논문 15-40-03-15 The Journal of Korean Institute of Communications and Information Sciences '15-03 Vol.40 No.03
http://dx.doi.org/10.7840/kics.2015.40.3.551

비인증 AP의 하드웨어 성능에 따른 시간 측정 기반의 비인증 AP 탐색 기법의 분석

장 룡 호◆, 강 전 일*, 양 대 헌**, 이 경 희°

Analysis of Time-Based Unauthorized AP Detection Methods According to Hardware Performance of Unauthorized AP

Rhong-Ho Jang◆, Jeon-Il Kang*, Dae-Hun Nyang**, Kyung-Hee Lee°

요 약

Wi-Fi 및 핫스팟의 사용이 많아짐에 따라, 최근 비인증 AP는 현대사회에 있어서 중요한 보안문제가 되어가고 있다. 그에 따라 2010년대 초반 비인증 AP를 탐지하는 연구가 꾸준히 이루어지고 있다. 특히나 무선 네트워크 자원을 이용하는 비인증 AP를 탐지하는 다양한 기법들이 제시되었다. 현재 많은 연구들에서 비인증 AP를 찾아내는 방식은 추가된 무선구간으로 인한 지연된 시간(평균이나 표준편차)을 이용하는 방식을 사용되고 있다. 그러나 앞선 대부분의 연구에서 비인증 AP는 노트북에 무선랜카드를 추가하여 구성되는데, 지연된 시간의 원인이 운영체제에 의한 소프트웨어 방식의 네트워크 공유에 있을 수 있음을 고려하지 않고 있다. 이 논문에서는 기존의 시간 측정 기반 비인증 AP 탐지 기법들이 고성능 하드웨어를 이용하여 구성된 비인증 AP를 효율적으로 분류해내지 못함을 보이려고 한다.

Key Words : evil-twin, unauthorized AP detection, high-performance unauthorized AP, wireless LAN, time-delay

ABSTRACT

As more people use Wi-Fi and hotspot, unauthorized APs become one of big security problems in modern society. From the beginning of 2010, researchers study about unauthorized AP continually and contributed a lot of methods of detecting unauthorized AP that use wireless resources. Many researches about unauthorized AP detection use time-delay measurement (e.g., average or standard deviation) which is caused by additional wireless connection. In the most previous researches, however, the unauthorized APs consist of laptop and pulg-in Wi-Fi adaptor, and researchers did not concern about time-delay caused by software network sharing. In this paper, we show that existing unauthorized AP detection scheme that can not efficiently classify the high performance unauthorized AP.

※ 이 논문은 2014년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임(NRF-2014R1A1A2059852)
◆ First Author : Inha University Computer Science Engineering, ziyoo521@naver.com, 학생회원
° Corresponding Author : The University of Suwon Electrical Engineering, khlee@suwon.ac.kr, 정회원
* Inha University Computer Science Engineering, dreamx@isrl.kr
** Inha University Computer Science Engineering, nyang@inha.ac.kr, 정회원
논문번호 : KICS2015-03-042, Received March 2, 2015; Revised March 17, 2015; Accepted March 17, 2015

Ⅰ. 서 론

비인증(unauthorized) AP는 유·무선 네트워크 자원을 이용하여 네트워크 관리자가 설치한 정상 AP처럼 사용자에게 인터넷 서비스를 제공하는 과정에서 중간자(man-in-the-middle) 공격을 수행하는 장치를 의미한다. 유선 네트워크 자원을 이용하는 비인증 AP 공격은 공공장소 혹은 기업내부의 유선 네트워크 자원과 IP를 확보한 다음 공격을 수행한다. 무선 네트워크 자원을 이용하는 비인증 AP 공격은 공공장소 혹은 기업내부에 설치된 정상 AP의 자원을 이용하여 공격을 수행한다. 공공장소 혹은 기업내부에서 유선자원 또는 IP를 확보하기가 어렵기 때문에 무선 네트워크 자원을 이용한 비인증 AP 공격이 더 큰 우려가 되고 있다. 특히 현재 공공장소에서 무료로 제공되는 무선 인터넷이 급증하면서 공격자에게 더 많은 공격 기회를 제공하고 있다.

현재 국내·외의 많은 비인증 AP 관련 연구들은 비인증 AP 구성할 때 존재하는 추가적인 무선 구간으로 인한 패킷 지연시간(평균이나, 표준편차)을 이용한다[1-7]. 또한 대다수의 연구에서 실험에 사용한 비인증 AP는 노트북에 무선랜카드를 추가하여 구성하였다. 이러한 경우, 비인증 AP는 소프트웨어 방식으로 네트워크를 공유하는데, CPU 성능에 따라 패킷을 처리하는 것에서 속도 차가 발생할 수 있다. 이러한 이유에서 비인증 AP의 성능도 패킷 지연의 원인으로 고려해야하지만, 이러한 요소는 고려되고 있지 않다.

이 논문에서는 기존의 시간 측정 기반 비인증 AP 탐지 기법들이 고성능을 하드웨어로 구성된 비인증 AP로 인하여 무력화 될 수 있음을 보인다. 2장에서는 기존의 evil-twin 방식을 포함한 비인증 AP 탐지 기법들에 대해서 살펴보고, 비인증 AP를 구성하는 다양한 방법에 대해서 살펴본다. 3장에서는 이 논문에서 중점적으로 분석하려고 하는 시간 지연 측정 방식의 evil-twin 탐지 기법의 예로 H. Han 등의 연구에 대해서 살펴본다. 4장에서는 고성능 하드웨어로 구성된 비인증 AP가 H. Han 등의 방법론에서 어떠한 결과를 보여주는 지 실험을 통해서 검증한다. 5장은 이 논문의 결론을 담고 있다.

Ⅱ. 관련 연구 및 비인증 AP 구성

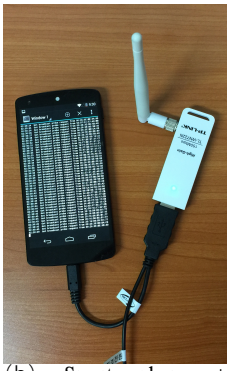
2.1 비인증 AP 탐지 방법론

비인증 AP를 탐지하는 방법은 크게 조사(snooping) 방식과 시간 측정(time measurement) 방식으로 나뉠 수 있다. 조사 방법에서는 추가적인 디바이스와 소프트웨어를 이용하여 AP에 대한 정보(SSID, MAC 주소, RSSI, clock skew 등)를 수집하고, 네트워크 관리자에게 전달되며 사전에 수집된 정상 AP 정보와 비교함으로써 비인증 AP를 찾아낸다. P. Bahl 등은 기업 무선 네트워크를 상대로 모니터링을 하는 프레임워크 DAIR 시스템을 제안하였다[1]. DAIR 시스템은 무선구간의 모든 패킷들을 모니터링하는 Air Monitor, 패킷을 분석하는 Inference Engine 그리고 적법하게 설치된 AP의 정보를 관리하는 데이터베이스로 구성된다. Air Monitor가 무선구간에서 패킷을 캡처하면 Inference Engine에게 전달하고 그 안에 담겨 있는 AP 관련정보를 해독한 다음, 데이터베이스에 저장되어 있는 정보와 비교하여 비인증 AP를 탐지한다. D. Schweitzer 등은 AP의 신호 세기와 위치정보를 이용한 비인증 AP 탐지 기법을 제안하였다[2]. 이 기법에서는 AP의 신호세기를 거리로 전환한 다음 해당 거리에 정상 AP의 설치정보와 비교하여 비인증 AP를 탐지한다. 그러나 evil-twin 방식의 비인증 AP의 경우, 기본적으로 비인증 AP가 MAC 주소 등을 위조하여 보여주기 때문에 이러한 방식들을 쉽게 무력화할 수 있다.

시간 측정 방식은 네트워크 트래픽에서 발생하는 이상적인 시간을 분석하여 비인증 AP를 탐지하는 방식으로, 다양한 방식이 존재한다. R. Beyah 등의 연구에서는 Inter-packet 도착시간과 같은 임시적인 특성을 이용하는 기법을 제시하였다[3]. 이 기법에서는 AP를 유·무선 상에서 설치하는데 발생하는 차이로 TCP/UDP 통신을 이용해 각 패킷이 도착하는 간격을 측정해 비인증 AP를 탐지한다. W. Wei 등도 역시 TCP 통신할 때 ACK을 응답하는 특성을 이용하여 유·무선 상에 차이로 비인증 AP를 탐지하였다[4]. H. Han 등은 Probe request/response와 DNS query의 RTT (round trip time)를 이용하여 안정적인(stable) 네트워크 상황에서 높은 성공률로 비인증 AP를 탐지 할 수 있다고 주장하였다[5]. 강성배 등은 H. Han이 제시한 기법을 바탕으로 직선의 방정식을 이용한 선형 분류 대신 SVM (support vector machine)을 사용함으로써 혼잡한 네트워크 상황에서도 비인증 AP를 찾아낼 수 있음을 보였다[6]. 이재욱 등 또한 k-SVM을 이용하여 비슷한 연구결과를 얻어낼 수 있었다[7].

시간 측정기반 탐지 방식은 사전 데이터가 필요 없고 실시간으로 탐지할 수 있다는 것이 장점이다. 그러나 비인증 AP장치의 성능이 앞으로 더 향상된다면 이


(a) Laptop + USB WiFi Adapter
(a) 노트북 + USB 무선랜카드


(b) Smart phone + OTG + USB WiFi Adapter
(b) 스마트폰 + OTG + USB 무선랜카드

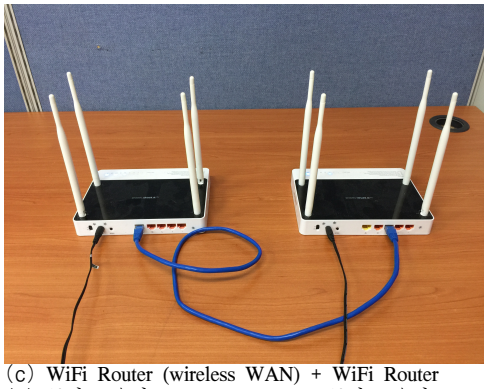

(c) WiFi Router (wireless WAN) + WiFi Router
(c) 무선 공유기 (wireless WAN) + 무선 공유기

그림 1. 비인증 AP를 구성하는 다양한 방법들
Fig. 1. Various methods of configuring unauthorized APs

러한 시간 측정기반 탐지 기법들이 여전히 높은 비인증 AP 탐지 성공률을 보여 줄 수 있을지는 의문으로 남아 있다. 이 논문에서는 이러한 의문으로부터 앞으로 새롭게 등장 가능한 비인증 AP 장치들에 대해서 살펴보고 이들이 기존 시간 측정기반 비인증 AP 탐지 기법들에 어떤 영향을 미칠 수 있는지 실험을 통해 분석하려고 한다.

2.2 비인증 AP를 구성하는 방법

앞선 대부분의 연구에서 비인증 AP는 [그림 1(a)]과 같이 노트북에 USB 무선 랜카드를 추가하여 구성하여 실험에 사용하였다. 윈도우즈 환경에서는 무선 핫스팟 기능과 인터넷 공유 서비스를 이용하여 비인증 AP를 구성할 수 있고, 리눅스 환경에서 Easy-creds를 이용하면 쉽게 비인증 AP를 구성할 수 있다.

오늘날 스마트폰의 하드웨어 성능이 향상되면서 일반적인 비인증 AP보다 휴대성이 더욱 뛰어난 비인증 AP도 생각해볼 수 있다. [그림 1(b)]는 스마트폰을 이용하여 비인증 AP를 구성하는 방법을 보여준다. 2014년 현재 많은 안드로이드에 사용하는 리눅스 커널의 경우 OTG(on-the -go) 케이블을 통한 USB 확장을 지원하지만, 무선 랜카드의 확장은 지원하지 않는다. 추가적인 무선 랜카드를 사용하기 위해서는 커널에 해당 무선 랜카드의 드라이버가 성공적으로 로드되어야만 한다. 때문에 스마트폰을 이용하여 비인증 AP를 구성하기 위해서는 Kali와 같은 커스텀 롬이나 Pwn Pad와 같이 수정된 커널을 가진 스마트 기기가 필요하다.

앞서 제시한 비인증 AP의 공통점은 휴대성이 좋은 반면 패킷을 전달할 때 소프트웨어 방식으로 작동한다는 것이다. 즉, 비인증 AP의 성능은 CPU에 많이 의존할 수밖에 없으며, 이는 곧 패킷 전달의 지연 등의 영향을 나타난다. 비인증 AP를 설치하려고 하는 공격자는 이러한 지연을 줄이기 위해서, 소프트웨어 방식이 아니라 하드웨어 방식을 사용하여 비인증 AP를 구성할 수도 있을 것이다. IEEE 802.11에서 무선 구간을 통해 패킷이 전달되는 시간은 OFDM 심볼 간격과 관련 있는데, 이는 4μs정도로 알려져 있다. 비인증 AP에 패킷 처리를 위한 지연과 버퍼링이 없다면(오류 등을 확인 하지 않고 시그널을 단순 재연하였을 때) 두 무선 구간을 통과 하는데 걸리는 시간은 8μs정도로 생각해볼 수 있다.

그러나 대부분의 비인증 AP 탐지 연구에서는 ms 단위의 지연 측정값이 제시됨을 고려해 보면, 패킷 처리를 위해서 상당한 양의 시간이 소요됨을 유추할 수 있다.

[그림 1(c)]이 하드웨어 방식으로 패킷을 처리 하는 비인증 AP를 구성하는 한 가지 방식을 보여준다. 두 개의 무선 공유기를 준비 한 뒤, 하나는 무선 연결을 유선 연결로 바꿔주도록 무선 WAN 기능을 사용하고 (정상 AP에 접속하는 역할을 수행한다), 하나는 기본적인 무선 공유기로 사용하도록 한다(비인증 AP로 동작하는 역할을 수행한다). 시중에 판매하는 몇몇 무선 공유기는 하드웨어 칩셋을 사용하여 CPU가 패킷을 처리하는 것에 비해 8~10배 정도 빠른 성능을 보이는 것으로 알려져 있다. 또한 많은 무선 공유기에서는 포트 미러링 기능을 지원하기 때문에, 비인증 AP를 지

나는 모든 패킷을 성능 하락 없이 엿들을 수 있다.

Ⅲ. 시간 기반의 비인증 AP 탐지 기법

3.1 기본 분류 기법

H. Han 등은 무선을 이용한 비인증 AP이 있을 경우 추가적인 무선 구간이 생겨서 DNS 패킷이 서버에 갔다 오는 시간 중에 유선 구간을 통과하는 시간이 증가한다는 이론 근거로 비인증 AP를 탐지하는 방법을 제안했다[5]. 그들은 DNS 패킷이 서버에 갔다 오는 시간 중에 유선구간을 통과하는 시간을 Δt로 정의했다.

$$\Delta t = \overline{RTT_{dns}} - \overline{RTT_{probe}} \tag{1}$$

$\overline{RTT_{dns}}$는 DNS 패킷의 왕복 시간(round trip time)의 평균값을 의미하며 $\overline{RTT_{probe}}$는 Probe request/response 통신 규격을 이용한 무선 구간 왕복 시간의 평균값을 의미한다. 일반적으로 DNS query가 발생 했을 때 패킷의 경로는 [그림 2]와 같다. 따라서,

$$\begin{aligned}\Delta t &= \overline{RTT_{dns}} - \overline{RTT_{probe}} \\ &= T^{ap\rightarrow serv} + T^{serv\rightarrow ap}\end{aligned} \tag{2}$$

라고 할 수 있다. 그러나 비인증 AP에 접속 했을 경우는 [그림 3]과 같이 비인증 AP와 AP 사이에서 추가적인 무선 구간이 생긴다. 따라서,

$$\begin{aligned}\Delta t' &= \overline{RTT_{dns}} - \overline{RTT_{probe}} \\ &= T^{rap\rightarrow ap} + T^{ap\rightarrow serv} + T^{serv\rightarrow ap} + T^{ap\rightarrow rap}\end{aligned} \tag{4}$$

이 될 것이다. 효율적인 비인증 AP 탐지를 위해서 $\Delta t < \theta < \Delta t'$을 만족하는 θ값을 찾아야 하는데, H. Han는 시험을 통해서 $\Delta t'$은 보편적으로 $1.3ms$보다 크다는 결과를 얻었다. 그러나 네트워크 상황이 혼잡함에 따라 $\overline{RTT_{dns}}$과 $\overline{RTT_{probe}}$은 불규칙하게 증가한다. 이러한 문제를 해결하기 위해서 θ값을 $\overline{RTT_{dns}}$과 $\overline{RTT_{probe}}$의 표준편차 σ_{probe}와 σ_{dns}에 의해서 동적으로 조절하도록 아래와 같은 식을 제안하였다.

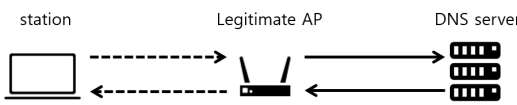


그림 2. 정상 AP의 DNS query 경로
Fig. 2. Path of DNS query with legitimate AP

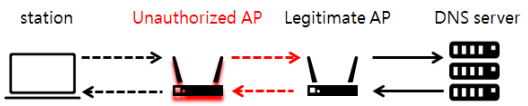


그림 3. 비인증 AP의 DNS query 경로
Fig. 3. Path of DNS query with legitimate AP

$$\theta = f(\sigma_{probe}, \sigma_{dns}) = \alpha \cdot \frac{\sigma_{probe} + \sigma_{dns}}{2} + \beta \tag{5}$$

H. Han 등은 실험을 통해 얻은 결과로 α값을 0.49로 정하고 β를 1.3으로 정하면 비인증 AP를 잘 분리할 수 있다고 주장했다. 실제 사용자는 자신의 스테이션(노트북, 스마트폰)에서 RTT의 샘플을 충분히 많이 측정한 다음 Δt와 θ을 계산하여, 만약 $\Delta t > \theta$면 연결된 AP를 비인증 AP로 판정 할 수 있다.

3.2 선형 분류와 비선형 분류

H. Han 등은 그들의 논문에서 α와 β 값을 특정하였는데, $x = (\sigma_{probe} + \sigma_{dns})/2$로 놓으면

$$\theta = f(x) = \alpha x + \beta \tag{6}$$

와 같은 직선의 방정식을 이용한 전형적인 선형 분류식이 됨을 알 수 있다. 환경이 바뀐다면, α와 β 값을 다시 구해서 사용할 필요가 있음을 보여준다. 하지만 이는 네트워크 환경에 대한 일종의 학습이 필요함을 보여주는 것이어서 H. Han 등의 방법을 사용할 때는 주의할 필요가 있어 보인다.

한편, 그들의 연구에서도 지적했다시피 네트워크 상황에 따라 직선의 방정식으로 분류할 수 없는 구간이 등장하게 된다. 강성배 등과 이재욱 등은 직선의 방정식으로 분류할 수 없는 부분을 고려하여 직선의 방정식 대신 SVM을 이용하면 다양한 네트워크 상황에서도 비인증 AP를 분류해낼 수 있음을 보였다[6,7].

3.3 소프트웨어 방식의 비인증 AP 구성

H. Han 등은 그들의 논문에서 [그림 1(a)]에 보이는 것과 같이 노트북에 무선 랜카드를 추가하여 구성한 비인증 AP를 사용하였다고 밝혔다. 하지만 앞서 언급했던 것과 같이 이러한 비인증 AP 구성은 노트북의 CPU가 패킷을 소프트웨어적으로 처리하기 때문에, 패킷이 비인증 AP를 지날 때 큰 시간 지연이 발생하게 된다. 즉, 보편적으로 얻어낸 $\Delta t'$ 값이 이러한

처리 시간이 포함되어 있는 것이다.

이 논문에서는 [그림 1(b)]와 [그림 1(c)]에 보이는 것과 같은 비인증 AP에 대해서 H. Han 등의 시간 기반의 비인증 AP 탐지 기법을 재현함으로써, 시간 지연 측정을 통한 비인증 AP 탐지 기법을 쉽게 회피할 수 있음을 보인다.

Ⅳ. 실험 및 분석

4.1 실험 환경

하드웨어 성능 제한을 최대한 줄이기 위해서 H. Han 등이 제안한 비인증 AP 탐지 알고리즘을 노트북이나 스마트폰 등과 같은 모바일 기기가 아니라 데스크 탑을 이용하여 스테이션 구현하였다. 스테이션의 사양은 [표 1]과 같다.

이 논문에서는 모바일 장치를 이용한 비인증 AP과 무선 장치를 이용한 고성능 AP 상대로 실험을 진행한다. H. Han 등의 논문에서 진행한 실험은 노트북을 이용한 비인증 AP 상대로 했으며 그 결과는 여러 논문에서 검증되었기 때문에 이 논문에서는 특별히 더 다루지 않는다. 대신 저사양 비인증 AP의 예로서 스마트폰을 이용한 비인증 AP를 구성하여 실험하였다. 스마트폰을 이용한 비인증 AP의 사양은 다음 [표 2]와 같다.

또한 무선 장치를 이용한 고성능 비인증 AP은 EFM ipTIME N8004R 두 개로, 하나는 무선 WAN으로 하나는 일반 무선 공유기로 세팅하여 사용하였다. 그리고 정상 AP는 EFM ipTIME N8004R하나로 구성이 되었다. EFM ipTIME N8004R은 리얼텍社의 RTL8198을 SoC로 사용하였으며, 하드웨어 NAT를 사용하고 있다.

이 논문에서는 정상 AP, 모바일 비인증 AP, 고성능 비인증 AP 상대로 각각 100번의 실험을 진행하였다. H. Han 등은 그들의 논문에서 네트워크상태에 따라 다양한 실험을 수행하였다. 혼잡 상태에서는 일정

표 1. H. Han 등의 탐지 알고리즘 탑재 장치의 사양
Table. 1 Specification of station for H. Han et al.'s unauthorized AP detection algorithm

	description
CPU	Intel Core i5-3570K
memory	4GB
OS	Ubuntu 12.04 (kernel 3.2.0-33-generic)
WiFi Adapter	D-Link DWA-125
library	Click toolkit 1.8[8]

표 2. 모바일 장치를 이용한 비인증 AP의 사양
Table. 2 Specification of unauthorized AP using smart phone

	description
Smart phone	Google Nexus 5 LG-D821
ROM	Omni-4.4.2-20140513-hammerhead-NIGHTLY
Kernel	kernel 3.4.0-ElementalX-0.21+
WiFi Adapter	TP-LinkTL-WN722N

확률로 비인증 AP 탐지 해내지지 못했고, 유휴 상태에서는 거의 완벽히 비인증 AP를 탐지 해냈다고 밝히고 있다. 따라서 그들의 기법이 가장 잘 비인증 AP를 분류해내는 유휴 상태에 대해만 실험을 진행하였다.

4.2 실험 결과 및 분석

정상 AP의 경우 H. Han 등의 기법에 의하여 94% 정상 AP 탐지로 분류되었다. 또한 스마트폰을 이용한 비인증 AP 상대로 한 실험에서는 99%로 비인증 AP로 분류하였다. 그러나 고성능 비인증 AP 상대로 진행한 실험에서는 비인증 AP로 분류한 경우는 전무했다.

[그림 4]는 정상 AP로부터 측정한 RTT값들 누적 분포 그래프다. [그림 4]에 따르면 $\overline{RTT_{dns}}$와 $\overline{RTT_{probe}}$의 차이 Δt는 0.3451에 불과하다. θ의 정의에 따르면 θ는 적어도 1.3보다 크므로 $\Delta t < \theta$이다, 즉 H. Han 등의 알고리즘을 따르면 정상 AP라는 판단을 내릴 것이다. 실험결과에 따르면 H. Han 등의 알고리즘으로 정상 AP를 잘 분리해 낼 수 있다는 사실을 알 수 있다.

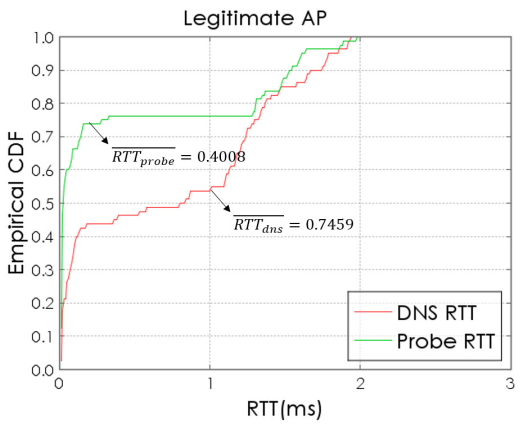


그림 4. 정상 AP RTT값의 누적 분포
Fig. 4 Cumulative distribution of RTT of legitimate AP

[그림 5]는 스마트폰을 이용한 비인증 AP에서 $\overline{RTT_{dns}}$ 과 $\overline{RTT_{dns}}$ 을 분석한 그래프다. 두 선이 확실하게 분리되는 모습이 보이며 [그림 4]와 구분하기가 쉽다. 스마트폰을 이용한 비인증 AP 상대로 한 실험에서는 Δt는 2.3764에 이르며, 분류 성공률이 99%에 달했다.

[그림 6]은 고성능 비인증 AP에 대한 결과를 보여준다. [그림 4]와 비교해 보았을 때 단순히 구분하기가 힘들고, 실제로 Δt값을 비교 했을 때도 0.5225로 스마트폰을 이용한 비인증 AP의 2.3764보다 정상 AP의 0.3451에 보다 가까웠다. 실험에서는 고성능 비인증 AP의 경우 정상 AP에 대해서 $\overline{RTT_{dns}}$가 다소 늦어지고, $\overline{RTT_{probe}}$가 다소 빨라졌다. 일부 측정치의

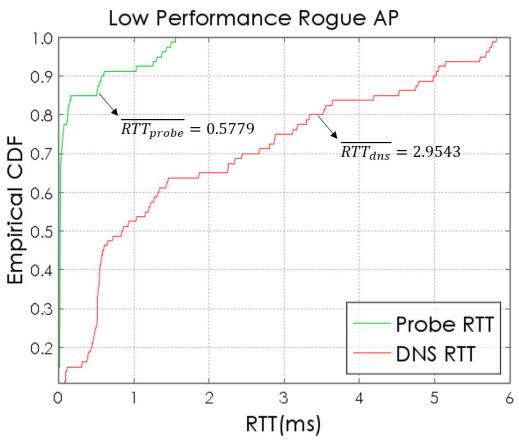


그림 5. 저성능 비인증 AP RTT값의 누적분포
Fig. 5. Cumulative distribution of RTT of low performance unauthorized AP

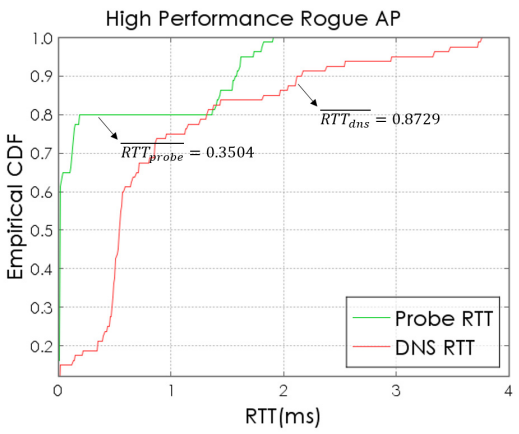


그림 6. 저성능 비인증 AP RTT값의 누적분포
Fig. 6. Cumulative distribution of RTT of high performance unauthorized AP

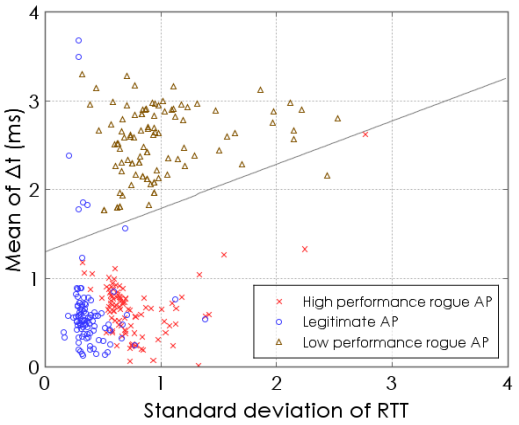


그림 7. RTT의 표준편차에 대한 평균 Δt
Fig. 7. Mean value of Δt against the average value of standard deviation of RTT

경우 RTT 값이 느려져 표준 편차를 다소 크게 하는 현상을 볼 수 있었다.

[그림 7]는 H. Han 등이 사용하였던 분류기법에 따라 정상 AP와 저성능 비인증 AP, 고성능 비인증 AP에 대한 전체 실험 결과를 정리한 것이다. 그림 중간의 직선은 H. Han 등이 제안하였던 직선의 방정식으로 직선보다 위에 있으면 비인증 AP로 아래에 있으면 정상 AP로 판단내릴 수 있다. 보는 바와 같이 저성능 비인증 AP의 경우 H. Han 등이 그들의 논문에서 밝혔던 것과 같이 잘 분류가 됨을 알 수 있다. 그러나 고성능 비인증 AP의 경우 모두 직선보다 아래에 있어 정상 AP로 판단 내렸음을 알 수 있다.

[그림 7]에서 정상 AP와 고성능 비인증 AP가 분포한 위치가 일부 겹치는 것은 고성능 비인증 AP가 정상 AP와 구별하기 힘듦을 의미한다. 만약 이 논문에서와 같이 두 대의 무선 공유기가 아니라 보다 최적화되고 더 빠른 비인증 AP를 제작 가능하다면 겹쳐지는 영역은 더 넓어질 수 있을 것이다. 이는 고성능의 비인증 AP가 실제로 등장하여 사용된다면 H. Han 등과 같이 시간 지연을 측정하는 방식으로는 더 이상 비인증 AP인지 아닌지를 구별해내는 것은 불가능할 수 있음을 시사한다.

V. 결 론

이 논문에서는 무선 공유기 2대를 연결하여 구성한 고성능 비인증 AP를 이용하여 기존에 H. Han 등이 제안하였던 시간 지연 측정을 통한 비인증 AP 분류 실험을 재현하였다. 실험 결과, 앞선 연구에서 특별히

고려하지 않았던 비인증 AP의 패킷 처리 성능이 실제로 비인증 AP 분류에 지대한 영향을 미치고 있음을 알 수 있었다. 고성능 비인증 AP의 경우에도 정상 AP와 비교하여 RTT의 표준 편차에서 차이가 남을 알 수 있었지만, 저성능 비인증 AP에 비해서는 그 차이가 크지 않아 기존의 직선의 방정식으로는 정상 AP와 고성능 비인증 AP를 분류하는 것은 쉽지 않을 것으로 보인다.

이 연구에서 보다시피, 앞으로 더 좋은 성능을 가진 비인증 AP가 등장한다면, H. Han 등이 제안하였던 기법으로는 더 이상 비인증 AP를 찾아낼 수 없음을 알 수 있었다. 더 나아가, H. Han 등이 제안하였던 기법뿐만 아니라, 기존의 모든 시간 측정 기반의 비인증 AP 탐지 기법이 고성능 비인증 AP에 의해서 무력화될 가능성이 있음을 알 수 있었다.

앞으로 더 다양한 시간 측정 기반의 비인증 AP 탐지 기법들에 대해서 고성능 비인증 AP에 대한 분류 성능에 대해서 검증해 보아야할 필요성이 있을 것으로 보인다. 그리고 시간 측정 기반이 하드웨어 성능의 발전에 의해 무력화되는 상황에서 위조 불가능한 '비인증 AP 탐지요소'에 대한 연구에도 더 많은 관심을 기울여야할 것이다.

향후 연구에서는 무선 자원을 사용하는 비인증 AP가 일반적으로 정상 AP와 성능상의 문제로 인하여 동일 채널이나 인접 채널을 사용하지 않는다는 점을 역으로 이용하여 비인증 AP를 찾아내는 방법에 대해서 연구하려고 한다. 현재 연결된 AP와 연관 없는 채널에 대한 강제적인 노이즈 삽입이 (재전송 증가에 의한) 통신 성능에 영향을 준다면, 이는 통신 경로에 무선 구간이 한 개 이상 존재함을 시사한다. 이러한 관측 요소는 통신 매체와 관련된 것으로 데이터가 특정한 경로를 돌아오는 시간과 연관성이 없기 때문에 비인증 AP의 성능에 영향을 받지 않을 것으로 기대한다.

References

[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, Uppsala, Sweden, Jun. 2006.

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

[3] R. Beyah, S. Kangude, G. Yu, B. Strickland, and J. Copeland, "Rogue access point detection using temporal traffic characteristics," in *Global Telecommun. Conf.*, pp. 2271-2275, Dallas, USA, Nov. 2004.

[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," in *Proc. ACM SIGCOMM*, pp. 365-378, San Diego, USA, Oct. 2007.

[5] H. Han, B. Sheng, C. C. Tan, Q. Li, and S. Lu, "A timing-based scheme for rogue AP detection," *IEEE Trans. Parallel and Distrib. Syst.*, vol. 22, no. 11, pp. 1912-1925, Nov. 2011.

[6] S. Kang, D. Nyang, J. Choi, and S. Lee, "Relaying rogue AP detection scheme using SVM," *J. The Korea Inst. Inf. Security & Cryptology*, vol. 23, no. 2, Jun. 2013.

[7] J. Lee, S. Lee, and J. Moon, "Detecting rogue AP using k-SVM method," *J. The Korea Inst. Inf. Security & Cryptology*, vol. 24, no. 1, Feb. 2013.

[8] UCLA.edu, [Click], http://read.cs.ucla.edu/click/click

장 룡 호 (Rhong-Ho Jang)

2013년 8월 : 인하대학교 컴퓨터정보공학과 졸업

2013년 9월~현재 : 인하대학교 컴퓨터정보공학과 석사과정

<관심분야> 네트워크 보안, 정보보호, 무선 인터넷 보안

강 정 일 (Jeon-Il Kang)

2003년 2월 : 인하대학교 컴퓨터공학과 졸업
2006년 2월 : 인하대학교 정보통신대학원 석사
2014년 8월 : 인하대학교 정보통신공학과 박사
2014년 9월~현재 : 인하대학교 컴퓨터공학과 박사연구원
<관심분야> RFID 보안, 생체 인식 보안, 무선 센서 네트워크 보안, 무선 인터넷 보안, 웹 인증 보안

양 대 헌 (Dae-Hun Nyang)

1994년 2월 : 한국과학기술원 과학기술 대학 전기 및 전자 공학과 졸업
1996년 2월 : 연세대학교 컴퓨터과학과 석사
2000년 8월 : 연세대학교 컴퓨터과학과 박사
2000년 9월~2003년 2월 : 한국전자통신연구원 정보보호연구본부 선임연구원
2003년 2월~현재 : 인하대학교 컴퓨터정보공학과 교수
<관심분야> 암호이론, 암호프로토콜, 인증프로토콜 무선 인터넷 보안, 네트워크 보안

이 경 희 (Kyung-Hee Lee)

1993년 2월: 연세대학교 컴퓨터과학과 학사
1998년 8월: 연세대학교 컴퓨터과학과 석사
2004년 2월: 연세대학교 컴퓨터과학과 박사
1993년 1월~1996년 5월 : LG 소프트(주) 연구원
2000년 12월~2005년 2월 : 한국전자통신연구원 선임연구원
2005년 3월~현재 : 수원대학교 전기공학과 부교수
<관심분야> 바이오인식, 정보보호, 컴퓨터비전, 인공지능, 패턴인식