Seamless Lawful Interception Handover for 3G IP Multimedia Subsystem (IMS)

Hoh Peter In[1], Myoungrak Lee[1,2], Dohoon Kim[1], Nunghoe Kim[1] and Byungsik Yoon[3]

[1] Department of Computer Science & Engineering, Korea University
Anam-Dong, Sungbuk-Gu, Seoul 136-713, Korea
[e-mail: {hoh_in, lmr2010, karmy01, nunghoi}@korea.ac.kr]
[2] The 83th I&C Maintenance Depot, Republic of Korea Air Force Logistics Command.
Mailbox 309-29, Sinjang-dong, Pyeongtaek-si, Gyeonggi-do, 459-799, Korea
[e-mail: lmr2010@korea.ac.kr]
[3] Wireless System Research Division, Electronics and Telecommunicating Research Institute (ETRI)
161 Gajeong-dong, Yuseong-gu, Daejeon, 305-350, Korea
[e-mail: bsyoon@etri.re.kr]
*Corresponding author: Hoh Peter In

Received February 16, 2011; revised April 14, 2011; revised May 30, 2011; accepted June 21, 2011; published July 28, 2011

Abstract

After the 9.11 terror attack, lawful Interception (LI) has emerged as an important tool for anti-terrorist activity. Law enforcement agents and administrative government bodies effectively monitor suspicious target users of permanent IP-based network devices by LI in Packet Data Networks (PDNs). However, it is difficult to perform LI in monitoring migrating users from a location to another, who change their IPs due to the proliferation of portable Internet devices enabling 3G IP Multimedia Subsystems (IMS). The existing, manual handover technique in 3G IMS makes it even more difficult to continue the LI activities due to time-lag reissuance of LI authority warrants when the target users move to a new LI jurisdiction via a roaming service. Our proposed model is a seamless LI handover mechanism in 3G IMS to support mobility detection of the target users. The LI warrants are transferred to the new LI agent automatically with the target users when they move to a new LI jurisdiction. Thus, time-lag human intervention of reissuance of the LI warrants is removed and enables the LI authorities to continue monitoring. In the simulation of our proposed mechanism, the quality of lawful interception achieves a mean score of over 97.5% out of the possible 100% maximum score, whereas the quality of the existing mechanism has a mean score of 22.725%.

Keywords: lawful interception, seamless handover, IP multimedia subsystem, 3G networks, dynamic triggering

This work was supported by the IT R&D program of MKE/KEIT. [KI001868, Development of WiBro Network Reliability and Location Awareness Technologies].

DOI: 10.3837/tiis.2011.07.007

1. Introduction

Lawful Interception (LI) has emerged as a tool for anti-terrorist activity after the 9.11 attack. LI is the legal interception of telecommunication conducted by law enforcement agents and administrative government bodies, local or federal, to monitor suspicious target users (e.g. terror suspects and specific criminals); thus, auditing the targets. The execution of a LI is allowed only when a competent authority authorizes such an activity [1]. Regardless of proper legal authority, it is impossible to intercept a specific telecommunication without cooperation from a network operator, a service provider, and an access provider. Under conventional networks, including wired and 3G cellular networks, a lawfully authorized body grants an LI authority in the form of a lawful order [2].

The European Telecommunications Standard Institute (ETSI) set forth most of the existing standards in Europe, while the Communication Assistance for Law Enforcement (CALEA) is making progress in the U.S.A. CALEA defines the responsibilities of Communications Service Providers (CSPs) to facilitate lawful electronic surveillance. The existing international LI standards focus on how to design the handover interface of the LI-related information [1][3]. These LI architecture standards have been used in wired and wireless network settings [4]. The IP Multimedia Subsystem (IMS) is an architectural framework to deliver Internet Protocol (IP) multimedia services. 3G is a generation of standards for mobile phones and mobile telecommunications services fulfilling specifications of the International Telecommunication Union (ITU).

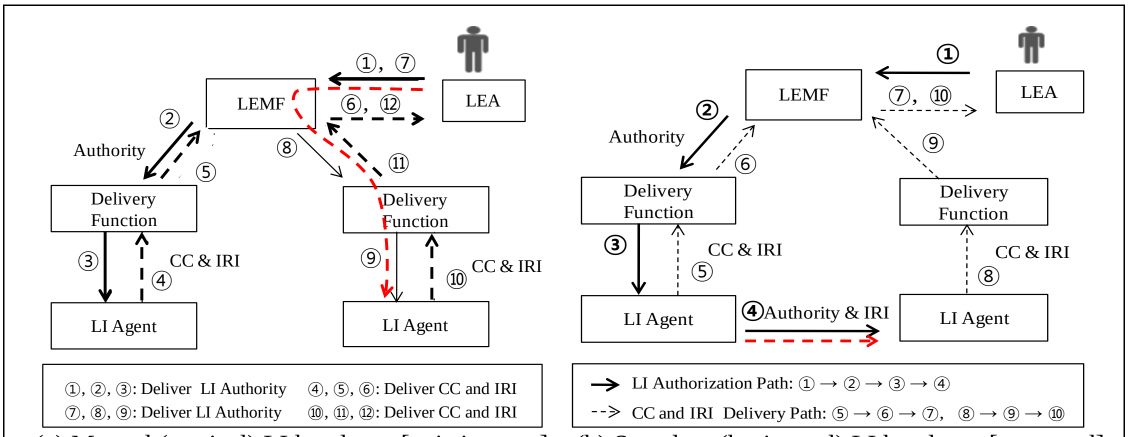
It is quite a challenge to perform LI under 3G networks-based IMS (3G IMS) that focuses on mobility-supported environments with merging cellular networks and the Internet. Unlike the LI in independent wired networks or cellular networks, the target users move from one location to another with session and IP mobility, while they are using the proliferate portable Internet devices enabling 3G IP Multimedia Subsystem (IMS). Especially, it is more challenging to perform LI when the target users move to a new LI jurisdiction via a roaming service. In the existing LI handover mechanism in 3G IMS, an LI authority warrant needs to be reissued manually via manual handover between the law enforcement agency and the LI agent concerned. This results in delayed and discontinued LI due to this manual human intervention for handover.

In 3G IMS, our proposed mechanism supports the detection of the mobile LI user who moves to another network area. The LI warrants are transferred to a new LI jurisdiction automatically. The main feature of our approach enables the LI authorities continuously to handover to the new LI agent without human intervention reissuing the LI warrants. The detailed mechanism is explained in **Fig. 1**.

In the existing, manual LI handover mechanism, the LI authority (LEA) should re-issue the LI authorization warrant manually when a targeted user moves to other 3G IMS environments of a new LI jurisdiction via a roaming service. In Fig. 1(a), for example, LEA issues the warrant of LI authorization to the LI agent (i.e., ①→②→③) and the LEA re-issues the LI authority warrant to the new LI agent when the targeted user moves to another LI jurisdiction (i.e., ⑦→⑧→⑨).

However, our proposed ***seamless*** handover transfers the LI authorization warrant ***with*** the mobile target user from the old LI agent to the new LI agent when the user moves to another LI jurisdiction (①→②→③→④ in **Fig. 1 (b)**). Thus, we removed the time-lag of the manual LI authorization process (i.e.,⑦→⑧→⑨ in **Fig. 1 (a)**). In addition, the proposed LI mechanism enables continuance of LI activities without stopping. Accordingly, our proposed mechanism has the following advantages:

- Transferring the LI authority automatically guarantees the LI quality (i.e., QoS) of the target user. That is, LI of the target user is operated continuously without time delay, since there is no human intervention.
- Our mechanism supports seamless LI handover without reference to the number of the LI target user
- Horizontal (seamless) handover of the LI authority enables removal of unnecessary processes of vertical LI authority and unnecessary maintenance work under the management of LEA. This improves the LI productivity of LEA.



(a) Manual (vertical) LI handover [existing one] (b) Seamless (horizontal) LI handover [proposed]

Fig. 1. Comparison of (a) **existing LI handover** and (b) **seamless LI handover**

The remainder of this paper is organized as follows. Section 2 describes the background and related work for LI handover. Section 3 explains the proposed seamless LI mechanism in 3G IMS. Section 4 presents the simulation results using Qualnet to compare the LI performance of the proposed mechanism. Section 5 concludes this paper.

2. Background and Related Work

2.1 Existing LI Architectures for Wireless Networks

ETSI and CALEA standards deem that LI domains fall into two categories: wired and wireless networks. A generic architecture is proposed to intercept wired and wireless networks via access to the Public Switched Telephone Network (PSTN) [6][7][8][18]. Other suggestions for LI architectures for VoIP are capable of capturing IP-based voice communications [9][10][14]. Two models are proposed in [10][11]: the Session Initiation Protocol (SIP)-based model, and the distribution system for LI on IP telephony networks, respectively. These architectures, however, mainly address permanent IP-based networks. In [12], a new LI architecture is proposed for 3G wireless networks. This new model enables a law enforcement agency to activate an LI by placing a request to a Mobile Switching Center (MSC).

A typical reference model of handover interface for LI authorization (HI1) in the General Packet Radio Service (GPRS) environment supporting GSM circuit switching and packet switching was reported in [13][14][15][16][17]. The reference model is divided into the LEA domain and the Communication Service Provider (CSP) domain. The CSP domain consists of the interface and the Internal Interception Function (IIF). Interception is executed in the Serving GPRS support Node (SGSN) or Gateway GPRS Support Node (GGSN). These nodes communicate with the Delivery Function (DF) via the X-interface (X1, X2 and X3) to activate, deactivate, interrogate and invoke the LI.

The interception authorization procedure has limited capacity to satisfy seamless LI due to the changing communication environment. This causes time delays of LI authorization triggering between the LEA and CSP domains. The LI agents are used by law enforcement agencies to intercept, monitor and collect the user data packets, and intercept and transport the collected data to LEMF via the Delivery Function (DF) embedded in CSP equipment.

2.2 Limitation of Handover in the Existing LI Architectures

It is impossible to enforce a warrant in the traditional LI scenarios, since the CSPs reside in different jurisdictions than the issuing jurisdiction. Technically, it is also impossible to inform the globally distributed CSPs of the Lawful Interception Identifier (LI ID) unique to the target specified by the warrant. Most of the existing international LI standards focus on the architectures for the handover interface of the LI-related information [1][18][19]. The ESTI technical report [20] states the following three handover interfaces are most commonly used to enforce an LI:

- Handover Interface one (HI 1): is used for communication between the CSP and the law enforcement agency (i.e., Law Enforcement Monitoring Facility or LEMF) with the LI authority embedded in the LI agent using the Lawful Interception Identifier (LI ID).
- Handover Interface two (HI 2): is related to the Intercept Related Information (IRI), which the CSP in turn sends to the LEMF as additional information on the intercept. The IRI represents the collection of data on the target identity, collected from telecommunication services.
- Handover Interface three (HI 3): is used for the Content of Communication (CC) to be handed over from a CSP to LEMF. Here, CC refers to the information exchanged between two or more users of telecommunication services.

HI 1 is the one most closely related of the aforementioned three interfaces to the issuance of an interception warrant. When a law enforcement agency places a lawful interception request with a CSP, the CSP in turn requests information from the LEA [21]. However, conventional LI standards, such as [21], have limited capacity to guarantee seamless interception of a moving target via LEA. Conventional LI handover would have to issue a bundle of warrants via LI authority delegation to secure seamless lawful interception to cover all possible user destinations. This task would be excruciatingly expensive.

2.3 Needs and Assumptions for Seamless LI Handover in 3G IMS

Fig. 2 illustrates the conceptual structures of the horizontal handover in the 3G IMS. It is easy for a target user to migrate out of the jurisdiction of the current the LI agent via a roaming service on 3G IMS networks. Such changes of location pose a set of difficult problems to law enforcement and LI agencies [5]. Particularly in the context of the 3G IMS networks, lawful interception is faced with the following challenges:

- IMS service provider and network access provider may belong to different CSPs.
- Security measures and encryption make it hard to conduct lawful interception.
- IP mobility may cause the session to extend over multiple CSP networks.
- When a user changes his/her IP addresses frequently, it becomes difficult to keep track

of the original identity.

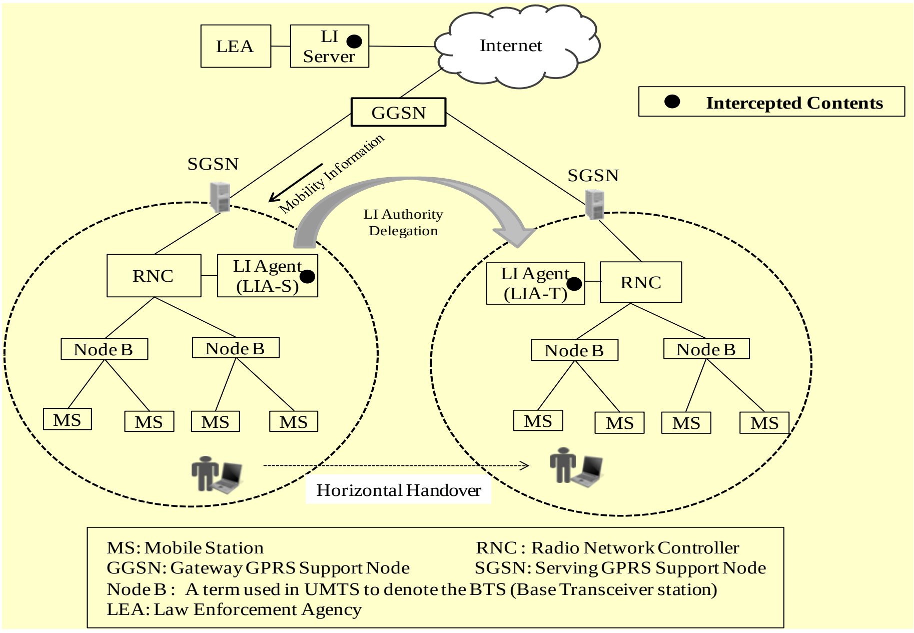


Fig. 2. Overview of LI handover in 3G

Despite the diverse proposals for IMS mobility in 3G IMS networks, the following LI problems commonly occur in the course of lawful interception:

- Signaling and multimedia traffic has different network paths.
- Network provider and IMS service provider is different.
- A target node's network provider is different due to SIP mobility.
- It is necessary to deliver HI 1 information, such as information on a warrant to the LI agent in advance, to secure seamless LI; however, it is difficult to inform all LI agents of the HI 1-related information prior to the target user movement.
- The LI agents identify all users and have the authority to enforce an LI so its realization does not require additional IRI; however, the traffic is increased between the LI agent and an access service network, such as the Authentication Authorization and Accounting (AAA) server and Home Agent (HA).

A new seamless lawful interception mechanism is needed to resolve the above problems. The following systems and communication conditions are assumed in this paper to secure seamless LI mechanism in 3G IMS:

- The CSP has to remain unchanged to avoid inconsistencies in the course of authentication, authorization and accounting during terminal mobility for the network handover.
- An LI is assumed to be enforced within a single national jurisdiction. Moreover, this paper assumes that seamless LI is executed within a country or between different countries with identical LI regulations.
- The Mobile Station (MS) and corresponding node should be able to communicate with each other, even under different CSPs.
- A roaming agreement is needed to trigger seamless LI between different states and/or countries.

- The LI agent of different CSPs should trace the identifier of the moving mobile node, even though the identifier is changed.

3. A Seamless Lawful Interception Handover Mechanism for 3G IMS

3.1 Overview of Seamless Lawful Interception handover in 3G IMS

Fig. 3 shows the proposed seamless LI mechanism for the IMS of 3G networks. In the architecture, the LI agents are located in a Radio Network Controller (RNC), and transmit intercepted Content of Communication (CC) and Intercept Related Information (IRIs) to the LI server. The LI agents have the basic components of the proposed seamless LI triggering mechanism and the specific functions of the LI agents and the server. The LI agents comprise *authority delegator*, *mobility detection function*, *interception function* and *delivery function*, basic components to guarantee seamless LI in IMS. The LI server consists of a collection function and an LI coordinator. These basic components of the LI agent and the LI server are derived from our previous work [5].

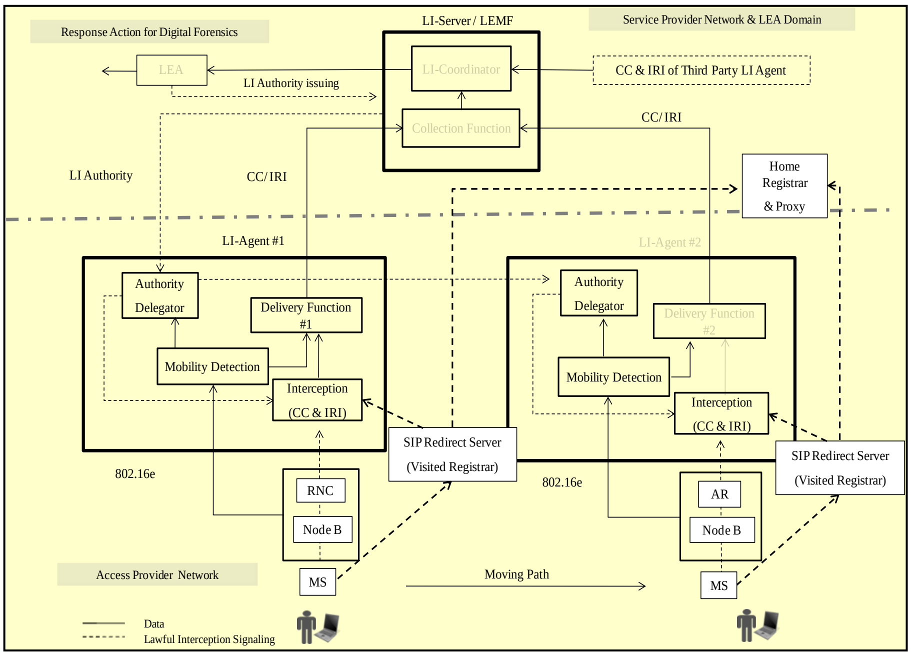


Fig. 3. Overview of proposed LI mechanism in 3G IMS

The authority delegator is the core to a dynamically moving LI target of 3G networks. The delegator gives a warrant for LI from the LEA to the first serving LI agent. Then, it delegates LI authority to the target LI agent. The mobility detection function detects the target user’s movement and notifies the movement information to the LI authority located in the same area. The authority delegator delegates LI authority to the target authority delegator, to whom the located target will be transferred, after receiving the movement information.

Next, the authority delegator, which acts as the interface with the mobility detection function on 3G networks, is discussed in detail.

3.2 LI Authority Delegations in IMS

Mobility of 3G wireless networks is divided into terminal mobility and session mobility. Terminal mobility allows terminal equipment to move between IP subnets, and session mobility maintains an ongoing media session between different types of terminal equipment. When the LEA issues an order to intercept the contents of a suspicious mobile user, the LI authority is delegated to the LI agent. The authority information consists of a Lawful Interception Identifier (LI ID), Communication Identifier (CID), and Network Identifier (NID). These identifiers are vital to uniquely identify the interception target and to correlate data transferred over different interfaces. When an illegal user moves from a PAR to a NAR, the previous Authority Delegator (AD) transmits the authority information to the AD in the new LI agent.

The ADs receive the migration information from the mobility detection component, which in turn functions as an interface to UMTS mobility management and IMS session mobility. The Home Subscriber Server (HSS) of the home network is a central repository of subscription related information, authentications and user authorizations. The Subscriber Location Function (SLF) provides information of HSS related to a particular user. I-CSCF and S-CSCF communicate with SLF to find an appropriate HSS based on the user profile in the case of more than one HSS. P-CSCF is the first point of contact for the IMS terminal.

GGSN and P-CSCF share the same network in IMS. We expect IMS deployments will locate P-CSCF in the home network [23]. Agents can reduce the expected turnaround time delays in issuing warrants for LI by avoiding reliance on the vertically exchanged LI authority and LI triggering signals between the LEA and LI. Additionally, the delay time is not a performance measure in evaluating LI architectures. It functions as an input parameter in the course of simulating the existing LI architectures, since the vertical handshaking protocol (used in the existing LI architecture) between a LEMF and the LI agents involves a human in the loop and the human agents take time to review and issue the LI authority (e.g., warrants). However, our architecture proposes an automatic LI architecture to support seamless LI service. That is, the delay time (i.e. time needed to issue warrants) is theoretically the same as the packet transfer time. In addition, we have adopted the concept of recall rate from information retrieval (IR) to measure effectiveness of LI service. We define recall rate “R” as the number of intercepted packets of all the packets transmitted from the target user; namely, a good LI service is capable of intercepting all the transmitted packets (100% recall rate), while a poor LI one is not able to catch any of those transmitted (0% recall rate).

Technically, The LI agents no longer need to send an uplink request to gain authority from the LEA. Instead, they find the next target agent autonomously, and enable the target agent to cooperate with the LEA to intercept and push the CCs obtained during monitoring. The triggered agent directly delivers IRI with an LI authority signal. Mobility detection enables these proposed process steps. Mobility detection is essential functionality for seamless lawful interception, because it helps a current the LI agent identify and nominate the target LI agent of candidate networks. The detailed steps of the conceptual lawful interception process, rather than using automatic cooperation between the LI agents in 3G networks, are described in subsection 3.3 and 3.4.

3.3 LI Triggering via Terminal Mobility Detection

Mobility Management (MM) functionality supports user mobility via CS and PS domains. In 3GPP release 5, the Home Subscriber Server (HSS) includes the Home Location Register (HLR) and Authentication Centre (Auc) as subsets. IMS consists of two main planes, signaling plane and media plane. These two planes traverse different paths. The major component in the signaling plane is the session control protocol. We adopt the IP mobility of

3G UMTS [23] for terminal mobility of 3G wireless networks.

The mobility detection component receives handover information from the mobile IP Home Agent (HA). A mobile node registers a Care of Address (CoA) from a new access router with the HA when it moves. Whenever a mobile node moves in the 3G wireless network environment, HA updates the binding information between the mobile's Home Address (HoA) and the CoA. The update information on the binding cache is transmitted to the LI agents via the base station. The serving LI agent collects the CCs and IRIs, and reports them to the LI server. The LI agents use the binding cache update information of 3G wireless networks for mobility detection. The LI agent detects the movement signature of the MS via HoA and CoA. Then, the LI server rearranges the intercepted CCs and IRIs in accordance with the original source IP (e.g., HoA). If MS receives a mobile neighbor advertisement message from the serving base station, the mobility detection function informs the delivery function and the authority delegator of the MS's new CoA. Session Initiation Protocol (SIP) is the session control protocol in IMS services [23]. A mobility management protocol is operated at the control plane, independent of the media plane, in UTRAN of 3G wireless networks. UTRAN supports a physical handover via a horizontal handover between different RNCs or Node Bs, when a target user agent moves from one visited network to another [24]. SIP supports the session mobility of the target user in the basic architecture and procedure of IMS. P-CSCF is the first contact point in the signaling plane between the IMS terminal and the IMS network, and the I-CSCF is a SIP proxy located at the edge of an administrative domain.

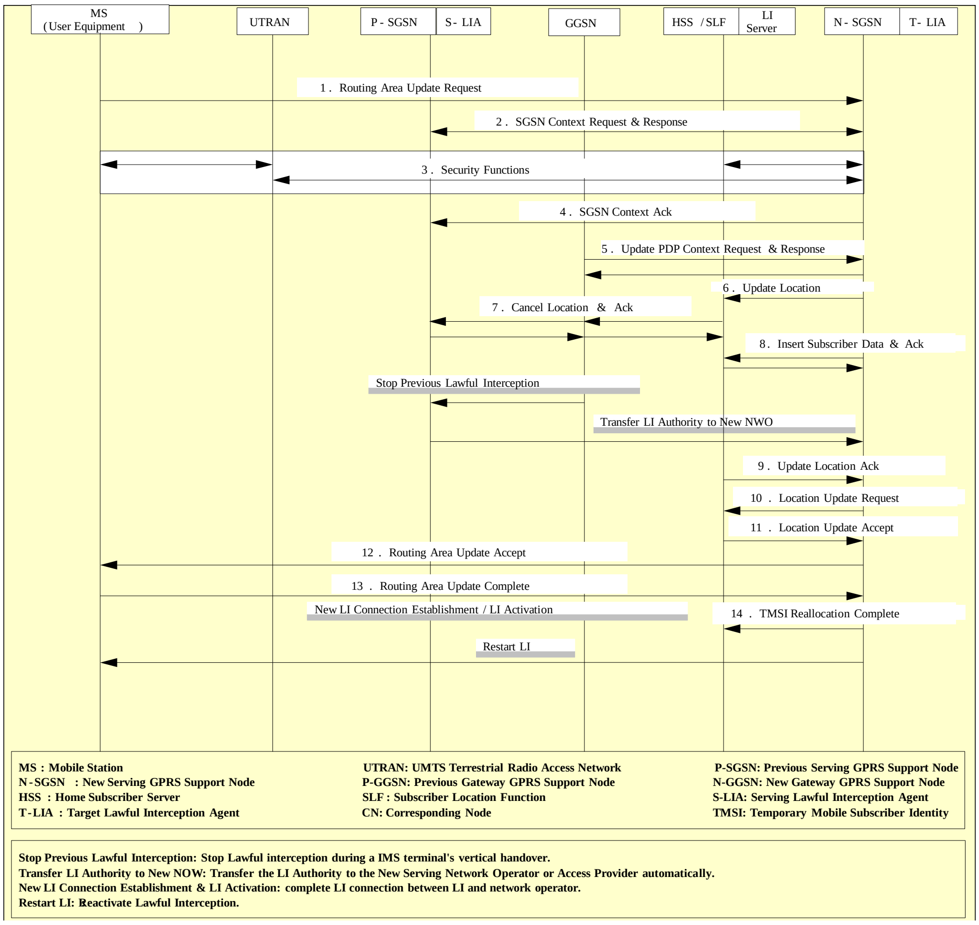
Fig. 4 shows the call flows within UTRAN to update the location of a user agent. The periodic Routing Area update allows the network to detect if a user agent is still attached to it [25]. The detailed procedure of seamless LI triggering via mobility detection in UTRAN in 3G is as follows:

- MS sends the *Routing Area Update Request* message to the N-SGSN. This *Routing Area (RA) Update* is a function to detect if an MS is attached to the network.
- The N-SGSN sends the *SGSN Context Request message* to the P-SGSN to obtain the Mobility Management (MM) and Packet Data Protocol (PDP) contexts, and the P-SGSN sends the response message to the N-SGSN.
- The N-SGSN sends the *SGSN Context Acknowledge* message to the P-SGSN to disable the SGSN-HSS association in the old MM context.
- The new SGSN sends the *Update PDP Context Request* message to the N-GGSN, and the N-GGSN replies with the *Update PDP Context Response* message after modifying it.
- The *Update Location* message of the N-SGSN informs the HSS that the SGSN for MS has changed.
- The HSS sends subscriber data to the N-SGSN, after exchanging the *Cancel Location message* between the P-SGSN and HSS.
- The Serving Lawful Interception Agent (S-LIA) deactivates the interception of CC and IRI, when the P-SGSN receives a *Cancel Location* message from the HSS.
- The N-SGSN sends the *Location Update Request* message to the HSS, and the HSS responds with the *Location Update Accept* message.
- The S-LIA transfers the LI authority to the Target Lawful Interception Agent (T-LIA) in other 3G networks, after exchanging a *Cancel Location* & *Ack* between the P-SGSN and HSS.
- The S-LIA also receives the *Cancel Location* and *Insert Subscriber data* messages. T-LIA monitors if MS is reconnected via the *Update Location Request & Accept* message.
- MS sends the *Routing Area Update Complete* message to the new-SGSN, when the

new-SGSN sends the *Routing Area Update Accept* message to the N-SGSN.

- A new LI connection is established and the LI process begins, when the *Routing Area Update Accept* and *Routing Area Update Complete* messages are exchanged.

If a new *Temporary Mobile Subscriber Identity (TMSI) Reallocation Complete* message is sent via MS, then the N-SGSN sends it to the HSS.


MS
(User Equipment)
UTRAN
P-SGSN
S-LIA
GGSN
HSS /SLF
LI Server
N-SGSN
T-LIA
1. Routing Area Update Request
2. SGSN Context Request & Response
3. Security Functions
4. SGSN Context Ack
5. Update PDP Context Request & Response
6. Update Location
7. Cancel Location & Ack
8. Insert Subscriber Data & Ack
Stop Previous Lawful Interception
Transfer LI Authority to New NWO
9. Update Location Ack
10. Location Update Request
11. Location Update Accept
12. Routing Area Update Accept
13. Routing Area Update Complete
New LI Connection Establishment / LI Activation
14. TMSI Reallocation Complete
Restart LI

MS : Mobile Station
N-SGSN : New Serving GPRS Support Node
HSS : Home Subscriber Server
T-LIA : Target Lawful Interception Agent
UTRAN: UMTS Terrestrial Radio Access Network
P-GGSN: Previous Gateway GPRS Support Node
SLF : Subscriber Location Function
CN: Corresponding Node
P-SGSN: Previous Serving GPRS Support Node
N-GGSN: New Gateway GPRS Support Node
S-LIA: Serving Lawful Interception Agent
TMSI: Temporary Mobile Subscriber Identity

Stop Previous Lawful Interception: Stop Lawful interception during a IMS terminal's vertical handover.
Transfer LI Authority to New NOW: Transfer the LI Authority to the New Serving Network Operator or Access Provider automatically.
New LI Connection Establishment & LI Activation: complete LI connection between LI and network operator.
Restart LI: Reactivate Lawful Interception.

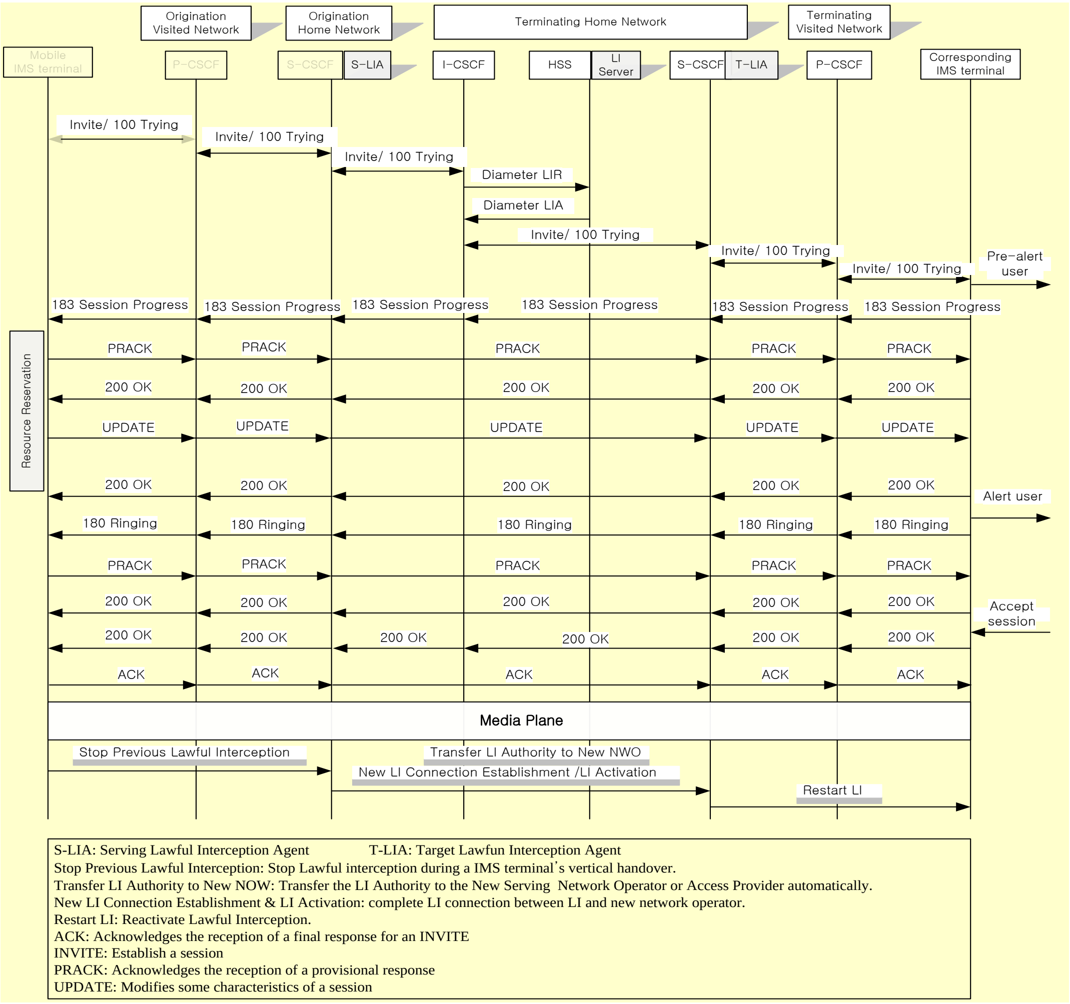
Fig. 4. Mobility detection and LI procedure in UTRAN

3.4 LI Triggering via Session Mobility Detection

Fig. 5 shows the detailed session setup process in the 3G IMS. We adopt the session setup process of [22]. This assumes that users are roaming to a network outside their home networks. Then, we determine when LI authority is delegated from the serving LI agent to the target LI agent. Two terminal users have different home networks, as they have different CSPs. We assume the initial visited network and initial home network are under different jurisdictions.

The address of the I-CSCF is listed in the DNS (Domain Name System) records of the domain. Therefore, the I-CSCF has an interface to the Subscriber Location Function (SLF) and the HSS. The S-CSCF acts as a SIP registrar that maintains binding information (e.g., the IP address of the terminal) [23].

Fig. 6 depicts the call flows of LI authority delegation on 3G networks. In **Fig. 6**, the previous LI agent remains capable of receiving both the same message from the HSS and the information of the next Node B of a nearby access router.



S-LIA: Serving Lawful Interception Agent T-LIA: Target Lawfun Interception Agent
Stop Previous Lawful Interception: Stop Lawful interception during a IMS terminal`s vertical handover.
Transfer LI Authority to New NOW: Transfer the LI Authority to the New Serving Network Operator or Access Provider automatically.
New LI Connection Establishment & LI Activation: complete LI connection between LI and new network operator.
Restart LI: Reactivate Lawful Interception.
ACK: Acknowledges the reception of a final response for an INVITE
INVITE: Establish a session
PRACK: Acknowledges the reception of a provisional response
UPDATE: Modifies some characteristics of a session

Fig. 5. Signaling of session control in IMS

Assuming the MS moves from the currently serving network to the next network, the serving LI agent obtains MS's movement information from the update message via the P-CSCF of visited network 1. The serving LI agent sends the LI authority delegation message to the target LI agent located on visited network 2. A moving IMS terminal obtains the IP address of theP-CSCF via P-CSCF discovery. The seamless LI authority handover from the serving LI agent to the target LI agent enables LEA to perform continuous reporting from the LI agents to the LI server. The LI agent executes the interception of the designated suspicious mobile users by LEA.

When a target mobile station accesses Node B and then RNC, the LI agent receives packets from the mobile station via the connected access provider, as authorized by a LEA warrant. The LI agents extract the CCs and IRIs from captured packets, and transmit them to the LI server via the delivery function.

The LI server is located on an access service network, and is responsible for monitoring the distributed LI agents and gathering all the CCs and IRIs of the target user. The LI agents are embedded with the authority delegator and the delivery function to receive the mobility related information of the MS via the mobility detection function. Then, the authority delegator in the first visited network delegates the LI authority to the next target LI agent in the next visited network.

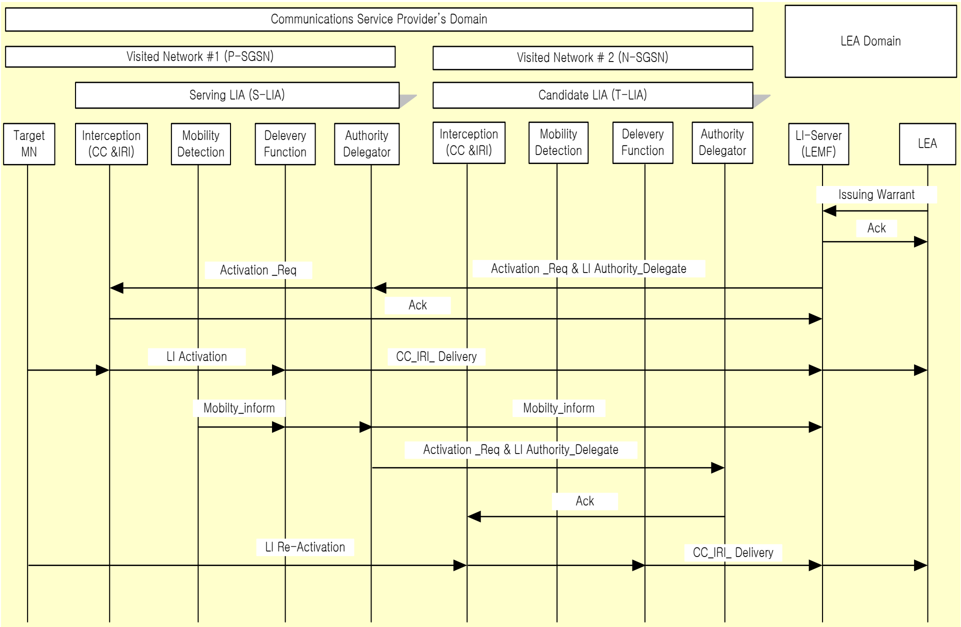


Fig. 6. Activation of seamless LI triggering for 3G networks with IMS

3.5 LI Coordination

An LI coordinator is intended to gather the CCs and IRIs in accordance with the related LI information. The LI coordinator is embedded in the LI server, and manages the connected operations between the LIs involved in SIP-based IMS mobility. The LI coordinator gathers the components of the CCs and IRIs that have been originally distributed to the LI agents to conduct seamless surveillance on target mobile units. Even if the LI server receives incomplete information from the agents, the LI coordinator is still capable of generating the complete IRI, including the target MS's identifier (e.g., the user's IP address). In this case, the MS's identifier is obtained from the IMS terminal, the IPv4 or IPv6 address of its P-CSCF [23]. The LI coordinator automatically orders the intercepted CCs, whenever a target user moves. Extraction of the IRI information is performed using the original IP address. It uses the IP addresses of the HSS's binding cache table to obtain IRI. Finally, the LI coordinator completes the target MS's traces.

4. Simulation Results

4.1 Simulation Configuration

The proposed seamless LI architecture has been implemented in a simulation configuration via Qualnet 4.5.1, Wireshark 1.2.0, and Skype (VoIP supported) to produce a simulated 3G-based IMS environment. We configured the horizontal handover environment of two 3G networks. One MS is designed to change the connectivity between two different 3G networks during migration in the simulation. The moving MS node and corresponding node were emulated in the simulator via the IP Network Emulator (IPNE) to configure a communication and handover between two different IMS services located in two different 3G networks. One moving MS communicates with the corresponding IMS terminal. Four Wireshark 1.2.0

networks were re-morphed into two LI agents and the LI server to produce and integrate the IRI.

When a target MS accesses a new SGSN, the authority delegator issues an interception command to the target LI agent. The mobility detection informs the authority delegator and the delivery function of the migration information on a mobile target. The LI coordinator classifies the collected CC and IRI on each target user.

We adopted the exponential distribution with an average *Minute of a User (MOU) per session* on a cellular phone and IP-based data communications to configure a large scalability of target users for interception. Here, an exponential distribution denotes a continuous random distribution with a continuous analog of a geometric distribution. The simulation reproduced four types of MOU [26].

First, voice communication had a connection time of about 10 minutes per session, a figure based on a survey of iPhone (i.e., an internet-connected multimedia smart phone) users' average per session [27]. The second data type was video-conference data; it had 25 minutes of average MOU. The third data type was 40 minutes of MOU [28] that can use the same type of video-conference data. The last type was 60 minutes of MOU. All four data types are distributed exponentially in the respective simulation.

The maximum length of use was set at 60 minutes for all data types. The probability density was 1. We gradually increased the number of target users from 1 to 10. The reproduced total traffic volume was 3.686 Megabyte constant bit rate (CBR) data, as the external traffic that had a 512 Byte packet size per 0.5 second interval. Both the conventional LI architecture and our proposed seamless architecture have two LI agents and one LI server. The LI agents are located in SGSN of 3G wireless networks, and are connected to the LI server.

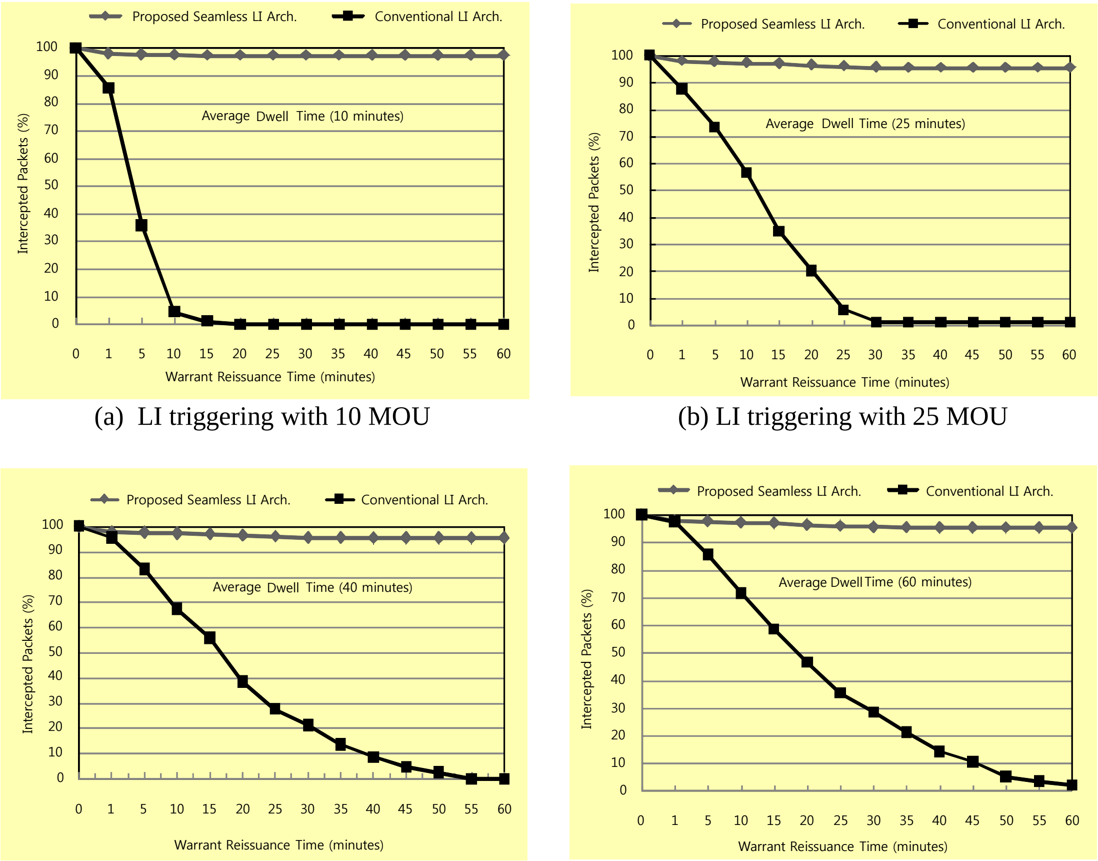
The target users are moved randomly from the old SGSN to new SGSN under 3G networks. The simulation lasted one hour. Traffic was intercepted from the operational nodes by the three different LI agents and one LI server. The specific scenarios are:

- The LI coordinator installed in the LI server extracts the complete CC and IRI by sequencing the partial information transmitted from the LI agents.
- Issuance of a warrant is affected by human intervention. ETSI standards provide that a minimum manual translation is required to deliver the warrant via the HI 1 [15]. Herein, it is assumed to take between 1 to 60 minutes for a law enforcement agency to issue a subsequent warrant.
- The time consumed for the first vertical handover from the old SGSN to new SGSN was set to last 50 seconds.

4.2 Experimental Results

Our proposed seamless lawful interception mechanism was evaluated from the viewpoint of mobility detection and LI authority delegation in 3G-based IMS service environments. **Fig. 7** compares the results of the four types' average MOU. These describe successful tracking of target mobile users and seamless lawful interception via the proposed mechanism.

Four types of communications were simulated in this paper; the volumes of the intercepted CCs and IRIs of the four types were compared. The proposed mechanism caused few packet losses at the LI agent and the server, and performed interception without much loss, and received partial information from the LI agents 1 and 2. The longer it takes to re-issue a warrant, the fewer packets are intercepted for the case of the conventional architecture. However, our proposed seamless mechanism achieves constantly high performance in terms of the total number of intercepted packets.



(a) LI triggering with 10 MOU

(b) LI triggering with 25 MOU

(c) LI triggering with 40 MOU

(d) LI triggering with 60 MOU

Fig. 7. Comparative Results of LI triggering with different Minutes Average Dwell Time

Even if the number of MOU increased, there was no performance variation due to automatic handover in the present study. Once the warrant issuance was enforced in the session initialize phase, no process for warrant reissuance is required, even if the suspicious target user is moving.

Conversely, a problem that may possibly arise, such as overhead, is only caused by human intervention in the existing LI architecture. The LI coordination policy is manually executed by a human, when the IP address of the suspicious target user is changed every time to re-issue a warrant. Thus, the overhead problem influences the interception QoS. The mechanism is not handled with network performance problems, such as packet delay, packet loss, and other QoS options, because our focus is to handover the LI warrant to other LI agencies seamlessly in terms of LI management.

Table 1 compares the handover performance of the conventional LI architecture to that of our mechanism proposed in this paper.

Each Probability Density Distribution (i.e.: area of graph in **Fig. 7**) is represented by Simpson’s Rules [29] to calculate the performance difference between our proposed seamless LI architecture and conventional LI architecture, as follows:

$$p(x) = \int_{x_a}^{x_c} f(x)dx \cong \frac{\Delta x}{3}[f(x_a) + 4f(x_b)f(x_c)] \quad (1)$$

$$\begin{aligned} \textit{where}\quad & p(x): \textit{The performance of graph} \\ & x_a, x_b, x_c : \textit{interval order of } x-\textit{axis} \\ & a, c : \textit{the end point},\quad b : \textit{the midpoint of the } a \textit{ and } b. \end{aligned}$$

The experiments revealed, the quality of lawful interception in our proposed mechanism achieves a mean score of over 97.5%, out of a possible maximum score of 100%, whereas the quality of the existing mechanism is a mean score of 22.7%, irrespective of the number of MOU.

Table 1. Performance analysis: Probability Density Distribution of Intercepted Packets

	10 MOU	25 MOU	40 MOU	60 MOU
Conventional LI handover Arch (Human intervention)	3.2%	18.2%	31.8%	37.7%
Proposed LI handover Arch (Automation intervention)	96.8%	97.4%	98.1%	97.9%

5. Conclusions

Lawful Interception is a powerful tool in criminal and security investigation, especially in 3G IMS environment. It is used to gather evidence for court cases, and to identify networks of relationships between suspected criminals. It is important to continue LI, without ceasing LI activity, when the target user moves to a new jurisdiction.

Our main contribution is to propose the seamless LI handover mechanism in 3G-based IMS. Namely, our proposed scheme utilizes horizontal cooperation between each LI agency in the new LI jurisdiction. The authority and IRI are directly handed over to the LI agent in charge of the user's new location, without additional LEA authorization. Thus, LI activities are continued without cessation. In addition, the simulation results showed the efficiency of our proposed seamless LI handover mechanism is better than that of the conventional LI handover mechanism. We did not consider all LI architecture security issues, such as LI authorization, authentication, confidentiality, integrity, and availability, since our focus is on the seamless LI handover mechanism. The current proposed mechanism is not incontrovertible for illegitimate interception, spam, and identity spoofing. The security community seeks a solution using Lawful Interception Identifier (LI ID) that is protected using various security mechanisms presented in the ETSI standard documents. We will investigate the LI security issues in future work. We will also work on topics, such as how to intercept IMS-based traffic, on heterogeneous wireless networks and how to delegate LI authority on them. Our attention is also being given to topics, such as identifier detection and the delegation of seamless LI authorization to P2P networks supporting VoIP services. Moreover, our simulation is based on S/W simulation that is a Qualnet simulator. Of course, it is possible to adopt various scenarios. However, this simulator has several limitations, such as the number of nodes due to being a JAVA-based simulator. Accordingly, we will have a specific plan for simulation to create diverse scenarios.

Acknowledgement

This study was jointly funded by Korea University Funding, the IT R&D program of MIKE (2008-S-001-02, Development of WiBro network reliability and location awareness technologies).

References

[1] ETSI TS 101.671: Lawful Interception (LI); Handover Interface for the Lawful Interception of Telecommunications Traffic, 2009.

[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. Article (CrossRef Link).

[3] S. Gleave, “The Mechanics of Lawful Interception,” *Network Security*, vol. 2007, no. 5, pp 8-11, 2007. Article (CrossRef Link).

[4] ETSI ES 201 158: Telecommunications Security; Lawful Interception (LI); Requirements for Network Functions, 2002.

[5] 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, 2009.

[6] RFC2804 “IETF Policy on Wiretapping”, 2000.

[7] 3GPP TS 33.106: Technical Specification Group Servicesand System Aspects; 3G Security; Lawful Interception Requirements (Release 5), 2002.

[8] National Handover Interface Specification version 1.0, Home Office, 2002,

[9] A. Milannovic, and Ivan Matosevic, “Distributed System for Lawful Interception in VoIP Networks,” in *Proc. of EUROCON*, 2003. Article (CrossRef Link).

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

[11] ETSI TR 101.514: Digital cellular telecommunications System (Phase 2+) Lawful Interception Requirement for GSM, 2001.

[12] ETSI ES 201 158: Telecommunications security; Lawful Interception (LI); Requirements for Network Functions, 2002.

[13] ETSI TS 101 331: Technical Specification Lawful Interception (LI); Requirements of Law Enforcement Agencies, 2006.

[14] ETSI, ES 201 671: Telecommunications Security; Lawful Interception (LI); Handover Interface for the Lawful Interception of Telecommunications Traffic, 2007.

[15] ETSI, TR 101 944: Telecommunications Security; Lawful Interception (LI); Issues on IP Interception, 2001.

[16] Juniper Networks FMC Security Solution.

[17] ETSI, TS 102 232-1: Lawful Interception (LI); Handover specification for IP delivery, 2008.

[18] National Handover Interface Specification version 1.0, Home Office, 2002.

[19] ETSI TR 102 053 v1.1.1 Telecommunications security; Lawful Interception (LI); Notes on ISDN Lawful Interception Functionality, 2002.

[20] ETSI TS 141 033: Digital Cellular Telecommunications System (Phase 2+); Lawful Interception Requirement for GSM (3GPP TR 41.033 version 8.0.0 Release8), 2009.

[21] S. M. Faccin, P. Lalwaney, B. Patil “IP Multimedia Services: Analysis of Mobile IP and SIP Interactions in 3G Networks,” *IEEE Communications Magazine*, Jan. 2004. Article (CrossRef Link).

[22] G. Camarillo, M. A Garcia-Martin, “The 3G IP Multimedia Subsystem (IMS), Merging the Internet and the Cellular Worlds,” 2nd Edition, John Wiley & Sons, Ltd, 2006.

[23] R. Kalden, E. E. D. GmbH “Mobility Management in UMTS,” Seminar: Datacommunication & Distributed Systems, 2003.

[24] Y.-B. Lin, Y.-R. Haung, Y.-K. Chen, I. Chlamtac, “Mobility Management: From GPRS to UMTS,” *Wireless Communications and Mobile Computing*, vol. 1, no. 4, pp. 339-360, 2001. Article (CrossRef Link).

[25] R. D. Yates, D. J. Goodman, “Probability and Stochastic Processes,” 2nd edition, John Willy and Sons, INC, 2005.

[26] http://as.wiley.com/WileyCDA/WileyTitle/productCd-EHEP000391.html

[27] http://www.mobilitmarketer.com/cms/news/advertising/3166.html.

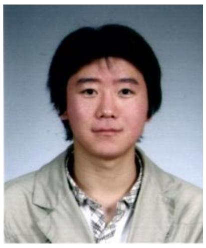
[28] http://www.cellular-news.com/story/33771.php

[29] http://en.wikipedia.org/wiki/Simpson's_rule

Hoh Peter In is a professor in Dept. of Computer Science at Korea University in Seoul, Korea. His primary research interests are requirements engineering, value-based software engineering, situation-aware middleware, and software security management. He created the WinWin requirements negotiation model for quality attributes as a team member. He has published over 100 research papers. He was an assistant professor at Texas A&M University. He received his Ph.D. from University of Southern California (USC) in 1998 and his B.S. and M.S. from Korea University in 1992 and 1994, respectively, all in computer science.

Myoungrak Lee is an information & communications officer (Major) at the Republic of Korea Air Force. His research interests are embedded software engineering, information security, and lawful interception architecture. He also has interests in sensor networks. He received a Ph.D. from Korea University and a M.S. from Korea National Defense University, all in computer science.

Do Hoon Kim is a PhD candidate in the Department of Computer Science and Engineering at Korea University in Seoul, Korea. His research interests are network security, risk management, software engineering and forecast engineering. He received B.S. and M.S. degrees in Computer Science and Engineering from Korea University in 2005 and 2007, respectively.



Neunghoe Kim is a PhD candidate in the College of Information and Communications at Korea University. His research interests are requirements engineering, value-based software engineering, software engineering economics, and embedded software engineering. He received his MS in computer science from Korea University.

Byungsik Yoon was born in Korea in 1967. He received a M.S. degree in electronics engineering from Kyung-Pook National University, Korea in 1992. Since 1992, he has been with the Electronics and Telecommunications Research Institute (ETRI). He has been attending a part-time Ph.D. course in Han-Yang University since 2004. He is now a Ph.D. candidate in Han-Yang University. Currently his research interests include speech coding, lawful interception and mobile communication systems.