Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.6, Dec. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.6.1411

3G 네트워크에서의 IMS/SIP 기반 합법적 감청 기법

이 명 락,[1†] 표 상 호,[1] 인 호[2‡]
[1]공군 공중전투사령부, [2]고려대학교

Techniques study of IMS/SIP based Lawful Interception in 3G networks

Myoung-rak Lee,[1†] Sang-Ho Pyo,[1] Hoh Peter In[2‡]
[1]Air Combat Command of ROK Air Force, [2]Korea University

요 약

음성망 중심의 전통적인 합법적 감청(Lawul Interception) 기술 표준은 최근의 IP 기반 음성망(VoIP)과 다양한 종류의 멀티미디어 어플리케이션에 대한 연속적 추적이나 네트워크를 이동하며 통신하는 IMS(IP Multimedia Subsystem)/SIP(Session Initiation Protocol) 기반의 패킷을 연속적으로 추적하기에는 기술적 한계를 가지고 있다. IMS/SIP에 대한 합법적 감청에 관한 기술 표준은 유럽의 ETSI(European Telecommunications Standards Institute)중심으로 표준 아키텍처를 제시하고는 있으나 연속적 감청 기법의 상세한 표준과 기술의 제시는 미흡하거나 공개를 제한하고 있는 실정이다. 본 논문은 전통적인 음성위주의 감청기법이 가지고 있는 한계를 극복하고 이동 중인 합법적 감청 대상 노드에 대한 IMS/SIP 기반의 연속적 감청을 위한 아키텍처를 제안하였다. 또한, 제안된 아키텍처의 효율성을 검증하기 위하여 시뮬레이션 상에 50개 이상의 감청 대상 노드와 패킷 통신을 구현하였다. 실험결과는 ETSI가 제시하고 있는 기존의 합법적 감청 아키텍처에 비해 높은 효율성과 연속적 패킷 수집에서의 기술적 고려요소들을 새롭게 식별하였다.

ABSTRACT

Lawful interception(LI) standard of telephone networks has technical limitations to lawfully intercept IMS/SIP-based mobile communication network subscriber who using Android and iPhone device. In addition, the technical standards related to legal interception of the IMS/SIP of the wireless network is insufficient compared to the systematic study of the development of a wireless network infrastructure. The architecture proposed in the standard of ETSI(European Telecommunications Standards Institute) for the seamless LI is insufficient to overcome the limitations of traditional voice-centric LI techniques. This paper proposes an IMS/SIP-based architecture to perform LI under 3G networks that focuses on mobility-supported environments with merging cellular networks and the Internet. We implemented the simulation to verify the efficiency of the proposed architecture, and the experimental results show that our method achieves higher lawful interception rate than that of existing interception methods.

Keywords: Lawful Interception, IMS/SIP, 3G Networks

I. 서 론

합법적 감청(lawful Interception)이란 사법수행기관이 영장 발부의 합법적 권한을 가지고 감청 대상의 음성, 영상, 이메일 등의 분석 또는 증거를 추적하기 위해 통신망의 데이터를 획득하는 것을 말한다[1,2]. 최근, 다양한 종류의 IP기반의 SNS 및 음성통신망 서비스가 급증하고 있으며, 이를 이용한

Received(08. 04. 2015), Modified(10. 19. 2015), Accepted(10. 21. 2015)

† 주저자, myoungrak@gmail.com
‡ 교신저자, hoh_in@korea.ac.kr(Corresponding author)

범죄행위 또한 증가하고 있다. 그러나 이들 IMS/SIP 기반의 통신망에 대한 합법적 감청 기법의 표준 아키텍처는 초보적인 연구수준에 머물러 있다. 이는 다양한 기법을 이용한 IMS/SIP기반의 범죄행위 및 사전 범죄모의 등에 대한 사전 탐지를 매우 어렵게 하고 있다. 또한, 범죄 발생이후 추가범죄 예방을 위하여 무작위로 이동 중인 감청대상 노드에 대한 합법적 사후조사나 연속적 추적을 어렵게 한다. 따라서, 통신망을 이용한 각종 범죄행위의 조사 및 사전 예방, 사후 조사 등을 위해서 다양한 어플리케이션에 대한 LI는 매우 중요한 문제로 대두되고 있다.

II. 관련 연구

2.1 ETSI의 합법적 감청 표준화 동향

유럽의 감청 표준화는 유럽 표준화 기구인 ETSI (European Telecommunications Standards Institute)의 LI TC 중심으로 활발히 진행되고 있으며, 43개 이상의 회원국이 서명한 유럽위원회에서 마련한 사이버 범죄 조약이 이를 지원하기 위한 법률 제도의 근간이 되고 있다. 또한, 서명 회원국은 실시간 데이터 수집을 위한 제도적 조치를 도입하도록 되어 규정하고 있으며, 대부분의 서명국이 자국의 정보통신사업자들에게 ETSI 표준에 기반한 합법 감청 기술을 지원할 것을 요구하고 있다[3]. ETSI의 LI에서 다루는 결과물은 크게 두 가지 이다.

하나는 통화 관련 데이터인 IRI(Intercept Related Information)이고 다른 하나는 통화 내용인CC(Communication Contents)이다. IRI는 대상 통신에 대한 시그널링 정보, 수신자 및 송신자의 정보(IP, MAC address 혹은 전화번호 등), 통신의 횟수, 기간, 시간 등의 정보를 말하고, CC는 통신의 내용인 음성, 비디오, 데이터 등을 말한다[4]. Fig. 1은 네트워크에서 수집된 감청 내용(CC)과 감청 관련 정보(IRI)가 감청 모니터링 장치(LEMF)로 전송됨에 있어 각각의 핸드오버 인터페이스를 통해 전달되는 일반적인 아키텍처를 나타낸다. Fig. 1에 나타낸 주요 기능과 기관의 기능은 다음과 같다.

- IIF(Internal Intercepting Function): 네트워크 또는 네트워크의 요소에서 통신의 내용물(Contents)을 활용 가능한 지점
- INI(Internal Network Interface): IIF와 Mediation Device 사이의 네트워크 내부 인터페이스
- LEA(Law Enforcement Agency): 국가의 법률에 근거하여 전기전자통신상의 감청자료를 획득할 수 있는 권한을 부여 받은 조직 또는 기관을 뜻한다.

Fig. 1.에서 ADMF(Administration Function)은 LEA로부터 감청에 관한 요청을 받아 이를 IIF에 보낸다. IIF는 전술상으로 네트워크 노드 안에 존재하며 두 가지 종류의 정보 통화 내용(CC)과 통화 관련 데이터(IRI)를 생성하며, Meditation Function(MF)은 두 개의 네트워크 사이의 연결을 담당한다. 이것들은 PSTN안에서 통신하기 위한 Internal Network Interface(INI)와 요청된 정보를 하나 이상의 LEMF에 보내기 위한 표준화된 인터페이스를 구현한다[5, 6].

합법적 감청에서의 핸드오버 인터페이스 종류는 Fig. 1.에서와 같이 HI1, HI2, HI3으로 나누어지며, 감청권한 부여를 위한 Authority 및 Authorization에 관한 내용은 주로 HI1에서 다룬다. 핸드오버 인터페이스2(HI2)는 통신 사업자가 사법감시기관 사이에서 감청 관련 정보(IRI)를 전달하기 위해 사용되며, 핸드오버 인터페이스3(HI3)는 감청된 콘텐트 정보(CC)를 사법감시기관에 전달하기 위해 사용된다. ETSI에서 제시한 감청표준의 핸드오버 인터페이스 기능 중 HI1은 HI2, HI3와 달리 임무(tasking)와 관리(management)의 관한 내용을 통신하기 위하여 사용되며, 보안상의 이유로 문서에서는 감청에 사용되는 완전한 절차를 공개하지는 않고 있다[7].

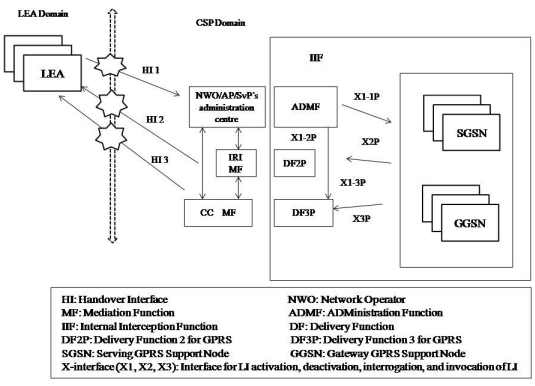

Fig. 1. LI Reference model of GPRS[5]

2.2 미국의 합법적 감청 표준화 동향

미국은 합법적 감청과 관련하여 CALEA(The Communications Assistance for Law Enforcement) 등 4개의 주요 법률을 가지고 있다.

1994년, 미 의회는 CALEA를 통하여 모든 통신사업자로 하여금 법률에 근거하여 합법적 감청기관을 위한 네트워크 기반을 유지하도록 명시하였다. 특히, 9/11 테러 공격 이후, 미 의회는 The USA PATRIOT Act에 의해 전자감시를 더욱 강화하였다. 이 법률은 이미 외국인 감시를 위해 시행하고 있던 FISA를 확장한 것이다. CALEA의 법령에 의하면 통신사업자는 신속하고도 조용하게 고객의 통신망에 접근할 수 있는 능력을 구비하도록 요구 받고 있다.

CALEA는 전기 통신 사업자가 그러한 능력을 구비하기 위하여 소요되는 장비 및 시설비에 대한 보상에 관하여도 규정하고 있으며, 1995년 이전에 만들어진 장비도 CALEA의 법령을 따르도록 규정하고 있다. The USA PATRIOT Act는 미 연방의 전자감시의 영역을 확대한 법률로서 테러리스트, 컴퓨터 기만행위, 금융 사범의 행위를 TitleⅢ의 감청 대상에 포함 시켰다. 미국의 CALEA는 합법적이며 제한적인 감청 정보의 활용에 관한 기준은 연방 통신위원회인 FCC(Federal Communications Commission)와 법원의 해석을 따르도록 하고 있다.

FCC는 미 통신산업협회(TIA)로 하여금 통신사업자 및 전기통신과 관련된 일반사업자의 의견이 반영된 임시 표준제정을 허락하고, 이를 반영한 최종 표준을 규칙제정공고(NPRM)을 통해 공지함으로써, 최종적인 표준의 시행 전 의견수렴 과정을 거쳤다

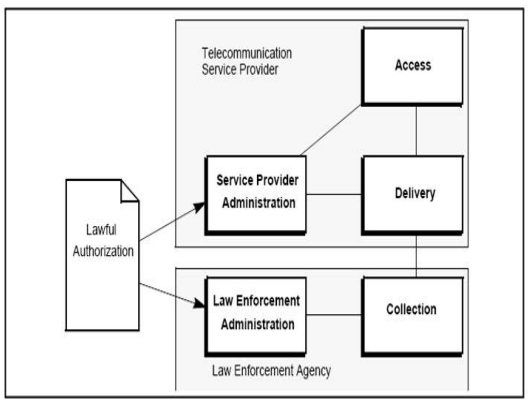

Fig. 2. Electronic Surveillance Model of CALEA[8]

[8]. 일반적으로 CALEA에서는 Fig.2.의 모델에서와 같이 전자 감시, 즉 감청을 위하여 access, delivery, collection, service provider administration의 5개의 카테고리를 필요로 한다. Fig. 2.은 CALEA의 전자 감시를 위한 일반적이고 기본적인 모델을 보여주고 있으며, 이들 기능은 실제 구현에 관한 상세한 기술적 문제보다는 기능적 측면에서 많은 논의가 이루어지고 있다[9, 10].

2.3 IMS/SIP기반의 감청표준화 동향

IMS/SIP 기반의 감청 표준 동향은 ETSI 중심으로 가장 활발히 이루어지고 있으며,ETSI의 SIP 감청 아키텍처는 단일 네트워크 사업자 도메인에서의 감청 아키텍처 또는 다수의 네트워크 사업자 도메인에서의 감청아키텍처로 구분할 수 있다[11].

Fig. 3은 ETSI의 IMS/SIP 기반 감청 표준 ESTI TS 102 677의 참조 모델로 공통 MF와 CCTF를 가지고 있는 단일 사업자의 Dynamic Triggering 모델이다. 전통적인 참조 모델은 모든 요소들이 같은 단일 사업자 망에 존재하고, 공통의 MF를 가지고 있으며, IP 기반의 모든 접속 네트워크(IP-CAN)와 서비스 도메인을 위한 CCTF(Content of Communication Trigger Function)을 가지고 있는 간단한 Dynamic Triggering(DT)에 대해서 표현한다.

합법적 감청의 준비와 감청의 활성화, 감청의 실시 등은 IRI-IIF(Internal Interception Fuction)에서 이루어지며, dynamic triggering은 TOF에서 이루어진다. Fig. 3에서 통신 활동과 관련된 감청 대상의 IRI-IIF 다음으로, CCTI를 통해 TOF에서 CCTF까지 정보를 전송한다. CCTF는 역시 CCCI를 통해서 특정 타겟의 통신 세션을 감청하기 위해 triggering 정보를 TRF로 보낸다. TOF와 TRF는 Dynamic Triggering 명령어들을 주고 받는 논리적인 기능들이다. CC-IIF의 기본적인 동작은 전통적인 non-dynamic triggering 감청과 다르지 않지만, 감청 대상의 ID와 다른 CC LI 정보들은 TOF를 통해서 감청 시작이 요청되기 전의 임의 지점보다 통신이 시작되는 시점에 CC-IIF로 전달된다.

TOF, CCTF와 TRF가 모두 같은 사업자 네트워크 망에 존재하기 때문에, CCTF는 TOF로부터 전송 받은 Dynamic triggering 명령어들이 합법

적으로 공인되었음을 절대적으로 신뢰할 수 있다. 그러므로 이 시나리오에서 AF(Administration Function)으로부터 전달받는 영장 집행 인터페이스(INI1b)는 CCTF에게 필요하지 않다. TO1a와 TO1b 참조 지점은 MF를 거쳐 연관성과 IP-CAN ID 정보와 함께 Dynamic triggering 감청이 시작되거나 재시작 되었다는 것을 LEMF에게 알리는데 사용된다.

또한 LEMF가 HI3 스트림이 Dynamic triggering을 위한 HI2와 상관성이 있음을 인식하는데 도움을 준다[12]. ESTI TS 102 677 표준은 IMS와 마찬가지로 서비스와 액세스 도메인이 하나의 사업자 또는 다수의 사업자로 분리된 아키텍처에서의 감청에 대한 개념에 대해 명시하고 있다. 각각의 도메인에서 감청될 트래픽(예를 들어, HI2를 통해 전달되는 IRI와 HI3를 통해 전달되는 CC의 결정을 위해, 서비스와 전송 도메인 등 다른 도메인에서 사용되는 주소들 (예를 들어, 서비스와 전송 도메인) 개체들 간의 관계, 혹은 고정된 개체에서 이루어지는 통신의 합법적 감청을 명시하고, CC의 동적 감청 실시를 수행하기 위한 프레임 워크와 아키텍처를 정의한다. 또한, Dynamic Triggering을 위한 명세를 제공한다. 하지만 IMS상에서 언제, 어떤 노드나 기능들을 통해 어떠한 방식으로 Dynamic Triggering이 발생해야 하는지에 대해서는 ESTI TS 102 677 표준에서는 구체적인 서술을 하고 있지 않다.

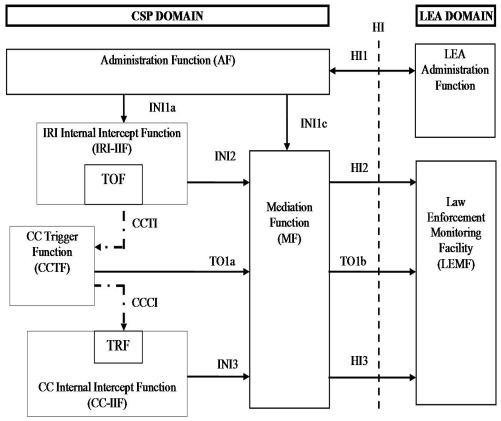

Fig. 3. Dynamic Triggering reference model of a single CSP with a common MF and CCTF[11]

III. IMS/SIP의 연속적인 합법적 감청 제안

3.1 IMS/SIP 메시지를 활용한 LI 수행

IMS에서의 3G 무선망은 다음 그림과 같이 사용자와 세션의 이동성(mobility)를 위해 CS(Circuit Switched) 도메인과 PS(Packet Switched) 도메인으로 나누어져 있으며 독립적이다[13].

Fig. 4.와 같이 서비스 사업자 도메인과 네트워크 도메인이 분리된 IMS기반의 무선망에서는 기존의 합법적 감청 수행방법과는 다른 방법으로 수행되어야 한다. 특히 서비스 사업자와 네트워크 사업자가 서로 다를 경우, 동일한 IMS 서비스를 이용하더라도 해당 IMS 서비스 사업자는 네트워크 사업자에게 감청 권한을 위임할 수 있어야 한다[14].

전통적인 감청 방법과는 달리, 이동하는 노드에 대한 합법적 감청은 내부적인 인터페이스를 통해 감청 권한을 가진 영장을 위임해야 하며 Dynamic

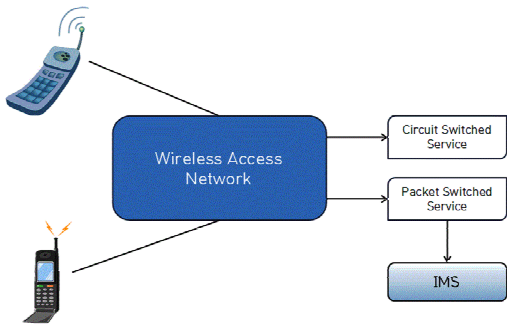

Fig. 4. Relationship between IMS and CS / PS domain

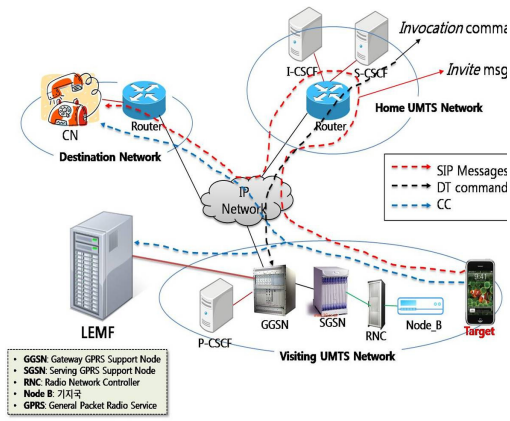

Fig. 5. Overview of LI activation by IMS-level register

Triggering을 통해서 다음 네트워크 사업자에게 감청 권한을 위임이 가능하여야한다.

본 논문에서는 IMS 상에서 발생될 수 있는 Dynamic Triggering 시나리오를 포함하여 단일 네트워크 사업자에 대한 기본적인 IMS/SIP 기반의 LI 수행 기법을 제안하였다. Fig. 5.는 IMS-level 등록을 통한 감청 활성화(Activation) 방안을 도식화한 내용이다.

3.2 IMS-level 등록을 통한 감청 활성화

Fig. 6.은 본 논문에서 제시한 IMS-level 등록을 통한 감청 활성화 방안과 과정을 제시한 그림이다. IMS 서비스 사업자의 AF가 P-CSCF에 포함되어 위와 같은 활성화 과정을 수행하며,'IRI Activation' 명령으로 감청할 정확한 타겟의 식별자를 필요로 하지 않고 단순히 미리 부여 받은 TRF 내의 감청 영장을 활성화시키는 작업을 수행한다. 또한 'IRI Invocation' 명령은 정확한 타겟식별자 정보를 활성화된 영장에 적용시켜 실제 IRI 감청을 실시하는 작업이다. 네트워크 사업자에서는 내부적으로 AF가 감청타겟이 IP 주소를 획득한 이후로 'CC Activation' 명령을 통해 감청을 활성화한다. CC 감청을 실시하지 않고, IRI 감청만 실시하는 이유는 아직 IMS 서비스에 세션이 맺어지기 전이기 때문에 실제 감청 내용은 발생되지 않기 때문이다.

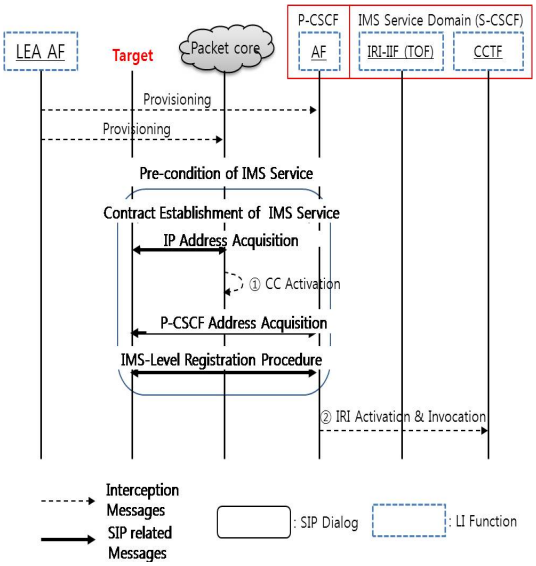

Fig. 6. LI activation Procedure by IMS-level register

3.3 세션 설정(INVITE) 메시지를 통한 감청 실시 (Invocation)

Fig. 7.과 같이 감청 타겟이 'REGISTER' 메시지를 통해 자신의 URI를 등록한 후, 통신을 원하는 상대와 세션을 설정하기 위해서 'INVITE' 메시지를 통해 수신측 사용자에게 통신을 요청한다.

'INVITE' 메시지의 Request-URI 헤더에는 수신측 URI와 Contact 헤더에는 감청 타겟 URI를 포함하고 있다. 감청 타겟의 URI는 'REGISTER' 메시지를 통해서 S-CSCF가 가지고 있으므로, IRI-IIF는 S-CSCF에서 'INVITE' 메시지를 감청한 후에 감청 타겟의 URI가 맞다고 판단되면 IRI-IIF에 속해 있는 TOF를 통해서 Dynamic Triggering을 실시하게 된다. S-CSCF는 세션 제어의 중심적인 SIP 서버로 감청 기능 중에 TOF(IRI-IIF)의 기능과 CCTF의 기능을 모두 수행할 수 있는 능력을 가지고 있으며, 세션 설정에 관련된 SIP 메시지를 감청하여 Dynamic Triggering을 수행할 수 있는 역할을 맡는다.

S-CSCF는 HSS로부터 다운로드 받은 가입자 정보를 보관 유지하므로, IMS MF를 통해 LEMF에게 감청 타겟의 정보를 전달 할 수 있다. 또한 B2BUA 기능을 통해 세션의 개시, 종료 및 SIP 메시지 경로를 감청할 수 있으므로, LEMF에게 지속적으로 SIP 메시지 감청 정보를 전달할 수 있다.

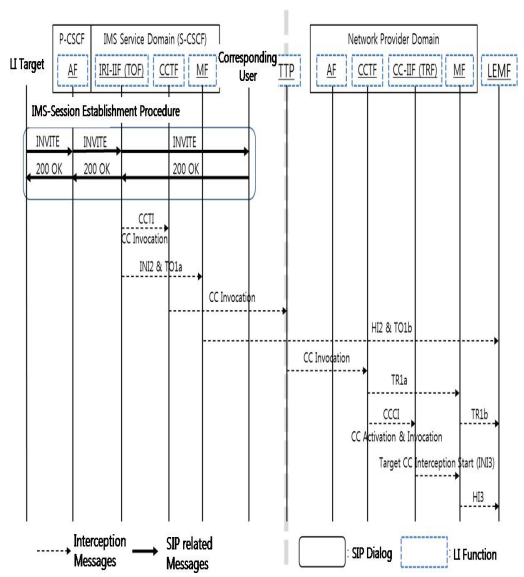

Fig. 7. The flow of messages for LI

3.4 Dynamic Triggering 시작

TOF에서 CCTI를 통해 CCTF로'Invocation' 명령어와 함께 현재 감청 타겟의 식별자로써 사용자 URI를 전달한다. 사용자 프로파일 및 SIP 메시지 감청의 세부 절차는 다음과 같다.

만약 네트워크 사업자가 Dynamic Triggering을 지원하지 않는 사업자라면, 오류 메시지를 반환하고 TO1b를 통해 LEMF에게 오류를 알린다.

3.4.1 사용자 프로파일 및 SIP 메시지 감청

사용자 프로파일 및 SIP 메시지의 감청을 위하여 IMS의 세션 설정 메시지를 이용한 합법적 감청 실시의 과정은 Fig. 8과 같다. Fig 8의 SIP 메세지 감청과정을 순서적으로 나타내면 먼저 IRI-IIF에서 INI2와 TO1a를 통해 MF로 IRI 관련 감청 데이터를 전달하고 이어서 INI2를 통해서는 S-CSCF에 저장된 타겟의 프로파일을 MF에 전달하여 감청 타겟의 프로파일을 입수한다. 또한 TO1a를 통해 'Invocation' 명령어와 타겟이 통신하는 네트워크 사업자의 식별자 및 전달되는 SIP 메시지들을 MF로 전달한다. TO1a를 통해 어떤 SIP 메시지들을 주고 받는지 감청할 수 있다. HI2와 TO1b는 각각 INI2와 TO1a 데이터를 MF에서 LEMF로 전달하는 인터페이스이다. TO1b는 TTP가 에러 메시지를 보낼 경우, 에러 메시지의 전달을 담당해야 하기 때문에 Dynamic Triggering 명령어가 TTP에 전달되고 난 후에 일어나야 한다.

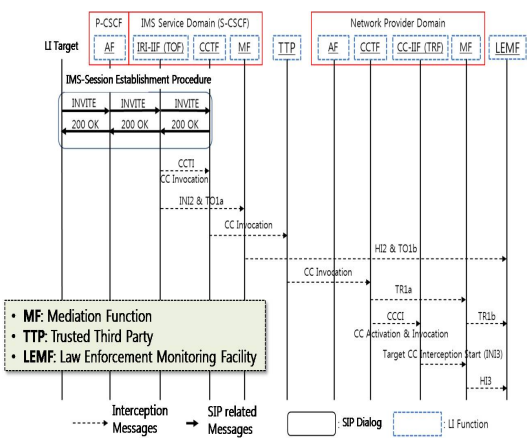

Fig. 8. Invocation of LI by the session set-up message

3.4.2 TTP에게 Dynamic Triggering 명령어 전달

감청 타겟이 통신하고자 하는 네트워크 사업자에게 'Invocation' 명령을 전달하기 위해 CCTIGI와 CCTFGID2를 통하여 TTP에게 전달한다. TTP는 'Invocation'명령어 헤더를 분석하여 유효한 영장 및 명령인지 확인하고, 통신하고자 하는 네트워크 사업자가 Dynamic Triggering을 위한 구현이 되었는지 체크한다. 모든 조건이 만족하면 네트워크 사업자에게 'Invocation' 명령을 전달한다.

이와 같은 절차를 통해 'Invocation' 명령이 감청 타겟이 통신하고자 하는 네트워크 사업자 도메인에게 전달되고, 비로소 CC에 대한 감청이 수행된다.

3.4.3 REGISTRATION 타임아웃과 감청의 종료

IMS 사용자가 통신 세션을 종료할 때에는 사용자 URI를 등록하는 'REGISTER'나 세션 설정을 위한 'INVITE' 메시지와는 다르게, P-CSCF나 S-CSCF 등을 경유하지 않고 직접 'BYE' 메시지를 주고, 응답을 받아 세션을 종료한다. 따라서 'BYE' 메시지를 통한 세션 종료 명령어로는 IMS 서비스 도메인에 포함되어 있는 감청 기능들이 세션의 종료를 감청할 수 없다. 하지만 IMS 사용자간에 통신이 지속될 경우, 최초 'REGISTER' 명령어를 통해 지정한 Expiration Time이 타임 아웃 될 때마다 등록상태를 갱신하기 위해 S-CSCF에 일정간격으로 'REGISTER' 명령과 동일한 순서로 'RE-REGISTRATION' 요청을 한다. 'BYE' 명령어를 통해 세션이 종료되었을 경우, 타이머가 타임아웃이 되었을 때 더 이상 사용자의 등록 상태가 갱신되지 않기 때문에타임 아웃이 되면, S-CSCF는세션이 종료되었다는 'NOTIFIY' 메시지를 P-CSCF에게 전달하고다시 P-CSCF는 사용자에게 전달한다. 사용자가 다시 이에 대한 응답을 S-CSCF에 보내면 관련된 모든 세션을 해제한다.

따라서 IMS 서비스 도메인에 속한 IRI-IIF가 타임 아웃이 발생하면 이를 감지하여 감청의 중지를 위한 'Revocation' 명령어 전달 절차가 수행된다.

'Revocation' 명령어는 TRF에서 현재 감청이 실시되는 타겟의 식별자의 제거를 수행함으로써 모든 감청 활동이 종료된다.

결과적으로 네트워크 사업자의 CCTF는 'CC Deactivation & Revocation'명령을 수행한다.

Deactivation에 의해서 감청에 대한 영장이 제거됨과 동시에 해당 영장과 관련된 모든 타겟식별자들의 모든 감청 활동이 종료된다. Fig. 9는 이를 위한 인터페이스와 메시지의 흐름을 나타낸다.

Fig.9의 감청종료 프로세스는 먼저 ①세션 종료에 따른 타임 아웃 발생으로 송신측과 수신측의 세션 종료 과정을 통해 S-CSCF에서 타임 아웃 이벤트가 발생한다. 이 이벤트가 발생됨과 동시에 세션이 종료되었다는 'NOTIFY' 메시지를 P-CSCF를 거쳐 송신 측(감청타겟)에 보내고, 송신측의 응답으로 인하여 S-CSCF에서 관련된 모든 세션을 종료한다.

②감청 종료 메시지의 전달은 IRI-IIF에서는 S-CSCF에서 발생되는 타임 아웃을 감시하여 감청 타겟의 세션이 종료되었음이 확인되면, TOF가 CCTI를 통하여 'CC Revocation' 명령어를 전달한다. 'Invocation'과 마찬가지로 감청 식별자를 포함하여 실시중인 감청 타겟의 감청 활동을 종료시킬 수 있게 한다. ③세션 종료에 관련된 SIP 메시지 전달은 TO1a 인터페이스를 통해서 IRI-IIF가 MF에게 관련된 모든 세션의 종료를 위한 SIP 메시지들을 전달하여 세션이 종료되는 과정을 전달한다. TO1b 인터페이스는 MF에서 LEMF로 TO1a 데이터를 전달한다. ④TTP에게 'Revocation' 명령어 전달은 'Invocation' 명령어 전달과 마찬가지로 'Revocation' 명령어를 CCTIGI와 CCTFGID2를 통하여 TTP에게 전달한다. TTP는 'Revocation' 명령어 헤더를 분석하여 유효한 영장 및 명령인지 검증한 후 네트워크 사업자의 CCTF에게 전달한다.

⑤감청 타겟의 감청 활동 중단과 영장 삭제은 'CC Revocation' 명령어를 전달 받은 네트워크 사업자의 CCTF는 CCCI를 통해서 CC-IIF에게 전달되며, TRF가 'CC De-Activation & Revocation' 명령어로 해당 감청 타겟의 모든 감청 활동을 중단시키고 감청 권한을 가진 영장을 삭제할 수 있다.

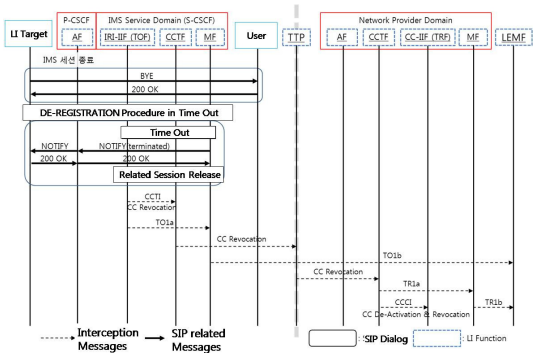

Fig. 9. The end of the LI by the end of the REGISTRATION timeout

3.5 제안한 IMS/SIP 기반의 LI 실험 결과

본 논문에서 제안한 아키텍처의 효율성 검증을 위한 실험환경 구성은 OPNET 16.0A를 이용하였으며, Fig.5.에서와 같이 3G 무선망에서의 이동하는 노드의 SIP/IMS에 대한 연속적 감청환경 구성을 위해 OPNET Modeler를 사용하여 구성하였다. IMS 기반 서비스의 중추적 역할을 수행하는 SIP 서버(P-CSCF, S-CSCF, I-CSCF)와 SIP 메시지 처리기능 및 기타 SIP 프로토콜을 구현하였다.

Fig. 5.와 같은 실험환경은 SIP서버 중 프록시 서버 역할을 하는 P-CSCF와 세션제어를 담당하는 S-CSCF를 중심으로 구축되었으며, 감청 타겟이 속해 있는 UMTS 네트워크망과, 다수의 노드로 이루어져 있으며, UMTS 네트워크 망은 기본적으로 IP Network와 연결된 GGSN을 시작으로 SGSN, RNC, 무선통신을 위한 Node B 순서로 연결하였다. 'Destination network' 망을 구성하여 감청 타겟과 통신하는 상대 노드를 구성하였으며, 감청 타겟의 상대 노드는 IMS 서비스를 이용하는 유선 사용자로 가정하였다. 시뮬레이션 상의 감청 서버(LEMF)는, 감청 타겟이 통신하는 내용을 감청하는 감청서버 역할을 수행하며, 다음과 같은 사양의 감청 서버로 구성하였다. 세부 실험환경 설정은 다음과 같이 공통변수, 독립변수, 그리고 종속변수로 나누어 다음과 같이 구성하였다.

- ● 공통 변수: 통화 유지 시간(3분)
- ● 독립 변수
  - 노드의 개수: 10개, 30개, 50개
  - 감청서버(LEMF)의 대역폭: 1G, 10G
  - VoIP 코덱: G.728 (16kbps), G.729 (8kbps)
  - 통화 유지 시간 확률 분포: exponential, poison
- ● 종속 변수
  - Voice application: Jitter (sec)
  - Voice application: MOS(Mean Opinion Score)
  - Voice application: Packet End-to-End Delay (sec)
  - Point-to-point: Throughput (packets/sec)

Table 1. Scenario set

Number of Nodes	Bandwidth	Codec	Probability Distribution	Scenario
10, 30, 50,	1G	G.728 (16kbps)	Exponential	Scenario 01/09/17
			Poission	Scenario 02/10/18
		G.729 (8kbps)	Exponential	Scenario 03/11/19
			Poission	Scenario 04/12/20
	10G	G.728 (16kbps)	Exponential	Scenario 05/13/21
			Poission	Scenario 06/14/22
		G.729 (8kbps)	Exponential	Scenario 07/15/23
			Poission	Scenario 08/16/24

본 논문에서 제안하는 실험환경에서 감청대상 노드 수는 Table 1.에서와 같이 10개, 30개, 50개 순으로 늘려가며, 2종류의 코텍과 지수(Exponential) 분포 및 포아송(Poisson) 분포의 확률을 적용한 8가지의 시나리오를 적용하여 연속적 감청의 효율성을 측정하였다. 실험결과 Fig. 10.은 통화유지시간

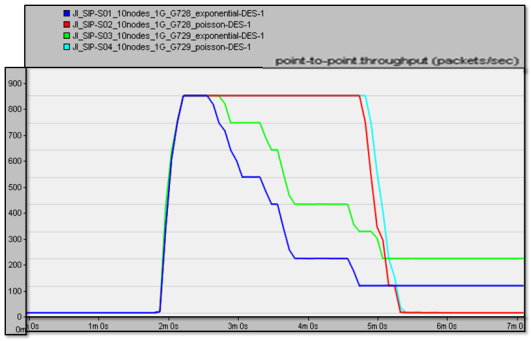

Fig. 10. Changes in throughput of Exponential and Poisson distribution

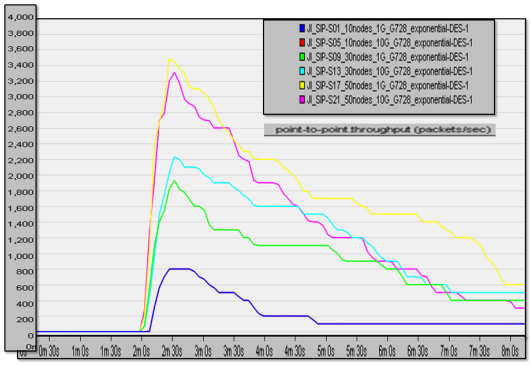

Fig. 11. Changes in throughput according to the bandwidth

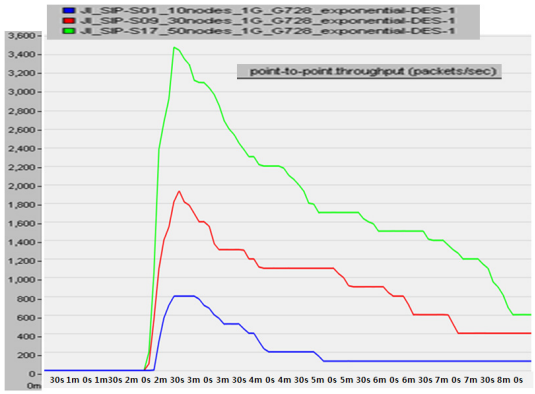

Fig. 12. Changes in throughput according to the number of LI nodes

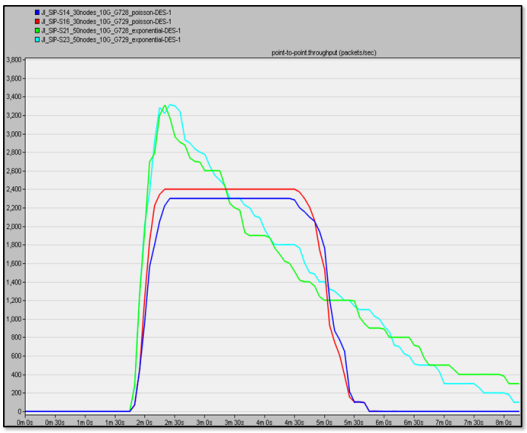

Fig. 13. Changes in the throughput of the Poisson and exponential VoIP codec

확률분포에서 지속적으로 동시 감청노드가 유지되는 포아송 분포가 지수분포보다 처리율이 높게 나타났으며, Fig. 11.에서와 같이 노드가 늘어날수록 동시 감청 대상수가 늘어남에 따라 낮은 대역폭(1G bps)에서 처리하는 패킷의 처리량이 많아져 6.7% 높은 처리율을 보였다.

Fig. 12.은 감청 대상 노드수가 50개까지 늘어날수록 10개의 노드에 비해 425% 높은 처리율을 보이며, 이는 노드가 많아짐에 따라 회선이 처리해야할 패킷의 수가 증가함을 나타낸다. Fig.13.은 G. 729(8kbps)의 패킷량이 G 728(16kbps) 패킷의 양보다 적기 때문에 상대적으로 낮은 처리율을 보였다.

IV. 결 론

본 논문에서는 3G 무선망에서 IMS/SIP 기반의 LI(Lawful Interception)의 필요성과 서비스 사업자 및 네트워크 사업자가 분리된 IMS의 특성에 따라 차별화된 LI수행 기법에 대해서 제안하였으며, Dynamic Triggering을 통한 기본적인 IMS/SIP 기반의 LI 수행 기법 및 아키텍처를 제시하였다.

또한, 전통적인 감청 표준들의 한계점을 보완하여 다양한 서비스를 제공하고 있는 IMS 환경에서의 연속적 감청 아키텍처를 제안하였다. 또한, 제안된 감청 아키텍처에서는 IMS의 세션 종료 메시지를 LEA에 전달하기 위한 이벤트 메시지를 구현하였다. 영장발부와 감청권한의 이동 CC와 IRI 감청, Triggering 명령어를 수행할 때 발생되는 지연 및 패킷손실을 최소화하기 위한 QoS 제어 기능이 필요함을 실험을 통해 증명하였다.

향후 연구로는 Fig.14.의 예와 같이 3G 무선망 단독이 아닌 IP 기반의 4G-LTE 등 다양한 종류의 무선망 및 사물통신(IoT) 환경을 연결하는 이 기종 연결에서의 IMS 감청 이슈, 세부적인 감청 Triggering 신호 제어에 관한 상세기술과 OPNET 시뮬레이터를 활용한 최적의 감청 아키텍처를 제안하고 그 효율성을 검증하고자 한다. 또한, 정교한 네트워크 시뮬레이션 환경 구성을 위하여 베이블 확률 분포를 적용하여 시뮬레이션을 적용할 계획이다.

References

[1] https://en.wikipedia.org/wiki/Lawful_interception

[2] M. Gorge "Lawful interception key concepts, actors, trends and best practice considerations," Elsevier Computer Fraud & Security, vol. 2007, no 9, pp. 10-14, Sep. 2007.

[3] Cable Television Laboratories, "PacketCable Electronic Surveillance Specification," PKT-SP-ES-DCI-101-060914, pp. 17-45, June 2006.

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

[5] ETSI, "Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic," TS 101 671 v3.12.1, Oct. 2013.

[6] ETSI, "Telecommunications Security; Lawful Interception (LI); Issues on IP interception," TR 101 944, May 2001.

[7] UK Home Office, "National Handover Interface Specification version 1.0," May 2002.

[8] http://www.calea.org/Online/AnnualReports/annualreports.htm

[9] Congress of the United States of America, "Communications Assistance for Law Enforcement Act of 1994 (CALEA)," Pub. L. No. 103-414, 108 Stat. 4279, Oct. 1994.

[10] ETSI, "Lawful Interception(LI); Dynamic Triggering of Content of Communication Interception," DTS 102 677 v0.2.2, Dec. 2009.

[11] ETSI, "Lawful Interception (LI); Handover and Service-Specific Details(SSD) for IP delivery," TS 102 232 v3.4.1, Oct. 2014.

[12] ETSI, "Lawful Interception requirements for GSM; Interception domain Architecture for IP networks," TR 528 v1.1.1, Oct. 2006.

[13] S.M. Faccin, P. Lalwaney and B. Patil, "IP multimedia services: analysis of mobile IP and SIP interactions in 3G networks," IEEE Communications Magazine, 42(1), pp.113-120, Jan. 2004.

[14] M. Lee, T. Lee, B. Yoon, H. Kim and H. P. In, "A Seamless Lawful Interception Architecture for Mobile Users in IEEE 802.16e Networks," Journal of Communications and Networks, vol.11, no.6, pp.626-633, Dec. 2009.

〈저자소개〉

이 명 락 (Myoung-rak Lee) 정회원
1994년 2월: 금오공과대학교 전자통신공학과 학사
2003년 2월: 국방대학교 전산정보학과 석사
2010년 8월: 고려학교 컴퓨터공학 박사
〈관심분야〉 정보보호, 디지털 포렌식, 합법적 감청 기술표준, 소프트웨어 보안

표 상 호 (Sang-ho Pyo) 정회원
1994 공군사관학교 컴퓨터과학과 학사
2002 국방대학교 전산정보학과 석사
2014 아주대학교 NCW학과 박사
〈관심분야〉 C4I, 전술데이터 링크, 상호 운용성

인 호 (Hoh Peter In) 정회원
1990 고려대학교 전산학과 학사
1992 고려대학교 전산학과 석사
1998 미국 University of Southern California(USC) 컴퓨터공학 박사
2003~현재 : 고려대학교 컴퓨터학과 교수
〈관심분야〉 요구공학, 자가적응 소프트웨어 공학, 임베디드 소프트웨어, 핀테크, IoT