Journal of The Korea Institute of Information Security & Cryptology(JKIISC) ISSN 1598-3986(Print)
VOL.23, NO.3, June 2013 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2013.23.3.431

SVM을 이용한 중계 로그 AP 탐지 기법*

강 성 배,[1†] 양 대 헌,[1‡] 최 진 춘,[1] 이 석 준[2]
[1]인하대학교, [2]한국전자통신연구원

Relaying Rogue AP detection scheme using SVM*

Sung-bae Kang,[1†] Dae-hun Nyang,[1‡] Jin-chun Choi,[1] Sok-joon Lee[2]
[1]INHA University, [2]Electronics and Telecommunications Research Institute

요 약

스마트기기가 보편화되고 있고 무선랜의 사용량이 증가함에 따라 로그 AP를 이용한 공격 가능성도 높아지고 있다. 로그 AP에 접속할 경우, 로그 AP는 중간자 공격(Man-in-the-middle attack)을 수행할 수 있으므로, 매우 쉽게 개인 정보를 획득할 수 있게 된다. 다양한 종류의 로그 AP를 탐지하는 방법에 관해 많은 연구가 이루어지고 있고, 이 논문에서는 그 중, 정상 AP에 무선으로 연결하고 이를 중계해서 자신은 정상 AP의 SSID를 보여줌으로써 정상 AP인 것처럼 하여 사용자를 속이는 로그 AP를 탐지하는 방법을 제안한다. 이런 로그 AP를 탐지하는 데 있어서 기계학습 알고리즘의 일종인 SVM(Support Vector Machine)을 사용하여, 사용자의 환경에 따라 자동으로 탐지 기준을 설정하여 로그 AP를 90% 이상의 확률로 탐지하는 알고리즘을 제안하고, 이의 성능을 실험을 통해 입증한다.

ABSTRACT

Widespread use of smartphones and wireless LAN accompany a threat called rogue AP. When a user connects to a rogue AP, the rogue AP can mount the man-in-the-middle attack against the user, so it can easily acquire user's private information. Many researches have been conducted on how to detect a various kinds of rogue APs, and in this paper, we are going to propose an algorithm to identify and detect a rogue AP that impersonates a regular AP by showing a regular AP's SSID and connecting to a regular AP. User is deceived easily because the rogue AP's SSID looks the same as that of a regular AP. To detect this type of rogue APs, we use a machine learning algorithm called SVM(Support Vector Machine). Our algorithm detects rogue APs with more than 90% accuracy, and also adjusts automatically detection criteria. We show the performance of our algorithm by experiments.

Keywords: Rogue AP, SVM, Wireless Network, Network Security

I. 서 론

스마트폰, 태블릿, 노트북 등의 사용이 보편화 되면서 무선망을 통한 인터넷 연결이 일반화되고 있으며 이러한 수요에 맞추어 통신사들은 자사의 고객유지를 위하여 광범위한 지역에 무선공유기를 설치하여 무선망을 사용하고 있다. 공공기관이나 개인 사업장 또한 무선공유기를 설치함으로써 학교, 회사, 커피숍, 지하철과 같은 공공장소에서의 무선망 사용량이 급증하고 있다.

이러한 무선망의 사용량이 급증함에 따라 악의적인 공격자에 의한 로그 AP(Rogue Access Point)에 대한 보안문제가 심각해지고 있다. 로그 AP는 실제

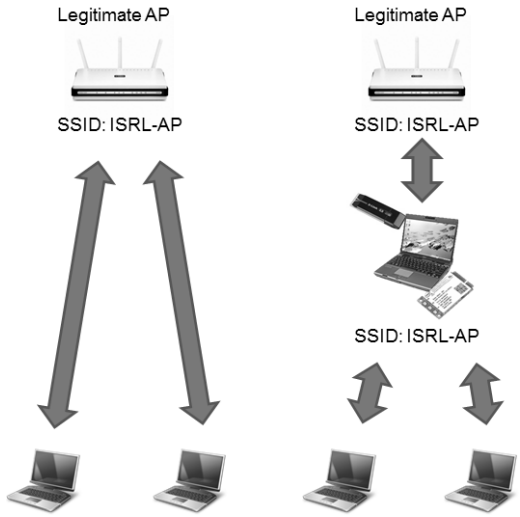
접수일(2013년 2월 15일), 수정일(2013년 4월 11일), 게재확정일(2013년 4월 17일)
* 본 연구는 미래창조과학부가 지원한 2013년 정보통신·방송(ICT) 연구개발사업의 연구결과로 수행되었음(12-912-06-001, "MTM기반 단말 및 차세대 무선랜 보안 기술 개발")
† 주저자, sbkang87@isrl.kr
‡ 교신저자, nyang@inha.ac.kr(Corresponding author)

정상적으로 인터넷을 제공해 주기 위해 해당 장소의 관리자 등에 의해 설치된 정상적인 AP가 아닌 무선망의 취약점을 이용하여 악의적인 공격자가 사용자의 정보를 가로채기 위하여 정상적인 AP인척하는 AP이다. 일단 사용자가 로그 AP에 접속하게 되면 공격자는 사용자의 특정 아이디나 비밀번호를 알아낼 수 있으며 사용자가 행하는 모든 행위에 대한 정보를 수집할 수 있으며 기업은 기업의 기밀정보 또한 유출될 수 있다. 악의적인 공격자는 로그 AP를 이용하여 피싱사이트를 제공하는 방식으로 공격자가 의도한 대로 정보를 변조하여서 사용자에게 제공할 수도 있다.

로그 AP를 만드는 방법으로는 AP를 직접 유선망에 연결하여 인터넷을 제공해주는 방법과 무선랜카드 2개를 가지고 1개의 무선랜카드는 인터넷에 연결하고 또 다른 1개의 무선랜카드는 인터넷을 제공해 주는 방법이 있다. 실제 공공장소에서 물리적으로 연결된 유선망의 유선을 찾아서 직접 AP를 가져다 꽂는 경우는 실제로 유선을 찾아 AP를 연결하는 행위를 하는 사람을 직접 찾아내기도 쉬울 뿐만 아니라 일단 몰래 AP를 연결하고 난 후에는 정상적인 AP와 구분할 수 없다. 따라서 본 논문에서는 언제 어디서나 쉽게 설치할 수 있으며 주변의 주목을 받지 않아도 되는 2개의 무선랜카드를 가진 장치에서 무선망으로 연결하여 인터넷을 제공해 주는 경우만을 고려한다.

기존의 로그 AP를 탐지하는 간단한 방법으로 AP의 MAC 주소, IP 주소, 판매자 이름, SSID 등의 AP의 정보를 이용하여 정상적인 AP에서는 나올 수 없는 정보를 발견하면 로그 AP로 간주하는 방법이 있다. 악의적인 공격자의 로그 AP는 점점 스마트해지고 있으며 이러한 간단한 방법은 MAC 주소 위조나 IP 주소 위조 등 각종 위조를 통하여 간단하게 회피할 수 있다. AP의 위치정보를 이용하여 정상적인 위치에 있는 AP인지를 판단하여 로그 AP를 탐지하는 기법이나 유, 무선망의 프로토콜 특성 또는 RTT 값을 이용하는 기법 등의 로그 AP 탐지 기법을 관련 연구에서 자세히 소개한다.

본 논문에서는 유, 무선망의 특성을 이용하여 정상적인 AP와 로그 AP 간의 RTT 값의 차이로 로그 AP를 탐지해 내는 H. Han 등이 제안한 기법을 기반으로 하여 해당 기법을 보완하였고 H. Han 등이 제안한 기법에 비해 좀 더 현실적이며 엄격한 실험환경을 구현하였으며 정상적인 AP와 로그 AP를 분류하는 알고리즘을 단순한 일차방정식이 아닌 SVM (support vector machine)을 이용하여 더 정확하게 분류한다.



〔그림 1〕 정상적인 AP와 로그 AP

기존 논문에서는 채널사용량의 증가에 따라서 로그 AP의 탐지율이 60%까지 떨어진 것을 RTT 값 측정 데이터 표본의 개수 증가로 80%까지 향상하게 시켰으나 본 논문에서는 더 나은 실험환경과 SVM을 사용한 분류로 덕분에 90% 이상의 로그 AP 탐지율을 보여준다.

본 논문의 2장에서는 기존의 로그 AP 탐지 기법들과 SVM의 개요 등 관련 연구에 대해 설명한다. 3장에서는 H. Han 등이 제안한 로그 AP 탐지 기법을 소개하고 해당 기법에서 보완해야 할 점에 대해 논의한다. 4장에서는 우리가 제안하는 탐지 기법을 소개하며 기존 논문과의 차이점을 설명한다. 5장에서는 로그 AP를 탐지하는 실험을 구현한 실험 환경에 대해서 설명한다. 6장에서는 실험 결과에 대한 분석과 기존 논문의 알고리즘을 적용한 로그 AP 탐지 결과와 본 논문에서 제안하는 SVM을 이용한 로그 AP의 탐지 결과를 비교하여 설명한다. 마지막으로 7장에서는 결론과 앞으로의 연구 계획을 소개한다.

II. 관련 연구

2.1 로그 AP

본 논문에서의 로그 AP는 〔그림 1〕에서처럼 무선랜카드 2개를 가진 장치에서 1개의 무선랜카드는 무선망을 이용하여 인터넷에 연결하고 나머지 1개의 무선랜카드는 인터넷을 제공해 주는 중계 로그 AP를 로

그 AP로 정의하여 사용한다. 사용자는 traceroute와 같은 명령어로 로그 AP인지 아닌지를 판단하려는 시도해볼 수 있으나 스마트해진 로그 AP는 자신이 연결된 정상적인 AP의 MAC 주소는 물론 IP 주소, 판매자 이름 등의 정보를 가져와서 위조할 수 있다. TCP ACK을 이용하거나 ping request를 이용한 RTT 측정값으로 로그 AP를 검출해내는 방법은 로그 AP가 ACK을 대신 대답하여 주거나 ping response를 대신하여 대답함으로써 간단하게 회피할 수 있다. 따라서 우리는 이러한 스마트해진 로그 AP를 효율적으로 탐지해내는 것을 목표로 한다.

2.2 로그 AP 탐지 기법

2.2.1 AP의 정보를 이용하는 탐지 기법

2006.년 P. Bahl 등은 AP의 SSID와 MAC 주소를 이용하여 정상적인 AP와 로그 AP를 분류하는 기법을 제안하였다[1]. 이 기법은 사용자들의 컴퓨터에 설치되어 위협상황을 알려주는 DAIR 시스템, 무선네트워크의 패킷들을 모니터링 하려는 Air Monitor, Air Monitor로부터 오는 위협상황을 DAIR 시스템으로 전송해주기 위한 Inference Engine으로 구성되어 있다. Air Monitor는 주변의 모든 무선데이터를 모니터링하며 새로운 AP의 SSID와 MAC 주소가 발견되는 경우 이를 데이터베이스에 저장된 정보와 비교, 일치하는 정보가 있을 때 정상적인 AP로 간주한다. 일치하는 정보가 없다면 로그 AP로 간주한다. 새로 발견된 AP가 로그AP로 판별될 때 Air Monitor는 이 사실을 Inference Engine에 알리고, Inference Engine은 이러한 사실을 DAIR 시스템으로 전송하고, DAIR 시스템은 로그 AP의 SSID와 MAC 주소를 사용자에게 알려준다. P. Bahl 등은 합법적인 AP의 SSID와 MAC 주소로 위조하는 로그 AP를 탐지해내는 방법들 또한 제시하였다. 합법적인 AP의 SSID와 MAC 주소를 위조하는 로그 AP를 가장 쉽게 식별하는 방법은 접속 이력 정보를 이용하는 방법이다. 새로운 AP가 다른 정상적인 AP의 SSID와 MAC 주소를 전송하면 Air Monitor는 기존의 접속 이력 정보에 해당 AP의 SSID와 MAC 주소가 없으면 이를 로그 AP로 판별한다. 하지만 로그 AP가 근처에 있는 정상적인 AP의 SSID와 MAC 주소를 위조할 때 첫 번째 메커니즘으로는 로그 AP를 식별해낼 수 없을 것이다. 이러한 문제를 해결하는 방법의 하나는 MAC 프레임의 순서 번호를 이용하는 방법이다. IEEE 802.11의 MAC 프레임에는 순서번호가 존재하며, 패킷이 전송할 때마다 이 값을 증가시킨다. 이러한 특징을 이용하여 Air monitor는 로그 AP가 보낸 패킷의 MAC 프레임의 순서번호와 정상적인 AP가 보낸 순서번호를 분석하여 로그 AP를 식별해낼 수 있다. 근처의 합법적인 AP의 SSID와 MAC 주소를 위조하는 로그 AP의 설치위치를 분석하여 식별해낼 수 있다. 해당 AP 근처에 있는 Air Monitor들로부터 해당 AP로부터 오는 신호의 세기를 측정하여 이를 분석하면, AP의 위치를 알 수 있을 것이며, 측정된 위치 정보를 이용하여 로그 AP를 식별한다. 이 기법은 무선 AP가 많은 네트워크 환경에는 적합하지 않으며, 장비의 이동이 잦은 조직에는 이를 적용하기가 어렵다. 또한, 로그 AP를 탐지하기 위해 추가적인 장비를 필요로 한다.

2007년 D. Schweitzer 등은 AP의 위치정보를 이용하여 로그 AP를 탐지하는 기법을 제안하였다[2]. 분산된 무선 네트워크 모니터링 시스템이 정상적인 AP들의 신호 세기를 중앙서버에 보내면 중앙서버는 모니터링 시스템이 보내온 정보를 이용하여 정상적인 AP의 신호반경을 나타내는 프로파일맵을 생성한다. 어느 특정위치에서 AP가 발견될 때 모니터링 시스템들은 해당 AP의 신호의 세기를 중앙 서버에 전송해주고, 중앙 서버는 생성된 프로파일맵을 이용하여 해당 AP의 위치가 정상적인 AP가 설치된 위치인지 판단한다. 프로파일과 일치하지 않는 신호 세기를 발생시키는 AP는 로그 AP로 분류된다. 이 기법은 P.Bahl 등이 제안한 기법과 마찬가지로 무선 AP가 많은 네트워크 환경에는 적합하지 않으며, 장비의 이동이 잦은 조직에는 이를 적용하기가 어렵다. 또한, 로그 AP를 탐지하기 위해 추가적인 장비들이 필요하다.

2.2.2 유, 무선망 의 차이를 이용하는 탐지 기법

2007년 L. Watkins 등은 유선 네트워크와 무선 네트워크의 RTT 값의 차이를 이용하여 유선망에 불법으로 연결된 로그 AP를 찾는 기법을 처음으로 제안하였다[3]. 일반적으로 무선 네트워크는 유선 네트워크와 비교하면 전송속도와 용량(Capacity)이 제한적이기 때문에 유선 네트워크와 비교하면 RTT 값이 클 수밖에 없다. 이러한 점을 이용하여 유, 무선 네트워크에 전송되고 있는 패킷들의 RTT 값들을 수집한 후 현재 전송되고 있는 패킷들의 RTT 값과 비교하는 방

식으로 로그 AP를 탐지하는 기법을 제안하였다. 이 기법은 네트워크상에 전송되는 패킷들의 정보를 수집해야 하고 수집한 패킷들의 정보를 비교, 분석해야 하는데 시간이 걸리는 단점이 있다.

W. Wei등은 TCP의 ACK(Acknowledge)을 이용하여 유선 네트워크에 불법으로 연결된 로그 AP에 접속한 사용자들을 탐지하는 기법을 제안하였다[4]. 이 기법은 TCP 패킷의 발신자가 패킷을 전송하면 수신자가 이에 대한 응답으로 ACK를 보낸다는 점을 이용하였다. 이 기법에서 Detection system은 자신과 통신하고 있는 AP들에 패킷을 전송하고 ACK를 받지 못한 패킷들을 각각의 IP에 대응하는 unacked-data-pkt-queue에 유지하고 ACK가 도착하면 해당 IP의 unacked-data-pkt-queue에서 대응하는 패킷을 식별하여 RTT 값을 구한다. 이렇게 구해진 RTT 값을 분석하고 난 후 무선 네트워크를 통해 패킷이 전달되었다고 판단하면 해당 IP를 사내의 무선 IP 리스트와 비교하여 공인된 IP가 아닌 경우에는 이를 로그 AP를 통해 접속한 사용자로 분류한다. 이 기법은 로그 AP가 Detection system이 보낸 패킷을 식별해낼 수 있는 경우 해당 패킷에 대한 ACK를 빠르게 전송하는 방식으로 탐지를 회피할 수 있다는 단점이 존재한다.

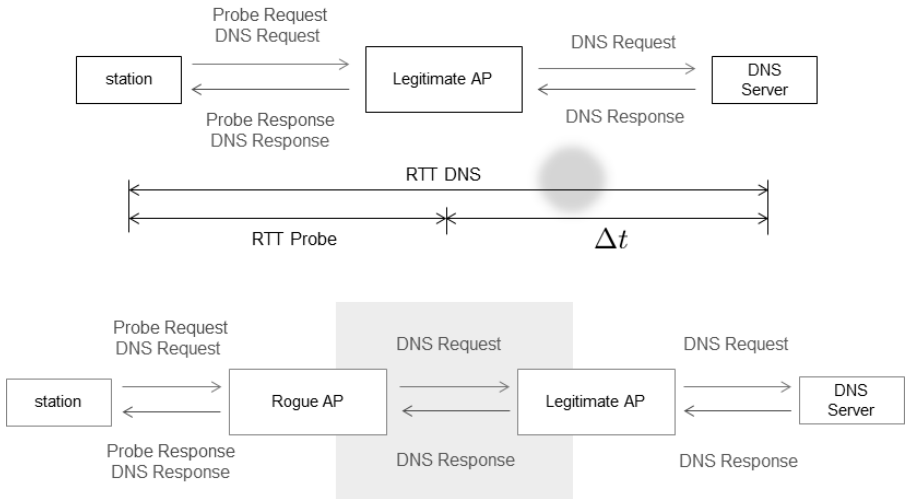
2012년 김이룩 등은 이동통신망(3G)을 사용하는 로그 AP를 탐지하는 기법을 제안하였다[5]. 이 기법에서 정상적인 AP는 사용자로 보낸 데이터를 유선 또는 무선망을 통해 다음 홉으로 전송하는 데 반해, 이동통신망을 사용하는 로그 AP는 사용자가 보낸 데이터를 기지국으로 전송하는 특징이 있다. 해당 기법에서는 RTT 값을 구하기 위해 TTL 값이 1과 2로 설정된 ICMP 패킷들을 n번 전송한다. 전송된 패킷은 RTT 값이 1 또는 2이기 때문에 기지국에서 폐기되며, 패킷을 폐기한 기지국은 ICMP 에러 메시지를 전송한다. 사용자는 1홉 거리에 있는 기지국으로부터 송신된 n개의 ICMP 에러 메시지 패킷의 타임스탬프를 이용하여 RTT_{hop1}을 구하고, 2홉 거리에 있는 기지국으로부터 송신된 n개의 ICMP 에러 메시지 패킷의 타임스탬프를 이용하여 RTT_{hop2}값을 계산해낸다. 그리고 ICMP 에러 메시지를 전송한 두 기지국 사이의 RTT값 t를 구한다. 측정 알고리즘을 통해 구한 t값을 K-NN분류기(K-Nearest Neighbor Classifier)를 이용하여 일반 유, 무선망을 사용하는 AP와 이동통신망을 사용하는 로그 AP로 분류하였다. 이 기법은 무선 채널 사용량(channel utilization)이 증가하더라도 100%의 높은 탐지율을 보였지만, 로그 AP가 TTL 값이 2인 ICMP 메시지를 받으면 이 패킷을 다음 홉에 전송하지 않고 직접 ICMP 에러 메시지를 전송하면 무력화될 수 있다는 단점이 존재한다.

〔표 1〕 알고리즘에서 사용되는 변수

변수	의미
RTT_{probe}	ICMP 패킷을 사용하여 사용자와 사용자가 접속한 AP까지의 Round Trip Time을 1회 측정한 값.
RTT_{dns}	DNS 패킷을 사용하여 사용자와 사용자가 접속한 AP까지의 거리를 포함하며 사용자가 접속한 AP와 DNS까지의 거리도 포함한 Round Trip Time을 1회 측정한 값.
$\overline{RTTprobe}$	측정한 RTT_{probe} 값 200개 중 상위 40개를 제외한 160개의 평균값.
$\overline{RTTdns}$	측정한 RTT_{dns} 값 200개 중 상위 40개를 제외한 160개의 평균값.
σ_{probe}	측정한 RTT_{probe} 값 200개 중 상위 40개를 제외한 160개의 표준편차값.
σ_{dns}	측정한 RTT_{dns} 값 200개 중 상위 40개를 제외한 160개의 표준편차값.
$\triangle t$	$\triangle t = \overline{RTTdns} - \overline{RTTprobe}$
δ	$\delta = \sigma_{probe} + \sigma_{dns}$

2.3 SVM 개요

SVM은 기본적으로 2개의 범주를 구분하는데 특화된 분류기이다. 로그 AP와 정상적인 AP의 각 데이터의 특성을 SVM의 요소로 입력하고 나서 SVM을 훈련하면 각 그룹의 가장 근접한 데이터를 보조 벡터(support vector)라고 하여 각 그룹의 보조 벡터간의 거리가 최대가 되는 지점에서 최적 분리 경계면을 설정하고 분리된 집단 사이의 간격(margin)을 최대화시키는 초평면(hyperplane)을 찾는 문제로 바꾸어 분류 문제를 더 쉽게 처리한다. 이렇게 훈련된 SVM 모델을 가지고 사용자가 접속한 AP에 대한 특성을 요소로 SVM 예측을 하게 되면 해당 AP에 대한 데이터가 로그 AP에 속하는 데이터인지 정상적인 AP에 속하는 데이터인지 분류한다.



〔그림 2〕 H.Han등의 기본 아이디어

III. H.Han등의 로그 AP 탐지 기법

3.1 H.Han등의 아이디어

2011년 H. Han등은 로그 AP와 정상적인 AP 사이의 추가적인 무선구간의 지연시간을 이용하여 로그 AP를 찾아내는 기법을 제안하였다[6]. 〔표 1〕에서 본 논문에서 사용되는 수식에 대한 변수 들을 정의 하고 있으며 〔그림 2〕는 H. Han 등이 제안한 기법의 기본 아이디어를 보여주고 있다. 〔그림 2〕에서 정상적인 AP는 정상적인 AP와 DNS 서버 사이의 유선망 구간의 RTT 값이 $\triangle t$이고, 로그 AP는 로그 AP와 정상적인 AP 사이의 추가적인 무선 구간과 정상적인 AP와 DNS 서버 사이의 유선 구간을 모두 포함한 구간의 RTT 값이 $\triangle t$이다. 로그 AP는 정상적인 AP와 무선으로 연결되어 있기 때문에 사용자가 정상적인 AP에 연결한 것과 비교하여 무선 구간이 하나 더 존재한다. 이것은 사용자가 알고 있는 무선구간을 제외한 구간의 RTT 값을 나타내는 $\triangle t$ 값이 정상적인 AP의 $\triangle t$값보다 더 크게 나올 수 있음을 의미한다. H. Han 등은 이러한 $\triangle t$ 값과 측정한 RTT 값의 표준편차 값에 특별한 연관성이 있다고 판단하여 두 값을 기준으로 로그 AP와 정상적인 AP를 분류한다.

3.2 RTT측정 방법

사용자로부터 사용자가 접속해있는 AP까지의 RTT_{probe}를 측정하는 방법에서 로그 AP가 대신하여 응답한다는 것은 의미가 없으므로 로그 AP이거나 정상적인 AP이거나 상관없이 즉각 응답을 받으면 되기 때문에 ICMP request-response패킷을 이용하여 시간을 측정한다. RTT_{dns}의 측정으로 DNS 패킷을 사용하는 이유는 ICMP 패킷이나 SYN ACK 패킷은 로그 AP가 대신하여 응답하게 되면 간단하게 회피할 수 있으므로 DNS 질의를 바꿔가며 RTT_{dns}를 측정하게 하여 로그 AP가 대신하여 응답하면 해당 DNS 질의에 대한 제대로 된 응답을 하지 못하므로 간단하게 회피할 수가 없기 때문이다.

***Algorithm* 1.** $RTTRecord$
1. $Connect$ and $associate$ with AP
2. **for** $i = 1$ to 200 ***do***
3. Send unicast $ICMPrequest$ to AP
   Record round trip time $RTTprobe$
4. Send $DNSquery$ to Local DNS server
   Record round trip time $RTTdns$
5. ***end*** **for**
6. Except the top 20% abnormal RTT value
7. $\overline{RTTprobe}$ = Average of remaining $RTTprobe$
8. $\overline{RTTdns}$ = Average of remaining $RTTdns$
9. σ_{probe} = Standard deviation of remaining $RTTprobe$
10. σ_{dns} = Standard deviation of remaining $RTTdns$
11. $\triangle T = \overline{RTTdns} - \overline{RTTprobe}$
12. $\delta = (\sigma_{probe} + \sigma_{dns})/2$
13. **if** $data-set$ is a $training-set$ ***then***
14. Insert ($\triangle T$, δ) into SVM $training-set$ as Factor
15. ***else*** **if** $data-set$ is a $predict-set$ ***then***
16. Insert ($\triangle T$, δ) into SVM $predict-set$ as Factor
17. ***end*** **if**

〔그림 3〕 SVM을 이용한 로그 AP 탐지 기법 알고리즘

3.3 H. Han등의 알고리즘

H. Han 등의 논문에서는 사용자와 사용자가 연결된 AP까지의 구간의 RTT값을 측정한 RTT_{probe}와 사용자와 Local DNS까지의 RTT를 측정한 RTT_{dns}값을 이용하여 구한 $\triangle t = (\ RTT_{dns} - RTT_{probe})$값을 이용하여 로그 AP를 분류한다. 즉, 추가적인 무선구간에 대한 지연시간을 이용하여 로그 AP를 탐지한다.

이 기법에서 제안한 로그 AP 탐지 알고리즘은 다음과 같다. 사용자는 AP에 n개의 ICMP 패킷과 n개의 DNS 패킷을 전송하여 RTT_{probe}와 RTT_{dns}를 구한다. 비정상적으로 수치가 높은 상위 20%를 제외하고 하위 80%의 데이터만을 가지고 RTT_{probe}와 RTT_{dns}의 평균을 구하여 사용자가 연결된 AP와 DNS 서버 사이의 추가적인 무선구간에 대한 RTT 평균값인 $\triangle t = (RTT_{dns} - RTT_{probe})$값을 구하고 RTT_{probe}와 RTT_{dns}의 표준편차를 구하여 σ_{probe}(RTT_{probe}의 표준편차)와 σ_{dns}(RTT_{dns}의 표준편차)를 구한 다음 $(\sigma_{probe} + \sigma_{dns})/2$값을 x축의 값으로, $\triangle t$ 값을 y축의 값으로 갖는 2차원 그래프를 그린다. 그리고 σ_{probe}와 σ_{dns}를 이용하여 직선의 방정식 $\alpha * (\sigma_{probe} + \sigma_{dns})/2 + \beta (\alpha = 0.49,\ \beta = 1.3)$ 으로 직선을 그림으로써 로그 AP와 정상적인 AP를 분류한다. 2차원 그래프 상에서 직선보다 위쪽에 있는 AP의 집합을 전부 로그 AP로 판단한다.

3.4 H.Han등이 제안한 기법에 대한 고찰

해당 기법에서 제안한 알고리즘에서 RTT_{probe}와 RTT_{dns}를 측정하는 시간이 동기화되어 있지 않을 수 있어 실제로는 DNS까지의 RTT에서 AP까지의 RTT를 정확하게 빼야 하지만 두 개의 RTT 값을 측정하기 위해 패킷을 동시에 내보내는 것이 어려웠을 수 있다. 또 로그 AP 그룹과 정상적인 AP 그룹을 분류하는 직선의 방정식을 구하는 데 있어서 사용되는 $\alpha = 0.49$, $\beta = 1.3$ 이라는 고정된 상수보다 실제 상황에 따라서 분류방법이 동적으로 변하면서 두 그룹을 분류하는 최적화된 방법이 필요하다. 따라서 우리는 이러한 RTT_{probe}와 RTT_{dns}를 보내는 시간을 최대한 동기화 하여 같은 네트워크상황에서의 시간을 측정하도록 하고 두 그룹을 분류하는 것은 두 그룹을 분류하는데 특화된 SVM을 이용하여 분류하려고 한다.

IV. SVM을 이용한 로그 AP 탐지 기법

4.1 탐지 기법 소개

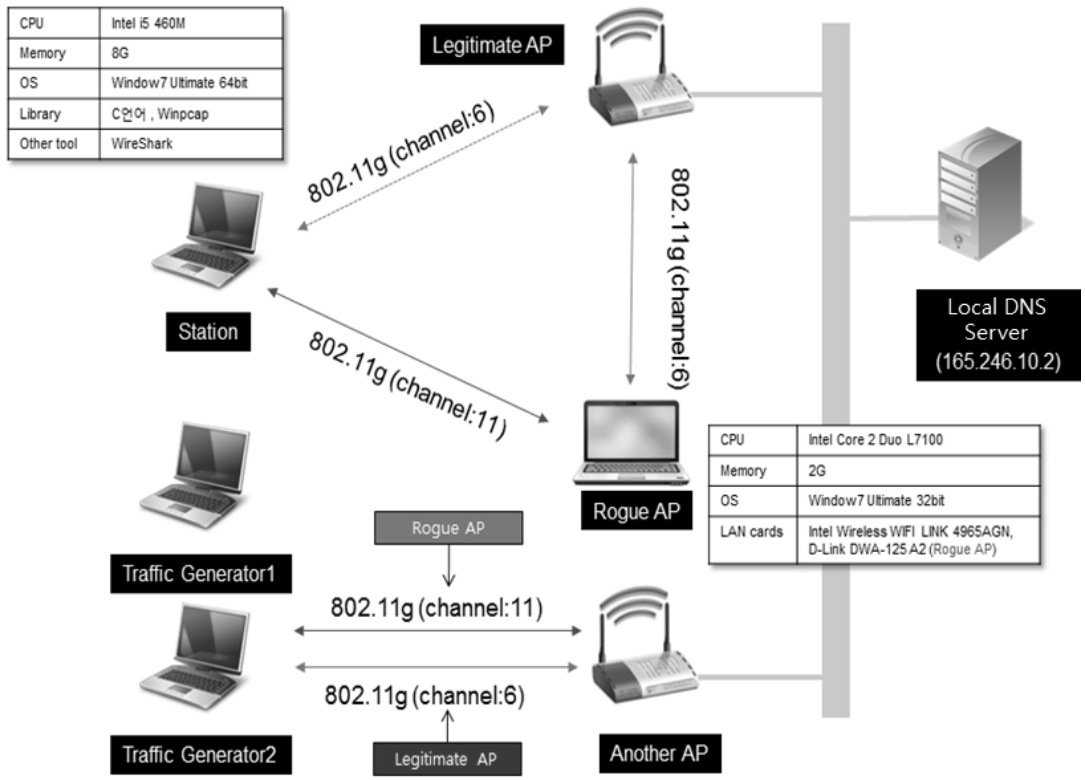
H. Han 등의 논문에서는 로그 AP와 정상적인 AP 사이의 추가적인 무선구간에 대한 지연시간이 포함된 $\triangle t$와 RTT 측정값의 표준편차인 $(\sigma_{probe} + \sigma_{dns})/2$값 사이의 연관성을 보고 특정한 직선의 방정식 $\alpha * (\sigma_{probe} + \sigma_{dns})/2 + \beta$으로 로그 AP와 정상적인 AP를 분류하였으나 우리는 두 값 사이의 연관성을 단순히 직선으로 분류하기보다는 좀 더 두 그룹을 확실히 분류해내는 방법이 필요했다. 따라서 우리는 로그 AP와 정상적인 AP를 분류하는 데 있어서 두 개의 범주를 분류하는데 특화된 분류기인 SVM을 사용하기로 하였다. 따라서 본 논문에서는 기존논문에서 사용하고 있는 두 값 사이에 연관성이 있다고 판단되는 $\triangle t$와 $(\sigma_{probe} + \sigma_{dns})/2$값에 대한 상관관계에 대하여 SVM을 이용하여 훈련하고 두 그룹을 분류하게 한다.

4.2 RTT측정 및 SVM 훈련

〔그림 3〕 알고리즘 1. 에서처럼 사용자는 이용하고자 하는 AP에 연결하고 AP까지 RTT 값인 RTT_{probe} 값과 DNS 서버까지 RTT 값인 RTT_{dns} 값을 200번 측정하도록 한 다음 측정한 200개의 RTT 값에서 비정상적으로 값이 큰 경우가 있으므로 상위 RTT 값 20%, 즉 40개의 큰 값을 제거한다. 비정상적인 값을 제거한 나머지 160개의 RTT값 을 가지고 RTT_{probe}와 RTT_{dns} 값의 평균인 $\overline{RTTprobe}$, $\overline{RTTdns}$를 구하고 각각의 표준편차를 구하여 σ_{probe}, σ_{dns}라고 한다. RTT 값의 평균을 이용하여 추가적인 무선구간에 대한 지연시간인 $\triangle t$를 구하고 σ_{probe}, σ_{dns}를 더한 값의 절반을 δ 라고 하여 표준편차를 구한다. 측정하여 구한 두 개의 값을 SVM의 훈련용으로 사용하려면 훈련용 데이터 집합의 요소로 넣게 되며 이미 충분히 SVM을 훈련한 후에 SVM을 이용하여 로그 AP의 여부를 판단하고 싶다면 데이터를 예측 집합의 요소로 넣어서 SVM 예측을 하게 하면 된다.

4.3 SVM 예측

SVM을 훈련할 데이터를 충분히 수집하여 SVM을 훈련하였다면 SVM 모델파일을 얻을 수 있다. 이 모



〔그림 4〕 실험 환경

델파일로 사용자는 사용자가 접속한 AP에서 알고리즘 1.을 이용하여 RTT 값을 측정하여 구한값 $\triangle t$, δ를 예측 집합의 요소로 넣어 SVM 예측을 하면 로그 AP인지 정상적인 AP 인지 분류할 수 있다.

V. 실험 환경

5.1 실험 구조

로그 AP와 정상적인 AP에 접속하는 두 가지 상황을 만들기 위하여 〔그림 4〕와 같은 실험환경을 구성하였다. 무선전송방식은 802.11g 방식으로 대역폭은 54Mbps로 통일되어 있으며 무선채널은 11번과 6번을 사용하게 된다. 로그 AP와 정상적인 AP 사이의 추가적인 무선구간이 혼잡하게 되면 로그 AP를 탐지해내기 더욱 쉬워지므로 로그 AP는 채널상태가 최적인 정상적인 AP에 연결할 것이라는 가정을 하며 사용자와 사용자가 접속한 AP 구간이 혼잡한 상황을 가정한다. 로그 AP는 사용자에게 최적의 채널상황을 제공해 줄 것이지만 사용자가 AP에 연결한 이후에 사용자와 사용자가 접속한 AP 구간 사이에 무선망 상황이 혼잡해지면 RTT 값에 대한 지연시간이 추가적인 무선구간에 대한 지연시간이 아닌 혼잡상황 때문에 발생한 지연시간이므로 로그 AP를 정상적인 AP로 분류하거나 정상적인 AP를 로그 AP로 분류하는 탐지오류가 발생할 수 있다. 그래서 사용자와 사용자가 접속한 AP 구간 사이의 채널만을 혼잡하게 하려고 또 다른 AP를 사용한다. 채널을 혼잡하게 하려고 사용자가 접속한 AP에 패킷을 전송하게 되면 해당 AP의 업무량 증가로 의도하지 않은 큐잉 지연(Queueing Delay)이 발생하여 RTT 값이 증가하게 되므로 정상적인 AP를 로그 AP로 탐지하게 되는 탐지오류가 발생할 수 있기 때문에 채널 혼잡을 만들기 위한 패킷은 또 다른 AP로 보내도록 한다. 확실한 채널의 혼잡을 발생시키기 위하여 2개의 트래픽 생성기를 사용하여 확실한 채널의 혼잡상황을 만든다. RTT_{dns}를 측정하기 위해 보내는 DNS 패킷은 Local DNS 서버인 교내 DNS 서버를 사용한다. 서브네트워크 내에 DNS까지 거리는 1홉이며 Local DNS까지의 거리는 7홉이다. 기존 논문에서는 서브네트워크 내에 있는 DNS

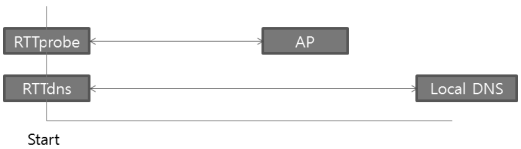
를 사용하였으나 우리는 7홉 거리에 있는 DNS를 사용한다. 이 실험에서 AP의 뒷부분인 추가적인 무선구간에 대한 지연시간 $\triangle t$를 구하는 데 있어서 유선구간이 짧을수록 좋으므로 서브 네트워크 내의 DNS를 쓴다면 로그 AP의 탐지율을 더욱 높일 수 있지만, 대부분의 인터넷을 사용하는 장소에서 서브네트워크 내에 자체적으로 DNS를 가지고 있는 것은 일반적이지 않기 때문에 Local DNS 서버를 사용한다.

5.2 IEEE 802.11g

기존 논문에서는 802.11b와 함께 802.11g 규약에서 제안한 알고리즘을 적용하여 실험하였다고 설명하고 있으나 기존 논문에서 보여주고 있는 채널에서의 대역폭이나 채널사용량 측정에서 사용된 값들 하드웨어 상의 스펙 등으로 보았을 때 802.11g보다는 802.11b에 가까우며 802.11g와 호환하여 사용하기에는 두 통신 규약 사이에 큰 차이가 있다. 무선망 사용이 일반화되고 무선망 기술이 발전하면서 현재는 802.11n 규약이 널리 사용되고 있으며 802.11b는 거의 사용되지 않고 있으며 대부분 802.11g 또는 802.11n을 혼합하여 사용하고 있다. 본 논문에서는 로그 AP로 사용되는 장치의 한계 때문에 인해 802.11g로만 서비스할 수 있었다. 따라서 우리는 802.11g로 통일된 상황에서 실험하며 802.11n으로의 확장성도 갖추고 있다.

5.3 RTT측정

RTT 값을 측정하는 데 있어서 RTT_{probe}는 ICMP 패킷을 이용하여 측정하며 로그 AP이거나 정상적인 AP이거나 상관없이 1구간 안에서의 ICMP 요청과 응답이 이루어지므로 중간에 위조되는 패킷이 있을 수 없고 바로 응답받을 수 있다. 일반적인 AP의 경우 방화벽을 켜놓지 않는다면 ICMP 요청에 응답해준다. RTT_{dns}는 DNS 질의를 해당 네트워크의 Local DNS 서버로 보내게 된다. 우리는 교내 DNS 서버로 DNS 질의를 전송한다. ICMP 패킷과 DNS 패킷은 Rawpacket으로 만들어 Winpcap을 이용해 전송하면 중간단계의 프로토콜을 거치지 않게 되므로 시간을 줄일 수 있으며 시간측정 단위는 마이크로초로 측정되어 매우 정확한 시간을 측정할 수 있다. 〔그림 5〕에서처럼 RTT_{probe}와 RTT_{dns}을 측정 시작하는 시간을 완전히 동기화하여 같은 채널상황에서의 RTT를 측정한다.



〔그림 5〕 RTT측정 시간

5.4 트래픽 제어

RTT 값의 측정은 현재 채널의 사용량, 즉 현재 채널의 혼잡 정도에 따라 측정값의 변동폭이 크게 변하게 된다. 채널이 유휴상태일 때에는 RTT 값의 변동폭이 크지 않지만, 채널이 혼잡한 상황일 때에는 변동폭이 크게 되어 측정한 RTT 값에 대한 신뢰도가 떨어지게 된다. 기존 논문에서 이러한 혼잡의 척도로 채널사용량을 측정하였으며 채널사용량이 많아지면 채널사용량이 적을 때보다 로그 AP의 탐지율이 현저하게 떨어짐을 볼 수 있었다. 기존 논문에서 유휴상태일 때 거의 100%에 가까운 탐지율을 보여주지만, 혼잡상태일 때는 RTT 값을 측정하는 샘플링의 횟수를 기본 100회에서 300회까지 늘려야만 80%의 탐지율을 보여주고 있다. 우리는 채널이 유휴상태일 때뿐만 아니라 채널사용량이 많을 때에도 샘플링의 횟수를 늘리지 않고 로그 AP 탐지율을 크게 떨어지지 않는 90% 정도의 탐지율을 보여준다. 채널의 혼잡제어를 위하여 UDP 패킷을 또 다른 AP로 보낸다. UDP 데이터(1401byte) + Ethernet header(14byte) + IP header(20byte) + UDP header (8byte)= 1443byte 의 패킷을 초당 1000개 정도 보내면 초당 11544Kbit=11.5Mbit 정도의 혼잡을 발생시킬 수 있다. 이더넷 헤더는 네트워크카드에서 자동으로 802.11 MAC 헤더로 변경되어 전송된다. 채널에서 혼잡제어와 흐름제어가 이루어지므로 채널의 혼잡을 위한 패킷의 개수는 의도한 대로 모두 전송할 수는 없다. 이러한 UDP 패킷을 트래픽생성기를 이용하여 또 다른 AP에 유니캐스트로 패킷의 개수를 조절하면서 보내게 되면 해당 채널의 사용량을 대략적으로 조절할 수 있다.

VI. 실험 결과

6.1 실험 결과값 분석

6.1.1 RTT값의 측정값 분석

〔그림 6〕은 측정한 RTT 값들에 대해서 누적분포 함수를 그린 것이다. 〔그림 6〕의 위쪽 그래프에서는 정상적인 AP에서의 RTT_{probe} 값과 RTT_{dns} 값 모두 2000마이크로초 이하의 측정값이 80% 정도이며 두 값의 차이는 크게 없어 보인다. 그림 6의 아래 그래프에서는 로그 AP에서의 RTT_{probe} 값은 5000마이크로초 이내에 측정값이 95% 정도이며 RTT_{dns} 값은 4000마이크로초에서 14000마이크로초까지 측정값이 90% 정도이며 고르게 분포하고 있음을 알 수 있다. RTT_{probe} 값과 RTT_{dns} 값 사이의 차이가 확연하게 나고 있음을 알 수 있다.

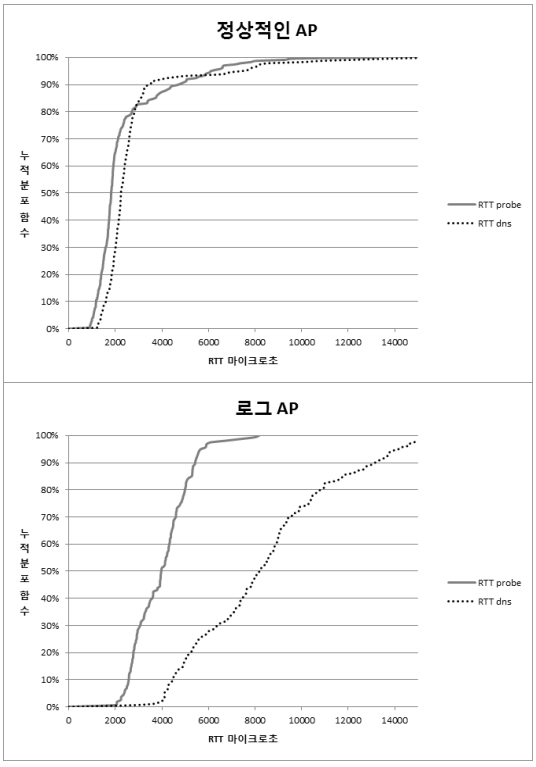
6.1.2 RTT 값의 표준편차 분석

〔그림 7〕은 측정한 RTT 값들에 대한 표준편차에 대해서 누적분포함수를 그린 것이다. 〔그림 7〕 위 의 그래프는 정상적인 AP에서의 RTT_{probe} 값과RTT_{dns} 값의 표준편차이다 두 표준편차 모두 90% 정도의 값이 2000마이크로초 이내에 있는 것을 확인할 수 있다. 〔그림 7〕아래의 그래프는 로그 AP에서의 RTT_{probe} 값과 RTT_{dns} 값의 표준편차이다. RTT_{probe} 값의 표준편차는 90% 정도의 값이 4000마이크로초 이내에 있는 것을 확인할 수 있고 RTT_{dns} 값의 표준편차는 2000마이크로초에서 8000마이크로초까지 값이 90% 정도를 이루며 고르게 분포함을 알 수 있다. RTT_{probe} 값의 표준편차와 RTT_{dns} 값의 표준편차도 RTT 값의 차이와 마찬가지로 두 값에 차이가 있다.

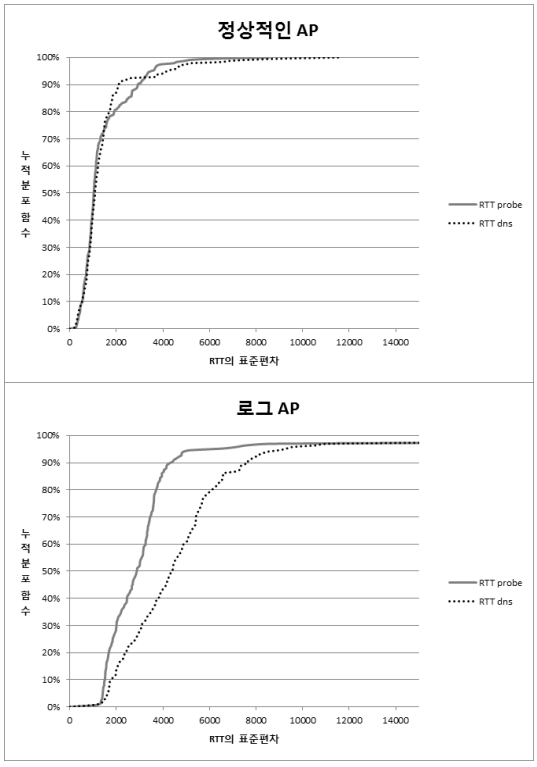
6.2 H.Han 등 과 SVM을 이용한 로그 AP탐지 결과 비교

6.2.1 전체 데이터 분포도

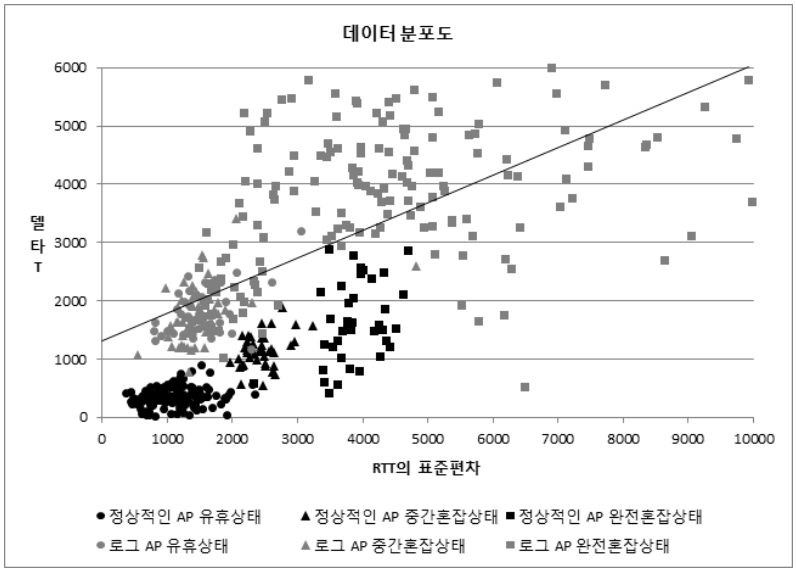
〔그림 8〕은 전체 실험한 자료들의 $\triangle t$ 값과 표준편차를 가지고 로그 AP와 정상적인 AP의 분포도를 보여주고 있다. 동그라미의 데이터들은 채널의 상황이



〔그림 6〕 RTT값의 누적 분포 함수



〔그림 7〕 RTT의 표준편차의 누적 분포 함수

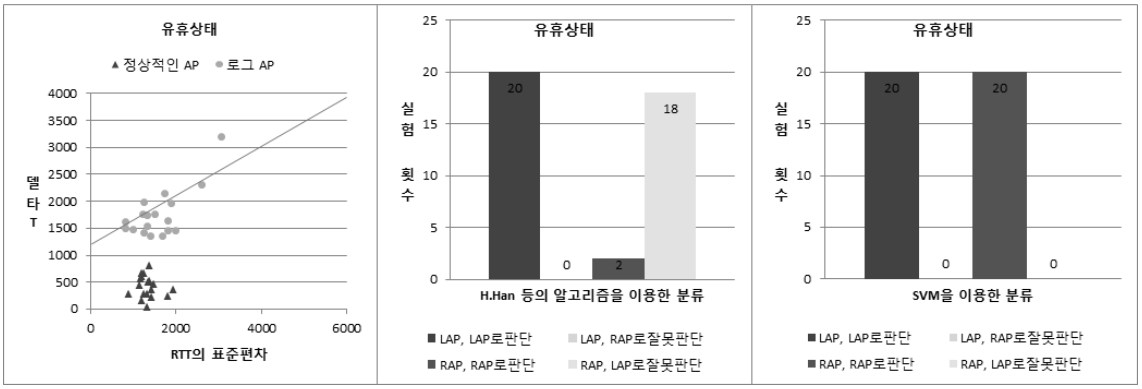


〔그림 8〕 전체 데이터 분포도

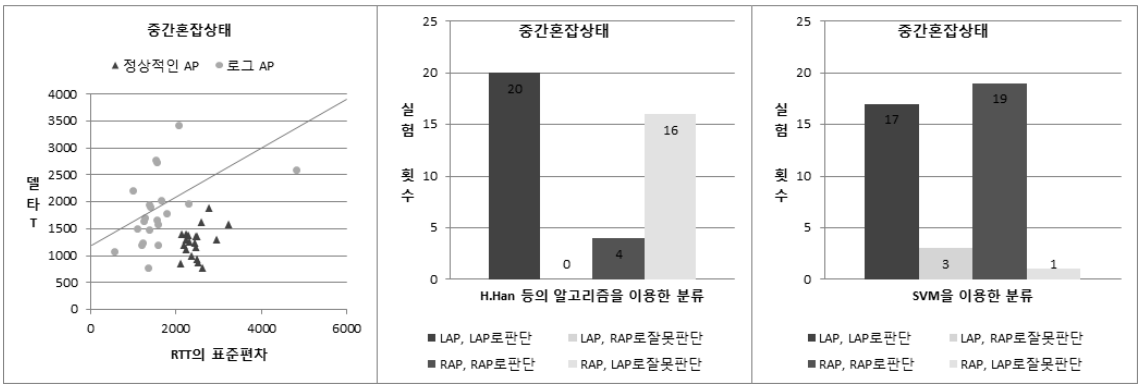
유휴상태일 때의 데이터이고 삼각형의 데이터들은 채널상황이 중간혼잡상황일 때의 데이터이고 사각형의 데이터들은 채널이 완전혼잡상황일 때의 데이터이다. 〔그림 8〕을 보면 채널의 혼잡상황에 따라 두 그룹의 데이터의 분포도가 달라지며 일정한 규칙이 있는 것이 아니므로 H. Han 등의 알고리즘처럼 단순한 직선으로 두 그룹을 분류하는 것에는 한계가 있다. 현재 사용자가 처한 상황에 따라 동적으로 바뀌는 분류기준이 필요하다. 실제로 H. Han 등의 알고리즘을 적용한 직선의 방정식은 모든 정상적인 AP가 직선의 방정식 아래에 있으므로 정상적인 AP로 분류하게 된다. 대부분의 로그 AP를 정상적인 AP로 분류하게 되는 탐지오류가 발생하여 더 최적화된 직선의 방정식이 필요하다. H. Han등의 알고리즘은 802.11b 환경에 최적화되어 있기 때문에 802.11g 에서 실험한 우리의 데이터에 제대로 적용되지 않았음을 보여준다. H. Han의 알고리즘을 이용하여 새로운 직선의 방정식을 구하여 두 그룹을 분류하여도 채널이 혼잡한 상황에서는 단순한 직선으로는 두 그룹을 분류하기 어렵다. 또한, 두 그룹을 분류하는 최적의 직선을 구하는 방법은 기존 논문에서 언급하고 있지 않으므로 우리 임의대로 새로운 직선의 방정식을 구하여 두 그룹을 분류하는 것은 본 논문의 목적을 벗어난다. 만약 두 그룹을 분류하는 최적인 직선의 방정식을 새로 구하여 분류하더라도 채널의 혼잡 상황이 유휴상태, 중간혼잡상태일 때에는 SVM을 이용한 로그 AP 탐지 기법과 탐지율 측면에서 크게 차이가 없지만, 채널 혼잡상태일 때에는 기존 논문의 탐지율이 크게 떨어진다. 본 논문의 목적은 혼잡상황에서도 로그 AP의 탐지율이 크게 떨어지지 않는 것이므로 H. Han등의 직선의 방정식을 새로 구하지 않아도 채널 혼잡상태에서 SVM을 이용한 로그 AP의 탐지결과만으로도 본 논문에서 제시하는 로그 AP 탐지 기법의 우수성을 알 수 있다. SVM을 이용하여 두 그룹을 분류하게 되면 두 그룹의 최적 분리 경계면을 설정하여 두 그룹을 분류하게 되므로 두 그룹의 분류가 성공적으로 이루어지며 사용자의 상황에 따라 탐지기준이 동적으로 변하게 되며 채널이 혼잡한 상황에서도 90% 정도의 탐지율을 보여준다.

6.2.2 채널 유휴상태에서의 탐지 결과 비교

유휴상태일 때 측정한 로그 AP와 정상적인 AP 각각의 데이터 60개는 SVM의 훈련용으로 사용되었으며 각각 20개의 데이터를 예측용으로 사용하였다. H. Han 등의 알고리즘을 적용한 결과 단 2개의 로그 AP만을 제대로 분류하고 나머지는 정상적인 AP로 분류하여 18개의 탐지오류를 발생시켰다. 〔그림 9〕의 유휴상태에서처럼 H. Han등의 알고리즘을 그대로 사용하는 것보다 직선의 방정식을 Δt값이 1000에서 가로로 X축에 평행한 직선을 긋는다면 두 그룹이 확실히 분류될 것으로 보인다. SVM을 이용한 탐지결과 로그 AP 20개 정상적인 AP 20개를 모두 성공적으로



〔그림 9〕 채널 유휴상태일 때의 로그 AP와 정상적인 AP의 데이터 분포도와 H.Han등의 알고리즘을 적용한 로그 AP 탐지결과와 SVM을 이용한 로그 AP 탐지 결과



〔그림 10〕 채널 중간혼잡상태일 때의 로그 AP와 정상적인 AP의 데이터 분포도와 H.Han등의 알고리즘을 적용한 로그 AP 탐지 결과와 SVM을 이용한 로그 AP 탐지 결과

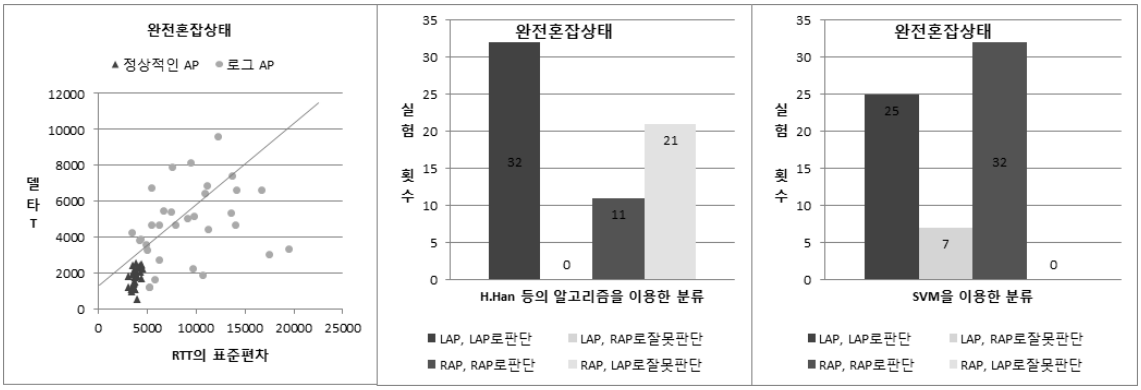
탐지해내는 것을 볼 수 있다.

6.2.3 채널 중간혼잡상태에서의 탐지 결과 비교

중간혼잡상태일 때 측정한 로그 AP와 정상적인 AP 각각의 데이터 40개는 SVM 훈련용으로 사용되었으며 각각 20개의 데이터를 예측용으로 사용하였다. H. Han등의 알고리즘을 적용한 결과 단 4개의 로그 AP만을 제대로 분류하고 나머지는 정상적인 AP로 분류하여 16개의 탐지오류를 발생시켰다. 〔그림 10〕의 중간혼잡상태에서 두 그룹을 분류하는 기준을 다르게 설정한다면 두 그룹은 어느 정도 분류가 가능해 보인다. SVM을 이용한 탐지결과 로그 AP 20개 중 1개를 정상적인 AP로 간주하는 탐지오류가 있었으며, 정상적인 AP 20개 중 3개를 로그 AP로 탐지하는 탐지오류가 있었다.

6.2.4 채널 완전혼잡상태에서의 탐지 결과 비교

완전혼잡상태일 때 측정한 로그 AP와 정상적인 AP 각각의 데이터 50개는 SVM 훈련용으로 사용되었으며 SVM 훈련용으로 사용되었으며 완전혼잡상태일 때의 탐지율이 중요하므로 예측 결과의 신뢰도를 높이기 위해 예측용의 개수를 늘려 각각 32개의 데이터를 예측용으로 사용하였다. H. Han 등의 알고리즘을 적용한 결과 11개의 로그 AP는 로그 AP로 제대로 분류하고 나머지는 정상적인 AP로 분류하여 21개의 탐지오류를 발생시켰다. 채널이 혼잡한 상황에서는 로그 AP와 정상적인 AP간의 분류가 단순한 직선으로는 힘들어 보이지만 〔그림 11〕의 완전혼잡상태에서처럼 분포도를 보게 되면 두 그룹 간에 분류는 가능해 보인다. SVM을 이용한 탐지결과 모든 로그 AP는 로그 AP로 성공적으로 분류해내었으며 7개의 정상적인



〔그림 11〕 채널 완전혼잡상태일 때의 로그 AP와 정상적인 AP의 데이터 분포도와 H.Han등의 알고리즘을 적용한 로그 AP 탐지 결과와 SVM을 이용한 로그 AP 탐지 결과

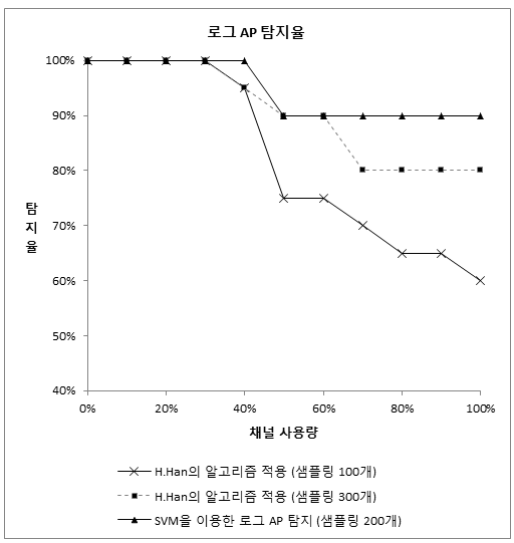
AP를 로그 AP로 분류해내는 탐지오류가 있었다.

6.2.5 탐지율 비교

현재 채널의 혼잡 상황은 혼잡한 환경을 만들기 위해 실험에서 인위적으로 조성한 환경이므로 사용자는 실제 SVM을 이용한 로그 AP를 탐지할 때에 이러한 채널 혼잡 상황에 대한 정보를 얻어 로그 AP 탐지에 이용할 수는 없다. 따라서 SVM을 훈련할 때에는 채널의 혼잡 상황과 관계없이 전체 데이터로 훈련하며. SVM 예측할 때에도 채널의 혼잡 상황을 알지 못하며 $\triangle t$ 값과 δ 값만을 SVM의 요소로 적용하여 탐지한다. 본 논문의 실험 결과는 기존 H. Han등의 알고리즘에 적절하게 적용되지 않아 탐지오류가 많으므로 탐지율 비교는 기존 논문에서 탐지율이 최적인 직선의 방정식을 도출했을 때의 탐지율과 비교한다. H. Han 등의 알고리즘에서 기존의 탐지율은 데이터의 샘플링의 개수가 100개일 경우에 유휴상태일 때에 100%이며 중간혼잡상태일 때 70%~90% 정도의 탐지율을 보이고 완전혼잡상태일 때에는 50%~60% 정도의 탐지율을 보여준다고 말하고 있다. 데이터의 샘플링의 개수가 300개일 경우에 유휴상태일 때에 100%, 중간혼잡상태일 때 90%, 완전혼잡상태일 때에 80% 정도의 탐지율을 보여준다고 한다. 실험결과에서 보듯이 H. Han등의 알고리즘은 로그 AP 탐지기준이 사용자의 환경에 따라 동적으로 변하는 것이 아닌 고정적인 기준이기 때문에 탐지율이 떨어질 수 있음을 보여준다. 실제로 기존 논문의 알고리즘을 실험자료에 적용해 보면 탐지율이 떨어짐을 볼 수 있다. 이것은 H. Han등의 알고리즘의 분류 방법이 802.11b에서 최적화되어있기 때문에 802.11g에서 실험한 우리의 실험결과에 잘 맞지 않는 것이다. SVM을 이용한 탐지율은 유휴상태일 때에 100% 탐지율을 보이며 중간혼잡상태일 때 90% 정도의 탐지율을 보이고 있다. 완전혼잡상태일 때에도 탐지율이 크게 떨어지지 않은 90% 정도를 유지하고 있는 것이 SVM을 이용한 로그 AP 탐지 기법의 최대 장점이다.

VII. 결 론

로그 AP 탐지 기법 중 H. Han등이 제안한 기법의 구현과 분석을 통해 해당 기법에서 로그 AP와 정



〔그림 12〕 H. Han등의 알고리즘 적용 탐지 결과와 SVM을 이용한 로그 AP 탐지 결과의 탐지율 비교

상적인 AP를 분류하는데 사용되는 알고리즘이 실용적이지 못함을 발견하였다. 이러한 문제를 해결하기 위해 이 연구에서는 SVM을 이용한 로그 AP 탐지기법을 개발하였다. 기존 논문의 기법은 두 그룹을 분류하는 것이 직선의 방정식이기 때문에 혼잡 상황에서의 탐지율이 크게 떨어지는 문제가 있었다. 두 그룹의 분류 방법을 SVM을 이용함으로써 사용자의 상황에 따라 분류 기준을 동적으로 설정하며 혼잡 상황에서도 탐지율이 크게 떨어지지 않도록 하였다. 기존의 기법은 채널 혼잡상황일 때 샘플링 n의 개수를 늘림으로써 탐지율을 80%까지 높일 수 있음을 보이고 있지만, 본 논문에서 제안한 바와 같이 SVM을 활용하여 두 그룹을 분류하면 채널사용량에 관계없이 약 90%의 탐지율을 보여주었다. 이 연구의 목적은 기존의 기법의 문제점을 발견하는 것이 아닌, 로그 AP를 효율적으로 탐지할 수 있는 향상된 기술을 개발하는 것이다. 앞으로 심층적인 분석을 통해 로그 AP를 식별하는데 유용하게 사용될 수 있는 정보들을 도출하고 이를 SVM의 입력 요소로 적용하여, 기존의 H. Han 등이 제시한 분류기준을 그대로 적용하지 않고 새로운 요소들로 분류를 시도함으로써 무선채널의 사용량이 많은 환경에서도 90% 이상의 탐지율을 보이는 기법으로 발전시킬 것이다.

참고문헌

[1] P. Bahl, R. Chandra, J. Padhye, L.Ravindranath, M. Singh, A. Wolman and B. Zill, "Enhancing the security of corporate Wi-Fi networks using DAIR," MobiSys, pp. 1-14, Jun. 2006.

[2] D. Schweitzer, W. Brown and J. Boleng, "Using visualization to locate rogue access points," Journal of Computing Sciences in Colleges, vol. 23, no. 1, pp. 134-140, Oct. 2007.

[3] L. Watkins, R. Beyah, and C. Corbeet, "a passive approach to rogue access point detection," IEEE Global Telecommunications Conference, pp. 355-360, Nov. 2007.

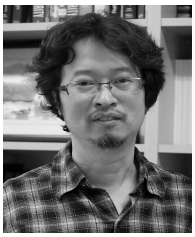
[4] W. Wei, K. Suh, B. Wang, Y. Gu and J. Kurose, "Passive Online Rogue Access Point Detection Using Sequential Hypothesis Testing with TCP ACK-Pairs," The 7th ACM internet measurement conference, pp. 365-378, Oct. 2007.

[5] 김이룩, 조재익, 손태식, 문종섭, "3G망을 사용하는 인가되지 않은 AP 탐지 방법," 정보보호학회논문지, 22(2), pp. 259-266, 2012년 4월.

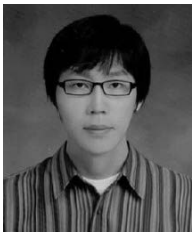
[6] H. Han, B. Sheng, C.C. Tan, Q. Li and S. Lu, "A Timing-Based Scheme for rogue AP Detection," IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 11, pp. 1912-1925, Nov. 2011.

〈저 자 소 개〉

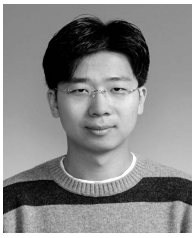
강 성 배 (Sung-bae Kang) 학생회원
2012년 2월: 인하대학교 컴퓨터 공학과 졸업
2013년 3월~현재: 인하대학교 컴퓨터 공학과 석사 과정
〈관심분야〉 정보보호, 무선 인터넷 보안, 네트워크 보안



양 대 헌 (Dae-hun Nyang) 정회원
1994년 2월: 한국과학기술원 과학기술 대학 전기 및 전자 공학과 졸업
1996년 2월: 연세대학교 컴퓨터 과학과 석사
2000년 8월: 연세대학교 컴퓨터 과학과 박사
2000년 9월~2003년 2월: 한국전자통신연구원 정보보호연구본부 선임연구원
2003년 2월~현재: 인하대학교 컴퓨터정보공학부 부교수
〈관심분야〉 암호 이론, 암호 프로토콜, 인증 프로토콜, 무선 인터넷 보안



최 진 춘 (Jin-chun Choi) 학생회원
2011년 2월: 인하대학교 컴퓨터공학과 졸업
2011년 3월~현재: 인하대학교 정보공학과 석사 과정
〈관심분야〉 네트워크 보안, WSN 보안



이 석 준 (Sok-joon Lee) 정회원
1998년 2월: 서울대학교 컴퓨터공학과 졸업
2000년 2월: 서울대학교 컴퓨터공학과 석사
2000년 2월~현재: ETRI 사이버보안연구단 선임연구원
2010년 9월~현재: KAIST 전산학과 박사과정
〈관심분야〉 무선랜 보안, 인증 프로토콜, 암호 이론