A Seamless Lawful Interception Triggering Architecture for the Heterogeneous Wireless Networks

Myoungrak LEE†, Byungsik YOON††, Hyogon KIM†, Nonmembers, and Hoh Peter IN†∗, Member

SUMMARY  Lawful Interception (LI) refers to a lawfully authorized process of looking into private communication under a court-issued warrant. Quite a number of countries have been drafting and enacting laws authorizing the LI procedures on packet-switched IP networks including traditional circuit-switched ones. As the IP mobility becomes more ubiquitous, propelled by wireless networks, it becomes an issue in the LI domain to keep track of a migrating target. However, with the world’s focus on the current LI architectures, little consideration has been given to a seamless LI triggering, which accommodates IP mobility and vertical handover. Proposed herein are a seamless LI architecture and relevant triggering algorithms for the heterogeneous wireless networks. The simulation results demonstrate that the proposed architecture secures a seamless LI by capturing all the suspected target traffics without any time delay, which usually occurs during an LI triggering between different service providers. Furthermore, when compared with the existing LI architectures, the architecture significantly helps reduce transmission and the time consumed for analysis of the content of communication (CC) and intercept related information (IRI).

key words: lawful interception, heterogeneous network, mobility detection, multiple access, application identifier

1. Introduction

Lawful interception refers to a legally authorized act of a law enforcement agency or a government agency intercepting a targeted communication. Execution of an LI is not allowed, unless an appropriate authorization is acquired from a competent authority [1], [2], [18]. In the electronic surveillance model of the CableLabs [19], it shall be guaranteed that “surveillance must not take place without specific lawful authorization.”

It is banned to intercept a specific telecommunication without an appropriate legal authority. On the other hand, it also requires cooperation between a law enforcement agency and a network operator. Under the current standard procedure, an LI is authorized only upon issuance of a warrant by a government authority [7], [15]. To conduct a lawful interception, an administrator typically requires the identity of the target, and the addresses of the law enforcement monitoring facility (LEMF), and the identities of the network operator and the service provider [5].

However, as to a heterogeneous wireless network, the authorization procedure runs the risk of missing some of the important intercept related information (IRI) and its content in the course of the suspected target’s vertical handover. In a heterogeneous network, it is difficult to track the dynamic target through the real time-based LI process between a law enforcement agency and a communication service provider (CSP). Since a law enforcement agency issues an LI warrant either in paper copy or electronic format, and the target, in turn, migrates through different areas, it becomes more difficult to execute a lawful interception [15]. International organizations are making efforts to set forth a standard vertical handover protocol. To the best of our knowledge, previous studies failed to address the dynamic nature of the IP mobility in the heterogeneous networks in connection with LI architectures. In this study, we propose a triggering architecture and the relevant algorithms that support, even in the presence of a continuous IP mobility, the seamless lawful interception for surveillance on illicit mobile users in the heterogeneous networks. To test the proposed system, a Qualnet 4.5 simulator was put to use, and the results showed a reduced delay time and an improved recall rate. The rest of this paper is organized, as follows: Sect. 2 explains the research context of the LI for the mobile IP. Section 3 describes the proposed seamless LI architecture and the algorithms required for mobility detection. Section 4 illustrates the simulation configuration and the assessment results on its performance, followed by a conclusion and future work in Sect. 5. To facilitate reader’s understanding, we summarize the acronyms and definitions in Table 1.

Table 1  Acronyms and definitions.

| Acronyms   | Definitions                                                                 |
|------------|-----------------------------------------------------------------------------|
| LEMF       | Law Enforcement Monitoring Facility (An organization designated as the transmission destination of the interception results on a particular interception target) |
| CC         | Content of Communication (Information exchanged between two or more users subscribing to a telecommunication service) |
| IRI        | Intercept Related Information (The information or data collected on the target identity, specifically on the communication associated information or data) |
| CSP        | Communication Service Provider                                            |
| LID        | Lawful Interception Identifier                                             |
| CID        | Communication Identifier                                                   |
| MHM        | Media Independent Handover                                                 |
| MN         | Mobile Node                                                                |
| CN         | Corresponding Node                                                         |
| HA         | Home Agent                                                                 |

Copyright © 2010 The Institute of Electronics, Information and Communication Engineers
2. Research Context

2.1 Lawful Interception and Authorization

After the 9/11 attacks, the United States has enacted the Communications Assistance for Law Enforcement Act (CALEA), a law that enables the government to conduct wiretapping. The CALEA defines the responsibilities of communications service providers in an effort to assist law enforcement agencies in legally authorized electronic surveillance [3]. In Europe, the standards of the ETSI[4]–[8] are being used as handbooks by the other countries to develop their own guidelines. Most of the existing international LI standards focus on the architecture for the handover interface of the LI-related information [12], [15], [20]. In the ESTI technical report [27], the following three handover interfaces are mostly commonly to enforce an LI:

- **Handover Interface one (HI 1):** It is used for communication between the CSP and the LEMF with the lawful interception identifier (LIID).
- **Handover Interface two (HI 2):** It is related to the IRI to be sent as additional information about intercept from the CSP to the LEMF.
- **Handover Interface three (HI 3):** It hands over the CC from CSP to the law enforcement agency.

In the GPRS environment supporting GSM circuit switching and packet switching, a reference model [5]–[10], [26] of handover interface for LI authorization (HI1) is shown in Fig. 1.

The LI agents, which a law enforcement agency uses to conduct an interception, monitor and collect the user data packets, and intercept and transport the collected data to the LEMF via the delivery function (DF) embedded in the equipment of a CSP.

In the traditional LI scenario, it is impossible to enforce a warrant, since CSP’s belong to the jurisdictions different from the issuing country. Technically, it is also impossible to inform the CSP’s spread around the world of the LIID’s unique to a target specified by the warrant.

A more serious problem arises out of the likelihood of missing the packets that are supposed to be intercepted, due to the impracticality or technical infeasibility of a vertically oriented handshaking protocol between an LEMF and LI agents for the purpose of intercepting the user data rapidly moving into and out of adjacent zones. These circumstances lead to a quest for an alternative LI architecture. The mandatory identifiers are required to enforce an LI. The following list shows the specific identifiers required for a specific LI target under the European LI standards:

- Agreed Lawful Interception Identifier,
- Communication Identifier,
- Network Identifier (NID), and
- Communication Identity Number (CIN).

2.2 Review of Existing Vertical Handovers

Efforts are being made, without much success, to set forth standards for the vertical handover between heterogeneous networks. To secure continuity during the handover on the next generation of networks, a two-way vertical handover is being considered between the universal mobile telecommunication system (e.g. High Speed Downlink Packet Access), the WLAN and the 802.16e (e.g. mobile WiMAX and WiBro) [13], [14], [17], [21]. These vertical handover scenarios carry a high feasibility. In the IEEE Standard [14], an L-based IEEE 802.21 media independent handover (MIH) has been suggested. The MIH supports vertical handovers through exchange of information, event, and control between the 802.3, 802.11 and the 802.16 networks.

As the L3 handover, the IETF RFC [24] and [25] suggests the HMIPv6 and the FMIPv6 to support seamless mobility on heterogeneous wireless access networks. The IETF RFC [24] and [25] focuses on reduction of the handover latency caused by the MN’s movement detection. As mentioned above, numerous efforts are being made to standardize the criteria for the vertical handovers on heterogeneous wireless networks. Aware of the issues, this study is designed to address the discontinuity issues during the vertical handover of a MN, and adopts the IEEE 802.21 MIH as a well-defined standard.

2.3 LI-Related Issues in Heterogeneous Networks

Triggering the seamless LI in the heterogeneous wireless networks faces more difficulties in lawful interception in the presence of packet switched networks than in circuit switched networks. The cooperation architecture is proposed for the IP telephony on cellular networks [8]. Three LI architectures are introduced for the 802.16e networks [10]. Despite the standardization and commercializa-
tation efforts, few researchers have committed themselves to the LI architecture for the heterogeneous networks and relevant algorithms, an architecture that facilitates a seamless LI in the IP mobility environment. Moreover, the seamless LI triggering function are not included in the global LI-related standards. An ever-migrating target on the heterogeneous networks hampers tracking, because it poses a risk of losing the IRI and CC in the process of triggering properly authorized signals between LI agents of a CSP and a law enforcement agency. For example, in the case of the VoIP, the CSP may differ from the VoIP service provider, because the session initiation protocol (SIP) usually facilitates the VoIP, while the signals and media traffic take different routes on the network [11], [23]. On the packet switched networks, the IP address as a target identifier is not significant helpful as a unique LI identifier. The problem is summed up as “‘a temporary IP address cannot be used to correctly identify a target and/or its traffic permanently” [7]. Likewise, the call-forwarding feature in the LI in the IP multimedia environment is described that the call forwarding feature renders it hard to enforce an LI [27].

Despite the diverse proposals for vertical handover standards in wireless networks, the following problems occur mostly commonly in the course of lawful interception:

- During communication between a MN and a CN, the triangle tunneling makes it impossible to intercept a packet destined to the CN within the HA. In other words, gateways such as a base station, an radio network controller and a Node B have to be considered to intercept a target user.
- A target user on heterogeneous networks may generate more CoA’s and other types of reference information than its horizontal handover; namely, the LI equipment should be able to correlate the various types of information generated during a target user’s migration, such as the IRI, the IP address and the LIID. Once incorporated, a new body of information is produced.
- To secure a seamless LI, it is necessary to deliver the HI 1 information like the information on a warrant to the LI agent in advance; however, it is difficult to inform all LI agents of the HI 1-related information prior to the move of a target user.
- In the absence of a migrating move, it is impossible to predict the path of a target user. In addition, the law enforcement agency is not able to inform LI agents of the IRI such as the CoA’s and the duration of the LI.
- LI agents should be able to identify all users and to have the authority enforce an LI in order to carry it out without the additional IRI; however, it may increase the traffic between an LI agent, and an access service network such as the authentication authorization and accounting (AAA) server and the HA.
- To deliver the HI 1 information to all LI agents prior the migration of a target user, the law enforcement agency should be able to accurately predict the path of the user. It is difficult, however, to produce the information on an event to occur in the future.

The HI 2 is generated from IRI data required by the delivery function. Contrary to the conventional LI architecture which renders it difficult to correlate the newly generated IRI in the form of MN’s movement and CC, the proposed architecture duplicates and transfers the information to the target LI agent, because it is necessary to transfer the IRI on the heterogeneous networks to the neighboring interception agents for easier correlation.

Consequently, most of existent international LI standards are designed to capture target users in the wired or the 3G wireless networks, which are permanent connection-oriented services in nature. In order to track the migrating target on heterogeneous networks and to instill the dynamic feature in the LI, it is required to comprehend the mobile path of a user in advance. Especially, an LI warrant on a particular target has to be issued in advance, and all CSP’s should be informed of it.

3. Proposed Seamless LI Architecture

3.1 Overview of the Architecture

To overcome the LI-related problems on the heterogeneous wireless access networks, a seamless LI triggering architecture is proposed, as shown in Fig. 2. The new structure reduces redundancy in the CC and the IRI generated on a same target user on a real-time basis. In the proposed architecture, each LI agent is located within a specific access router (AR) and the radio network controller (RNC), and transmits the intercepted CC and IRI to the LI server located in the authentication and service authorization domain (e.g., HA, AAA). The LI server carries out the same functions as the LEMF does, and receives the LI authority from the law enforcement agency. The LI agent helps the law en-
forcement agency intercept the communication of the target mobile user.

Figure 2 illustrates the conceptual structures of the vertical handover and a seamless LI among the WLAN, the 802.16e networks and the 3G Universal Mobile Telecommunications System (UMTS). Although vertical handover protocols differ from one another and are yet to be commercialized, it is to become possible in the near future to realize the vertical handover scheme shown in Fig. 2 [21]. Considering the current trend of the wireless communication market like in South Korea, the foregoing scheme seems more promising [13].

In Fig. 2, LI agents located on heterogeneous networks transmit, to the LI server, the intercepted CC and the IRI. The server receives the CC and the IRI from the LI agents, and utilizes the binding cache information from the previous AR and RNC. Once the data are gathered, the server transmits the information to the law enforcement agency. To enforce an LI without any breach, the local agents must send the IRI to the server, including the information on the target user’s moves.

3.2 Basic Assumptions for the Vertical Handover

Active efforts are being made to standardize the IP-based heterogeneous wireless network. Thus, the seamless LI triggering architecture proposed herein takes on the most plausible vertical handover schemes. Our assumption for the seamless LI execution is based on the IEEE 802.21 standards supporting an MN, which has three L2 interfaces, namely IEEE 802.11, IEEE 802.16, and UMTS as shown in Fig. 2. Although there are a variety of mechanisms previously proposed for the vertical handover, the seamless LI requires the following basic communication conditions:

- During a vertical handover, the CSP has to remain unchanged to prevent consistency problems in the course of authentication, authorization and accounting.
- An LI is assumed to be enforced within a single national jurisdiction.
- Basically, a mobile node contains multiple interfaces to support the IEEE 802.3, the 802.11 and the 802.16e networks.
- This study assumes that the seamless LI be executed within a country or between different countries with the identical LI regulations.

Upon commercial application, however, multiple CSPs could get involved during the vertical handover, especially, to support roaming through a region consisting of different states or a group of sovereign countries (e.g., European Union). Still in this environment, the proposed seamless LI triggering architecture serves the purpose under the following conditions:

- The mobile node and corresponding node should be able to communicate with each other, even under the different CSPs.
- A roaming agreement is needed to trigger a seamless LI between different states and/or countries.
- The LI agents of different CSPs should be able to trace identifier of the moving mobile node even through the identifier may be changed.

The tracking identifier (or universal identifier) of the MN constitutes a key success factor of an authentication, authorization and accounting (AAA) policy under different CSPs. Numerous studies have been conducted to address the problems arising out of identifier tracking. Herein, however, the topic is not addressed, since it lies outside the scope of this study.

3.3 Media Independent Handover (MIH)

Media independent handover is a standard being developed via IEEE 802.21. The major feature of the MIH lies in its ability to enable handovers between heterogeneous technologies (e.g., IEEE 802 and cellular technologies) without service interruption [14], [22], [28]. The key function of the 802.21 is the Media Independent Handover Function (MIHF), which serves as an intermediate layer between upper and lower layers. The MIHF functions mainly to coordinate exchange of information and commands between different devices that are associated with the handover decision-making procedure and the execution thereof. The MIHF encompasses three different services: namely, Media Independent Event Service (MIES), Media Independent Command Service (MICS) and Media Independent Information Service (MIIS). Figure 3 shows the interaction of MIH components. The MIES carries out three functions (i.e. event classification, event filtering and event reporting) in accordance with dynamic changes in link characteristics, link status, and link quality. The MIES also provides services to the upper layers by reporting both local and remote events. The MICS enables higher layers to control such lower layers as physical, data link and logical link layers. Therefore, MIH application uses the MICS to control the MAC layer and, thereby, enables handover and mobility.

In addition, the MIIS provides details about the characteristics and the services, which in turn have been provided by the serving and the neighboring networks. Consequently, efficiency improves concerning system access and handover.
decisions. Figure 4 shows the MIHF communication model. The MN exchanges MIH information with its MIH point of service (PoS). The MIHF in a Network Entity becomes an MIH PoS, when it communicates directly with an MN-based MIHF. When an MIHF in a Network Entity does not have a direct connection to the MN, it stops serving as an MIH PoS for that particular MN. However, the same MIH Network Entity can still act as MIH PoS for a different MN. An MN can have multiple L2 interfaces. However, MIHF communication does not necessarily take place on all of the L2 interfaces of an MIH-capable MN. For example, it may occur on an MIH-capable MN with three L2 interfaces of IEEE 802.11, IEEE 802.16, and IEEE 802.3.

3.4 Concept of Automatic LI Authorization

Automatic LI Authorization is required to support seamless LI service. Otherwise, the LI is interrupted by manual or electric transmission of the LI authorization by a human. A law enforcement agency issues an authorized legal order (e.g., warrant) to intercept the communication of a target user, and the LI authority is relegated to the LI agent located in the CSP domain. When a target user moves from a previous CSP (P-CSP) to a new CSP (N-CSP), the previous authority delegator transmits the authorization information to the new authority delegator manually or electronically by a human. The mobility detection component sends out to the LI authority delegators the information on the moves. The mobility detection algorithm applies to the authority delegator, and the delivery function is described in the Sects. 3.5 and 3.6. The authorization information contains the data on the LIID, the CID, and NID. These identifiers help identify a target for interception and correlate between the data exchanged over different interfaces [5]. This scheme of authority relegation is vital to tracking a migrating mobile user. On a 3G wireless network, which is also a mobile environment in nature, the law enforcement agency relegates the authority of LI to a mobile service-switching center [16]. This human-intervention authorization procedure, however, runs the risk of missing important information pieces in a dynamic mobile Internet environment. Thus, we propose automatic LI authorization. Figure 4 depicts the entire lawful interception process step by step. The less reliant the vertically exchanged control signals become, the shorter it takes to process interception requests and relevant data. Thus, it becomes unnecessary for an LI agent to send an uplink request in order to gain authority from the LEMF. On the contrary, the next target agent is automatically detected, enabling the target agent to cooperate with the LEMF in order to intercept the user data obtained during monitoring. To authorize LI automatically, the triggered agent directly sends out the IRI upon an authority signal. The mobility detection mechanism enables the proposed process. The function of mobility detection plays an essential role in the seamless lawful interception, because it helps a current agent identify and screen out a target agent from among diverse candidates.

3.5 Authority Delegator

The LI mechanism for authority relegation is vital to a dynamic vertical handover environment. On a 3G wireless network, which is also a mobile environment in nature, the law enforcement agency relegates the LI authority to a mobile service-switching center [16]. However, this authorization procedure runs the risk of missing important contents in dynamic mobile Internet environments, arising out of a human intervention on the issuance of a warrant. The law enforcement agency issues an order to intercept the communication of a target user, and the LI authority is relegated to the LI agent. When a target user migrates from a serving access router of the 802.11 to a new access router of the 802.16e, the authority delegator immediately transfers the LI authority and the IRI to the target agent without a new authorization from a law enforcement agency to trigger the LI. The previous authority delegator transmits the LI authority, and automatically intercepts the related information to the new authority delegator located on a candidate network.

As shown in Figs. 5 and 6, the authority delegators receive the migration information from the mobility detection component. The mobility detection algorithm applies to the authority delegator through the delivery function described in the Sect. 3.6. The authorization information contains the data on, for example, the lawful interception identifier and the target identity, the starting and ending points of the interception, the destination addresses of the IRI and the CC [15], [27]. These identifiers help identify the interception target and correlate the data exchanged over different interfaces [5].

Presented in the Sects. 3.6 and 3.7 are the detailed descriptions of mobility detection, collecting function and LI correlation, all of which are applicable to both of horizontal and vertical handovers.

3.6 Mobility Detection

Mobility detection refers to the process of detecting target MN’s, based on the handover binding cache information on
the heterogeneous networks. The handover binding cache information is transmitted to LI agents via the BS, as shown in Fig. 4. Whenever a target user moves to a candidate network (e.g. new access router), a serving LI agent collects the content of the subject communication and the IRI, and reports it to the LI server. To detect the mobility, an LI agent uses the binding cache information on the heterogeneous networks. An LI agent detects the traces of a move of a target mobile user through the HoA and the CoA. Then, the LI server rearranges the intercepted CC and the IRI of the moving target.

The mobility detection component receives the handover information from the media independent information service (MIIS) server. When a mobile node moves, the MIIS server updates the CoA with the serving PoS, and the CoA of the mobile node.

**Algorithm 1**: Pseudocodes for Mobility Detection in LI Agent

```
// Detects mobility and informs delivery function and authority delegator of the target IP address
PROCEDURE MN() IS
  WHILE(true)
    [Code]
```

**Fig. 5** Components of seamless LI architecture.

**Fig. 6** Call flows during activation of seamless LI triggering in the proposed architecture.
receive link_measurement_report from serving_PoA
IF move_detected=true THEN
send MIH_GetInformation.confirm to MIIS_server
ELSEIF receive_msg=true THEN
send cache_s, cache_j to Delivery_Function_Module
send cache_s, cache_j to Authority_Delegator
ENDIF
ENDWHILE
END

// Deliver the content of communications and intercept related information
// v1 is the data to be delivered via each functional module
// v2 is the each functional module of proposed architecture
PROCEDURE send v1 to v2 IS
CASE v2 OF
    serving-MIH_PoS: cache_s=HoA; send v1 to target-MIH_PoS
    serving-LIA: cache_s=HoA; send v1 to target-LIA
    target-MIH_PoS: cache_s=CoA; send v1 to target_BS
    serving-LIA: cache_s=HoA; send v1 to target-LIA
    target_BS: receive ack_permit_msg from get-MIH_PoS
    serving-MIH_PoS: cache_s=HoA; send v1 to target-MIH_PoS
    target-MIH_PoS: cache_s=CoA; send v1 to t_BS
    target_BS: receive ack_permit_msg from target-MIH_PoS:
        Delivery_Function_Module:
            Collection_Function(CC(v1),IRI(v1))
        Authority_Delegator: target_LI_Agent(authority_info(v1),IRI(v1))
ENDCASE
ENDPROCEDURE receive v1 from v2 IS
CASE v2 OF
    target-MIH_PoS: receive v1 from serving-MIH_PoS:
        target-LIA: receive v1 from serving-MIH_PoS
        serving-MIH_PoS: receive v1 from MIIS_server
        serving-LIA: receive v1 from MIIS_server
        serving-MIH_PoS: receive v1 from MN
        MN: receive_msg=true
ENDCASE
END

3.7 LI Coordinator

An LI coordinator is intended to gather the CC and the IRI in accordance with the related LI information. To conduct a seamless surveillance on target mobile units, the LI coordinator gathers parts of the CC and the IRI that have been originally distributed to the LI agents. When an LI server receives incomplete information from the agents, the LI coordinator is still capable of generating the complete IRI including the target user’s CoAs. The LI coordinator automatically puts in order the intercepted CC, whenever a target user moves. Extraction of the IRI information is carried out, using the original IP address. It uses the CoAs and the HoAs of the HA’s binding cache table in order to sort out and complete various pieces of the CC and the IRI. Finally, the LI coordinator completes the target user’s traces.

4. LI Triggering Procedure

4.1 LI Triggering in Horizontal Handover

The horizontal handover mechanism refers to the technical ability to move from one access point to another within the same type of networks. There could be various horizontal handover scenarios such as inter-WLAN, inter-802.16e and inter-3G networks. Figure 7 shows an example of horizontal handover and LI authority delegation on the WLAN networks. In Fig. 7, the previous LI agent remains capable of receiving both the same message from the MIIS server and the information of the next AP of a nearby access router. During a horizontal handover, the MIIS server transmits the information that is needed to perform a horizontal or a vertical handover. According to the proposed algorithm 1 (mobility detection), the MIIS server encompasses a nearby access router available and a next target access router; thereby, a serving LI agent (LIA-s) delegates the LI authority to the target LI agent (LIA-T). Figure 7 presents, in detail, how messages are exchanged. When compared with vertical handover, horizontal handover stands out with the MN’s next point of attachment such as access point of 802.11 or base station of 802.16e networks.

4.2 LI Triggering in Vertical Handover

While horizontal handover mechanisms are usually used within the same type of networks, vertical handover involves an operation between different types of networks. In the latter case, the MN determines the types to be put to use. Figure 5 shows the basic components of the proposed seamless LI triggering architecture and the specific functions of the LI agents and the server. In Fig. 5, an MN migrates from the current access point (AP) of a WLAN to the RNC of a 3G UMTS via the access router (AR) on an 802.16e network. It also transmits a handover request. When an MN is connected to a BS via an AR and a HA, an LI agent intercepts the CC and the IRI from the captured packets. An LI agent receives packets from the linked access provider, and transmits them to the LI server via the delivery function. The LI coordinator is embedded in the proposed seamless LI architecture in order to guarantee the continuity of an LI on heterogeneous networks.

Figure 6 shows the call flows between components of the proposed LI triggering architecture. In the meanwhile, Fig 8 describes the LI procedure within a communication mechanism on heterogeneous wireless networks. The detailed procedure of the seamless LI triggering is as follows:
An MN receives a report on the WLAN (IEEE 802.11) link through the MIH_Get-Information request and its response.

An MN sends an MIH_MN_HO_Candidate_Query message to the serving point of service (PoS) to check the linkage of candidate checks, and the resource availability of the 802.16e networks.

After the serving PoS (s-PoS) receives the MIH_MN_HO_Candidate_Query request from an MN, the s-PoS retrieves the resource information from the target network by sending an MIH_N2N_HO_Query_Resources message to the candidate PoS’s.

The serving lawful interception agent (LIA-S) also receives an MIH_MN_HO_Candidate_Query request. The target lawful interception agent (LIA-T) monitors whether or not the MN is reconnected via the MIH_MN_HO_Candidate_Query request/response queries.

When the s-PoS receives an MIH_N2N_HO_Query_Resources response, the LIA-S deactivates the interception of the CC and the IRI.

The LIA-S relegates the LI authority to all candidate LIA’s in the candidate network.

An MN sends an MIH_MN_HO_Candidate_Query request to the s-PoS to disseminate the selected information on the target network. The s-PoS reserves the data on the target network by means of MIH_N2N_HO_Query_Resources messages.

After transmitting a registration request (REG_REQ) and a registration response (REG_RSP) between the
MN and the BS of an 802.16e network, the LIA-S transfers the LI authority to a new LIA in the 802.16e network.

- When the mobile IP registration and the binding update are completed, a new LI connection establishes and the LI process gets started.
- The s-PoS exchanges the MIH_N2N_HO_Complete messages with the previous PoS on the WLAN network to release the resources and to restart LI in 802.16e networks.

Figure 8 describes the flow of the vertical handover and the seamless LI between 802.11 and 802.16e networks. The handover mechanism is basically based on MIH of the IEEE 802.21 standards. In Fig. 5, an MN has a multiple network interface and can be connected to different types of networks.

Based on the MIH_MN_HO_Candidate_Query request, the LIA-T checks the MN CoA, and continues the LI process. Both of the LIA-S and the LIA-T are closely related to the handover mechanism of the IEEE 802.21 standards, and take consideration of the messages. The LI server is located on a service provider network, and is responsible for monitoring the distributed LI agents and gathering the CC and the IRI on the target users.

5. Performance Assessment

5.1 Simulation Configuration

We used the Qualnet 4.5 simulator, the Wireshark 1.2.0 and the IP network emulator (IPNE) to produce a simulated heterogeneous network. We configured the vertical handover environment such as the coexistence networks of IEEE 802.11, IEEE 802.16e and UMTS. In the simulation, the MN is designed to change the connectivity between various networks during a migration. To configure a communication and handovers between different wireless networks, the operational node generated real data, which, in turn, were reproduced in the Qualnet 4.5 as a virtual node. In order to produce and integrate the IRI, four Wireshark 1.2.0 networks were re-morphed into three LI agents and a LI server. When a target MN accessed a new access router, the authority delegator issued an interception command to the target LI agent. The function of 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 by putting in sequence the partial information transmitted from the LI agents. The coordination installed in the LI server extracts the complete CC and IRI by putting in sequence the partial information transmitted from the LI agents.

The LI coordinator gathers, sorts out the distributed CC and IRI from the LI agents and arrange them in order, partial information transmitted from the LI agents.

The LI coordinator installed in the LI server extracts the complete CC and IRI by putting in sequence the partial information transmitted from the LI agents.

The LI coordinator gathers, sorts out the distributed CC and IRI from the LI agents and arrange them in order, using the original IP addresses.

Issuance of a warrant is affected by human intervention. The ETSI standards provide that a minimum about of the manual translation is required to deliver the warrant via the HI 1 [6]. Herein, it is assumed to take between 1 to 40 minutes for a law enforcement agency to take out a subsequent warrant.

- The time consumed for the first vertical handover from the WLAN to the 802.16e was set to last 50 seconds, and the time for the second handover from the 802.16e to the UMTS was set to last 150 seconds.

Per the foregoing procedure, the LI server collected the CC and the IRI unique to a target mobile user, and delivered
them to the law enforcement agency via the LEMF.

5.2 Assessment of Results

An assessment was carried out on the proposed seamless lawful interception architecture from the viewpoint of mobility detection and LI authority relegation on the heterogeneous wireless networks. Concerning the content interception on a heterogeneous network, the simulation results showed that the proposed architecture lost a small amount of the packets during interception. It follows that the delay time is reducible through mobility detection and triggering of a seamless LI. When an MN accessed a new access point, the authority delegator automatically delivered an interception command to the target LI agent. For the triggering of a seamless LI on the heterogeneous networks, the mobility detection provided real-time information to the LI agents and the authority delegators located on the 802.16e and other networks.

Figure 9 tallies the results, which demonstrate the successful tracking of the target mobile users and the seamless lawful interception through the proposed architecture. Two types of exponentially distributed communications were tested in this study, and the volumes of the intercepted CC and IRI of the two were compared. The proposed architecture caused little packet losses at the LI agent and the server, and intercepted, without much loss, the partial information received from the LI agents 1, 2 and 3. The results are quite significant, because execution of a seamless LI on the next heterogeneous wireless networks and in a pervasive computing environment addresses one of the emerging LI-related issues. In case of the conventional architecture, the longer it takes to re-issue a warrant, the fewer packets are intercepted. On the other hand, our proposed seamless architecture shows a constantly high performance in terms of the total number of intercepted packets.

6. Conclusions

This study proposes an architecture for the seamless execution of an LI in the heterogeneous wireless networks. It also examined, in detail, the main issues concerning lawful interception on heterogeneous wireless networks. The prototype of the proposed architecture, which was put to use herein, has demonstrated the possibility of a lawfully authorized seamless tracking of a target mobile user in complicated network environments. The results also demonstrate that it helps reduce the time for transmission and analysis of the CC and the IRI, compared with the existing LI architectures. We are currently working on how to apply the identifier detection and the relegation of seamless LI authorization to P2P networks supporting VoIP services. Our attention is also being given to topics such as authority information and authority message format for the complicated pervasive computing environment consisting of diverse message formats and communication mechanisms.

Acknowledgments

This study was supported by Korea University Funding, the IT R&D program of the MKE (2008-S-001-02, Development of WiBro network reliability and location awareness technologies), and the Korea Research Foundation Grant (MOEHRD, Basic Research Promotion Fund) (KRF-2007-331-D00360). For more information, contact Hoh P. In at hoh_in@korea.ac.kr

References

[1] http://www.newport-networks.com/cust-docs/87-Lawful-Intercep.pdf
[2] M. Gorge, “Lawful interception key concepts, actors, trends and best practice considerations.” Elsevier Computer Fraud & Security, vol.2007, no.9, pp.10–14, Sept. 2007.
[3] S. Gleave, “The mechanics of lawful interception,” Network Security, Elsevier, vol.2007, no.5, pp.8–11, May 2007.
[4] ETSI ES 201 158: Telecommunications security; Interception (LI); Requirements for network functions.
[5] ETSI ES 201 331: 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.
[7] ETSI, TR 101 944: Telecommunications Security; Lawful Interception (LI); Issues on IP interception.
[8] “Juniper Networks FMC Security Solution,” http://www.juniper.net/solutions/literature/solutionbriefs/351287.pdf
[9] “WiMAX Lawful Interception for Communication Service Providers,” Verint Systems white paper, 2008.
[10] http://www.calea.org/Online/AnnualReports/annualreports.htm
[11] P. Branch, “Lawful Interception of IP Traffic,” Proc. Australian Telecommunications Networks & Applications Conference (ATNAC), Dec. 2003.
[12] ETSI, TS 102 232: Lawful Interception (LI); Handover specification for IP delivery
[13] K. Kim, Y.H. Kim, J. Kim, and S.H. Lee, “PMIP based WiBro-HSDPA seamless mobility support,” KNOM Review, vol.11, no.1, pp.12–26, 2008.
[14] IEEE Standard for Local and metropolitan area networks, part21: Media Independent Handover Services, 2008.

[15] ETSI TS 101 671 v3.4.1: Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic, 2009.

[16] ETSI TS 101 509 v8.1.0: Digital cellular telecommunications system (Phase 2+); Lawful Interception; Stage2 (3GPP TS 03.33 version 8.1.0 Release 1999), 2000.

[17] RFC5270 Mobile IPv6 Fast Handovers over IEEE 802.16e Networks, 2008.

[18] RFC2804 IETF Policy on Wiretapping, 2000.

[19] Cable Television Laboratories: PacketCable Electronic Surveillance Specification, PKT-SP-ES-DCI-101-060914, 2006.

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

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

[22] D.L. Oliva, A. A. Banchs, I. Soto, T. Melia, and A. Vidal, “An overview of IEEE 802.21: media-independent handover services,” IEEE Wireless Commun., vol.15, no.4, pp.96–103, 2008.

[23] J. Seedorf, “Lawful interception in P2P-based VoIP systems,” IPTComm 2008, LNCS 5310, pp.217–235, 2008.

[24] S. Hierarchical, “Mobile IPv6 mobility management,” IETF RFC 4140, 2005.

[25] K. Fast, “Handovers for mobile IPv6,” IETF RFC 4068, 2005.

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

[27] ETSI TR 102 053 v1.1.1 Telecommunications security; Lawful Interception (LI); Notes on ISDN lawful interception functionality, 2002.

[28] W. Lee, M.S. Kang, and M.S. Lim, “Implementation of 802.21 for seamless handover across heterogeneous networks,” APNOMS 2007, LNCS 4773, pp.326–333, 2007.

[29] R.D. Yates and D.J. Goodman, Probability and Stochastic Processes, 2nd ed., p.115, John Willy and Sons, 2005.

[30] http://www.mobilemarketer.com/cms/news/advertising/3166.html

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

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 a M.S. in computer science from Korea National Defense University.

Byungsik 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 is also attending Part-time Ph.D. course in Han-Yang 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 the 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, and computational neuroscience.

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).