A Seamless Lawful Interception Architecture for Mobile Users in IEEE 802.16e Networks

Myoungrak Lee, Taek Lee, Byungsik Yoon, Hyogon Kim, and Hoh Peter In

Abstract: **Lawful interception (LI) involves legally accessing private communication such as telephone calls or email messages. Numerous countries have been drafting and enacting laws concerning the LI procedures. With the proliferation of portable Internet services such as the IEEE 802.16e wireless mobile networks, surveillance over illegal users is an emerging technical issue in LI. The ever-migrating users and their changing IP's make it harder to provide support for seamless LI procedures on 802.16e networks. Few studies, however, on seamless LI support have been conducted on the 802.16e mobile networks environments. Proposed in this paper are a seamless LI architecture and algorithms for the 802.16e networks. The simulation results demonstrate that the proposed architecture improves recall rates in intercepting mobile user, when compared to the existing LI architectures.**

Index Terms: **802.16e networks, lawful interception (LI), mobile WiMAX, mobility detection, seamless tracking.**

I. INTRODUCTION

Lawful interception (LI) is a legal interception of telecommunications conducted by law enforcement agents and administrative government bodies, local or federal, to monitor illegal and unauthorized users (e.g., terror suspects for public and hackers). The execution of an LI is allowed only when a competent authority authorizes such activity [1], [2]. In addition to the 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 the conventional networks, including wired and 3G cellular networks, a lawfully authorized body grants an LI authority in the form of a lawful order [3].

Traditionally, when a user under surveillance moves out of the currently authorized interception point, the LI authority needs reissuing via vertical handshaking between the law enforcement agency and the LI agent concerned. The term "vertical handshaking" means that issuance of the interception authority to an LI agent is based not on an automatic process, but on the human and case-by-case judgment of a law enforcement agency in charge of interception. The architectural limitations in the traditional approach prevent the LI agent from intercepting the rapidly and timely migrating illegal users. One of the grave consequences lies in the generation of a gap between different intercepted data streams, resulting in an effort to correspond to the lost packets caused by the vertical handshaking between a law enforcement monitoring facility (LEMF) and an LI agent. The longer a vertical handshaking process lasts, the larger the gap becomes between different sets of the intercepted data. Thus, a need arises for an alternative LI architecture especially tailored for the newly emerging networks.

In this paper, we propose a novel architecture which supports seamless lawful interception in the course of monitoring illegal mobile users with continuous IP mobility on 802.16e networks. This work will probably be the first of its kind addressing the architectural issues arising out of the dynamics of IP mobility in 802.16e networks. The proposed architecture has been tested via an experiment with a Qualnet 4.5 simulator, and the results show improved recall rate in intercepting mobile users.

The rest of the paper is organized as follows. Section II puts our work in perspective by providing the background and the related work. It also raises the issues in LI, with the specific example of the mobile WiMAX network. Section III discusses our approach, and describes the proposed seamless LI architecture for mobility detection. Section IV presents the simulation configuration and performance evaluation, as well as the experimental results. Finally, Section V concludes the paper.

II. BACKGROUND

A. Existing LI Architectures

Lawful interception refers to a legally authorized interception by a law enforcement agency or a government body of a targeted communication. The European Telecommunications Standard Institute (ETSI) has set forth most of the existing standards. These LI architecture standards have been used both in the wired and wireless network settings. Non-European countries have also used the standards of the ETSI [4]–[7] as reference models for developing their own ones. Each country has set forth its domestic LI agreements and relevant standards, which were developed by the regulatory agencies and law enforcement agencies [8], [9]. After the 9/11 terror attacks, for instance, the U.S.A. has enacted their own wiretapping law known as the Communications Assistance for law enforcement act (CALEA) [10]. To facilitate lawful electronic surveillance, the CALEA defines the responsibilities of communications service providers (CSPs). The existing international LI standards focus on how to structure the handover interface of the LI-related information [1], [6], [11], [12].

The ETSI and CALEA standards deem LI domains into two categories: Wired and wireless networks. A generic architec-

Manuscript received April 29, 2009.

This work was supported by the IT R&D program of MKE/IITA [2008–S–001–02, Development of WiBro network reliability and location awareness technologies], National Research Foundation of Korea Grant [KRF–2004–041–D00670], and MKE/ITRC program supervised by the NIPA [NIPA-2009-(C1090-0903-0004)]. H. P. In is the corresponding author.

M. Lee, T. Lee, H. Kim, and H. P. In are with the Department of Computer Science and Engineering, Korea University, Korea, email:{lmr2010, comtaek, hyogon, hoh_in}@korea.ac.kr.

B. Yoon is with the Department of WiBro Convergence Research Team, ETRI, Korea, email: bsyoon@etri.re.kr.

1229-2370/09/$10.00

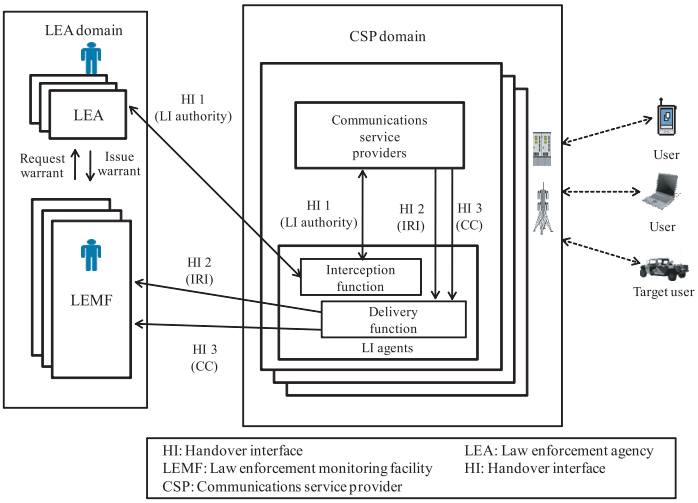


Fig. 1. Architecture of reference LI from the ETSI.

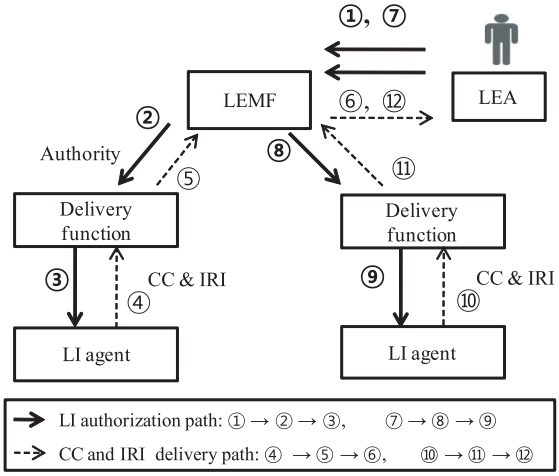


Fig. 2. The interception procedure of existing LI.

ture is proposed to intercept the wired networks and the wireless networks via access to the public switched telephone network (PSTN) [3], [13]–[15]. Another suggestion is made as to the LI architectures for VoIP, which are capable of capturing IP-based voice communications [16]–[18]. Two mode models are proposed in [17] and [18]: The session initiation protocol (SIP)-based model, and the distribution system for the LI on IP telephony networks, respectively. These architectures, however, mainly address permanent IP-based networks. In [19], 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).

In [20], three types of LI architectures are presented for the 802.16e networks: Passive, active, and hybrid solutions. Under these solutions, the network element vendor and the tapping device play a crucial role in transparent interception. The hybrid solution consists of passive and active parts. The LI architecture for international CSPs proposed in [20] fails to take into consideration how to issue warrants seamlessly. All of the existing standards and research works focus only on various vertical handshaking procedures concerning LI authorization, which, in turn, inevitably entails involvement of law enforcement agencies.

Fig. 1 exemplifies the typical architecture of the LI reference standard from the ETSI [4]–[7]. The conventional LI architecture has three types of handover interfaces (HI), where HI 1, HI 2, and HI 3 are logically separate entities. The HI 1 is used for communication between the CSP and the law enforcement agency, with the LI authority embedded in the LI agent. The 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 is represents the collection of data on the target identity, collected from telecommunication services. The HI 3 is used for the content of communication (CC) that is to be handed over from a CSP to a law enforcement agency. Here, the CC refers to the information exchanged between two or more users of telecommunication services. The law enforcement agency issues an authorization (e.g., warrant) allowing interception of the communication of a target user, and the LI authority is relegated to the LI agent located in the CSP domain.

Out of the aforementioned three interfaces, the HI 1 is most closely related to the issuance issuing an interception warrant. It is possible to transfer, via HI 1, the administrative information including, for example, (de)activation requests. The HI 1 takes on one of two forms: "Manual interface" or "electronic interface." When a law enforcement agency places a lawful interception request with a CSP, the CSP in turn requests information from the LEA [11].

Fig. 2 illustrates the interception procedure adopted in the existing LI architectures, with the arrows indicating the workflows in a lawful interception process. To initiate the interception, an administrator typically requires the identity of the target, the address of the LEMF and the network operator and service provider etc. [4]. The identity means the technical label which represents the origin or destination of all telecommunications traffic. These labels are identified according to the physical and logical locations within the network operator and the service provider's telecommunications facilities which provide access to the CC and intercept related information (IRI) [4]. As shown in Fig. 2, a human figure (i.e., law enforcement agency) alone can decide whether to issue the LI authority within the frame of the conventional LI architecture. The idea of vertical handshaking kicks in herein, referring to the arrangements made, upon issuance of a warrant, among the law enforcement agency, the LEMF, the delivery function, and the LI agent.

If a user migrates from the jurisdiction of an LI agent to that of another, the law enforcement agency should reissue the authority for the new LI agent to continue the surveillance. Due to the role played by humans during the vertical handover under the conventional LI architecture, it is likely to lose important parts of the intercepted information stream upon a user's migration. For instance, on the IEEE 802.16e wireless network, the LI targets can move throughout the different jurisdictions and CSP's domains. In this study, we assume that these issues arise in dynamic mobile environments, specifically in the context of the emerging IEEE 802.16e networks (a.k.a. mobile WiMAX networks). Hereunder, an in-depth discussion follows, concerning the challenging LI issues in the 802.16e networks.

B. Issues with Existing Architectures

LI agents are responsible for monitoring the user data packets, and intercepting and pushing the data to an LI server as ordered by a law enforcement agency. The communication overhead incurred by the LI agent and the LEMF causes, from time to time, performance problems in the course of interception, especially when a user migrating dynamically; namely, the LI agent and the LEMF are likely to sustain a significant delay (i.e., warrant-issuing time) during the vertical handshaking of a lawful interception.

As a result, some of the packets subject to interception are missed, arising out of a human error during a vertical handshaking protocol between an LEMF and an LI agent. The situation gets seriously worse, when the high bandwidth triggers rapid data exchanges, thus failing to intercept an ever-migrating moving LI target. To secure seamless lawful interception, conventional LI architectures would have to issue a bundle of warrants via vertical handshaking to cover all possible destinations of the user. A task that is excruciatingly expensive.

On the IEEE 802.16e networks, it is easy for a target user to migrate out of the jurisdiction of the current LI agent. Such change of location poses a set of difficult problems to law enforcement agencies and LI agencies [20]. Particularly in the context of the 802.16e networks, lawful interception is faced with the following challenges:

- Service networks and access thereto may belong to different CSPs.
- Security measures and encryption make it hard to conduct lawful interception.
- It may not be possible to access the location information of a mobile station from all points on a network.
- IP mobility may cause the session to extend over multiple CSP networks.
- When a user changes her IP addresses frequently, it becomes difficult to keep track of the original identity.

Considering these issues, the conventional protocol for issuing warrants is not flexible enough to secure the seamless tracking of target users. Thus, a need arises for a new automatic LI architecture in order to support seamless LI services, and a new one is proposed herein. We will discuss the proposed architecture in the next section.

III. A SEAMLESS LI ARCHITECTURES

A. Architecture Overview

Fig. 3 illustrates the proposed seamless LI architecture for the IEEE 802.16e networks. In the architecture, each LI agent is situated in an access router (AR), and transmits intercepted CC and IRIs to the LI server. The server can exist hand in hand with the AAA functionality. The LI server has the functionality of the LEMF, and receives the LI authority from the law enforcement agency. The LI agent executes the interception of the designated suspicious mobile users by the LEA.

In Fig. 3, arrows 1 and 2 indicate that the LI agents transmit the intercepted CC and IRI to the LI server. Upon receiving them, the server looks up, through the home agent (HA), the binding cache information from the previous access router

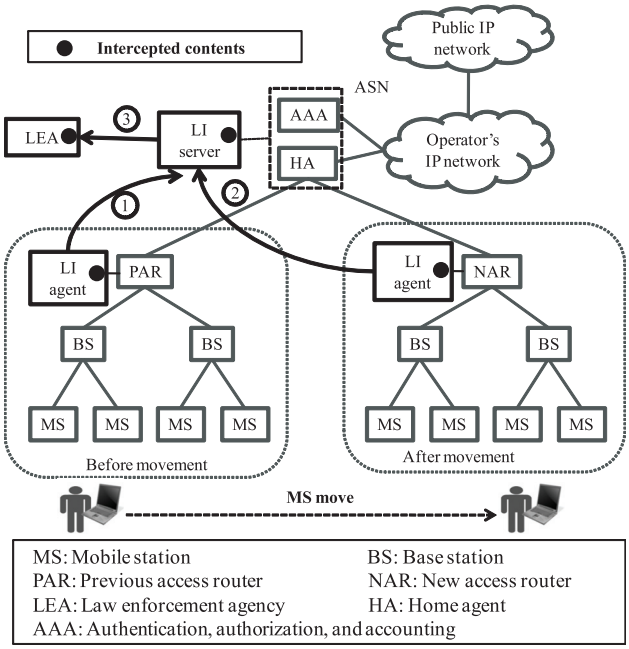


Fig. 3. Overview of seamless LI architecture.

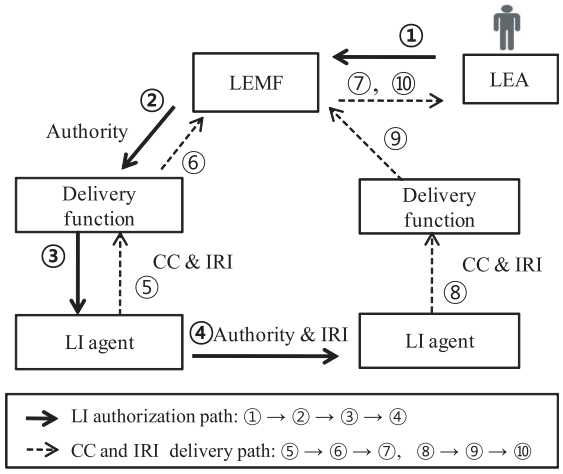
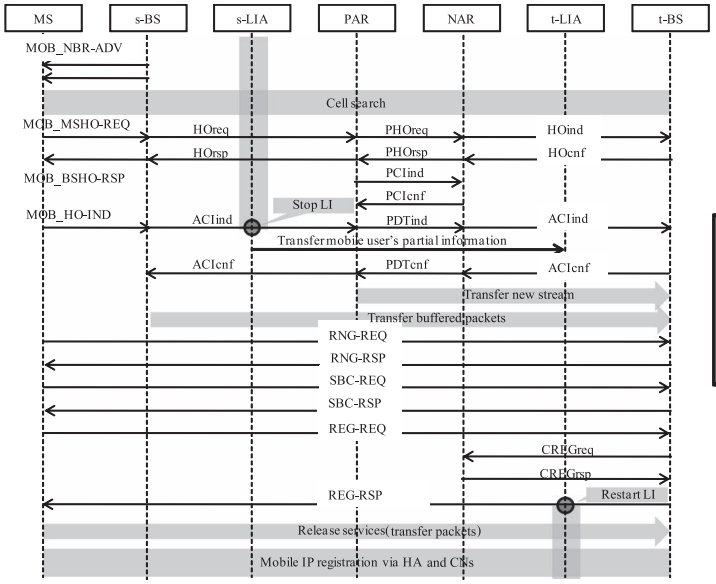


Fig. 4. Proposed interception of 802.16e.

(PAR) and the new access router (NAR). After gathering the data, the server transmits it to the law enforcement agency (arrow 3). To continue the execution of the seamless LI, the local agents must send the IRI to the server, including the information on the suspicious user's migrating paths.

Fig. 4 shows our proposed model for lawful interception, which utilizes not the vertical handshaking, but the horizontal cooperation between the LI agencies concerned to determine the new LI jurisdiction; namely, the authority and IRI are directly handed over to the LI agent in charge of the user's new location without additional authorization. Now, LI agents no longer need to send an upstream request in order to gain the authority from a law enforcement agency. Rather, they find the next target agent autonomously and enable the target agent to cooperate with the LEMF in order to intercept and push user data obtained in the course of surveillance. In order to find the target LI agent, however, mobility detection is essential, as it helps the current agent



MOB_NBR_ADV: Mobile neighbor advertisement message
MOB_MSHO_REQ: Handover request message
PHOreq: Packet access router handover request message
ACIind: Context indication message
HOind : Handover indication message
HOcnf: Handover confirmation message
ACIind: AP context information indication message
ACIcnf: AP context information confirmation message

CID: Connection identifier message
RNG-REQ: Ranging request message
RNG-RSP: Ranging response message
REG-REQ: Registration request message
REG-RSP: Registration response message
SBC-REQ: Subscriber station basic capability request message
SBC-RSP: : Subscriber station basic capability response message

Fig. 5. The procedure for the seamless LI handover.

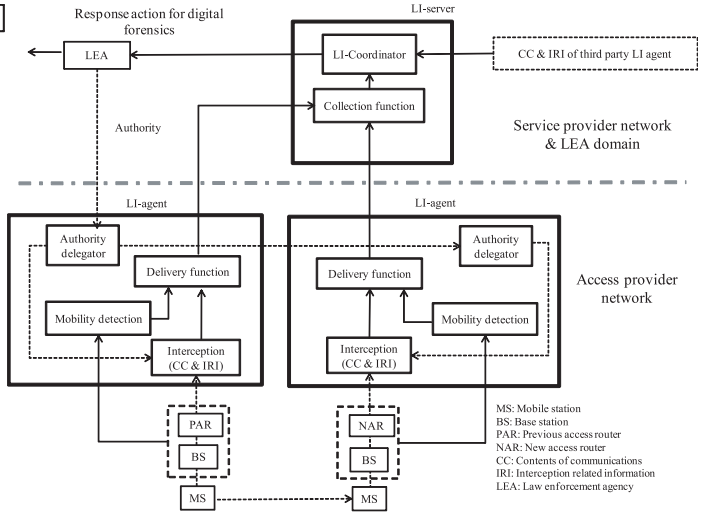


Fig. 6. The components of the seamless LI architecture.

identify the target agent among adjacent candidates. The Section III-B discusses, in detail, how to link the mobility detection to the inter-LI authority delivery. Once the target agent is found out, the LI agent previous in charge of the interception directly delivers the interception-related information with an authority signal, as shown by arrow 4 in Fig. 4. By removing the vertically exchanged control signals, it becomes possible to reduce the delay and the consequent loss of packets generated by the migrating target user.

B. Intercept Mechanism

In Fig. 3, a mobile station (MS) is assumed to move from a currently serving PAR to a target NAR. According to the IEEE 802.16e standard, and as indicated by the call flow shown in Fig. 5, a MS gets its neighbor base station (BS) information via a mobile neighbor advertisement message (MOB_NBR-ADV), which has been sent by a serving base station (s-BS). When a MS attempts to move from a previous access router (PAR) and an NAR, it places a handover request to the s-BS in the form of a handover request message (MOB_MSHO_REQ). If an s-BS requests a handover to the PAR, the PAR in turn sends out a packet access router handover request message (PHOreq) to the NAR.

Now, the seamless LI handover mechanism taps into the possible exchange of the 802.16e mobility-management messages to trigger the consequent LI handover. When the s-BS receives an access point context indication message (ACIind), the serving lawful interception agent (s-LIA) also receives a copy of the ACIind. The target lawful interception agent (t-LIA) checks the ACIind to determine whether or not the tracked MS is reconnected to a new location, and obtains the information on the MS's connection identifier (CID). Based on the CID message, the t-LIA checks the MS's CoA, traces the temporary IP address of the mobile device back at its foreign location, and executes a continuous LI. Both the s-LIA and t-LIA are closely coupled with the handover management mechanism of the 802.16e networks, and can refer to and utilize its messages. As a consequence, the LI server becomes capable of monitoring the 802.16e network and gathering all mobility-related information on the suspicious user.

Fig. 6 illustrates, in detail, the functionalities of the LI agents and the server. As authorized by a warrant, when a target mobile user accesses a BS and then an AR, the LI agent receives packets from the user via the connected access provider. The LI agent extracts CCs and IRIs from the captured packets, and transmits 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 CC's and IRI's of the target user. The LI coordinator is embedded in the LI Server, and manages the connected operations between the LIs involved in the 802.16e handoff. LI agents are embedded with the authority delegator and the delivery function to receive ACIind and CID messages via mobility detection function. Hereunder, the authority delegator is discussed in detail, which acts as an interface with the mobility detection function on the 802.16e network.

C. Authority Delegator

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 (LIID), a communication identifier (CID), and a

Algorithm 1: Pseudocodes for mobility detection in LI agent

```
// Detects mobility and informs delivery function and authority delegator of
//the target IP address
PROCEDURE MS() IS
      WHILE(true)
           receive MOB_NBR_ADV from s_BS
        IF move_detected=true THEN
          send req_confirm_msg to PAR
        ELSEIF receive_msg=true THEN
          send cache_s,cache_t to Delivery_Function_Module
          send cache_s,cache_t to Authority_Delegator
        ENDIF
       ENDWHILE
END
// Deliver the CC and IRI in the serving LI agent
// v1 is the data to be delivered via each functional module
// v2 is the each functional module of the proposed architecture
PROCEDURE send v1 to v2 IS
      CASE v2 OF
          PAR: cache_s=HoA; send v1 to NAR
          NAR: cache_t=CoA; send v1 to t_BS
          t_BS: receive ack_permit_msg to NAR
          Delivery_Function_Module
          Collection_Function(CC(v1),IRI(v1))
          Authority_Delegator: t_LI_Agent(authority_info(v1),IRI(v1))
      ENDCASE
END
// Deliver the CC and IRI
PROCEDURE receive v1 from v2 IS
      CASE v2 OF
          NAR: receive v1 from PAR
          PAR: receive v1 from s_BS
          s_BS: receive v1 from MS
          MS: receive_msg=true
      ENDCASE
END
```

network identifier (NID). These identifiers are vital to uniquely identifying the interception target and to correlation between data transferred over different interfaces [4]. 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. As shown in Figs. 5 and 6, the ADs receive the migration information from the mobility detection component, which in turn functions as an interfaces with the 802.16e mobility management.

The mobility detection component receives the handover information from the mobile IP HA. When a mobile node moves, it registers care of address (CoA) from NAR with the HA. In the 802.16e mobile network environment, whenever a mobile node moves, the 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 BS, as shown in Figs. 3 and 6. Algorithm 1 describes the procedure for mobility detection in LI agents. The pseudocode shows that whenever illegal users move to the target NAR, the serving LI agent collects the CC and IRI, and reports them to the LI server. For mobility detection, LI agents use the binding cache update information of the 802.16e networks. The LI agent detects the movement signature of the MS through the HoA and CoA. Then, the LI server rearranges the intercepted CC and IRI in accordance with the original source IP (e.g., HoA). In Algorithm 1, if the MS receive a mobile neighbor advertisement message (MOB_NBR-ADV) from the serving BS (s_BS), the mobility detection function informs the delivery function and the authority delegator of the MS's new CoA.

Algorithm 2: Pseudocodes for integration and IP ordering at the LI coordinator

```
// //During packet interception, LI agents gather the logged information from all
//intercepted packets
PROCEDURE LI-Coordinator
    FOR I =1 to End_of_ table
     FOR j=1 to End_of_table
      IF LI_table[i]= BindingCache [j].CoA
        LI_table[i]=BindingCache[j].HoA
    ENDFOR
    ENDFOR
    SORTBYTIME(LI_table );
END
```

D. LI Coordinator

The collection function of the LI server gathers and compiles the CC and the IRI from the LI agents. The collection function is embedded in the LI Server, and it guarantees the seamless LI in the 802.16e network environment. Because of the IP mobility, the LI server and the law enforcement agent may find it difficult to screen out all the suspicious user contents from the partially distributed CCs in the respective LI agents. For example, in order to screen out predefined malicious words embedded in CCs, all distributed partial CC's must be integrated and put in order, according to the suspicious user's home address (HoA). In this procedure, a target user's unique media access control (MAC) address is used to detect any IP spoofing. The collection function integrates partial CCs into a complete CC set so that the LI server recognizes the captured CCs and IRIs as valid and accepts them. Algorithm 2 is the pseudocode of the operation performed at the LI coordinator.

IV. EXPERIMENTAL RESULTS

A. Simulation Configuration

To evaluate the performance of the proposed LI architecture for the 802.16e networks, we conduct a simulation study. We model the mobile interception environment with the Qualnet4.5 simulator, Snort version 2.8.2 and the IP Network Emulation (IPNE), as shown in Fig. 7. A PC serves as an experimental platform, as long as it is equipped, at least, with a Pentium 4 Core 2 6,400 CPU and 2 Gbytes RAM. We used the Linux operating system, Ubuntu 8.10. To process the CC and the IRI, Snort is run at three LI agents and one LI server via IPNE. Consequently, the moving target can receive and transmit real data from LI agent

and LI server which are emulated as virtual nodes in the simulation via IPNE as an interface between the real data and the simulated data.

A single mobile node was used, along with 12 BSs, 3 ARs, and a HA. The LI agents and the LI server were embedded in the sensor-based Snort running on the Linux operating system. To configure communication and handovers between nodes, we used a laptop computer as an operational node, which is similar to a migrating virtual node in the simulator. External real-world data were received by the LI agents and the LI server. The real-world data was generated by the operational node, and was reproduced in Qualnet4.5 as a virtual node. The datasets include predefined words such as "terror" and "attack." In order to produce and integrate IRIs, we produced four Snort systems as three LI agents and one LI server. The IRI includes source IPs, destination IPs, alert messages, and time stamps. A 12 megabyte dump file containing malicious words was transmitted to the emulated FTP server located at the corresponding node. CC's and IRI's were captured by every LI agent and delivered to the law enforcement agent via the LI sever. To facilitate the IRI production, predefined specific Snort rules were added to the Snort as follows:

The rule set for malicious words detection in LI-agent & LI-server
R1: alert tcp any any → 192.152.36.1/24 21
(content:"LET'S DO;" msg:"Interesting user came;")
R2: alert tcp any any → 192.152.36.1/24 21
(content:"TERROR;" msg:"Suspicious noun detected;")
R3: alert tcp any any → 192.152.36.1/24 21
(content:"DESTROY;" msg:"Suspicious verb detected;")
⋮
R43: alert tcp 192.152.36.57/32 21 → any any
(content:"attack;" msg:"Suspicious verb detected;")
R44: alert tcp 192.152.36.57/32 21 → any any
(content:"bomb;" msg:"Suspicious noun detected;")
R45: alert tcp 192.152.36.57/32 21 → any any
(content:"nuclear;" msg:"Suspicious noun detected;"

The added Snort rules enable a search for malicious words e.g., "let's do," "terror," "destroy," and "kill." The simulation lasted 600 simulated seconds, and the traffic was transferred from the operational nodes to the corresponding nodes via the three ARs and one HA. An operational node was virtualized as a mobile node in the simulation. The node transferred the dataset via the three ARs. The traffic is divided through the three AR's into three parts for the LI agents. The simulation scenario is as follows:

- An operational node is emulated as a mobile unit, and it moves through the simulated environment with the LI agents located in the three ARs.
- The mobile unit uploads/downloads real-world traffic from an FTP server via BSs, ARs, and HA, once it moves through the simulated environment.
- To execute an internal interception function (IIF) as an example of an LI, we configured three real-world LI agents via virtual AR nodes. Consequently, an operational node is connected to it via an emulated VN.
- Real-world traffic, including the traffic containing malicious words, migrates through the simulated environment, and arrives at the CN. The Snort rule set captures malicious words embedded in the traffic flow.
- The LI Coordinator installed in the LI Server extracts the complete CC and IRI by ordering the partial information from the LI agents.
- The LI coordinator gathers and sorts out all the distributed CCs and IRIs from the LI agents, which have been ordered for each of the original IP addresses.
- In each LI agent, the average delay of LI authority issuance by the LEA was assumed to be 10s, 200s, and 390s, respectively.

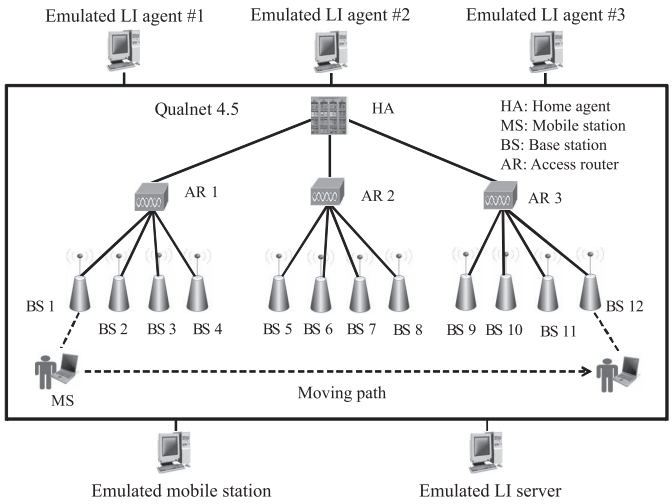


Fig. 7. The simulation configuration.

To measure the performance of the proposed seamless LI architecture for the 802.16e networks, we adopted the recall rate as the metric. In the information retrieval (IR), the recall rate measures the ratio of the number of complete documents retrieved by a search divided by the total number of relevant documents which should have been retrieved. In this paper, we define the recall rate R to be the number of intercepted packets from all transmitted packets from the target user; namely,

$$R = \frac{\text{Number of relevant packets intercepted}}{\text{Total number of relevant packets}}. \quad (1)$$

B. Evaluation of Results

Table 1 summarizes the results of the simulation conducted with 45 predefined words that are subject to interception by each LI agent and the LI server. Then, the results are compared with the scheme where the law enforcement agent (i.e., human being) takes charge of reissuing the authority upon the target's migration.

As we expected, the average recall rates for the existing architecture is significantly lower than the proposed architecture. They are 62.2%, 48.8%, and 37.7% in LI agent 1, 2, and 3, respectively, while the recall rate of the LI server is 97.8%. Fig. 8 shows how the recall is processed over a long period of time. The results are summed up in Table 1.

Table 1. Simulation results.

Types of LI architecture	Delay (human factor)	Malicious words		Detection rate (%)
		# observable words	# detected words	Recall
Vertical handshaking arch. # 1	10s	45	28	62.2
Vertical handshaking arch. #2	200s		22	48.8
Vertical handshaking arch. #3	390s		17	37.7
Seamless LI arch. (proposed)	No delay		44	97.8

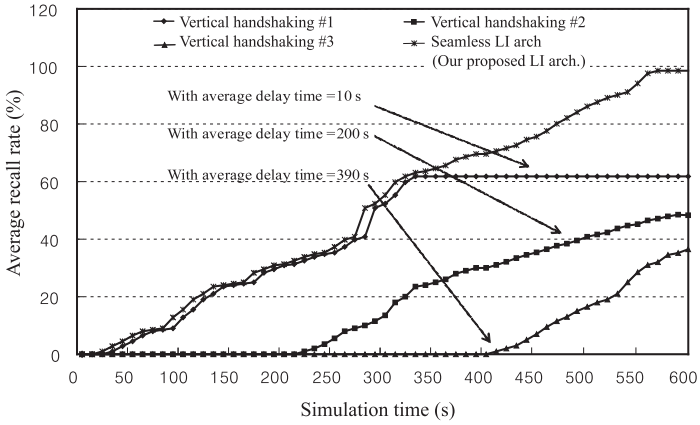


Fig. 8. Evaluation results of two approaches: Vertical handshaking vs. horizontal handshaking.

V. CONCLUSION AND FUTURE WORK

In response to an increasing number of security threats on the 802.16e networks, surveillance over suspicious users is beginning to command our attention. We presented a seamless lawful interception architecture and a specific scheme for the 802.16e network. This newly proposed architecture contributes to detection of malicious activities occurring during migration, as it integrates partial pieces of information distributed among multiple LI sensors along the migration paths of the target user. When compared with the existing LI authorization architectures, the proposed architecture better guarantees seamless interception of the CC and the IRI. We are currently working on topics such as how to detect locations and how to realize automatic LI authorization on heterogeneous large-scale networks. Another area of interest is how to summarize authority information and how to format authority messages between different service providers with different LI authorization policies.

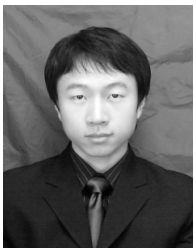
Table 2. Acronyms and definitions.

Law enforcement agency (LEA)	A government body authorized to request interception measures and to receive the results of telecommunications interceptions.
Law enforcement monitoring facility (LEMF)	An organization designated as the transmission destination of the interception results on a particular interception target.
Content of communication (CC)	Information exchanged between two or more users subscribing to a telecommunication service.
Intercept related information (IRI)	The information or data collected on the target identity, specifically on the communication associated information or data; and the services associated with the information or data.
Handover interface (HI)	Physical and logical interface(s) across which a network operator requests the interception measures.
AAA	Authentication, Authorization and Accounting.
Care of address (CoA)	A temporary IP address for a mobile device, allowing a home agent to forward messages to the mobile device.
Target agent	Adjacent LI agent that receive the LI authority from the previous LI agent

REFERENCES

[1] ETSI TS 101.671: Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic, 2009.
[2] [Online]. Available: http://www.newport-networks.com/cust-docs/87-Lawful-Intercept.pdf
[3] 3GPP TS 33.106: Technical Specification Group Services and System Aspects; 3G Security; Lawful interception requirements (Release 5), 2002.
[4] ETSI ES 201 158: Telecommunications security; Lawful Interception (LI); Requirements for network functions, 2002.
[5] ETSI TS 101 331: Telecommunications Security; Lawful Interception (LI); Requirements of law enforcements agencies.
[6] ETSI, ES 201 671: Telecommunications Security; Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic, 2007.
[7] ETSI, TR 101 944: Telecommunications Security; Lawful Interception (LI); Issues on IP interception, 2001.
[8] M. Gorge, "Lawful interception key concepts, actors, trends and best practice considerations," *Elsevier Computer Fraud & Security*, vol. 2007, no. 9, Sept. 2007, pp. 10–14.
[9] S. Gleave, "The mechanics of lawful interception," *Netw. Security*, vol. 2007, no. 5, pp 8–11, 2007.
[10] Accreditation: A Proven Management Model, 2008. [Online]. Available: http://www.calea.org/Online/AnnualReports/annual-reports.htm
[11] 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
[12] National Handover Interface Specification version 1.0, Home Office, 2002. [Online]. Available: http://www.gliif.org/standards.htm
[13] RFC2804 IETF, Policy on Wiretapping, 2000.
[14] ETSI, TS 102 232-1: Lawful Interception (LI); Handover specification for IP delivery, 2008.
[15] Communications Assistance for Law Enforcement Act of 1994 (CALEA), Pub. L. No. 103–414, 108 Stat. 4279, Congress of the United States of America.
[16] ETSI TS 101 331: Technical Specification Lawful Interception (LI); Requirements of law enforcement agencies, 2006.
[17] B. Karpagavinayagam, R. State, and O. Festor, "Monitoring architecture for lawful interception in VoIP networks," in *Proc. IEEE ICIMP*, 2007.
[18] A. Milannovic and I. Matosevic, "Distributed system for lawful interception in VoIP networks," in *Proc. EUROCON*, 2003.
[19] ETSI TR 101.514: Digital Cellular Telecommunications System (Phase 2+); lawful interception requirement for GSM, 2001.
[20] "WiMAX Lawful Interception for Communication Service Providers," Verint Systems white paper, 2008.

Myoungrak Lee is a Ph.D. candidate in the Dept. of Computer Science at Korea University in Seoul, Korea and 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 M.S. in Computer Science from Korea National Defense University (KNDU).



Taek Lee is a Ph.D. candidate in the Dept. of Computer Science at Korea University. His research interests are information security, risk analysis, security economics, and software engineering. He received his M.S. in security damage estimation and modeling from Korea University.

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

Hyogon Kim is a Professor at Korea University. He got his Ph.D. from the University of Pennsylvania in 1995. Prior to joining the Korea University, he was a research scientist at Bell Communications Research (Bellcore). His research interests include Internet protocols and applications, wireless networking, network security.

Hoh Peter In is an Associate Professor in the 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 has created the WinWin requirements negotiation model for quality attributes as a team member. He published over 100 research papers. He was an Assistant Professor at Texas A&M University. He received his Ph.D. in Computer Science from University of Southern California (USC).