IMS/SIP 기반의 감청을 위한 아키텍처 연구

엄태훈*, 김도훈*, 이정빈*, 최송인**, 이명락***, 인 호*†
*고려대학교 컴퓨터학과
e-mail: {ompa, karmy01, jungbini, hoh_in}@korea.ac.kr
**한국전자통신연구원
e-mail: sichoi@etri.re.kr
***공군 군수사령부 제 83정보통신 정비창
e-mail: lmr2010@korea.ac.kr
†교신저자: 인 호

Study for the IMS/SIP based Lawful Interception Architecture

Tae-hoon Um*, Do-Hoon Kim*, Jung-Been Lee*, Song-In Choi**,
Myoung-Rak Lee***, Hoh Peter In*
*Dept of Computer Science and Engineering, Korea University
**WiBro Service Rearch Team, Electronics and Telecommunicating Research Institute (ETRI)
***Republic of Korea Air Force Logistics Command
†Corresponding Author: Hoh Peter In

요 약

전화와 같은 음성통신이 네트워크 트래픽의 주류를 이루었던 과거와는 달리 최근 다양한 멀티미디어 콘텐츠의 사용 증가와 함께 이를 효율적으로 제공할 수 있는 IP기반의 IMS(IP Multimedia Subsystem)기술이 도입되었다. 이러한 통신기술의 발달과 함께 다양한 수법을 이용한 범죄가 증가하고 있으며 이에 따른 감청의 필요성이 점점 커지고 있다. 감청에 관한 법률은 각 국가별로 시행되고 있으며 특히 미국과 유럽의 감청표준은 국제 감청표준의 근간이 되고 있다. 그러나 기존의 감청 아키텍처는 IMS 환경에 적절하지 않은 몇몇 한계점을 지니고 있기 때문에 새로운 환경에 적합한 아키텍처가 필요하다. 본 논문에서는 현재까지의 감청기술 및 동향을 다루고 IMS 환경에서의 개선된 감청 방안을 제시한다.

1. 서론

합법적 감청(Lawful Interception)이란 사법수행기관(LEA: Law Enforcement Agencies)이 법적절차를 통해 영장을 발부받고 감청 대상에 접근하여 음성 및 영상, E-Mail 등의 내용을 조사하는 행위를 말한다[1]. 최근, 통신기술의 발달과 함께 새로운 형태의 진화된 범죄 행위를 추적하기 위한 합법적 감청은 필수 불가결한 요소가 되었으며 합법적 감청을 용이하게 하기 위한 활발한 감청표준화 활동이 미국과 유럽 국가들을 중심으로 수행되고 있다[2]. 근래에는 스마트폰 사용률의 증가와 더불어 인터넷 액세스나 멀티미디어 서비스 이용이 급격히 확대됨에 따라 네트워크 트래픽의 주요인이 음성에서 멀티미디어 서비스로 대체되고 있으며, 이것이 IP 기반의 IMS가 등장하게 된 배경이 되었다[3]. 하지만 현재까지의 감청표준은 IMS 구조와 연동될 수 있는 방법을 명시하고 있지 않기 때문에 IMS의 구성요소를 반영한 메커니즘이 필요하다. 본 논문에서는 IMS 표준화의 동향 및 현재까지의 감청 표준 동향을 각각 2장과 3장에서 소개하고 4장에서는 최신 감청표준을 바탕으로 IMS 환경에 적용 가능한 개선된 감청방안을 제시한다.

2. IMS 기술의 표준화 동향

이동통신 분야의 대표적 국제 표준화기관인 3GPP(3rd Generation Partnership Project)는 2002년 3월 처음으로 IMS를 채택하였다. 3GPP는 릴리즈 99를 시작으로 거의 매년 IMS와 관련된 새로운 릴리즈를 배포하고 있다. 릴리즈 99의 참조모델을 기반으로 하여 이동통신 네트워크가 무선 액세스 네트워크(RAN)와 코어 네트워크로 구분되어 코어 네트워크는 다시 패킷교환(PS)과 회선교환(CS) 도메인으로 분류된 구조가 현재까지 유지되고 있다. IMS는 릴리즈 5에서 최초로 도입되었고 PS 도메인과 연결되어 종래의 CS 도메인에서 제공하던 서비스를 IP 기반 서비스로 제공할 수 있게 되었다. 릴리즈 5

이후로는 과금 처리, 무선 LAN의 연동, Presence, Push와 같은 기능이 추가되었으며 PAN(Personal Area Network), WiMAX 통합 및 AIPN(All IP Network) 등의 항목이 표준화 대상으로 선정되었다[3]. IMS는 기본적으로 텍스트 기반의 메시지를 통해 세션을 제어하는 프로토콜인 SIP(Session Initiation Protocol)를 사용한다. 다양한 멀티미디어 서비스 지원을 위해 크게 서비스 영역과 네트워크 영역으로 나뉘며 기본적인 호 처리는 SIP 서버인 CSCF(Call Session Control Function)의 세션제어를 통해 수행된다. CSCF는 P(Proxy)-CSCF, I(Interrogating)-CSCF, S(Serving)-CSCF의 3가지 종류로 분류되며 각각의 자세한 기능은 [4]에 기술되어 있다.

3. 국가별 감청규제 및 표준화 동향

감청관련 표준은 미국과 유럽을 중심으로 정의되고 있으며 세계 각국 감청법규의 근간이 되고 있다. 국내의 경우 1993년에 통신 비밀 보호법이 제정되어 감청관련 내용을 규정하고 있다[5]. 본 절에서는 감청의 국제 표준과 관련하여 가장 활발히 활동하고 있으며 세계 각국의 감청 표준에 가장 밀접한 영향력이 있는 미국과 유럽의 동향을 살펴본다.

3.1 미국

미국의 경우, 합법적 감청을 위한 규제와 감청 장비설치 의무화를 핵심으로 하는 CALEA를 제정하였다[6]. CALEA[1]는 합법적이며 제한적인 감청 정보의 활용에 관한 기준을 FCC[2]와 법원의 해석을 따르도록 하였다[7]. 또한, 감청을 위한 일반적인 전자감시 참조모델을 제시하였는데 CALEA의 참조모델은 감청을 위한 Service Provider Administration, Access, Delivery, Collection, Law Enforcement Administration(LEA)의 5가지 기능을 사용한다[8].

3.2 유럽

유럽의 감청 표준화는 ETSI[3]를 중심으로 활발히 진행되고 있으며 특히 LI TC[4]에 의해 차세대 통신망과 이동통신망 등의 기술적 표준 개발이 이루어지고 있다[8]. 유럽의 43개국은 사이버 범죄 조약에 서명하여 자국의 정보통신사업자들에게 ETSI 표준에 근거한 감청기술지원을 요구하고 있다[9].

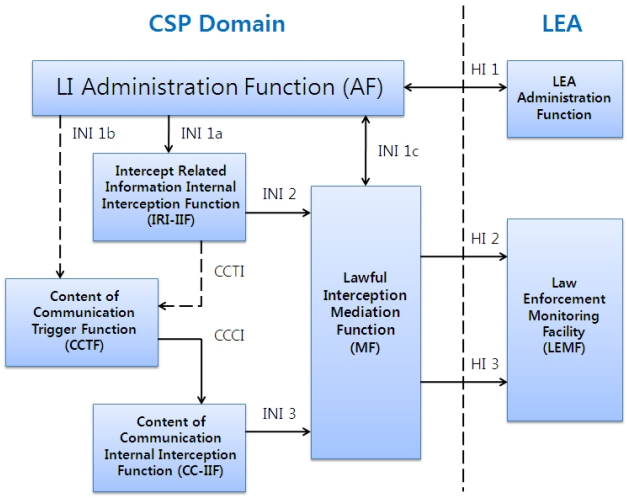

그림 1. IP 네트워크에서의 감청 참조모델

그림 1은 ETSI TS 101 943[10] 표준의 일반적인 감청 참조모델을 보여주고 있으며 이 모델을 기반으로 국내외적인 감청연구가 진행되고 있다. 이 밖에도 감청 데이터의 타입, 핸드오버 인터페이스(HI) 등을 다루는 다양한 감청관련 표준들이 제정되었다.

ETSI 표준	주요 포함 내용
합법적 감청의 요구사항과 관련된 표준	
TS 101 943	일반적인 네트워크 아키텍처에서의 감청개념
TS 102 677	CC감청을 위한 Dynamic Triggering
TS 101 772	LI 상위 레벨 요구사항
TR 41 033	GSM을 위한 LI 요구사항
TS 33 06	UMTS를 위한 LI요구사항
TS 101 944	IP 감청에서의 이슈 (다양한 Application ID고려)
TS 101 331	법 집행 기관의 요구사항
합법적 감청의 서비스 별 상세 기능을 기술한 표준	
TR 102 053	ISDN LI의 기능적인 내용
TS 102 232	IP 전달을 위한 핸드오버 명세
TS 102 233	E-mail을 위한 서비스의 구체적 항목
TS 102 234	인터넷 액세스 서비스를 위한 구체적 항목
TR 101 772	TIPHONE 3번째 배포: 서비스 독립 요구사항
TS 102 227	TIPHONE 4번째 배포: 기능적 요소 및 flow정의
TS 101 909	스트림(Streamed) 멀티미디어 서비스
ES 201 671	통신 트래픽의 LI를 위한 핸드오버 인터페이스
TS 33 108	LI를 위한 핸드오버 인터페이스

표 1. ETSI의 감청 및 관련기술 표준

표 1은 ETSI에서 제정한 감청관련 주요표준들을 나타내고 있다. TS 102 677[11]과 TS 102 232-5[12]의 경우 IMS에 대한 직접적인 언급은 없지만 IMS를 제공하는 Service Domain과 실제로 감청된 데이터가 전송되는 IP-CAN Domain의 두 영

1) CALEA: Communications Assistance for Law Enforcement Act
2) FCC: Federal Communication Commission
3) ETSI: European Telecommunications Standards Institute
4) LI TC: Lawful Interception Technical Commitee

역으로 구분하여 감청 아키텍처를 표현하고 있기 때문에 본 연구에 활용되었다.

4. IMS 환경에서의 감청수행 방안

본 절에서는 Service Domain과 IP-CAN Domain으로 나누어진 IP 기반의 통신환경을 고려하여 현재 ETSI에서 연구 중에 있는 TS 102 677 표준의 몇 가지 한계점을 거론하고 IMS 환경에서 적합한 감청 아키텍처를 위한 방안을 제시한다.

4.1 TS 102 677 표준 참조모델을 적용한 IMS 환경에서의 감청 아키텍처

분리된 도메인 영역에서 원활한 감청을 수행하기 위해서는 Dynamic Triggering을 통한 두 사업자간의 감청활성 신호전달이 필요하다. TS 102 677 표준의 참조모델은 두 영역 사이에서의 감청흐름을 Dynamic Triggering을 통해 보여주고 있지만 현재의 참조모델을 IMS에 적용하기에는 크게 두 가지 문제점들이 있다. 첫째, 현재의 표준에는 감청 자료(CC 및 IRI)의 전송, 권한정보제어, Triggering 신호전달을 담당하는 기능이 감청의 측면에서만 제시되었고 IMS 구성요소들과의 연관성이 언급되지 않았다. 또한, IMS에서의 감청을 위해 사용되는 노드와 감청 활성화 시기 및 감청 위치가 명시되어야 한다.

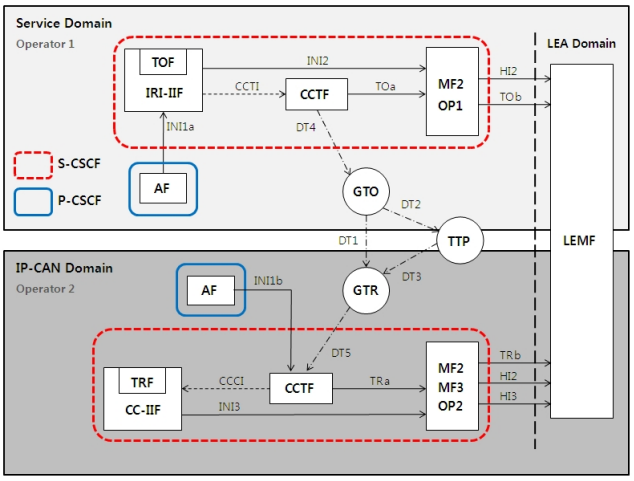

그림 2. IMS 환경에서의 개선된 감청 아키텍처

종래의 IMS에서는 핵심 구성요소인 SIP 서버들이 SIP 메시지의 제어와 송수신만을 담당하였다. 본 연구에서는 위에서 언급한 표준상의 한계를 보완하고자 SIP 서버(P-CSCF, S-CSCF)에 TS 102 677 표준의 감청기능을 적용하여 그림 2과 같이 IMS에서 적용 가능한 감청 아키텍처를 기능적 측면으로 제시하였다. P-CSCF는 감청대상이 처음으로 네트워크에 접근하는 지점이므로 감청권한과 승인정보생성을 비롯한 감청 활성화의 시작을 담당하는 AF를 포함한다. S-CSCF는 감청된 데이터가 전송되는 동안 실질적인 세션 제어서비스를 수행하기 때문에 CC, IRI, Triggering 정보를 처리하는 IRI-IIF, CC-IIF, TO(R)F[5], CCTF[6], MF(Mediation Function)를 포함한다. I-CSCF는 S-CSCF를 연결하고 송수신자 네트워크 사이를 이어주는 역할을 담당하지만 감청수행과 직접적인 연관성은 없다. 다수의 사업자가 운영하는 망에서의 감청방식은 기본적으로 Dynamic Triggering 방식이 사용되며 감청된 IRI로부터 획득한 감청대상의 정보를 근거로 CC 감청을 수행하는 메커니즘이다. 감청수행절차는 다음과 같다.

(1) LEA 측에서 감청요청과 동시에 감청 권한을 AF(Administration Function)에 전달한다. 감청대상이 IMS에 접근하기 위해 P-CSCF로 액세스한 후 S-CSCF를 통해 IMS 등록을 하고 이 과정에서 감청을 위한 준비가 시작된다.

(2) AF는 IRI-IIF에게 감청 승인신호를 보내고 IRI-IIF는 사용자 식별 정보 및 통신 관련정보를 포함한 IRI 감청을 수행한다. TOF는 감청 활성화를 위한 Triggering 신호의 시작점으로서 CC의 감청을 위해 CC Triggering Command를 CCTF에게 넘겨준다.

(3) GTO[7]와 GTR[8]은 서로 다른 두 영역의 출입구 역할을 하며 각 영역의 CCTF끼리 서로 Triggering 명령을 송수신 할 수 있도록 한다. 두 사업자 영역 사이에는 TTP(Trusted Third Party)를 두어 Triggering 명령을 승인하고 중재한다. 단일 사업자의 경우 GTO와 GTR은 TTP의 중재 없이 직접 Triggering Command를 전달할 수 있다. 이러한 방식으로 DT(Dynamic Triggering) 인터페이스를 통해 두 사업자 영역간의 Triggering 명령이 전송된다.

(6) Service Domain으로부터 감청권한을 전달받은 IP-CAN 영역에서는 IRI로부터 획득한 감청대상의 정보를 기반으로 실질적 통신 내용인 CC

5) TO(R)F: Triggering Origination(Receiving) Function
6) CCTF: Content of Communication Triggering Function
7) GTO: Gateway Triggering Originating
8) GTR: Gateway Triggering Receiving

를 감청하여 MF를 거친 후 LEMF로 전송한다. 감청된 CC 데이터와 Triggering Command가 전달되는 일련의 과정은 S-CSCF의 세션제어에 의한 데이터 전송을 통해 이루어진다. LEA측은 최종적으로 전달받은 IRI와 CC를 분석하여 감청된 내용을 확인할 수 있다.

4.2 추가적인 요구사항

4.1절에서 제안된 감청 아키텍처가 새로운 표준으로 제정되기 위해서는 다음과 같은 세부적인 추가기능 및 QoS가 향후 반영되어야 한다.

- 세션종료를 위한 BYE 메시지가 송수신 단말끼리 직접 전달된 후 세션이 종료되면 LEA 측에서는 감청의 종료시점을 파악할 수 없으므로 이를 알려주는 이벤트 메시지가 필요하다.

- 영장발부와 감청권한의 이동 그리고 CC와 IRI 감청, Triggering Command를 수행할 때 발생되는 지연 및 패킷손실을 최소화해야한다. 음성 및 화상통신과 같은 실시간 멀티미디어 서비스에서는 감청대상이 현재의 감청사실을 감지하지 못하도록 하는 QoS 제어기능이 필요하다.

- 이동통신에서의 로밍 기능은 필수기능 중의 하나이다. 감청대상이 로밍 서비스를 이용할 때 해외에서 네트워크 사업자 변경이 있을 경우 지연을 최소화시켜야한다.

5. 결론 및 향후연구

본 논문에서는 이동통신의 발달과 멀티미디어 서비스 확장에 따른 IMS 및 감청표준 동향을 소개하였고 현재의 감청표준이 안고 있는 한계점을 보완하고자 IMS 환경에서 사용될 수 있는 개선된 감청 아키텍처를 제안하였다. 또한, IMS에서 핵심 역할을 하는 CSCFs에 감청수행노드를 포함시킴으로써 IMS 환경에서도 원활한 감청을 수행할 수 있도록 기능을 확장하였다. 아울러, IMS 기반의 감청 표준에 최적화되고 네트워크의 QoS를 보장하기 위한 추가적인 요구사항을 제시하였다. 향후 연구로는 IMS 등록절차 및 세션종료와 관련된 감청이슈 그리고 세부적인 Triggering 신호 흐름에 대한 정의를 하고 시뮬레이션 툴(EXata[13])을 활용한 실험을 통해 개선된 감청 아키텍처의 효용성을 검증하고자 한다.

6. 사사

본 연구는 지식경제부 및 한국 산업기술 평가관리원의 산업 원천기술 개발사업(정보통신)의 일환으로 수행하였음. [KI001868, IMS/SIP기반 효율적인 Lawful Interception 기법 연구]

참고문헌

[1] M. Gorge, “Lawful interception key concepts, actors, trends and best practice considerations”, Elsevier Computer Fraud & Security, Volume 2007, Issue 9, September 2007, pp. 10-14.

[2] 염흥렬, “합법 감청 표준화 동향”, 정보통신연구진흥원 학술정보 2007권 33호

[3] 김무완, 우노 신타로, 이토우 료조우, 나카무라 미츠히로, “차세대 네트워크 서비스 제어 기술 IMS”, 광문각, 2008, p.22-29

[4] G.Camarillo, Miguel A. G. Martin, "The 3G IP Multimedia Subsystem, Merging the Internet and the Cellular Worlds", Willy, 2008, p.33-35

[5] 통신비밀보호법, 법률 제9819호, 2009.11.2 http://likms.assembly.go.kr

[6] Communications Assistance for Law Enforcement Act, http://www.calea.org

[7] IEEE Standard for Local and metropolitan area networks, Media Independent Handover Services, 2008.

[8] P.Hoffman, K.Terplan, "Intelligence Support Systems, Technologies for Lawful Intercepts", Auerbach Publications, 2006, p.74-81,85,86

[9] H. Labiod and M. Badra, New Technologies, Mobility and Security, 2007 Springer, pp. 207-216, 2007.

[10] ETSI TR 101 943 v2.2.1: Lawful Interception (LI); Concepts of Interception in a Generic Network Architecture

[11] ETSI DTS 102 677 v0.4.1: Dynamic Triggering of Content of Communication Interception

[12] ETSI TS 102 232-5 v2.4.1: Lawful Interception (LI); Part5: Service-Specific details for IP Multimedia Services

[13] http://www.scalable-networks.com/exata