# IEEE 802.16e/WiBro 휴대 인터넷망을 위한 합법적 감청 아키텍처에 관한 연구

이명락, 이동현, 김승빈, 인호*
고려대학교 정보통신 대학
e-mail :{ lmr2010, tellmehenry, consoli, hoh_in}@korea.ac.kr

# A Study on Lawful Interception Architecture for IEEE 802.16e Wireless/Mobile Networks

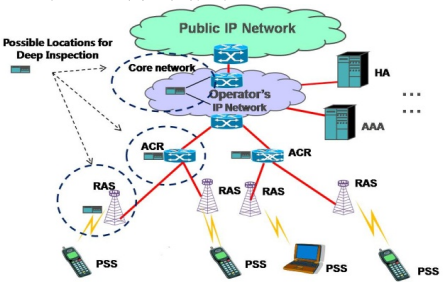
Myoung-rak Lee, Dong-hyun Lee, Seung-bin Kim, Hoh Peter In*
Dept. of Computer Science and Engineering, Korea University

**요 약**

Lawful Interception (LI) 이란 합법적인 형태의 도청을 말하며, 전통적인 Wired tapping 뿐만 아니라, 최근의 복잡해진 인터넷 및 통신환경의 여러 형태의 데이터들에 대한 감청이 포함 될 수 있다. 미국과 유럽 중심으로 개발 된 감청 표준들은 3 세대 통신망 위주의 감청을 위한 표준들이 대부분이며, 802.16e 기술 중의 하나인 모바일 WiMax 를 위한 합법적 감청 표준 개발은 진행 중에 있는 실정이다. 특히, Wibro 와 같이 모바일 유닛(MU)이 Radio Access Contro (RAS)와 Access Control Router (ACR)를 자유롭게 이동하는 상황에서 패킷들에 대한 지속적인 추적은 합법적 감청 분야의 중요한 이슈 중의 하나이다. 따라서, 본 논문에서는 국내의 802.16e/WiBro 네트워크 사용자의 증가 및 그에 따른 보안위협 발생의 가능성 증가에 따라 합법적인 감청을 위한 효과적인 아키텍처를 제안하고자 한다. 본 논문에서 제안하는 아키텍처는 802.16e/WiBro 망내의 합법적 감청을 위하여 네트워크상에서의 효과적인 감청 관련 정보 교환을 위한 기본적인 메커니즘을 포함하고 있다.

## 1. 서론

국제전기통신연합(ITU)는 국내 휴대인터넷 기술인 WiBro 를 IMT-2000 의 6 번째 표준으로 확정하였다. WiBro 와 같이 사용자의 이동성을 보장하는 휴대 인터넷망의 보급 확산과 함께 모바일 IP 를 기반으로 하는 802.16e 네트워크의 합법적 감청 방안에 대한 아키텍처는 LI 연구 분야의 중요한 국제적 이슈 중의 하나이다[1]. 즉, 과거의 wired 기반의 통신방식과는 다르게 최근의 VoIP 및 데이터 통신은 그 경로를 사전에 예측하기 어려우므로 합법적인 감청이 용이하지 못하다. 그러나, WiBro 와 같이 날로 증가하는 사용자와 새로운 휴대 인터넷망에 대한 보안위협의 증가 함께 802.16e wireless/mobile 네트워크를 오고 가는 패킷들에 대한 검사 (Inspection)의 중요성 또한 커지고 있는 실정이다. IEEE 802.16e 와 같은 무선망에서는 무단 인증, 패킷 가로채기, IP spoofing 과 같은 위협들이 있을 수 있으며, 이 들 위협은 Radio Access Control (RAS) 와 Access Control Router (ACR) 과 같은 경로를 통하여 발생 할 수 있다[2]. 802.16e 네트워크 환경에서는 모바일 유닛들의 이동에 따라 이들이 접속하는 RAS 및 ACR 의 위치가 달라 질 수 있으며, 모바일 유닛이 이동하여 새로운 지역의 ACR 을 접속할 때 부여 받는 Care of Address (CoA) 또한 달라진다. 이와 같은 802.16e wireless/mobile 환경에서 합법적 감청을 수행하기 위해서는 여러 지역에 분산되어 있는 LIA(Lawful Interception Agent) 들이 이동하는 감청 대상 유닛에 대한 감청 결과를 지속적으로 LI 서버로 보고하여야 한다. 즉, 패킷 검사를 위한 대부분의 Deep Packet Inspection (DPI) 알고리즘 들은 기존의 wired network 에서와 동일한 알고리즘으로 검사를 수행하므로, 특정 사용자가 핸드오버가 일어나기 전에 한 지역에서 발생시켰던 컨텐츠를 연속적으로 감청하지는 못하는 문제점이 있다.




(그림 1) 802.16e/WiBro 네트워크의 LI 가능 위치

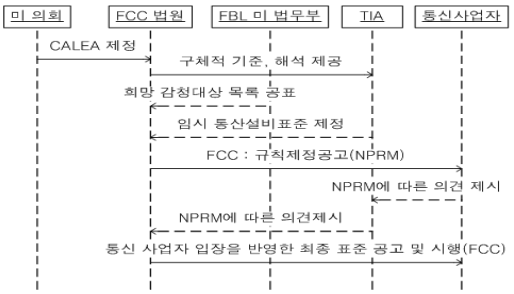
본 논문에서는 802.16 과 같이 모바일 IP 를 지원하는 환경하에서 모바일 유닛이 여러 지역을 옮겨 다닐 때 각 지역에서의 감청결과를 LI 서버로 보고하고 종합하여 연속적 감청결과를 생성하는 LI 아키텍처를

제안한다. 그림 1 은 WiBro 네트워크의 기본적인 구조를 나타내고 있으며 점선 안의 원들은 합법적 감청이 가능한 위치들을 나타낸다. 본 논문의 2 장에서는 LI 에 대한 국제적 표준화 동향을 기술하고, 3 장에서는 802.16e 에서의 효과적인 아키텍처 및 세부사항을 포함하였다.

## 2. 배경: Lawful Interception 의 국제 표준화 동향

### 2.1 미국

미국은 통신사업자가 합법적 감청을 위한 장비의 설치를 의무화하는 CALEA[3]를 1994 년에 제정하였으며, 2000 년 초부터, VoIP, 휴대형 인터넷 등 IP 기반의 서비스 확산 및 2001 년 9.11 테러 발생 이후 IP 기반 서비스에 대한 LI 제공의 필요성이 강하게 제기되었다[4, 5]. 그림 1 은 CALEA 의 LI 표준 제정 절차를 나타내며, 미 연방 통신위원회 (FCC: Federal Communications Commission)와 미연방 수사국, 법무부 등이 CALEA 제정을 위한 구체적인 기준과 그에 따른 해석을 제공하며, FCC 는 미 통신산업협회(TIA)로 하여금 통신사업자 및 전기통신과 관련된 일반사업자의 의견이 반영된 임시 표준제정을 허락하고, 이를 반영한 최종 표준안을 규칙제정공고(NPRM)을 통해 공지함으로써, CALEA 의 최종적인 시행 전 관련기관 및 통신사업자의 의견수렴 과정을 거쳤다.

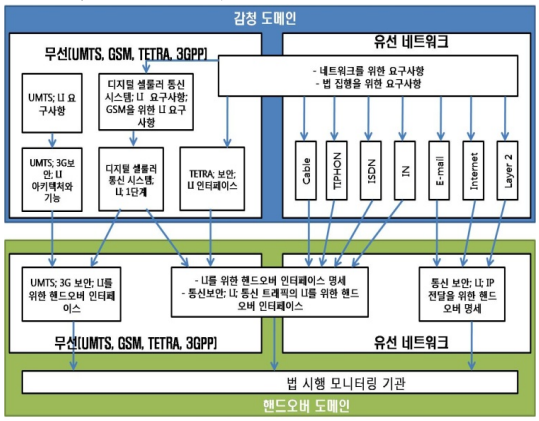



(그림 2) 미국 CALEA 의 LI 표준 제정 절차

또한, 미 의회는 CALEA 의 제정을 통하여 법 집행기관 (LEA)이 전자적 수사를 진행할 때 이를 지원하기 위한 의무를 부과하여 국가안보와 공공의 안녕을 보호하고자 하였고, CALEA 의 제정은 통신 사업자로 하여금 적법한 권한의 전자적 수사가 실행 될 수 있도록 자신들의 시스템을 고안하거나 변경하는 것을 법률적으로 의무화하고 있다[3, 6]

### 2.2 유럽

유럽의 경우, ETSI(European Telecommunications Standards Institute)의 주도적 역할을 중심으로 LI 에 관한 표준을 개발하고 있다. ETSI 산하 LI, AT, TSPAN, TETRA, 3GPP 등의 여러 TC(Technical Committee)에서 감청 관련 표준화 작업이 진행되고 있다. 특히 TC LI 를 중심으로 차세대 통신망 및 이동통신망 등의 기술적 이슈를 고려한 표준 개발 작업이 활발히 이루어지고 있다. ETSI 는 보안 문제를 다루는 TC SEC 에 LI 관련 조직을 두어 표준을 개발 하였으나, 관련 업무량이 늘어 TC LI 로부터 독립하여 표준 개발을 진행하고 있다. 또한, ETSI 에서는 그림 1 과같이 LI 의 Interception 및 Handover 에 관한 국제 표준을 제시하고 있다[7] [8, 9, 10]. 그림 2 에서 보는 바와 같이 ETSI 에서 제안한 표준은 크게 감청 도메인과 핸드오버 도메인으로 나눌 수 있으며, 그림 2 와 같이 각 영역별 대표적인 표준들을 중심으로 각 망과 서비스 형태에 따른 어플리케이션 별 요구사항 들을 포함한 표준들이 지속 보완, 개발되고 있다. ETSI 에서 제안한 Lawful Interception 표준은 크게 두 영역으로 나눌 수 있는데 감청 도메인 영역과 핸드오버 영역으로 나뉘며 이들 두 영역은 다시 무선 영역과 유선영역으로 구분된다.




(그림 2) ETSI 의 표준들의 영역별 분류

Lawful Interception 의 전반적인 요구사항에 관한 정의와 관련된 ETSI 표준들은 표 1 와 같으며, 주요 포함 내용에는 일반 네트워크 아키텍처에서의 감청 개념과 Lawful Interception 를 위한 요구사항, 다양한 통신망에서의 Lawful Interception, LEA 의 요구사항 등을 포함하고 있다 [11]

<표 1> ETSI 의 Lawful Interception 표준 목록

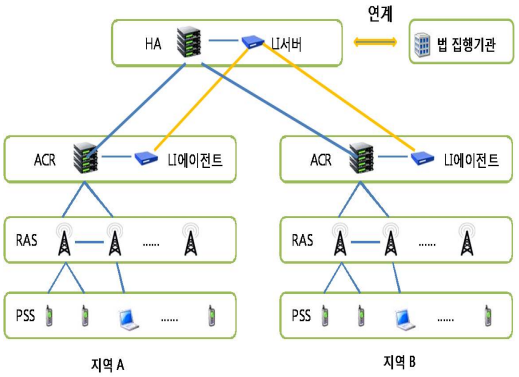
| ETSI 표준 | 주요 포함 내용 | 비 고 |
|---|---|---|
| TR 101 943 | Concepts of Interception in a Generic Network Architecture | TC LI |
| EG 201 781 | Lawful Interception | TISPAN |
| TS 101 772 | LI-top level requirements | TISPAN |
| TR 41.033 | LI requirements for GSM | 3GPP |
| TS 33.106 | LI requirements for UMTS | 3GPP |
| ES 201 158 | Requirements for Network Function | SEC LI |
| TS 101 944 | Issues on IP interception | SEC LI |
| TS 101 331 | Requirements of Law Enforcement Agencies | SEC LI |

## 3. Lawful Interception 아키텍처 제안

국내에서는 국회 법제사법 상임위원회 회의를 통해 통신비밀보호법 개정을 추진 중에 있으나, WiBro 와 같은 휴대인터넷에 대한 구체적인 감청 아키텍처를 포함하고 있지는 못하다. 이러한 IP 이동성 제공환경은 Lawful Interception 의 국제표준화에 있어서도 중요한 이슈 중의 하나이며, WiMAX 포럼에서는 이러한 휴대 인터넷 환경하에서의 Lawful Interception 방안에 대해 활발한 논의가 진행 중에 있다[12]. 이에 본 장에서는 상용화가 빠르게 진행되고 있는 WiBro 휴대 인터넷에 대한 Lawful Interception 의 기본 아키텍처를 제안하고자 한다.

### 3.1 IEEE 802.16e 에서의 LI 를 위한 기본 아키텍처

802.16e/WiBro 환경에서는 특정 사용자의 컨텐처를 연속적으로 감시하기 위해서는 모바일 IP 에 대한 지속적인 추적이 가능하여야 한다. LI 수행을 위해서는 컨텐처 검사를 위한 Deep Packet Inspection (DPI)과 같은 기본적인 툴이 제공되어야 한다. 그림 3 은 802.16e/WiBro 와 같은 모바일 환경에서 지속적인 컨텐처 검사를 수행하기 위한 기본적인 개념도로서 그림 1 의 3 곳의 LI 가능 지점 중에서 가입자 수가 급증하고 있는 추세를 감안 시, L2/L3 레이어 핸드오버를 모두 지원하고 있는 ACR 단에서 LI 가 수행되는 것으로 가정하였다




(그림 3) WiBro Lawful Interception 아키텍처

그림 3 에서 제시한 합법적 감청 아키텍처에 대한 세부적인 동작 절차는 다음과 같다.

① 법 집행기관에서 감청 대상을 선정하고, 감청 수준을 결정하여 LI 서버에 감청 대상 정보 요청
② 감청 목적에 맞도록 LI 에이전트를 결정하고 관리
③ LI 서버는 감청 대상의 정보와 범위를 LI 에이전트에 전달
④ 지정된 LI 에이전트에서 감청 수행
⑤ LI 에이전트는 모니터링 후 결과를 LI 서버로 보고
⑥ LI 서버에 의해 법 집행기관에 최종 전달

## 4. Lawful Interception 아키텍처 Analysis

802.16e 네트워크의 모바일 환경을 고려한 LI 아키텍처의 특성(Characteristics) 요구사항은 다음과 같다

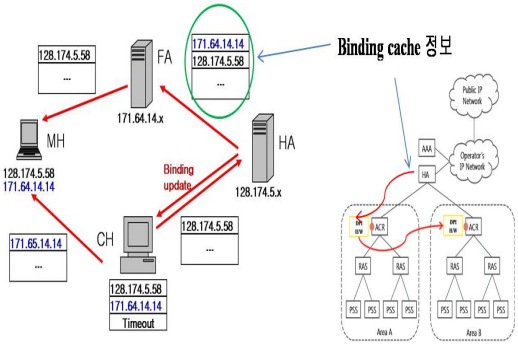
.

### 4.1 Mobility Detection 및 감청결과의 인수 인계

특정 MN 의 mobility detection 을 위해서는 802.16e 네트워크의 핸드오버 특성을 이용한다. 802.16e 네트워크는 그림 5 와 같이 HA 의 binding cache 를 update 시키기 위해서 사용되는 binding request 및 binding acknowledge 정보를 발생한다

그림 4 는 모바일 노드가 이동하였을 때 FA 로부터 새로이 부여 받는 CoA 와 binding update 과정을 보여준다. MN 가 홈 네트워크를 떠나 외부 네트워크로 이동하였을 때, 홈 에이전트는 MN 의 HoA 로 향하는 모든 패킷들을 MN 를 대신 하여 가로채고 MN 의 현재 위치인 CoA 로 전달해주는 역할을 수행한다 [12]. 802.16e 네트워크에서의 Mobility detection 을 위한 알고리즘의 내용을 요약하면 다음과 같다.

- HA 는 모바일 유닛의 홈 네트워크에 존재하는 라우터로써, 이동 노드의 HoA 와 CoA 에 대한 바인딩을 유지 및 관리한다
- Layer 1, 2 및 Layer3 핸드오버가 일어날 때 ACR 에 위치한 LI 서버는 Old-ACR 과 Target-ACR 가 핸드오버 Acknowledgement 메시지를 주고 받을 때 모바일 유닛의 이동성을 감지한다.
- 핸드오버가 완전히 이루어졌을 때, 그림 5 와 같이 HA 로부터 MN 의 이동한 위치에서의 모바일 IP 인 CoA 정보를 받는다.




.

(그림 4) Mobility Detection 을 위한 Binding Cache 정보의 활용

만약, 특정 모바일 유닛이 바인딩 테이블의 CoA 를 갱신하면, CoA 를 할당한, FA 가 위치한 ACR 단에 위치한 LI 에이전트로 LI 수행결과인 패턴매칭 정보의 전달이 가능하다

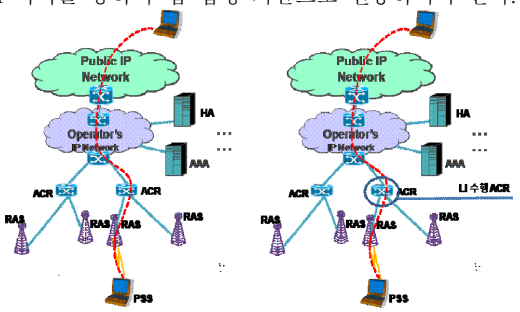
### 4.2 Lawful Interception 의 연속성 보장

802.16e 와 같이 모바일 인터넷 환경에서 특정 커넥션에 대한 연속적인 감청이 이루어지기 위해서는 그림 3 의 LI 서버에 의한 지속적인 모니터링과 함께 각 ACR 단에서 행하여진 모니터링의 결과는 DPI 수행, 이동 감지, DPI 정보의 전송 및 완전한 정보의 생성

을 위한 4 단계의 절차를 필요로 한다. 또한, 그림 4 에서와 같이 HA 와 ACR 간에 오고 가는 모바일 IP 의 바인딩 update 정보를 LI 에이전트들이 활용 함으로써 LI 의 연속성을 보장 할 수 있다. 즉, 모바일 유닛의 이동과 동시에 새로운 지역에 위치한 LI 에이전트에게 지속적인 LI 를 수행할 수 있게 한다.

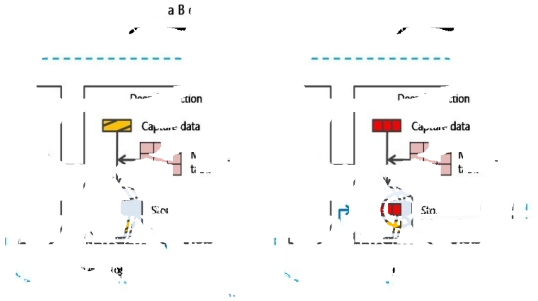
### 4.3 부분적인 Lawful Interception 정보들의 통합

인터넷 환경에서 분산된 LI 에이전트들이 특정 MU 에 대하여 수행한 정보의 통합을 위해서는 그림와 같이 각각의 LI 에이전트에서 실시한 LI 결과를 LI 서버를 통하여 법 집행 기관으로 전송하여야 한다.




(그림 5) MU 의 이동 및 LI 에이전트의 변경

이때 각기 다른 지역의 LI 에이전트에서 수행한 LI 결과들을 그림 5 와 같이 전송 할 수가 있으며, 그림 6 과 같이 MU 의 mobility 로 인한 핸드오버가 발생하기 직전까지의 감청 결과를 LI 서버에서 종합하여 완전한 정보를 재생할 수 있다. 또한, LI 서버 지역에서는 HA 로부터 전달받은 CoA 및 HoA 정보를 활용하여 감청하고자 하는 특정 MU 의 유일한 ID (Identification)를 식별할 수 있다.



(그림 6) LI 수행 결과의 전달 및 종합

## 5. 결론

본 연구에서는 WiBro 와 같이 모바일 IP 를 지원하는 네트워크 환경에서 이동하는 MU 에 대한 지속적인 합법적 감청을 수행하기 위한 기본 아키텍처를 제안하였으며, 제안된 LI 아키텍처는 고정 네트워크 중심에서 사용되고 있는 일반적인 DPI 알고리즘의 적용 가능성을 포함하고 있다. 본 논문에서는 모바일 IP 환경하에서 적용 가능한 LI 아키텍처를 제시하였으며, 제안하는 802.16e wireless/mobile LI 아키텍처는 이동성이 복잡한 휴대 인터넷 환경하에서 특정 사용자에 대한 합법적 감청을 연속적으로 가능케 할 것으로 기대하며, 세부적인 기술적 구현은 국제 표준들에서 제시하는 바와 같이 일반 통신사업자가 Lawful Interception 표준을 따르도록 제도화 되어야 할 것이다. 향후 연구는 제안된 아키텍처를 기반으로 IEEE 802.16 표준을 따르는 다양한 종류의 패킷에 대한 LI 수행 시 고려하여야 할 세부 요소들의 식별 및 분석을 위해 공개기반의 DPI 알고리즘을 활용, 시뮬레이터 등을 활용한 실험을 통하여 그 효율성을 검증하고자 한다.

## 6. Acknowledgements

본 연구는 정보통신부 및 정보통신진흥원의 IT 연구개발 지원사업의 연구결과로 수행되었음. [2008-S-001-01, Development of WiBro network reliability and location awareness technologies]

## 참고문헌

[1] 박소영, 김은숙, 강신각, “미국의 IP 서비스 감청 규제 동향”, 전자통신동향분석 제 21 권 제 5 호, 2006.10

[2] Michel Barbeau, WiMax/802.16 Threat Analysis, ACM, Q2SWinet'05, October 13, 2005, pp. 8-15.

[3] Communications Assistance for Law Enforcement Act, http://www.askcalea.net/calea.html

[4] FCC News, FCC Adopts Order to Enable Law Enforcement to Access Certain Broadband and VoIP Providers, 2006.5.3.

[5] FCC, First Report and Order and Further Notice of Proposed Rulemaking, 2005.9.23.

[6] FCC, Second Report and Order and Memorandum Opinion and Order, 2006.6.12

[7] ETSI ES 201 158: Telecommunications security; Lawful Interception (LI); Requirements for network functions

[8] ETSI TS 101 331: Telecommunications Security; Lawful Interception (LI); Requirements of Law Enforcements Agencies.

[9] ETSI, ES 201 671: Telecommunications Security; Lawful Interception (LI); Handover Interface for the Lawful Interception of Telecommunications Traffic.

[10] ETSI, TS 101 671, Telecommunications Security; Lawful Interception (LI); Handover Interface specification for LI of telecommunications traffic.

[11] ETSI EG 201 781: Lawful Interception (LI); Concepts of Interception in a Generic Network Architecture.

[12] Lawful intercept for release 1.5, WiMax forum, 2006.