

SIP/IMS Service Mobility 탐지를 통한 Lawful Interception Dynamic Triggering 기법에 관한 연구

이명락*, 이정빈**, 한영섭***

*공군 공중전투사령부 지휘통신과, **고려대학교 정보통신대학

***국방기술품질원 정보화 기획실

e-mail : myoungrak@gmail.com, jungbini@korea.ac.kr, yshan@dtaq.re.kr

A Study on Dynamic Triggering mechanism for Lawful Interception via a SIP / IMS Service Mobility detection

Myoungrak Lee*, Jung-Been Lee**, Youngsub Han***

*Dept. of Command & Communications, Air Combat Command, Korea

** Dept. of Computer Science and Engineering, Korea University

***IT Planning Dept., Defense Agency for Technology and Quality

요약

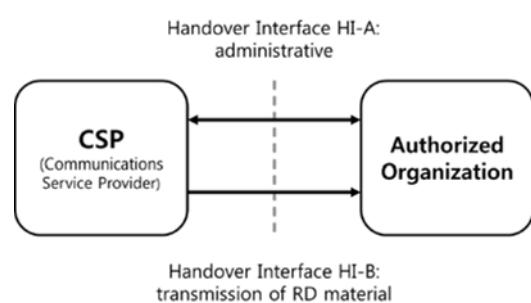
Lawful Interception (LI) 이란 합법적인 형태의 통신내용 및 관련 정보의 수집활동을 말한다. 최근의 4G LTE 기반의 이 기종 통신망에서의 합법적 감청은 전통적인 유선 및 3G 네트워크 중심의 감청기법 이외의 새로운 기법과 표준이 필요한 실정이다. 특히, LTE 와 같이 User Equipment (UE)가 네트워크상에서 핸드오버를 통해 자유롭게 이동하거나, 3G 와 같은 이 기종 망에서의 연결을 포함한 다른 사업자의 새로운 지역에서의 네트워크 연결이 보장되는 형태의 환경에서의 연속적 감청을 보장하는 것은 합법적 감청분야의 중요한 이슈중의 하나이다. 따라서, 본 논문에서는 국내의 4G-LTE 망을 중심으로 기존의 3G 망을 자유롭게 이동하는 네트워크 도메인과 IMS/SIP 기반의 서버의 연속성을 보장하는 서비스 도메인 영역에서의 합법적 감청 기법을 제안한다. 본 논문에서 제안하는 기법은 이 기종 무선망과 유선망이 혼재된 네트워크에서의 IMS/SIP 기반 서비스의 이동성을 감지하여 합법적 감청의 연속성을 보장하기 위한 기법을 포함하고 있다.

1. 서론

합법적 감청(LI: Lawful Interception)이란, 합법적 개인 통신망에 대한 공식적인 접근이 인가된 감청 행위를 말하며, 서비스 공급자나 네트워크 운용자로 하여금 수집된 통신정보를 사법집행기관에 공식적 제공을 위한 보안 프로세스를 말한다. 이러한 합법적 감청 행위는 국가 또는 각 지역별로 정해진 법률과 기술적 규정에 따라서만 이루어진다. 음성통신 위주의 1, 2 세대 통신기술과 달리 3, 4 세대 통신은 IP 기반의 VoIP, 금융거래, 영상제공 서비스 등 사용자 편의를 위한 다양한 컨텐츠를 제공하고 있다. 그러나, IP 이동성을 이용한 보이스 피싱, 패밍, 스미싱 등의 범죄 기술 역시 나날이 진화되고 있으며, 이는 국제테러를 포함한 다양한 형태의 위협적인 행위나 각종 범죄행위의 사전 탐지나 사후 추적을 매우 어렵게 하고 있다. 또한 사법수행기관(LEA: Law Enforcement Agencies)에 의한 적법한 절차에 따른 합법적 감청이라 하더라도 감청을 위한 아키텍처 및 세부 기술의 한계점으로 이동하는 감청 타깃에 대한 연속적 감청이 쉽지 않는 실정이다. 따라서, 최근의 4G-LTE 및 이를 포함한 이 기종 네트워크에서 운용되는 스마트폰 및 스마트 기기들에

대한 합법적 감청 이슈들의 특징은 사용자의 이동성과 IP 의 이동성 및 SIP 기반의 서비스 이동성까지도 고려되어야 한다 [2].

그림 1 은 유럽전기통신표준협회(ETSI: European Telecommunications Standards Institute)의 감청 정보 전달에 관한 표준[2]의 일부로써, 통신사업자가 보유하고 있는 감청관련 정보인 Retained Data (RD)의 전송을 위한 참조모델을 나타내고 있다. 본 참조모델은 RD 의 핸드오버 인터페이스(HI: Handover Interface)의 HI-A 와 RD material 전송에 관한 핸드오버 인터페이스인 HI_B 의 기능적 다이어그램을 보여주고 있다.



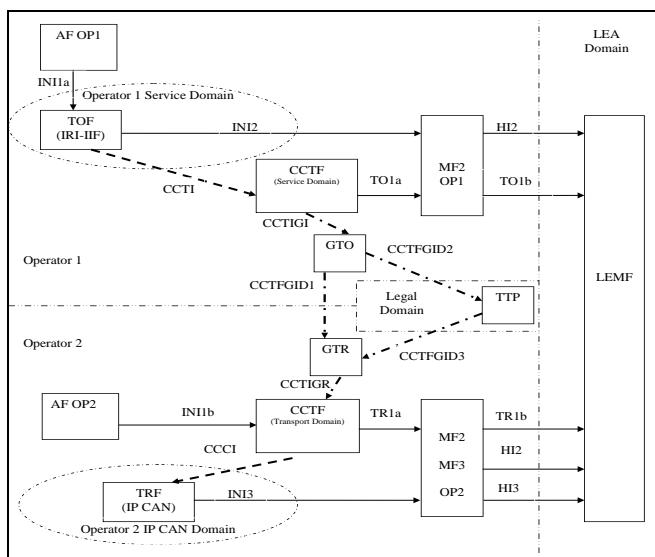
(그림 1) 핸드오버 인터페이스의 기능 [2]

* 교신저자

4G-LTE 기반 단일 네트워크에서 3GPP의 Evolved Packet System (EPS)으로 IP 기반의 서비스를 제공하고 있으며, EPS는 감청기관에 IP 기반의 RD를 제공할 수 있다. 그러나, SIP/IMS 기반의 서비스가 4G-LTE 망과 이 기종 망을 자유롭게 이동하는 상황에서는 다수의 네트워크 사업자 도메인에서의 감청이 이루어져야 하며, 여러 지역의 분산되어 있는 감청 타깃의 관련 정보들이 LI 서버로 보고되어야만 연속된 합법적 감청이 보장될 수 있다. 또한, 다수의 네트워크 사업자 환경에서는 모바일 유닛들의 이동에 따라 이들이 접속하는 망과 사업자의 위치가 달라 질 수 있는 환경에서는, 새로운 지역의 망을 접속할 때 부여 받는 주소 또한 달라진다. 이와 같은 환경에서 연속적 감청을 수행하기 위해서는 분산되어 있는 LIA (Lawful Interception Agent)들이 이동하는 합법적 감청 타깃에 대한 결과를 지속적으로 LI 서버로 보고할 수 있어야 한다.

2. 다수 사업자 망을 위한 ETSI의 감청 표준화 동향

그림 2는 ETSI의 IMS/SIP 기반 감청 표준 ESTI TS 102 677의 참조 모델[3]로 분리된 Monitoring Facility (MF)와 Content of Communication Trigger Function (CCTF)를 가지고 있는 다수 사업자의 Dynamic Triggering 모델을 나타낸다. 네트워크 사업자가 다수 일 경우, Content of Communications Triggering Function Gateway Inter Domain (CCTFGID)를 통해 전송된 Dynamic Triggering 명령을 승인하기 위한 법적 개입이 필요하다.



(그림 2) 다수의 사업자 망에서 분리된 CCTF와 MF 참조 모델 [3]

Trusted Third Party (TTP)는 Operator 영역 사이에 존재하며 국가 법 체제의 일부로서 국가기관에 의해 승인된 단체이며, Dynamic Triggering 명령 허가와 검사 기능을 제공한다. Operator 1의 CCTF와 Operator 2의 CCTF는 CCTFGID1을 통해 직접적으로 통신할 수도 있고, CCTFGID2/3를 통해 TTP를 거쳐 통신할 수도

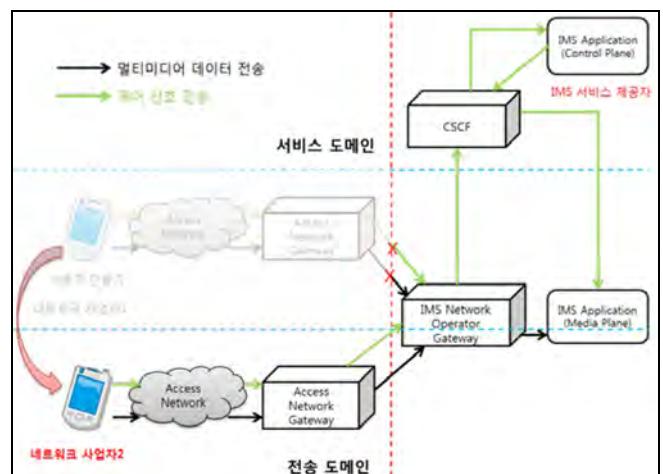
있다. 만약 Operator 2가 Dynamic Triggering을 지원하지 않는다면 TTP는 Operator 1에게 오류 메시지를 보내고, Operator 1은 Triggering Origination (TO1b) 인터페이스를 통해서 Law Enforcement Monitoring Facility (LEMF)에게 이를 알린다. 전통적인 참조 모델은 모든 요소들이 같은 단일 사업자 망에 존재하고, 공통의 MF를 가지고 있으며, IP 기반의 모든 접속 네트워크 (IP-CAN: IP-Connectivity Access Network)와 서비스 도메인을 위한 CCTF를 가지고 있는 간단한 Dynamic Triggering 구조와는 다르다.

감청의 실시는 Intercept Related Information Internal Interception Function (IRI-IIF)에서 이뤄지며, Dynamic Triggering은 Triggering Origination Function (TOF)에서 이뤄진다. 그림 2에서 통신 활동과 관련된 감청 대상의 IRI-IIF 다음으로, Content of Communication Triggering Interface (CCTI)를 통해 TOF에서 CCTF까지 정보를 전송한다. CCTF는 역시 CCCI를 통해서 특정 타깃의 통신 세션을 감청하기 위해 triggering 정보가 Triggering Receiving Function (TRF)로 보내지며, TOF, TRF는 Dynamic Triggering 명령어들을 주고 받는 논리적 기능들이다.

3. IMS/SIP Service Mobility 를 탐지를 통한 다수 사업자 망에서의 합법적 감청 활성화

3.1 다수의 네트워크 사업자에서의 Dynamic Triggering 수행 시나리오

ETSI의 SIP 감청 아키텍처(그림2)는 단일 또는 다수의 네트워크 사업자 도메인에서의 감청아키텍처를 구분하였다. 그러나, IMS상에서 언제, 어떤 노드나 기능들을 통해 어떠한 방식으로 Dynamic Triggering이 발생해야 하는지에 대해서는 구체적인 서술을 하고 있지 않다. 따라서, 본 연구에서 그림 2의 ETSI의 기본 아키텍처를 기반으로 그림 3과 같이 IMS/SIP기반에서의 연속적 감청을 위한 세부적인 시나리오를 제안하였다.

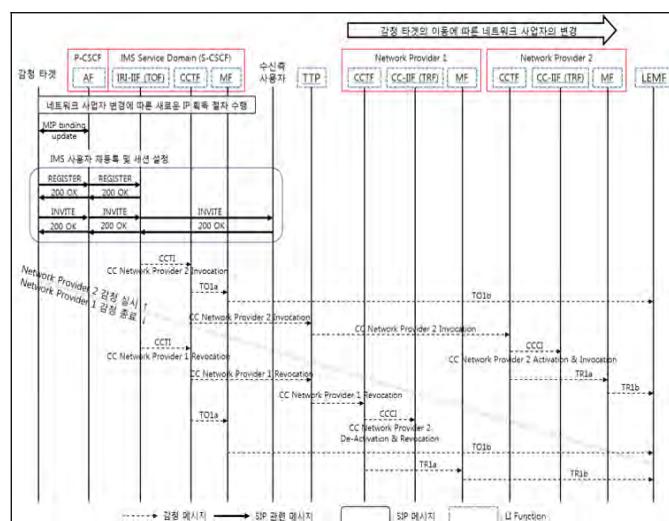


(그림 3) 다수의 네트워크 사업자의 이동에 따른 Dynamic Triggering 시나리오

기본적으로 IMS 에서는 사용자의 IP-CAN 이 변경되면, 다시 ‘REGISTER’ 메시지를 통해서 자신의 변경된 IP 와 URI 를 다시 등록하게 된다. 또한 이미 세션이 맺어진 경우에도 ‘RE-INVITE’ 메시지를 통해 지속적으로 세션관계를 유지하도록 한다. 하지만 Mobile IPv4 를 사용하는 GPRS 와 같은 망에서는 IP 가 변경되어도 SIP Mobility 의 특성상 상대방이 변경된 IP 를 알지 않고도 Home Agent 를 통해 지속적으로 통신을 유지할 수 있다. IP-CAN 레벨에서 변경된 IP 를 알려주지 않으면 사용자가 새로 자신의 IP 를 IMS 에 등록하지 않는 이상, 현재 유지되는 세션을 통해서는 감정을 수행하기 어렵다. 이에 대한 이슈사항은 네트워크 사업자 도메인 레벨과 IMS 서비스 도메인에서의 IP Mobility 에 관한 다양한 연구를 통해서 이루어지고 있다[4, 5, 6].

3.2 Dynamic Triggering 수행 절차

그림 4 는 IMS 사용자의 네트워크 사업자가 변경되어 IP 변화가 일어날 때 Binding update 를 Proxy Call Session Control Function (P-CSCF)로 보내어 IMS 서비스 도메인에서 이를 인식한다는 조건[7]을 적용하여 다수의 네트워크 사업자에서의 Dynamic Triggering 의 절차이다. 네트워크 사업자 1 에서 네트워크 사업자 2 로 감정 타깃이 이동하였을 경우의 전체적인 인터페이스와 메시지의 흐름을 나타내고 있으며, HI2 와 HI3 에 대한 메시지 전달 과정은 생략하였다.



(그림 4) 네트워크 사업자의 변화로 인한 Dynamic Triggering 메시지 흐름

IMS 서비스를 이용하는 사용자가 장소를 이동함에 따라 접속해 있는 네트워크 사업자가 바뀌면서 IP 의 변화가 일어난다. 예를 들어, GPRS 의 경우 ‘GPRS attach’ 절차를 통해 Serving GPRS Support Node (SGSN)으로부터 Home Location Register (HLR), GGSN 의 노드들을 통해 GPRS 네트워크를 이용하기 위한 인증을 거친다. 이 과정이 끝난 후, IMS 사용자 단말은 IPv4 또는 IPv6 네트워크 중에 하나와 연결하기 위한 ‘Activate PDP Context Request’ 메시지를 SGSN

에게 보낸다. 이 메시지는 특정 APN(Access Point Name)과 패킷 연결 태입에 대한 요청을 담고 있다. APN 은 발급 받은 IP 주소에 연결하고자 하는 네트워크와 주소 공간을 식별한다. IMS 사용자 단말의 경우 APN 은 연결하고자 하는 IMS 네트워크와 IPv4 또는 IPv6 와 같은 연결 태입을 나타낸다. SGSN 은 APN 와 연결 태입(IPv4 또는 IPv6)에 따라서 적절한 GGSN 을 선택한다. SGSN 은 이때 ‘Create PDP Context Request’ 메시지를 GGSN 에게 보낸다. GGSN 은 새로운 IP 주소를 할당하는 역할을 가지고 있으며, 할당 받은 IP 주소를 다시 IMS 사용자 단말에게 전달한다. 이와 같은 절차를 통해 P-CSCF 의 IP 주소도 획득할 수 있다. 새로운 IP 를 할당 받은 IMS 단말은 P-CSCF 에게 ‘Binding Update’ 메시지를 P-CSCF 에게 보내 IP 가 변경되었음을 IMS 서비스 도메인에게 알려준다.

● IMS 사용자 재등록 및 세션 설정

네트워크 사업자의 변화에 따라 IMS 사용자를 등록하고, 세션을 설정하는 두 가지 시나리오가 존재할 수 있다. 첫 번째는 사용자가 세션을 정상적으로 종료하고, 다른 네트워크 사업자로 이동한 후에 다시 IMS 서비스를 이용하는 경우 변경된 IP 주소를 바탕으로 다시 사용자 등록하고, 세션을 설정한다. 이와 같은 경우는 IMS 세션 설정이 이미 종료된 상태이기 때문에 감정 역시 이전에 종료되었으므로, 감정 활성화(Activation)가 사전에 수행되어야 하며 이와 같은 절차는 생략되었다.

두 번째 시나리오는 세션이 이미 설정되어 통신 중인 상태에서 IMS 사용자의 이동으로 인해 네트워크 사업자가 변경되는 경우이다. 네트워크 사업자 간의 통신은 앞서 말한 바와 같이 지속적으로 통신이 유지되지만 감정의 경우 변경된 IP 를 인지하지 못하므로, 변경 이전의 네트워크 사업자 망을 감시할 수 없다. 이때, IMS 는 ‘INVITE’ 메시지 대신 ‘RE-INVITE’ 메시지를 사용하여 현재 통신하고 있는 세션 설정을 업데이트 한다.

● 변경된 네트워크 사업자에 따른 감정 실시 및 종료

IRI-IIF 는 이 ‘INVITE’ 및 ‘RE-INVITE’ 메시지를 감시하여 변경된 IP 주소를 바탕으로 새로운 네트워크 도메인의 감정을 실시한다. 새로운 네트워크 도메인 2 에게 CCTF, TTP 를 통해서 감정 실시 메시지를 보내고, 그 후 네트워크 도메인 1 에게 감정 종료 메시지를 보낸다. 감정 실시와 종료 절차는 기본 감정 실시 및 종료 절차와 같다.

지속적인 감정을 위해서 먼저 네트워크 도메인 2 의 감정 실시 절차를 수행하며 최종적으로 CCCI 를 통해 실제 CC 감정이 실시(CC Network Provider 2 Activation & Invocation), 될 때 IMS 서비스 도메인의 IRI-IIF 가 감정 종료 메시지(CC Network Provider 1 Revocation)를 CCTI 를 기점으로 네트워크 도메인 1 에게 동시에 전달한다.

이미 세션이 설정되어 통신이 이루어지고 있는 경우,

사용자가 새로운 IP로 등록(*REGISTRATION*)을 수행하였을 때 이를 감지하여 세션 설정이 수행되기 이전에 미리 감청 절차를 수행하거나, 세션 설정과정과 함께 병렬적으로 수행하여 지속적인 감청을 실시할 수 있다.

TIIS, Volume 5 Issue 7, ISSN : 1976-7277 PP. 1329-1345, 2011.

4. 결론

본 연구에서는 IMS/SIP 기반의 서비스를 이용하는 모바일 유닛이 IP 이동성을 이용하는 네트워크에서의 활동뿐만 아니라 다수의 네트워크 사업자 망을 이동하는 환경에서의 연속적인 감청을 위한 아키텍처를 제안하였다. 본 연구에서 제안한 아키텍처는 4G-LTE를 포함한 이기종 네트워크에서의 다수의 사업자 망에서도 적용 가능한 Dynamic Triggering 기법으로 이동성이 나날이 발전하고 복잡해지는 네트워크 환경에서 합법적 감청의 연속성을 보장할 것으로 기대한다. 세부적인 기술적 적용은 ETSI를 포함한 국제표준들에서와 같이 각국 통신사업자가 관련 법규를 준수하는 제도가 선행되어야 할 것이다.

향후 연구는 본 논문에서 제안한 아키텍처를 기반으로 다수의 통신사업자 망에서의 복잡한 서비스를 이용하는 다양한 종류의 통신 패킷에 대한 연속적 감청의 효율성을 실험을 통하여 검증하고자 한다.

Acknowledgement

이 논문은 2015년도 정부(미래창조과학부)의 재원으로 한국연구재단-차세대정보·컴퓨팅기술개발사업의 지원을 받아 수행된 연구임(2012M3C4A7033345)

참고문헌

- [1] <http://tech.queryhome.com/42618/location-based-services-lcs-architecture-for-lte-eps>
- [2] ETSI TS 102 657 V1.3.1 (2009-09) Lawful Interception (LI); Retained data handling; Handover interface for the request and delivery of retained data
- [3] ETSI DTS 102 677 v0.2.2 (2009-12): Lawful Interception (LI); Dynamic Triggering of Content of Communication Interception
- [4] Faccin, S.M., Lalwaney, P., Patil, B., IP multimedia services: analysis of mobile IP and SIP interactions in 3G networks, Communications Magazine, IEEE, 42(1), pp.113-120, 2004.
- [5] TapfumaMvere, Neco Ventura, A Mobility Management Framework for the IP Multimedia Subsystem, SATNAC 2008.
- [6] AC Pang, JC Chen, YK Chen, PK Agrawal, Mobility and session management: UMTS vs. cdma2000, Wireless Communications, IEEE, 11(4), pp. 30-43, Aug. 2004.
- [7] Hoh Peter In, Myoungkak Lee, Dohoon Kim, Nunghoe Kim, Byungsik Yoon, Seamless Lawful Interception Handover for 3G IP Multimedia Subsystem (IMS), KSII