무선랜 보안관리를 위한 정보 수집 에이전트 설계 및 구현

김동필°**, 백병욱*, 김상욱*

*경북대학교 컴퓨터과학과

**경북대학교 정보보호학과

{dpkim°, bwback, swkim}@woorisol.knu.ac.kr

A Status Monitoring Agent Design and Implementation for Wireless Lan Security Management

D. Kim°**, B. Back*, S.Kim*

Computer Science Department, Kyungbook National University

요약

무선랜 환경에서는 데이터 링크 레이어의 전달 매체와 물리적 계층이 기존의 유선 네트워크와는 근본적으로 다른 특성을 지닌다. 무선랜 환경에서는 공중망을 전달 매체로 하여 통신이 이루어진다. 그리고 무선랜 환경에서는 단말기들의 이동성에 의해 네트워크 상태가 가변적으로 변하기 때문에, 이러한 환경에서 유선과는 또 다른 보안상의 문제점들을 가지게 된다. 본 논문은 무선 구간에서 유동적으로 발생하는 네트워크의 상태와 정보들을 수집하여 무선 구간에서만 이루어질 수 있는 보안상의 문제점들을 파악하고 대처하는 무선랜 환경에서 상태 정보 수집 에이전트를 설계하고 구현한다.

1. 서론

본 논문은 무선랜 환경에서 이동 단말기와 액세스 포인트들의 상태와 정보를 수집하는 에이전트를 설계하고 구현한다. 무선랜 기술의 주요 쟁점은 전송속도와 보안에 있다. 특히, 보안 문제는 무선랜 기술의 보급과 사용에 커다란 장애요소이다. WiFi(Wireless-Fedelity Alliance)에서 채택하고 있는 무선랜의 전송 표준은 IEEE 802.11b이다. IEEE 802.11b 표준에서는 무선랜 환경에서 이용되는 네트워크 각 레이어 가운데, MAC과 Pysical Layer에 대해서 구체적으로 기술하고 있다.[1] 무선랜에서 전송되는 데이터는 공중망을 통하여 브로드 캐스팅되므로 네트워크 도메인 안에 있는 모든 단말기에서 도청이 가능하다. 이것은 무선 랜 환경이 보안에 매우 취약하다는 것을 의미한다. 그리고 MAC은 윈도우의 경우에 간단한 레지스트리 편집기로, 유닉스의 경우에는 루트 쉘의 간단한 명령어로 수정이 가능하다.[2] 이러한 방법으로 통해서 인가된 단말기나 액세스 포인트로 위장하는 공격을 가할 수 있다.

유선 네트워크의 보안을 위해서는 방화벽, 침입 탐지 시스템 등을 이용하고 있다. 특히 방화벽은 외부 네트워크와 내부 네트워크의 연결점에 해당하는 게이트웨이 단에서 동작하면서 침입 탐지, 패킷 필터링 등의 역할을 하는 것이 일반적이다. 무선랜 환경의 경우에는 스테이션(Station)의 전원을 켠 후, 액세스 포인트(Access Point)에 접속만 이루어지면, 직접적으로 내부 네트워크와 연결이 이루진다. 이것은 방화벽을 우회하는 효과를 가지므로 많은 문제점을 야기 시킨다. 따라서 물리적인 영역 내에 존재하는 스테이션(Station)들에 대한 상태를 실시간으로 모니터링하고 위협에 대응할 수 있도록 하는 연구는 매우 중요하다. 더욱이 이러한 연구는 무선랜 침입 탐지의 기초로 사용될수 있다.

본 논문에서는 물리적인 영역 내에 존재하는 스테이션(Station)들의 존재 및 상태에 대한 정보를 실시간으로 수집하고 이상 패킷을 탐지하는 에이전트를 설계하고 구현한다.

2. 관련연구

2.1 관련 연구

현재 무선랜 모니터링 도구에는 Tcpdump, NetStumble 등이 있다. 다음은 이 공개용 도구들에 대하여 설명한다.

Tcpdump

Tcpdump는 네트워크를 모니터링하고 데이터를 볼 수 있는 도구로서, 관리자에 의해 널리 사용되고 있는 공개용 패킷 수집 도구이다. 커맨드 라인에서 특정 형식의 조건식에 따르는 패킷의 정보를 텍스트 형태로 나열해 주는 기본적인 기능과 패킷의 정보를 Tcpdump만의 고유한 형식으로 저장할 수도 있다. 현재 3.7.2 버전까지 나와 있으며, libpcap 라이브러리를 이용한다. 특히, 802.11의 MAC 레이어의 패킷은 libpcap 0.7.1 버전이상, Tcpdump 3.7.1 버전 이상에서만 제공된다. 따라서, 3.7.1 버전 이상의 Tcpdump를 이용하면, 802.11b의 무선 패킷을 수집할 수가 있다. Tcpdump는 802.11b라는 무선 네트워크에 한정된 도구가 아니고, 모든 형태의 프로토콜을 이용하는 패킷을 다 수집하는 장점이 있으나, 802.11의 무선랜의 상태를 한 눈으로 보여주는 그래픽 유저 인터페이스를 제공하지 못하고, 현재 네트워크에 존재하는 스테이션(Station)의 존재, 연결 상태에 대한 분석내용을 보여주지 못한다. 또한, 사용이 허용되어 있지 않는 스테이션(Station)의 정보를 찾아 낼 수 없고, 패킷의 이상 상황을 일일이 각 라인을 찾아가면서 분석해야 하는 단점이 있다.

NetStumbler

NetStumbler는 무선 신호의 도달범위(coverage)를체크하고자 하는 관리자들이나 스누핑(Snooping)을 하기 위한 정보수집 도구로 이용되고 있다.[4] NetStumbler는 무선랜에 이용되고 있는 액세스 포인트의 목록, 액세스 포인트의 MAC 주소, 채널 정보 등을 수집할 수 있는 기능을 제공해 준다. 그러나, 현재 네트워크에 존재하는 스테이션의 존재, 연결 상태에 대한 분석내용을 보여주지 못하고, 사용이 허용되어 있지 않는 스테이션의 정보를 찾아 낼 수 없다. 뿐만 아니라, 단순히 액세스 포인트에 대한 정보를 제공해 줄 뿐, 스테이션들의 정보를 확인할 수 없는 단점이 있다.

2.2 무선랜 정보 수집

무선랜 환경에서는 802.11b이라는 표준화된 프로토콜을 이용하고 있으며, 이것은 기존과는 다른 MAC과 물리 계층을 이용한다. 특히 MAC 프레임 타입은 관리 프레임(Management frame), 컨트롤 프레임(Control frame), 데이터 프레임(Data frame)으로 구분된다. 이들중 관리 프레임(Management frame)은 무선 단말들 사이의 관리를 위해 이용되는 프레임이다.[3] 이러한 관리 프레임으로는 Beacon 프레임, Association 프레임, Disassociation 프레임, Probe Request 프레임, Probe Response 프레임 등이 존재한다. 이러한 관리 프레임들은 무선 단말들 사이에 인증, 네트워크 연결 설정, 네트워크 종료 설정, AP의 정보, 이용되는 ESSID 등의 내용을 포함한다. 무선랜의 상태 모니터링은 이러한 MAC 프레임 중에 관리 프레임(Management frame)을 목표로 한다. 관리 프레임의 관찰을 통해서 무선랜에 이용되고 있는 무선 단말의 정보와 액세스 포인트의 정보, 무선 단말과 액세스 포인트의 상태, 그

리고 악의적으로 이용되고 있는 무선 단말의 탐지 등이 가능하다.

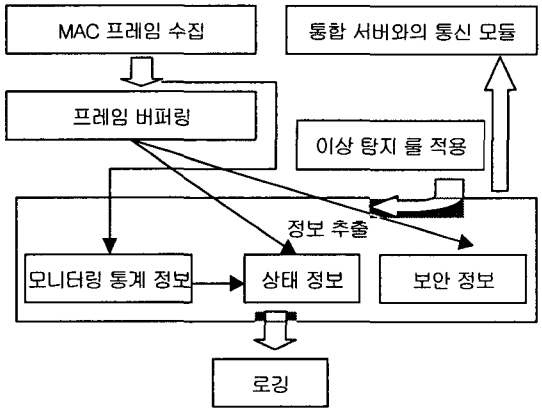
3. 정보수집 에이전트

본 절에서는 무선랜 정보를 수집하고 수집된 정보를 추출, 가공하는 정보 수집 에이전트를 설계하고 구현한다.

3.1 구조

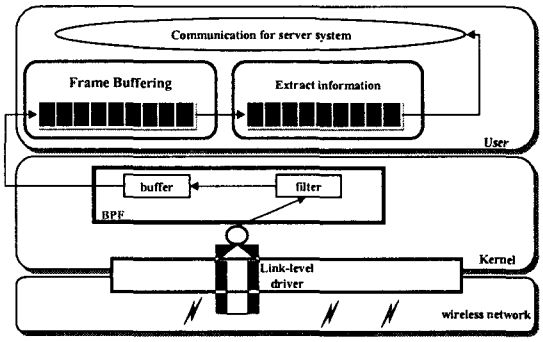
정보 수집 에이전트는 두 개의 인터페이스를 가진다. 하나는 무선 네트워크의 신호 정보를 수집하는 무선 인터페이스이고 다른 하나는 수집된 정보를 관리 서버와 통신을 하기위한 유선 인터페이스를 가진다. 정보 수집 에이전트는 다음과 같은 모듈로 구분된다.

- o 프레임 수집
- o 프레임 버퍼링
- o 정보 추출
- o 로깅
- o 통합 서버와의 통신



(그림 1) 정보 수집 에이전트의 구조

네트워크 인터페이스를 통해 전달되는 패킷은 BPF(BSD Packet Filter)에 전달된다. BPF에 전달되는 패킷은 블록 단위로 유저 프로그램으로 전달된다. 무선 네트워크의 정보 수집 에이전트는 BPF로부터 전달되는 패킷을 정보 추출을 위해 필요한 정보만을 중간 형태의 포맷으로 변환하여 버퍼링한다. 버퍼링된 프레임은 정보 추출 과정을 거치면서 상태 정보, 보안 정보, 모니터링 통계 정보로 분류된다. 이렇게 분류된 정보는 통합 관리서버의 요청에 따라 유선랜을 통해 전송해 줌으로써 통합 서버에서는 원거리에서 무선 정보 수집 에이전트를 통해 무선랜의 상태를 확인할 수 있다.



(그림 2) 정보 수집 에이전트의 동작과정

3.2 관리 프레임 수집과 버퍼링

802.11b MAC 프레임을 효율적으로 수집하기 위해서 BPF를 사용하는 pcap 라이브러리를 이용한다. 그리고 802.11b MAC 프로토콜을 이용하는 모든 프레임을 수집하기 위해서는 무선랜 카드를 RFMON(Radio Frequency Monitor) 모드로 전환을 하여야 한다. 무선랜 카드를 모니터링 모드로 전환한 후에는 다음과 같은 절차에 따라 무선랜의 인터페이스로부터 MAC 프레임을 획득한다.

① 네트워크 디바이스의 이름을 읽어오거나 지정한다.
② MAC 프레임 획득을 위한 네트워크 디바이스를 연다.
③ 필요한 정보만을 패킷에서 읽어 들이기 위해 해당 길이를 설정한다.
④ 필요한 정보만을 읽어오기 위해서 필터를 설정한다.
⑤ 프레임을 읽어 들인다.

802.11b의 MAC 프레임을 수집한 후에는 정보를 추출하기 전에 버퍼링을 수행한다. 이것은 프레임의 정보를 처리하는 동안, 수집된 패킷의 처

리가 이루어지지 못하고 상실되는 상황을 없애주기 위해서 필요한 작업이다. 다시 말해, 커널에 존재하는 BPF는 블록 단위로 수 마이크로초 안에 다량의 수집된 패킷을 사용자 프로그램으로 전달해 준다. 이렇게 전달된 패킷으로부터 정보를 추출해 내는 동안 계속 패킷이 전달되면 BPF 내의 버퍼 처리에 문제가 발생한다. 따라서, 정보 추출에 필요한 자료만을 빠른 시간 안에 추출해서 버퍼링을 수행해야 한다.

본 논문에서는 무선랜의 프레임들 가운데, 관리 프레임을 이용해서 상태를 모니터링하기 때문에 관리 프레임만을 획득하기로 한다. 이 외의 프레임은 간단히 통계 자료만을 획득한 후에 버려진다.

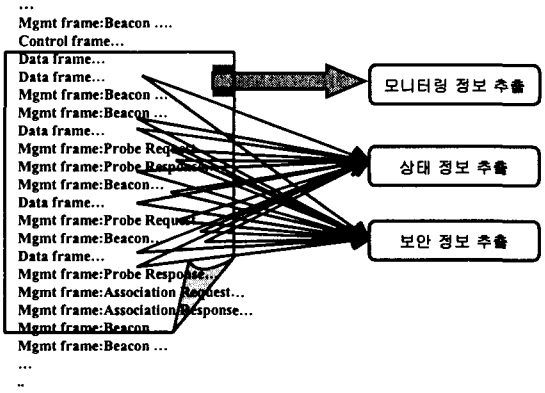
3.2 프레임 정보 추출

무선랜에 전달되는 프레임은 물리적인 네트워크에 존재하는 모든 신호를 발생하는 순서에 따라 순차적으로 수집을 한다. 이러한 연속적인 프레임들의 연관관계를 따져서 네트워크의 상태 정보, 프레임의 통계 정보, 보안 관련 정보를 추출해야 한다. 본 논문에서는 무선랜에 존재하는 802.11b MAC 프레임을 모니터링 통계 정보, 상태 정보, 보안 정보로 구분하여 정보를 추출한다. [그림3]은 모니터링 통계 정보, 상태 정보, 보안 정보로 구분하여 추출하는 그림이다. 모니터링 통계 정보는 프레임 타입별 통계를 나타내는 정보이고, 상태 정보는 현재 무선 네트워크를 구성하고 있는 스테이션들과 액세스 포인트들의 정보를 표현하는 정보이다. 마지막으로 보안 정보는 무선랜에서 공격을 위해 이용하는 프레임들의 연관성을 찾아서 이상을 탐지할 수 있도록 추출한 정보이다.

3.2.1 모니터링 통계 정보 추출

모니터링 통계 정보는 물리적인 무선 네트워크에 존재하는 모든 프레임의 수를 채널별 종류별로 분류한 정보이다. 이것은 기본적인 네트워크의 트래픽양을 확인할 수 있는 정보로 가장 기본적인 정보이다. 모니터링 통계 정보는 각 채널별로 관리한다. 이를 통해서 각 채널별 총 프레임의 개수, 컨트롤 프레임의 개수, 관리 프레임의 개수, 데이터 프레임의 개수를 파악할 수 있다. 그리고, 특히 데이터 프레임의 경우, 어떤 채널에서 많은 트래픽을 이용하는지 파악할 수 있다.[5]

다음은 모니터링 통계정보가 포함하는 내용이다.



(그림 3) 모니터링 정보, 상태 정보, 보안정보 추출

3.2.2 상태 정보 추출

상태 정보는 현재 무선랜에 존재하는 액세스 포인트와 스테이션의 정보를 나타낸다. 이것은 어떤 액세스 포인트와 어떤 스테이션이 연결설정이 이루어져 있는지, 어떤 스테이션이 현재 연결되지 않고 존재하는지 파악할 수 있다. 그리고, 어떤 스테이션이 가장 많은 트래픽을 사용하는지 등의 정보를 획득할 수 있다. 액세스 포인트에 대한 정보는 beacon 프레임과 association response 프레임을 통해서 획득할 수 있다. beacon 프레임은 액세스 포인트가 스테이션에 접속할 수 있도록 자신의 존재와 정보를 주기적으로 브로드 캐스트 하는 프레임이다. 그리고, association response 프레임은 등록된 스테이션이 액세스 포인트와의 연결 설정이 이루어질 때 액세스 포인트에서 스테이션으로 전달하는 프레임이다. 이 두 프레임을 통해서 현재 액세스 포인트의 정보와 액세스 포인트와 연결되어 있는 스테이션의 정보를 확인할 수 있다. 스테이션이 액세스 포인트와 연결 설정에 관여하는 프레임은

probe request 프레임, probe response 프레임, Authentication 프레임, association request 프레임, association response 프레임이다. 이 가운데 probe request 프레임은 스테이션이 액세스 포인트와 연결을 이루기 전에 액세스 포인트를 확인하기 위해 이용된다. 따라서, 이것은 스테이션의 존재를 확인할 수 있는 단서가 된다.

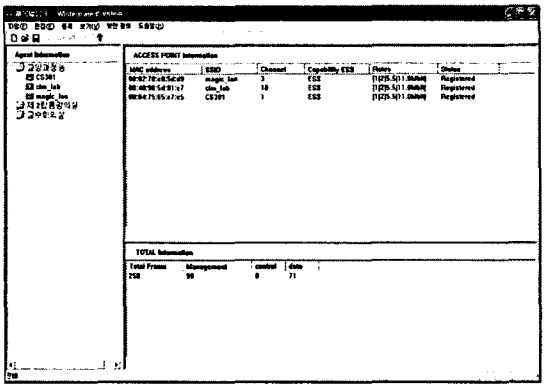
3.2.3 보안 정보 추출

보안 정보는 무선 네트워크의 공격에 대한 징후를 파악하기 위한 정보를 의미한다. 보안 정보는 단위 시간당 전달되는 ARP 패킷의 개수, 단위 시간당 전달되는 Association Request 프레임의 개수, 단위 시간당 전달되는 Authentication 프레임의 개수, 허가되지 않은 위장 액세스 포인트 혹은 스테이션의 목록, 워 드라이빙(War Driving)을 수행하고 있는 스테이션의 목록을 포함한다. 이러한 정보는 특히 세션 하이재킹, DoS, 워 드라이빙 공격에 대한 징후 탐지를 목적으로 한다. 이러한 보안 정보들은 무선 네트워크의 위치와 평소 트래픽의 사용량, 이용하는 스테이션의 특성에 따라 다르게 적용될 수 있다. 이것은 보안 정책의 설정을 통해서 각 무선 네트워크의 특성에 따라 공격 징후를 판별할 수 있도록 한다. 특히, ARP패킷의 개수와 association request 프레임의 개수, Authentication 프레임의 개수는 무선 네트워크의 규모에 따라 상이하다. 따라서, 보안 정책에 포함되는 내용은 트래픽의 경고 수준의 임계값와 위험 수준의 임계값 설정을 통해 보안 수준을 설정할 수 있다.

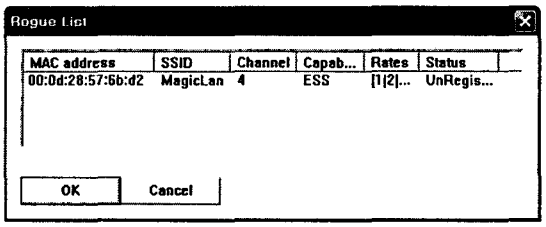
4. 구현

정보 수집 에이전트는 RedHat Linux 9.0 version, pcap 라이브러리 0.7.2를 참조하여 구현되었다. 그리고, 무선랜 카드는 Cisco Aironet 350을 이용하였다. 정보 수집 에이전트는 두 개의 쓰레드를 포함하고 있으며, 그 중 하나는 관리 프레임을 버퍼링 작업을 수행하고 있으며, 다른 쓰레드는 버퍼링된 데이터를 통해, 정보를 추출하는 작업을 진행한다. 추출된 정보는 모니터링 통계 정보, 상태 정보, 보안 정보로 구체화되고, 통합 관리 서버의 요청에 따라, 적합한 정보를 전달해 주는 역할을 수행한다. (그림 4)는 정보 수집 에이전트에 의해 수집된 정보들을 간단한 애플리케이션을 통하여 보여주고 있다.

그리고 (그림 5)는 위장 액세스 포인트를 설치했을 경우 판별한 내용이다. 액세스 포인트는 주기적으로 beacon 프레임을 브로트 캐스트하는데, beacon 프레임에는 beacon interval, capability 정보, SSID 등 액세스 포인트의 정보를 포함하고 있다. 이러한 beacon 프레임은 위장 액세스 포인트를 판별해 낼 수 있는 단서를 제공한다.



(그림 4) 에이전트에서 수집한 정보를 나타낸 화면



(그림 5) 위장 액세스 포인트 판별

일반적으로 액세스 포인트는 고정된 위치에 설치하기 때문에, 설치된 액세스 포인트의 정보를 에이전트에 등록할 수 있다. 등록된 액세스 포인트의 목록과 현재 무선 네트워크에 존재하는 액세스 포인트의 목록의 비교를 통해서 등록되지

않은 위장 액세스 포인트를 판별해 낼 수 있다.

5. 결론

무선랜 환경에서 이동 단말기와 액세스 포인트 사이에서 이루어지는 데이터 통신은 브로드캐스팅되기 때문에, 보안상 취약하다. 이러한 문제의 해결을 위해 IEEE 표준에서 무선랜 보안 표준을 기술하고 있지만, 이것은 DoS, 위장 액세스 포인트 등의 공격에 대한 근본적인 해결책은 제시하지 못하고 있다.

따라서 본 논문에서는 무선 네트워크의 실시간 모니터링 및 감시를 통하여 무선 네트워크의 취약성을 분석하기 위한 정보 수집 에이전트를 제안한다. 정보 수집 에이전트는 MAC 프레임들 가운데 관리 프레임을 대상으로 한다. 수집된 정보는 모니터링 통계 정보, 상태 정보, 보안 정보로 구분하여 추출되며, 추출된 정보는 무선 네트워크의 상태를 확인하고, 이상 징후를 탐지할 수 있는 자료가 된다.

정보수집 에이전트를 통해 분석된 자료는 무선 네트워크의 보안 정책 수립에 기틀을 제공할 수 있을 뿐만 아니라, ESM(Enterprise Security Management)과 같은 통합 보안 관리 시스템에 적용될 수 있을 것이다.

이후 연구 과제로는 이상 탐지를 위한 좀 더 구체적인 방법과 공격에 대한 대응 방안이 마련되어야 할 것이다.

참고 문헌

[1] IEEE. Lan man standard of the ieee computer society. wireless Lan medium access control (mac) and physical layer (phy) specification. IEEE Standard 802.11, 1999

[2] K. Randall and C. Nichols "Wireless Security : Model Threats and Solutions", MacGraw-Hill, 2002

[3] J. Geier, "Wireless LANS", SAMS, 2001

[4] B. Christian and B. Tony, O. Eric and P. Jeffrey, HACK PROOFING YOUR WIRELESS NETWORK, SYNGRESS, 2002

[5] R. T. Braden, "A Pseudo-machine for Packet Montoring and Statics," In proceedings of SIGCOMM '88,1988,ACM