불법으로 접속하여 패킷을 보고 조작하거나 정보를 유추해 낼 가능성이 제기된다. 따라서 무선 네트워크 환경에서 트래픽을 주기적으로 모니터링이 필요하며 각 스테이션의 정보와 AP의 정보를 캡처하여 보안상의 취약 점을 알아내고 분석할 수 있는 시스템을 개발하고자 한다. 본 시스템은 주변에 어떤 AP와 스테이션이 있는지와 각 무선 랜이 어떤 인증 방식과 암호화를 사용하는지, 또한 각 스테이션의 송수신 패킷의 내용, 사용하는 트래픽의 서비스명과 IP의 통계를 알려줌으로 전반적인 네트워크를 모니터링 할 수 있게 한다.

또한 각 계층의 헤더들을 분석하여 패킷의 내용도 볼 수 있다. 더욱이 그 패킷들을 분류하여 각 스테이션의 트래픽 사용량과 어떤 IP를 접속하고 어떤 서비스를 받았는지 알 수 있도록 하였다. 실제 고가의 스니퍼 장비와 기능 비교를 통하여 본 도구의 효율성에 대해서 비교 분석해 보고자 한다.

또한 본 논문은 최근 스마트폰의 보급 확대에 따른 모바일 상의 보안문제가 크게 대두되고 있는 시점에서 값비싼 장비가 아닌 쉽게 무선랜 환경에서 패킷 분석을 위한 모니터링 시스템을 설계하고 구현할 수 있도록 하였다.

II. 관련 연구

1. 802.11 무선 네트워크

IEEE.802.11[3]는 현재 주로 쓰이는 유선 LAN 형태인 이더넷의 단점을 보완하기 위해 고안된 기술로, 이더넷 네트워크의 말단에 위치해 필요 없는 배선 작업과 유지관리 비용을 최소화하기 위해 널리 쓰이고 있다. 보통 폐쇄되지 않은 넓은 공간(예를 들어, 하나의 사무실)에 하나의 핫스팟을 설치하며, 외부 WAN과 백본 스위치, 각 사무실 핫스팟 사이를 이더넷 네트워크로 연결하고, 핫스팟부터 각 사무실의 컴퓨터는 무선으로 연결함으로써 사무실 내에 번거로이 케이블을 설치하고 유지보수를 하지 않아도 된다.)은 AP와 Ad-hoc의 MAC, PHY layer가 초점, 무선 랜 MAC과 PHY layer의 Specification. local 범위 안에서 공기 중의 네트워킹 필수이며 다른 802 기반의 표준 같이 MAC Service Date Unit(MSDU)과 Logical Link, Control(LLC)를 전송한다. 특징은 다음과 같다.

1) 전력 관리 : MAC layer의 기능으로 보낼 게 없을 때 sleeping 모드 전환

2) Bandwidth : 제한된 범위
3) Security : 유선보다 더 큰 범위의 보안이 필요
4) Addressing : 유동적 topology 때문에 목적지의 위치가 항상 일치하지 않음.
5) Topology구성
- IBSS (Indepedent basic service set) : 집중된 AP를 통하지 않고 개개의 스테이션이 서로 주고 받는 ad-hoc 네트워크
- ESS (Extended service set) : ad-hoc과 다르게 확장된 인프라스트럭쳐 네트워크로 각각의 BSS는 AP를 통해 주고 받으며 다른 BSS들은 백본망으로 통합하여 통신

2. 무선 네트워크 보안

최근 기업의 업무환경이 정적인 유선에서 동적인 무선으로 변화하고 있으며 이에 따라 Wi-Fi 네트워크 구축과 서비스가 활발해지고 있다. 기업의 Wi-Fi 인프라 도입이 본격화 되고 가정 내 유/무선 공유기의 보급으로 인하여 Wi-Fi의 사용이 대중화 되고 있다. [4]

하지만 급속한 대중화 과정에서 Wi-Fi 사용자 및 운영자의 보안의식 부족으로 각종 Wi-Fi 해킹 위협에 노출 되어있다.[5]

Wi-Fi는 일반적으로 무선이라는 특성 때문에 허공으로 데이터를 전송하여 Wi-Fi을 사용하는 기관이나 업체의 물리적인 경계선을 뛰어 넘으며 특히, 고정통신용 Wi-Fi 등 강력한 지향성 안테나를 사용하는 경우 설계된 경계를 벗어난 먼 곳까지 도달이 가능하다. 따라서 무선 주파수 범위내의 모든 사용자가 패킷에 접근할 수 있으므로 기존의 물리적인 보안 제어기능이 무력화된다.

노트북 컴퓨터와 Wi-Fi, Scanner, Sniffer 같은 프로그램만 있으면 여러 가지 보안 취약점을 이용해 무선패킷을 수신하여 가저장/분석할 수 있다. 또한 간단한 Jamming[6] 트랜스미터만 있으면 통신을 불가능하게 만들 수 도 있다.

또한, AP가 해커의 수중에 들어가면 네트워크 자원을 공격하는데 악용될 수 있다. AP는 비교적 소형이고 일반 전자부품 판매점에서도 구입이 용이하므로 해커가 AP를 수중에 넣고 건물 안에 들어가 교묘히 설치하는 것은 쉽다. 예를 들면 AP를 회의실 테이블 밑에 붙여서 가동 중인 네트워크에 연결시켜 놓을 경우, 주차장에 주차된 자동차 내부 등 자신이 원하는 장소에서 네트워크로 침입이 가능하다.[7]

하지만 현재는 Wi-Fi 보안 현황이 제대로 파악 되어있지 못해 어떤 부분에 대한 보안이 시급한지에 대한 정보가 부족하였다. 이에 Wi-Fi IDS(Intrusion Detection System)를 이용한 Wi-Fi 보안 실태 조사[8]를 실시하여, 실제 여러 지역의 Wi-Fi 보안 현황을 통계치 기반으로 파악하고 이전의 설문조사를 통한 시스템운영 실태 조사 보다 정확하고 실질적인 데이터를 얻었다. 이를 바탕으로 'Wi-Fi 보안 알고리즘에 대한 취약성 인식 부족[9]', 'Mac Filtering[10] 에 대한 과도한 신뢰, Wi-Fi을 사용하는 Client 보호 부족' 이라는 현재 Wi-Fi 환경에서 가장 중요하고 발생 가능성이 높은 문제점을 제시하고 그 해결을 위한 가이드라인을 제시한다.

하드웨어적이나 소프트웨어적으로 Wi-Fi 보안에 대한 많은 솔루션 개발이 진행되고 있다. Wi-Fi 환경의 보급만큼이나 보안에 대한 안보의식의 필요성이 요구 되어지는 시점이기 때문이다. 아직까지도 많은 유저들이 Wi-Fi의 취약성이나 위협성에 대해 의식 하지 못하는 부분들을 많은 연구가들의 노력에 의해서 보안의 대한 방안과 대책들이 강구되고 있다.

III. 패킷 분석을 위한 모니터링 시스템

1. 시스템 요구사항

표 1. 시스템 요구사항
Table 1. System Requirement

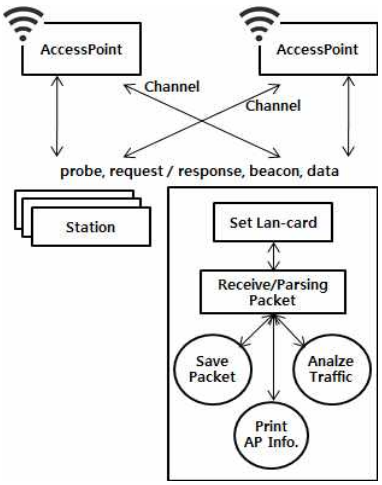
시스템 요구사항
○ 모니터 모드 설정
○ 패킷 수신
○ 패킷 파싱
○ 화면 출력 및 UI
○ 패킷의 데이터 저장
○ 트래픽 분석

- 모니터 모드 설정 : 오픈소스 랜 카드 디바이스 드라이버로 모니터 모드 인터페이스 생성 후 프로그램 내에서 ioct()로 랜 카드를 세팅하였다.[11]
- 패킷 수신 : socket()로 Raw 소켓 생성 후 read()로 받는다.
- 패킷 파싱 : 책과 패킷 캡쳐 프로그램(wireshark)으로 패킷 분석(계층 별 헤더의 정보위치) 후 그에 맞춰 파싱해 출력할 스트링 생성한다.
- 화면 출력 및 UI : 파싱에서 생성된 스트링을 화면에 출력하고 터미널 컨트롤로 출력 공간 조정한다.

- 패킷의 데이터 저장 : 패킷의 IP, mac address 와 포트 정보를 데이터 내용과 같이 저장한다. 파일 입출력을 이용하여 파일 생성한다.
- 트래픽 분석 : 파싱해서 추출한 데이터를 분석하고 스테이션 별로 접속했던 IP들의 목록을 구조체로 가지고 있고, 출력 정보(접속 했던 IP 목록, 각 IP 서비스(포트) 이름, 각 IP data량, 서비스 사용 백분율)로 나타낸다.

2. 시스템 설계

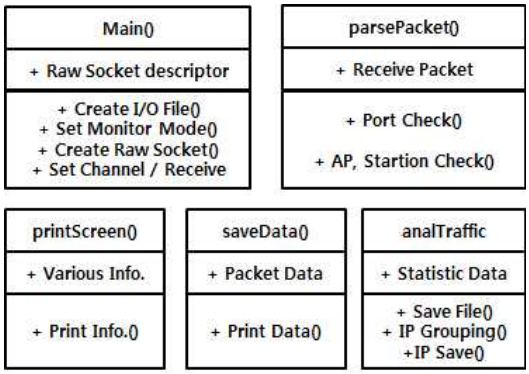
본 시스템은 inter pentium D 프로세서와 2GB 메모리 환경에서 Atheros AR5006X, Wireless Network Adapter 랜카드를 이용해 Red Hat 7.0 환경에서 개발되었다.



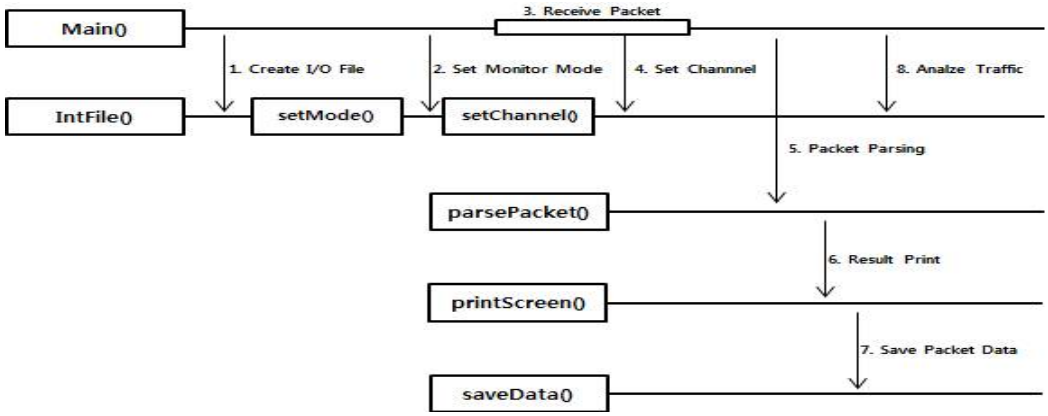
[그림 1] 시스템 개요도
Fig. 1. System Architecture

아래의 [그림 1]는 패킷 분석을 이용한 모니터링 시스템의 전체 시스템 개요도이다. AP는 무선 접속 장비이며, 스테이션은 사용자가 사용하고 있는 PC이다. 각각의 장비들은 서로 Probe, request/response, beacon, data 등을 서로 무선 통신을 하며 AP에서는 AP의 식별자인 beacon 프레임을 전송하여, 자신이 어떤 AP인지를 알리며 스테이션에서는 Probe 패킷을 전송함으로서 AP가 있는지 지속적으로 scanning을 하게 된다. 각 채널에 따라 스테이션과 AP가 통신을 하게 되며 요청/응답 패킷과 데이터 등을 주고받으며 통신을 하게 된다. 이때 모니터링장비에서는 로우 패킷을 생성해 주변에 있는 모든 패킷을 접수하여 AP와 스테이션을 구분 후 각 장비에 맞는 정보를 분석 하여 결과를 파일로 저장하게 된다.

3. 시스템의 클래스 다이어그램



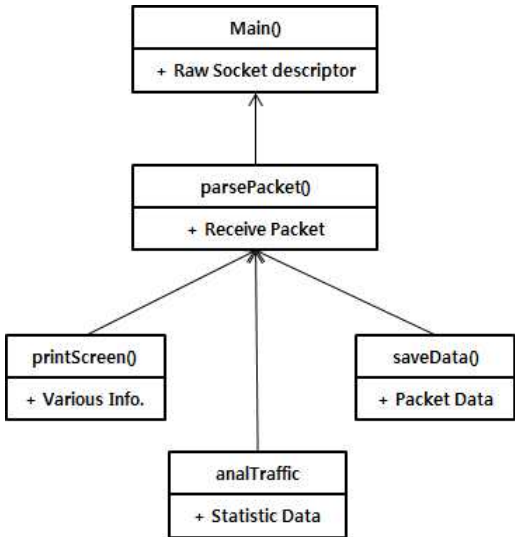
[그림 3] 시스템 클래스 구조
Fig. 2. System Class Structure



[그림 4] 패킷 모니터링 시스템 시퀀스 다이어그램
Fig. 4. Sequence Diagram of Packet Monitoring System

위의 [그림 2]과 같이 모니터링 시스템은 메인(Main), 파스 패킷(Parse Packet), 프린트스크린(Print screen), 세이브 데이터(Save Data), 트래픽 분석(anal Traffic)으로 5가지 클래스 부분으로 나눌 수 있다. 메인에서는 로우 패킷생성과 모니터 모드 설정, 채널 및 수신 루프가 해당되며 메인에서 파스 패킷으로 넘겨진다. 파스 패킷에서는 수신되어진 패킷을 포트 검사와 AP검사, 스테이션 검사 등을 통해서 프린트스크린과 트래픽 분석, 세이브 데이터로 보낸다. 프린트스크린에서는 추출되어진 각종 정보를 출력 해 주는 것이며 트래픽 분석에서는 분석되어진 IP리스트와 통계 정보 등을 출력한다.

세이브 데이터에서는 분석 결과로부터 패킷의 데이터를 분류하며 IP 기준으로 파일 형태로 저장한다.



[그림 3] 시스템 클래스 다이어그램
Fig. 3. System Class Diagram

4. 시스템의 시퀀스 다이어그램

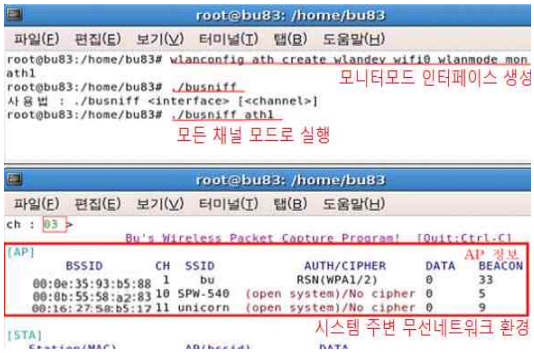
패킷 분석을 위한 모니터링 시스템이 동작하면서 가장 먼저 입출력 파일을 생성 한다. 이 입출력파일은 패킷 트래픽 분석 결과로부터 데이터를 분류하고 저장하는데 사용된다. 설정 패킷을 수신 하고 채널을 설정함으로써 모니터 모드로 설정된다. 모니터 모드 설정 이후에 수신되는 패킷에 대해서는 parsePacket()으로 파싱을 요청한다. 패킷 분석 결과를 화면에 출력 하고 분석되어진 패킷을 데이터로 저장하고 트래픽을 분석한다.

Ⅳ. 시스템 수행 결과

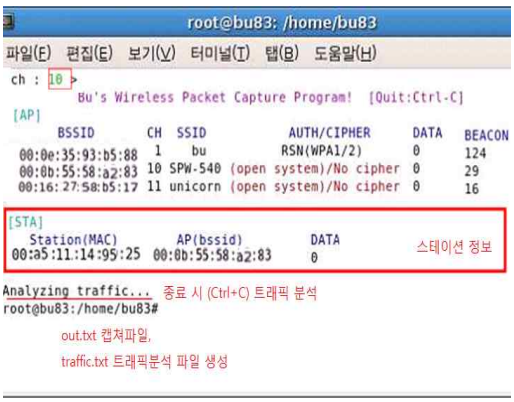
1. 모니터모드 및 채널 설정

첫 번째 결과 화면에서는 스니퍼 장치를 실행 하는 장면으로 먼저 모니터 모드 인터페이스 생성 후 모든 채널 모드로 실행 하게 된다. 두 번째 결과 화면에서는 채널 과 BSSID(AP의 MAC주소)와 SSID(AP의 식별자) AUTH/CIPHER(보안정보), DATA, BEACON(AP의 정보)등을 알 수 있다.

위 <그림 5>에서는 스테이션의 MAC주소와 연결 되어진 AP의 SSID가 보여지고 있다. ctrl+c시 트래픽 분석이 되어 지며 out.txt 캡쳐파일과 traffic.txt 트래픽 분석파일 등 두 개의 파일이 생성된다.

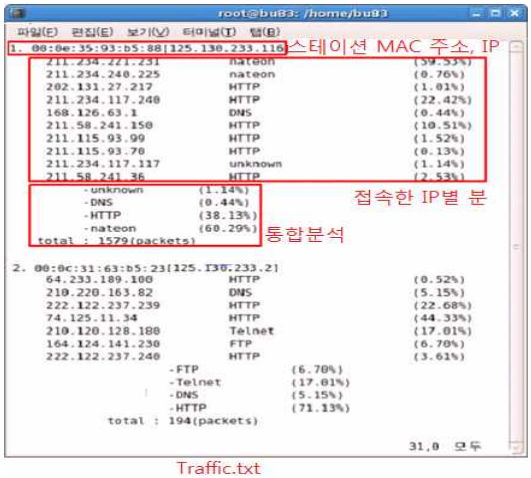


[그림 5] 모니터 모드 세팅 및 주변 무선 네트워크 확인
Fig. 5. Set Monitoring Mod&&&



[그림 6] 채널 설정을 통한 패킷 모니터링
Fig. 6. Packet Monitoring by Setting Channel

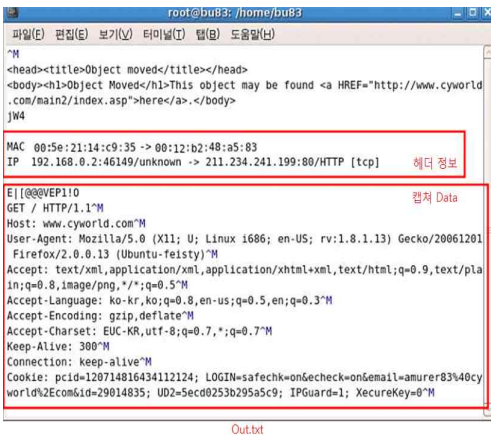
2. 트래픽 분석



[그림 7] Traffic.txt 파일의 내용
Fig. 7. Traffic.txt File

먼저 traffic.txt 캡쳐 파일을 살펴 보면 맨 위에 스테이션 MAC 주소와 IP주소를 볼 수 있으며 스테이션이 어떤 포트와 서비스를 사용하였는지 목적지의 IP주소를 확인 할 수 있으며 더 나아가 이용 분포율과 포트별 이용 현황 등을 살펴 볼 수 있다. total 정보를 통하여 패킷량을 알 수 있다.

마지막으로 out.txt에서는 캡쳐 된 패킷의 헤더에서는 스테이션이 어떤 정보를 이용하였는지에 대해 좀더 자세히 분석해 볼 수가 있다. MAC주소와 IP를 확인 할 수 있고 DATA 부분에서는 서비스와 해당 호스트 주소 사용되어진 언어와 Encoding방식 등을 자세히 살펴 볼 수 있다.



[그림 8] out.txt 파일의 내용
Fig. 8. out.txt File

3. 패킷 모니터링 시스템 성능 평가

미니 스니퍼와 실제 고가 장비의 스니퍼와의 비교 도표이다. 현 도표를 보게 되면 미니 스니퍼와 실제 스니퍼의 기능적, 성능적 차이를 한 눈에 볼 수 있다. 차이에 대해 살펴 보면 미니 스니퍼는 송수신지 주소 와 포트 번호 패킷의 헤더 내용에 대해서 분석 하는 기능적인 능력은 실제 스니퍼 장비와 동등 할 정도의 수준이다. 실제 스니퍼 장비는 미니 스니퍼가 구현 할 수 없는 다양한 기능들을 가지고 있으며 네트워크 관리자가 운영 할 시 원하는 조건에서 동작 및 구현이 가능 하다. 예를 들어 일정 기간이나 시간대별 설정을 통한 모니터링 및 패킷 수집 기능, 패킷에 대한 정보를 수집 시에 원하는 특정 패킷에 대해서 필터링을 통하여 정보 수집이 가능하며 각종 분석 내용에 대한 그래프 등의 시각화, 네트워크에 임의의 트래픽을 통하여 현 네트워크의 성능을 평가 등이 가능 하다. 전체적인 성능적 비교를 통하여 실제 스니퍼 장비의 우수성을 알 수 있었다.

하지만 미니 스니퍼가 가지고 있는 기본적인 기능들은 실제 스니퍼와 비교했을 때 전혀 뒤지지 않음을 알 수 있었다. 미니 스니퍼에서 가지고 있는 기능들은 스니퍼가 가져야 할 가장 기본적 측면에서 충실하기 때문이다. 실제 스니퍼 장비가 우수 하기는 하지만 일반인들이 집에서 혹은 작은 사무실 등에서 사용하기 에는 너무나 고가의 장비이며 훈련을 통해서 다루어 보지 못하였다면 활용도는 가격 대비 의미가 없어 질 것이고 복잡한 기능들은 사용자를 더욱더 혼란스럽게 만들 것이다.

표 2. 미니 스니퍼와 실제 스니퍼의 차이
Table 2. Different Between Mini-Sniffer and Sniffer

비교 내용	미니 스니퍼	실제 스니퍼	비 고
송/수신지 주소 캡쳐	가능	가능	IP, MAC
포트번호 캡쳐	가능	가능	프로토콜 포트번호
패킷 헤더 분석	가능	가능	헤더 내용
계층별 헤더 해석	불가능	가능	OSI7계층
네트워크 성능 테스트	불가능	가능	임의 트래픽 생성
전체망 분포도 모니터링	일부	전체 가능	현재 망 현황 모니터링
실시간 모니터링	불가능	가능	지속적으로 모니터링
예약 모니터링	불가능	가능	특정 시간대 예약설정
필터링캡쳐	불가능	가능	특정 패킷 필터링
그래프 표시	불가능	가능	캡쳐 내용 그래프
분석내용 저장	가능	가능	파일로 저장
가격	저가 (10만원 미만)	고가 (천만원선)	구축비용

미니스니퍼를 통해서 저렴하게 Wi-Fi과 프로그램만으로 가장 중요한 패킷 분석과 네트워크 주소 정보 등을 알기에 충분하기 때문에 일반인들도 쉽게 사용이 가능하며 조금만 더 기능적인 측면을 보완 한다면 보급형으로 일반 유저들에게도 폭넓게 사용 될 수 있을 것이며 무선 랜 보안의 안전에 좀 더 기여 할 수 있을 것이다.

V. 결론

본 논문은 무선 네트워크를 관리하는 입장에서 주변의 AP와 스테이션을 모니터링 함으로 취약한 곳을 알아내고 대처하고자 본 시스템을 설계하고 구현하였다. 본 시스템은 기본적으로 스니퍼의 기능을 갖고 있으며 주변의 AP와 스테이션의 송수신 패킷을 로우 소켓으로 받는데 한글과 유니코드 같은 다양한 포맷을 적절하게 디코딩한다면 자세한 내용을 볼 수 있다. 또한 마지막으로 받은 패킷들에서 얻는 여러 가지 정보를 이용하여 트래픽 분석을 할 수 있다. 예를 들면 스테이션 사용자가 접속한 웹사이트의 IP 주소와 포트번호를 통해 HTTP를 사용한다고 알 수 있고 만약 새로운 포트를 사용하는 프로그램이 생겼다면 포트리스트에 포트 번호와 서비스 이름만 추가 하면 된다. 또한 각 서버가 사용한 데이터를 수를 계산하여 통계량을 알려준다.

전반적인 무선 랜을 모니터링 함으로 악의적인 스테이션, Access Point을 확인 할 수 있고 사용자들의 트래픽을 통계를 도출함으로써 효율적으로 네트워크를 관리 할 수 있는 정보를 제공한다. 실제 고가의 스니퍼 장비와 현 시스템을 직접 비교 분석해 보았을 때 고가 장비의 스니퍼와 거의 동등한 수행 능력을 확인 할 수 있었고 가격 대비 효율적인 면을 확인 할 수 있었다.

참고문헌

[1] "Wireless Fidelity (WiFi) Technology". ITAA. January 2004. Retrieved 2009-11-30.

[2] Si-Choon Noh, "A Designing Method of Network Security Infrastructure", Journal of The Korea Society of Digital Industry & Information Management, Vol. 2, No. 2, 2006. 06.

[3] IEEE 802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. (2007 revision). IEEE-SA. 2007. 06.

[4] Dong-Hoon Shine, Dong-Myung Shin, Kyoung-Hee Ko "Research preventative measures Wireless-LAN Security incident" Autumn Conference on Korea Institute of Information Scientists and Engneers Vol. 31, No. 2, 2004.

[5] Hyun-Chul Jung, Hee-jo Lee, "Study on Security Reinforcement Method by Wireless Security Status Survey and Analysis", Spring Conference on Processing Society, Vol. 13, No. 1, 2006. 05.

[6] NIST 800-97 Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i.

[7] Kyu Won Lee, Jae Won Ji, Hyun Woo Chun, Sang-jo Youk, "Traffic Analysis Technique for Intrusion Detectionin in Wireless Network", Journal of Security Engineering, Vol. 7, No. 6, 2010. 12.

[8] Jong-Ho Lee, "Wireless-LAN Security Protocol", Kyohacsa, 2005. 08.

[9] Tae-Kyung Kim, "A Study on the Authentication Mechanism for Wireless Mesh Network", Journal of The Korea Society of Digital Industry & Information Management, Vol. 5, No. 2, 2009. 09.

[10] IEEE, "Wireless Medium Access Control (MAC) and physical layer (PHY) specification", IEEE Std 802.11, 1999.

[11] Matthew S. Gast, "802.11 Wireless Networks; The Definitive Guide", O'Reilly Networking, 2002. 04.

저 자 소 개

서 희 석

2000 : 성균관대학교 산업공학과 공학사.

2002 : 성균관대학교 전기전자 및 컴퓨터공학과 공학석사

2005 : 성균관대학교 전기전자 및 컴퓨터공학과 공학박사

현 재 : 한국기술교육대학교 컴퓨터공학부 부교수

관심분야 : 모델링&시뮬레이션, 네트워크보안, 보안 시뮬레이션, USN

Email : histone@kut.ac.kr

김 희 완

1987 : 광운대학교 전자계산학과 이학사.

1995 : 성균관대학교 공학석사(컴퓨터공학)

2002 : 성균관대학교 공학박사(컴퓨터공학) 정보관리기술사, 정보시스템 수석감리원

현 재 : 삼육대학교 컴퓨터학부 교수

관심분야 : 정보보호 및 보안, 데이터베이스, 정보시스템 감리

Email : hwkim@syu.ac.kr

안 우 영

1988 : 중앙대학교 전자계산학과 이학석사

1999 : 홍익대학교 전자계산학과 이학박사

현 재 : 대전보건대학 바이오정보과 교수

관심분야 : 모바일컴퓨팅, 지식데이터베이스, 바이오인포메틱스

Email : wyahn@hit.ac.kr