Implementation of Lawful Interception Within IMS

Zhang Lu, Kong Min
(Central R&D Institute of ZTE Corporation, Nanjing 210012, P. R. China)

Abstract:
Lawful Interception (LI) is a system which monitors a user or a communication in support of criminal investigation. It is a necessary function of the telecommunication operator. The telecommunication standards bodies such as ETSI, 3GPP are producing technical specifications on LI system, and have developed standards on handover areas and interception areas which can guide the implement. IP Multimedia Subsystem (IMS) is a new core-network architecture introduced after the version of 3GPP Release 5, which is layer-designed, IP-based, and using Session Initiation Protocol (SIP) as application protocol. There are two typical implementations of LI within IMS, distributed type and centralized type.

1 Introduction to IMS

IP Multimedia Subsystem (IMS) is a subsystem supporting IP multimedia services, which was proposed by the 3GPP in Release 5. Its main features include layered architecture, IP-based core network and using Session Initiation Protocol (SIP) as its communication protocol[1-2].

2 Lawful Interception Overview

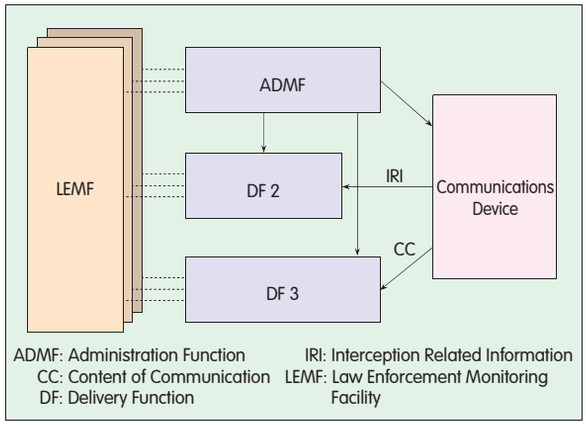
Lawful Interception (LI) is the interception of telecommunications by security authorities for the purpose of law enforcement. It involves two aspects: signaling and content of communication. Figure 1 is an interception framework proposed by the ETSI[3].

3GPP and ETSI have done lots of work in developing standards for LI. Up to now, they have worked out the standard for handover interface between Law Enforcement Monitoring Facility (LEMF) and Administration Function (ADMF)[4-5] as well as the standard for the interface between communications device and LI device[6]. However, in the Next Generation Networks (NGNs), represented by IMS, implementation of interception data collection in the core network is still not clearly defined. One key problem is how to deploy the interception data collection function into IMS network. In an interception system, the interception data collection is a logic function, which can either be integrated into each functional entity of IMS or be performed with an independent device. By the arrangement of interception data collection unit, the interception can be divided into two types: distributed and centralized. Below the two interception types, especially the centralized one, will be discussed in detail.

3 Implementation of LI

3.1 Distributed Interception

In distributed interception[7], the Lawful



▲Figure 1. Interception framework proposed by ETSI.

Interception Collection Facility (LICF) is arranged between IMS network elements that perform interception functions. Often, the LICF is placed between the access device and a Proxy–Call Session Control Function (P–CSCF) device or a Serving–Call Session Control Function (S–CSCF) device.

The implementation of distributed interception proceeds as follows:

(1) Configure the identification information of interception target on the LICF, such as user ID or service ID[8]. The user ID should be the unique information of the user, for instance, the user identity or the user's telephone number; while the service ID can be the service feature code that uniquely identifies the user service.

(2) The LICF receives signaling streams and media streams from other network nodes.

(3) Upon receiving the streams, the LICF checks whether the messages of the interception target are included in these streams.

(4) If the messages of interception target are contained, the LICF sends the signaling streams and media streams to both their receivers and monitoring device; otherwise, it only sends these streams to their receivers.

3.2 Centralized Interception

In centralized interception[9], the LICF is placed in the IMS' core network. One scenario is to use the LICF as a SIP Application Server (AS) of IMS network. The LICF is used with the Home Subscriber Server (HSS) to implement or release interception of a target user by dynamically changing the Initial Filter Criteria (iFC)[10]. In the following chapters, we will discuss this interception mode from three aspects: setting, releasing, and implementing.

3.2.1 Interception Setting

To intercept the telecommunications of a specific user, it is necessary to follow the steps below to set the interception target.

(1) The interception center gives an interception instruction to an interception AS, where the target user identity and contents for interception are included.

(2) The interception AS then makes a request to the HSS, asking to activate the subscription rule of the target user if it already exists or to add and activate the subscription rule if it does not exist. The iFC that triggers the interception can be configured in the HSS in advance and activated by the interception AS; or it can be first changed by the interception AS or other network elements through the interface the HSS provides, and then dynamically added into the HSS by the interception AS.

(3) After the HSS updates the subscription rule of the interception target, it notifies the S–CSCF of the updated information.

(4) Upon receiving an initial request related to the interception target, the S–CSCF sends the request to the interception AS based on the subscription rule[11].

Now, the signaling and media streams of the target user can be intercepted.

3.2.2 Interception Release

To release the interception of a specific user, do the following:

(1) The interception center sends an interception release instruction to an interception AS, where the identification information of the user which will be released from the interception is included.

(2) The interception AS then sends a request to the HSS, asking to deactivate the subscription rule of the user.

(3) The HSS updates the subscription rule of the user and notifies the S–CSCF of the updated information.

(4) When receiving an initial request related to the user, the S–CSCF does not send the request to the interception AS.

So far, the interception of the specific user is released.

3.2.3 Interception Implementation

Suppose the interception center instructs to intercept the conversations of user A. The implementation procedure is illustrated in Figure 2.

(1) The interception center sends an interception instruction to the interception AS, instructing to intercept the conversations of user A.

(2) The interception AS sends a subscription rule modification request to the HSS to activate the interception subscription rule of user A.

(3) The HSS notifies the S–CSCF of the change of user A's interception subscription rule.

(4) User A initiates an INVITE call request to user B, where user A's media description (SDP A) is included.

(5) The S–CSCF sends the INVITE request to the interception AS based on user A's interception subscription rule.

(6) The interception AS updates the media description in the INVITE request, adding itself as a receiver (SDP AS).

(7) The interception AS reports signaling messages to the interception center.

(8) The interception AS forwards the updated INVITE request to the S–CSCF.

(9) The S–CSCF forwards the INVITE request to user B.

(10) User B replies with Response 183, where user B's media description (SDP B) is included.

(11) The S–CSCF forwards Response 183 to the interception AS.

(12) The interception AS updates the media description in Response 183, and changes the destination as itself.

(13) The interception AS forwards the updated Response 183 to the S–CSCF.

(14) The S–CSCF forwards Response 183 to user A.

(15) The interception AS reports signaling messages to the interception center.

(16) User A exchanges signaling messages with user B via the S–CSCF and the interception AS to set up a call.

(17) User A sends media to the interception AS.

(18) The interception AS forwards media to the interception center.

(19) The interception AS forwards the media to user B.

(20) User B sends the media to the interception AS.

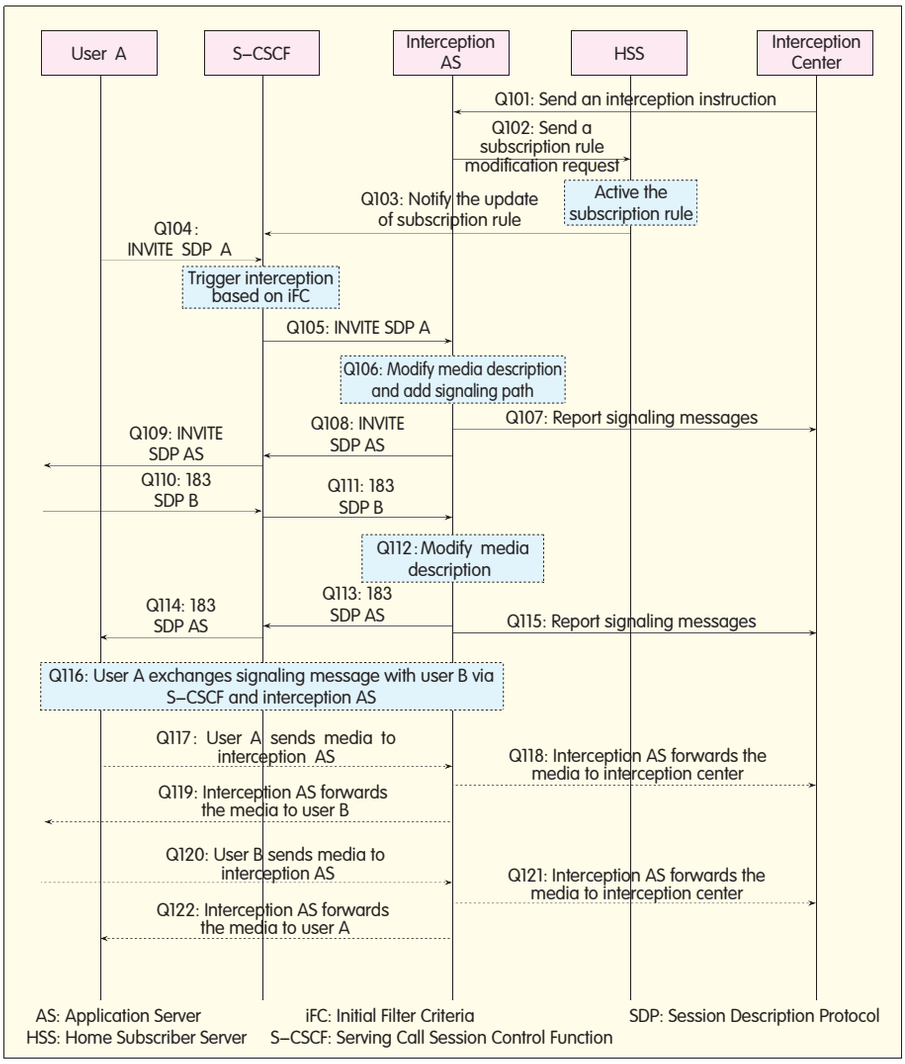
(21) The interception AS forwards the media to the interception center.

(22) The interception AS forwards the media to user A.

In this way, the interception of user A's conversation is completed. This procedure is designed for user A–originated calls. For user A–terminated calls, the interception procedure is similar.

3.3 Comparison between Two Interception Modes

Distributed interception is a traditional



▲Figure 2. Interception implementation procedure.

solution. Its advantage is that many interception points can be set, allowing relatively comprehensive information to be collected. Its disadvantage is the interception points are distributed. In IMS, there is a large number of access networks, P–CSCFs and S–CSCFs, so the interception is difficult to implement and the networking is restricted. Moreover, because the signaling and media streams of all users are collected by the LICF, the network's fault points and the risk of congestion increase.

The centralized interception adopts IMS network architecture and has the following advantages;

(1) The centralized arrangement of interception devices effectively solves the engineering and management problems of interception devices, which always perplex distributed interception.

(2) By modifying the iFC, the centralized interception method ensures the interception device to collect specific user's signaling and media for interception. As a result, the load of the interception device is considerably decreased and congestion is unlikely to occur.

(3) The centralized interception method treats interception as one application of IMS. All interception operations follow the processing rules of IMS and they have no impact on existing IMS, thus ensuring the feasibility and backward compatibility of this method.

(4) The triggering of interception with iFC will not affect the normal call process even if the interception AS does not work. Therefore, the robustness of the entire system is enhanced.

4 Conclusion

IMS is a new network architecture. Taking advantage of the scalability of IMS for various applications has become an important research topic. The interception solution discussed in this paper not only realizes the interception within existing IMS network, but also provides useful reference for implementation of other applications in IMS.

References

[1] CAMRAILLO G, MARTIN M A G. 3G IP**多媒体子系统** IMS: **融合移动网与因特网** [M]. **张同须, 等译. 北京: 人民邮电出版社**, 2006.

[2] POIKSELKA M, MAYER G, **等**. IMS:**移动领域的**IP**多媒体概念和服务** [M]. **赵鹏, 译. 北京: 机械工业出版社**, 2005.

[3] ETSI TR 101 943 V2.2.1. Concepts of Interception in a Generic Network Architecture [S]. 2006.

[4] ETSI TS 101 671 V3.2.1 Handover Interface for the Lawful Interception of Telecommunications Traffic [S]. 2007.

[5] ETSI TS 101 331 V1.2.1. Requirements of Llaw Enforcement Agencies [S]. 2006.

[6] ETSI TR 102 528 V1.1.1. Interception Domain Architecture for IP networks [S]. 2006.

[7] **杨雁飞. 一种监听方法和监听数据收集设备及系统: 中国**, CN1937545A [P]. 2007–03–28.

[8] 3GPP TS 23.002 V7.1.0. Network Architecture [S]. 2006.

[9] 3GPP TS 23.228 V8.3.0. IP Multimedia Subsystem (IMS); Stage 2 [S]. 2007.

[10] 3GPP TS 29.228 V7.2.0. IP Multimedia (IM) Subsystem Cx and Dx Interfaces; Signalling Flows and Message Contents [S]. 2006.

[11] 3GPP TS 24.229 V8.2.0. Internet Protocol (IP) Multimedia Call Control Protocol Based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3 [S]. 2007.

Biographies

Zhang Lu

Zhang Lu obtained his master's degree from Nanjing University of Aeronautics and Astronautics and is now a system engineer in Central R&D Institute of ZTE Corporation, engaged in IMS research. Up to now, he has applied for several patents and published over 20 proposals and papers.

Kong Min

Kong Min got his master's degree from Southeast University. Now he is an engineer in Central R&D Institute of ZTE Corporation, mainly engaged in research and development of access control devices for IMS and Softswitch network.