IAD 기반 패킷 마킹과 유무선 트래픽 분류를 통한 무선 DDoS 공격 탐지 및 차단 기법

Wireless DDoS Attack Detection and Prevention Mechanism using Packet Marking and Traffic Classification on Integrated Access Device

조제경*, 이형우*, 박영준**

한신대학교 컴퓨터공학부*, 청강문화산업대학 물류유통정보과**

Je-Gyeong Jo(aiking@hs.ac.kr)*, Hyung-Woo Lee(hwlee@hs.ac.kr)*,
Yeoung-Joon Park(joonpark@chungkang.ac.kr)**

요약

무선 네트워크 환경에서 DDoS 공격이 수행될 경우 기존 유선 네트워크 환경보다 공격 패턴에 대한 탐지 및 공격지 역추적이 어렵다는 문제점을 보인다. 특히 무선 네트워크 환경에서는 사용자 인증 공격 및 패킷 스니핑 공격에 취약점을 보이고 있어 이에 대한 대응 기술이 연구되어야 한다. 최근 유무선 라우팅 기능과 함께 VoIP 통신 기능 등을 통합하여 지원하는 Integrated Access Device(IAD)가 개발되어 널리 배포되며 기존의 AP 기능을 대체하고 있다. 따라서 IAD 기반 무선 네트워크 환경에서도 유무선 트래픽에 대한 분류와 실시간 공격 탐지 기능이 제공되어야 한다. 본 연구에서는 AirSensor를 이용하여 IAD에 접속한 무선 네트워크 클라이언트 정보를 수집하며 무선 클라이언트의 공격 패킷에 대해 사전 차단 기능을 수행하도록 하였다. 또한 IAD에 수신된 패킷에 대해 W-TMS 시스템과 연동하여 DDoS 공격 트래픽을 판단하도록 하였고 이를 직접 차단하여 안정적으로 IAD 기반 무선 네트워크 서비스를 이용할 수 있도록 하였다.

■ 중심어 : | DDoS | IAD | 유무선 분류 | 패킷마킹 | W-TMS | AirSensor |

Abstract

When DDoS attack is achieved, malicious host discovering is more difficult on wireless network than existing wired network environment. Specially, because wireless network is weak on wireless user authentication attack and packet spoofing attack, advanced technology should be studied in reply. Integrated Access Device (IAD) that support VoIP communication facility etc. with wireless routing function recently is developed and is distributed widely. IAD is alternating facility that is offered in existent AP. Therefore, advanced traffic classification function and real time attack detection function should be offered in IAD on wireless network environment. System that is presented in this research collects client information of wireless network that connect to IAD using AirSensor. And proposed mechanism also offers function that collects the wireless client's attack packet to monitoring its legality. Also the proposed mechanism classifies and detect the attack packet with W-TMS system that was received to IAD. As a result, it was possible for us to use IAD on wireless network service stably.

■ keyword : | DDoS | IAD | Wired-Wireless Classification | Packet Mark | W-TMS | AirSensor |

* 본 연구는 지식경제부 및 정보통신연구진흥원의 대학IT연구센터 지원사업의 연구결과로 수행되었습니다.
(IITA-2008-C1090-0801-0016)

접수번호 : #080304-002
접수일자 : 2008년 03월 04일
심사완료일 : 2008년 06월 05일
교신저자 : 이형우, e-mail : hwlee@hs.ac.kr

I. 서 론

IEEE 802.11 기반 무선 네트워크 클라이언트는 무선 프레임을 통해 네트워크에 접속하기 때문에 편리한 이동성을 제공한다. 하지만 무선 네트워크 환경에서는 기존의 유선 네트워크에서의 공격 방식을 그대로 사용할 수 있으면서 무선 네트워크 클라이언트의 이동성 때문에 공격의 탐지 및 대응이 불가능하다. 따라서 무선 네트워크의 특성을 이용한 공격이 증가하고 있으며 이러한 무선 네트워크 보안취약성 해결을 위한 연구가 필요하다.

악의적인 무선 네트워크 공격자는 개방된 Access Point를 이용하여 자신의 위치를 공격 대상이나 방화벽에 노출 시키지 않고도 Victim 호스트에 대한 공격을 수행 할 수 있다. 또한 Access Point를 통해 Auth/Deauth Flooding 공격과 같은 DoS/DDoS 공격을 시도하여 일반적인 사용자의 접속을 차단할 수 있다. 특히 악의적 공격자는 Soft AP라 불리는 무선 네트워크 라우팅 모듈을 이용하여 Fake AP[1]를 구축한 다음 일반 사용자가 전송하는 무선 클라이언트의 패킷을 스니핑 하거나 MITM(Man In The Middle) 공격[2]을 수행 할 수 있기 때문에 이에 대한 대응 방안이 제시되어야 한다.

무선 네트워크 DDoS 공격에 대처하기 위하여 기존에 제시된 연구들 중에는 (1) Snort-Wireless[3]와 같이 무선 네트워크의 패킷을 캡처한 다음 패킷의 신호를 분석하여 공격의 가능성을 알려주는 Wireless IDS 시스템 구축 기법, (2) 무선 네트워크 공격 중 시퀀스 값의 일정한 증가 등 특정 패턴을 비교 평가 후 악의적 공격자의 불법적인 MAC Address Spoofing을 탐지하는 기법[4], (3) 기존의 웜(Worm) 공격 모델을 이용하여 유무선 네트워크 환경에서의 DDoS 트래픽을 분석하고 차단하는 기법[5] 등 다양한 연구가 수행 되었다.

하지만 기존의 연구들은 유선 네트워크와 무선 네트워크의 차이점이 고려되지 않은 상태로 수행된다는 문제점이 존재한다. 무선 네트워크는 IEEE 802.11에서 선언한 관리 프레임[6]을 이용하여 통신을 하게 되는데 이때 발생 가능한 공격 패턴에 대해서는 고려하지 못하고 있다. 단순히 공격 시그니처(Signature) 중심의 공격 탐지로 인하여 공격자가 관리 프레임 등을 이용해 Auth/Deauth Flooding과 같은 공격을 수행할 경우 이를 능동적으로 탐지하지 못하고 있다. 따라서 이와 같은 취약점을 해결하기 위해서는 라우터를 통해 전송되는 대량의 유무선 패킷에 대한 명확한 분류가 선행되어야 한다.

기존의 유무선 패킷을 분류하기 위한 연구[7]에서는 Victim에 접속한 클라이언트에 대하여 ICMP 신호를 일정 간격을 두고 송출한 다음 ACK 신호의 시간 차이를 확인하여 사용자 클라이언트의 유무선 네트워크 접속 및 이용 환경을 판단하고 있다. 하지만 기존 연구에서 제시한 기법을 사용할 경우 ICMP 패킷에 대해 응답하지 않거나 방화벽이 설정되어 있다면 정확한 분류가 어렵다는 단점이 있으며, 특히 무선 네트워크 환경에서는 장비 및 물리적 환경요소와 트래픽 정도에 따라 응답 속도가 달라진다는 문제점도 발견되었다.

따라서 본 연구에서는 유무선 네트워크 환경에서 패킷 분류 및 DDoS 공격 탐지 성능을 높이기 위해 기존의 Access Point보다 다양한 기능(블루투스, 모뎀, VoIP)을 수행하도록 설계된 Integrated Access Device (이하 IAD)에서 일차적으로 마킹 작업을 수행하고 이를 통하여 유무선 트래픽 분류 모듈로 전달하며, 또한 전송되는 무선 패킷에 대한 정보를 AirSensor에서 모니터링 하여 패킷에 대한 시그니처 정보를 W-TMS(Wireless-Threat Management System)[8]로 전송하도록 하였다.

기존의 Access Point를 사용할 경우 공격의 탐지 및 차단 등 다양한 기능을 수행하기에 부족한 부분이 있기에 다양한 기능을 수행하기 위해 성능이 향상된 IAD를 이용하여 실험을 하였다.

W-TMS는 AirSensor와 IAD로부터 전송 받은 패킷 정보를 저장하여 DDoS 공격을 판단하고 차단하기 위한 작업을 수행한다. 특히 IAD에서의 부하로 인한 패킷 전송 시간 지연을 줄이고 성능을 향상시키기 위하여 DDoS 공격에 대한 판단은 AirSensor나 W-TMS에서 수행하도록 하였다.

본 연구의 2장에서는 무선 네트워크 환경에서의 공격

기법이나 분류 기법을 분석하여 관련 연구의 문제점을 제시하며, 이를 해결하기 위해 본 연구에서 설계한 모델을 3장에서 제시하였다. 또한 구현 및 성능 평가 결과를 4장에서 제시한다. 5장에서는 본 연구를 통하여 나온 결과를 분석하였으며 결론을 제시한다.

II. 기존의 무선 DDoS 공격 대응 연구

2.1 무선 DDoS 공격 기법의 현황 및 문제점

현재 무선 네트워크 환경에 대한 공격 기법 중 가장 많이 이용되는 툴인 AirJack[9]은 IEEE 802.11b 프로토콜을 이용하여 다음과 같은 단계로 작동한다.

- 1단계 : 주변 네트워크의 MAC 주소 및 IP 주소, AP에 대한 정보를 Channel Hopping[10] 방식으로 수집한다.
- 2단계 : 수집한 MAC 주소 및 IP 주소 리스트를 이용하여 공격 패킷을 생성한다.
- 3단계 : 생성된 패킷의 타입을 Auth/Deauth와 같은 관리 프레임으로 바꾼다.
- 4단계 : 생성된 패킷의 SSID와 ESSID를 입력하여 Auth/Deauth 패킷을 완성 시킨다.
- 5단계 : 생성된 공격 패킷을 무선 NIC를 통하여 전송한다.

DDoS의 경우 악의적인 공격자가 무선 NIC를 가지고 있는 클라이언트에 대하여 Deauth 공격을 시도한 다음 Auth 공격을 통하여 자신이 만든 Fake AP를 통하여 통신을 시도하도록 한다. 이렇게 Fake AP에 연결된 클라이언트에 대하여 악의적인 공격자는 패킷 변조 및 취약점 공격 등을 통하여 자신이 만든 웜을 대량으로 전송할 수 있으며 이는 다수의 DDoS 공격 클라이언트로 확대된다.

무선 클라이언트를 통한 DDoS 공격은 클라이언트의 이동성으로 인하여 역추적이 어려우며 역추적을 하더라도 AP의 가상 IP 분배로 인하여 AP의 위치까지만 확인이 가능하며 클라이언트의 식별이 어렵다. 따라서 무선 네트워크 환경에서의 공격을 판단하고 사전에 차단하며 새로운 공격 발견시 빠르게 찾아내 대응 할 수 있는 기술이 필요하다.

2.2 웜 관련 트래픽 및 통계에 따른 분석

DoS/DDoS 공격에서 가장 많이 사용되는 방법 중 하나는 웜을 이용하여 감염 클라이언트를 확대하는 것이다. 따라서 무선 네트워크 환경에서도 웜을 탐지하는 기법을 적용하여 DDoS 공격 대응 기술에 적용할 수 있다. 특히 웜 트래픽을 대상으로 통계 분석을 이용한 탐지 기법[5]은 관리/제어 프레임 등의 비중이 많은 IEEE 802.11 무선 네트워크 환경에 적용할 수 있다. 구체적으로 본 연구에서는 기존의 TRW[11] 기반 비정상 트래픽 패턴 분류 기법과 통계 기반 공격 탐지 기법[12]에 대해 살펴보면 다음과 같다.

2.2.1 TRW 기법

MIT에서 이루어지고 있는 연구로써 수학적 알고리즘인 TRW(Threshold Random Walk)[11] 방법을 이용해서 트래픽 패턴을 분석해 웜을 찾아내는 방법이다. 이 방식은 TCP 프로토콜을 사용한 웜을 대상으로 한 것으로, TCP 프로토콜의 처음 연결을 위한 SYN 패킷을 스캐닝 동작으로 보고 이 정보를 바탕으로 Sequential Hypothesis Testing 방식을 이용해서 아래 수식 (1)과 같이 비정상 트래픽 패턴을 찾아낸다.

$$\Phi(Y_i) = \frac{\Pr[Y_i|H_{scanning}]}{\Pr[Y_i|H_{begining}]} \qquad (1)$$

$$\Lambda(Y_i) = \prod_{i=1}^{n} \frac{\Pr[Y_i|H_{scanning}]}{\Pr[Y_i|H_{begining}]} = \prod_{i=1}^{n} \Phi(Y_i)$$

Y_i라는 값을 어떤 특정 호스트의 TCP 연결의 성공과 실패를 나타내는 연속적인 값이라고 할 때 어떤 호스트에 대하여 스캐닝이 발생한 경우와 아닌 경우에 따라 Y_i의 값을 다르게 하여 연산을 수행한다. TCP 연결에 대한 SYN 패킷을 보낼 때마다 Y_i의 값에 대한 A (Y_i) 값은 변하게 되고 TCP 연결을 실패하는 경우 이 값은 계속 증가 하게 된다. 이때 증가하는 값이 Threshold 값보다 크게 되면 웜 공격으로 간주한다.

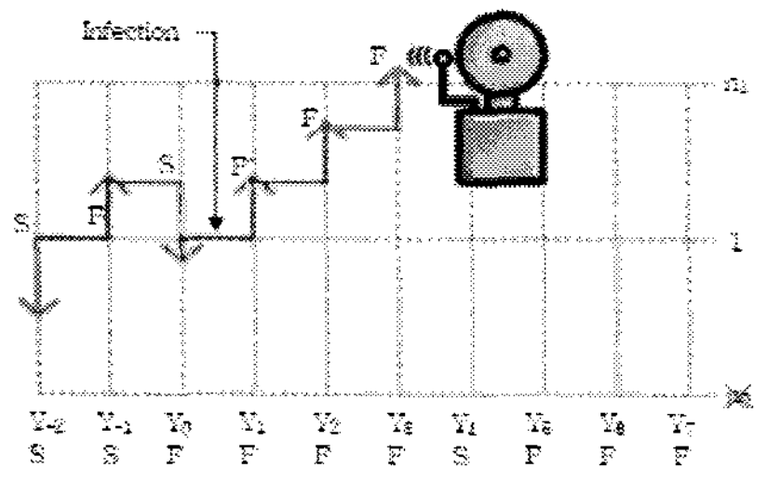


그림 1. TRW 기법을 이용한 웜 탐지 기법

그러나 TRW 방식은 UDP 웜에 대한 탐지가 불가능한 단점이 존재하며 무선 네트워크에 적용시키기에는 Access Point에서의 연산이 증가하므로 패킷 손실의 증가 및 패킷 전송 지연이 발생한다는 단점이 있다.

2.2.2 Statistical Intrusion Detection 방식

Statistical Intrusion Detection[12] 방식은 통계학적인 방식을 이용하여 웜을 탐지하는 방식이다. 실제 네트워크 트래픽을 가지고 네트워크 모델을 만든 다음 웜 공격을 수행하여 실제 웜에 대한 자료를 수집한다. 기존 연구는 Epidemic Model을 이용한 것으로 CodeRed와 Slammer 웜에 대한 자료를 수집해서 실제 웜 공격 모델을 구축하였다. 아래 수식 (2)에서 I(t)는 시간 t에서 감염된 호스트의 수이고, N은 모집단의 크기, β는 감염률을 나타낸다.

$$[Simple\ Epidemic\ Model] \quad (2)$$
$$dI(t)/dt = \beta I(t)S(t) = \beta I(t)[N - I(t)]$$

하지만 기존 연구에서는 호스트 하나에서 하나의 패킷이 전송되는 것을 기반으로 하였기 때문에 하나의 호스트에서 여러 DDoS 공격 패킷을 만드는 것에 대해서는 고려되지 않았다. 무선 네트워크 환경에서는 패킷의 수정이 비교적 자유롭기 때문에 하나의 호스트에서 여러 호스트를 가장한 패킷을 송출할 수 있는 환경을 고려해야 한다.

2.3 엔트로피 기반 유무선 트래픽 분류 기법

무선 사용자에 의한 DDoS 공격 등을 효율적으로 판별하기 위해서는 우선 라우터에 도착한 패킷에 대해 유선 클라이언트로부터 발송된 패킷과 무선 클라이언트로부터 발송된 패킷을 우선적으로 분류/구별할 필요가 있다. 기존의 유무선 트래픽을 분류하는 기법[7]에는 ICMP 패킷을 일정한 간격으로 송출하여 그에 대한 ACK 신호가 돌아오는 응답 시간의 차이/분포를 엔트로피(Entropy)화 하여 클라이언트의 네트워크 접속 환경을 구분하였다. 사전에 ADSL, cable, wired, wireless와 같은 네트워크 환경 모델을 구축하여 해당 클라이언트에게 ICMP 패킷을 송출한다. 각 네트워크 환경에 따른 ACK 값의 간격 차이는 엔트로피화 되어 특정 값을 가지게 되며 이렇게 나타난 값들은 유무선 뿐만 아니라 ADSL, cable 모뎀 기반 네트워크를 구분할 수 있다.

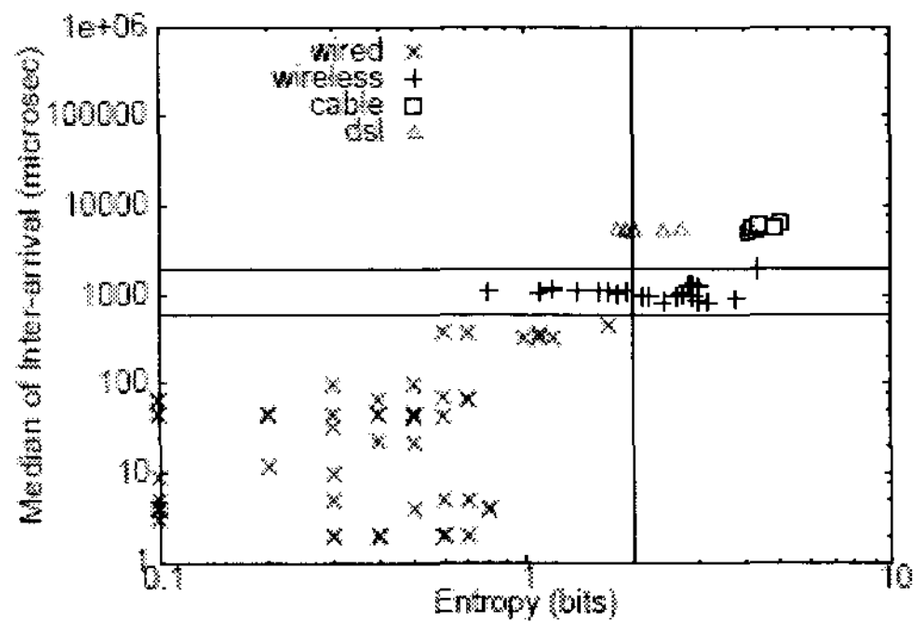


그림 2. ACK 값의 간격을 이용한 패킷 분류 기법

하지만 기존 연구는 네트워크 환경에 따라 ACK 신호의 간격이 달라지기 때문에 오차율이 상당히 높으며 무선 네트워크에서는 거리에 따라 전송 속도에 차이가 난다. 또한 이 기법은 ICMP 패킷에 대해 응답하지 않도록 설정되거나 방화벽이 존재하는 경우 정확한 분류가 어렵다는 단점이 있다.

2.4 해결 방안

앞에서 제시한 기존 연구는 악의적인 공격에 대하여 탐지 위주의 기능을 수행하고 있으며 공격에 대한 차단 기능은 제공하고 있지 않다. 본 연구에서는 유무선 네트워크의 분류를 위하여 특정 필드에 대한 마킹을 수행하여 패킷을 수신하는 Victim이나 중간의 방화벽 모두

유무선 패킷을 분류할 수 있도록 하였다. 또한 DDoS 공격에 대해 IAD에서 차단할 수 있도록 하였으며 무선 네트워크 환경에서의 DDoS 공격을 빠르고 정확하게 판단하기 위하여 AirSensor와 IAD에서 패킷의 정보를 W-TMS로 전송 한 후 DDoS 공격을 판단하도록 하였다. 제안한 시스템 모델은 다음과 같다.

III. 제안한 시스템 모델 및 기법

3.1 전체 시스템 구조

본 연구에서 제안하는 시스템 구조는 AirSensor와 IAD, W-TMS로 구성된다. AirSensor는 채널 호핑과 패킷 분석을 수행하며, IAD는 임베디드 리눅스와 커널의 Message QUEUE[13], IPTABLES를 이용하여 패킷 마킹을 통한 유무선 트래픽 분류 및 무선 프레임에 대한 정보 전송 기능을 수행한다. W-TMS에서는 패킷의 정보를 IAD와 AirSensor로부터 전송 받아 DDoS 공격을 판단하고 DDoS 공격을 시도한 클라이언트에 대하여 차단 기능을 수행한다. 본 연구에서의 전체적 시스템 흐름 순서는 다음과 같다.

- 1단계 : 악의적인 공격자는 무선 네트워크의 IAD/AP중 오픈된 IAD/AP에 접속하여 네트워크를 사용 중인 무선 클라이언트에 DDoS를 위한 웜을 퍼뜨린다.
- 2단계 : 1단계에서 퍼진 웜은 악의적인 공격자의 명령에 의해 Victim에 대하여 공격을 시도한다.
- 3단계 : IAD는 자신을 통해 지나가는 클라이언트의 트래픽으로부터 Source IP 주소, Destination IP 주소, Protocol Type, Checksum등의 정보를 수집하여 W-TMS로 전송한다.
- 4단계 : IAD로부터 전송 받은 정보는 W-TMS의 무선 DDoS 공격 모듈을 통하여 DDoS 공격에 대한 판단을 내린 후 IAD로 차단 신호를 보낸다.
- 5단계 : IAD는 W-TMS로부터 받은 차단신호를 확인하여 해당 패킷이 가고자 하는 주소에 대한 패킷을 차단한다.
- 6단계 : 차단 신호가 아닐 경우 패킷 마킹 모듈을 통하여 특정 필드에 대하여 마킹 작업을 수행 후 정상적인 통신을 시도한다.

위와 같은 흐름을 통하여 차단을 할 경우 다음과 같은 형태의 시스템 구조를 가진다.

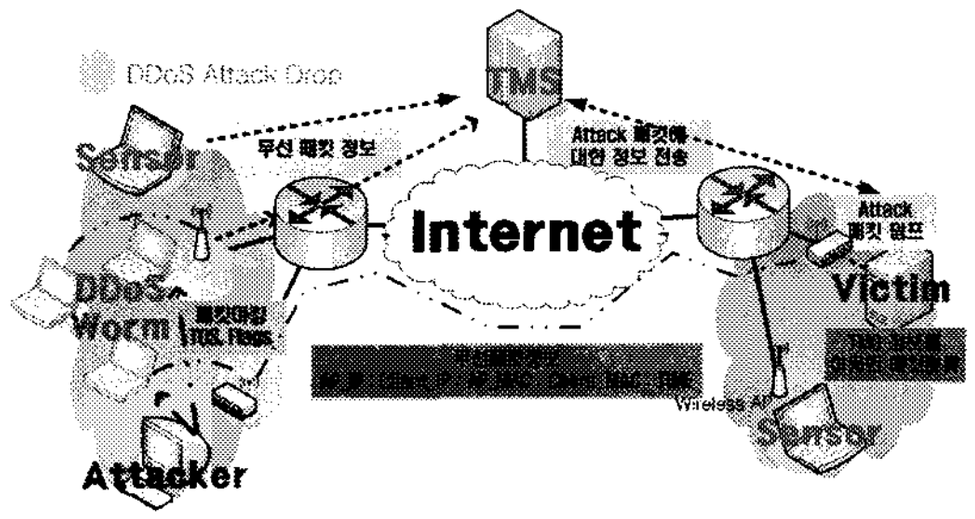


그림 3. 제안한 시스템 모델의 전체 시스템 구조

3.2 무선 패킷의 관리 구조

무선 네트워크 환경에서의 액세스 네트워크 노드인 IAD는 리눅스를 이용하여 무선 패킷의 정보를 추출하여 W-TMS에 전송하며, W-TMS로부터 DDoS에 대한 판단을 수신하여 악의적인 공격을 직접 차단하는 기능을 수행한다. 내부 구조는 [그림 4]와 같이 무선 패킷에 대한 정보를 추출하여 큐로 전송하는 부분과, 패킷 마킹을 통해 W-TMS로 전송하는 부분으로 구성된다.

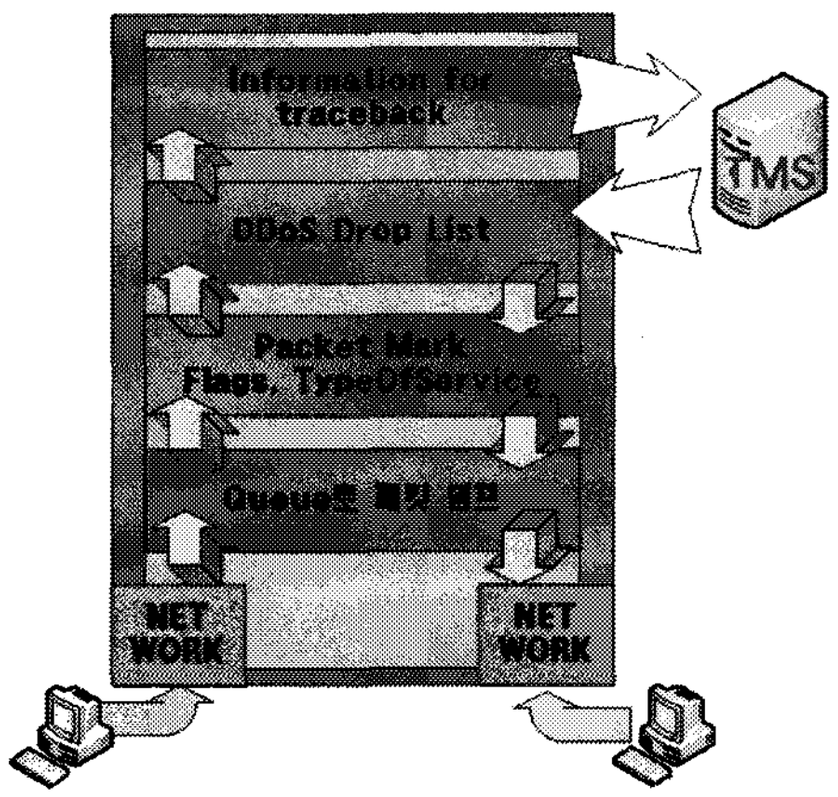


그림 4. IAD 시스템 내부 모듈 구성

3.2.1 무선 패킷 정보 추출 및 전송

IAD는 무선 패킷을 IPTABLES와 커널의 Message

QUEUE를 이용하여 임시적으로 저장 하며, W-TMS에 전송할 무선 패킷의 IP주소와 Protocol type등 다양한 정보를 추출한다. 이렇게 추출한 무선 패킷의 정보는 W-TMS로 전송한다.

- 1단계 : Kernel의 Message QUEUE로부터 패킷을 읽는다.
- 2단계 : 읽어 들인 패킷으로부터 무선 NIC를 통해 들어 왔는지 확인한다.
- 3단계 : 무선 NIC를 통하여 들어온 패킷일 경우 패킷 마킹 모듈로 전송한다.
- 4단계 : 무선 NIC를 통하여 들어온 패킷이 아닐 경우 수정 작업 없이 그대로 전송한다.
- 5단계 : 패킷 마킹 모듈로 전송한 패킷에 대하여 Source IP 주소와 Destination IP주소, MAC 주소, 프로토콜 타입 등 다양한 정보를 추출 W-TMS로 전송한다.

3.2.2 무선 트래픽에 대한 패킷 마킹

IAD의 QUEUE에 저장된 패킷은 전송률의 향상을 위해 패킷을 그대로 전송시키는 것을 중심으로 하되 지금 현재 전송하고자 하는 패킷과 해당 패킷의 IP 주소가 동일한 경우 기존 정보와의 차이를 이용하여 패킷 마킹 작업을 수행한다. 본 연구에서는 Time의 차이가 5초 차이 이상이 날 경우 패킷의 마킹 작업을 수행하며 패킷의 TOS(Type of Service) 필드와 Flags 필드를 사용한다[14].

무선 패킷 마킹을 위해서 사용하는 필드는 현재 일반적인 무선 네트워크 환경에서는 사용하지 않는 필드로써 TOS 필드의 1bit와 Flags 필드의 1bit를 사용한다. 각각의 bit는 기본적으로 0으로 채워져 있으며 본 연구에서는 각 필드의 값을 1로 변경한다.

- 1단계 : 유무선 패킷 분류 모듈로부터 무선 패킷을 받는다.
- 2단계 : 무선 패킷에 대하여 Flag 필드와 TOS 필드를 추출한다.
- 3단계 : TOS 필드에 대하여 1을 추가하며 Flags 필드에 대하여 128을 추가한다.

```
flag bit 0 0 0
default don't defragement 0 1 0
using reserved bit 1 1 0
010 = 0x40
110 = 0xC0
100 = 0x80 = (decimal) 8*16 = 128
```

- 4단계 : Kernel의 Message QUEUE에 있는 해당 패킷은 차단을 시키고 수정된 패킷을 전송한다.

3.2.3 무선 DDoS 공격 차단

무선 네트워크의 DDoS 공격을 차단하기 위해서 Victim의 IP 주소와 포트 정보를 저장한다. 저장되는 IP 주소와 포트 정보는 W-TMS로부터 받은 DDoS공격 판단에 따라 저장이 된다.

IAD의 패킷 정보를 전송하는 모듈에서 패킷의 정보를 W-TMS로 전송하면 W-TMS에서는 일정 규칙에 따라 DDoS공격 판단 후 차단할 패킷의 정보를 IAD로 전송한다. 이렇게 W-TMS로부터 전송된 패킷의 정보는 IAD의 차단리스트에 등록이 되며 커널의 QUEUE에 저장된 패킷은 차단리스트에 따라 차단된다.

표 1. DDoS 공격 패킷 차단을 위한 리스트

Block IP	Block Port	Send Interval
192.168.0.101	80/8080	0.2sec
203.252.19.4	22	0.01sec
203.252.23.8	20/21	0.4sec

3.3. 무선 관리 프레임 DoS 공격 탐지를 위한 AirSensor

3.3.1 무선 패킷 탐지 및 분류

무선 네트워크 환경에서는 IEEE802.11에서 선언한 표준을 따른다. 주파수의 채널 및 전송하는 전파의 내용 등을 선언하였으며 국내에서는 13개의 채널만을 이용하고 있다[15]. 본 연구에서는 13개의 채널에 대하여 채널을 번갈아가며 각 채널의 데이터를 스니핑 하는 채널호핑 기법을 이용하였으며 채널호핑을 통하여 얻은 패킷 데이터를 무선 네트워크 공격 판단 모듈로 전송한다.

- 1단계 : 무선 네트워크 인터페이스 카드의 속성을

가진 변수를 읽는다.

- 2단계 : Channel에 대한 속성과 Listen 모드에 대한 속성을 찾는다.
- 3단계 : Listen에 대한 속성을 true로 수정, 패킷을 보내는 것이 아니라 읽어 들이는 방식으로 수정한다.
- 4단계 : Channel의 값을 13이 될 때까지 1씩 증가하면서 Listen 모드를 유지한다.
- 5단계 : Listen 모드에 대한 반환 값인 패킷에 대하여 공격 판단 모듈로 전송한다.

3.3.2 무선 관리 프레임 DoS 공격 탐지

무선 네트워크 환경에서는 연결 및 데이터 통신 과정에서 충돌이 없도록 하기 위하여 패킷 타입을 선언하였다. 이렇게 선언된 패킷 타입을 통하여 Access Point와의 연결 및 통신을 수행하는데 악의적인 공격자는 선언된 패킷 타입을 이용하여 무선 네트워크 환경을 공격해 들어 올 수 있다.

무선 네트워크 환경에서의 Deauth 공격은 유선 네트워크에서의 RST 신호 생성에 따른 공격과 유사하다. 악의적인 공격자가 Deauth 신호를 계속적으로 Access Point에 보냄으로써 무선 클라이언트와 Access Point의 연결을 단절 시킨다.

본 연구에서는 무선 패킷 감지 모듈에서 감지한 패킷을 관리 프레임인지 아닌지 판별한 후 관리 프레임일 경우 감지된 패킷에 대하여 통계 연산을 수행한다. 탐지된 관리 프레임은 사용자가 설정한 임계치에 따라 관리프레임 DoS공격으로 판단한다.

전 패킷량 + 설정한 오차 범위 < 지금의 패킷량

3.3.3 무선 프레임 정보 전송

AirSensor는 무선 네트워크 패킷을 감지하여 패킷에 대한 정보를 추출한다. 추출한 정보를 통해 데이터 프레임과 관리 프레임으로 분류를 하는데 이때 데이터 프레임에 대하여 IP주소와 프로토콜 타입, AP의 ESSSID 등 다양한 정보를 W-TMS로 전송한다.

본 연구에서는 기존에 W-TMS와 AirSensor의 연계 연구로써 무선 패킷의 정보뿐만 아니라 무선 네트워크 공격에 대한 판단 정보까지 W-TMS로 전송한다. W-TMS로 전송된 정보는 W-TMS가 무선 네트워크 공격을 판단하는데 기초 자료로 사용된다.

3.4 무선 DDoS 공격 탐지 및 차단을 위한 W-TMS

3.4.1 무선 패킷 정보 수신

W-TMS는 AirSensor와 IAD에서로부터 받은 무선 패킷의 정보를 저장한다. 저장된 무선 패킷의 정보는 AirSensor로부터 받은 정보와 IAD로부터 받은 정보로 분류되며 분류된 두 분류는 또다시 공격을 탐지한 결과인 IDS 정보와 무선 네트워크 패킷에 대한 정보로 나누어 진다. 이렇게 수신된 정보는 네트워크 관리자에게 보여주는 용도 이외에도 무선 네트워크 공격 판단의 자료로도 사용된다.

3.4.2 무선 패킷 정보 검색

본 연구에서는 유무선 네트워크 패킷의 분류를 중심으로 추후 나타날 수 있는 공격 중 무선 네트워크 환경에서 자주 나타날 수 있는 공격이거나 무선 네트워크 사용자의 통계 등을 위하여 무선 패킷을 찾는 기능을 제공한다.

본 연구에서 제시한 모델의 중심인 본 모듈은 IAD에서 무선 네트워크 패킷에 마킹 작업을 수행 후 마킹된 패킷에 대한 정보를 W-TMS로 전송한다. W-TMS는 전송 받은 패킷을 네트워크 관리자에게 보여주며 IP주소 등 다양한 검색 기능을 제공한다.

추후 공격이 일어났을 경우 Victim의 요청에 의해 무선 네트워크를 통한 공격인지 확인할 수 있으며 또한 해당 IP 주소가 가상 IP 주소일 경우 실제 IP 주소와 MAC 주소의 확인으로 역추적 정보로 사용할 수 있다.

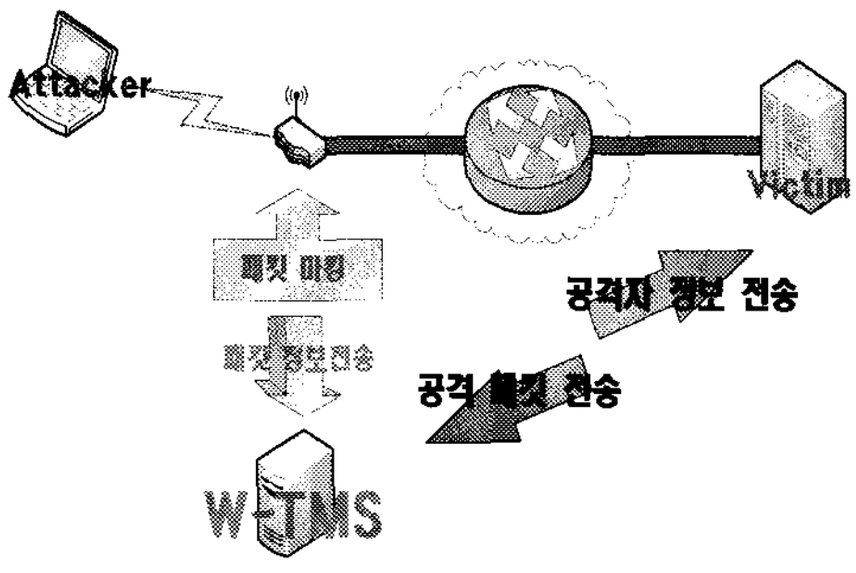


그림 5. Victim의 공격자 패킷에 대한 정보 검색

3.4.3 W-TMS의 DDoS 공격 탐지 및 차단

본 연구 제시한 DDoS 공격 탐지 모듈은 IAD와 AirSensor로부터 받은 무선 네트워크 패킷의 정보를 기초로 DDoS공격에 대한 판단을 수행한다. IAD와 AirSensor로부터 받은 패킷의 정보는 Source IP 주소와 Destination IP 주소, 프로토콜 타입 등 다양한 정보를 수신하며 수신된 정보를 계산하여 임계치 이상의 패킷이 전송될 경우 DDoS 공격으로 판단한다.

- 1단계 : AirSensor와 IAD로부터 받은 패킷 정보를 저장한다.
- 2단계 : 저장한 패킷의 정보를 새로운 정보가 들어올 때마다 갱신한다.
- 3단계 : 갱신할 때 Destination IP 주소에 대하여 같은 경우 DDoS 탐지를 위한 비교 작업을 수행한다.
- 4단계 : IP 주소 및 프로토콜 타입, Checksum 과 같은 웜에 의해 생성되는 트래픽의 공통점과 같을 경우 DDoS공격으로 의심, 패킷의 전송 횟수에 대한 변수에 값을 더해준다.
- 5단계 : 4단계의 절차를 계속 걸쳐 패킷의 전송 횟수가 관리자가 설정한 임계치를 넘어갈 경우 DDoS 공격으로 판단 IAD로 차단 메시지를 전송한다.

본 연구에서는 인터넷 웜 공격 탐지 기법[5]중 하나인 Statistical Intrusion Detection 방식[12]을 응용하였다. 실제로 DDoS 공격을 시도하여 공격이 이루어질 때의 패킷의 통계를 구한다음 본 연구와의 일치성을 확인 및 파라미터들을 조정하여 실제 값과 유사하게 만들었다. 이렇게 나온 값과의 유사 값을 보일 경우 DDoS 공격으로 판단 IAD의 DDoS 공격 차단 모듈로 판단 결과를 전송한다.

IV. 구현 결과 및 성능 평가

4.1 구현 결과

4.1.1 IAD 구현 결과

본 연구의 실험에 사용된 IAD는 802.11a/b/g/n을 지원하며 32M의 램을 가지고 있는 장비를 이용하였다. 가상의 네트워크 브리지 인터페이스를 생성하여 무선 NIC와 유선 NIC를 브리지 인터페이스에 추가하였다. 이렇게 생성된 브리지를 통과하는 패킷에 대하여 유무선 트래픽 분류를 위한 패킷 마킹 작업을 수행한다.

패킷 마킹이 수행된 경우 해당 패킷에 대한 정보를 W-TMS로 전송이 된다. IAD는 W-TMS로 패킷의 정보 전송뿐만 아니라 공격 차단 정보를 수신한다. IAD는 수신된 공격 차단 정보를 기반으로 해당 클라이언트에 대하여 차단 기능을 수행한다.

4.1.2 AirSensor

본 연구에서 제시한 AirSensor는 Atheros 칩셋을 사용하여 윈도우즈 환경에서 무선 네트워크 패킷 캡처 기능을 지원한다. 우선 본 연구에서 제시한 AirSensor 시스템에서는 무선 클라이언트와 연결된 네트워크 중 채널 선택 기능 및 W-TMS와의 연동기능을 제공하기 위해 [그림 6]과 같은 환경 설정 기능을 제공한다.

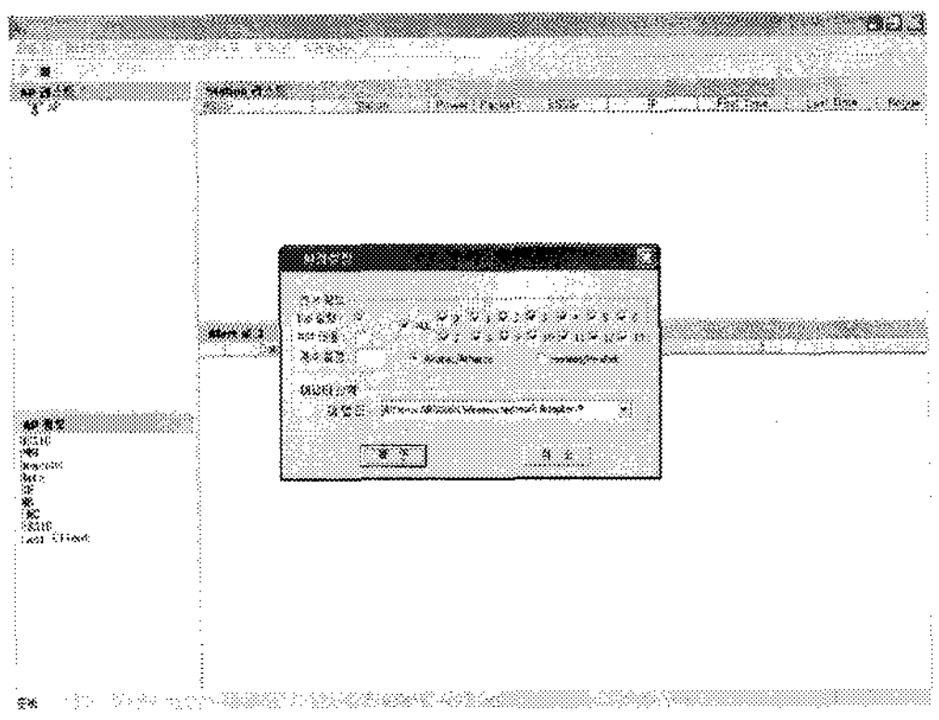


그림 6. AirSensor의 환경설정

AirSensor는 사용자가 설정한 환경에 따라 무선 데이터를 모니터링 한다. 캡처한 데이터는 AirSensor내 Snort-Wireless의 공격 탐지 룰을 이용하여 아래 [그림 7][그림 8]과 같이 시그니처 기반 공격 탐지 및 관리 프레임에 대한 DDoS 공격 탐지를 수행한다. 탐지된 공격에 대해서는 RST 신호를 생성하여 공격자의 연결을 차단한다.

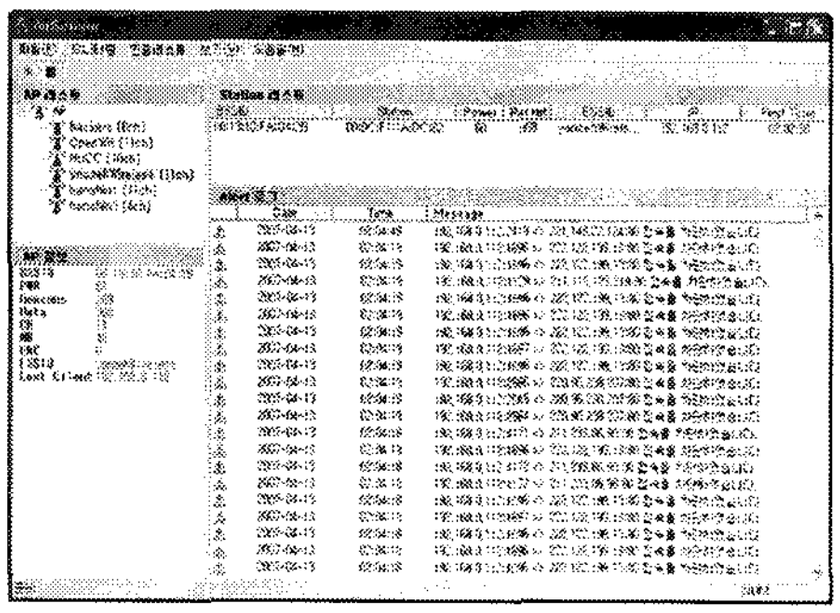


그림 7. AirSensor에서의 시그니처 기반 공격 탐지/차단

공격 프레임이 탐지될 경우 [그림 7]과 같은 경고를 보여주며 사용자로 하여금 공격에 대처할 수 있도록 AP의 ESSID와 BSSID, 그리고 클라이언트의 MAC주소와 IP주소 등 관리 프레임 내 정보를 추출하여 보여준다.

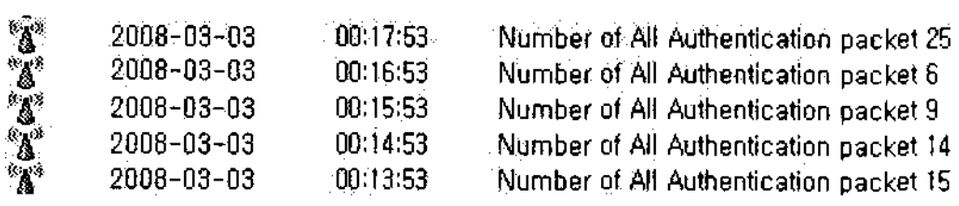


그림 8. AirSensor에서의 관리프레임 공격 탐지

AirSensor에서 DDoS 공격 탐지를 위한 임계치 설정을 위해 기존의 무선 인증 취약점 공격 툴인 MDK3를 이용하였다. 무선 인증 DDoS 공격 탐지 방식은 Statistical Intrusion Detection[12] 방식을 사용하였으며 성능 평가의 정확도를 높이기 위해 아래 [그림 9]와 같이 총 7번의 실험을 수행하였다.

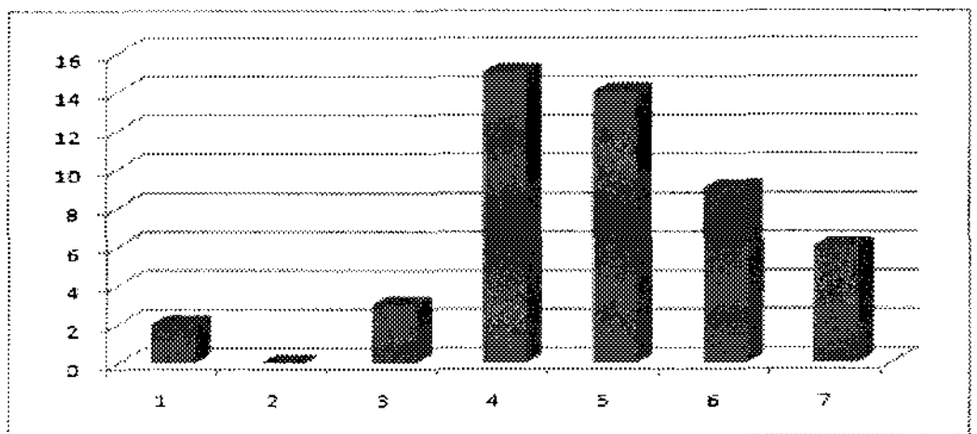


그림 9. 무선 인증프레임을 이용한 DDoS 공격 실험

실험 결과 처음 1,2,3회의 시도에서는 정상적인 무선 네트워크 클라이언트에 의해 발생한 인증 프레임의 수를 나타내며, 4번째 시도인 경우는 MDK3 무선 네트워크 공격 툴을 작동 시켰을 경우에 발생한 인증프레임 수이다. 1,2,3회인 경우 초당 10회 미만의 관리 프레임이 탐지되었으나 4회인 경우에는 초당 25회, 5회인 경우에는 초당 14회의 관리프레임이 탐지되었다. 4회인 경우에서 공격을 중지 했음에도 불구하고 전파의 특성상 사라지지 않고 계속 남아 네트워크상의 비인증 공격 시도를 하고 있다. 따라서 실험결과 임계치를 초당 25회로 설정하여 공격을 탐지하도록 하였다.

4.1.3 무선 DDoS 공격 위협 관리 시스템

본 연구에서 제시한 W-TMS는 AirSensor와 IAD로부터 패킷의 정보를 수신한다. 888번 포트를 통하여 AirSensor 및 IAD로부터 패킷의 정보를 받으며 999번 포트를 통하여 패킷의 차단신호를 전송한다. W-TMS에서는 관리자에게 패킷 정보, 클라이언트 정보, AP의 정보와 무선 DDoS 공격에 대한 탐지 및 차단 기능을 제공한다.

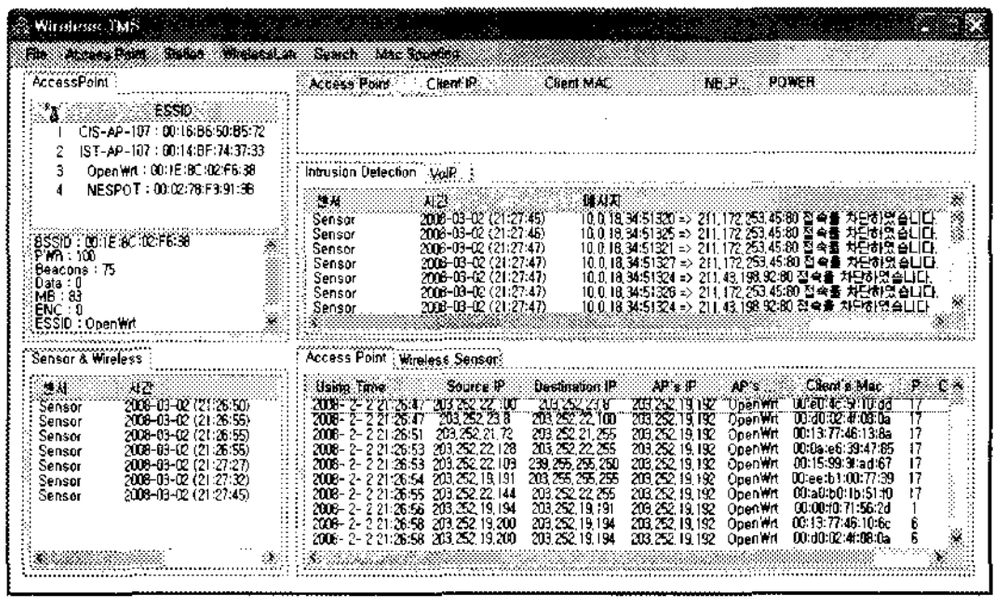


그림 10. W-TMS의 무선 패킷 정보 수집

AirSensor에서 DDoS 공격 탐지를 위한 임계치 설정을 위해 기존의 무선 인증 취약점 공격 툴인 MDK3를 이용하였다. 무선 인증 DDoS 공격 탐지 방식은 Statistical Intrusion Detection[12] 방식을 사용하였으며 성능 평가의 정확도를 높이기 위해 아래 [그림 9]와 같이 총 7번의 실험을 수행하였다.

패킷의 정보는 날짜와 시간대 별로 저장이 되며 이전에 AirSensor와 IAD로부터 수신된 패킷의 정보를 검색할 수 있도록 하였다. 검색시 무선 패킷내 IP 주소와 MAC 주소 및 접속한 AP 주소 등의 무선 네트워크 사용 정보를 보여준다. 무선 DDoS 공격이 탐지 되었을 경우 IAD로 공격 차단 신호를 송신하며 관리자에게 경고 메시지를 보여준다.

4.2 성능 평가

본 연구에서 제시한 기법의 패킷 분류 기능과 무선 네트워크 DDoS 공격 탐지 기능의 성능을 평가하였다. 무선 네트워크 환경에서 가상의 DDoS 공격을 수행하고 본 연구에서 제시한 모듈을 이용하여 탐지/차단되는 패킷을 측정하여 실험 결과의 신빙성을 높이고자 하였다. 무선 네트워크 DDoS 공격을 시도하기 위해 6개의 클라이언트에서 ICMP 패킷을 VICTIM에게 동시에 전송하였다.

우선 IAD 시스템에서는 본 연구에서 제공한 패킷마킹 모듈을 수행하기 때문에 [그림 11]과 같이 약간의 전송 지연이 발생하는 것을 확인할 수 있었다. 하지만 패킷 마킹으로 인한 손실은 발생하지 않는 것을 확인할 수 있었다.

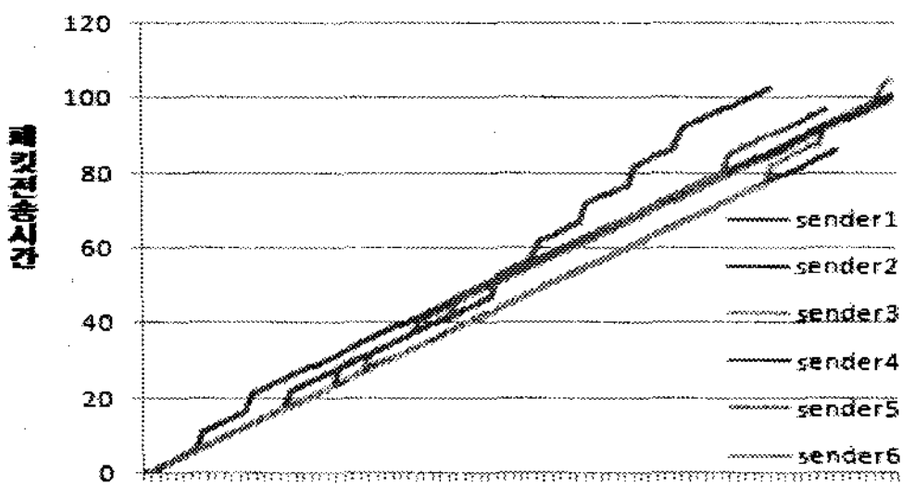


그림 11. IAD내 패킷 마킹으로 인한 송수신 지연

확률 기반 무선 패킷 마킹 기술을 이용하였기 때문에 아래 [그림 12]와 같이 대부분의 패킷에는 별도의 마킹 과정을 수행하지 않고 통과시키며 확률에 따라 특정 패킷에 대해서만 유무선 트래픽 분류를 위한 패킷 마킹 작업을 수행한다.

본 연구에서 제안한 DDoS 공격 탐지 및 대응 성능 실험 환경은 다음과 같다. IAD에서는 일반 패킷에 대해서는 마킹 등을 수행하여 전송하지만, 아래 [그림 13]과 같이 초당 6개 이상의 클라이언트가 18번의 패킷을 송신할 경우 DDoS 공격 패턴으로 판단하고 이를 차단한다는 것을 확인할 수 있었다. 6개의 클라이언트가 18번의 송신을 할 경우 총 108번의 동일 패킷을 전송한 경우로 DoS공격 외에는 드문 경우이다. 따라서 100번 이상의 DDoS 공격을 수행한 결과 IAD에서 차단 기능을 제공하는 것을 확인할 수 있었다.

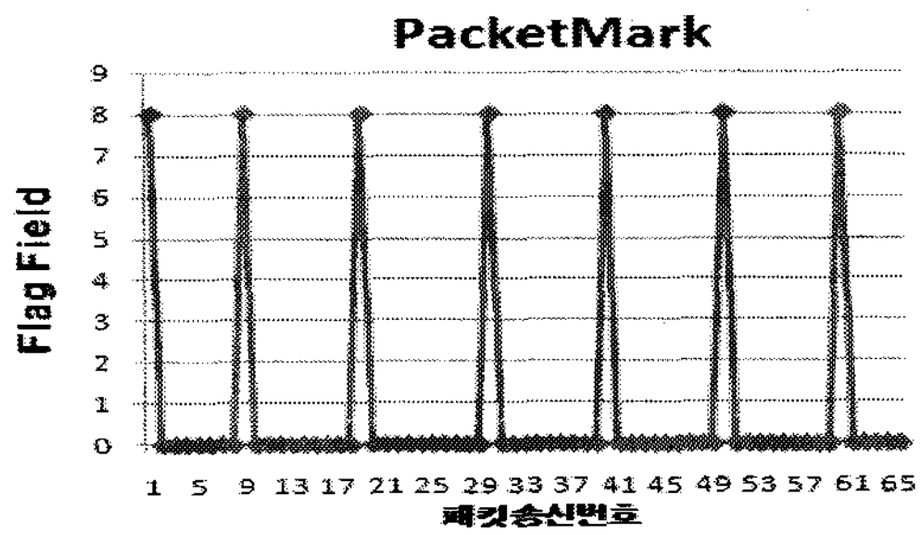


그림 12. 제안 알고리즘을 통한 패킷 마킹

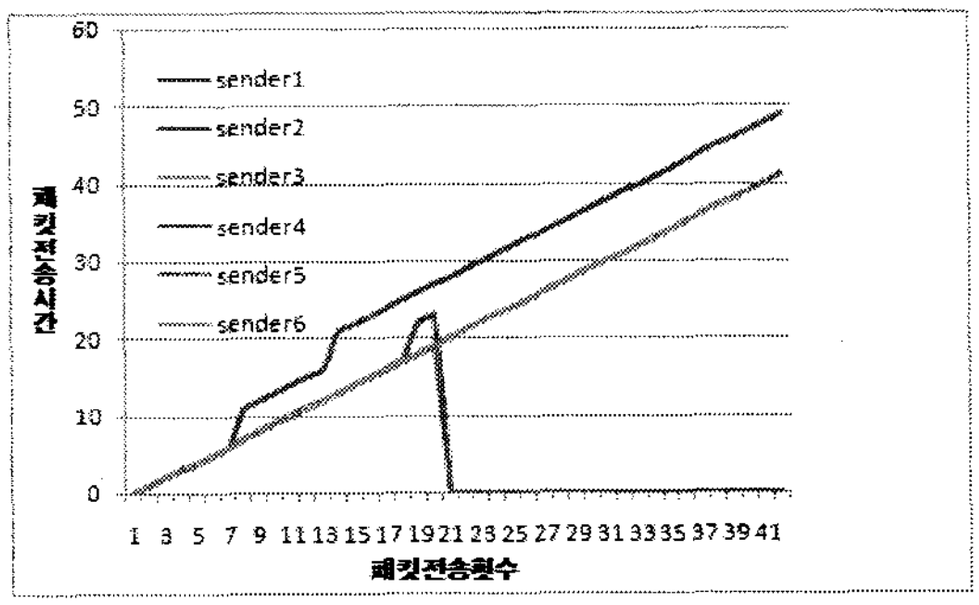


그림 13. DDoS 공격 탐지 및 대응

V. 결론

무선 네트워크 기술은 유선 네트워크에 비해 이동이 편리하고 네트워크 환경을 구축하는 비용이 저렴하다. 이러한 이유로 무선 네트워크 환경은 나날이 발전하고 있으며 사용자 수도 급증하고 있다. 하지만 무선 네트

워크 환경에서 DDoS 공격이 수행될 경우 기존 유선 네트워크 환경보다 공격 패턴에 대한 탐지 및 공격 근원지 역추적이 어렵다는 문제점이 발생한다.

기존 무선 네트워크의 취약점을 보완하기 위한 방안 중 하나는 IEEE 802.11i[15] 기술로써 관리 프레임 및 클라이언트에 대한 인증 기술을 높이고자 하였으나, 기존 장비와 호환이 되지 않는다는 단점이 존재한다. 따라서 본 연구에서는 최근 유무선 라우팅 기능과 함께 VoIP 통신 기능 등을 통합하여 지원하는 Integrated Access Device(IAD)가 개발되어 널리 배포되며 기존의 AP 기능을 대체하고 있다. 따라서 IAD 기반 무선 네트워크 환경에서도 유무선 트래픽에 대한 분류와 실시간 공격 탐지 기능이 제공되어야 한다.

본 연구에서는 AirSensor 모듈을 이용하여 IAD에 접속한 무선 네트워크 클라이언트 정보를 수집토록 하였으며, 무선 클라이언트의 공격 패킷에 대해 사전 차단 기능을 제공하였다. 또한 IAD에 수신된 패킷에 대해 W-TMS 시스템과 연동하여 DDoS 공격 트래픽을 판단하도록 하였기 때문에 안정적으로 IAD 기반 무선 네트워크 서비스 환경을 구축할 수 있었다. 물론 본 연구에서 제시한 기법은 AirSensor 모듈을 이용하여 무선 트래픽을 분산된 형태로 모니터링하고 있어야 한다는 단점이 있으나, 이 부분에 대해서는 현재 네스팟 기반 무선 네트워크 환경 및 최근 급속도로 연구가 확산되고 있는 무선 매쉬 네트워크(Wireless Mesh Network) 환경을 통해서 무선 환경에 대한 트래픽 모니터링 방식으로 해결 가능하다고 판단된다.

향후 연구로는 본 연구에서 제시한 패킷 마킹 및 트래픽 분류 기반 공격 탐지 기술을 무선 VoIP 서비스 기반 SIP 프로토콜에 적용하여 SIP 프로토콜에서의 비정상 트래픽을 판별하고 이를 모니터링 하는 기법에 대한 연구를 수행하고자 한다.

참 고 문 헌

[1] Y. X. Lim, T. Schmoyer, H. Levine, and H. L. Owen, "Wireless Intrusion Detection and Response," Proceedings of the 2003 IEEE Workshop on Information Assurance, pp.68-75, 2003.

[2] R. Fleck and J. Dimov, "Wireless Access Points and ARP Poisoning: Wireless vulnerabilities that expose the wired network," 2001.

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

[4] R. Beyah, S. Kangude, G. Yu, B. Strickland, and J. Copeland, "Rogue Access Point Detection Using Temporal Traffic Characteristics," Proceedings of IEEE GLOBECOM, 2004.

[5] 신승원, 오진태, 김기영, 장종수, "인터넷 웜 공격 탐지 방법 동향", 전자통신동향분석, Vol.20, No.1, pp.9-16, 2005.

[6] J. Branch, N. Petroni, V. Doorn, and D. Safford, "Autonomic 802.11 Wireless LAN Security Auditing," IEEE Security & Privacy, 2004.

[7] W. Wei, B. Wang, C. Zhang, J. Kurose, and D. Towsley, "Classification of Access Network Types: Ethernet, Wireless LAN, ADSL, Cable Modem or Dialup ?" Proceedings of IEEE INFOCOM, pp.1060-1071, 2005.

[8] S. J. Scott, "Threat Management Systems, The State of Intrusion Detection," SNORT, 2002.

[9] M. Lynn and R. Baird, "Airjack: a device driver for 802.11 raw frame injection and reception," 2003.

[10] V. Navda, A. Bohra, and S. Ganguly, "Using Channel Hopping to Increase 802.11 Resilience to Jamming Attacks," IEEE Infocom Minisymposium, 2007.

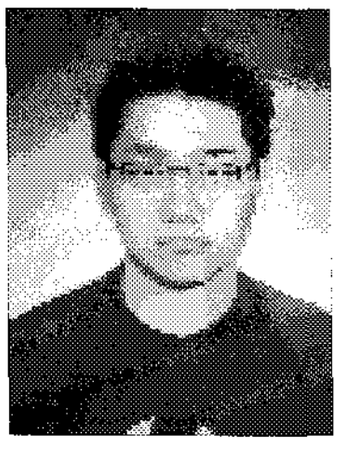
[11] J. Y. Jung, S. Schechter, and Arthur W. Berger, "Fast Detection of Scanning Worm Infections," RAID 2004, Sophia Antipolis French, 2004(10).

[12] C. Z. Cliff, G. Weibo, and T. Don, "Worm Propagation Modeling and Analysis under Dynamic Quarantine Defense," ACM WORMS '03, Washington DC, USA, 2003(10).

[13] R. David, "Message Queues," The Linux Kernel, 2001.
[14] 윤종호, *무선 LAN 보안프로토콜*, 교학사, 2005
[15] IEEE Standards, "IEEE 802.11i-2004: Amendment 6: Medium Access Control (MAC) Security Enhancements," Retrieved on 2007.

저 자 소 개

조 제 경(Je-Gyeong Jo) 준회원



- 2006년 2월 : 한신대학교 정보시스템공학과(공학사)
- 2006년 9월 ~ 현재 : 한신대학교 대학원(석사과정)

<관심분야> : 시스템보안, 네트워크보안, 보안공학, etc.

이 형 우(Hyung-Woo Lee) 정회원

- 1994년 2월 : 고려대학교 컴퓨터학과(이학사)
- 1996년 2월 : 고려대학교 컴퓨터학과(이학석사)
- 1999년 2월 : 고려대학교 컴퓨터학과(이학박사)
- 1999년 3월 ~ 2003년 2월 : 백석대학교 정보통신학부 교수
- 2003년 3월 ~ 현재 : 한신대학교 컴퓨터공학부 교수

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

박 영 준(Yeong-Joon Park) 정회원

- 1979년 2월 : 고려대학교 산업공학과(공학사)
- 1985년 2월 : 고려대학교 경영대학원 전자정보처리(경영학석사)
- 1997년 3월 ~ 현재 : 청강문화산업대학 물류유통정보과 부교수

<관심분야> : 컴퓨터네트워크, 유통정보