IEEE 802.1x AP에서의 TTL 기반 패킷 마킹 기법을 이용한 무선 트래픽 분류 및 IP 역추적 기법

TTL based Advanced Packet Marking Mechanism for Wireless Traffic Classification and IP Traceback on IEEE 802.1x Access Point

이형우
한신대학교 컴퓨터정보소프트웨어학부

Hyung-Woo Lee(hwlee@hs.ac.kr)

요약

IEEE 802.1x 기반 무선랜 환경은 Auth/Deauth Flooding 공격과 같이 무선랜 프로토콜의 취약점을 이용한 DoS 공격 등에 노출되어 있다. 무선랜 공격자는 유선에서와 마찬가지로 근원지 IP 주소를 스푸핑하여 대량의 트래픽을 발생시키는 등 무선 네트워크에 대한 DoS 공격을 수행할 수 있다. 따라서 무선랜에 대한 공격에 능동적으로 대응하기 위해서는 기존의 유선망에서의 IP 역추적 기술을 변형하여 무선망에 적용할 수 있다. 이에 본 연구에서는 무선랜 환경에서 발생하는 트래픽에 대해 TTL 기반의 개선된 패킷 마킹 기법을 제시하여 무선 트래픽에 대한 분류 기능도 제공하면서 동시에 스푸핑된 무선 IP 패킷의 근원지 정보를 재구성하는 기법을 제시한다. 실험 결과 AP를 기반으로 역추적 기능을 이용하여 보다 안전한 무선랜 환경을 구축할 수 있었다.

■ 중심어 : | 무선랜 | IEEE 802.1x | 역추적 | 트래픽 분류 | 패킷마킹 |

Abstract

The vulnerability issue on IEEE 802.1x wireless LAN has been permits the malicious attack such as Auth/Deauth flooding more serious rather than we expected. Attacker can generate huge volume of malicious traffic as the same methods on existing wired network. The objective of wireless IP Traceback is to determine the real attack sources, as well as the full path taken by the wireless attack packets. Existing IP Traceback methods can be categorized as proactive or reactive tracing. But, these existing schemes did not provide enhanced performance against DoS attack on wireless traffic. In this paper, we propose a "TTL based advanced Packet Marking" mechanism for wireless IP Packet Traceback with wireless Classification function. Proposed mechanism can detect and control DoS traffic on AP and can generate marked packet for reconstructing on the real path from the non-spoofed wireless attack source, by which we can construct secure wireless network based on AP with enhance traceback performance.

■ keyword : | Wireless LAN | IEEE 802.1x | Traceback | Packet Classification | Packet Marking |

* 본 연구는 학술진흥재단 2005년 지역대학우수과학자지원과제(KRF 2005-202-D00487)의 연구지원으로 수행되었습니다.
* 본 연구는 2006년 정보통신부 및 정보통신연구진흥원의 대학IT연구센터 지원사업의 연구지원으로 수행되었습니다. (IITA-C1090-0603-0016)

접수번호 : #061128-003
접수일자 : 2006년 11월 28일
심사완료일 : 2006년 12월 20일
교신저자 : 이형우, e-mail : hwlee@hs.ac.kr

Ⅰ. 서 론

최근 IEEE 802.1x를 기반으로한 무선랜(Wireless LAN)이 급속도로 확산되고 있다. 무선랜을 이용하여 인터넷을 이용할 경우 기존의 유선 기반 네트워크 구성보다 저렴하면서도 편리하게 인터넷을 사용할 수 있어서 현대 대학 캠퍼스망, 기업 및 가정 등에서 급속도로 확산되고 있다. 하지만 무선랜 공격자는 유선에서와 마찬가지로 근원지 IP 주소를 스푸핑하여 대량의 트래픽을 발생시키는 등 무선 네트워크에 대한 DoS 공격을 수행할 수 있다[1][2].

네트워크 관리자 입장에서는 기존의 백본망을 통해 전달되는 패킷을 모니터링할 경우 기존의 유선 인터페이스를 통해 전송되는 패킷과 무선 인터페이스를 이용한 트래픽에 대해 별다른 분류 방법이 없는 현실이다. 단순히 전송되는 패킷에 기록된 IP 정보만을 가지고 유선과 무선 사용자를 구별할 수 있으나, 만일 IP 주소에 대해 스푸핑(IP Spoofing)을 하여 송신한다면 이것 역시 정확하게 유선과 무선 트래픽을 구별해 낼 수 없다[1].

특히 무선랜 등을 통한 공격 툴에 대해서는 손쉽게 구할 수 있으며 무선랜을 통한 공격인 경우 기존의 유선 보다도 훨씬더 추적 등이 어렵기 때문에 이에 대한 대응 기법 등에 대한 연구가 필요한 실정이다.

무선랜을 이용하기 위해서는 AP(Access Point)를 설치하여 무선 랜카드를 장착한 노드와 통신하게 된다[3]. 현재의 IEEE 802.1x 기반 무선랜 사용자 환경에서는 기존의 유선망에서와 같이 서비스 거부 공격(DoS: Denial of Service)[2]을 통해 손쉽게 공격 가능하기 때문에 최근에는 무선 침입탐지 시스템(W-IDS:Wireless Intrusion Detection System)[4-6]을 통한 대응 기술이 제시되고 있다. 하지만 이것 역시 무선 인터페이스를 통해 AP 또는 목적지 시스템에 도착한 이상 트래픽에 대한 검출 및 차단 기능만을 제공하는 수동적 해킹 대응 기술이다. 따라서 기존의 W-IDS는 무선 네트워크 환경에서의 DoS 공격 근원지에 대한 확인, 추적 등과 같이 능동적인 측면에서의 해킹 대응 기능을 제공하지 못하고 있다.

무선랜 환경에서의 공격 기법 역시 기존의 유선을 통한 공격과 마찬가지로 무선 사용자의 근원지 IP 주소를 스푸핑하는 방식으로 수행되므로 이에 대한 능동적 대응 기술이 개발되어야 한다. 유선 트래픽을 대상으로 패킷의 특정한 필드에 마킹하여 근원지를 역추적 하는 기법이 제시되었다. 이와 마찬가지로 무선랜 트래픽 역시 역추적 및 분류를 위해서는 우선적으로 AP를 통해 전달되는 패킷에 대해 라우터 또는 목적지 노드에서 이를 판별할 수 있어야 한다[4]. 무선랜을 통해 전달된 트래픽에 대한 판별을 위해서는 기존의 유선 방식과 마찬가지로 AP를 중심으로한 무선랜 기반 프로토콜에서 IP 패킷에 대한 식별 및 판단 기능을 제공할 수 있어야 한다.

본 연구에서는 IEEE 802.1x 기반 무선랜 환경에서 유무선 트래픽에 대한 판별/분류 기능을 제공하면서도 무선랜 인터페이스를 통한 DoS 공격에 능동적으로 대응하기 위해 AP를 기반으로 스푸핑된 패킷에 대한 IP 역추적 기능을 제공하고자 한다. AP에서 트래픽에 대한 전달/제어 기능을 수행하면서 동시에 DoS 공격이 발생하였을 경우 라우터는 역추적 정보를 해당 패킷의 헤더에 마킹하여 전달하게 된다. 라우터는 마킹된 정보를 기반으로 일차적으로 무선 인터페이스를 통해 전달된 패킷이라는 것을 확인할 수 있으며, 동시에 무선 기반 공격자에 대한 역추적 기능을 제공할 수 있게 된다. 본 연구에서는 TTL 필드 정보를 이용하여 AP 경로 정보를 마킹하는 새로운 기법을 제시하였다. 제시된 기법은 무선 네트워크 환경에서 패킷에 대한 분류 기능을 제공하면서도 안전성을 향상시킬 수 있다.

Ⅱ장에서는 IP 스푸핑 공격 등과 같은 기존의 무선 공격 기법과 이에 대한 대응 방안을 고찰하고, Ⅲ장에서는 무선 프로토콜 구조 및 패킷 분류의 중요성에 대해 고찰하였다. Ⅳ장에서는 무선랜에서의 스푸핑된 형태의 DoS 공격 근원지를 역추적하기 위해 TTL 기반의 새로운 패킷 마킹 기법을 제시하였으며 Ⅴ장에서는 제시한 기법에 대한 성능을 비교 평가하였으며 마지막 Ⅵ장에서는 결론을 맺는다.

II. IEEE 802.1x 기반 무선랜

1. IEEE 802.1x 무선랜 프로토콜

무선 LAN은 액세스 포인트(AP : Access Point)와 무선랜 네트워크 어댑터(WNIC : Wireless Network Interface Card)로 구성된다. AP는 유선 네트워크에 접속되어 무선 사용자들의 트래픽을 중계하는 역할을 담당하는 장비이고 WNIC은 해당 무선 단말을 의미하는 스테이션(STA: Wireless Station)에서 AP로 접속하기 위한 네트워크 인터페이스를 담당하는 장비이다[3][4].

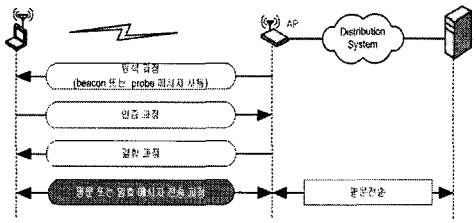

그림 1. IEEE 802.1x 무선랜 연결 구조

IEEE 802.1x 기반 무선랜 프로토콜은 [그림 1]과 같은 과정을 통해 무선 인터넷 서비스를 제공한다. 가상 캐리어 감지 방식을 이용하여 패킷에 대한 충돌을 회피하는 방식으로 작동하는 CSMA/CA 기법을 적용하고 있다. 구체적으로는 RTS(Request To Send) 및 CTS(Clear To Send) 메시지를 전송하여 NAV (Network Allocation Vector) 값을 설정하는 방식으로 채널을 점유한다[10].

또한 [그림 2]와 같은 IEEE 802.1x MAC 프레임을 생성하여 노드와 AP는 무선 인터페이스를 제공하게 된다[3].

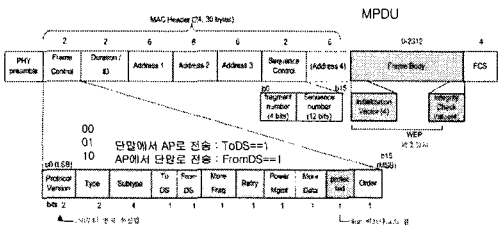

그림 2. IEEE 802.1x MAC 프레임 구조

2. 유무선 트래픽 분류의 어려움

AP를 통한 무선 트래픽과 기존의 유선망을 통해 전달되는 트래픽을 구별하는 것은 매우 어렵다. [그림 3]과 같이 유선과 무선은 서로 복합적으로 연결되어 있다. 라우터에서는 단순히 패킷의 발신자 IP 정보 등을 통해 추출해 낼 수 있으나 유무선을 구별할 수 있는 방법은 단순히 IP 리스트만을 가지고 판별하는 방법밖에는 없다. 하지만 이것 역시 공격자에 의해 송신자 IP가 스푸핑되어 전달된다면 유선망과 무선망을 통한 전송을 판별할 수 있는 방법은 뚜렷하게 없는 것이 현실이다. 특히 최근에는 무선망을 이용한 공격 등이 널리 확산되고 있어서 단순히 IP 주소 리스트 값만 가지고는 발신자 정보를 판별할 수 없다.

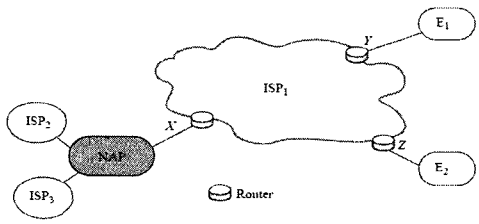

그림 3. 유무선 네트워크 연결 구조

물론 [그림 4]와 같이 라우터 A에서 노드 B로 동일한 패킷 두개를 전송하여 이에 대한 응답 시간을 분석하여 노드 B에 대한 접속 형태를 판별하고자 하는 연구도 수행되었다[4].

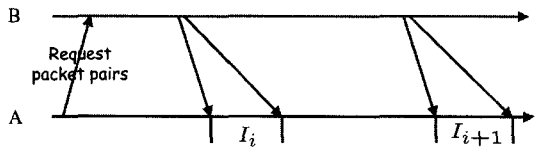

그림 4. 유무선 트래픽 판별 방식

하지만 이와 같은 연구인 경우 노드 B가 정상적인 노드일 경우만 가능하며 만일 공격자 노드와 같은 형태라면 A로부터 전달된 패킷에 대해 응답하지 않게 되어 연결 형태에 대한 정확한 분류 역시 어렵다는 단점이 있다.

USN 등 무선 망을 통한 서비스 등이 확산되고 있기

때문에 무선 인터페이스 등을 기반으로한 공격에 대한 대응 방안이 제시되어야 하는 실정이다. 유비쿼터스 환경에서 사용하는 기본적인 네트워크 방식은 무선 방식을 사용하고 있기 때문에 무선 인터페이스를 통한 공격 등에 대한 판별 기능을 제공해야 한다. 따라서 우선 무선랜에서의 취약점을 이용한 대표적인 공격 기법에 대해 고찰해 보면 다음과 같다.

3. 무선랜의 취약성

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]. 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 AP (Access Point)의 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 이루어진다[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.

무선 패킷 스니핑을 하기 위해서는 에어로피크(AiroPeek) 등을 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 Brute-Force 공격이나 Dictionary 공격 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 이루어질 수 있다.

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

4. 무선랜 공격 기법

악의적인 사용자들에 의해서 사이버 공격 기법은 날로 다양해지고 있으며, 해킹 기법의 발달로 자동화, 지능화 된 해킹 툴이 공개적으로 유포되어 국내·외 해킹 발생빈도는 급격히 증가하고 있는 추세이다. 특히 네트워크의 취약점이 지속적으로 증가하고 있으며, 웜바이러스와 같은 치명적인 공격에 의해 네트워크 서비스를 마비시킬 수 있는 분산 서비스 거부 공격(DDoS :Distributed Denial of Service)이 급증하고 있는 가운데 무선 네트워크상에서의 무선랜 공격은 [그림 5]와 같이 passive, active, rogue AP 공격으로 분류할 수 있다[7][8].

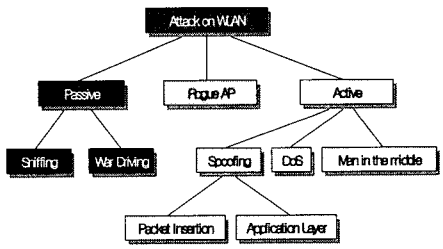

그림 5. 무선랜 공격 유형

4.1 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.

4.2 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 유도하거나 MAC을 spoofing 하여 세션을 가로채는 기법이다. 또한 [그림 6]과 같이 DDoS 공격이 가능하기 때문에 이에 대한 대응 기술이 제공되어야 한다[3][4].

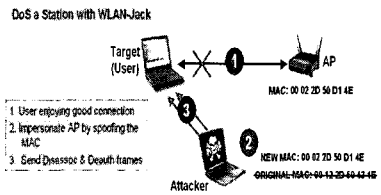

그림 6. 무선랜 DDoS 공격 기법

5. 해결방안 : 무선 트래픽 마킹을 통한 패킷 분류 및 역추적

무선랜에 대한 취약점을 보완하면서도 DoS 공격 등과 같이 무선랜을 이용한 공격에 능동적으로 대응하기 위해서는 AP를 통해 전달되는 패킷에 대해 마킹을 수행하고 이를 통해서 수신자 또는 라우터에서 이를 판별하여 기존의 Wireless IDS/IPS 기능과 접목하는 방법이 필요하다[6].

본 연구에서는 기존의 패킷 마킹 기법에 대해 분석하고 이를 무선망에 적용하기 위한 방법에 대해 제시하고자 한다.

III. 기존의 IP 역추적 기법

1. IP 스푸핑 기반 DoS 공격 대응 방법

기존의 기법은 [그림 7]과 같이 공격자가 IP 스푸핑 방식을 통해 공격하였을 경우 역추적 경로를 찾아 해커의 위치 또는 접속 경로 등을 파악하는 방법이 제시되어야 한다.

기존의 유선망에서는 라우터를 중심으로 IP 스푸핑된 패킷에 대해 일정한 확률 P로 패킷을 선택하여 라우터 자신의 ID 정보와 IP주소 정보를 패킷 헤더에 마킹하는 방식을 사용하고 있다. 피해 시스템에서는 마킹된 정보가 도착하면 패킷에 기록되어 있는 라우터 관련 마킹 정보를 추출하여 스푸핑된 패킷의 실제적인 공격 경로를 재구성하는 방식을 사용하고 있다[8].

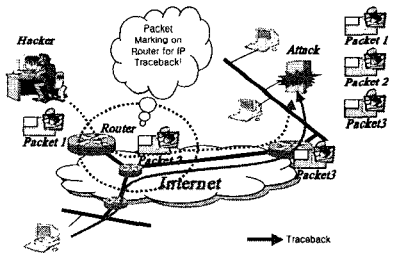

그림 7. 공격 근원지 역추적을 위한 패킷 마킹

패킷 전달 과정에서 각각의 라우터는 IP 계층에 해당하는 패킷 헤더 정보에서 라우터가 수정 가능한 부분을 선택하여 라우터 자신의 IP 주소 정보를 마킹하게 된다. 현재까지 제시된 기법에서는 일반적으로 IP 헤더 구조에서 ID 필드에 해당하는 16비트 필드 정보에 라우터 자신의 IP 주소 정보를 마킹하는 방식을 사용하고 있다.

2. 역추적 기술 분류

역추적 기술을 시스템 측면에서 분류하면 크게 IP 패킷 역추적 기술과 연결 역추적 기술로 분류할 수 있다. IP 패킷 역추적 시스템인 경우 DoS 공격에서 IP 주소가 변경된 경우 이를 찾아내기 위한 방법을 제공한다. Host B에 패킷을 보낸 시스템의 실제 위치를 추적하는

방식으로 패킷에 대한 마킹 기법(Marking)을 적용한다[9][10].

역추적 기술을 다시 세분화하면 호스트 기반 역추적, 네트워크 기반 역추적으로 구분할 수 있다. 호스트 기반 역추적 시스템(Host-based traceback system)은 모든 호스트에 역추적 모듈을 설치하는 방식이다. 따라서 모든 역추적 경로상의 호스트들로부터 정보를 얻어야 역추적이 가능한 기법이다. 기존의 모든 시스템에 역추적 모듈을 설치한다는 것이 상당히 어렵기 때문에 현재의 라우터에 많은 부분 수정을 가해야 한다는 단점이 있다[9-11].

네트워크 기반 역추적 시스템(Network based traceback system)은 네트워크 상에 송수신되는 패킷들로부터 정보를 추출하여 존재하는 연결 정보들간의 연관성을 파악하여 역추적 경로를 파악하는 방식이다[9-11]. 예를 들어 해커가 ls 및 cd 라는 명령어를 계속적으로 입력하였을 경우 이와 같은 명령어가 흘러가는 경로를 분석하여 전체적인 해킹 및 바이러스 경로를 분석하는 방식이다. 역추적 기법 등 중에서 기존의 패킷 마킹 기반 역추적 기법은 다음과 같다.

3. 기존 역추적 기술 분석

일반적으로 패킷 마킹 기법은 기존의 다른 IP 역추적 기법과 달리 관리 부하가 적으며, 네트워크에 대한 부하 및 분산 처리 기능이 우수하다고 할 수 있다. 그러나 확률 p로 샘플링하여 마킹하는 과정에서 상대적으로 많은 패킷을 샘플링해야 하고 경로 재구성 과정에서도 완전한 경로를 재구성할 수 없다는 단점이 있기 때문에 라우터에서의 부하가 크며 보안 기능도 취약하다[11].

또한 기존의 기술은 네트워크 패킷 중심에서 각 트렌젝션간의 연계성을 이용한 연결 중심 방식의 네트워크 기반 역추적 기술이지만, 해킹 및 바이러스에 대처하기 위해 지금까지 제시된 방식에서는 현재의 인터넷 네트워크 구조를 전체적으로 변경하고 새롭게 개선된 환경을 구축한 다음에 적용 가능하다는 단점을 갖고 있다.

특히 기존의 패킷 마킹 기법은 패킷을 확률 p로 샘플링하여 마킹 후에 전송하는 과정에서 만일 특정 라우터에서의 에지 정보 또는 노드 정보 등이 마킹되지 않고 전달된다면 나머지 마킹된 정보를 가지고는 완벽한 공격 경로를 재구성할 수 없다는 문제점도 발견할 수 있다[11].

또한 기존의 PPM 기법[12]인 경우 패킷에 대해 일정 확률 p를 만족할 경우 샘플링하여 전송하는 기법을 사용하는 과정에서 DDoS 공격 트래픽에 대해서 마킹하지 않고 보내는 경우도 발생한다. 이 경우 DDoS와 같은 해킹 공격이 발생하였을 경우 스푸핑된 공격 근원지를 재구성할 수 없다는 단점이 있다. 또한 무선 환경에 적용할 경우 많은 수정/보완이 필요한 실정이다. 이밖에 해쉬 기법을 이용한 역추적[13] 기법 및 ICMP 방법을 이용한 역추적[14] 방법 등이 제시되었다. 또한 패킷 필터링 기법을 이용한 기법[15]도 제시되었지만 기존의 기법에 대해 무선 트래픽을 대상으로 적용하기 위해서는 재고찰이 수행되어야 한다.

따라서, 본 연구에서는 기존의 환경적 변화를 최소화하면서도 무선 트래픽에 대한 분류 및 역추적 기능을 제공하기 위해 AP 기반의 능동적인 역추적 기능을 제공하기 위해 새로운 접근 방식을 제시하고자 한다.

IV. AP에서의 TTL 기반 DoS 패킷 마킹 기법

1. 패킷 마킹을 위한 네트워크 구조

네트워크는 노드 집합 V와 에지 집합 E로 구성된 그래프 $G=(V,E)$로 정의할 수 있다.

$G=(V,E))$ V: 라우터 또는 AP, E: 단말

다시 네트워크 노드 집합 V는 종단 시스템과 내부 노드에 해당하는 라우터로 나눌 수 있다. 에지는 V 집합 내에 있는 노드들에 대한 물리적인 연결에 해당한다. 또한 공격자와 피해 시스템을 아래와 같이 정의할 수 있다.

$S \subset V$: 공격자, $t \in V/S$: 피해 시스템

만일 $|S| = 1$ 일 경우 단일 공격자에 의한 해킹 공격을 의미하고, 만일 공격자에 의한 경로 정보가 $P = (s, v_1, v_2, \ldots, v_d, t)$ 이라면 이는 공격 시스템 s에서 피해 시스템 t로 d개의 AP와 라우터를 통해 전

달된 공격 경로를 의미한다.

이때 전달된 패킷의 수를 N이라고 하자. 만일 패킷 내에 라우터에 대한 링크 정보 $(v, v') \in E$를 마킹할 수 있는 필드가 있다면 이를 확률 p로 샘플링하여 전달하게 된다. 패킷에 대해서 라우터에서는 일정한 확률로 패킷을 선택하여 에지에 대한 정보와 라우터에 대한 거리 정보를 패킷내에 포함시켜 전달할 수 있다.

기존의 기법에서는 임의의 확률 p로 패킷을 선택하여 여기에 라우터에 대한 링크 정보를 마킹하여 전달하게 된다. 만일 네트워크 상에서 노드 v_i에서 마킹하였을 경우 다른 라우터에 의해서는 재마킹되지 않고 전달될 확률 α_i을 계산하면 다음과 같다.

$$\begin{aligned} \alpha_i &= Pr\left(x_d = (v_{i-1}, v_i)\right) \\ &= p\left(1-p\right)^{d-1} \left(i = 1, 2, \ldots, d\right) \end{aligned} \quad (1)$$

따라서 확률 α_i는 공격자에 해당하는 패킷 정보가 다른 라우터에 의해서는 재마킹되지 않고 피해 시스템에 전달될 확률을 의미한다. 결국 피해 시스템에서 α_i 값을 높이기 위해서는 p 값을 크게 해야 하는데, 이는 라우터에서 빈번하게 마킹 과정을 수행해야 한다는 것을 의미하므로 기존의 기법에서는 결과적으로 네트워크 성능을 저하시키게 된다.

본 연구에서 제시하는 기법은 AP에서 임의의 확률 p로 패킷을 샘플링하여 마킹하지 않고 이상 트래픽이 발견되었을 경우 패킷에 대한 마킹 과정을 수행하게 된다. 본 연구에서 제안한 구조는 [그림 8]과 같다.

본 연구에서 제시한 기법은 다음과 같다.

[단계 1] AP에서는 수신된 패킷에 대해 폭주 여부를 판단

[단계 2] 만일 일반 패킷일 경우

[단계 2-1] 패킷에 대한 마킹 여부를 확인

[단계 2-2] 만일 마킹되어 있지 않으면 AP에 대한 주소 정보에 대해 마킹하여 전달한다.

[단계 3] 무선랜을 통한 DoS 공격 등에 해당하는 이상 트래픽인 경우

[단계 3-1] TTL 필드 값을 추출

[단계 3-1] TTL 필드 값을 이용하여 패킷 마킹을 수행하고 다음 노드로 전송

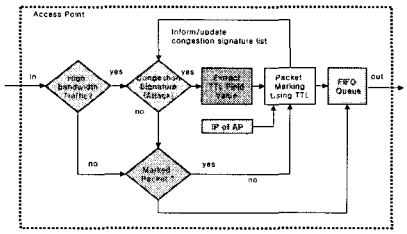

그림 8. 제안한 라우터 기반 DDoS 근원지 역추적 구조

본 연구에서 개발한 AP의 내부 구조는 [그림 9]와 같다. 앞에서 제시한 바와 같이 무선랜을 구성하는 AP에서는 패킷에 대한 분석을 통해 침입 여부를 판별하고 이상 트래픽에 대한 할 경우 패킷에 대한 마킹 과정을 수행한 후에 다음 노드로 전송한다.

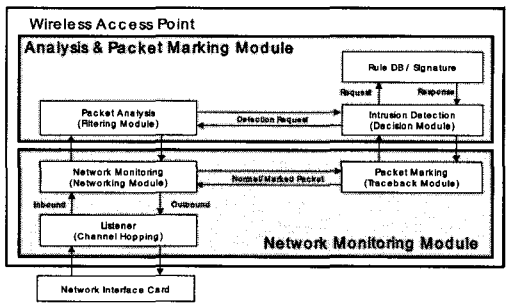

그림 9. AP에서의 패킷 마킹 구조

제안한 구조에서는 라우터에 들어온 패킷에 대해 트래픽의 대역폭을 검사하고 일정 이상으로 도착하게 되면 공격 형태에 해당하는 혼잡 시그너쳐인지를 판단하게 된다. 만일 공격 형태 트래픽에 해당한다면 패킷에 마킹과정을 수행하고 동시에 해당 패킷에 대한 pushback 메시지를 생성하여 이를 라우터의 출력 큐로 하여금 앞단에 위치한 라우터에게 전송토록 한다. 만일 대역폭 조건을 만족하지 않을 경우에는 이전에 트래픽에서 유사한 패킷이 있었는지를 확인하고 만일 해당된다면 마찬가지로 패킷에 대한 마킹 과정을 수행한다.

위 조건을 만족하지 않을 경우 일반적인 트래픽으로 간주하여 다음 라우터로 전달한다.

2. TTL 필드 정보를 이용한 패킷 마킹 기법

2.1 패킷 헤더 마킹 필드 M_x

AP R_x의 IP 주소를 A_x라고 하자. [그림 10]과 같이 R_x에 도착한 IP 패킷을 P_x라고 할 때, P_x에서의 해더에서 마킹 정보를 저장할 수 있는 25 비트를 M_x라고 하자.

[AP, 패킷 및 주소 기호]

- AP : R_x
- AP의 IP 주소 : A_x
- AP R_x에 도착한 패킷 : P_x
- 패킷에서의 변형 가능한 헤더 25 비트 : M_x
- AP로부터 전달받은 라우터 : R_y
- AP 다음 라우터의 IP 주소 : A_y

패킷 P_x에서 M_x는 [그림 10]과 같이 TOS(type of service) 필드 8비트와 ID 필드 16비트 및 Fragmentation 필드에서 사용하지 않는 1비트로 구성된다. TOS 필드인 경우 현재 필드에 대한 정의만 되어 있을 뿐 실제적으로 사용하고 있지 않다. 따라서 TOS 필드 값을 사용한다고 하더라도 전체 네트워크에 영향을 미치지 않는다. 현재의 TOS 필드는 상위 3비트가 우선순위 비트로 설정되어 있고, 다음 3비트는 최소지연, 최대 성능 및 신뢰성 필드로 정의되어 있으나 현재는 사용하고 있지 않다.

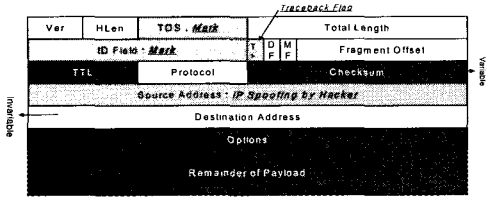

그림 10.제안한 기법에서의 패킷 마킹 필드

2.2 TTL 정보를 이용한 마킹

25비트 M_x 정보에 대해서 AP R_x에 대한 IP 주소 A_x 값을 패킷 헤더에 마킹하는 구조는 [그림 11]과 같다.

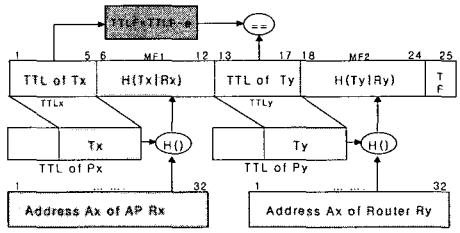

그림 11.제안한 기법에서의 패킷 마킹 구조

모든 패킷의 TTL(time to live) 필드는 8비트 정보로 구성되며 패킷 전송시 TTL 값은 1씩 감소되어 최종적으로 목적지에 전달된다. 이때 다음과 같이 패킷의 전송거리(hop count)를 정의할 수 있다.

[전송거리] 만일 패킷 P_x가 피해 시스템 V에 도착하였을 경우 TTL 값의 변화는 AP에서 피해 시스템까지의 전송 거리를 의미한다.

임의의 AP R_x에 도착한 패킷 P_x의 TTL 필드에 설정되어 있는 값을 $TTL of\ P_x$라고 하였을 경우, 이 값은 근원지 호스트에서 AP R_x까지의 전송 거리(hop count)에 해당하는 정보를 포함하고 있다. 그리고 따라서 패킷에서의 TTL 필드 값을 이용한다면 패킷에 전달된 경로 정보와 연계하여 역추적 방식에 활용할 수 있다.

기존의 패킷 마킹 기법에서는 TTL 값을 사용하지 않고 다만 ID 16 비트 필드 내에 별도의 hop 카운터 필드를 두어 마킹을 수행한 AP에서 패킷이 전달된 거리 정보를 계산하도록 하였다.

기존의 기법에서는 패킷의 16비트 ID 필드 내에 5 비트 hop 카운트 필드를 설정하여 마킹 과정에서 1로 설정하여 패킷을 전달하고 다음 라우터에서는 이 값을 1씩 증가시키는 방식을 사용하였다. 그러나 이와 같은 경우 패킷이 전달되는 경로상에 있는 모든 AP가 ID 필드내에 있는 5비트 필드 값을 반드시 1씩 증가시켜주어야 경로 계산이 정확해 진다는 단점이 발생한다. 따라

서 본 연구에서는 AP R_x에 도착한 패킷 자체에서의 TTL의 특성을 이용하여 마킹하는 방법을 사용하였다.

3. TTL 기반 패킷 마킹 방식

이상 트래픽이 발생하게 되면 AP R_x에서 패킷 P_x에 대해 마킹 과정을 수행하는 과정을 살펴보면 다음과 같다.

우선 이상 트래픽 패킷에 대해 AP에서 마킹이 가능한 25 비트 필드에 정보를 삽입하여야 한다. 이때 25 비트 필드에는 패킷이 전달된 경로 정보를 모두 포함하고 있어야 하기 때문에 AP R_x 자신의 32 비트 IP 주소 A_x와 다음 단계 라우터 R_y의 32 비트 IP 주소 A_y에 해당하는 64 비트 정보를 패킷 내에 마킹하여야 한다.

25 비트 내에 AP와 라우터 주소 값을 동시에 마킹하기 위해서는 해쉬 함수를 적용할 필요가 있고, 해쉬 함수를 이용하게 되면 AP 및 라우터에 대한 인증 기능도 제공하면서 해당 패킷에 대한 전송 경로를 25 비트 내에 마킹할 수 있게 된다. 이를 위해 본 연구에서는 AP의 IP 주소 32 비트 정보에 대해 7 비트 해쉬 함수를 적용하여 생성된 값을 패킷에 마킹하는 방식을 사용하였다.

AP R_x에 도착한 패킷 P_x가 이상 트래픽에 해당된다면 아래와 같은 과정을 수행한다.

[일반적 특징] 유무선 네트워크 패킷은 일반적으로 32홉 이상 전송되지 않음

패킷이 전달되는 과정에서 일반적으로 네트워크 홉 최대 거리는 일반적으로 32 홉 이상을 넘지 않기 때문에 AP R_x에 도착한 패킷 P_x에 대해 IP 패킷의 TTL 필드 8비트에서 TTL 필드 하위 5 비트 정보만으로도 패킷이 전달된 홉 거리 정보를 계산할 수 있다.

[단계 1] TTL 필드에서 하위 5비트 정보를 추출하여 P_x^{TTLx}에 저장

패킷 P_x에서 TTL 필드에서 하위 5비트 정보에 추출하여 이를 T_x라고 하고 [그림 10]에 제시된 TOS 필드에서의 상위 5비트 필드 P_x^{TTLx}에 저장한다.

TTL 필드 5비트를 추출하는 함수를 $Mask(P_x) = TTLof P_x \wedge 00011111$와 같이 정의할 수 있다.

$$T_x = Mask(P_x),\ P_x^{TTLx} = T_x \qquad (2)$$

□ T_x : 공격 근원지 시스템으로부터 패킷이 AP까지 전달된 홉 거리 정보를 의미함

따라서 T_x 값을 패킷에 마킹하여 목적지 피해 시스템 V에 전송하였을 경우, V에 도착한 패킷에서의 TTL 값과 마킹되어 전달된 T_x 값을 비교한다면 패킷이 AP R_x로부터 피해 시스템까지 전달된 홉 거리 정보를 계산할 수 있다.

[단계 2] $H(T_x|A_x)$ 값을 생성하여 P_x^{MF1}에 마킹하고 P_x^{TF}를 1로 설정

패킷 P_x에서의 5 비트 TTL 값 T_x과 AP R_x 자신의 IP 주소 A_x에 대해 해쉬 함수 $H(\cdot)$를 사용하여 7 비트 해쉬 값 $H(T_x|A_x)$를 계산하고 이를 P_x^{MF1}에 마킹한다. 그리고 동시에 역추적 마킹 필드 P_x^{TF} 값을 1로 설정하여 패킷 전송 경로상의 다음 라우터 R_y로 전송한다.

$$P_x^{MF1} = H(T_x|A_x),\ P_x^{TF} = 1 \qquad (3)$$

[단계 3] 다음 라우터 R_y는 패킷 마킹 여부를 확인함

라우터 R_y에 도착한 패킷을 P_y라고 하자. 패킷이 전송되는 경로상에 있는 임의의 라우터 R_y는 이상 트래픽에 해당하는 패킷에 대해 우선 P_x^{TF} 필드 값을 보고 만일 1로 설정되어 있는 경우 다음과 같은 검증 과정을 수행한다.

[단계 4] 라우터 R_y에서 T_y를 생성하여 P_y^{TTLy}에 마킹

P_y에서의 8비트 TTL 필드에서 5비트 정보를 T_y를 추출하고, T_y 값과 패킷에서의 $TTLx$ 필드에 저장된

T_x 값에 대해 $T_x XOR T_y$를 수행하여 이 값을 P_y^{TTLy}에 마킹한다.

$$T_y = Mask(P_y),\ P_y^{TTLy} = T_x XOR T_y \quad (4)$$

□ P_y^{TTLy} : AP R_x와 라우터 R_y간의 홉 거리를 의미한다.

[단계 5] $H(T_y|A_y)$ 값을 생성하여 P_y^{MF1}에 마킹하여 전송

이제는 라우터 R_y에 도착한 패킷 P_y에서의 TTL 필드 5비트 정보 T_y와 자신의 IP 주소 A_y에 대해 해쉬 함수 $H()$를 적용하여 이를 P_y^{MF2} 필드에 마킹한다. 마킹된 패킷은 이제 최종 목적지 V로 전송된다.

$$P_y^{MF2} = H(T_y|A_y) \quad (5)$$

4. 역추적 경로 재구성

4.1 DoS 공격 패킷 역추적

네트워크를 통해 전달된 패킷에 대해 피해 시스템 V에서는 DoS 공격 경로를 재구성하게 된다. [그림 12]와 같이 DoS 공격을 $S1, S2, S3$에서 수행하였다고 가정하자. 공격 패킷에 대해 AP R_x, R_y 및 R_z는 패킷 헤더 25 비트 정보내에 AP 자신의 IP 정보와 패킷에서의 TTL 필드 5비트 정보를 조합하여 각각 마킹하였다. 피해시스템에서는 DDoS 공격이 발생하였을 경우 도착한 패킷에 대해 아래와 같이 경로 역추적 과정을 수행한다.

□ P_v : 피해 시스템 V에 도착한 패킷이라고 할 경우, P_v 값은 DoS 공격에 해당하는 패킷들로 구성된 집합

□ M_v : 이 중에서 AP에 의해 마킹되어 전달된 패킷을 정의

피해 시스템에 도착한 패킷 집합 P_v에서 M_v를 구별하는 방식은 다음과 같이 P_v에 속한 임의의 패킷 P_x에 대해서 TF 필드에 해당하는 P_x^{PF} 부분이 설정되어 있는 패킷을 샘플링하는 과정을 수행하면 된다.

$$M_v = [P_x|P_x^{TF} == 1, x \in v] \quad (6)$$

피해 시스템에서 마킹되어 있는 패킷 M_v의 원소에 해당하는 임의의 패킷 M_i에 대해서 8비트 TTL 값을 $TTLof\ M_i$라고 할 때, 이를 M_i의 25비트 마킹 필드 T_M값과 비교한다면 패킷 M_i가 임의의 AP R로 부터 마킹된 후에 전송된 네트워크 홉 거리 $D(M_i)$를 다음과 같이 계산 할 수 있다.

□ 피해 시스템으로부터의 홉거리 $D(M_i)$

$$D(M_i) = M_{i=x}^{TTLx} - (Mask(M_i)) \quad (7)$$

만일 $D(M_i) == 1$이라면 피해 시스템 바로 앞에 있는 AP에 의해서 마킹되었다는 것을 알 수 있다. $D(M_i)$는 피해 시스템에 도착한 패킷 중에서 임의의 AP에 의해 마킹된 정보를 포함하고 있기 때문에 이를 기반으로 아래와 같은 사항을 도출할 수 있다.

[정리 1] 피해 시스템 V에 도착한 패킷 M_i에서 $d == M_{i=x}^{TTLx} - TTLof\ M_i$이라면, 이는 패킷 M_i이 피해 시스템 V로부터 홉 거리 d에 위치한 임의의 AP R_x에 의해 마킹되었다.

[정리 2] 피해 시스템 V에 도착한 패킷 M_i에서 $D(M_i) == d$이면서 $M_{i=y}^{TTLy} == \alpha$라면, 이는 패킷 M_i이 피해 시스템과 홉 거리 $d-\alpha$에 위치한 임의의 라우터 R_y에 의해 마킹되었다.

4.2 TTL 기반 DDoS 공격 경로 재구성

[단계 1] $D(M_i) == 2$를 만족하는 패킷 M_i

패킷 M_i에서 우선 2 홉 거리를 갖는 AP R_x를 다음과 같이 판별할 수 있다.

$$M_i^{MF1} == H(M_{i=x}^{TTLx}|A_x),\ (R_x \in D(M_i) == 2) \quad \text{and}$$

$$M_i^{MF1} == H(Mask(M_i)+2|A_x), \quad (R_x \in D(M_i) == 2) \tag{8}$$

[단계 2] 이제는 $D(M_j) == n, (n \geq 3)$를 만족하는 M_j에 대해서 위와 같은 과정을 반복

DoS 공격 패킷 집합 P_v에서 패킷이 전달된 실제 공격 경로를 재구성할 수 있다.

[그림 12]와 같은 네트워크 구조에 대해 본 연구에서 제시한 기법을 적용하게 되면 피해 시스템 V에 대한 DoS 공격 경로를 다음과 같이 구할 수 있다.

이와 같은 과정을 통해 AP에서는 이상 트래픽이 발생하였을 경우 DoS 공격 경로를 역추적하기 위해서 개선된 패킷 마킹 기술을 적용하여 스푸핑된 패킷에 대한 역추적 기능도 제공하여 공격자에 대한 근원지를 재구성할 수 있다.

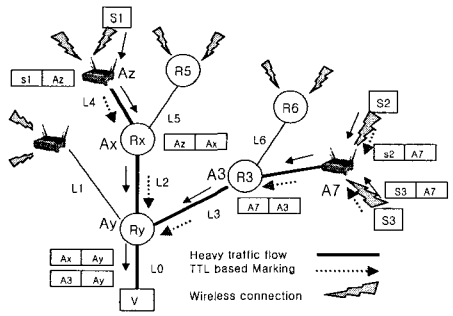

그림 12.제안한 기법에서의 공격 경로 역추적

5. 유무선 트래픽 분류

본 연구에서 제시한 기법은 마킹된 패킷을 중심으로 유선 트래픽과 무선 트래픽을 분류할 수 있다.

[단계 1] 마킹된 패킷 M_i을 수집

피해 시스템 또는 라우터 R_y에서는 전송되는 패킷에 대해 마킹 필드를 살펴보고 일반적인 패킷과 AP에 의해 마킹된 패킷을 수집할 수 있다.

[단계 2] 패킷에 대해 유무선 분류

수집된 패킷 중에서 마킹 필드가 설정된 패킷은 AP에 의해 이상 트래픽이 탐지된 후에 역추적을 위해 마킹된 것이기 때문에 결국 IEEE 802.1x 기반 무선 인터페이스를 통해 전송된 패킷이라는 것을 알 수 있다.

따라서 위와 같이 간단한 방법으로 유무선 통합망에서 무선 트래픽에 대한 분류 과정을 수행하게 된다.

V. 제시한 기법의 성능 분석

제안한 기법과 기존의 유선 중심 IP 역추적 관련 기술들의 성능을 비교 분석하면 [표 1]과 같다. [표 1]에 제시된 성능 비교 분석 결과는 [10] 논문에 제시된 기존의 비교 결과를 토대로 작성되었으며 일반적으로 역추적 관련 기법의 비교 분석에 사용되는 도표이다. 본 연구에서 제시한 AP 기반의 역추적 기법과 기존의 라우터 중심의 역추적 기법을 비교하는 이유는 무선에서의 AP 역시 기존의 유선상에서의 허브 장치 등과 유사하게 라우팅 기능을 수행하게 되며, 기존의 역추적 기능인 경우 라우터에 역추적 기능을 추가하는 방식이었기 때문이다. 따라서 본 연구 역시 기존의 유선 기반 역추적 방식과 성능을 비교 분석하는 방법을 사용하였다. 기존에 라우터를 중심으로 접근 제어 기능을 제공하는

표 1. IP 역추적 기법 성능 비교 평가

특성 / 기법	구성요소	작동 방식	네트워크 부하	역추적 기능	무결성 제공	DoS 대응	경로 재구성 패킷수	무선패킷 분류	네트워크 처리율
Ingress filtering[15]	라우터	패킷 필터링	×	×	×	×	×	×	△
PPM[12]	라우터	패킷 마킹	↑	◇	◇	▽	n-1	×	▽
iTrace[14]	라우터	ICMP	↑	△	◇	△	×	×	◇
제안한 TTL 기반 기법	AP 및 라우터	TTL 마킹	↓	△	△	△	n-1	○	▽

○: A ×:N/A ↑:high, ↓:low △:good ◇:moderate ▽:bad

Ingress Filtering 기법[15]은 라우터에 유입되는 패킷에 대한 판별 기능만을 수행한다. 따라서 추가적인 네트워크 부하가 없다는 장점은 있지만 역추적 기능을 제공하지 못한다. 이는 라우터 자체에서 패킷에 대한 검사를 수행하는 기법이다.

라우터에서 패킷 정보에 대한 로그 정보를 관리하는 Logging 기법은 라우터에 대해 많은 메모리를 필요로 하며 일부 역추적 기능을 제공하지만 전반적으로는 낮은 보안 구조와 DoS 공격 대응에 취약점을 보인다.

기존의 노드 및 에지 샘플링 등에 의한 패킷 마킹 기법과 iTrace 기법[14]은 관리 시스템 및 네트워크 부하는 적은 반면 피해 시스템에서 역추적 경로 재구성시 많은 부하를 필요로 하며, 역추적 기능 및 확장성 측면에서 적절하다고 할 수 있다. 전체적으로 현재까지 제시된 IP 역추적 기법을 검토하였을 경우 대부분 기존 라우터에 대한 변형 및 추가적인 네트워크/시스템 부하가 발생한다는 것을 알 수 있다.

본 연구에서 제시한 기법은 AP에서 패킷에 대한 판별 및 제어 기능을 적용하였기 때문에 DoS와 같은 해킹 공격이 발생하였을 경우 전체 네트워크의 부하를 줄일 수 있다는 장점을 제공한다. 또한 기존의 PPM 기법[12]에서는 임의의 확률 p로 패킷을 선정하여 마킹 과정을 수행하였으나 본 연구에서 제시한 기법은 TTL 필드 값을 이용하여 경로 정보를 마킹하기 때문에 피해 시스템에 도달하는 역추적 경로 재구성에 필요한 패킷의 수를 줄일 수 있었다.

또한 경로 정보에 대해 해쉬 함수를 적용하였기 때문에 중간 라우터에 의해 수정 등이 불가하기 때문에 경로 정보에 대해 간략한 형태의 인증 및 무결성 기능을 제공한다.

또한 본 연구에서 제시한 기법은 무선 트래픽에 대한 패킷 마킹 기능을 제공하며 무선 트래픽에 대한 판별 기능까지도 제공할 수 있다. 무선 네트워크 환경에서의 공격 경로 재구성을 위해서는 네트워크에서 n개의 라우터를 거치는 경우 단지 n-1개의 역추적 메시지만으로 근원지 경로를 재구성할 수 있다는 장점을 제공한다.

하지만 본 연구에서 제시한 기법인 경우 AP를 통해 무선 트래픽에 대한 공격 여부를 판별하고 만일 공격이라고 판단될 경우 패킷에 마킹을 수행하는 과정이므로, 전체적으로 무선 트래픽 환경에서의 처리율의 저하를 유발하게 된다.

또한 AP 본연의 역할인 패킷 전송 과정에서 부가적으로 패킷에 대한 모니터링 및 패킷 마킹 과정을 수행하기 때문에 전체적인 네트워크 속도의 저하를 유발할 수 있다.

하지만, 본 연구를 통해 제시된 AP를 통해 무선 네트워크에서 급속도록 증가하고 있는 무선 트래픽 공격에 대해 우선적으로 유선과 무선에 대해 분류할 수 있는 기능을 제공하며 이를 기반으로 좀 더 안전한 무선랜 환경을 구축할 수 있다.

VI. 결 론

본 연구에서는 최근 급속도로 확산되고 있는 IEEE 802.1x 기반 무선랜 환경에서 DoS 공격 등이 발생하였을 경우 스푸핑된 트래픽에 대한 실제적인 공격 근원지 IP를 피해 시스템에서 역추적하는 기술을 제시하였다. 제시한 기법은 기존의 기법보다 부하, 성능, 안전성 및 역추적 기능에서 개선된 특징을 보인다.

특히 제한한 기법은 AP를 기반으로한 패킷 마킹 기법으로 유무선 통합망에서의 무선 트래픽에 대한 분류 및 판별 기능을 제공하며 앞으로 USN 및 유비쿼터스 기반 무선 네트워크 환경에서 빈번하게 발생할 것으로 예상되는 무선 네트워크 공격에 능동적으로 대응할 수 있는 방안을 제시하였다.

근래 모바일 네트워크 및 Ad-hoc 기반 네트워크 환경에서의 DDoS 공격에 대한 취약점이 발견되고 있다. 따라서 무선 환경에서 패킷에 대한 필터링 기능을 제공하고 공격 근원지에 대한 역추적 기능을 제공할 수 있는 방안을 제시하였다. 제시된 기술은 W-IDS 기반 AP 모듈과 접목한다면 좀더 안전한 무선망 환경을 구축할 수 있을 것으로 예상된다.

참 고 문 헌

[1] Computer Emergency Response Team, "TCP SYN flooding and IP Spoofing attackts," CERT Advisory CA-1996-21, Sept. 1996.

[2] L. Garber, "Denial-of-service attacks trip the Internet," Computer, p.12, Apr. 2000.

[3] B. Potter, *802.11 Security*, OReilly, Dec. 2002.

[4] W. Wei, B. Wang, C. Zhang, and J. Kurose, Don Towsley, "Classification of Access Network Types: Ethernet, Wireless LAN, ADSL, Cable Modem or Dialup?," IEEE, 2006.

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

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

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

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

[9] T. Baba and S. Matsuda, "Tracing Network Attacks to Their Sources," IEEE Internet Computing, pp.20-26, March 2002.

[10] A. Belenky and N. Ansari, "On IP Traceback," IEEE Communication Magazine, pp.142-153, July 2003.

[11] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Practical Network Support for IP Traceback," Technical Report UW-CSE-2000-02-01, Departmentof Computer Science and Engineering, University of Washington, 2000.

[12] D. X. Song and A. Perrig, "Advanced and Authenticated Marking Scheme for IP Traceback," Proc, Infocom, Vol.2, pp.878-886, 2001.

[13] A. C. Snoeren, C. Partridge, L. A. Sanchez, W. T. Strayer, C. E. Jones, F. Tchakountio, and S. T. Kent, "Hash-Based IP Traceback," BBN Technical Memorandum No.1284, Feb. 2001.

[14] S. Bellovin and T. Taylor, "ICMP Traceback Messages," RFC 2026, Internet Engineering Task Force, Feb. 2003.

[15] P. Ferguson and D. Senie. "Network ingress Filtering: Defeating denial of service attacks which employ IP source address spoofing," RFC 2827, May 2000.

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