https://doi.org/10.14400/JDC.2017.15.7.201

모바일 환경에서의 공격자 위치 특정 및 알람 기법

봉진숙, 박상진
숭실대학교 컴퓨터학과

A Location Recognition and Notification Method of Attacker in Wireless Network Environment

Jin-Sook Bong, Sang-Jin Park
Dept. of Computing, Soongsil University

요 약 유동 IP와 모바일 IP를 사용하는 무선 네트워크 기술은 사용자에게 접속과 이동의 편의성을 제공한다. 그러나, 이러한 IP 기술들은 악의적인 사용자에게 정상 사용자를 위장하여 네트워크 및 서비스에 접속할 수 있는 기회를 제공하기도 한다. 이에 본 논문은 네트워크 관리자와 서비스 제공자가 악의적인 사용자의 네트워크 및 서비스에 대한 접근 의도를 빠르게 인지하고, 악의적인 사용자의 위치를 특정하여 적절한 대응을 할 수 있도록 wifi, LTE 네트워크의 사용자 정보를 통합 관리하는 개체(W_L_M)와 위치 특정과 알람을 위한 메시지를 정의하고 그 절차를 제안하였다. 본 논문의 성능 평가는 정성적 분석을 통해 이루어졌으며 제안기법의 적용으로 인해 일부 새로운 비용이 발생하나 전체 네트워크 운용비용 대비 적은 수준으로 분석 되었다. 본 논문의 제안은 기존의 유, 무선네트워크 정보와 구조를 활용한 관리적인 방법으로 네트워크의 보안성을 높이고자 할 때, 참고 자료로 활용 될 수 있다.

주제어 : 공격자 위치 특정, 알람, LTE-wifi연동, 모바일, 보안

Abstract Wireless network using dynamic IP and mobile IP technology provides the user with convenience of access and movement. However, this causes the attacker who disguises normal user(pretending to be a regular user) to have more opportunity in regard to access and acquisition of information. This paper help the network administrator and the service provider quickly to recognize the attacker's intention to access network and service. Therefore network administrator and service provider can specify and respond the location of the attacker appropriately. To achieve above, we define an entity (W_L_M) that manages user information of WiFi and LTE network, and propose messages and procedures for attacker's location identification and alarm. The performance evaluation of this paper is based on qualitative analysis. By using the proposed method, some cost (message creation, processing and transmission) occurred but it was analyzed to be less than the total network operation cost. The proposal of this paper is a management method that utilizes existing network information and structure. This method can be used as a reference material to enhance security.

Key Words : Attacker's location recognition, Alarm, LTE-wifi interworking, Mobile, Security

Received 8 May 2017, Revised 26 June 2017
Accepted 20 July 2017, Published 28 July 2017
Corresponding Author: Sang-Jin Park
(Dept. of Computing, Soongsil University)
Email: neoparking@ssu.ac.kr

1. 서론

1.1 연구 배경 및 목적

4G, LTE의 이동통신 네트워크와 wifi 네트워크 등 무선 기술의 발전은 스마트 디바이스의 활용을 극대화 할 수 있는 다양한 서비스(IoT, O2O, 핀테크 등)를 가능하게 하였다. 그리고 사용자들은 시간과 공간의 제약 없이 네트워크에 접속할 수 있어 무선 네트워크 이용 시간은 더욱 증가하게 되었다.

이로 인해 공격자는 사용자 정보(IP 등)에 보다 쉽게 접근, 획득할 수 있는 환경이 되었고, 이동성이라는 무선 네트워크의 특성으로 인해 다양한 시간과 장소에서 공격이 발생 할 수 있게 되었다[1, 2, 3].

따라서, 모바일 환경에서는 공격자의 공격의도를 가능한 빠른 시간 안에 파악하고 대처하며, 더하여 공격자의 위치를 특정하는 기술이 필요하게 되었다. 현재까지 연구된 기술은 유선 네트워크를 기반으로 한 IP 추적 기술이 주류를 이루고 있으며[4, 5], 무선 쪽으로는 ad hoc 네트워크에서의 역추적 기술이 일부 연구[6, 7] 되었으나 이러한 기술을 그대로 현실의 무선 환경에 적용하기에는 어려운 점이 있다.

본 논문에서는 wifi, LTE 등 무선 환경의 특징을 이해하고 이동의 자유로움으로 인해 더욱 어려워진 공격자의 위치를 특정하고자, 멀티 인터페이스(LTE, wifi 인터페이스)를 활용한 공격자의 위치 특정 및 알람 기법을 제안한다. 이를 통해 사용자는 보다 빠르게 공격자의 공격에 대처할 수 있다.

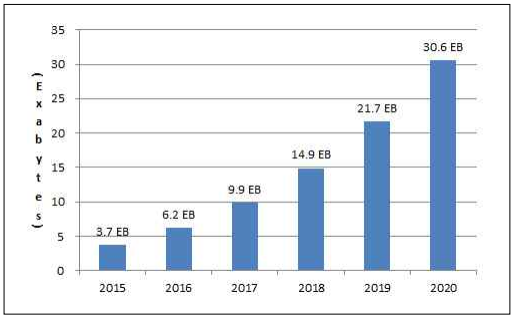
2. 관련연구

본 장에서는 무선 네트워크의 특징을 이해하고 현재까지 연구된 추적 기술들이 무선 공격자의 위치 특정에 적용 가능한지 확인하고자 한다. 이를 위해 wifi, LTE 네트워크를 기술 동향, 인증, 보안의 측면에서 조사하고 이와 더불어 기 연구되었던 유·무선 공격자 역추적 기술에 대해 조사하였다.

2.1 무선랜(wifi)의 특징

2.1.1 무선랜 동향

이동 단말을 이용한 고화질 비디오 스트리밍 감상 및 사물인터넷(IoT)의 활용 등 증가하고 있는 모바일 데이터[Fig. 1]의 적절한 처리를 위해 무선랜 쪽에서도 다양한 표준들이 연구되고 있다[8, 9].



[Fig. 1] Mobile data traffic forecast
Source: CISCO VNI global mobile data traffic forecast

전송속도를 높이기 위한 802.11ac, 802.11ad, 서비스 확장을 목적으로 넓은 커버리지를 수용할 수 있도록 하는 802.11af, 802.11ah, 신속한 접속을 가능하게 하는 802.11ai가 그것이다. 이처럼 속도 향상 및 넓은 서비스 커버리지 수용은 wifi 발전의 중요한 요소가 되고 있다.

2.1.2 무선랜 인증

무선랜은 무선 보안적용 방식에 따라 <Table 1>과 같이 구분된다[10].

<Table 1> Wireless LAN authentication technique

Classification	Authentication	Characteristic	Confidentiality
Pre-RSNA	- Open system Authentication	- No Authentication, only require SSID - Check MAC address of mobile device	- WEP
	- Shared-Key Authentication	- Check pre-shared key already setup between mobile device and AP	
RSNA (Robust Security Network Association)	- EAP (Extensible Authentication Protocol)	- Encryption key is derived from dynamically generated key through authentication procedure	- CCMP - TKIP

PreRSNA기법에서는 무인증 또는 단말을 확인하는 정도 수준으로 인증을 수행하며 RSNA는 보다 수준 높은 인증을 제공하기 위하여 새로운 하드웨어 및 소프트웨어를 필요로 한다.

2.1.3 무선랜 보안 취약점

무선랜은 무지향성 전파를 이용하므로 전파 수집 및 교란을 통한 다양한 보안위협이 발생할 수 있다[11, 12, 13]. 무선랜은 통신 단계[14]뿐 아니라 접속 설정 단계(① 채널 탐색, ② 인증, ③ IP할당, ④ 터널 생성)에서조차 많은 보안 취약점이 존재한다.

채널 탐색 단계에서 공격자는 스니핑을 통해 AP의 정보를 획득할 수 있으며, 다량의 probe request 메시지를 전송하여 AP가 response 회신을 반복하게 함으로써 정상적인 이동 단말의 접속을 방해할 수 있다. 또한 공격자는 위조된 AP를 이용하여 강력한 전파를 송신함으로써 정상적인 이동 단말을 유인할 수도 있다. 인증 단계에서는 공격자가 스니핑을 통해 획득한 AP 정보를 이용하여 무선랜에 접속할 수 있으며 (AP에 별도의 암호화 방식 또는 인증절차가 설정되어있지 않은 경우), 무선구간에서 사용되는 WEP, WPA/WPA2 의 키 값 추출 혹은 유추를 통해 AP에 접속할 수 있다. 또한 공격자는 불법 AP를 이용하여(인증 및 암호화에 WEP 이용) 이동 단말의 인증 정보와 무관하게 접속을 허용한 후, 이동 단말의 개인정보를 탈취할 수 있다.

이처럼 무선랜은 전파를 이용한 정보 전송의 특징으로 인해 도청이 용이 하며 도청된 정보가 암호화 되어 있지 않거나 취약한 암호화 정책을 적용하는 경우 해킹을 통한 도청이 가능하다.

2.2 LTE 네트워크의 특징

2.2.1 LTE 동향[15]

소형셀은 급증하는 모바일 트래픽으로 인한 망의 과부하 및 사용자 서비스의 품질저하 이슈 해결을 위하여 사용된다. 이동통신망 사업자들은 소출력의 적은 커버리지를 갖는 소형셀을 주거지, 도심 음영지 또는 핫스팟에 설치하여 적은 비용으로 단위면적당 용량 증대 및 사용자의 QoS(Quality of Service)를 높이고자 한다.

3GPP에서도 모바일 트래픽의 폭증을 해결하고 사용자의 QoS/QoE(Quality of Experience)를 향상하기 위한 기술로 소형셀 향상 기술과 매크로 기지국 커버리지 안에 소형셀 기지국[1]이 중첩된 HetNet(Heterogeneous Network)환경에 대한 연구 및 표준화를 진행하고 있다. 셀 크기의 소형화는 단위면적당 주파수 이용 효율을 증가시킬 수 있으므로(Martin Cooper의 법칙) 소형셀은 지속적으로 연구·발전 될 것으로 예상된다.

2.2.2 LTE 인증[16]

LTE 네트워크를 통한 사용자 단말(이하 UE)의 접속은 ① 인증, ② 보안설정, ③ IP할당, 보안설정, ④ EPS 세션 설정 등 4단계를 거쳐 진행된다.

LTE는 망과 가입자간에 EPS-AKA 방식을 사용하여 상호인증을 수행하기 위하여 UE와 HSS(가입자 DB)에 가입자 고유 식별자인 IMSI와 LTE Security Key인 LTE K 값을 가지고 있다. UE가 전원을 켜고 망에 인증 요청을 하면 이 메시지를 수신한 MME는 HSS에게 해당 가입자를 인증하기 위한 인증정보(Authentication Vector)를 받는다. MME는 이 인증정보를 이용하여 가입자를 인증하고, 또한 가입자도 HSS가 하는 것과 동일한 방식으로 망을 인증한다.

UE와 망간에 인증 과정이 성공적으로 끝나게 되면 그 결과로 Master Key가 생성되며, 이 Master Key를 사용하여 제어 메시지와 데이터 메시지 각각에 대해 무선구간에서 무결성 확인과 암호화를 할 수 있는 Key들을 생성한다. 이후 UE와 MME/eNB간에는 제어신호가 암호화 및 무결성 보호되어 전송되고, UE와 eNB간에는 트래픽이 암호화되어 전송되므로 안전하다.

2.2.3 LTE 보안 취약점

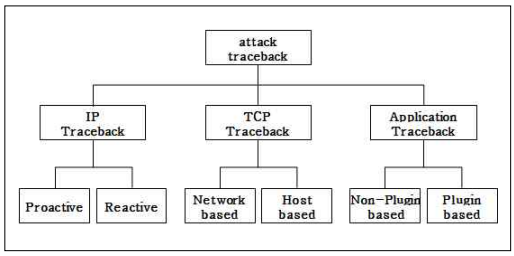
이동통신망은 서비스를 제공하는 이동통신사의 폐쇄적인 환경 때문에 외부에서의 접근이 어려웠으나 LTE(4G)로 넘어오면서 그 구조가 개방형으로 바뀜으로 인해 다양한 모바일 앱의 사용이 자유로워졌다. 이러한 환경 변화에 따라 모바일 악성코드의 증가로 감염 단말의 악성·비정상 트래픽이 이동통신 망으로 유입되고, 이로 인해 개인정보 또는 단말정보 유출, DDoS 공격 등 보안 위협이 발생할 수 있다.

1) 소형셀 기지국: 10~수백 m 정도의 소출력 커버리지를 갖는 기지국

2.3 기존의 역추적 기술 동향

2.3.1 유선 역추적 기술 동향[4,5]

역추적 기술은 공격에 사용되는 시스템의 위치와 실제 해킹을 시도하는 공격자의 위치가 다르더라도 공격의 근원지를 추적할 수 있는 기술이다[Fig. 2].



[Fig. 2] Classification of the traceback[4]

IP기반 역추적 기술은 사전에 저장된 역추적 경로정보 사용하여 역추적을 수행하는 proactive방식과 공격 발생 후 남겨진 시스템의 로그 분석 후 홉 단위 위치 추적을 수행하는 reactive 방식으로 나뉜다. proactive 방식에서 라우터는 경로 정보 수집에 관여하므로 라우터 인증이 필요하며 의도된 정보에 취약한 특징을 가진다. reactive방식은 기존 망에 장비 또는 SW에이전트의 추가적인 설치가 필요하며 로그파일을 의도적으로 삭제하는 경우 추적이 불가하므로 로그파일을 대체/보호하는 기법이 필요하다.

TCP기반 역추적 기술은 네트워크에 분산 설치된 모니터링 장치에 의해 추적을 수행하는 network-based 방식과 호스트가 직접 역추적에 참여하는 host-based 방식으로 나뉜다. network-based의 경우 추적 기능이 없는 네트워크 장비 및 ISP를 경유하는 경우 위치 추적이 불가능하며, host-based의 경우 의도된 정보에 노출된 호스트가 존재 할 수 있어 호스트 선별 기술이 필요하다.

Application기반 역추적 기술은 사용자 시스템에서 독립적으로 동작하는 non-plugin based 방식과 웹 브라우저나 OS 등에 부가적으로 동작하는 plugin based 방식으로 나뉜다. non-plugin based의 경우 피해자 PC(경유지 포함)의 OS, 메모리 상주 프로세스 및 로그분석 수행하기 위하여 해당 사이트나 세션 별로 별도의 플러그인 설치가 필요하며 백그라운드에서 사용자 행위에 대한 실시간 보안 추적 및 검사기능, 업데이트 기능이 제공된다. plugin-based의 경우 실시간으로 공격근원지에 대한 추적 및 대응이 가능하며 현행 시스템과 네트워크에 부하 없이 동작할 수 있다.

2.3.2 무선 역추적 기술 동향[6,7]

무선 역추적 기술은 유선에 비해 많이 연구되고 있지 않으며, 대부분이 ad hoc분야를 기반으로 연구되고 있다. 다음은 기 연구된 무선 역추적 기술을 정리하였다. 이 중 TTL 기반 패킷 마킹 기법만이 무선랜에서의 역추적 기술을 다루고 있다.

① SWAT(Small World-based Attacker Traceback): SWAT은 Contact 노드를 기준으로 지역을 나누고 지역별로 추적을 수행한다. 타협된 노드가 존재할 수 있어 잘못된 보고와 같은 잡음 트래픽이 많은 경우 역추적에 실패할 수 있다. 또한 역 추적 이후 대책 메커니즘을 제공하지 않는다.

② 크로스-레이어 모니터링(cross-layer monitoring): 기본 동작은 SWAT과 유사하나 SWAT의 문제점을 개선하고자 노력하였다. 시그니처 에너지를 사용하여 잘못된 보고를 줄이고자 하였고, 크로스-레이어 정보(네트워크, MAC 계층)를 역추적에 이용하였다.

③ 시간 태그 블룸 필터(time-tagged bloom filter): 클러스터 헤드 노드의 로그 정보를 활용하여 역추적을 수행한다. 네트워크를 클러스터로 나누고 클러스터 헤더 노드는 시간 태그 블룸 필터를 이용하여 로그정보 유지함으로써 로깅 기반 IP 역추적에서 토폴로지 변경 문제와 리소스 문제를 해결하였다.

④ TTL 기반 패킷 마킹 기법: 이상 트래픽에 삽입된 경로상의 라우터 및 AP의 IP주소를 이용하여 추적하는 기법이다. 라우터는 이상 트래픽을 발견하면 패킷에 마킹을 수행하고 자신의 IP 주소를 헤더 내에 삽입(해쉬 함수사용)하여 목적지로 전송한다. 이는 기존 패킷 마킹 기법이 확률적 방법으로 패킷에 마킹을 수행함으로써 많은 양의 패킷이 수집 되어야 추적 경로 확보할 수 있는 문제를 해결하였다.

2.4 분석

본 섹션은 wifi와 LTE네트워크를 특징, 인증, 보안취약점의 관점에서 비교·분석하고, 기 연구된 추적 기술을

현재의 IP 네트워크 적용 관점에서 분석하였다.

2.1.1에서 살펴본 바와 같이 무선랜은 속도 및 커버리지 면에서 다양하게 연구 발전하고 있으며 가정, 공공장소, 무선랜 핫스팟 등 다양한 장소에서 그 사용이 증가하고 있으나 무선랜 서비스에 있어 사용자 관리를 위한 등록 및 인증은 필수 요구사항이 아니다.

인증 및 암호화 측면에서(2.1.2), wifi는 EAP기반의 가입자 인증, 공유키 인증, 개방 인증 중의 하나를 수행하며 암호화도 AES-CCMP 암호화에 의해 보호되는 것을 권고하고 있으나 WEP 또는 TKIP과 같이 예전 암호화 알고리즘만 지원하는 경우가 발생하기도 한다.

반면 LTE 네트워크는 2.2.1에서와 같이 스몰셀 기술을 적용하여 셀의 반경을 좁힘으로써 망의 과부하를 해결하고 이동단말의 식별을 더욱 신속하게 하였다. 이는 LTE 인터페이스를 이용한 공격자의 위치 특정에도 유리하게 작용할 것으로 판단된다.

또한 LTE 네트워크는 MME(Mobility Management Entity)와 UE(User Equipment)간에 EPS-AKA 방식을 통한 상호인증(2.2.2)을 수행하고 Master key를 이용하여 무선구간에서의 무결성 확인 및 암호화에 사용되는 key들을 생성·이용함으로써 wifi보다 상대적으로 안전한 통신을 수행할 수 있다.

무선 환경에서의 공격자들이 유동 IP를 사용하여 공격을 수행하는 경우 2.3.1절에서 정리한 기존의 유선 추적 기술을 그대로 적용하기에는 한계가 있으며, 2.3.2절에서와 같이 주로 ad-hoc 네트워크를 대상으로 한 역추적 기법을 그대로 사용하기에도 무리가 있다고 판단된다.

이러한 분석의 결과를 토대로 본 논문에서는 LTE 인터페이스를 이용한 모바일 환경에서의 공격자 위치 특정 및 알람 기법을 제시하고자 한다.

3. 모바일 공격자 위치 특정 및 알람 기법

3장에서는 정상 사용자의 IP와 MAC을 스푸핑 한 후 wifi망을 이용하여 일반 서비스 서버 해킹을 시도하는 공격자가 있는 경우, 실제 공격자가 위치한 wifi 영역을 LTE 인터페이스를 활용하여 공격자의 위치를 특정하고 이를 사용자 단말에 알려주는 알람 기법을 제안한다.

3.1 가정

본 논문의 가정 사항은 다음과 같다.

- UE는 2개의 인터페이스(wifi, LTE)를 가짐
- LTE 인터페이스는 항상 on 상태임
- IDS가 일반 서비스 서버 영역을 감시하고 공격 징후가 있는 경우 W_L_M와 서버에게 알림
- AP와 서버는 트래픽 및 망 분리 기능을 가지고 있음
- 다수의 AP가 존재하며 이를 관리하기 위한 APC(AP Controller)들이 존재
- 공격자는 wifi 영역 또는 일반 서비스 영역의 서버 해킹을 통하여 사용자 정보를 획득

3.3절의 공격 시나리오에 사용되는 네트워크의 각 개체들에 대한 설명은 <Table 2>와 같다.

<Table 2> Network entity definition

Entity	role
UE/STA	- Mobile device having a LTE/wifi interface
eNB	- Called as LTE base station, connection providing via LTE interface between UE and EPC
S-GW	- Serves as an anchoring point for inter eNB handover
P-GW	- Serves as an anchoring point for inter S-GW handover - Assigns an IP address to a UE
MME	- Entity to authenticate UE - Mobility management of UE(position and status
HSS	- Save subscriber profile: subscriber ID(IMSI), authentication key, QoS profile and so on
AP	- Entity that allows a UE to connect to a wired network
ePDG	- Inserted entity to solve security problem of Untrust access network - Performing a authentication between UE and ePDG then tunnel creation
AAA	- Server to authenticate STA
IDS	- Performs a detection about server attacktion in general service area
W_L_M	- Management entity combined wifi and LTE information of UE · wifi: AP/APC that has completed connection setup provides IP and MAC information of UE · LTE: eNB provides IP and GUTI information of UE after forwarding IP address to UE

3.2 제안하는 W_L_M(wifi_LTE_Merge)개체

W_L_M는 wifi와 LTE 정보(MAC, IP, GUTI 등)를 모두 가지고 있으며, 이들 정보를 매핑하여 공격자의 위치를 특정하는 개체이다. W_L_M은 신뢰할 수 있는 개체이며, 라우터 상에 구현될 수 있다. W_L_M은 하나의 LTE 영역을 관리하며 W_L_M들 간 통신은 안전하다.

W_L_M이 획득하는 정보는 기존 wifi나 LTE가 통신 과정 중에 사용하는 메시지의 파라미터를 활용하여 얻을 수 있다.

3.2.1 wifi 정보획득[17]

UE가 인증 절차 이후 AP로부터 획득한다. AP는 DHCP/DHCP Relay로 동작하므로 IP 주소를 UE에게 전송한다. DHCP Offer의 파라미터는 아래와 같으며 이 파라미터 정보 중 Client MAC과 IP 값을 AP는 W_L_M에게 전송(sendinfo_wifi(Client MAC, IP))한다.

- DHCP Offer 메시지의 파라미터[18, 19]: Client MAC, IP, Subnet Mask, Router, DNS, IP Lease Time, DHCP Server Identifier

3.2.2 LTE 정보획득

LTE영역 정보는 UE의 초기 접속절차 이후 eNB로부터 획득한다. Attach Accept의 파라미터는 다음과 같으며 이 파라미터 정보 중 GUTI와 UE IP 값을 eNB는 W_L_M에게 전송(sendinfo_LTE(GUTI, UE IP))한다.

- Attach Accept 메시지의 파라미터[2]: GUTI, UE IP, TAI List, TAU Timer, APN, EPS Bearer ID, Authorized QoS Profile(QCI, APN-AMBR(UL)), TFT(UL)

3.3 공격 시나리오

본 논문의 공격시나리오에서 공격자는 wifi 영역 또는 일반 서비스 영역의 서버 해킹을 통하여 사용자 정보를 획득하며, 관리자는 IDS를 통해 공격자를 감지한다.

논문에서 다루는 공격 시나리오는 총 3가지로 ① 공격자가 동일 LTE 영역 내 동일 AP영역에 있는 경우[Fig. 3], ② 동일 LTE 영역 내 다른 AP 영역에 있는 경우[Fig. 4], ③ 다른 LTE 영역 안에 있는 경우[Fig. 5]를 설명한다.

2) (8.2.1) 3GPP TS 24.301

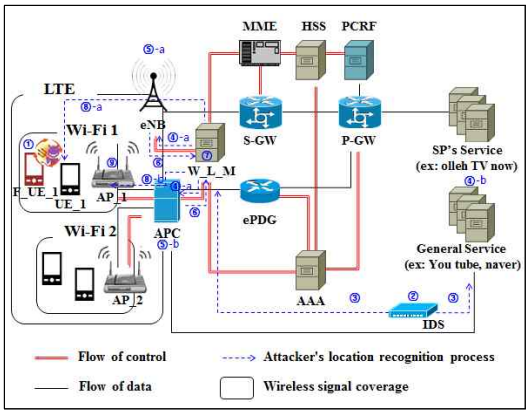
본 논문에서 제안한 시나리오의 절차는 <Table 3>과 같이 6단계로 구성되며, 각 단계의 정의와 비용을 설명하였다. 이는 '4. 성능 분석' 에서 공격자의 위치 특정 비용으로 사용된다.

<Table 3> Scenario Procedures or Costs

Procedure name	Definition
[Attack and Detection]	A procedures or costs that a IDS detects attack attempts by attackers
[Providing a attack information]	A procedure or cost that the IDS provides the information detected to the attack responding entities(server, W_L_M)
[Requesting a attacker's position search]	A procedure or cost in which an attack responding entity(W_L_M) requests attacker's position search to wifi(APC) and LTE(eNB)
[Responding to attacks: server]	A procedure or cost in which an attack responding entity(server) defends attacker's attack
[Checking a attack position]	A procedure or cost in which wifi(APC) and LTE(eNB) recognize attacker's position
[Responding to attacks: W_L_M]	A procedure and cost in which an attack responding entity(W_L_M) instructs a user terminal and an AP to defend of attack

3.3.1 공격자가 동일 LTE 영역에 있는 경우 (동일 W_L_M의 관리 영역)

W_L_M은 LTE 영역당 하나씩 존재하므로 본 절의 시나리오는 공격자가 동일 LTE 영역 내에, 동일 AP 영역에 있는 경우와 공격자가 이동하여 다른 AP영역으로 이동한 경우 두 가지의 시나리오를 설명한다. AP는 다르지만 같은 APC 관리 하에 있으므로 IP는 변하지 않는다.



3.3.1.1 공격자가 같은 AP 영역에 있는 경우

[공격 탐지]

① Fake UE(이하 F_UE_1)는 UE_1으로 가장하여 일반 서비스 서버에 공격 시도

② 일반 서비스 영역의 IDS가 공격을 탐지

IDS: *detection_attack*( )

[공격정보 제공]

③ IDS는 서버와 W_L_M으로 공격 정보 제공 (source IP, source MAC 등)

IDS → Server/W_L_M: *info_attack*( )

[공격 위치 탐색 요청]

④-a. W_L_M은 공격정보를 기반으로 APC와 eNB에게 탐색 요청

W_L_M → APC(AP1, 2)/eNB: *Req_search*( )

[공격에 대한 대응: 서버]

④-b. 서버는 공격을 인지하고 해당 트래픽을 차단하거나 역추적 시간을 확보하기 위해 논리적 또는 물리적인 방법(망 분리, 허니팟 등)을 수행

Server: *defense_attack*( )

[공격 위치 확인]

⑤-a. eNB는 이동 단말 탐색: 위치확인 성공

eNB: *location_confirm*( )

⑤-b. APC는 이동 단말 탐색: 위치확인 성공(AP_1)

AP_1 → APC: *location_confirm*( )

⑥ eNB와 APC는 위치확인 사실에 대해 W_L_M에게 보고

eNB/APC → W_L_M: *location_confirm*( )

⑦ W_L_M은 APC의 보고를 토대로 UE_1이 스푸핑 되었음을 인지

W_L_M: *recognition_attack*( )

[공격에 대한 대응: W_L_M]

⑧-a. W_L_M은 LTE 인터페이스를 이용하여 UE_1에게 스푸핑 경고 전송

W_L_M → eNB(UE_1): *notice_attack*( )

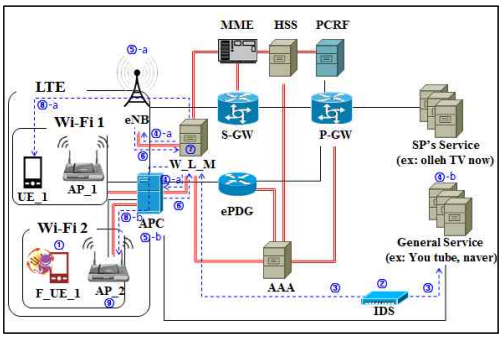
⑧-b. W_L_M은 APC에게, APC는 AP_1에게 스푸핑 경고 전송

W_L_M → APC(AP_1): *notice_attack*( )

⑨ AP_1는 공격을 인지하고 해당 트래픽 차단하거나 논리적 또는 물리적인 방법(망 분리, 허니팟 등)을 수행

AP_1: *defense_attack* ( )

3.3.1.2 공격자가 다른 AP 영역에 있는 경우 (동일 APC)



[Fig. 4] Case2: attacker in different AP area

[공격 탐지]

① F_UE_1는 UE_1으로 가장하여 일반 서비스 서버에 공격 시도

② 일반 서비스 영역의 IDS가 공격을 탐지

[공격정보 제공]

③ IDS는 서버와 W_L_M으로 공격 정보(source IP, source MAC 등) 제공

[공격 위치 탐색 요청]

④-a. W_L_M은 공격정보를 기반으로 APC와 eNB에게 탐색 요청

[공격에 대한 대응]

④-b. 서버는 공격을 인지하고 해당 트래픽을 차단하거나 역추적 시간을 확보하기 위해 논리적 또는 물리적인 방법(망 분리, 허니팟 등)을 수행

[공격 위치 확인]

⑤-a. eNB는 이동 단말 탐색: 위치확인 성공

⑤-b. APC는 이동 단말 탐색: 위치확인 성공(AP_2)

⑥ eNB와 APC는 위치확인 사실에 대해 W_L_M에게 보고

⑦ W_L_M은 APC의 보고를 토대로 UE_1이 스푸핑 되었음을 인지

[공격에 대한 대응]

⑧-a. W_L_M은 LTE 인터페이스를 이용하여 UE_1에게 스푸핑 경고 전송

⑧-b. W_L_M은 APC에게, APC는 AP_2에게 스푸핑 경고 전송

⑨ AP_2는 공격을 인지하고 해당 트래픽 차단하거나 논리적 또는 물리적인 방법 수행

3.3.2 공격자가 다른 LTE 영역에 있는 경우 (다른 W_L_M의 관리 영역)

본 시나리오는 공격자가 다른 LTE 영역으로 이동한 경우로 다른 APC 영역으로 이동하였으므로 공격자는 새로운 APC 영역에서 wifi를 사용하기 위한 IP를 새로이 할당 받는다[Fig. 5].

[공격 탐지]

① F_UE_1는 UE_1으로 가장하여 일반 서비스 서버에 공격 시도

② 일반 서비스 영역의 IDS가 공격을 탐지

[공격정보 제공]

③ IDS는 서버와 W_L_M들(W_L_M_1, W_L_M_2)에게 공격 정보(source IP, source MAC 등) 제공

[공격 위치 탐색 요청]

④-a. W_L_M들은 공격정보를 기반으로 APC들과 eNB들에게 탐색 요청

[공격에 대한 대응]

④-b. 서버는 공격을 인지하고 해당 트래픽 차단하거나 역추적 시간을 확보하기 위해 논리적 또는 물리적인 방법(망 분리, 허니팟 등)을 수행

[공격 위치 확인]

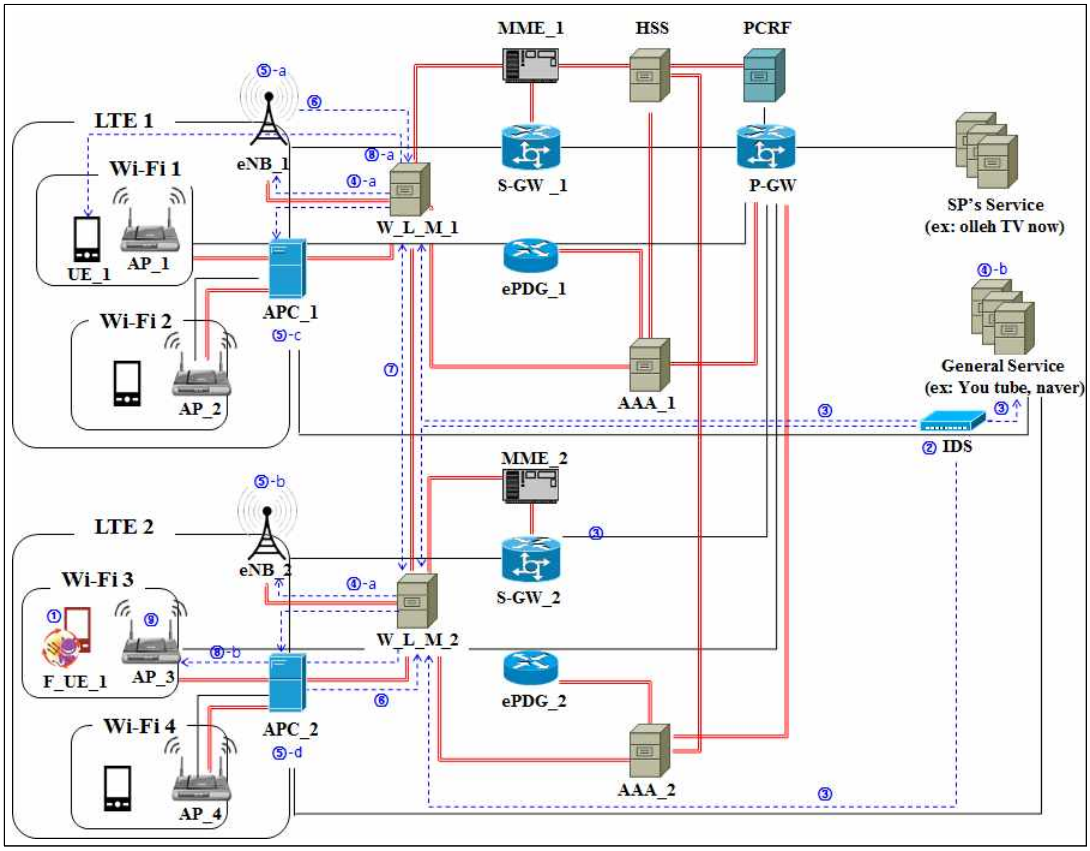
⑤-a. eNB_1은 이동 단말 탐색: 위치확인 성공

⑤-b. eNB_2는 이동 단말 탐색: 위치확인 실패

⑤-c. APC_1은 이동 단말 탐색: 위치확인 실패

⑤-d. APC_2는 이동 단말 탐색: 위치확인 성공

⑥ eNB_1와 APC_2은 위치확인 성공 사실에 대해 각각 자신의 W_L_M에게 보고



⑦ W_L_M간 통신을 통해 W_L_M_1과 W_L_M_2는 UE_1의 두 인터페이스(LTE, wifi)의 통신 위치가 서로 다름을 확인하고, UE_1이 스푸핑 되었음을 인지

[공격에 대한 대응]

⑧-a. W_L_M_1은 LTE 인터페이스를 이용하여 UE_1에게 스푸핑 경고 전송

⑧-b. W_L_M_2는 APC_2를 통해 AP_3에게 스푸핑 경고 전송

⑨ AP_3는 공격을 인지하고 해당 트래픽 차단하거나 논리적 또는 물리적인 차단 수행

4. 성능분석

성능 분석은 기능 및 비용 측면에서 실시하였으며, 기능은 보안 기능<Table 4> 및 위치특정 기능<Table 5>으로 나눠 분석하였다.

<Table 4> Performance analysis(security)

Factors	Not using multi-interface	Using multi-interface
Authentication	- Limited offer · Open authentication, shared-key, RSNA(EAP)	- Support mutual authentication between network and UE · EPS-AKA
Encryption	- Limited offer · Pre-RSNA (WEP), RSNA(CCMP, TKIP)	- Verify integrity and perform encryption · Generate integrity and encryption key using master key generated as an authentication result

<Table 5> Performance analysis(location recognition)

Factors	Not using multi-interface	Using multi-interface
Wifi	- Impossible to specify attacker's location	- Possible to specify attacker's location · Use mapping information in W_L_M : GUTI, LTE IP, MAG, wifi IP : APC(AP)/W_L_M: location_confirm( )
LTE	- Impossible to specify attacker's location	- Possible to specify attacker's location · Use mapping information in W_L_M : GUTI, LTE IP, MAG, wifi IP : eNB/W_L_M: location_confirm( )

성능 평가 요소로써 보안기능은 무선네트워크의 자체적인 취약점에 대한 대안으로 유의미한 요소라 판단하여 인증 및 암호화 두 가지 요소를 기준으로 평가하였다.

위치 특정 기능은 기존의 추적 기법들이 무선네트워크 영역에서 제한적 또는 제공하지 못했던 측면에서 유의미한 요소라 판단하였으며 wifi영역과 LTE영역으로 구분하여 분석하였다.

비용측면에 대한 분석은 다음과 같다.

- 전체 네트워크 비용 = wifi/LTE 기본 통신 비용 + 공격자의 위치 특정 비용
  ① wifi/LTE 기본 통신 비용 = 채널 설정 및 해제 비용 + 인증 비용 + IP 할당 비용 + 데이터 송수신 비용 + 핸드오프 비용
  ② 공격자의 위치 특정 비용 = 공격 탐지 비용 + 공격정보 제공 비용 + 공격위치 탐색 요청 비용 + 공격에 대한 대응(서버) 비용 + 공격 위치 확인 비용 + 공격에 대한 대응(W_L_M)비용

전체 네트워크 비용 중 ① wifi/LTE 기본 통신 비용은 본 제안절차와 관계없이 항상 존재하는 비용이며, ② 공격자의 위치 특정 비용이 본 논문의 제안으로 인해 추가된 비용으로 새로운 개체(W_L_M)가 공격자의 위치 특정을 위하여 수행하는 <Table 3>의 절차로 인해 발생한다.

<Table 6>는 ②의 발생 비용을 제안한 위치특정기법을 사용한 경우와 그렇지 않은 경우로 각각 나누어 프로세싱 비용 및 메시지 전송 과정을 비교하여 정리한 표이다. 이는 [공격탐지]~[공격에 대한 대응]과정에서 발생하는 비용으로 3.3.1.1절을 근거로 작성하였다.

본 논문에서 제안한 W_L_M 개체가 획득, 유지하는 정보는 통신사업자들이 위치관련 서비스(T-map, 네비게이션, 위치기반 서비스 등)들을 제공하기 위해 수집하는 일반적인 정보와 유사하므로 LTE 인터페이스의 위치 정보 획득에는 어려움이 적을 것으로 보여진다.

정리하면, 본 논문에서 제안하는 위치특정과 알람 기능을 제공하기 위해 추가적인 비용(W_L_M 개체 추가, 위치특정 관련 프로세싱 및 전송비용)이 발생하지만 전체 네트워크 운용비용 대비 낮은 비용으로써, 얻는 이점을 감안하면 감내할 수준으로 판단된다.

<Table 6> Performance analysis(cost)

Factors	Not using multi-interface	Using multi-interface
Processing	- basic processing cost	- Extra processing cost □· IDS: *detection_attack*( ) □· Server, AP: *defense_attack*( ) □· eNB, AP, W_M_L: *location_confirm*( ) □· W_L_M: *confirm_attack*( )
Message transmission	- basic message transmission cost	- Extra processing cost □· IDS → Server/W_L_M: info_attack ( ) □· W_L_M → APC(AP)/eNB: Req_search ( ) □· eNB/APC → W_L_M: location_confirm ( )

5. 결론

무선 네트워크 기술의 발전으로 무선 네트워크 이용 시간은 더욱 증가 되었고 유동 IP와 모바일 IP 기술의 사용으로 인해 악의적인 사용자들은 더욱 쉽게 사용자 정보에 접근하여 이를 획득할 수 있게 되었다.

본 논문은 이러한 상황에서 공격자의 공격의도를 빠른 시간 내에 파악하고 대처 할 수 있도록 공격자의 위치를 특정하고 알려주는 알람 기능을 제안하였다. 제안 기법은 사용자와 공격자가 접속한 wifi와 LTE 네트워크 정보를 모두가진 W_L_M 개체를 제안하고 이를 통해 공격자의 위치를 특정하고 사용자에게는 공격에 대한 알람기능을 제공한다.

제안 기법은 LTE망에서 제공하는 인증 및 암호화를 통해 보안 기능을 향상 시켰고 위치특정 및 알람 기능을 제공할 수 있게 되었으나, W_L_M 개체를 새로이 정의함으로써 기본 프로세싱 비용 이외에 공격 탐지 및 대응에 필요한 프로세싱 및 메시지 전송 비용이 추가적으로 발생하였다. 그러나, 전체 네트워크 운용 비용 대비 작은 수준의 비용으로써 성능 대비 감내할 수 있는 수준으로 판단된다.

본 논문의 성능 평가는 wifi, LTE 네트워크 운용에 있어 발생하는 정량적 비용평가가 아닌 정성적 분석에 기초하고 있으나 제안 기법의 우수성을 증명하였다.

본 논문의 제안은 이동 통신관련 사업자가 보다 적은 비용으로 안전한 망을 구축하고 사고 발생 시 빠르게 대처할 수 있는 방안을 새로운 기술개발로 해결하는 것이 아닌 기존의 네트워크에서 수집되는 사용자 정보와 네트워크 구조를 활용한 관리적인 방안으로 해결하고자 할 때 참고 자료로 활용할 수 있다.

REFERENCES

[1] J.H. Oh, K.H. Lee, “Attack Scenarios and Countermeasures using CoAP in IoT Environment”, Journal of the Korea Convergence Society, Vol. 7. No. 4, pp. 33-37, 2016.

[2] C.R. Seo, K.H. Lee, “ARP Spoofing attack scenarios and countermeasures using CoAP in IoT environment”, Journal of the Korea Convergence Society, Vol. 7. No. 4, pp. 39-44, 2016.

[3] S.W. Cho, W.J. Jang, H.W. Lee, “mVoIP Vulnerability Analysis And its Countermeasures on Smart Phone”, Journal of the Korea Convergence Society, Vol. 3, No. 3, pp. 7-12, 2012.

[4] J.T. Kim, M.H. Han, J.H. Lee, J.H. Kim, I.K. Kim, "Technical Trends of the Cyber Attack Traceback", Electronics and Telecommunications Trends, Vol.29, No.1, pp.93-103, 2014.02.

[5] J.T. Kim, I.K. Kim, K.H. Kang, "Technical Trends of the Cyber Targeted Attack Traceback-Connection Chain & Traceback", Electronics and Telecommunications Trends, Vol. 30, No. 4, pp. 120-128, 2015.08.

[6] D.H. Lee, D.G. Yeo, J.h. Jang, H.Y. Youm, "Traceback technology trends at Ad-hoc network", Review of KIISC, Vol.20, No.4. pp.85-94, 2010.08.

[7] H.W. Lee, "TTL based Advanced Packet Marking Mechanism for Wireless Traffic Classification and IP Traceback on IEEE 802.1x Access Point", Journal of the Korea Contents Association, Vol.7. No.1. pp. 103-115, 2007.01

[8] H.G. Cho, "Trend and prospect of wireless LAN standards", TTA Journal, Vol.147, pp. 39-42, 2013.05. (in Korean)

[9] J.S. Lim, “Design of Fusion Multilabeling System Controlled by Wi-Fi Signals”, Journal of the Korea

Convergence Society, Vol. 6, No. 1, pp. 1-5, 2015.
[10] H.C. Kwon, "Technologies for Next Generation Wireless LAN Security", 2015 Annual Security Users' Festival, 2015.11. (in Korean)
[11] M.S. Gu, Y.Z. Li, "A Study of Countermeasures for Advanced Persistent Threats attacks by malicious code," Journal of IT Convergence Society for SMB, Vol. 5, No. 4, pp. 37-42, 2015.
[12] S.H. Hong, Y.J. Seo, "Countermeasure of Sniffing Attack: Survey," Journal of IT Convergence Society for SMB, Vol. 6, No. 2, pp. 31-36, 2016.
[13] M.Y. Shin, S.H. Hong, "A Defending Method Against DDoS Attacks With Router Control," Journal of IT Convergence Society for SMB, Vol. 5, No. 1, pp. 21-26, 2015
[14] KISA, "A handbook for wireless LAN security", Korea Communications Commission, Korea Information Security Agency, 2010.01. (in Korean)
[15] J.H. Na, K.S. Kim, D.S. Kwon, H.K. Chung, "Technical Trends of Small Cell Base Stations for LTE", Electronics and Telecommunications Trends, Vol.30, No.1, pp.102-113, 2015.02.
[16] NMC Consulting Group, "LTE Security I: LTE Security Concept and LTE Authentication", Netmanias Technical Document, 2013.07.
[17] NMC Consulting Group, "EMM Procedure 1. Initial Attach - Part 2. Call Flow of Initial Attach", Netmanias Technical Document, 2014.01.
[18] C.M. Yoo, "Understanding the Basic Operations of DHCP", NETMANIAS TECH-BLOG, 2011.12
[19] R. Droms, Dynamic Host Configuration Protocol, RFC 2131, IETF, 1997.03.

봉 진 숙(Bong, Jin Sook)

- 2002년 2월 : 독학사(이학사)
- 2005년 2월 : 숭실대학교 컴퓨터학과(공학석사)
- 2011년 3월 ~ 현재 : 숭실대학교 컴퓨터학과(박사과정 수료)
- 관심분야 : IPv6, 모바일, 보안,
- E-Mail : jsbong@ssu.ac.kr

박 상 진(Park, Sang Jin)

- 1998년 2월 : 세명대 전자계산학과(이학사)
- 2002년 8월 : 숭실대학교 컴퓨터학과(공학석사)
- 2005년 8월 : 숭실대학교 컴퓨터학과(박사과정 수료)
- 관심분야 : 모바일 IP, 정보보호,
- E-Mail : neoparking@ssu.ac.kr