(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 October 2013 (03.10.2013)

WIPO | PCT

(10) International Publication Number
WO 2013/144669 A1

(51) International Patent Classification:
H04M 3/22 (2006.01)

(21) International Application Number:
PCT/IB2012/000646

(22) International Filing Date:
30 March 2012 (30.03.2012)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **WIPRO LIMITED** [IN/IN]; Doddakannelli, Sarjapur Road, Bangalore 560 035 (IN).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **JAYARAMAN, Venkata Subramanian** [IN/IN]; No. 41, Venkateswara Colony, 10th Street, M.M.C, 600051 Chennai, TamilNadu (IN).

(74) Agent: **ALANKI, N. V. Pradeep Kumar**; Global IP Services, 198F, 27th Cross, 3rd Block, Jayanagar, 03062 Bangalore, Karnataka (IN).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *of inventorship (Rule 4.17(iv))*

Published:

— *with international search report (Art. 21(3))*

(54) Title: SYSTEM AND METHOD FOR LAWFUL INTERCEPTION IN VOICE CALL CONTINUITY FOR TELECOMMUNICATION NETWORKS

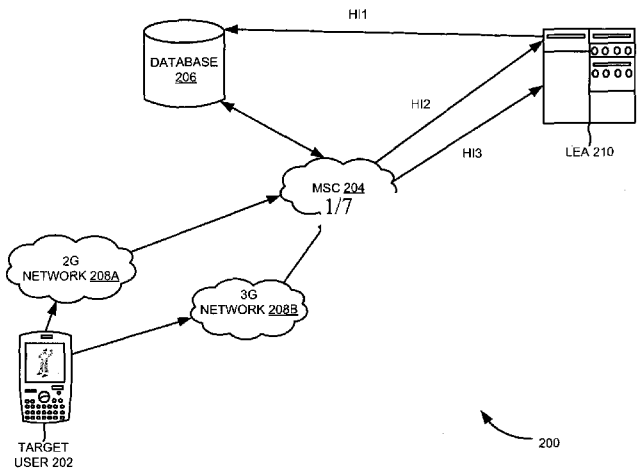

FIG. 2

(57) Abstract: A system and method for providing lawful interception (LI) data in voice calf continuity for telecommunication networks are disclosed. In one embodiment, the data associated with a registered telecommunication network user (i.e target user) coming from a first telecommunication network is intercepted by a VCC gateway. Further, the Intercepted data is sent to the LEA in a format desired by the LEA. Furthermore, the VCC getaway is configured based on a successful determination of network properties associated with the second telecommunication network upon the target user moving to the second telecommunication network. The second telecommunication network Is based on a technology that Is different from the first telecommunication network. In addition, the data associated with the target user coming from the second telecommunication network is continuously intercepted by the VCC gateway and continuously sent to the LEA by the VCC gateway in the format desired by the LEA.

WO 2013/144669 A1

SYSTEM AND METHOD FOR LAWFUL INTERCEPTION IN VOICE CALL CONTINUITY FOR TELECOMMUNICATION NETWORKS

BACKGROUND

[0001] Even with the advancement of telecommunication networks towards long term evolution (LTE) and other such advanced technologies, there is still a requirement for maintaining call continuity across various networks. Further, the term "network convergence" is becoming very popular in the advanced telecommunication networks. Furthermore, the concept of "voice call continuity" (VCC) is starting to emerge from a cell-to-cell movement towards a network-to-network movement. The VCC requires maintaining a voice call during the network-to-network movement when the telecommunication networks are based on various technologies. For example, the VCC requires seamlessly maintaining a voice call when a user/subscriber moves from one telecommunication network that is based on one technology, for example, a second generation (2G) network or a WiMax based network to another telecommunication network that is based on another technology, for example, a third generation (3G) network or a Wi-Fi based network.

[0002] Based on existing technologies, in the above-described scenario, if a user/subscriber moves from one network to another network and the user is lawfully intercepted by a law enforcement agency (LEA), such a lawfully intercepted call cannot be re-established and maintained in the network-to-network movement during the entire

period without the user knowing it. This is because the infrastructure needed for doing lawful interception of a call is not unified and varies based on different technologies and the real-time communication may go from circuit switching to packet based switching. Further, the telecommunication networks based on different technologies operate under different frequency ranges. Furthermore, the interface protocols needed between telecommunication networks based on different technologies and mobile stations operate under different standards. Typically in such a scenario, the call may either get dropped or the LEA may be unable to continue the lawful interception of the call. In both the scenarios, the LEA can lose the needed important data/voice associated with the conversation of the lawfully intercepted user/subscriber.

SUMMARY

[0003] A system and method for lawful interception (LI) in voice call continuity (VCC) for telecommunication networks is disclosed. According to one aspect of the present subject matter, data associated with a registered telecommunication network user coming from a first telecommunication network is intercepted by a VCC gateway upon a successful detection/authentication by the law enforcement agency (LEA).

[0004] In one example embodiment, intercepting the data associated with the registered telecommunication network user coming from the first telecommunication network includes detecting the data associated with the registered telecommunication network user coming from the first telecommunication network by the VCC gateway, authenticating the registered telecommunication network user by an LI gateway via the VCC gateway, and duplicating the data associated with the registered telecommunication network user upon a successful authentication.

[0005] Further, the intercepted data is sent to the LEA by the VCC gateway in a format desired by the LEA. In one embodiment, sending the intercepted data to the LEA includes sending the duplicated data associated with the registered telecommunication network user to the LEA by the VCC gateway in a format desired by the LEA.

[0006] Now consider that the registered telecommunication network user moves to a second telecommunication network. In one embodiment, the second telecommunication network is based on a technology that is different from the first telecommunication network. In one example embodiment, the first telecommunication

network and the second telecommunication network are technologies selected from the group consisting of 2G network, 3G network, VOIP networks. Wi-Fi network, and WiMax. For example, when the first telecommunication is a GSM network, then the second telecommunication network can be one of the Wi-Fi network and WiMax network.

[0007] In one embodiment, the VCC gateway determines network properties associated with the second telecommunication network using a VCC backend upon the registered telecommunication network user moves to the second telecommunication network. In this case, the movement of the user from the first telecommunication network to the second telecommunication network is detected by using the VCC backend and the corresponding co-ordinates (i.e., X, Y, Z co-ordinates) of the registered telecommunication network user.

[0008] Furthermore, the VCC gateway is configured based on a successful determination of the network properties associated with the second telecommunication network upon the registered telecommunication network user moving to the second telecommunication network. Also, intercepting the data associated with the registered telecommunication network user coming from the second telecommunication network is continued by the VCC gateway upon configuring the VCC gateway based on the network properties associated with the second telecommunication network.

[0009] In one example embodiment, continue intercepting the data coming from the second telecommunication network includes duplicating the data associated with the

registered telecommunication network user coming from the second telecommunication network by the VCC gateway upon configuring the VCC gateway based on the network properties associated with the second telecommunication network. In one embodiment, the data associated with the registered telecommunication network user coming from the second telecommunication network is duplicated towards the LEA even if the registered telecommunication network user moves from the first telecommunication network to the second telecommunication network.

[0010] In addition, sending the intercepted data coming from the second telecommunication network to the LEA is continued by the VCC gateway in the format desired by the LEA. In one embodiment, continue sending the intercepted data coming from the second telecommunication network to the LEA includes continue sending the duplicated data coming from the second telecommunication network to the LEA by the VCC gateway in the format desired by the LEA.

[0011] According to another aspect of the present subject matter, a non-transitory computer-readable storage medium for providing lawful interception (LI) data in voice call continuity (VCC) in telecommunication networks having instructions that, when executed by a computing device cause the computing device to perform the above described method.

[0012] According to yet another aspect of the present subject matter, a system for providing lawful interception (LI) data in voice call continuity (VCC) in telecommunication networks includes a first telecommunication network, a second

telecommunication network that is based on a technology different from that of the first telecommunication network, a LI gateway, and a VCC gateway coupled to the first telecommunication network, the second telecommunication network, and the LI gateway. Further, the VCC gateway includes a VCC server to perform the above described method.

BRIEF DESCRIPTION OF THE DRAWINGS

[0013] Various embodiments are described herein with reference to the drawings, wherein:

[0014] FIG. 1 is a block diagram illustrating providing lawful intercepted (LI) data in a VOIP/Wi-Fi network movement scenario;

[0015] FIG. 2 is a block diagram illustrating providing LI data in a GSM network (e.g., 2G or 3G telecommunication network) movement scenario;

[0016] FIG. 3 a block diagram illustrating of a voice call continuity (VCC) being carried in a network-to-network movement environment, in the context of the invention;

[0017] FIG. 4 is a block diagram illustrating providing LI data in a VCC in a Wi-Fi/VOIP network to GSM network movement scenario, according to an embodiment of the invention;

[0018] FIG. 5 illustrates a flow diagram of a method for providing LI data in a VCC in telecommunication networks, according to one embodiment of the invention;

[0019] FIG. 6 is a sequence diagram illustrating sequential exchange of signals when providing the LI data in a VCC in a network-to-network movement scenario, according to another embodiment;

[0020] **FIG. 7** is an enhanced sequence diagram illustrating a process in the VCC back end when providing the LI data in the VCC in the network-to-network movement scenario, such as those shown in **FIG. 6**, according to one embodiment;

[0021] The drawings described herein are for illustration purposes only and are not intended to limit the scope of the present disclosure in any way.

DETAILED DESCRIPTION

[0022] A system and method for lawful interception (LI) in voice call continuity (VCC) for telecommunication networks is disclosed. In the following detailed description of the embodiments of the present subject matter, reference is made to the accompanying drawings that form a part hereof, and in which are shown by way of illustration specific embodiments in which the present subject matter may be practiced. These embodiments are described in sufficient detail to enable those skilled in the art to practice the present subject matter, and it is to be understood that other embodiments may be utilized and that changes may be made without departing from the scope of the present subject matter. The following detailed description is, therefore, not to be taken in a limiting sense, and the scope of the present subject matter is defined by the appended claims.

[0023] In the document, the terms "registered telecommunication network user" and "target user" are used interchangeably throughout the document. Further, the term "VCC" refers to voice call continuity which requires maintaining a voice call when a mobile terminal (e.g., a user) is moving from one cell to another. In this case, the another/neighboring cell can use the same technology or a different technology to the one the user has originated the call. For example, moving from a second generation (2G) to a third generation (3G) network (i.e., same technology scenario) or moving from a WiMax to a Wi-Fi network (i.e., different technology scenario) and so on.

[0024] Furthermore, the term Lawful interception (LI) refers to a legally sanctioned official access to private communications, such as telephone calls, e-mail messages, and the like. In general, LI is a security process in which a network operator or service provider gives law enforcement officials/law enforcement agencies (LEA) access to the communications of private individuals or organizations. The LEA often interacts with both network access (i.e., typically managed by a network access provider (AP), who's infrastructure relies on that of a network operator, such as an incumbent telecom operator, local cable TV service, or wireless services operator) and network services (such as E-mail, chat, and Wi-Fi) to intercept the target user's call.

[0025] Further, the terminology "Handover Interface 1 (HI1)" refers to an interface for administrative information. The HI1 transports all kinds of administrative information from/to the law enforcement agencies (LEA) and network operators (NOW). The HI1 port can be used for the transmission of the request to establish or to remove the interception action from the LEA to the NWO or service provider (SP). In case if the automatic transmission between the LEA and NWO/SP is not possible for some reasons, the HI1 port supports manual transmission (e.g., voice, fax, etc.) and not only focuses on automatic transmission from/to the law enforcement mediation function (LEMF) and the NWO/SP facility.

[0026] Further, the terminology "Handover Interface 2 (HI2)" refers to an interface for intercept related information (IRI). The HI2 transports all IRI. The HI2 interface is used to transmit information or data associated with the telecommunication services of the identified target user apparent to the network. The HI2 includes signaling information

used to establish the telecommunication service and to control its progress (e.g., target identification, identifications of the other party's communication, basic service used, direction of the call or the event, answer indication and/or release causes, time stamps, and the like). If available, further information such as supplementary service information or location information may be included.

[0027] For example, the IRI record type includes record type description, begin record at the first event of the call or service attempt, end record at the end of the call or service attempt, continue record at any time during the call or service attempt (e.g., in-call service activation/deactivation), report record if no call association is available (e.g. activation/deactivation of features, use of a non-call associated service).

[0028] Furthermore, the terminology "Handover Interface 3 (HI3)" refers to an interface for content of communication. The HI3 transports the content of the communication of the intercepted telecommunication service to the LEMF. The content of communication shall be presented as a transparent en-Clair copy of the information flow during an established, frequently bi-directional, communication of the interception subject. The HI3 may contain voice or data. The transmission media used to support the HI3 interface is usually associated with a telecommunications network or its access arrangements. In case of failures, the content of communication is lost. The network may not provide any recording functions.

[0029] **FIG. 1** is a block diagram 100 illustrating providing lawful intercepted data in a VOIP/Wi-Fi network movement scenario. Particularly, **FIG. 1** illustrates a target user 102

initiating a call with another user 104 in a VOIP/Wi-Fi network. A media gateway controller (MGC) 106 receives signaling information (e.g., dialed digits) from a media gateway and instructs the media gateway to alert the called party (i.e., the other user 104) to send and receive voice data. The communication protocols used between the MGC 106 and the media gateway include but not limited to gateway control protocol (H.248), media gateway control protocol (MGCP) or session initiation protocol (SIP) (i.e., 110A-B).

[0030] In the VOIP/Wi-Fi network, the target user is recognized from a database 108 via the MGC 106 when the target user 102 originates or terminates the call. Further, upon recognizing the target user 102, the target user's speech is tapped by a call duplication device 112 and a real-time transport protocol (RTP) is directly transferred to an LI gateway (LIG) 114 and from there to a LEA 116. In this case, the RTP streams are directly duplicated by the duplication device 112, which is external to the VOIP/Wi-Fi network and the duplicated packet is directly routed towards the LEA 116.

[0031] **FIG. 2** is a block diagram 200 illustrating providing lawful intercepted data in a GSM network (e.g., 2G telecommunication network 208A or 3G telecommunication network 208B) movement scenario. Particularly, **FIG. 2** illustrates a target user 202 initiating a call with another user in a GSM network.

[0032] In the GSM network (i.e., 2G telecommunication network 208A or 3G telecommunication network 208B), the target user 202 is recognized by a mobile switching center (MSC) 204 using a database 206 when the target user 202 originates

or terminates the call. Further, upon recognizing the target user 202, the target user's speech is transferred from an air interface to the MSC 204. Furthermore, the MSC 204 uses an internal duplication mechanism to convert the user's speech and transfers the converted user's speech to a LEA 210. This delivery mechanism is triggered via a normal #7 signaling link. Further, the interception center in the LEA 210 receives information of the call as a normal #7 signaling call with voice channels.

[0033] **FIG. 3** a block diagram 300 illustrating of a voice call continuity (VCC) being carried in a network-to-network movement environment, in the context of the invention. Particularly, **FIG. 3** illustrates a smart phone 302 (associated with a target user) seamlessly roaming between a Wi-Fi network 306 and a cellular network 312. Further, **FIG. 3** illustrates a modem 304 providing the Wi-Fi network 306 (such as VOIP network 306A) to the smart phone 302, a PC 308 and/or a voice over Internet protocol (VoIP) phone 310. Furthermore, the cellular network 312 includes global system for mobile communications (GSM) network 312A such as 2G or 3G network. The cellular network 312 can also include other networks such as code division multiple access (CDMA) network, advanced mobile phone system (AMPS) network, and so on.

[0034] In operation, **FIG. 3** illustrates a seamless roaming of the smart phone 302 between the Wi-Fi network 306 and the cellular network 312. In other words, network coverage is available for the smart phone 302 either by Wi-Fi network 306 or by cellular network 312 to ensure voice call continuity (VCC) in a network-to-network movement environment such as when the user moves from the Wi-Fi network 306 to cellular network 312 or vice versa.

[0035] For example, consider a basic call handling scenario in case of VCC. A target user (associated with the smart phone 302) initiates the call using a registered telecommunication network, for example GSM network 312A. Further, the call interception is started by the GSM network 312A via a mobile switching center (MSC). Furthermore, the MSC sends the intercepted information/data (i.e., speech content) directly to a law enforcement agency (LEA) which is explained in **FIG. 2**. The HI2 information is forwarded towards the LEA from a lawful interception management system (LIMS).

[0036] Now consider that the target user (e.g., associated with the smart phone 302) moves to the Wi-Fi network 306. In this case, the interception information from the GSM network 312A is not forwarded to the Wi-Fi network 306. Therefore, the interception call by the GSM network 312A is terminated abruptly and hence the intercepted information in the Wi-Fi network 306 cannot be sent any more towards the LEA. However, the target user call still continues in the Wi-Fi network 306.

[0037] With respect to **FIGS. 1-3**, the LI cannot be continued when the user moves from one network to another because of the following reasons:

1. The infrastructure for doing lawful interception (LI) is different in case of GSM and Wi-Fi networks. In GSM network, the mobile switching center is included for HI1 and the LEA 210 directly for HI2 and HI3. In case of GSM network, the MSC 204 uses an internal duplication mechanism to convert the user's speech and transfers the converted user's speech to

the LEA 210. In case of the Wi-Fi network, the LIG 114 and call duplication device 112 are situated in between the MGC 106 and the LEA 116. The conversion of the user's speech is done by the LEA. The call duplication device 112 is used for the duplication of data which is controlled by the MGC 106 and these packets are forwarded to LIG 114 and then to LEA 116.

   i. Identifying the lawful interception data is difficult as the target speech still remains in one location and not in both the GSM and Wi-Fi network databases.

2. The underlying technology for communication of the GSM network and Wi-Fi network is different. The GSM network is based on direct conversion of voice and then transfer it to #7 signaling signals and then send it to the LEA. In case of a Wi-Fi network, the packet communication is directly duplicated and duplicated packet is send towards the LEA.

   i. Since the infrastructure is not unified, it not possible to intercept the call continuously during switch over of a call from GSM to Wi-Fi or vice versa.

   ii. The LEA cannot decode both the data as the first part of the data might come as #7 signaling speech from the GSM and the second part would come as packetized data from the Wi-Fi network if the call is moving from GSM to Wi-Fi (integrity of data).

3. LEA does not have any intelligence to accept non standard information.

[0038] Therefore, there arises a need to maintain the tracking session across networks having different technologies and to share the complete tracking information among the LEA's of different networks.

[0039] **FIG. 4** is a block diagram 400 illustrating providing lawful interception (LI) data in VCC in a Wi-Fi/VOIP network to GSM network movement scenario, according to an embodiment of the invention. Particularly, **FIG. 4** illustrates a first telecommunication network (e.g., Wi-Fi/VOIP/IMS network 406), a second telecommunication network (e.g., GSM network 412), a LI gateway 410A associated with a law enforcement agency (LEA) 410, and a VCC gateway 408 coupled to the first telecommunication network 406, the second telecommunication network 412, and the LI gateway 410A. Also, **FIG. 4** illustrates another telecommunication network 404A (e.g., Wi-Fi/VOIP/IMS network) including a calling gateway 404B and a MGC 404C associated with a receiving user (i.e., other user 404). In one embodiment, the VCC gateway 408 connects itself to the target user 402 for the HI3 delivery.

[0040] Further, the first telecommunication network 406 includes a calling gateway 406A, a database 406B, a MGC 406C and a duplication gateway 406D. Furthermore, the second telecommunication network 406 includes a calling gateway 412A, a database 412B, a MSC 412C and a duplication gateway 412D. Also, the VCC gateway 408 includes a VCC server 408A and a VCC backend 408B.

[0041] In operation, the target user 402 originates a call to another subscriber 404 via Wi-Fi/VOIP/IMS network 406. In this case, the VCC gateway 408 is connected to the target user 402 via the first telecommunication network 406. In one embodiment, VCC is a feature which is marked in the profile of the user 402 (i.e., subscriber) that he can use the VCC. Further, if the user 402 is marked as the target user and if he originates or terminates the call, the VCC gateway 408 is activated.

[0042] When the target user 402 initiates a call, the VCC gateway 408A monitors the target user 402 continuously. Further, the VCC gateway 408 tunes itself to the HI3 delivery point and always consistently delivers the same intercepted data to the LEA 410 via the LI gateway 410A, for example, even when the target user 402 moves from Wi-Fi/VOIP/IMS network 406 to the GSM network 412 as shown in dotted lines. In this case, if the communication has started in the #7 signaling way then the same can be continued throughout the call in VCC.

[0043] In one example embodiment, during the course of this movement the target user 402 cannot feel that he is intercepted because the target user 402 does not feel the switch of technologies. The same is applicable for the LEA 410 because the LEA 410 also gets only a single output throughout the call. In one embodiment, the VCC gateway 408 includes the VCC server 408A and the VCC backend 408B to perform the method described below in **FIG. 5**.

[0044] **FIG. 5** illustrates a flow diagram 500 of a method for providing LI data in VCC in telecommunication networks by a VCC gateway (i.e., such as the VCC gateway 408 of

FIG. 4), according to one embodiment of the invention. At block 502, data associated with a registered telecommunication network user (hereinafter refers to as "the target user") coming from a first telecommunication network is intercepted by a VCC gateway upon a successful detection/authentication by a LEA.

[0045] For intercepting the data associated with the target user coming from a first telecommunication network, first the data associated with the target user coming from the first telecommunication network is detected. Further, the target user is authenticated by the LEA via a LI gateway. Then, the data associated with the target user is duplicated to the LEA upon a successful authentication.

[0046] At block 504, the intercepted data is sent to the LEA by the VCC gateway in a format desired by the LEA. For example, sending the intercepted data to the LEA includes sending the duplicated data associated with the target user to the LEA in a format desired by the LEA.

[0047] Now consider that the target user moves to a second telecommunication network. In one embodiment, the second telecommunication network is based on a technology that is different from the first telecommunication network. In one example embodiment, the first telecommunication network and the second telecommunication network are technologies selected from the group consisting of GSM network (i.e., 2G network, 3G network), VOIP network, Wi-Fi network, and WiMax. For example, when the first telecommunication is a GSM network, then the second telecommunication network can be one of the VOIP network, Wi-Fi network and WiMax network.

[0048] Further, the VCC gateway determines network properties associated with the second telecommunication network using a VCC backend upon the target user moves to the second telecommunication network. In this case, the movement of the target user from the first telecommunication network to the second telecommunication network is detected by using the VCC backend and the corresponding co-ordinates (i.e., X, Y, Z co-ordinates) of the location information of the target user.

[0049] At block 506, the VCC gateway is configured based on a successful determination of the network properties associated with the second telecommunication network when the target user moving to the second telecommunication network. At block 508, intercepting the data associated with the target user coming from the second telecommunication network is continued by the VCC gateway upon configuring itself (i.e., the VCC gateway) based on the network properties associated with the second telecommunication network.

[0050] For continuing intercepting the data coming from the second telecommunication network, the data associated with the target user coming from the second telecommunication network is duplicated by the VCC gateway. In one embodiment, the data associated with the target user coming from the second telecommunication network is duplicated towards the LEA when the target user moves from the first telecommunication network to the second telecommunication network.

[0051] At block 510, sending the intercepted data coming from the second telecommunication network to the LEA is continued by the VCC gateway in the format desired by the LEA. For continuing sending the intercepted data coming from the second telecommunication network to the LEA includes continuing sending the duplicated data coming from the second telecommunication network to the LEA by the VCC gateway in the format desired by the LEA, thereby sending single output to the LEA throughout the call.

[0052] **FIG. 6** is a sequence diagram 600 illustrating sequential exchange of signals when providing the LI data in VCC in a network-to-network movement scenario, according to another embodiment. As illustrated, the sequence diagram 600 includes a target user A 602, a first telecommunication network (herein after referred to as a network 1) 604, a LI database 606, a VCC server 608, a user B 610, HI3 delivery 612, a second telecommunication network (herein after referred to as a network 2) 614, a network 1 call duplication function (CDF) 616, a network 2 CDF 618, and a VCC backend 620.

[0053] In one embodiment, **FIG. 6** depicts the sequence diagram comprising a number of steps as may be performed during the LI in the VCC when the target user A 602 moves from one network 1 604 to the network 2 614. In one embodiment, the network 2 614 is based on a technology that is different from the network 1 604. For example, if network 1 604 includes a Wi-Fi network then the network 2 614 includes a GSM network, and so on.

[0054] In step 1, the target user A 602 initiates/originates a call with the user b 610 using the network 1 604. In step 2, a check is made to recognize/detect whether the target user A 602 is listed in the LI database 606 associated with the network 1 604 for lawful interception. In other words, the LI database 606 is checked to see whether the target user's call needs to be tracked. In step 3, if the target user A 602 matches for LI (i.e., i.e., the target user's identity matches with an identity in the LI database 606 for LI), then a new VCC server 608 is introduced for tracking the speech information (i.e., LI data) of the target user A 602 in step 4.

[0055] In step 5, the VCC server 608 contacts a duplication server 1 which duplicates the target user's speech using a call duplication function (CDF) 616 associated with the network 1 604. Upon a successful duplication of the target user's speech in step 6, the VCC server 608 allows the target user A 602 to contact the user B 610 in step 7. In step 8, the lawful interception data (i.e., HI3) in the network 1 604 is delivered to the LEA via the LI gateway.

[0056] In step 9, the target user A 602 moves from the network 1 604 to network 2 614 which is based on the technology that is different from the network 1 604. In step 10, the VCC server 608 sends movement request to the network 2 614. In one example embodiment, the VCC server 608 detects the movement of the target user A 602 from the network 1 604 to the network 2 614 using the VCC backend 620 and corresponding X, Y and z co-ordinates of the target user A 602. In step 11, the VCC server 608 determines and analyzes the network properties associated with the network 2 614 using the VCC backend 620 when the target user A 602 moves to the network 2 614.

[0057] In step 12, the result of analyzing the network properties associated with the network 2 614 is sent to the VCC server 608. In step 13, the VCC server 608 successfully authenticates the movement of the target user A 602 to the network 2 614. In step 14, the VCC server 608 contacts a duplication server 2 which duplicates the target user's speech using a CDF 618 associated with the network 2 614. Upon a successful duplication of the target user's speech in step 14, the duplication server 2 sends the response of the CFD 618 associated with the network 2 614 to the VCC server 608 in step 15. Further in step 16, the target user A 602's call continues to the user B 610 via the network 2 614. In step 17, delivering the lawful interception data (i.e., HI3) in the network 2 614 to the LEA via the LI gateway is continued.

[0058] In this way, the interception is taken care by the CDF (i.e., the CDF 616 and CDF 618) that is present in both the networks (i.e., the network 1 604 and the network 2 614 respectively) be it the #7 signaling conversion of direct duplication of the packet.

[0059] **FIG. 7** is an enhanced sequence diagram illustrating a process in the VCC back end when providing the LI data in the VCC in a network-to-network movement scenario, such as those shown in **FIG. 6**, according to one embodiment. As illustrated, the sequence diagram 700 includes the target user A 602, the first telecommunication network (herein after referred to as a network 1) 604, the LI database 606, the VCC server 608, the user B 610, the HI3 delivery 612, the second telecommunication network (herein after referred to as a network 2) 614, the network 1 call duplication

function (CDF) 616, the network 2 CDF 618, the VCC backend 620, and a VCC database 702.

[0060] In one embodiment, the VCC backend 620 refers to a network which includes a VCC database 702 and a control algorithm based on a location of a particular area (i.e., using X, Y, and Z coordinates) of what are all the available networks and their intercepting techniques. Based on the request for the movement, the VCC communicates to the VCC server 608 of what and where to route the new request so that the VCC-LI is not lost.

[0061] In step 1, the target user A 602 initiates/originates a call with the user b 610 using the network 1 604. In step 2, a check is made to recognize/detect whether the target user A 602 is listed in the LI database 606 associated with the network 1 604 for lawful interception. In other words, the LI database 606 is checked to see whether the target user's call needs to be tracked. In step 3, if the target user A 602 matches for LI (i.e., i.e., the target user's identity matches with an identity in the LI database 602 for LI), then a new VCC server 608 is introduced for tracking the speech information (i.e., LI data) of the target user A 602 in step 4.

[0062] In step 5, the VCC server 608 contacts the VCC backend 620 to check the ways of intercepting the target user's call. In step 6, the VCC backend 620 queries the VCC database 702 regarding the ways of intercepting the target user's call. In step 7, the VCC database 702 responds to the VCC backend 620 with the CDF 1 for intercepting

the target user's call. In step 8, the VCC backend 620 sends the result of the analysis (i.e., intercept using CDF 1) to the VCC server 608.

[0063] In step 9, the VCC server 608 contacts a duplication server 1 which duplicates the target user's speech using the CDF 1 616 associated with the network 1 604. Upon a successful duplication of the target user's speech in step 10, the VCC server 608 allows the target user A 602 to contact the user B 610 in step 11. In step 12, the lawful interception data (i.e., HI3) in the network 1 604 is delivered to the LEA via the LI gateway.

[0064] In step 13, the target user A 602 moves from the network 1 604 to network 2 614 which is based on a technology that is different from the network 1 604. In step 14, the VCC server 608 sends movement request to the network 2 614. In one example embodiment, the VCC server 608 detects the movement of the target user A 602 from the network 1 604 to the network 2 614 using the VCC backend 620 and corresponding X, Y and z co-ordinates of the target user A 602. In step 15, the VCC server 608 determines and analyzes the network properties associated with the network 2 614 using the VCC backend 620 when the target user A 602 moves to the network 2 614.

[0065] In step 16, the VCC backend 620 queries the VCC database 702 regarding the ways of intercepting the target user's call in the network 2 614. In step 17, the VCC database 702 responds to the VCC backend 620 with the CDF 2 for intercepting the target user's call.

[0066] In step 18, the result of analyzing the network properties associated with the network 2 614 is sent to the VCC server 608. In step 19, the VCC server 608 successfully authenticates the movement of the target user A 602 to the network 2 614. In step 20, the VCC server 608 contacts a duplication server 2 which duplicates the target user's speech using the CDF 618 associated with the network 2 614. Upon a successful duplication of the target user's speech in step 20, the duplication server 2 sends the response of the CFD 618 associated with the network 2 614 to the VCC server 608 in step 21. Further in step 22, the target user A 602's call continues to the user B 610 via the network 2 614. In step 23, delivering the LI data (i.e., HI3) in the network 2 614 to the LEA via the LI gateway is continued in the same format as that of the LI data sent from the network 1 604.

[0067] Therefore, the call setup is initiated from the target user A 602 is never lost and there is always continuous LI data delivery whereby LI is never lost. The VCC server 608 detects the movement of target user A 602 using the X, Y, Z co-ordinates that the target user A 602 moves and uses the same to identify which network the target user A 602 is going into.

[0068] The above described architecture is very easy to implement and can be adapted to any kind of network as there is no big change in the way the call handing is to happen and if done once then when new networks are added the same can be easily modified in the database. If there is a new network to be added then the same could be done easily by adding the new network configuration in the corresponding tables.

[0069] Further, the above technique described in **FIGS. 4-7** provides the VCC server that lies directly in the path of the target user and the other user, and receives all the corresponding information about the network which the target user moves from the VCC backend and hence addresses VCC in case of LI in any kind of network. Furthermore, the above technique described in **FIGS. 4-7** allows the target user to move between network and topologies as all information are fed and readily available for the VCC server from the VCC backend. Also, the above technique described in FIGS. 4-7 allows to place the new VCC server and the VCC backend as separate components in the network that take care of the CFD function of LI in case of VCC and hence there is no need to change the existing infrastructure. In this case, the VCC server and the VCC backend can be used to replicate the speech content of the target user and could provide the content to the LEA in the format required by the LEA without making any change in the network topology or architecture of the LEA.

[0070] An article comprising a non transitory computer readable storage medium having instructions thereon which when executed by a computer, cause the computer to perform the above described method. The method described in the foregoing may be in a form of a machine-readable medium embodying a set of instructions that, when executed by a machine, cause the machine to perform any method disclosed herein. It will be appreciated that the various embodiments discussed herein may not be the same embodiment, and may be grouped into various other embodiments not explicitly disclosed herein. For example, the VCC server may include a processor and a memory coupled to the processor. The memory includes the set of instruction for executing by the processor.

[0071] In addition, it will be appreciated that the various operations, processes, and methods disclosed herein may be embodied in a machine-readable medium and/or a machine accessible medium compatible with a data processing system (e.g., a computer system), and may be performed in any order (e.g., including using means for achieving the various operations). Accordingly, the specification and drawings are to be regarded in an illustrative rather than a restrictive sense.

[0072] In various embodiments, the above-described methods and systems of FIGS. 4 through 7 provides an easy to implement in the existing network topology and heterogeneous networks today, helps in preventing the LI call drop during VCC in a heterogeneous network, and also provides a smooth transfer and thus takes care of LI in case of VCC.

[0073] Further, the above-described methods can also be applicable for future network upgrades. Because once a new technology is introduced the VCC server and VCC backend can be adapted with the new technology by providing information about the new technology. The above-described methods provides a non intrusive solution because there is no change in packet header and no changes in the IP addresses and does not put any over head to the network and hence does not affect the performance of the network.

[0074] Although, the present embodiments have been described with reference to specific example embodiments, it will be evident that various modifications and changes may be made to these embodiments without departing from the broader spirit and scope of the various embodiments. Furthermore, the various devices, modules, analyzers, generators, and the like described herein may be enabled and operated using hardware circuitry, for example, complementary metal oxide semiconductor based logic circuitry, firmware, software and/or any combination of hardware, firmware, and/or software embodied in a machine readable medium. For example, the various electrical structure and methods may be embodied using transistors, logic gates, and electrical circuits, such as application specific integrated circuit.

CLAIMS

What is claimed is:

1. A method for providing lawful interception (LI) data in voice call continuity (VCC) in telecommunication networks, comprising:

intercepting data associated with a registered telecommunication network user coming from a first telecommunication network by a VCC gateway upon a successful detection/authentication by a law enforcement agency (LEA);

delivering the intercepted data to the LEA by the VCC gateway in a format desired by the LEA;

configuring the VCC gateway based on a successful determination of network properties associated with a second telecommunication network upon the registered telecommunication network user moving to the second telecommunication network, wherein the second telecommunication network is based on a technology that is different from the first telecommunication network;

continue intercepting the data associated with the registered telecommunication network user coming from the second telecommunication network by the VCC gateway upon configuring the VCC gateway based on the network properties associated with the second telecommunication network; and

continue sending the intercepted data coming from the second telecommunication network to the LEA by the VCC gateway in the format desired by the LEA.

2. The method of claim 1, wherein the first telecommunication network and the second telecommunication network are technologies selected from the group consisting of GSM networks, VOIP networks, Wi-Fi networks, and WiMax networks.

3. The method of claim 1, wherein configuring the VCC gateway based on the successful determination of network properties associated with the second telecommunication network, comprises:

detection of the movement of the registered telecommunication network user from the first telecommunication network to the second telecommunication network using a VCC backend and corresponding co-ordinates of the registered telecommunication network user;

determining the network properties associated with the second telecommunication network using the VCC backend by the VCC gateway upon the registered telecommunication network user moves to the second telecommunication network; and

configuring the VCC gateway based on a successful determination of the network properties associated with the second telecommunication network.

4. The method of claim 1, wherein intercepting the data associated with the registered telecommunication network user coming from the first telecommunication network by the VCC gateway upon the successful detection/authentication by the LEA comprises:

detection of the data associated with the registered telecommunication network user coming from the first telecommunication network by the VCC gateway;

authenticating the registered telecommunication network user by an LI gateway via the VCC gateway; and

duplicating the data associated with the registered telecommunication network user towards the LEA upon a successful authentication.

5. The method of claim 4, wherein sending the intercepted data to the LEA by the VCC gateway in the format desired by the LEA comprises:

sending the duplicated data associated with the registered telecommunication network user to the LEA by the VCC gateway in a format desired by the LEA.

6. The method of claim 4, wherein continue intercepting the data associated with the registered telecommunication network user coming from the second telecommunication network by the VCC gateway upon configuring the VCC gateway based on the network properties associated with the second telecommunication network, comprises:

duplicating the data associated with the registered telecommunication network user coming from the second telecommunication network by the VCC gateway upon configuring the VCC gateway based on the network properties associated with the second telecommunication network, wherein the data associated with the registered telecommunication network user coming from the second telecommunication network is duplicated towards the LEA when the registered telecommunication network user

moves from the first telecommunication network to the second telecommunication network.

7. The method of claim 6, wherein continue sending the intercepted data coming from the second telecommunication network to the LEA by the VCC gateway in the format desired by the LEA, comprises:

continue sending the duplicated data coming from the second telecommunication network to the LEA by the VCC gateway in the format desired by the LEA.

8. A non-transitory computer-readable storage medium for providing lawful interception (LI) data in voice call continuity (VCC) in telecommunication networks having instructions that, when executed by a computing device cause the computing device to:

intercept data associated with a registered telecommunication network user coming from a first telecommunication network by a VCC gateway upon a successful detection/authentication by a law enforcement agency (LEA);

deliver the intercepted data to the LEA by the VCC gateway in a format desired by the LEA;

configure the VCC gateway based on a successful determination of network properties associated with a second telecommunication network upon the registered telecommunication network user moving to the second telecommunication network, wherein the second telecommunication network is based on a technology that is different from the first telecommunication network;

continue intercepting the data associated with the registered telecommunication network user coming from the second telecommunication network by the VCC gateway upon configuring the VCC gateway based on the network properties associated with the second telecommunication network; and

continue sending the intercepted data coming from the second telecommunication network to the LEA by the VCC gateway in the format desired by the LEA.

9. The non-transitory computer-readable storage medium of claim 8, wherein the first telecommunication network and the second telecommunication network are technologies selected from the group consisting of GSM networks, VOIP networks, Wi-Fi networks, and WiMax networks.

10. The non-transitory computer-readable storage medium of claim 8, wherein configuring the VCC gateway based on the successful determination of network properties associated with the second telecommunication network, comprises:

detection of the movement of the registered telecommunication network user from the first telecommunication network to the second telecommunication network using a VCC backend and corresponding co-ordinates of the registered telecommunication network user;

determining the network properties associated with the second telecommunication network using the VCC backend by the VCC gateway upon the registered telecommunication network user moves to the second telecommunication network; and

configuring the VCC gateway based on a successful determination of the network properties associated with the second telecommunication network.

11. The non-transitory computer-readable storage medium of claim 8, wherein intercepting the data associated with the registered telecommunication network user coming from the first telecommunication network by the VCC gateway upon the successful detection/authentication by the LEA comprises:

detection of the data associated with the registered telecommunication network user coming from the first telecommunication network by the VCC gateway;

authenticating the registered telecommunication network user by an LI gateway via the VCC gateway; and

duplicating the data associated with the registered telecommunication network user upon a successful authentication.

12. The non-transitory computer-readable storage medium of claim 11, wherein sending the intercepted data to the LEA by the VCC gateway in the format desired by the LEA comprises:

sending the duplicated data associated with the registered telecommunication network user to the LEA by the VCC gateway in a format desired by the LEA.

13. The non-transitory computer-readable storage medium of claim 11, wherein continue intercepting the data associated with the registered telecommunication network user coming from the second telecommunication network by the VCC gateway upon

configuring the VCC gateway based on the network properties associated with the second telecommunication network, comprises:

duplicating the data associated with the registered telecommunication network user coming from the second telecommunication network by the VCC gateway upon configuring the VCC gateway based on the network properties associated with the second telecommunication network, wherein the data associated with the registered telecommunication network user coming from the second telecommunication network is duplicated towards the LEA when the registered telecommunication network user moves from the first telecommunication network to the second telecommunication network.

14. The non-transitory computer-readable storage medium of claim 13, wherein continue sending the intercepted data coming from the second telecommunication network to the LEA by the VCC gateway in the format desired by the LEA, comprises:

continue sending the duplicated data coming from the second telecommunication network to the LEA by the VCC gateway in the format desired by the LEA.

15. A system for providing lawful interception (LI) data in voice call continuity (VCC) in telecommunication networks, comprising:

a first telecommunication network;

a second telecommunication network that is based on a technology different from that of the first telecommunication network;

a LI gateway; and

a VCC gateway coupled to the first telecommunication network, the second telecommunication network, and the LI gateway, wherein the VCC gateway includes a VCC server to:

intercept data associated with a registered telecommunication network user coming from the first telecommunication network upon a successful detection/authentication by a law enforcement agency (LEA);

deliver the intercepted data to the LI gateway associated with the LEA in a format desired by the LEA;

configure the VCC gateway based on a successful determination of network properties associated with the second telecommunication network upon the registered telecommunication network user moving to the second telecommunication network;

continue intercepting the data associated with the registered telecommunication network user coming from the second telecommunication network upon configuring the VCC gateway based on the network properties associated with the second telecommunication network; and

continue sending the intercepted data coming from the second telecommunication network to the LI gateway associated with the LEA in the format desired by the LEA.

16. The system of claim 15, wherein the first telecommunication network and the second telecommunication network are technologies selected from the group consisting of GSM networks, VOIP networks, Wi-Fi networks, and WiMax networks.

17. The system of claim 15, wherein the VCC server detects movement of the registered telecommunication network user from the first telecommunication network to the second telecommunication network using a VCC backend and corresponding co-ordinates of the registered telecommunication network user, determines the network properties associated with the second telecommunication network using the VCC backend upon the registered telecommunication network user moves to the second telecommunication network, and configures the VCC gateway based on a successful determination of the network properties associated with the second telecommunication network.

18. The system of claim 15, wherein the VCC server detects the data associated with the registered telecommunication network user coming from the first telecommunication network, wherein the LI gateway authenticates the registered telecommunication network user via the VCC gateway, and wherein the VCC server duplicates the data associated with the registered telecommunication network user upon a successful authentication.

19. The system of claim 18, wherein the VCC server sends the duplicated data associated with the registered telecommunication network user to the LEA in a format desired by the LEA.

20. The system of claim 18, wherein the VCC server duplicates the data associated with the registered telecommunication network user coming from the second

telecommunication network upon configuring the VCC gateway based on the network properties associated with the second telecommunication network, wherein the data associated with the registered telecommunication network user coming from the second telecommunication network is duplicated towards the LEA when the registered telecommunication network user moves from the first telecommunication network to the second telecommunication network.

21. The system of claim 20, wherein the VCC server continues sending the duplicated data coming from the second telecommunication network to the LEA in the format desired by the LEA.

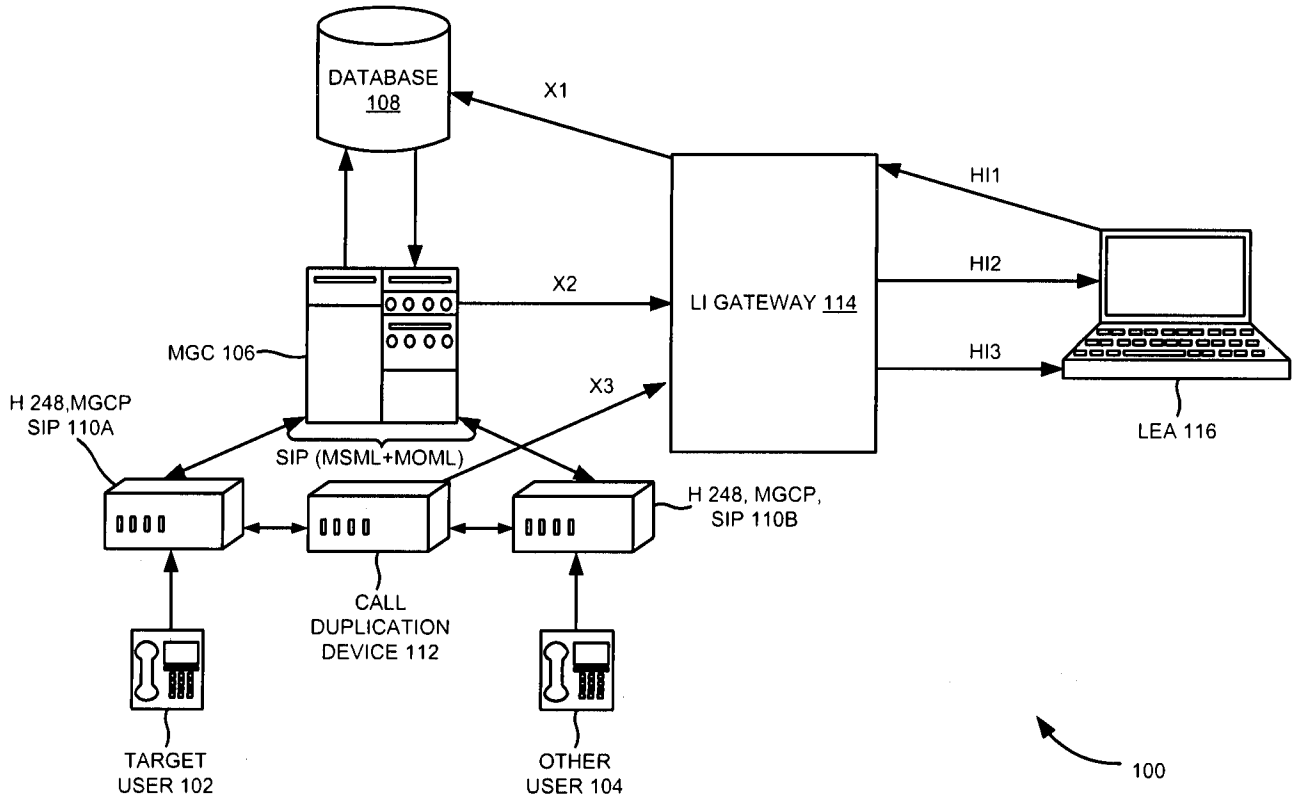
DATABASE
108
X1
HI1
HI2
HI3
X2
LI GATEWAY 114
MGC 106
X3
H 248,MGCP
SIP 110A
SIP (MSML+MOML)
LEA 116
H 248, MGCP,
SIP 110B
CALL
DUPLICATION
DEVICE 112
TARGET
USER 102
OTHER
USER 104
100

FIG. 1

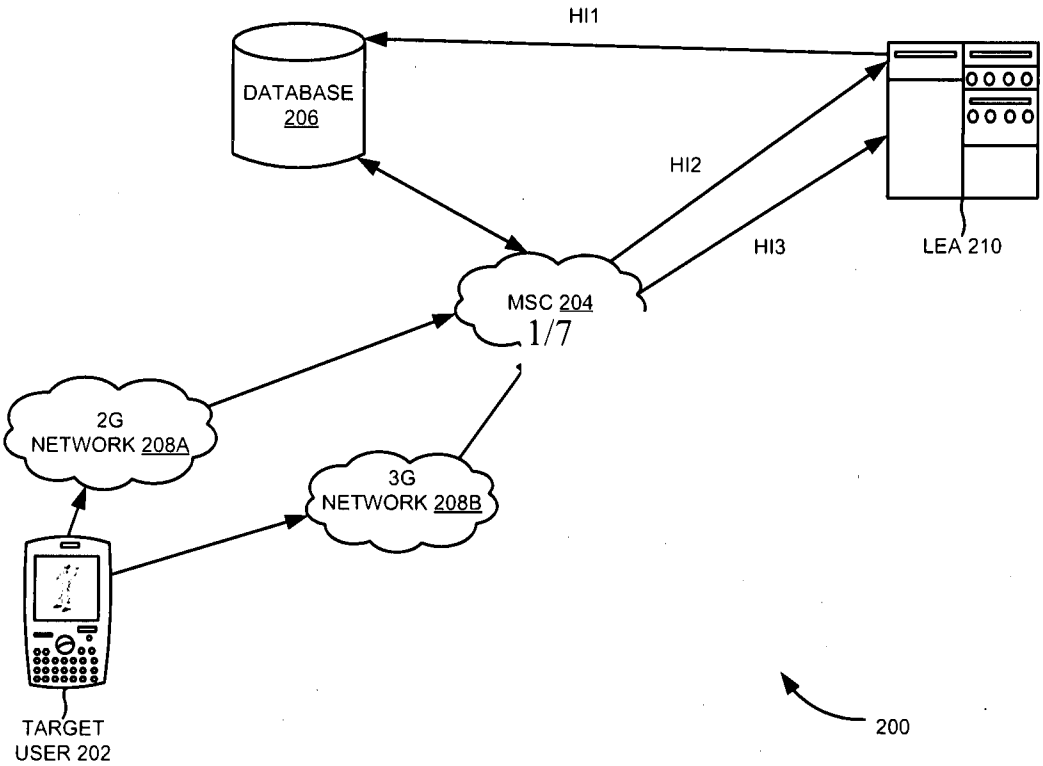
HI1
DATABASE
206
HI2
HI3
LEA 210
MSC 204
1/7
2G
NETWORK 208A
3G
NETWORK 208B
TARGET
USER 202
200

FIG. 2

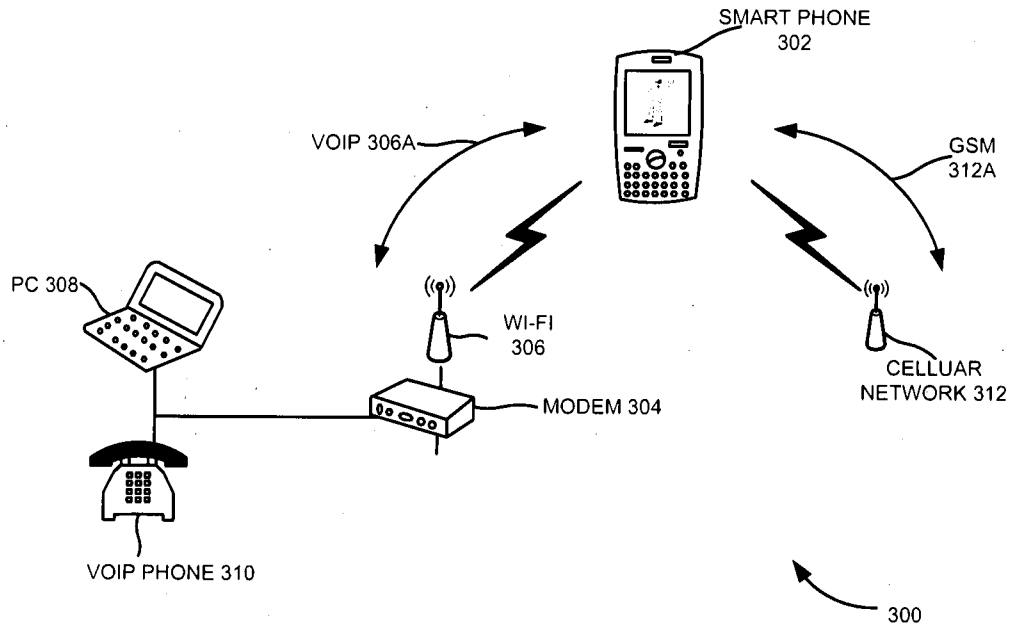
SMART PHONE
302
VOIP 306A
GSM
312A
PC 308
WI-FI
306
MODEM 304
CELLUAR
NETWORK 312
VOIP PHONE 310
300

FIG. 3

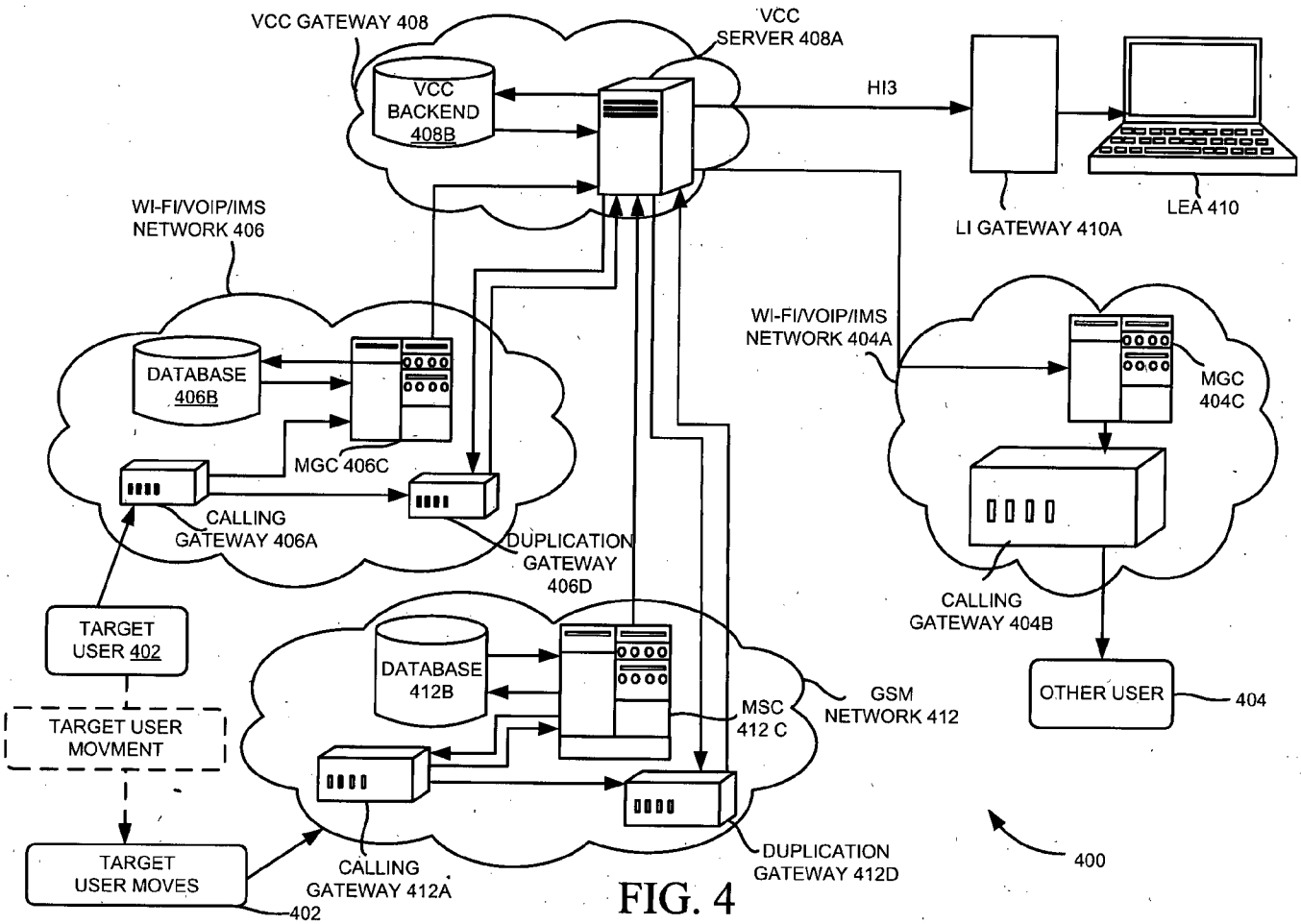
VCC GATEWAY 408
VCC SERVER 408A
VCC BACKEND 408B
HI3
LI GATEWAY 410A
LEA 410
WI-FI/VOIP/IMS NETWORK 406
DATABASE 406B
MGC 406C
CALLING GATEWAY 406A
DUPLICATION GATEWAY 406D
WI-FI/VOIP/IMS NETWORK 404A
MGC 404C
CALLING GATEWAY 404B
OTHER USER
404
TARGET USER 402
TARGET USER MOVMENT
TARGET USER MOVES
402
DATABASE 412B
MSC 412 C
GSM NETWORK 412
CALLING GATEWAY 412A
DUPLICATION GATEWAY 412D
400

FIG. 4

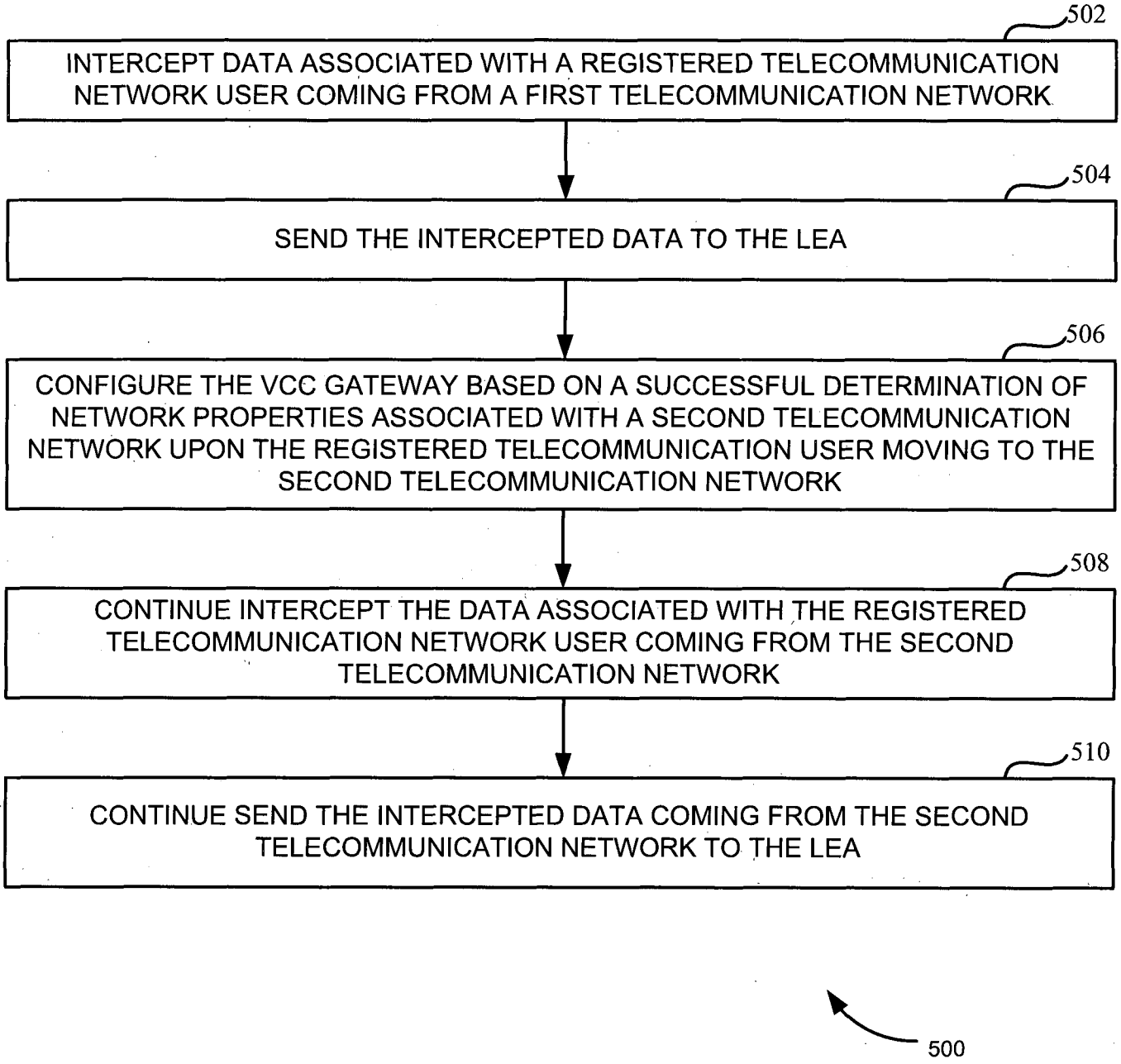
502
INTERCEPT DATA ASSOCIATED WITH A REGISTERED TELECOMMUNICATION NETWORK USER COMING FROM A FIRST TELECOMMUNICATION NETWORK
504
SEND THE INTERCEPTED DATA TO THE LEA
506
CONFIGURE THE VCC GATEWAY BASED ON A SUCCESSFUL DETERMINATION OF NETWORK PROPERTIES ASSOCIATED WITH A SECOND TELECOMMUNICATION NETWORK UPON THE REGISTERED TELECOMMUNICATION USER MOVING TO THE SECOND TELECOMMUNICATION NETWORK
508
CONTINUE INTERCEPT THE DATA ASSOCIATED WITH THE REGISTERED TELECOMMUNICATION NETWORK USER COMING FROM THE SECOND TELECOMMUNICATION NETWORK
510
CONTINUE SEND THE INTERCEPTED DATA COMING FROM THE SECOND TELECOMMUNICATION NETWORK TO THE LEA
500

FIG. 5

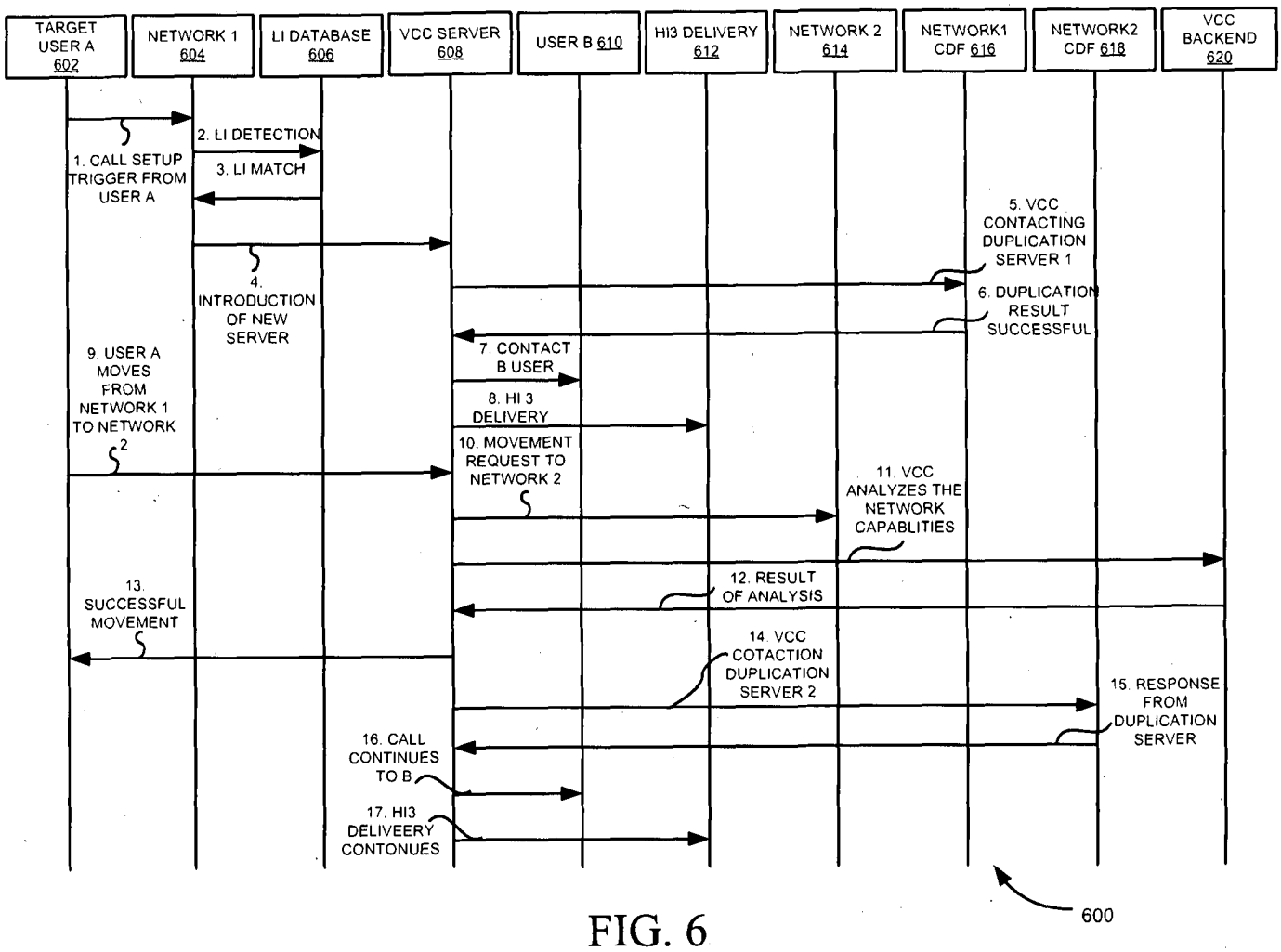
TARGET USER A 602
NETWORK 1 604
LI DATABASE 606
VCC SERVER 608
USER B 610
HI3 DELIVERY 612
NETWORK 2 614
NETWORK1 CDF 616
NETWORK2 CDF 618
VCC BACKEND 620
1. CALL SETUP TRIGGER FROM USER A
2. LI DETECTION
3. LI MATCH
4. INTRODUCTION OF NEW SERVER
5. VCC CONTACTING DUPLICATION SERVER 1
6. DUPLICATION RESULT SUCCESSFUL
7. CONTACT B USER
8. HI 3 DELIVERY
9. USER A MOVES FROM NETWORK 1 TO NETWORK 2
10. MOVEMENT REQUEST TO NETWORK 2
11. VCC ANALYZES THE NETWORK CAPABLITIES
12. RESULT OF ANALYSIS
13. SUCCESSFUL MOVEMENT
14. VCC COTACTION DUPLICATION SERVER 2
15. RESPONSE FROM DUPLICATION SERVER
16. CALL CONTINUES TO B
17. HI3 DELIVEERY CONTONUES
600

FIG. 6

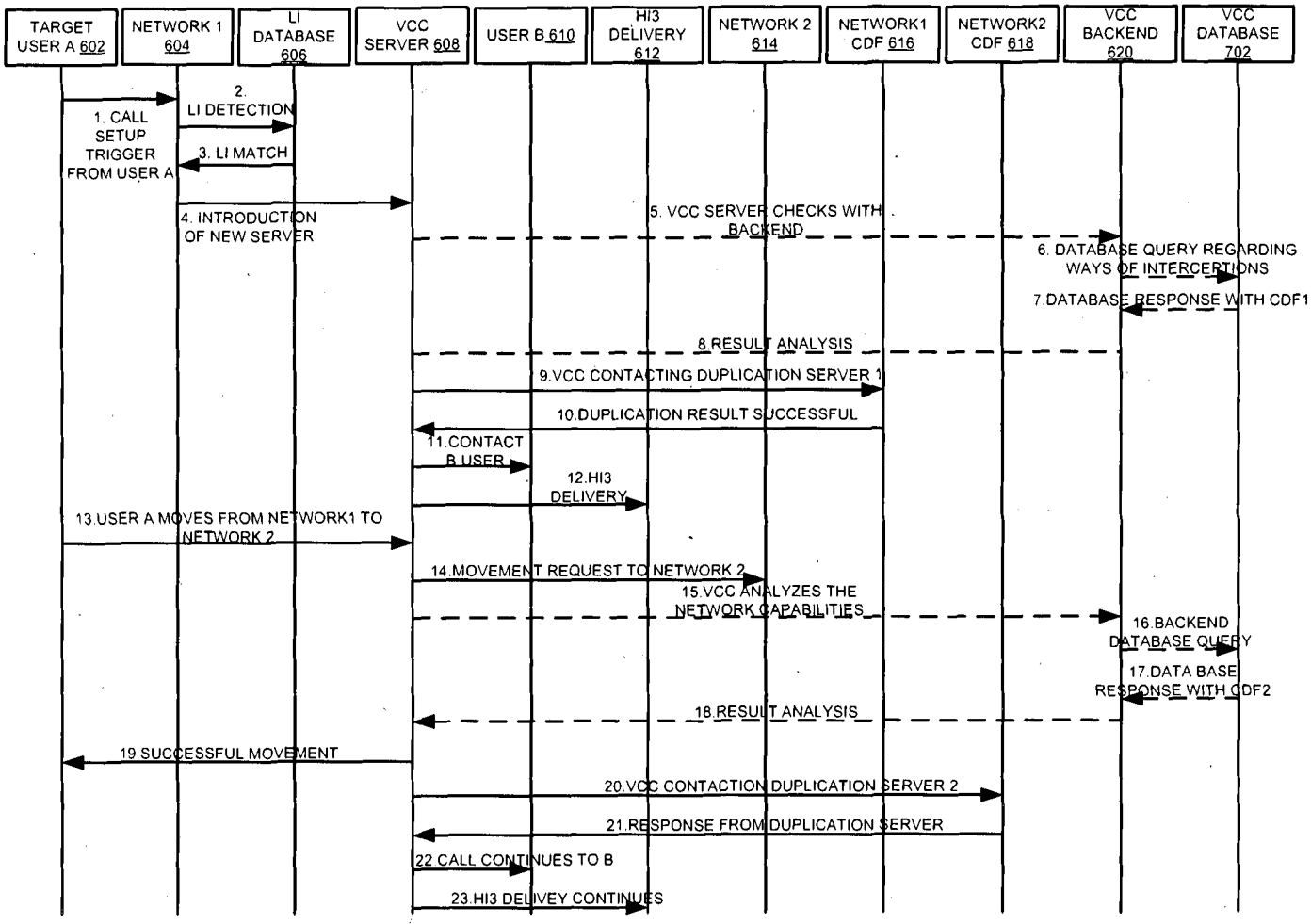
TARGET USER A 602
NETWORK 1 604
LI DATABASE 606
VCC SERVER 608
USER B 610
HI3 DELIVERY 612
NETWORK 2 614
NETWORK1 CDF 616
NETWORK2 CDF 618
VCC BACKEND 620
VCC DATABASE 702
1. CALL SETUP TRIGGER FROM USER A
2. LI DETECTION
3. LI MATCH
4. INTRODUCTION OF NEW SERVER
5. VCC SERVER CHECKS WITH BACKEND
6. DATABASE QUERY REGARDING WAYS OF INTERCEPTIONS
7.DATABASE RESPONSE WITH CDF1
8.RESULT ANALYSIS
9.VCC CONTACTING DUPLICATION SERVER 1
10.DUPLICATION RESULT SUCCESSFUL
11.CONTACT B USER
12.HI3 DELIVERY
13.USER A MOVES FROM NETWORK1 TO NETWORK 2
14.MOVEMENT REQUEST TO NETWORK 2
15.VCC ANALYZES THE NETWORK CAPABILITIES
16.BACKEND DATABASE QUERY
17.DATA BASE RESPONSE WITH CDF2
18.RESULT ANALYSIS
19.SUCCESSFUL MOVEMENT
20.VCC CONTACTION DUPLICATION SERVER 2
21.RESPONSE FROM DUPLICATION SERVER
22.CALL CONTINUES TO B
23.HI3 DELIVEY CONTINUES

FIG. 7 700

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB12/00646

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - H04M 3/22 (2012.01)
USPC - 379/32.01, 35; 455/ 414.1
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC(8) Classification(s): H04W 24/00; H04M 3/22 (2012.01)
USPC Classification(s): 455/ 414.1, 417, 422.1, 436, 466; 370/352, 401, 410; 379/32.01, 35

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
MicroPatent (US Granted, US Applications, EP-A, EP-B, WO, JP, DE-G, DE-A, DE-T, DE-U, GB-A, FR-A); DialogPro (Derwent, INSPEC, NTIS, PASCAL, Current Contents Search, Dissertation Abstracts Online, Inside Conferences); IP.com; Google; Search Terms: Voice call continuity, lawful intercept, network properties, location, configure

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2005/0152275 A1 (LAURILA A. et al.) July 14, 2005, Figure 1, Paragraphs [0001], [0009], [0011]-[0013] and [0022] and Claims 4 and 5	1-21
Y	US 2006/0268921 A1 (EXTROM B. et al.) November 30, 2006, Figure 5 and Paragraphs [0036] and [0037]	1-21
Y	US 2007/0249316 A1 (RAO A.) October 25, 2007, Paragraphs [0019]-[0021]	3, 10, and 17

☐ Further documents are listed in the continuation of Box C. ☐

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 August 2012 (16.08.2012)	12 SEP 2012
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Shane Thomas PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (July 2009)