논문 14-39B-01-03

한국통신학회논문지(J-KICS) '14-01 Vol.39B No.01
http://dx.doi.org/10.7840/kics.2014.39B.1.17

스마트폰을 위한 무선 AP 인증 방법

신 동 오◆, 강 전 일*, 양 대 헌*, 이 석 준**, 이 경 희°

A Method of Authenticating WLAN APs for Smartphones

DongOh Shin◆, Jeonil Kang*, DaeHun Nyang*, Sokjoon Lee**, KyungHee Lee°

요 약

스마트폰 사용자의 증가는 이동 통신사업자에게 커피숍, 지하철과 같은 공공장소에 와이파이 핫스팟을 제공함으로써 폭증하는 3/4G 트래픽을 분산시키는 노력을 하게 하였다. 전통적인 무선랜에서의 인증은 서비스 제공자측면에서 설계되었기 때문에, 서비스 이용자는 서비스 제공자에게 자신이 고객임을 증명하는 방식으로 이루어진다. 802.11 표준에서는 802.1X를 이용한 상호인증이 지원되지만, 서비스 이용자는 자신이 접속하려는 무선 AP가 정말 서비스제공자가 설치한 것인지 확인하는 것은 어렵다. 공격자는 사용자들의 개인 정보를 얻어내기 위하여 서비스 제공자가 설치한 AP와 동일한 SSID를 가진 위장 AP를 설치할 수 있다. 이 논문에서는 스마트폰 사용자 입장에서 정상적인 무선 AP를 인증하는 기법에 대해 소개한다. 그리고 이 논문의 제안이 이미 제공된 와이파이 핫스팟에서 보안 플러그인 형태로 잘 동작할 수 있음을 보이고, 이를 실험을 통해 증명한다.

Key Words : WLAN AP, smartphone, authentication, geometric positioning system, rogue AP prevention

ABSTRACT

The increase of smartphone users have made mobile carriers offload increasingly congested traffic of 3/4G by providing Wi-Fi hot-spots in the public places such as coffee shops and subway stations. In the traditional authentication in WLAN, the users should convince the service providers that they are valid customers before they use WLAN services. Since the authentication protocol is designed for service providers. Even with the mutual authentication based on the IEEE 802.1X, which is supported by IEEE 802.11 standard, it is difficult to be convinced of that the service providers really have installed the WLAN APs, which users are confronted with. An attacker can install rogue APs that masquerade as legitimate APs by copying the SSID, MAC address, etc. in order to obtain users' private information. In this paper, we introduce a method of authenticating legitimate APs for smartphone users. And we show our proposal can be well utilized for the current Wi-Fi hot-spots as a security plug-in and prove it through our experiments.

Ⅰ. 서 론

전통적인 무선랜(WLAN, Wireless Local Area Network)에서의 인증은, 무선랜 서비스 제공자의 입장에서 서비스 이용자가 인가된 이용자인지를 인증하는 것에 초점을 두었다. 기업 및 이동통신사는 스마트

※ 본 연구는 미래창조과학부가 지원한 2013년 정보통신·방송(ICT) 연구개발사업의 연구결과로 수행되었음(12-912-06-001. "MTM기반 단말 및 차세대 무선랜 보안 기술 개발")
◆ First Author : 인하대학교 컴퓨터정보공학과 정보보호연구실, mannershin@isrl.kr, 정회원
° Corresponding Author : 수원대학교 전기공학과, khlee@suwon.ac.kr, 정회원
* 인하대학교 컴퓨터정보공학과 정보보호연구실, dreamx@isrl.kr, nyang@inha.ac.kr, 정회원
** 한국전자통신연구원 사이버보안연구본부 선임연구원, junny@etri.re.kr, 정회원
논문번호 : KISC2013-12-524, 접수일자 : 2013년 12월 5일, 심사일자 : 2013년 12월 23일, 최종논문접수일자 : 2014년 1월 8일

폰이 일반화됨에 따라 고객의 편의를 위해 와이파이 핫스팟을 설치하여 자사의 고객에게 무선인터넷 서비스를 제공하였는데, 자사의 고객만이 서비스를 이용할 수 있도록 802.1X 표준에 근거하여 인증시스템을 구성하였다. 서비스이용자는 와이파이 핫스팟에 대한 접근성이 높아졌지만, 자신의 스마트폰에서 이용 가능한 무선 AP를 누가 설치한 것인지 확인할 방법이 없다는 문제점이 생겼다. 공격자는 이러한 문제점을 이용하여 기업 또는 이동통신사에서 관리하는 무선 AP와 동일한 SSID를 가진 위장 AP(rouge AP)를 설치하여 사용자를 속이는 것이 매우 쉬우며, MITM(Man-In-The-Middle) 공격을 통해 위장 AP에 접속한 사용자의 개인 정보를 쉽게 탈취할 수 있다. 우리는 이러한 문제점에 착안하여 사용자의 입장에서 접속하고자 하는 무선 AP의 신뢰성을 인증할 수 있는 방안에 대해 연구하였다. 그리고 현재 서비스 중인 상황에서 이 논문에서의 연구결과가 보안 플러그인 형식으로 어렵지 않게 도입될 수 있음을 보인다.

이 논문의 2장은 무선랜 환경에서 다루어진 인증방법 및 위장 AP 탐지기법에 대해 소개하며 이 연구의 차별성에 대해 논한다. 3장과 4장은 GPS(Global Positioning System) 좌표에 기반을 둔 무선 AP 인증 방법에 대해 소개하고 여러 전략과 예상되는 문제점에 대해 논한다. 5장은 시뮬레이션을 통해 얻은 결과 및 분석을 보인다. 6장은 현재 관리되고 있는 기업 및 이동통신사의 무선 AP에서 우리의 연구 결과를 보안 플러그인 형식으로 도입하기 위해서 추가적으로 고려해야 하는 여러 사항들에 대해 이야기한다. 7장에서는 이 연구의 결론을 담는다.

Ⅱ. 관련연구

전통적인 WLAN의 연구에서 인증의 대상은 무선 AP가 아니라 사용자이기 때문에 인가된 사용자에게만 무선랜 서비스를 제공하는 연구가 주를 이루었고 표준으로 자리 잡았다[1]. 하지만 스마트폰의 사용과 공공장소에서 무선 인터넷 서비스 이용이 일반화된 현재의 상황에서는, 사용자 입장에서 접속하려는 무선 AP가 신뢰할만한 것인지 확인하는 것이 중요하다. 무선 AP 인증은 사용자가 접속하려는 무선 AP가 서비스 제공자가 설치한 것인지, 공격자가 설치한 것인지 확인할 수 있는 방법을 마련해주는 것에 그 목적이 있다. 하지만 사용자 입장에서 무선 AP를 인증하는 것과 관련된 연구는 아직까지 국내·외에서 찾아보기 어렵다.

그와는 반대로, 위장 AP를 탐지하는 문제는 꾸준하게 연구되어 왔다. 김이룩 등의 연구는 네트워크의 RTT(round trip time)값을 측정하여 3G망을 이용하는 위장 AP를 탐지하는 것이다[2]. 하지만 유무선망을 이용한 무선 AP보다 느린 이동통신사의 3G 전송속도에 기반을 둔 측정방법으로, LTE 또는 LTE-A망을 이용하는 공격자는 이러한 방법으로 탐지가 어렵다. 강성배 등의 연구는 위장 AP를 탐지하기 위해 데이터 수집 및 훈련 과정이 필요한데, 무선 AP하나당 이러한 일련의 과정이 소요되기 때문에 스마트폰에 탑재하여 무선 AP를 인증용으로 이용하기에는 적절하지 않다[3]. H. Han 등의 연구도 앞의 두 연구와 마찬가지로 위장 AP를 탐지하는 주요 요소로 RTT 값을 이용한다[4,5].더 쾌적한 인터넷을 제공하는 AP를 시스템적으로 선택하는 방법에 대한 연구도 있었지만, 이는 위장 AP를 탐지하는 기법은 아니다[6]. 이는 이 연구 결과의 주 기능이라기보다는 부가적인 기능에 의해 발생하는 효과라고도 할 수 있다. 하지만 사용자가 위장 AP만의 전파를 수신하고, 그것이 인접한 다른 AP들보다 나은 통신 환경을 제공한다면 사용자는 위장 AP로 접속하게 될 것이다.

지리정보를 이용한 인증은 Denning과 Macdorman의 연구를 시작으로 다양하게 연구되었지만, 인증을 수행하는 주체는 서비스 제공자이지 사용자가 아니다[7]. 그 중 Takamizawa와 Kaijiri는 웹에 기반을 둔 인증시스템에서 GPS 정보를 이용하여 보안성을 향상시키는 방법을 제안하였다[8]. 저자들은 ID와 패스워드에 더해 모바일 기기의 GPS정보를 같이 전송하여 웹 서버에 접속을 요청한 사람이 정말 그 사람인지, 아니면 계정을 공유하거나 훔친 사람인지 판별할 수 있다고 주장한다. 저자들은 GPS정보가 쉽게 변조될 수 있다는 점은 간과하였지만, 모바일 기기에서 GPS좌표를 인증에 이용하였다는 것에 그 의의가 있다. Zhang 등은 스마트폰의 위치정보를 이용한 인증 및 권한 부여 방법을 제안하였다[9]. 저자들은 하드웨어 수준, 운영체제 수준, 응용프로그램 수준에서 각각 발생할 수 있는 지리정보 속임에 대해 설명하며 지리정보 생성 및 전송, 검증하는 모든 과정에 대하여 포괄적인 보호기법을 제안하였다.

이상과 같이 위장 AP를 탐지하는 대부분의 연구는 사용자가 일단 위장 AP에 접속한 뒤에 RTT 값 등을 통해 위장 AP 여부를 판단한다. 서비스 제공자 차원에서 서비스 이용자가 위장 AP에 접근하는 것을 효과적으로 보호해주는 것은 어려운 일이다. 한국 인터넷진흥원에서는 공공 WLAN을 안전하게 운영하는 위

하여 주기적으로 불법 AP를 점검하라고 권고하고 있을 뿐이다[10]. 따라서 신뢰할 수 있는 무선 AP 인증 기법을 서비스 제공자 차원에서 개발하고, 이를 서비스 이용자에게 이용하게 함으로써 보다 안전하게 서비스를 이용할 수 있도록 하는 연구가 필요하다고 할 수 있다.

Ⅲ. GPS 좌표에 기반을 둔 무선 AP 인증: 기본 아이디어

3.1 무선 AP를 식별할 수 있는 정보들

1) 통신 프로토콜 정보: 무선 AP에서 주기적으로 발송하는 비콘 프레임에 담긴 정보는 표 1과 같다. 비콘 프레임에는 총 10개의 정보가 있으나 그 중 Timestamp, Beacon interval, Capability Information, SSID, Supported Rates 항목만이 필수 정보이고 나머지는 무선 AP의 설정 및 역할에 따라 포함여부가 달라진다. 따라서 무선 AP를 인증하기 위해 비콘 프레임의 정보를 이용한다면 표 1의 1번~5번 정도에서 선택하거나, 비콘 프레임을 수신한 채널 정도를 이용할 수 있을 것이다. 하지만 비콘 프레임은 공격자도 수신 가능하기 때문에 이 정보만 이용하여 무선 AP를 인증하는 것은 공격에 취약할 수밖에 없다. 무선 AP의 비콘 프레임을 보고 동일한 비콘 프레임을 발생시키는 위장 AP를 만들어내는 것은 공격자에게 어려운 일이 아니기 때문이다. 따라서 무선 AP에 서비스를 요청하는 사용자와 무선 AP를 설치한 서비스 제공자가 같이 '알고 있는' 정보를 동시에 이용해야만 한다.

2) 우편 주소: 국내 이동통신사가 제공하는 와이파이 핫스팟의 정보 중 '우편 주소'를 이용할 수 있다. 국내 이동통신사는 WiFi 핫스팟을 관리하며 이미 핫스팟 이름, 업종, 주소를 포함한 정보를 웹과 스마트폰 앱을 통하여 서비스 이용자에게 제공하고 있기 때문에, 서비스 이용자는 접속 가능한 무선 AP의 신뢰성을 검증하기 위하여 자신의 위치한 주소를 이용할 수 있다[11-13]. 하지만 주소를 문자로 다루기에는 표기하는 방법의 차이 등, 변수가 다양하기 때문에 실제로는 사용하기 힘들다.

표 1. 비콘 프레임 몸체
Table 1. Beacon frame body[1]

Order	Information
1	Timestamp
2	Beacon interval
3	Capability Information
4	SSID
5	Supported Rates
6	FH Parameter Set
7	DS Parameter Set
8	CF Parameter Set
9	IBSS Parameter Set
10	TIM

3) GPS 좌표: 일반 지리 정보 시스템에서 널리 이용하는 GPS 좌표계는 위도(Latitude)와 경도(Longitude)는 구성되어있다. 위도는 지구상에서 적도를 기준으로 하여 남북으로 각각 90등분한 값이고, 경도는 본초 자오선을 기준으로 하여 동서로 각각 180등분한 값이다. 지구상의 한 점에 대한 위도와 경도는 십진수 도(°)로 표현한다. 구글맵, 네이버 지도, 다음 지도는 실제 주소를 GPS 좌표 체계로 변환해주는 Geocoding 서비스를 제공한다[15-17]. 하지만 실제 AP가 설치된 장소의 GPS주소와 사용자가 위치한 GPS 주소는 다를 수 있고, 전파반경으로부터 일정거리 떨어져있어도 서비스가 되어야한다.

이 논문에서는 GPS모듈에서 얻을 수 있는 GPS 좌표를 변형하여 이용한다. 따라서 필연적으로 우리 연구가 대상으로 하는 장치는 스마트폰과 같이 GPS 모듈이 기본으로 탑재되어 있는 장치로 한정된다.

3.2 GPS 좌표를 단위 좌표로 변환

스마트폰의 GPS모듈은 위도와 경도를 소수 여섯 번째 자리까지 표현한다. 위도를 기준으로 소수 여섯 번째 자리는 약 0.0036초 단위로 나뉘며, 이를 거리로 환산하면 약 0.1m로, 무선 AP에 접속하려는 사용자와 무선 AP가 일정 범위 내에 같이 있음을 검사하는 용도로 사용하기에 지나치게 높은 정밀도를 갖고 있다. 따라서 우리는 GPS좌표의 정밀도를 필요한 수준으로 낮추기 위해 다음과 같은 방식을 이용하였다.

단위 거리 δ가 주어졌을 때, 단위 위도 d_{lat}은 적도부터 북극(또는 남극)까지의 거리를 단위 거리로 나누었을 때 얻을 수 있는 각도이다. 그림 1과 같이 적도부터 극까지의 거리는 약 10,000,000m이고, 각도는 90°이므로, 1°당 거리는 약 111,111m가 된다. 따라서 사용자가 $lat_{\max} \geq u_{lat} \geq lat_{\min}$을 만족하는 어떠한 좌표계 (u_{lat}, u_{lng})가 있을 때, 해당 위치에서 단위 위도 d_{lat}과 단위 경도 d_{lng}는 각각,

$$d_{lat} = \delta / 111111\ (m/^\circ),$$
$$d_{lng} = \frac{360 \times \delta}{(2\pi \times 6371000 \times \cos(\frac{lat_{\max} + lat_{\min}}{2}))} \quad (1)$$

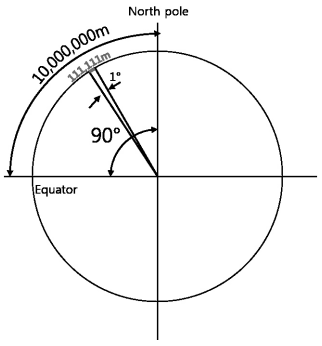


그림 1. 1도당 호의 길이
Fig. 1. The arc length per degree

로 구할 수 있다. 상수 6371000은 지구의 평균 반지름이다. $lat_{\max}$와 $lat_{\min}$은 일정한 단위 경도로 자르고자하는 지역의 최북단과 최남단이 될 수 있다. 예를 들어 $lat_{\max}$는 '강원도 고성군 현내면 송현진'으로 38° 27'가 될 수 있고, $lat_{\min}$은 '제주도 남제주군 마라도'로 33° 06'이 될 수 있다. 이는 극에 가까워질수록 동위도의 둘레의 길이가 줄어 단위 경도는 평균적으로밖에 사용할 수 없기 때문이다. 사용자의 위치 (u_{lat},u_{lng})는 d_{lat}, d_{lng}로 각각 나누어, 다음과 같이 변환될 수 있다.

$$t_{lat} = \lfloor u_{lat}/d_{lat} \rfloor \\ t_{lng} = \lfloor u_{lng}/d_{lng} \rfloor \quad (2)$$

실제 인증에 사용되는 정보인 (t_{lat},t_{lng})는 지구의 적도부터 북극 (또는 남극)까지의 거리를 각도 d_{lat}으로 나누었을 때, 현재의 위치가 북쪽(또는 남쪽)으로 몇 번째에 위치하는가와 현재 위도 상에서 본초자오선을 기준으로 현재의 위치가 동쪽(또는 서쪽)으로 몇 번째에 위치하는가를 의미한다.

3.3 멤버십 구조체 생성 및 테스트

신뢰할 수 있는 n개의 AP를 인증하기 위한 멤버십 구조체(또는 멤버십 필터)를

$$\mathbb{F} = \cup_{i=1}^{n}(|H(\mu_i,c_i,(t_{lat},t_{lng})_i,\cdots)|_1^m) \quad (3)$$

와 같이 구성할 수 있다. μ_i은 i번째 무선 AP의 MAC 주소이며, c_i은 무선 AP가 이용하고 있는 채널 정보이다. $(t_{lat},t_{lng})_i$는 무선 AP의 GPS 좌표계를 단위 위도와 경도로 변환한 정보이다. $H()$는 암호학적 해시 함수를 의미하며, $|\ |_1^m$ 는 1부터 m까지의 비트열을 의미한다. 구조체 $\mathbb{F}$는 사용자에게 사전에 배포된다[1]. 여기서 m은 정상적인 무선 AP가 주는 정보 이외에는 올바른 인증 팩터를 생성할 수 없을 정도로 충분한 길이를 가져야만 한다. 이에 대해서는 6.1절에서 추가적으로 논의한다.

사용자는 자신의 위치 (u_{lat},u_{lng})로부터 (t_{lat},t_{lng})를 구하고, 테스트하려는 AP로부터 MAC 주소 μ', 채널 정보 c' 등을 알아내고 인증 팩터

$$f = |H(\mu',c',(t_{lat},t_{lng}),\cdots)|_1^m \quad (4)$$

를 계산하고 $\mathbb{F}$에 해당 정보가 있는 지 확인한다. 만약 구조체 $\mathbb{F}$에 인증 팩터 f가 포함되어 있다면 ($f \in \mathbb{F}$), 기존과 동일하게 802.1X 인증 프로토콜을 수행한다. 인증 팩터 f가 구조체 $\mathbb{F}$ 안에 포함되지 않는 경우($f \notin \mathbb{F}$)는 사용자의 위치가 무선 AP와 충분히 가깝지 않기 때문에 발생할 수도 있으며, 서비스 제공자와 동일한 MAC 주소, 채널 정보 등으로 위장한 위장 AP를 공격자가 설치함으로 인해 발생할 수 있다. 이 경우 서비스 제공자에 의해서 그림 2처럼 안내 메시지를 출력할 수 있을 것이다.

그림 2. 멤버십 테스트에 실패했을 경우 가능한 대응방법
Fig. 2. A possible solution when the membership test is failed

1) 현재 국내 주요 이동통신사업자는 자사의 서비스를 이용하는 단말기에 이미 자체적인 와이파이 접속 매니저 프로그램을 탑재하였다. KT와 U+는 단순 와이파이 접속관리 기능을 제공하지만, SKT의 Smart Wi-fi CM은 기본 기능뿐만 아니라 사용자 환경에 맞춘 자동 접속 기능, 신호가 약한 와이파이를 검색에서 제외할 수 있는 기능도 포함시켰다.

3.4 정상 AP로 위장한 위장 AP의 발견 및 대응

충분한 m의 길이를 갖는 인증 팩터의 경우 암호학적 해시 함수의 충돌을 찾아야하는 어려움이 있다. 따라서 위와 같은 멤버십 테스트를 통과하기 위하여 공격자는 자신의 위장 AP를 어떠한 정상적인 무선 AP와 동일하게 설정해야만 한다. MAC 주소와 같은 MAC 주소는 쉽게 위조가능하며, 다른 여러 가지 정보도 소프트웨어적으로 얼마든지 위조 가능하다. 하지만 위장 AP를 정상적인 무선 AP와 멀리 떨어뜨려 놓게 되면, GPS 좌표계가 달라지기 때문에 멤버십 테스트에서 실패하게 된다. 따라서 위장 AP가 멤버십 테스트를 통과하려면, 자신이 복재한 정상적인 무선 AP 근처에 위치할 수밖에 없다. 이 경우 위장 AP는 정상 AP와 동일한 영역에 위치하게 되며, 사용자의 입장에 있어서는 단지 하나의 AP로 보이게 되며, 위장 AP와 정상 AP를 구별할 수 없게 된다. 사용자는 멤버십 테스트를 수행할 것이고, 위장 AP에 접속할 수 있다.

이러한 경우를 막기 위해서는 정상 AP의 도움이 필요하다. 위장 AP와 사용자간에 통신이 시작되면, 정상 AP의 입장에서는 무선 네트워크에 자신과 동일한 정보를 보내는 다른 AP가 존재함을 알 수 있다. 자신이 보낸 적이 없는 메시지에 대한 응답(사용자가 보낸 메시지)이 자신의 MAC 주소를 도착점으로 해서 보내지는 것이다. 정상 AP는 이 경우, 사용자에 대해서 연결해제를 위한 프레임을 보내 연결을 종료하도록 할 수 있다. 또한 이에 대한 기록을 자신을 관리하는 시스템 관리자에게 통보하여, 주위에 위장 AP가 보이니 이를 물리적으로 해결하도록 유도할 수 있다.

연결해제 프레임을 이용하는 공격자의 서비스 거부 공격과 그 대응방법은 이 논문의 요지를 벗어나므로 다루지 않는다.

Ⅳ. GPS 좌표에 기반을 둔 무선 AP 인증: 인증 영역의 결정

4.1 경계선 문제와 단위 거리 δ의 결정

GPS의 정확도를 희생하여 일정 단위별로 구역을 나눈다면 그림 3과 같이 반드시 경계선 문제가 발생한다. 예를 들어, 단위 거리 δ가 0.001이라고 가정하였을 때, 사용자의 위치와 신뢰할 수 있는 무선 AP 사이의 거리는 0.001보다 가까운 0.0007임에도 불구하고 서로 속한 영역이 달라 인증이 되지 않을 것이다. 실제로는 신뢰할 수 있는 무선 AP이지만, 경계선 문제로 인해 신뢰할 수 없다고 판단하는 것은 사용자 편의성을 심각하게 저해할 수 있다. 이러한 문제를 해결

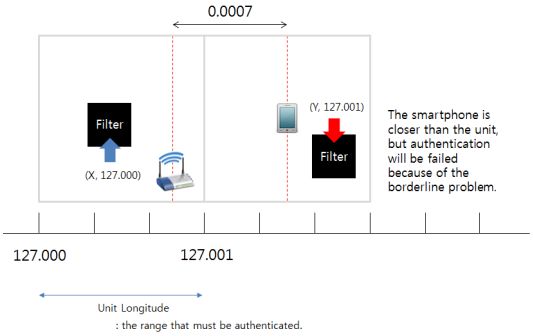


그림 3. 경계선 문제 예시
Fig. 3. An example of the borderline problem

하기 위해서 검색 영역을 상하좌우로 확대하는 등의 방법을 반드시 이용해야한다. 사용자는 그림 4처럼 상하좌우로 1씩 인접한 영역까지 무선 AP의 멤버십 테스트를 수행할 수 있다.

이상과 같이 상하좌우 3칸(3x3)에 대한 멤버십 테스트를 수행하는데 있어서, 단위 거리 δ를 지나치게 크게 잡으면, 공격자는 실제로는 사용자로부터 통신을 수행할 수 없을 정도로 멀리 위치한 무선 AP로 자신의 위장 AP를 위장할 수 있는 가능성을 주게 된다. 따라서 멤버십 테스트를 수행하는 모든 영역은 실제 사용자와 통신이 가능한 영역이어야만 한다.

사용자는 3x3 영역의 한 가운데에만 위치할 수 있고, 무선 AP는 3x3 영역 어디라도 위치할 수 있다. 사용자와 무선 AP가 최대한 멀리 떨어져 있는 경우를 가정하면, 사용자와 무선 AP의 최대 통신 거리를 R은 높이와 너비가 2δ인 정사각형의 대각선의 길이와 같아야만 한다. 피타고라스의 정리에 의하여, 단위 거리 δ와 통신 거리 R의 관계는

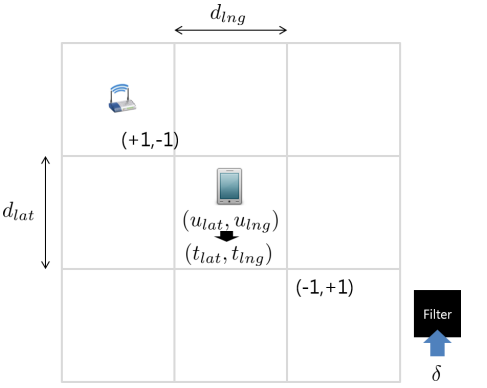


그림 4. GPS 좌표 변환과 인접 지역에 대한 멤버십 테스트 수행
Fig. 4. Conversion of GPS positions and membership tests for adjacent areas

$$R^2=(2\delta)^2+(2\delta)^2 \Leftrightarrow \delta=\sqrt{1/8}\cdot R \qquad (5)$$

와 같다.

4.2 인증 대상 영역 확대

그림 5는 인증 영역을 단순 확대하는 방법의 한계점을 보여준다. 그림 5의 AP1의 위치는 최대 전파 반경 R에 포함되며, 확장된 검색영역에 포함되기 때문에 멤버십 테스트를 통과할 것이다. 하지만 AP2의 경우, 스마트폰으로부터 $2\delta+\alpha$의 거리에 위치하여 스마트폰의 전파 반경 R에 충분히 포함되지만 검색 영역에는 포함되어있지 않기 때문에 멤버십 테스트를 통과하지 못한다. AP3은 거리적으로 AP1와 AP2보다 사용자와 더욱 가까이에 있지만 마찬가지 이유로 멤버십 테스트를 통과하지 못한다. 이는 사용자의 편의성을 크게 떨어뜨릴 수 있으므로, 스마트폰의 전파반경 이내라면 충분히 멤버십 테스트를 통과할 수 있도록 인증 대상 영역을 더욱 넓히는 방법이 반드시 필요하다.

스마트폰의 통신반경을 최대한 활용하기 위해서라면 인증영역을 넉넉하게 확장할 수도 있을 것이다. 하지만 공격자를 고려하지 않고 확장을 우선시 한다면 공격자로부터 안전하지 않은 상황이 발생할 수 있다.

예를 들어 그림 6과 같이 멤버십 테스트되는 모든 영역이 항상 통신 반경 안에 들어오는 경우를 생각해보자. 그림 6에서는 최대 16(4x4)개의 구역에 대해서 멤버십 테스트를 수행한다. 사용자의 통신 반경 R에 3개의 AP가 존재하지만, 위장 AP는 어떠한 AP로도 위장하지 못하게 된다. 공격자의 위장 AP가 AP1과 동일한 맥주소와 채널을 이용하도록 설정되었다면, 사

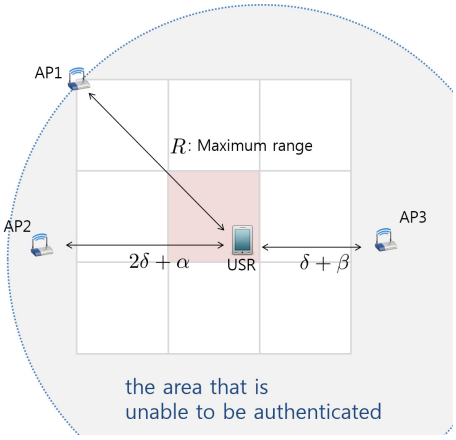


그림 5. 최대전파반경과 인증영역
Fig. 5. Maximum range and its coverage

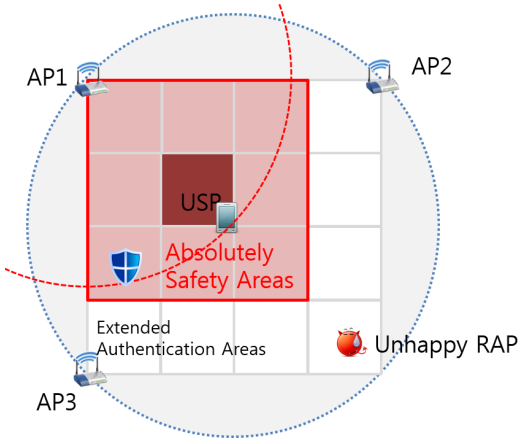


그림 6. 인증 영역의 확장
Fig. 6. Extension of the authentication areas

용자는 AP1과 위장 AP로부터 동일한 비콘 프레임을 수신할 것이다. 그리고 이 둘 모두 사용자의 전파 반경에는 속해있지만 서로의 전파는 받지 못하는 상황이다. 사용자가 운이 나빠서 위장 AP에 접속이 되어 통신 서비스를 이용하는 경우, 사용자의 데이터프레임은 이 둘 모두에게 전달된다. 이는 AP1의 입장에서 굉장히 이상한 일이다. 자신과 결합을 맺지 않은 어떤 사용자가 자기에게 데이터프레임을 보내는 상황이기 때문이다. 이러한 경우 AP1은 사용자가 현재 자신의 정보를 복제한 위장 AP를 통해 인터넷 통신을 하는 것이라 판단하여 연결해제 프레임(disassociation frame) 또는 인증해제 프레임(deauthentication frame)을 사용자에게 보냄으로써 위장 AP와 맺어진 결합을 해제시킬 수 있다. 이 경우 사용자는 무선 인터넷 서비스를 이용할 수 없게 되지만, 개인 정보 유출의 위협으로부터 보호받을 수 있다.

그러나 이 경우 그림에서 알 수 있다시피, 여전히 많은 영역에서 멤버십 테스트가 수행되지 않기 때문에, 무선 AP가 해당 영역에 존재한다면, 통신 반경 안에 있어도 멤버십 테스트에 실패하게 된다.

반면, 그림 7처럼 통신 반경 안에 위치한 무선 AP(정상)를 상당부분 정상적으로 인증하기 위해서 25개의 구역을 테스트하는 경우를 생각해볼 수 있다. 이 경우 통신 반경 R보다 멤버십 테스트 영역이 넓기 때문에, 그림 6과 같은 문제가 발생하지는 않는다. 그러나 멤버십 테스트 영역 중에 통신 반경보다 더 먼 위치에 무선 AP가 존재하면 어떠한 공격자는 해당 무선 AP로 자신의 위장 AP를 위장할 수 있게 된다. (위장 AP와 사용자는 통신 반경 안에 위치한다.) 역으로 생각해보면, 어떠한 무선 AP가 있으면 그 무선 AP로 위

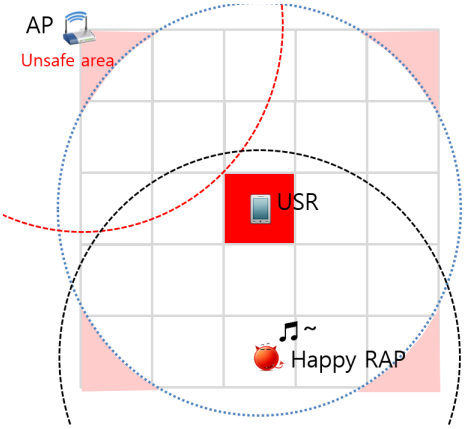


그림 7. 지나친 확장과 그로 인해 발생 가능한 위협
Fig. 7. Excessiveness extension and possibility of threats

장하고도 사용자에게 발각되지 않는 위치가 항상 존재한다는 것이다. 이는 "위험한 영역"의 크기가 멤버십 테스트를 통과하는 영역에 비해서 상대적으로 매우 작다고 안전성에 대해서 무시하면 절대로 안 되는 이유이다.

4.3 다단계 멤버십 테스트

우리는 무선 AP에 대한 멤버십 테스트의 성공률을 높이기 위하여 그림 8과 같이 단위 거리의 $\delta/2$에 해당하는 멤버십 구조체를 이용하여 인증 영역을 확대할 수 있다. 사용자는 우선 단위거리 δ에 해당하는 구조체 $\mathbb{F}_1$에 멤버십 테스트를 수행하고, 멤버십 테스트에 실패하면 단위 거리 $\delta/2$에 해당하는 구조체 $\mathbb{F}_2$에 대해서 멤버십 테스트를 수행한다. 각각의 멤버십 테스트는 (d_{lat}, d_{lng})와 $(d_{lat}/2, d_{lng}/2)$를 기준으로 (t_{lat}, t_{lng})와 $(t_{lat}/2, t_{lng}/2)$에 대한 대한 것이다. 세로 가로의 길이가 각각 (d_{lat}, d_{lng})인 사각형 영역은 최소 13곳부터 최대 17곳까지, $(d_{lat}/2, d_{lng}/2)$ 경우 최소 24곳부터 최대 37곳에 대해 멤버십 테스트를 수행하게 된다. 물론 이미 구조체 $\mathbb{F}_1$에서 테스트된 지도상의 영역에 대해서 구조체 $\mathbb{F}_2$에서 중복하여 테스트할 필요는 없다.

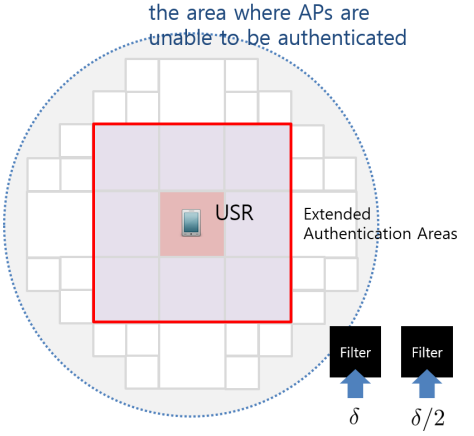


그림 8. 유저의 위치에 기반을 둔 인증영역의 확장예시
Fig. 8. An example for extending the authentication areas based on user's location

V. 시뮬레이션 및 결과 분석

5.1 실험 준비

우리는 SK텔레콤의 T와이파이존 정보를 수집하여 시뮬레이션에 이용하였다. 인터넷을 통해 얻을 수 있는 총 136,450개의 T와이파이존 정보중 약 11.4% 가량은 주소가 잘못 기재되어 다음지도, 네이버지도, 구글맵에서 검색되지 않아 이용하지 못했지만, 나머지 88.6%의 정보는 지오코딩(Geocoding) API를 이용하여 GPS 좌표로 변환하는데 큰 어려움이 없었다[14-16]. MAC 주소와 채널정보는 인터넷을 통해 얻을 수 없는 정보이므로 임의로 생성하였다. 우리는 각 실험 당 하나의 무선 AP를 임의로 선택하고, 이 위치로부터 각각 $R/6, 2R/6, \cdots, 6R/6$ 거리 이내에 위치한 사용자를 임의로 생성하였다. 이 후 사용자의 위치를 중심으로, 무선 AP를 신뢰할 수 있는지 여부를 테스트하였다. 실험은 한 라운드 당 각 거리에 대해 100회씩, 총 6,000회에 걸쳐 진행되었다. 그림 9는 이러한 실험을 수행한 시뮬레이터를 보여준다.

5.2 실험 결과 및 분석

표 2는 거리에 따른 신뢰성 테스트 통과율을 보여준다. $0 \sim 2R/6$ 범위는 그림 8에서의 테두리가 굵은 사각형영역 내부로, 사용자와 무선 AP의 위치가 매우 근접하여 100%의 신뢰성 테스트 성공률을 보인다. 하지만 이 범위를 넘어서 스마트폰과 무선 AP의 거리가 멀어질수록 멤버십 테스트의 성공율은 다소 낮아지는 모습을 보인다. $4R/6 \sim 5R/6$ 범위에서 낮아지기 시작하여 해당 범위에서는 97.70%로 성공하였으며, $5R/6 \sim R$ 범위에서는 평균 34.70%로 낮아진다. 스마트폰의 통신 반경에 포함되어있다 하더라도 멤버십 테스트가 실패하는 이유는 스마트폰의 반경 안에 '신뢰할 수 없는' 영역이 존재하기 때문이다. 그림 8을 예로 들면, 스마트폰의 통신반경에는 속하지만 사각형 영역에는 속하지 않는 영역 모두가 신뢰할 수 없는 영

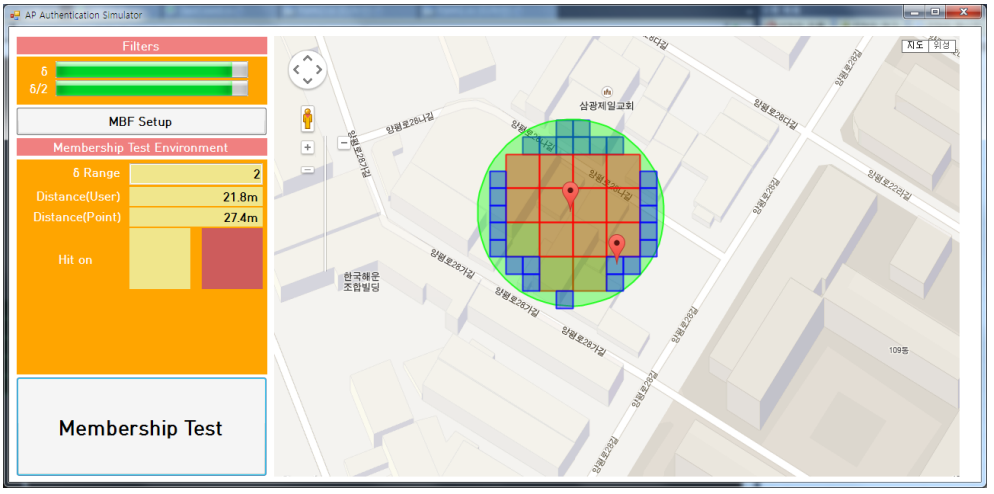


그림 9. 멤버십 테스트 시뮬레이터 (C#, Google map API, SKT T-WiFi Zone)
Fig. 9. Membership test simulator (C#, Google map API, SKT T-WiFi Zone)

표 2. 사용자와 AP사이의 거리에 따른 멤버십 테스트의 성공률 (%)
Table 2. Success and failure rates of membership tests according to the distances between user and WLAN AP (%)

	$R/6$	$2R/6$	$3R/6$	$4R/6$	$5R/6$	R
1	100	100	100	100	98	33
2	100	100	100	100	98	30
3	100	100	100	100	99	40
4	100	100	100	100	97	37
5	100	100	100	100	97	39
6	100	100	100	100	100	29
7	100	100	100	100	99	39
8	100	100	100	100	98	35
9	100	100	100	100	94	33
10	100	100	100	100	97	32
Average	100	100	100	100	97	34
Std.dev	0.0	0.0	0.0	0.0	1.6	3.9

역이 된다. 이 영역을 신뢰하기 위해 인증영역을 무리하게 확장하면 그림 7과 같은 상황에 놓일 것이고, 사용자는 공격자로부터 안전하지 않은 경우가 발생할 수 있다. 이러한 영역이 존재함으로써 결과적으로 사용자의 편의성이 낮아지게 되지만, 적어도 사용자가 위장 AP에 접속하는 일은 발생하지 않으므로 안전성을 최대로 높였을 때 잃게 되는 기회비용이라고 할 수 있다. 현실적으로 스마트폰의 최대 반경에 인접한 무선 AP는 사용자에게 원할한 서비스를 제공하기 어렵기 때문에 이렇게 잃는 기회비용이 크다고 보긴 어렵다. 예를 들어, Keenan-Motley의 자유 공간 전파 손실 모델에 따르면 스마트폰의 최대 통신반경이 $30m$라고 할 때, 실내의 선형 경로 손실 상관계수 $\alpha = 0.44dB/m$경우 신호는 $-83dB$까지 (5Ghz대역의 경우 $-90dB$까지) 감쇄하여 사실상 무선랜 서비스를 원활하게 이용하기 어렵다[17,18].

표 3은 무선 AP의 멤버십 테스트가 성공하는 경우, 평균적으로 수행되는 연산횟수를 보여준다. $0 \sim 2R/6$ 범위는 그림 8에서 볼 수 있는 테두리가 굵은 사각형 영역 내부로, 단위거리가 δ인 필터만을 이용하여 충분히 신뢰성이 인증됨을 알 수 있다. 무선 AP가 사용자로부터 멀어질수록 신뢰성 테스트 수행 횟수가 늘어남을 알 수 있다. 멤버십 테스트에 실패하는 경우 (d_{lat}, d_{lng})에 의해 나뉜 공간에서 평균 15.36회, $(d_{lat}/2, d_{lng}/2)$에 의해 나뉜 공간에서 평균 24.19

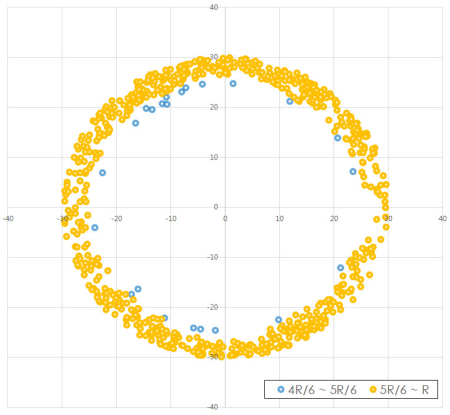


그림 10. 멤버십 테스트에 실패한 AP의 분포
Fig. 10. The distribution of APs which failed to membership test

표 3. 사용자와 AP의 거리에 따른 멤버십 테스트의 평균 수행 횟수 (성공한 경우만)
Table 3. The number of membership tests according to the distances between user and WLAN AP (when membership tests success)

	$R/6$		$2R/6$		$3R/6$		$4R/6$		$5R/6$		R	
	δ	$\delta/2$	δ	$\delta/2$	δ	$\delta/2$	δ	$\delta/2$	δ	$\delta/2$	δ	$\delta/2$
1	15.31	0	15.25	0	15.3	0	15.04	0.72	15.27	9.7	15.21	14.76
2	15.29	0	15.26	0	15.26	0	15.25	1.09	15.27	7.95	15.03	15.37
3	15.34	0	15.24	0	15.39	0	15.12	0.82	15.19	9.33	15.28	12.53
4	15.18	0	15.32	0	15.09	0	15.24	1.08	15.35	9.55	15.22	9.68
5	15.34	0	15.14	0	15.25	0	15.24	1.44	15.34	6.82	15.51	13.87
6	15.11	0	15.37	0	15.41	0	15.36	1.99	15.18	7.36	15.31	12.79
7	15.17	0	15.11	0	15.22	0	15.28	0.66	15.31	8.9	15.31	12.51
8	15.18	0	15.26	0	15.22	0	15.29	0.9	15.38	9.53	15.11	13.6
9	15.12	0	15.14	0	15.3	0	15.21	0.44	15.32	6.02	15.48	12.27
10	15.38	0	15.25	0	15.14	0	15.34	1.26	15.31	8.44	15.19	13.31
Average	15.24	0	15.23	0	15.26	0	15.24	1.04	15.30	8.36	15.27	13.79
Std.dev	0.10	0	0.08	0	0.10	0	0.10	0.45	0.07	1.28	0.15	1.56

회 테스트를 수행한다. 신뢰성이 검증되지 않음 확인하기 까지 약 40회의 테스트가 수행되지만 현재의 스마트폰의 연산 능력으로 미루어보아 크게 부담되지는 않을 것이다.

그림 10은 멤버십 테스트에 실패한 무선 AP들의 분포를 보여준다. 앞선 실험 결과에서도 보여주다시피, $4R/6$보다 가까운 무선 AP들은 모두 성공하였으며, 멤버십 테스트에 실패한 무선 AP들은 사용자로부터 $5R/6$보다 멀리 떨어져 있었다. 특히나 대각선에 몰려 있는 경우가 실패할 확률이 더 높았는데, 그것은 통신 반경은 원형인데 반하여 이 연구에서 정사각형 영역을 기본으로 멤버십 테스트를 수행하기 때문으로 보인다. 따라서 이러한 부분을 다소 보완하기 위해서 정사각형 이외에 육각형이나 원형을 기본으로 하는 멤버십 테스트에 대한 연구가 필요할 것으로 보인다.

Ⅵ. 시스템 적용을 위한 고려 사항들

6.1 인증 팩터 f의 길이

공격자가 정상 AP인 것처럼 위장 AP를 위장하는 문제는, $f=|H(x)|_1^m$ 이므로 암호학적 해시 함수에 대한 2차 사전이미지(second pre-image)를 공격하는 문제로 볼 수 있다. 이는 암호학적 해시 함수 $(x,H(x))$에 대해 $H(x)=H(y)$인 $y\neq x$를 찾는 문제와 동일하다. 인증 팩터 f를 구성하는 모든 정보는 서비스 제공자로부터 주어진다. 2차 사전이미지 문제에서는 주어진 이미지의 크기가 m비트인 경우, 공격자가 0.5의 확률로 충돌을 찾기 위해서는 평균 2^{m-1}만큼의 공간을 검색해야한다. SK텔레콤의 T 와이파이존이 13만 개라고 할 경우, 2^{17}개의 사전 이미지가 주어진 것으로 볼 수 있다. 따라서 공격자의 능력이 다항식 시간에 $2^{m'}$만큼의 공간을 검색할 수 있다고 할 때, 인증 팩터의 길이 $m\geq m'+17+1$비트이면 된다. 예를 들어, $m=80$이면 T 와이파이존에 대해서 다항시간에 2^{64}만큼의 공간을 검색할 수 있는 공격자에 대해 안전하다고 할 수 있다. 한 편, 2^{17}개의 사전 이미지가 주어졌을 때, 내부 충돌이 발생할 가능성이 50% 이하이기 위해서는 $m\geq 34$이어야 한다[19]. $m=80$일 때, T 와이파이존이 13만 개에 대한 구조체 $(\mathbb{F}_1,\mathbb{F}_2)$의 크기는 2.48 MB 정도이다.

사용자의 스마트폰에 내장된 멤버십 구조체$(\mathbb{F}_1,\mathbb{F}_2)$를 수정하여 위장 AP가 인증되게끔 만드는 공격에 대한 대응방법은 이 논문의 요지를 벗어나므로 다루지 않는다.

6.2 블룸 필터를 이용한 멤버십 테스트

멤버십 테스트를 수행하는데 이용될 수 있는 구조체 중에서는 잘 알려진 블룸필터(Bloom filter)가 있다. 블룸필터는 B. H. Bloom이 1970년에 고안한 데이터구조로, 밀집되지 않은 데이터를 저장할 수 있다. 블룸필터는 기본적으로 데이터의 저장과 검색을 위해 다수의 해시함수를 이용하기 때문에 긍정오류(false positive)가 발생한다. 블룸필터는 사용자가 패스워드를 결정하는 순간 약한 패스워드를 선택하지 못하도록 도울 수 있으며, 이 때 발생하는 긍정오류는 시스템 운영에 큰 영향을 미치지 않는다[20].

하지만 이 논문에서 제안하는 기법을 블룸필터를 통해 구현할 때에는 주의가 따른다. 긍정오류는 곧 공

격자의 위장 AP가 신뢰할 수 있는 AP라고 응답하는 것이기 때문이다. 따라서 긍정오류발생확률을 고려하여 충분한 안전성을 가지도록 입력 n에 대해서 적당한 수의 해시 함수들과 블룸필터의 크기를 가지고 설계해야 하나, 이런 경우 해시의 결과를 잘라서 사용하는 것에 비해 특별한 이득이 없다는 것은 맹영재 등에 의해서 잘 증명되었다[21].

6.3 GPS 정확도와 연산량, 구조체의 크기에 대한 고려

멤버십 테스트를 위한 연산량과 구조체의 크기를 희생하더라도 사용자 편의성을 더 높이기 위해서는 단위 거리 δ와 $\delta/2$에 대한 멤버십 테스트뿐만 아니라 $\delta/4$, $\delta/8$처럼 더 작은 영역에 대해 멤버십 테스트를 수행할 수 있다. 그러나 GPS의 정확도는 수 m이내이기 때문에[22] 단위 거리를 무한정 줄일 수만은 없다. 무선랜카드의 수신 감도에 따라 다르지만, Keenan-Motley 자유 공간 전파 손실 모델에서 $R \geq 30$인 경우, 일반적으로 무선랜 통신이 원활하지 않다고 볼 수 있다[18,19]. $R=30m$인 경우 $\delta \approx 10.61m$정도이기 때문에, $\delta/4 \approx 2.65m$, $\delta/8 \approx 1.33m$가 되어 GPS 정확도의 한계에 다다르게 된다. 따라서 우리의 기법에서 다단계 멤버십 테스트는 2단계 이상을 넘기가 현실적으로 어려워 보인다.

6.4 이미 설치된 무선 AP에 대한 적용가능성

5.1절에서 지오코딩(Geocoding) API를 이용하면 현재 이동통신사가 설치 및 운영 중인 무선 AP의 주소로부터 GPS 좌표를 얻는 것이 어렵지 않음을 기술하였다. 특히 구글의 지오코딩 API를 이용하면 무선 AP의 맥주소만 알아도 매우 정밀한 GPS 정보를 얻을 수 있다. 따라서 현재 설치 및 관리되는 와이파이 핫스팟 정보에 지오코딩 과정만 거치면 이 논문에서 제시하는 서비스를 어렵지 않게 구현할 수 있을 것이다. 하지만 GPS좌표는 위도와 경도만을 보여주기 때문에, 한 빌딩의 서로 다른 층에 위장 AP와 신뢰할 수 있는 AP가 있는 경우 이 논문에서 제시하는 기법으로는 이 둘을 구분하기 어렵다. 또한 버스, 지하철 등에 설치된 이동형 와이파이 핫스팟의 경우 설치된 위치가 유동적이기 때문에 이 논문에서 제시하는 기법으로는 무선 AP의 신뢰성을 테스트하기 어렵다. 그럼에도 불구하고 이 논문의 결과는 SSID만 동일하게 설정하면 어디서든 공격이 성공하는 현재의 상황에 비해서 공격자의 자유도를 크게 제한함으로써 공격이 어렵도록 만든다는 관점에서 의미있다고 할 수 있다.

이 연구의 결과는 이동통신사뿐만 아니라 2017년까지 1만 2천여 개의 와이파이 핫스팟을 구축할 예정인 공공와이파이[23], 기업에서 제공하는 와이파이 핫스팟 등에 적용될 수 있으며, 사용자가 보다 안전하게 무선 AP에 접속할 수 있도록 도울 것이다.

6.5 고도를 고려한 인증방법

이 논문에서는 해결하기 어려운 다양한 문제로 인해 고도를 고려하지 않는다. 일단, '주소' 정보에는 고도가 포함되어 있지 않아 지오코딩 API를 이용할 수 없어 AP의 위치를 직접 측량해야한다. 무엇보다도 고도를 고려하는 경우 3차원 공간에서의 인증을 고려해야하는데, 이는 생각보다 어려운 문제이다.

예를 들어, 고층 빌딩에 사용자와 신뢰할 수 있는 AP가 그 높이로 인해 서로 통신할 수 없는 위치에 존재한다고 가정하자. 사용자와 AP의 위치를 평면상의 좌표로 정사영시키면 논리적으로 AP는 스마트폰의 전파 반경 안에 포함된다. 공격자는 이를 이용하여 위장 AP를 설치하고 사용자의 접속을 유도할 수 있을 것이다. 이는 이미 6.4절에서 기술한바와 같이 이 기법에서는 해결하기 어려운 문제이다. 다만 높낮이까지 고려하여 AP를 인증한다면 사용자와 AP의 위치를 평면상으로 정사영시키는 것보다는 3차원 공간을 그대로 이용하여 이러한 문제를 해결할 수 있을 것이다. 하지만 이 경우 멤버십 테스트를 수행해야하는 영역을 결정하기가 무척 어렵다. 자유공간에서 전파는 구형으로 전송되지만, 실내 공간이나 빌딩 내부에서는 그 모양이 완벽한 구형을 이루지 않기 때문이다.

뿐만 아니라 사용자의 통신 반경이 입체적인 모양을 갖기 때문에 멤버십 테스트의 횟수가 크게 증가하게 된다. 또, 평면이 아니라 공간을 분할해야하기 때문에 높낮이는 필연적으로 수직으로 잘려질 수밖에 없다. 예를 들어, 사각 기둥의 경우 작은 사각 기둥을 도입하는 것으로 공간을 8등분 할 수 있다. 이 경우 평면에서와 경우와 동일하게 2개의 멤버십 구조체만 사용할 수 있다. 고도를 고려한 멤버십 테스트의 경우, 그 테스트 횟수가 고도를 고려하지 않았던 경우보다 약 제곱근배로 늘어나게 된다. 원의 넓이는 πr^2이며, 구의 부피는 $4\pi r^3/3$이므로, 평면에서 약 $15 \sim 30$회 정도 요구되었던 멤버십 테스트의 수행횟수는 3차원 공간에서 대략 $77 \sim 219$회 정도로 늘어나게 된다.

Ⅶ. 결론 및 향후 연구방향

이 논문에서는 사용자가 기업망 또는 이동통신사에

서 제공하는 무선 AP를 신뢰하고 접속하는 방법에 대해 논의하였다. 지금까지 무선랜에서의 인증은 무선 AP 또는 서비스 제공자 입장에서만 다루어져왔다. 이 연구의 결과는 사용자 입장에서 접속하려는 무선 AP가 실제로 서비스 제공자가 설치한 것인지 여부를 확인할 수 있게 되었다는 점에서 큰 의미를 가진다. 또한 이 논문에서 제시한 방법은 공격자의 공력능력을 크게 제한하는 효과도 갖추어 위장 AP를 설치하고 서비스 이용자의 개인정보를 노리는 공격자로부터 사용자를 보호할 수 있다. 하지만 무선 AP를 인증하는 방식에 있어서 동일한 성질의 멤버집합을 두 개나 만들어 배포해야 한다는 점이 아직도 해결해야 할 문제로 남는다.

또한 스마트폰의 전파반경은 원형임에도 불구하고 무선 AP를 인증하기 위한 단위 영역은 사각형으로 설정함으로써 발생하는 인증불가영역을 줄이는 것도 해결해야할 것이다. 이에 우리는 단위 영역을 정육각형으로 나누고, 일부 영역에 대해선 겹치는 것을 허용함으로써 멤버십 구조체를 하나로 통일하면서도 인증불가영역을 줄일 수 있는 더욱 진보된 방법에 대해 연구할 것이다.

References

[1] Editors of IEEE 802.11, “Wireless LAN medium access control (MAC and physical layer (PHY) specification, draft,” *Standard IEEE 802.11*, 1997.

[2] I. Kim, J. Cho, T. Shon, and J. Moon, “A method for detecting unauthorized access point over 3G network,” *J. The Korea Institute of Information Security & Cryptology(JKIISC)*, vol. 22, no. 2, pp. 259-266, Apr. 2012.

[3] S. Kang, D. Nyang, J. Choi, and S. Lee, “Relaying rogue AP detection scheme using SVM,” *J. The Korea Institute of Information Security & Cryptology(JKIISC)*, vol. 23, no. 3, pp. 431-444, Jun. 2013.

[4] H. Han, B. Sheng, C. C. Tan, Q. Li, and S. Lu, “A measurement based rogue ap detection scheme,” in *Proc. INFOCOM*, pp. 1593-1601, Rio de Janeiro, Brasil, Apr. 2009.

[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 Distributed Syst.*, vol. 22, no. 11, pp. 1912-1925, Nov. 2011.

[6] A. J. Nicholson, Y. Chawathe, M. Y. Chen, B. D. Noble, and D. Wetherall, “Improved access point selection,” in *Proc. MobiSys ’06*, pp. 233-245, NY, Jun. 2006.

[7] D. Denning and P. Macdoran, “Location-based authentication: Grouding cyberspace for better security,” *Computer Fraud & Security*, vol. 2, pp. 12-16, Feb. 1996.

[8] H. Takamizawa and K. Kaijiri, “A web authentication system using location information from mobile telephones,” in *Proc. IASTED Int’l Conf. Web-based Education*, pp. 31-36, Phuket, Thailand, Mar. 2009.

[9] F. Zhang, A. Kondoro, and S. Muftic, “Location-based authentication and authorization using smart phones,” in *Proc. Trust, Security and Privacy in Computing and Commun. (TrustCom)*, pp. 1285-1292, Liverpool, UK, Jun. 2012.

[10] Korea Internet & Security Agency, *Wireless LAN security guide*, Dec. 2011.

[11] SKT, *T Wi-Fi zone*, Retrieved Dec., 5, 2013, from http://www.twifi.co.kr/.

[12] KT, *olleh Wi-Fi zone*, Retrieved Dec., 5, 2013, from http://zone.wifi.olleh.com/.

[13] LG U+, *U+ Wi-Fi zone*, Retrieved Dec. 5, 2013, from http://www.wifiworld.co.kr/main.s2.

[14] Daum DNA Developer Network, *Local API*, Retrieved Dec. 5, 2013, from http://dna.daum.net/apis/local.

[15] Naver Developer Center, *Map API*, Retrieved Dec. 5, 2013, from http://developer.naver.com/wiki/pages/MapAPI.

[16] Google Developers, *Google Maps API*, Retrieved Dec. 5, 2013, from https://developer s.google.com/maps/.

[17] IEEE Report 802.11-03/845r1. (2003). Receiver sensitivity tables for MIMO-OFDM 802.11n, Nov. 2003.

[18] J. M. Keenan, and A. J. Motley, “Radio coverage in buildings,” *J. British Telecom Technol.*, vol. 8, no. 1, pp. 19-24, Jan. 1990.

[19] B. Schneier, *Applied Cryptography, Second Edition*, John Wiley & Sons, 1996.
[20] E. Spafford, "Opus: Preventing weak password choices," *Computer and Security*, vol. 11, pp. 273-278, May 1992.
[21] Y. Maeng, K. Kang, D. Nyang, and K. Lee, "On nessage length efficiency of two security schemes using bloom filter", *KIPS Trans.: Part C*, vol. 19C, no, 3, pp. 173-178, Jun. 2012.
[22] S. von Watzdorf and F. Michahelles, "Accuracy of positioning data on smartphones," in *Proc. 3rd Int'l Workshop on Location and the Web (LOCWEB)*, Article no. 2, NY, USA, Nov. 2010.
[23] Ministry of Science, ICT and Future Planning, *Plan to increase the number of public Wi-Fi zones to 12,000 by 2017,* Retrieved Jul., 12, 2013, from http://www.msip.go.kr.

신 동 오 (DongOh Shin)

2010년 2월 : 인하대학교 컴퓨터 정보공학과 공학사
2012년 2월 : 인하대학교 컴퓨터 정보공학과 석사
2012년 9월~현재 : 인하대학교 컴퓨터 정보공학과 박사과정
<관심분야> 인터넷 보안, 네트워크 보안, 금융 보안

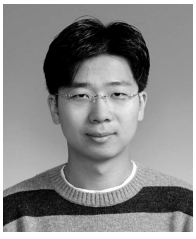
강 전 일 (Jeonil Kang)

2003년 2월 : 인하대학교 컴퓨터 공학과 학사
2006년 2월 : 인하대학교 정보통신공학과 석사
2006년 3월~현재 : 인하대학교 정보통신공학과 박사과정
<관심분야> 인식 보안, WSN 보안, 무선 인터넷 보안, 웹 인증 보안

양 대 헌 (DaeHun 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 부교수
<관심분야> 암호이론, 암호프로토콜, 인증프로토콜, 무선 인터넷 보안

이 석 준 (Sokjoon Lee)



1998년 2월 : 서울대학교 컴퓨터 공학과 졸업
2000년 2월 : 서울대학교 컴퓨터 공학과 석사
2000년 2월~현재 : 한국전자통신연구원 사이버보안연구본부 선임연구원
2010년 9월~현재 : KAIST 전산학과 박사과정
<관심분야> 무선랜 보안, 인증 프로토콜, 암호 이론

이 경 희 (KyungHee Lee)

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