International Journal of Security and Its Applications
Vol.9, No.1 (2015), pp.337-346
http://dx.doi.org/10.14257/ijsia.2015.9.1.32

A Novel Method of Protection of Monitor Link

Guo Hong-tao

North China University of Water Resources and Electric Power,
Zhengzhou, Henan, 450045, China
67416809@qq.com

Abstract

Automation control systems demand high availability by providing its' users with reliable and uninterrupted service. Traditional monitor system fails to provide reliable service due to lack of protection of monitor link. It also requires TCP/IP, X.25, E1 and other interfaces to realize monitoring channels such as setting monitored object, reporting status information of monitored call, reporting voice data of monitored call. The organization of the system is very complicated. Besides, some old devices can't provide all the interfaces. Thus these old devices can't have access to the lawful interception system. This paper presents a method to provide the ability of monitor link protection under abnormal circumstance. This method offers complete monitor link protection with fewer interfaces. According to the result of experiment and practical application in many countries, the availability and reliability of the interception system have been greatly improved by using this method.

Key words: *system availability; Lawful Interception; Interception-link protection*

1. Introduction

To meet high availability requirements, Automation system should provide uninterrupted and reliable services to its users. In the communications field, because of its' real-time performance characteristics, communication systems require higher reliability. Especially in some important business applications, system availability requirements can reach 99.999%, or even higher. The research work about the reliability in communication systems began in the 60's [1-2].

To begin with we will provide a brief introduction of the lawful interception. Lawful interception (LI) is the legally sanctioned official access to private communications. According to legal authority, state security organs will require network operators or service providers to monitor the results of a specific target listener authority. In general, LI is a security process in which a network operator or service provider gives law enforcement officials access to the communications of private individuals or organizations. Monitor product is a kind of special communication products. Its reliability requirements are much higher than ordinary business products. Reliability of the monitor link is an important part of monitor system's reliability. Most of the time reliability of the monitor link is closely related to the national security.

Most police monitor interface specifications and standards do not involve the implementation of the monitor link protection under abnormal circumstances [3-6], including ETSI (European Telecommunications Standards Institute) standards. There is much old network equipment in the network system in the running state. Some old network equipment can't provide the monitoring function, and without monitor link protection function some network equipment can't provide the reliable monitoring service [7-8]. Considering the special nature and the importance of monitor system and interception-links, this paper proposes a novel method to solve the problem and improve the reliability and availability of the monitor system.

ISSN: 1738-9976 IJSIA

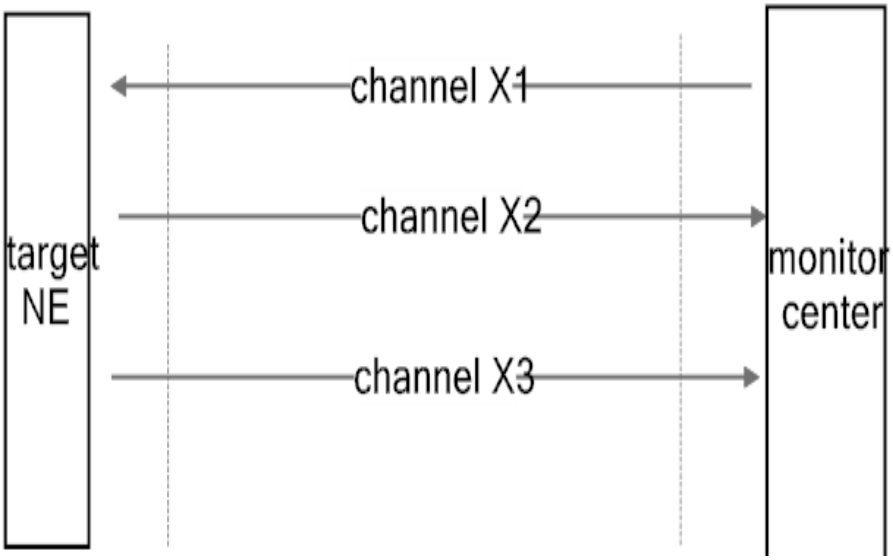

Figure 1. Architecture of the Traditional Monitor System

2. Analysis of Monitor System

2.1. Principle of Monitor System

The existing lawful interception technology usually copy user's voice from monitored target time slot exchange network, and transport the voice to the monitor center via a standard E1 [9-11]. The monitored target network elements can be fixed network elements or mobile network elements. The existing monitoring channel typically includes: X1(setting object to be monitored), X2(monitored call status reporting), X3(voice data of monitored call) [12-13].

The architecture of the traditional monitor system is showed in Figure 1. The chart consists of monitor center, the target NE (network element) and the E1 connection between monitor center and target NE. The contents of three monitor channel are transferred between the monitor center and the target network element through the E1. Channel X1 also can be called channel X1. Channel X2 also can be called channel X2. Channel X3 also can be called channel X3[14-15].

Channel X1 is designed to transfer the commands from monitor center to the target NE being monitored, and the response message transmitted from the target NE to the monitor center. The commands include the command to start the monitor system in the target monitored NE, the command to stop the monitor system; the command to add monitored user, the command to update monitored user info, the command to delete monitored user, and the command to request the info of monitored user.

Channel X2 is designed to transfer the real-time message about the monitored user from the monitored target NE to the monitor center, including (1) the information about the establishment of a call, the disconnection of a call; (2) the information about the location update of the monitored user; (3) short message sent or received by the monitored user.

Channel X3 is designed to transfer the real-time voice data of the monitored user during the user in a call session. Data in X3 will be transferred from the monitored target NE to the monitor center [16].

2.2. Monitor Link

The bearer link is the carrier to carry the logical information or the logical channel. There are many types of specific bearer link to carry the three monitor channel. Usually the information in channel X1 and X2 can be transferred via ITU-T X.25 or TCP/IP protocol, the information in channel X3 can be transferred via the standard El.

Therefor the link between the monitor center and the monitored target NE should support many interfaces, such as E1, X.25 and TCP/IP. Generally speaking monitor link is treated as a common communication link. And no special technology is applied to improve the reliability of the monitor link. Many old type network elements in running status support neither the interface of X.25 nor the TCP/IP interface. Therefore those NE can't provide the ability to transmit the information of channel X1, X2. System without channel X1 and X2 can't provide monitor service. Apparently this architecture can't meet the requirements of monitor system from the point of view of providing the ability of monitor and providing the reliability of the monitor system.

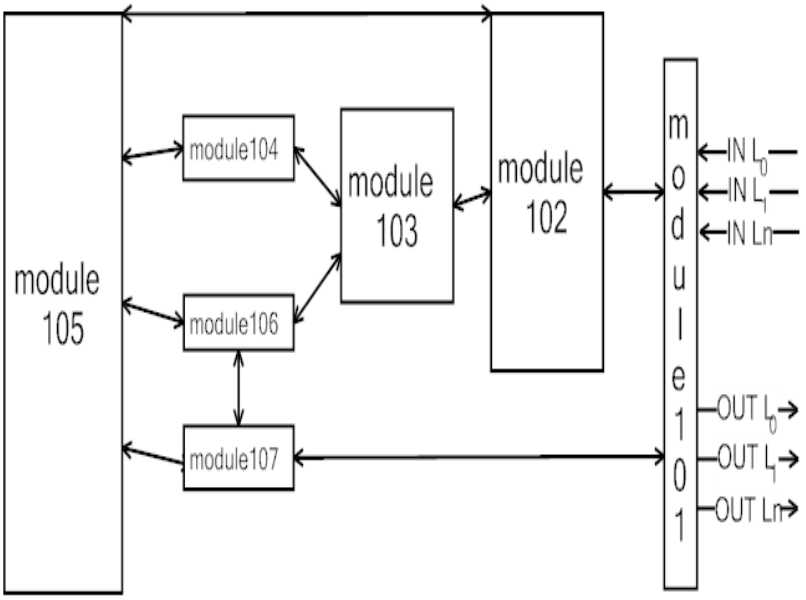

Figure 2. Logic Diagram of the Target NE being Monitored

To improve the reliability of the monitor system, in this paper, we focus on the need for monitor link protection. A novel method of monitor link protection is proposed. This method can simplify the monitor link interface and improve the reliability of monitor link.

3. Monitor Link Protection

3.1. The Overall Logical Framework

Figure 2 shows a logic diagram of the target NE being monitored. There are several modules in Figure 2, including: time slot multiplex module 101, monitor link control module 102, coding and decoding module 103, X1 channel message processing module 104, database module 105, call monitor module 106, call control module 107. The features of these modules are described below.

Function of time slot multiplex module 101 is to multiplex the content of X1, X2, X3 channel to time slots of the E1 specified when sending a message to the monitor center; to demultiplex each time slot content in E1 to a X1, X2, X3 channel when receiving messages from monitor center.

The function of monitor link control module 102 is to monitor the link status, and to notify the call monitor module 106 and database module 105 to switch the monitor link when the monitor link is detected abnormal or receive switchover command from monitor center.

Module 103 is designed to encrypt and code messages be send through channel X1 or channel X2, and to decode and decrypt messages received from channel X1 or channel X2.

X1 channel message processing module 104 is designed to execute the command received from channel X1.

Database module 105 is designed to store and manage user information to be monitored, and the monitor link resources used to finish the monitor. Provide the function to identify the user being monitored by matching the user number in a call session with the monitored user number stored in database. Database module 105 maintains a non-idle monitor link table and an idle monitor link table. A link is an idle link, if there is an idle time slot in the link. If a link has no idle time slot, then we can call the link a non- idle link. When the monitor system is started and initialized, all the time slots in system are idle slots, all the links are idle links. The monitor link is numbered from 0 to n, namely the links are L_0, L_1 ……L_n. The monitor system set the first link L_0 as the master link, and the others as the backup links. When a monitor time slot resource request is received, an idle time slot from the current master link will be assigned to the request, and mark the status of the slot as no-idle. If the time slot in current master link L_0 is used over, L_0 will be moved from idle link table to the no-idle table. And then the next link L_1 in the idle link table will be the current master link. So, L_2……Ln may be the current master link. At the end of a particular monitor call, the no-idle time slots will be freed, and its status will be changed to idle. When there is idle time slot in a no-idle link, the link will be move from no-idle link table to idle link table.

Call monitor module 106 is designed to process messages to be sent or received through X2 channel; and progress voice data to be sent through channel X3. In case of message of channel X2, module 106 sent a message indicating the calling status of the monitored users to the monitor center, after module 106 receive a call status updating message from the call control module 107. In case of message of channel X3, module 106 should provide the voice data of the monitored user's when the user is in a call session.

Module 107 is also can be called module call control. It is designed to control the progress of call session, and to monitor the call when either the caller number or the called number is found should be monitored based on match result given by the database module.

Exceptions with the monitor link can be found independently by the module 102 of the monitored NE. In case of monitor link under abnormal circumstances, module 102 can give the switchover command to the other modules. Switchover command can also be executed when the monitored NE receive a switchover command from monitor center. As a result the monitor link can be protected, and the reliability of the monitor system can be improved.

3.2. Monitor Network Structure

As shown in Figure 3, there are n (n>=2) physical links of E1 between the monitor center and the target monitored NE. In Figure 3, $Link_0$, $Link_1$…$Link_n$ stand for n logical links contained by E1 between the target monitored NE and the monitor center respectively. There are 30 TSes (time slots) that can be selected from E1 for us to use: $TS_{1\text{-}15}$, $TS_{17\text{-}31}$. Each time slot will be a logical link. Among these 30 ts, two time slot TS_i, TS_j ($i \neq j$) are chosen to transfer the message from channel X1 and channel X2. The other 28 time slots in E1 can be used to transfer the voice data from channel X3.

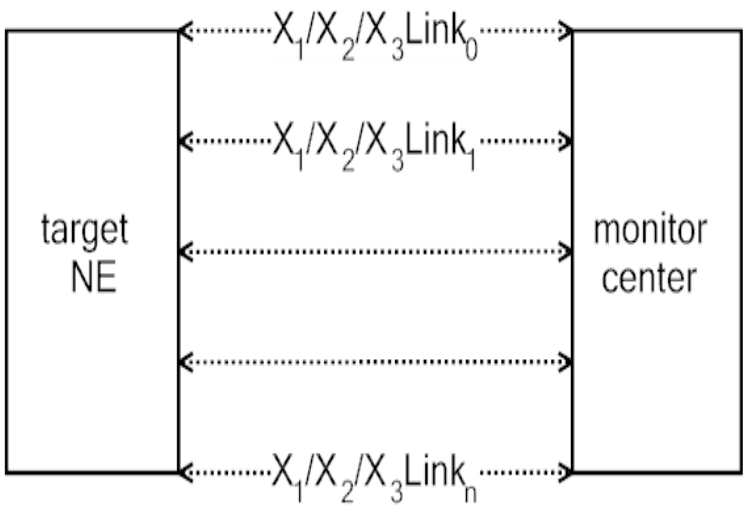

Figure 3. The Architecture of the Novel Monitor System

So messages from channel X1 and X2 and X3 can be transferred by the physical link of E1. Old network element even without interface TCP/IP and channel X.25 can also have access monitoring network.

3.3. Monitor Link Protection

The working principle of this system is as follows:

First the module 101 in the monitored target network element extracts the messages of channel X1 and X2 coming from time slot TS_i and TS_j in the E1 connecting to the monitor center. The messages of channel X1 and channel X2 are transferred through the module 102 to module 103. Module 103 will decode and decrypt the messages, and then transfer the message "$msgX1_1$" of channel X1 to module 104, and transfer the message "msgX2" of channel X2 to module 106.

To exclude uncertainties like network error and system attacks, after X1 processing module 104 receives the message "$msgX1_1$", it will judge the consistency of the message firstly. If the consistency check passes, X1 processing module 104 will send a message "msgDb1" to database module 105. If the message "$msgX1_1$" is a message to setup the information about the user to be monitored, the message "msgDb1" is to ask the module 105 to update the information about the user to be monitored. If the message "$msgX1_1$" is a message to query the information about the user being monitored, then the message "msgDb1" should be a message to query the information about the monitored user stored in the database module 105.

The database module 105 sets or queries the information about the monitored user according to the message "msgDb1", and then returns the processing results to X1 processing module 104. Module 104 sends the results to module 103, and module 103 will code and encrypt the results. The encrypted result message including information needed by channel X1 message will be transferred to monitor link control module 102. Module 102 request the time slot TS_i of current master link, and then send the channel X1 message to module 101 asking module 101 to send the channel X1 message to the monitor center through the master link.

After call monitor module 106 receives the X2 message sent by the codec module 103, it will process differently depending on the different message:

For message to inquire the call status of the monitored user, module 106 send the call status message of the monitored user to the codec module 103. To construct the call status message, firstly module 106 should get the attribute of the monitored user by sending a

request to database module 105. And then based on the response message from module 105 and the monitor call data area of module 106 the call, the call status message can be constructed. After codec module 103 codes and encrypts the call status message, the message is sent to the module 102. Module 102 will request the time slot TS_j of master link from database module 105, and then send the channel X2 message to module 101 asking module 101 to send the message to the monitor center throuth the master link.

If the message is switchover monitor link message, the message containing the CALLID of the monitored call should be switched over and the identifier of the monitor link which should be disconnected. CALLID represent the identifier of a distinguish call. After module 106 receive the switchover message. Module 106 should request the call control module 107 to disconnect the current monitor link, and then request the database module 105 to release the resources used by the monitored call. Module 105 will choose a new master link from the backup link group to replace the current master link and allocate a new time slot from the new master link. Module 106 will request module 107 to establish a new monitored call with the time slot allocated by module 105. The voice data of the new monitored call will be the content of the channel X3 message after being switched over. So module 107 will ask module 101 to send the message of new channel X3 through the new master link.

Generally a monitor call will be established by module 107 only when one of the users in call is a monitored user. So the number of the caller and called will be compared to the number of the monitored user by module 105 to make sure the call should be monitored. If the call should be monitored, module 105 will inform call control module 107 with the information “MONID” and “CALLID”. “MONID” is the unique identifier of the monitored user in database. “CALLID” is the unique identifier of the call. And module 107 will inform module 106 that a monitored user is in a call session to trigger the monitor to the call.

After the call monitor module 106 is informed, the call should be monitored, and module 106 will request module 105 for the resource “MTS1” to be used in the monitor process. “MTS1” stands for the monitor time slot in the monitor trunk. “MTK1” stands for the monitor trunk allocated to the new monitor call. A monitor trunk is a physical monitor link. After “MTS1” is allocated, module 106 will request module 107 to establish a monitor call connected to the monitored call. The voice data of monitored call will be the content of the message transferred in channel X3. And then module 107 will request module 101 send message in channel X3 to the monitor center, and module 107 will also inform module 106 to transfer the call status message “$MX2_1$” to the monitor center by module 101. The information about “MONID” “CALLID”, “MTK1” and “MTS1” will be included in the message “$MX2_1$”. So the monitor center can extract the corresponding voice data from monitor trunk.

On the monitor center side message of channel X1 X2 X3 can be obtained from the incoming E1 linking to the monitored network element. The time slot information of the voice data about the specific monitored call can be extracted from message of channel X2. So the voice data in channel X3 can be decoded from the trunk.

Abnormal link status can be detected in the target monitored NE side. The process to detect abnormal link and the steps for link switching are as follows:

When the monitor system is booting, module 102 will inform module 105 to choose a master monitor link. Generally the first link L_0 will be the master link. And the other links (L_1……L_n) will be the backup links. And then module 102 will send handshake messages to the monitor center periodically through the master link to detect the fault in the master link. If there is something wrong with the handshake message, there must be something wrong with the master link. Then module 102 will inform module 105 that the master link is down.

After module 105 gets the message that the master link is down. Module 105 mark the current mater link as unavailable, and then choose a new master link, according to the

order L_0->L_1->⋯. L_n->⋯->L_1-> L_0. Then 105 send a switchover message to monitor link control module 102, X1 processing module 104, and the call monitor module 106 module. As a result the master link switchover occurs.

4. Improved Results

This method has been verified using C language under VxWorks operation system. The method can be tested according to the architecture of the test system depicted in Figure 4.

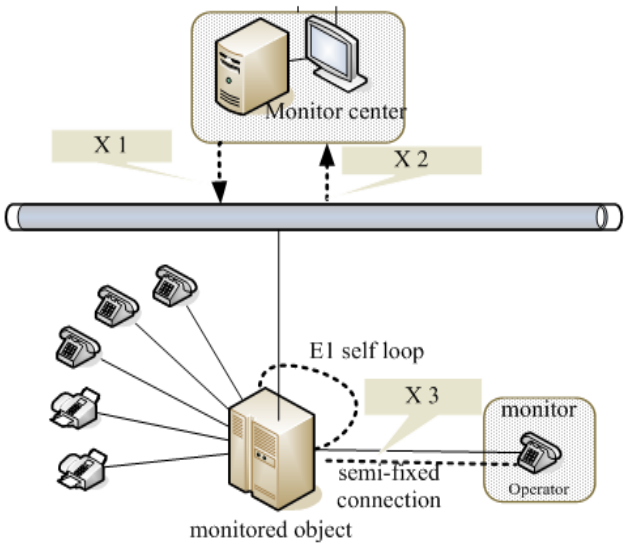

Figure 4. Architecture of the Test System

Services can be simulated by E1 loop in the target monitored NE, such as a basic call. Messages in channel X1 and channel X2 can be packaged into the message transfer between the console computer and the target monitored NE. The voice data in channel X3 can be obtained by establishing a semi-permanent connection between the monitored call and the monitor operator.

Experiment result is depicted in Figure 5. When the current master monitor link is abnormal, system using the method proposed in this paper can detect this abnormal situation and switch the current master monitor link to an available link. In Figure 5, the difference between before and after switching is marked out using circle, and the switchover alarm message is also marked with underline.

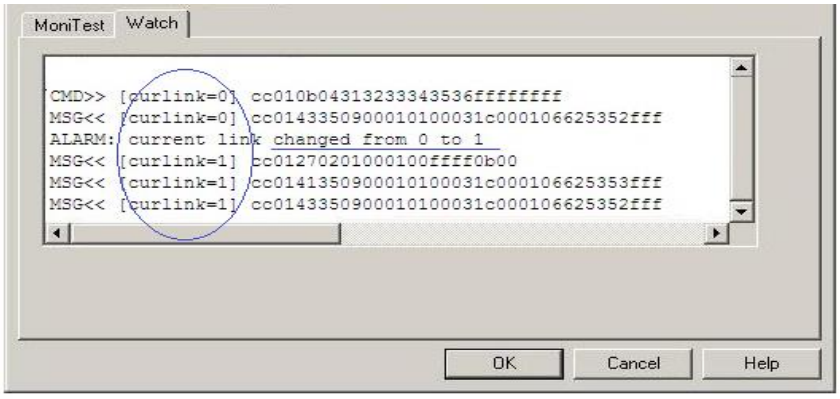

Figure 5. Experiment Result

The improved method has been in large-scale business use in police equipment of many countries and regions. The system has satisfied all the requirements.

According to the theoretical analysis, experiment result, and effect of the large-scale business use, it can be concluded that this method has the following advantages:

(1) By using monitor link backup and switchover, when the monitor link is under abnormal conditions the monitored network can switch the monitor link actively or passively. So this method can improve the reliability of the monitor system.

(2) Multiplexing the content channel X1, X2, X3 into the same physical link, thus a lot of old NEs running in the current network can provide the ability to be monitored as new NEs.

(3) switching the non-master monitor link and master monitor link, so the backup links share the running pressure, and improve the capacity of the target monitored network elements.

Therefore, load of monitor network elements can be shared evenly by using this approach, improving the reliability and the capacity of the monitor system.

5. Conclusions

We have demonstrated in this paper the common logical architecture of a monitor system, and the novel architecture of a target monitored network element on the basis of the comparative analysis the difference between the old monitor method and the novel monitor method. Through the experiment, the following conclusion can be made: the novel method can simplify the interface of the monitor system; the novel method can improve the reliability of the monitor under abnormal conditions for the old target monitored network elements by multiplexing message of channel X1 X2 X3 into the E1 link, and improve the processing capacity of the monitor link by switching the master link. Besides, the novel method of monitor link protection has been applied to the network elements running in the existing network. And good results have been achieved by using the novel method proposed in this paper.

Acknowledgements

This work was supported by the National High-Tech Research and Development Program of China (863 Program) under grant No 2011AA01A104 and Key Science and Technology Program of He'nan Province of China under grant No 132102210044. It was also supported by Foundation of He'nan Educational Committee under grant No 14A520010.

References

[1] H.-p. Hu, H.-q. Cao and W. Wang, "Survey of Modeling and Evaluating Telecommunications Network Reliability", COMPUTER ENGINEERING & SCIENCE, vol. 23, no. 5, (**2001**), pp. 97-101.
[2] CN-YD.900/1800MHz TDMA Digital cellular mobile communication system for police use Interface Specification, (**2002**).
[3] ETSI TR 101 943. Ver.2.2.1 Lawful Interception (LI); Concepts of Interception in a Generic Network Architecture, (**2006**).
[4] X.-y. Xu, Y.-l. Zheng and Z. Xu, "Lawful Interception for Circuit Switched Services in 3rd Generation Mobile Communications System", Telecommunications Science, vol. 26, no. 11A, (**2010**), pp. 171-175.
[5] L. Byeong-Choon and S. Seung-Jung, "The study of privacy security in mobile traffic control environment", International Journal of Security and its Applications, vol. 8, no. 2, (**2014**), pp. 173-182.
[6] M. Yang and H. Liu, "Implementation and performance of VoIP interception based on SIP session border controller", Telecommunication Systems, vol. 55, no. 3, (**2014**), pp. 345-361.
[7] ETSI TS 101 331 Ver. 1.4.1, Lawful Interception (LI); Requirements of Law Enforcement Agencies, (**2014**).
[8] ETSI TS 102 232-6 Ver. 3.3.1, Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 6, Service-specific details for PSTN/ISDN services, (**2014**).

[9] TR 101 943 Ver. 2.2.1, Lawful Interception (LI); Concepts of Interception in a Generic Network Architecture, (**2012**).
[10] ETSI TS 133 107 Ver. 11.4.0, Universal Mobile Telecommunications System (UMTS); LTE;3G security; Lawful interception architecture and functions(3GPP TS 33.107 version 11.4.0 Release 11), (**2014**).
[11] ETSI TS 103 221, Lawful Interception (LI) Internal Network Interfaces for Lawful, (**2013).**
[12] ETSI TR 102 519 Ver. 1.2.1, Lawful Interception (LI);Lawful Interception of public Wireless LAN Internet Access. (2014)
[13] ETSI TS 101 331 Ver. 1.4.1, Lawful Interception (LI); Requirements of Law Enforcement Agencies, (**2014**).
[14] ETSI TS 101 158 Ver. 1.3.1, Telecommunications security; Lawful Interception (LI);Requirements for network functions, (**2014**).
[15] ETSI TS 101 671. V3.2.1 Handover Interface for the Lawful Interception of Telecommunications Traffic, (**2007**).
[16] ETSI TS 101 671. Ver. 3.12.1, Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic, (**2013**).

