W-TMS(Wireless-Threat Management System)에서의 효율적 관리를 위한 위협 분류기법

Threat Classification Schemes for Effective Management based on W-TMS(Wireless-Threat Management System)

서종원, 조제경, 이형우
한신대학교 컴퓨터정보소프트웨어학부

Jong-Won Seo(seo0207@gmail.com), Je-Gyeong Jo(aiking@hs.ac.kr),
Hyung-Woo Lee(hwlee@hs.ac.kr)

요약

지난 10년 동안 인터넷은 빠른 속도로 모든 분야에 확산되어 왔으면 이와 비슷한 현상으로 최근 몇 년 동안 무선 네트워크의 확산 역시 빠른 속도로 보급되고 있는 추세이다. 그리고, 무선 네트워크 공격 시도 및 침입에 성공하는 공격의 횟수도 증가하고 있다. 이런 무선 네트워크 위협을 극복하기 위해 기존의 TMS는 필요에 따라 자동화되고 능동적인 대응 수단을 제공하기도 하지만, 새로운 형태의 무선 공격 등에는 효율적으로 대응하지 못한다는 취약점을 가지고 있다. 따라서 본 연구에서는 정보검색분야에서 사용되는 Vector Space모델을 이용해 실시간으로 유입되는 패킷과의 유사도를 비교하여, 분석된 유사도의 패턴을 분석해 무선 네트워크의 이상 징후를 탐지하고 자동으로 분류하는 기법을 설계했다.

■ 중심어 : | 무선네트워크 보안 | 무선네트워크 위협관리 시스템 | 공격 패킷 분류 |

Abstract

Internet had spread in all fields with the fast speed during the last 10 years. Lately, wireless network is also spreading rapidly. Also, number of times that succeed attack attempt and invasion for wireless network is increasing rapidly. TMS system was developed to overcome these threat on wireless network. Existing TMS system supplies active confrontation mechanism on these threats. However, existent TMS has limitation that new form of attack do not filtered efficiently. Therefor this paper proposes a new method that it automatically compute the threat from the imput packets with vector space model and detect anomaly detection of wireless network. Proposed mechanism in this research analyzes similarity degree between packets, and detect something wrong symptom of wireless network and then classify these threats automatically.

■ keyword : | Wireless Network Security | Wireless-Threat Management System | Attack Packet Classification |

* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학IT연구센터 지원사업의 연구결과로 수행되었습니다.
(IITA-(C 1090-0603-0016)

접수번호 : #070108-001
접수일자 : 2007년 01월 08일
심사완료일 : 2007년 01월 30일
교신저자 : 이형우, e-mail : hwlee@hs.ac.kr

I. 서론

네트워크의 발달과 더불어 네트워크 공격 유형의 변화도 빠르게 진행되고 있다. 과거에는 단일 기법의 소규모 시스템 및 서버에 대한 공격이 주를 이루었지만, 현재는 다양한 형태의 다수 피해를 동시다발적으로 발생시키는 공격으로 발전해나가고 있으며, 유선 네트워크 중심에서 무선 네트워크에 대한 공격 형태로 발전하고 있는 추세이다.

이처럼 자동화되고 강력해지는 무선 네트워크 공격에 대해 기존의 W-IDS(Wireless Intrusion Detection System)는 공격의 탐지를 통해 대응하는 시스템이다. 하지만 기존의 W-IDS는 탐지된 공격에 대해 적절히 대응하지 못하고 있으며 새로운 형태의 공격에 대한 탐지 등에 문제점을 보이고 있다. 따라서 W-IDS의 취약점을 보완하고 사전에 공격이 예상되는 패킷에 대해 능동적으로 대응하기 위해서는 무선 트래픽을 대상으로 한 W-TMS(Threat Management System)가 필요하다. 하지만 기존의 W-TMS는 위협의 판단 기준이 모호하고 비효율적인 관리로 실시간 유입되는 트래픽에 대한 대처가 수동적이다. 따라서 무선 트래픽의 MAC 헤더 정보를 이용하여 트래픽 분포 분석을 수행하고 이를 통해 이상 트래픽에 대한 탐지와 효과적인 위협 관리 체계를 구축할 필요가 있다.

본 연구에서는 패킷의 유사도를 분석하고 무선 트래픽 분포 분석을 통해 무선 네트워크에서 발생하는 모든 이상 징후을 조기에 파악하여 피해를 최소화 함으로서 네트워크 자원을 효율적으로 운영하고 관리 할 수 있는 W-TMS의 위협 분류 기법을 제안하였다. 본 연구에서 제안하는 W-TMS는 트래픽량과 흐름의 통계적 특성(Statistical Profiles) 및 패턴, DoS 공격 등에 의해 발생하는 일시적인 비정상적 트래픽의 패턴에 대해 탐지(Anomaly Detection) 기능을 제공한다.

본 논문의 구성은 다음과 같다. II장 관련연구에서는 기존의 TMS 기술에 대한 취약점 분석과 기존 네트워크 공격 분류 기법에 대해 살펴본다. III장에서는 무선 프레임의 캡처, 캡처된 무선 프레임의 분류를 위한 좌표공간에 표현 기법에 대해 설명하고, 위협탐지 방법 및 분석 방법에 대해 설명한다. 그리고 IV장에서는 무선 프레임의 분류에 이용된 MAC 헤더별 프레임 정보 및 분류의 예를 제시한다. 마지막으로 V장에서는 제안 기법에 대한 결론 및 향후 발전 가능한 분야 및 연구에 대해 설명 한다.

II. 관련연구

1. 기존 TMS(Threat Management System)

위협관리시스템(TMS; Threat Management System)이란 바이러스, 해킹 등 아직 일어나지 않은 사이버 위협을 예측하고 기술과 정보를 상호 보완적으로 결합해 능동적으로 방어할 수 있는 시스템이다[1]. [그림 1]과 같이 TMS는 일기예보의 기능과 유사하게 사전에 네트워크에 대한 공격 등을 예보할 수 있는 기능을 제공한다.

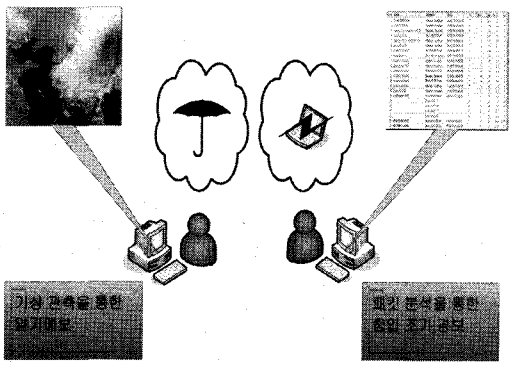


그림 1. 일기예보와 TMS의 비교

TMS 시스템의 가장 큰 특징으로는 단순히 외부 위협의 통계를 보여주는 것이 아니라 이를 종합적으로 분석해 대응책을 마련할 수 있기 때문에 보다 효과적인 보안 대응이 가능하다. 이처럼 네트워크의 위협의 분석을 위해서는 유입되는 패킷으로 부터 비정상적인 패킷을 탐지하는 방법이 가장 중요하다. 하지만 기존 TMS는 위협에 대한 정의가 모호해 전문가의 분석을 필요로 하고 객관성이 떨어지는 분석 정보를 시스템에서 사용하고 있다. 또한 자동화되지 않은 형태로 위협에 대한

분석 정보가 생성 되므로 실시간으로 유입되는 무선 패킷에 적절히 대응하기 어렵다. 따라서 최근 급속도로 확산되고 있는 무선 네트워크에서의 새로운 형태의 위협에 능동적으로 대응하지 못하고 있다. 따라서 본 연구에서는 기존 네트워크 공격 분류 기법에 대한 분석을 통해 문제점을 파악하고 무선 환경에 맞는 개선된 공격 분류기법에 대해 고찰하고자 한다.

2. 기존 네트워크 공격 분류 기법

효율적으로 공격에 대해 분류하기 위해서는 충분조건을 만족해야 한다. 충분조건들을 많이 수용할수록 좋은 분류법이라 할 수 있으며 다음과 같은 항목을 일반적으로 사용한다. 유무선 트래픽에 대한 효율적 분류를 위해서는 입증성, 이해성, 완벽성, 확정성, 상호배제, 반복성, 명확성 및 유용성 등을 만족해야 한다[2,3,4].

Howard의 분류법[3]은 광범위한 공격들을 포함할 수 있는 공격 프로세스 기반(process based) 분류법이다. 공격자, 도구, 접근, 결과, 목적의 다섯 개의 카테고리로 되어 있다. 공격의 전체 프로세스를 관찰하기에는 적절하지만 구체적인 공격 특성이 나타나 있지 않다. 예를 들면, Code Red와 같은 공격을 이 분류법으로 나누기에는 어려움이 따른다.

Lough의 분류법[7] Lough 는 공격의 특성에 기반을 둔 VERDICT(Validation Exposure Randomness Deallocation Improper Conditions Taxonomy)를 제안하였다. 공격의 특성에 기반 하였으므로 새로운 공격이나 혼합형(blended) 공격 등 어떤 공격이든지 분류에 포함시킬 수 있다. 그러나 모든 공격을 포함시키기 위해 분류 자체를 구체적으로 만들지 못했다는 단점이 있다. 예를 들면, 공격에 사용된 구체적인 기법(skill)뿐만 아니라, 이 공격이 흔히 알려져 있는 웜에 속하는지 바이러스에 속하는지에 대한 결정도 모호해진다.

따라서 기존의 분류기법들은 너무 일반적인 의미로서만 분류되어 실제 대응 방법 개발에 도움을 받기에는 빈약한 정보를 제공하고, 결국 개발자의 입장에서는 네트워크 보안 시스템이 바이러스, 웜, DoS공격, 스파이웨어(spyware), 애드웨어(adware)등과 같은 수많은 공격들 중 어떤 것들을 차단하려는 목적으로 설계되어야 할 지 조차 불명확해지게 된다[8].

따라서 본 연구에서는 무선 네트워크에 대한 고의적이고 불법적인 접근으로 인한 트래픽 증가 추이를 효율적으로 분석하기 위해 Vector Space 모델[9]을 적용하여 킷들 간의 유사도를 계산하고, 패턴 분류 모듈을 이용하여 무선 트래픽에서 비정상적인 이상 징후를 탐지하고 위협을 분류하는 것을 목적으로 한다.

3. Vector Space 모델

Vector Space[9] 모델은 질의(Input packet)와 문서(기 정의된 공격 packet)를 모두 용어 집합(MAC헤더 집합)으로 표현해 질의와 문서간의 global similarity를 계산하는 정보검색 모델이다. W-TMS은 공격 가능성이 있는 packet을 탐지 해내는 것이 일차적인 목표이다. 따라서 기존의 이분법적인 분류를 통한 위협 탐지는 위협의 범위를 극소화 시켜 해커들의 우회 공격 탐지에 부적합하다. 하지만 비 이진 가중치를 할당하는 전통적 정보검색 모델중 하나인 벡터 모델은 부분 정합이 가능한 틀을 제공해 보다 광범위한 무선 네트워크의 위협 탐지에 적용 가능한 방법이다. 본 연구에서 제안하는 모델에서는 Vector Space 모델을 사용하여 기 정의된 공격 packet과 실시간 유입되는 Input packet과의 유사도를 계산해 위협을 탐지해낸다.

수식 (1)의 $\overrightarrow{q}$는 기 정의된 공격 유형의 벡터이다. 그리고 w_{iq}는 공격 packet에서 추출된 MAC헤더 정보들의 Weight 값을 나타낸다. 그러므로 MAC헤더에서 추출해낼 수 있는 Indexing수와 t의 값은 같다. 그리고 각각의 MAC헤더 정보(w_{iq})의 Weight값은 무선 네트워크의 환경에 맞춰 임의적으로 설정할 수 있다.

$$\overrightarrow{q} = (w_{1q}, w_{2q}, w_{3q}, \ldots\ldots w_{tq})$$
$$w_{iq} \geq 0 \quad (1)$$

$$\overrightarrow{d}_j = (w_{1j}, w_{2j}, w_{3j}, \ldots\ldots w_{tj})$$
$$w_{ij} \geq 0 \quad (2)$$

예를 들어 Rouge AP에 대한 위협이 예상되는 무선 네트워크에서는 MAC헤더 정보의 BSSID에 대한 Weight 값을 높여 유사도 비교시 사용한다면 Rouge AP에 대한 위협 탐지률이 상승할 것이다.

수식(2)의 $\overrightarrow{d}_j$는 실시간으로 들어온 j번째 packet의 백터이다. w_{ij}는 수식(1)에서와 같은 방법으로 정의 된다.

수식(3)은 수식(1), 수식(2)의 기 정의된 공격 packet과 Input packet의 MAC헤더 정보(w_{iq}, w_{ij})의 Weight값을 이용해 cos유사도(similarity) 를 구한다. 이때 cos유사도의 값은 수식(4)와 같다.

$$sim(d_i,q) = \frac{\vec{d_j} \bullet \vec{q}}{|\vec{d_j}| \times |\vec{q}|} = \frac{\sum_{i=1}^{t} w_{ij} \times w_{iq}}{\sqrt{\sum_{i=1}^{t} w_{ij}^2} \times \sqrt{\sum_{i=1}^{t} w_{iq}^2}} \quad (3)$$

$$0 \le \mathrm{sim}\ (d_i, q) \le 1 \quad (4)$$

기 정의된 공격 packet과 Input packet과의 cos유사도의 값은 [그림 2]에서의 Θ 값에 의해 결정 되어 진다. Θ 값이 작으면 작을수록 유사도가 높아지는 것이다.

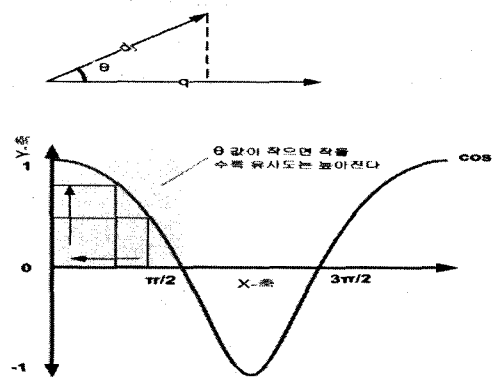


그림 2. cos 유사도(similarity)

III. 제안 기법

1. 제안하는 구조

본 연구의 핵심 사항중 하나인 위협의 탐지 방법은 유입되는 무선 패킷의 MAC 헤더 정보를 이용해하여 유사도 분석을 통한 무선 패킷의 이상 패턴을 탐지 하므로, 앞으로 있을 공격 위협에 대한 탐지 및 분류를 통해 보다 안정적이고, 능동적인 관리 시스템을 제안 한다. 본 논문에서 제안하는 위협 탐지 및 분류 모듈은 [그림 3]과 같은 형태로 수행된다. Local Incident Management System은 센서 역할을 담당하므로 자신의 영역에서의 무선 데이터에 대한 패킷 정보를 수집하여 Global Threat Management System으로 패킷 정보를 전송한다. Global Threat Management System은 수집된 패킷정보를 바탕으로 위협에 대한 탐지 및 분석을 담당하여 관리자에게 그 정보를 제공한다.

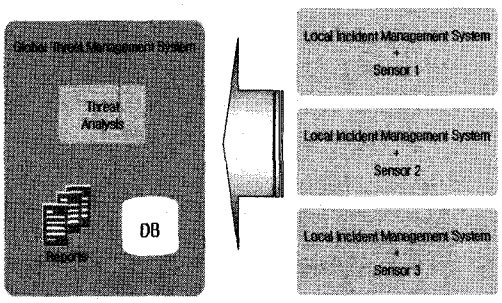


그림 3. W-TMS의 핵심 모듈 구조

[그림 4]는 본 연구에서 제시하는 W-TMS 시스템에서의 전체적인 처리 과정을 보인다. 우선 Wireless Sensor를 통해 무선 패킷 정보를 수집하고, 수집된 무선 패킷을 MAC 프레임별로 분류해 분석 모듈에게 전달한다. 또한 수집된 정보는 좌표 공간에 0부터 1사이의 값으로 변형된다. 이 변형된 값을 이용해 각 패킷간의 유사도를 계산하고, 시간에 따른 유사도의 분포 정보를 분석하여 무선 네트워크에서의 이상 패킷 발생 여부 및 이상 징후를 파악한다.

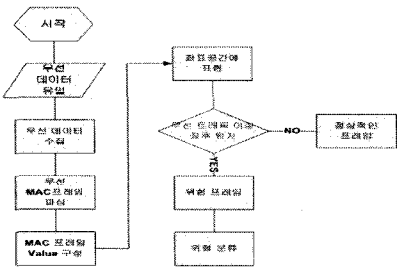


그림 4. W-TMS 프로세스

2. 1단계 : 무선 프레임 정보 수집

W-TMS(Threat Management System)은 무선 프레임의 캡처에 따라 위협 분석 및 관리의 신뢰도가 결정된다, 즉 무선 프레임의 캡처 없이는 어떠한 위협의 분석 및 관리도 이루어 질 수 없다. 그리고 캡처한 데이터를 Global Thread Management System으로 전송해 위협에 대한 탐지 및 분류를 할 수 있다.

이때 무선 네트워크의 Channel이 존재하는데 이 Channel Hoping을 통해 모든 Channel의 무선 프레임을 캡처해야한다. [그림 5]는 [그림 3]에서 제시한 Sensor를 이용하여 무선 프레임에 대한 캡춰 결과를 보인다.

1단계 과정에서는 센서에 의해 무선 프레임을 수집하는 과정이다. 각 센서에서는 무선 프레임에 대한 수집 및 파싱 과정을 수행하게 된다.

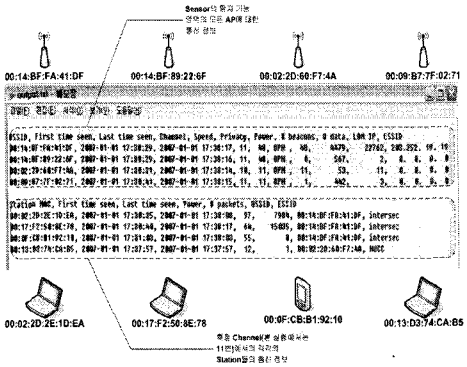


그림 5. Sensor 캡처 결과

무선 프레임에 대한 정보 수집 과정은 Windows XP를 기반으로 airodump 2.1 S/W를 사용하였고, 무선 랜카드는 Atheros Chipset(PCMCIA Type)의 3COM 3CRPAG175B, 디바이스 드라이버는 The WildPackets Atheros Wireless Driver v4.2이다. airodump 2.1를 지원하는 하드웨어 정보는 [10]에서 확인 할 수 있다.

3. 2단계 : MAC 헤더 정보 추출

네트워크 보안을 위한 공격 분류 체계를 따르면, 특정 공격에 대해 일반적으로 다음과 같은 정보에 따라 공격 유형이 결정되어 진다. "A라는 공격자가 B라는 취약점을 이용해 C의 방식으로 D라는 공격 목적을 달성하기 위해 E라는 공격 대상에 F라는 공격 기법들을 사용한다[8]". 따라서 무선 프레임 정보로부터 공격과 관련된 연관성 정보를 얻을 수 있다면 위협에 대한 사전 탐지 및 분류가 가능해 진다. 따라서 본 연구에서는 [그림 6]과 같이 무선 패킷 MAC헤더 정보를 이용해 추출된 MAC 헤더정보의 특성 값으로 전환하여 좌표 공간에 표현한 후에 이를 분석하여 위협 패턴을 탐지하고 분류하는 기법을 사용하였다.

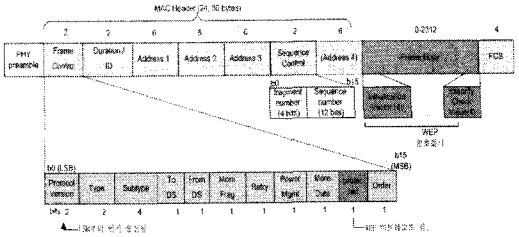


그림 6. 802.11 MAC 프레임

아래 [표 1]은 공격 유형을 결정짓는 MAC헤더 정보를 보여주고 있다.

표 1. 공격유형을 결정 짓는 MAC헤더 정보

정보 유형 / 공격요소	MAC헤더 정보	비고
A(공격자)	Source	Rogue AP 탐지 용이
B(취약점)	Protocol	■
C(공격 방식)	Protocol, packet량	■
D(공격 목적)	■	■
E(공격 대상)	Destination, BSSID	DoS공격 탐지 용이

4. 3단계 : MAC 프레임 특성값 구성

Sensor에 의해 캡처된 패킷들을 효율적으로 자동화된 위협 분류에 사용하며 무선 패킷에 대한 유사도 분석을 위한 Input데이터로 적용하기 위해서는 수치화하여 Vector 값으로 표현하는 것이 가장 중요한다. 본 논문에서는 좌표공간의 Vector형태로 모든 패킷들을 표현하기 위해 [표 2]와 같이 MAC 프레임 단위로 특징값들을 추출한다.

표 2. 유사도 분석을 위한 Packet Features 구성

Index	MAC헤더 정보	Type Value
1	Protocol Version	0
2	Type	Real
3	Subtype	Real
4	ToDs	Real
5	FromDs	Real
6	More Frag	Real
7	Retry	Real
8	Power Mgmt	Real
9	More Data	Real
10	Protectde	Real
11	Order	Real
12	Duration/ID	Real
13	Address 1	Real
14	Address 2	Real
15	Address 3	Real
16	fragment number	Real
17	sequence number	Real
18	Address 4	Real

[표 2]에서 정의된 Type Value는 MAC 헤더의 실제 값이 2진값으로 전달되므로 헤더정보들을 10진수로 전환한 후 0~1의 수로 표현한다. MAC 헤더 정보의 Type Value를 이용해 각 패킷들은 좌표공간의 Vector 형태로 표현할 수 있다.

5. 4단계 : 좌표공간위에 무선 프레임 표현

무선 프레임을 좌표 공간에 표현할 경우 위협에 대한 탐지 및 분류가 용이해 진다. 그러나 효율적인 위협의 탐지를 위해 Index 추출(좌표 공간의 축)기준에 따라 위협 분류엔진의 성능이 결정된다.

본 연구에서는 [그림 7]과 같이 현재 무선 네트워크에 유입되는 무선 패킷들의 MAC 헤더 정보를 보고 Indexing된 좌표공간에 표현할 수 있다. 한마디로 이상 트래픽에 대한 탐지를 통해 위협의 추이를 분석하여 앞으로 있을 위협 및 침입에 대한 예상을 할 수 있는 사전 감지 시스템을 구축할 수 있다.

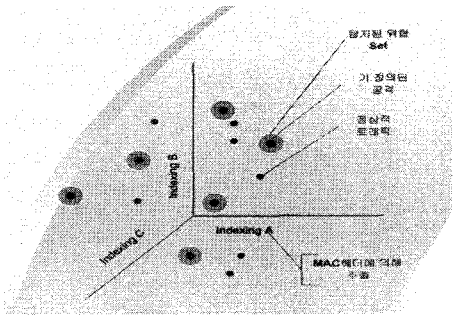


그림 7. 좌표공간에 표현된 제안 모델

6. 5단계 : 위협 탐지 모듈 적용

일반적으로 무선에 대한 위협은 특정한 패턴을 가지고 있다. DoS공격 같은 경우는 특정 목적지로 많은 패킷이 유입되는 특성을 알 수 있다. 이때 가장 큰 특징을 보면 AP에 많은 양의 접속 요청 메세지인 Probe Req를 전송해 AP의 자원을 낭비 시키는 것을 볼 수 있다. 이처럼 무선 패킷들에 대한 유사도를 분석 후 특정 공격에 대한 패턴을 분석해 무선 네트워크의 이상 징후를 파악하고 탐지 할 수 있다. [그림 8]은 위협 탐지 및 분류 기법의 예로, 입력된 데이터에 대한 분포 분석 모듈의 결과를 보여주고 있다.

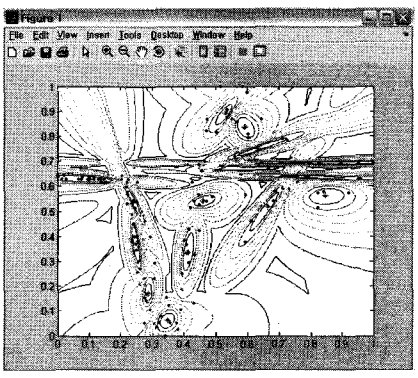


그림 8. 입력 데이터의 분포에 대한 분류

[그림 8]는 Matlab을 이용해 입력된 데이터에 대한 분포를 패턴 별로 분류하는 모듈이다. 이러한 분류 과정을 통해 무선 데이터의 이상 트래픽에 대한 탐지 및 분류를 하며, 분류된 자료를 통해 무선 네트워크 공격으로 발전 할 수 있는 수 많은 알려지지 않은 위협에 대해 관리 할 수 시스템을 구축 할 수 있다.

7. 6단계 : 탐지된 위협의 관리 및 분류

탐지된 위협은 관리 대상이 되어 관리의 편의성을 위해 잠재적 위협, 활성화된 위협, 상승하는 위협, 감소하는 위협으로 분류해 단계별로 적적한 대응에 필요한 의사 결정을 지원하기 위해 기술과 정보를 제공한다. (맞춤형 관리 시스템) 이러한 관리 기법은 탐지된 위협 집합의 원소들의 변화로 정의되어 관리자에게 정보로 제공된다.

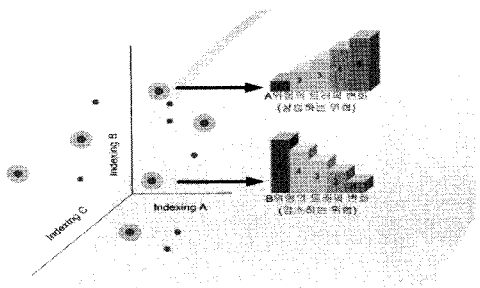


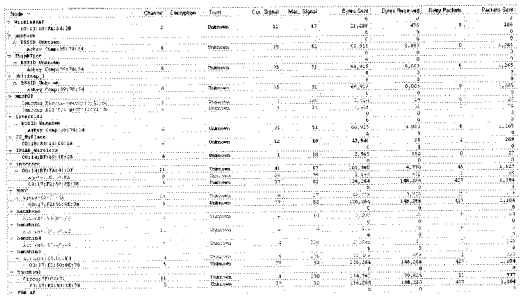
그림 9. 위협 분석 기법

[그림 9]은 실시간으로 유입되는 무선 프레임의 분석을 통해 위협을 관리 할 수 있는 형태로 변형시킨 것이다. 막대그래프의 값은 유입된 무선 패킷의 수를 의미한다.

IV. 실험

본 연구의 실험은 III장 1절 "무선 프레임 캡처"에서 캡처한 packet들을 Channel별 시그널 정보, AP별 packet량, protocol별 정보, 각각의 station의 peer map을 도시화하여 위협 탐지에 사용될 수 있는 Index별 추출에 기반이 되는 정보를 가공하였다.

실험 환경은 Windows XP이고 캡처 프로그램은 WildPackets AiroPeek NX, 무선 랜 카드는 Atheros Chipset(PCMCIA Type)의 3COM 3CRPAG175B, 디바이스 드라이버는 The WildPackets Atheros Wireless Driver v4.2이다. 그리고 Channel Hopping을 통해 모든 Channel을 캡처하였다.



무선 트래픽 정보

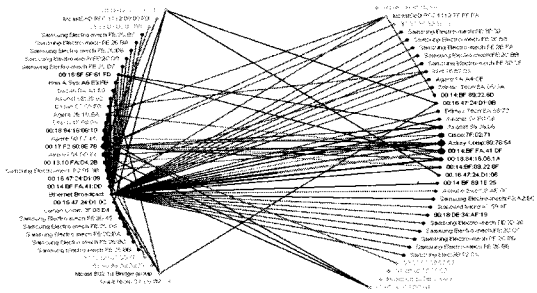


그림 10. MAC헤더 정보를 이용해 공격 분류체계에 사용될 정보 단위로 정리한 실험 결과

[그림 10]의 MAC헤더 정보를 이용해 Vector Space 모델을 적용한 유사도 비교과정을 거쳐 패킷들의 패턴을 분석 할 수 있다. 이때 패킷들의 유사도 패턴 분석은 [그림 8]과 같은 형태로 이루어져 분류된 패턴에 대한 관리 체계를 마련 할 수 있는 정보를 제공하게 된다.

V. 결론 및 향후연구

네트워크 공격을 분류하는 목적은 다양한 공격들을 미리 정의된 원칙에 따라 분류하고 이 분류된 자료를

바탕으로 공격의 특성을 쉽게 파악하여 그에 대한 방어 수단 마련에 도움을 주기 위함이다. 이런 관점에서 본다면, 본 연구는 위협의 단순한 경고 시스템을 넘어 차세대 보안 시스템인 Risk Management System에도 활용되어 위험의 실시간 관리가 가능하도록 위협의 탐지 방법에 대해 제안했다. W-TMS와 정보검색의 Vector Space 모델을 이용해 정상적인 무선 packet과 위협 및 공격적인 packet을 분류할 수 있다. 그러므로 본 연구는 기존의 W-TMS는 보다 지능적이고 자동화된 무선 사전경고 시스템의 핵심 모듈을 제안했다, 말할 수 있다. 향후 MAC 헤더에서 packet의 중요도에 따른 효율적인 위협 탐지 및 정확도를 높이는 방법에 대한 연구가 필요하다.

참 고 문 헌

[1] 임채호, *능동 보안위협관리*, ca expo, 2004.

[2] E. Amoroso, "Fundamentals of Computer Security Technology," Englewood Cliffs, New Jersey, Prentice Hall, 1994.

[3] J. D. Howard, "An Analysis of Security Incidents on The Internet 1989-1995," PhD thesis, Carnegie Mellon University, 1997.

[4] U. Lindqvist and E. Jonsson, "How to Systematically Classify Computer Security Intrusions," IEEE Security and Privacy, 1997.

[5] I. V. Krsul, "Software Vulnerability Analysis," PhD thesis, Purdue University, 1998.

[6] M. Bishop, "Vulnerabilities Analysis," International Symposium on Recent Advances in Intrusion Detection, 1999.

[7] D. L. Lough, "A Taxonomy of Computer Attacks with Applications to Wireless Networks," PhD thesis, Virginia Polytechnic Institute and State University, 2001.

[8] http://kidbs.itfind.or.kr/new-bin/WZIN/WebzineRead.cgi?recno=0901014408&mcode=jugidong

[9] http://en.wikipedia.org/wiki/Vector_space

[10] http://www.wildpackets.com/support/product_support/airopeek/hardware

[11] http://en.wikipedia.org/wiki/Information_entropy

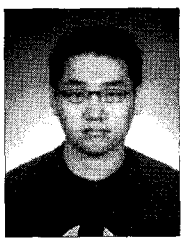
저 자 소 개

서 종 원(Jong-Won Seo) 준회원

- 2006년 2월 : 백석대학교(구 천안대학교) 정보통신학부 (공학사)
- 2006년 3월 ~ 현재 : 한신대학교 컴퓨터정보대학원 (석사과정)

<관심분야> : 네트워크 보안, Bio 정보보호, 암호학

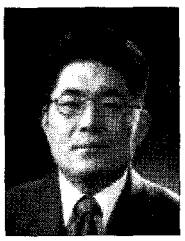
조 제 경(Je-Gyeong Jo) 준회원



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

<관심분야> : 시스템보안, 네트워크보안, 소프트웨어 공학

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 : 천안대학교 정보통신학부 조교수
- 2003년 3월 ~ 현재 : 한신대학교 컴퓨터정보소프트웨어학부 부교수

<관심분야> : 네트워크 보안, Bio 정보보호, 스팸메일 방지, 암호학