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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 July 2011 (07.07.2011)

PCT

(10) International Publication Number
WO 2011/080638 A1

(51) International Patent Classification:
H04W 12/12 (2009.01)

(21) International Application Number:
PCT/IB2010/055717

(22) International Filing Date:
10 December 2010 (10.12.2010)

(25) Filing Language: Turkish

(26) Publication Language: English

(30) Priority Data:
2009/10109 31 December 2009 (31.12.2009) TR

(71) Applicant *(for all designated States except US)*: **TURKCELL TEKNOLOJI ARASTIRMA VE GELISTIRME ANONIM SIRKETI** [TR/TR]; Tubitak Marmara Arastirma Merkezi, Gebze Yerleskesi, Teknoloji Serbest, Bolgesi, Gebze, 41470 Kocaeli (TR).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **SENGUDER, Sinan** [TR/TR]; Turkcell Teknoloji Arastirma Ve, Gelistirme Anonim Sirketi, Tubitak Marmara Arastirma Merkezi, Gebze Yerleskesi, Teknoloji Serbest Bolgesi, Gebze 41470 Kocaeli (TR). **BUK, Onur** [TR/TR]; Turkcell Teknoloji Arastirma Ve, Gelistirme Anonim Sirketi, Tubitak Marmara Arastirma Merkezi, Gebze Yerleskesi, Teknoloji Serbest Bolgesi, Gebze 41470 Kocaeli (TR). **KOKSAL, Bulent** [TR/TR]; Turkcell Teknoloji Arastirma Ve, Gelistirme Anonim Sirketi, Tubitak Marmara Arastirma Merkezi, Gebze Yerleskesi, Teknoloji Serbest Bolgesi, Gebze 41470 Kocaeli (TR).

(74) Agent: **ANKARA PATENT BUREAU LIMITED**; Bestekar Sokak No.10, Kavaklidere, 06680 Ankara (TR).

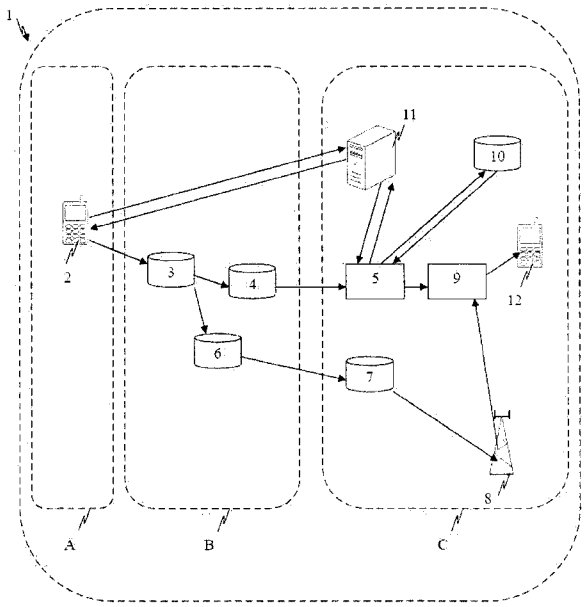
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, 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, RO, RS, RU, 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, 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,

[Continued on next page]

(54) Title: ILLEGAL CARRIER DETECTION PLATFORM AND METHOD

Figure 1



(57) Abstract: The present invention relates to an illegal carrier detection platform (1) and method (100) for detecting the MS-ISDN numbers, which illegally transfer traffic from abroad into the GSM system as if it is a domestic call, and which are defined as Simbox.

WO 2011/080638 A1

SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

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

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

ILLEGAL CARRIER DETECTION PLATFORM AND METHOD

Field of the Invention

The present invention relates to an illegal carrier detection platform and method for detecting the MS-ISDN (Mobile Subscriber Integrated Services Digital Network) numbers, which illegally transfer the traffic from abroad into the GSM (Global System for Mobile communications) system as if it is a domestic call, and which is defined as simbox.

Background of the Invention

Systems used nowadays can detect illegal carrier numbers, which illegally transfer the traffic from abroad into the GSM system causing the operators to be devoid of their income, by post processing the detailed records of the domestic and international calls (CDR – Call Detailed Record).

The United States patent document no. **US6023619**, known in the state of the art, discloses a method for eliminating illegal operations conducted by third persons via authentic subscribers. In the said method based on RF (radio frequency) signature exchange between the foreign and home service areas, RF signatures are evaluated in the foreign or home service areas. In the said invention, when the mobile user passes to the area of a foreign network, the user is determined to be roaming by the SID and MIN information and when a call is made, MTSO is informed. The RF signature of the mobile device is detected if there is any, or a new RF signature is assigned. RF signature analysis is performed by the fraud control system in the home service area and thereby it is determined whether the call is fraudulent or not.

The United States patent document no. **US6856982**, known in the state of the art, discloses a system and method for performing a real time fraudulent call analysis.

The system comprises a switching point (e.g. MSC) which receives a call and an intelligent network service engine which receives the call data from the switching point. The service engine (e.g. HLR, service control point, INSight platform, etc.) uses real time fraud management tools to analyze the call origination data and to determine whether or not the call has a fraudulent content.

The international patent document no. **WO0024219,** known in the state of the art, discloses a device for detecting fraudulent operations in radio networks. The device comprises a mobile station (MS) having a nonvolatile memory that saves electronic identification numbers and first calling event table. The invention also includes an MSC or HLR having a second calling event table containing a mirror image of the first calling event table (if no fraud has occurred). Both calling event tables contain outgoing call event data for the MS. The invention also includes a method for detecting fraudulent operations in radio networks. According to the said method; the calling data are retrieved from the MSC for the MS; the MS is queried with the retrieved data; a response message sent from the MS to the MSC; the query data and the response message are compared; and fraud is detected if the response message does not conform to the calling data.

The United States patent document no. **US2007072587**, known in the state of the art, discloses a system controlling fraudulent activity for cellular telephones roaming in a foreign network. The system comprises a fraud management which monitors telephone activity on the network, detects fraudulent patterns within the activity and prevents these activities. The system also comprises a roaming signaling interrogation unit that is associated with the fraud management unit. The interrogation unit monitors connections set up by subscribers from other networks and forwards information of the roaming to the fraud management unit. The forwarded information allows detecting the fraudulent activities amongst the roaming connections.

The International patent document no. **WO2008128742**, known in the state of the art, mentions about monitoring of the calls made by roaming users. For this purpose, at the first location (e.g. at HPLMN), defining features of the roaming calls are received from the second location (e.g. VPLMN) and thus calls of the roaming subscribers are reported to the first location. In response to the first information received, the second information defining the roaming calls being allowed and comprising requests for data is transmitted to the second location. The third information comprising the data and the responses is received from the second location and is used for evaluating the roaming calls and detecting fraudulent activities.

Summary of the Invention

The objective of the present invention is to provide an illegal carrier detection platform and method which enables to detect the MS-ISDN numbers that illegally transfer traffic from abroad into the GSM system as if it is a domestic call.

Detailed Description of the Invention

The illegal carrier detection platform and method realized to fulfill the objective of the present invention is illustrated in the accompanying figures wherein,

Figure 1 is the schematic view of the devices included in the system.
Figure 2 is the flowchart of the illegal carrier detection method.

The parts in the figures are each given a reference numeral where the numerals refer to the following:

1. Illegal carrier detection platform
2. Device calling from abroad
3. Legal Carrier network

4. Legal Carrier network
5. International gateway
6. Illegal Carrier network
7. Illegal carrier
8. Base station
9. MSC
10. HLR
11. Server
12. Called device

A. Visited public land mobile network
B. Carrier network
C. Home public land mobile network

The inventive illegal carrier detection platform comprises

— at least one device (2) calling from abroad,

— at least one visited public land mobile network (A) from which the device (2) calling from abroad receives service,

— at least one legal carrier network (3) which enables the visited network to provide service,

— at least one international gateway (INTL GW (5)) which enables connection of the visited public land mobile network (A) to the home public land mobile network (C),

— at least one mobile switching center (MSC) (9) which enables routing calls,

— at least one home location register (HLR) (10) which provides calling authorization the user,

— at least one server (11) which manages the incoming calls and is used for detecting illegal carriers (7),

— at least one called device (12).

CAMEL protocol is a protocol which is developed to enable the operator to determine services over the standard services of global system for mobile

communications (GSM) or universal mobile telecommunications system (UMTS) in the GSM or UMTS networks. CAMEL architecture is based on the Intelligent Network standards.

The carrier network (B) is the network that provides services such as audio, data communication to the users.

The illegal carrier (7) is the device which illegally transfers calls from abroad into the home public land mobile network (C).

The illegal carrier detection algorithm is the script that is run in the server (11) for detecting illegal carrier numbers.

The Home Public Land Mobile Network (HPLMN) (C) is the GSM network wherein the user is registered and profile of the user is stored.

The Visited Public Land Mobile Network (VPLMN) (A) is the GSM network wherein the user, who has left her/his home public land mobile network (C), is roaming.

The **server (11)** is at least one server which detects illegal carriers (7) while managing incoming calls.

IAM (RRN) (Initial Address Message, Rerouting Number)

SETUP (RRN) (Initial Message, Rerouting Number)

MSC (Mobile Switching Center) (9) is the location where the calls coming to or made by the subscriber are each routed to their targets.

HLR (Home Location Register) (10) is the component of the home public land mobile network(C) which authorizes and saves the user as the subscriber of the concerned network and stores the location of the user.

Intl GW (International Gateway) (5) is the gateway used by the visited public land mobile network (A) for connection with the home public land mobile network (C) when a subscriber in the visited public land mobile network (A) calls a subscriber in the home public land mobile network (C). In legally made calls, the visited public land mobile network (A) should reach the home public land mobile network (C) via international gateway (5).

The illegal carrier (7) is the device that transfers the call, which should reach the called subscriber via international gateway (5), into the GSM system showing it as if it is a domestic call.

CAMEL (Customised Applications for Mobile networks Enhanced Logic) profile is provided by the home location register (10) to the postpaid subscribers who travel abroad. The Originating CAMEL subscription information (OCSI) feature is activated by the visitor location register of the visited public land mobile network (A), and all of the calls made by the subscriber abroad are enabled to arrive at the new platform (Server (11)) by the help of the originating CAMEL subscription information profile. ,

When the subscriber makes a call in a visited public land mobile network (A) supporting CAMEL, the CAMEL Initial Detection Point (IDP) message is sent to the Server (11) by the visited public land mobile network (A). Initial Detection Point message is transmitted to the Server (11), when the postpaid subscriber makes a call abroad, by the visitor location register of the visited public land mobile network (A) due to the originating CAMEL subscription information feature at the subscriber. The initial detection point message includes information such as the calling number, called number, location number, service value, time

slice value, originally called number, redirecting number, IMSI (International Mobile Subscriber Identity) information.

The server (11) checks the called number information in the initial detection point message in order to decide whether the call is towards the home public land mobile network (C). The server (11) checks the called number information and decides whether this number includes the home public land mobile network (C) prefix. If the number includes the home public land mobile network (C) prefix, an interrogation is transmitted to the MNP DB (Mobile Number Portability Database), which is kept by the Information and Communication Technologies Authority and which the operators periodically make a copy, by means of MAP ATI (Mobile Application Part AnyTimeInterrogation) message. Thus, the home public land mobile network (C) operator from which the number, independent of its prefix, receives service is determined.

The server (11) sends CAMELConnect message towards the visitor location register of the visited public land mobile network (A) in response to the incoming initial detection point message, and this message enables the call to be routed to a temporary number. A rerouting number which is a temporary number is sent in the CAMELConnect message. The temporary number is used for the call to arrive at the home public land mobile network (C) the second time through the international gateway (5). Due to the rerouting number that is used, the call arrives at the home public land mobile network (C) again. The server (11) stores information related to the incoming call such as rerouting number, Initial Detection Point (IDP) Calling number, Initial Detection Point (IDP) Called Number, Initial Detection Point (IDP) Called Number Type, Operator Code (the number stored in the database according to the operator where the subscriber exists), Initial Detection Point 1 Time (arrival time of the initial detection point), Initial Detection Point 1 visitor location register, visitor location register where there is a roaming subscriber.

In case of a legal call, the Second Initial detection point is expected to be triggered towards the server (11) via the international gateway (5). If triggering is performed from home mobile switching centers (9) rather than the international gateway (5), it is determined that this call is not coming through legal means. The calling number in the Second Initial detection point is an illegal carrier (7) number that transfers the call into the home GSM system through illegal means. This detected number is saved into the database.

Based on configuration either CAMELConnect message is sent to the Second Initial detection point (the used Called Number is the called number received at the first Initial detection point) or the call is terminated by the CAMELReleaseCall message sent by the Server (11) to the visitor location registers included in the home public land mobile network (C).

The inventive illegal carrier detection method (100) comprises the steps of

— the roaming subscriber initiating a call (101),

— Initial detection point being communicated to the Server (11) by the visitor location register of the visited public land mobile network (A) (102),

— The server (11) checking the called number information in the initial detection point message (103),

— The server (11) determining whether the number includes home public land mobile network (C) prefix (104),

— MAP ATI interrogation being transmitted to MNP DB in order to determine the operator of the number (105),

— the Server (11) sending CAMELConnect message to the visitor location register of the visited public land mobile network (A) in response to the Initial detection point (106),

— the Server (11) storing information of Rerouting number, Initial detection point calling number, Initial detection point called number, Initial detection point called number type, Operator code, Initial detection point 1 Time, Initial detection point 1 visitor location register (107),

— expecting the call to arrive, with the rerouting number, at the home public land mobile network (C) through the international gateway (5) (108),

— the second Initial detection point being triggered towards the server (11) by international gateway (5) or by the visitor location registers in the home public land mobile network (C) (109),

— detecting the source of triggering (110),

— detecting whether triggering comes from the international gateway (5) or the visitor location registers in the home public land mobile network (C),

— detecting the illegal carrier (7), and continuing or terminating the call depending on a parameter changed on the platform (112) in case the triggering comes from the visitor location registers in the home public land mobile network (C).

The roaming subscriber initiates a call towards her/his own home public land mobile network (C) (101). When a call is initiated in the visited public land mobile network (A), the visitor location register of the visited public land mobile network (A) sends an Initial detection point message to the Server (11) (102). The server (11) receives the incoming Initial detection point message and checks the Called Number information in this message (103). The server (11) determines whether the called number is in the home public land mobile network (C) by looking at the prefix of the called number (104). If the called number is not in the home public land mobile network (C), the call is not interfered. For the numbers determined to be in the home public land mobile network (C), the Server (11) sends MAP ATI interrogation to MNP DB, whereby the operator of the called number is determined (105). After the operator is determined, the Server (11) sends CAMELConnect message to the visitor location register of the visited public land mobile network (A) in response to the incoming Initial Detection point message (106). The Server (11) stores information such as Rerouting number (RRN), Initial detection point Calling Number, Initial detection point Called Number, Initial detection point Called Number Type, Operator code, Initial detection point 1 Time, Initial detection point 1 visitor location register (107). By

means of the rerouting number, the call is enabled to arrive at the home public land mobile network (C) the second time (108). The visitor location registers in the home public land mobile network (C) trigger a second Initial detection point message towards the Server (11) (109). The Server (11) determines the source of this triggering (110). The Server (11) checks whether the source of this triggering is the international gateway (5) (111). If the triggering is realized through a mobile switching center (9) in the home public land mobile network (C) instead of the international gateway (5), the Calling Number in the second Initial detection point is an illegal carrier (7) number. In this case, the call may be continued or terminated depending on a parameter changed on the Platform. If the call will be continued, a CAMELConnect message is sent to the second Initial detection point. If the call will be terminated, CAMELReleaseCall message is sent by the Server (11) to the visitor location registers in the home public land mobile network (C) (112). If the call is triggered through an international gateway (5), then it is a normal call and the call is continued by using the called number in the first initial detection point.

It is possible to develop a wide variety of embodiments of the inventive Illegal Carrier Detection Platform (1). The invention cannot be limited to the examples described herein and it is essentially according to the claims.

CLAIMS

1. An illegal carrier detection platform (1) comprising

— at least one international gateway (5) which enables connection of the visited public land mobile network (A) to the home public land mobile network (C),

— at least one home location register (10) which provides calling authorization the user,

— at least one mobile switching center (9) which enables routing calls,

— at least one server (11) which detects illegal carriers (7) while managing incoming calls,

and characterized by

at least one server (11) which routes calls within the network.

2. An illegal carrier detection platform (1); which is used for detecting the illegal carrier (7) that transfers the call, which should reach the called subscriber via international gateway (5), into the GSM system showing the call as if it is a domestic call; by employing

— at least one device (2) calling from abroad,

— at least one visited public land mobile network (A) from which the device (2) calling from abroad receives service,

— at least one international gateway (5) which enables connection of the visited public land mobile network (A) to the home public land mobile network (C),

— at least one mobile switching center (MSC) (9) which enables routing calls,

— at least one server (11) which manages the incoming calls and is used for detecting illegal carriers (7),

— at least one called device (12);

and characterized by an illegal carrier detection method (100) comprising the steps of

— the roaming subscriber initiating a call (101),

— Initial detection point being communicated to the Server (11) by the visitor location register of the visited public land mobile network (A) (102),

— the Server (11) checking the called number information in the initial detection point message (103),

— the Server (11) determining whether the number includes home public land mobile network (C) prefix (104),

— MAP ATI interrogation being transmitted to MNP DB in order to determine the operator of the number (105),

— the Server (11) sending CAMELConnect message to the visitor location register of the visited public land mobile network (A) in response to the Initial detection point (106),

— the Server (11) storing information of Rerouting number, Initial detection point calling number, Initial detection point called number, Initial detection point called number type, Operator code, Initial detection point 1 Time, Initial detection point 1 visitor location register (107),

— expecting the call to arrive, with the rerouting number, at the home public land mobile network (C) through the international gateway (5) (108),

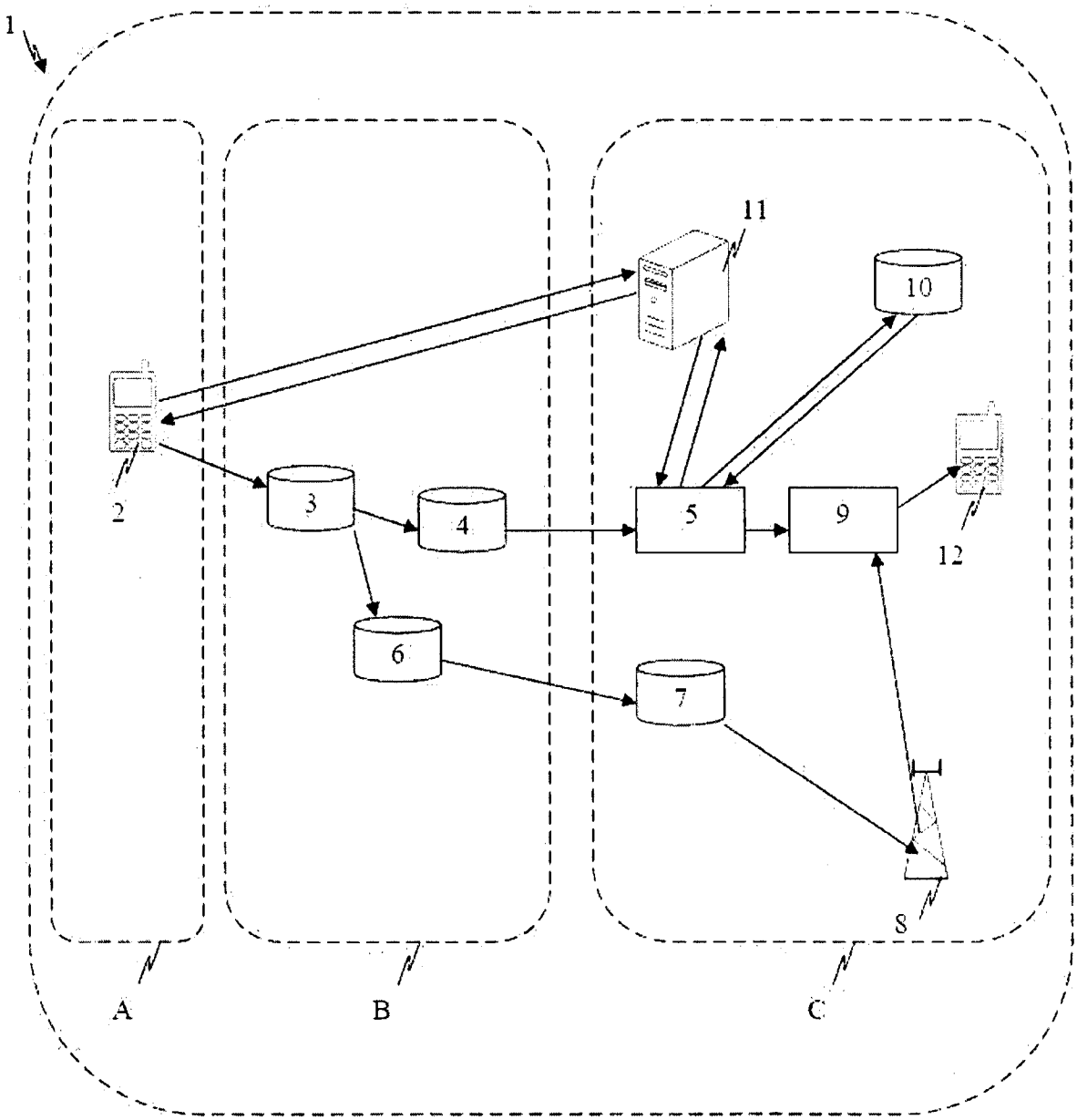
— the second Initial detection point being triggered towards the server (11) by international gateway (5) or by the visitor location registers in the home public land mobile network (C) (109),

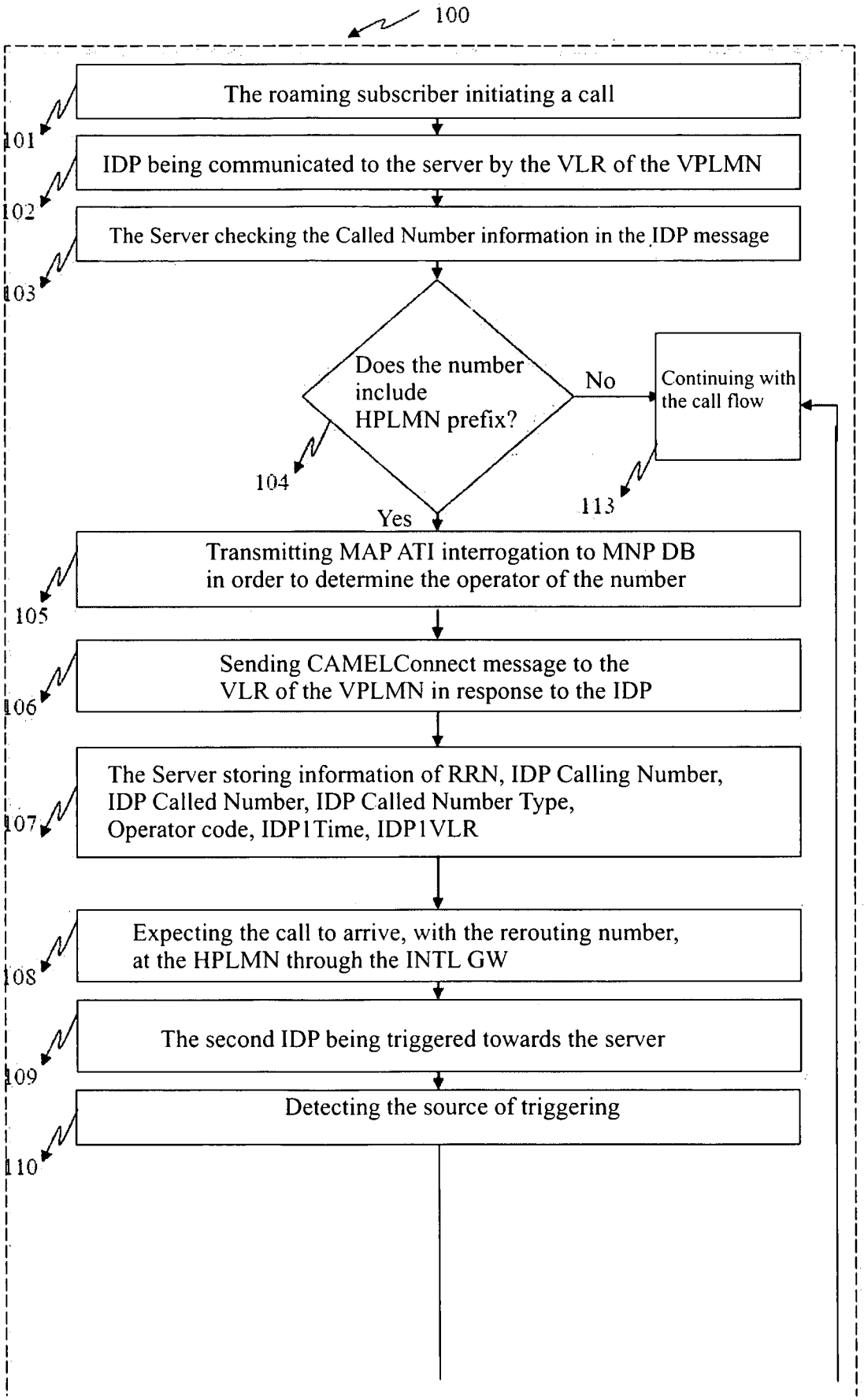
— detecting the source of triggering (110),

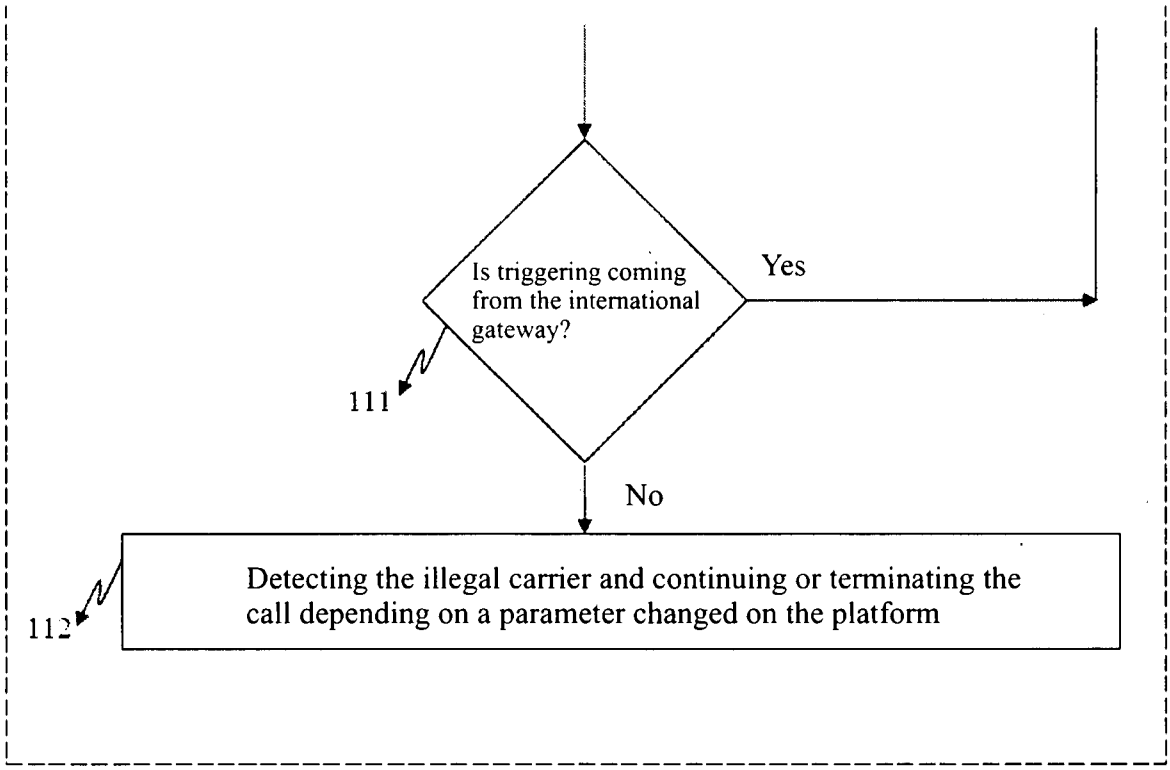
— detecting whether triggering comes from the international gateway (5) or the visitor location registers in the home public land mobile network (C) (111),

— detecting the illegal carrier (7), and continuing or terminating the call depending on a parameter changed on the platform (112) in case the triggering comes from the visitor location registers in the home public land mobile network (C).

Figure 1




100
The roaming subscriber initiating a call
101
IDP being communicated to the server by the VLR of the VPLMN
102
The Server checking the Called Number information in the IDP message
103
Does the number include HPLMN prefix?
No
Continuing with the call flow
104
113
Yes
Transmitting MAP ATI interrogation to MNP DB in order to determine the operator of the number
105
Sending CAMELConnect message to the VLR of the VPLMN in response to the IDP
106
The Server storing information of RRN, IDP Calling Number, IDP Called Number, IDP Called Number Type, Operator code, IDP1Time, IDP1VLR
107
Expecting the call to arrive, with the rerouting number, at the HPLMN through the INTL GW
108
The second IDP being triggered towards the server
109
Detecting the source of triggering
110


Is triggering coming from the international gateway?
Yes
111
No
Detecting the illegal carrier and continuing or terminating the call depending on a parameter changed on the platform
112

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2010/055717

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W12/12
ADD.

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)
H04M H04Q H04W

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 practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2007/072587 A1 (DELLA-TORRE REUVEN [IL]) 29 March 2007 (2007-03-29) cited in the application figure 2 paragraph [0061] - paragraph [0077] paragraph [0085] - paragraph [0093] -----	1
X,P	EP 2 209 331 A1 (VODAFONE PLC [GB]) 21 July 2010 (2010-07-21) figure 7 paragraph [0117] - paragraph [0124] -----	1,2
A	EP 1 675 420 A1 (ORANGE S A [FR]) 28 June 2006 (2006-06-28) paragraph [0031] paragraph [0034] - paragraph [0037] -----	1,2
	-/--	

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* 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 document 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
29 April 2011	13/05/2011

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Lamelas Polo, Yvan

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2010/055717

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2009/069047 A1 (RUSSELL TRAVIS E [US] ET AL) 12 March 2009 (2009-03-12) paragraph [0004] - paragraph [0006] paragraph [0027] paragraph [0033] - paragraph [0039]	1,2

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/IB2010/055717

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2007072587 A1	29-03-2007	NONE	
EP 2209331 A1	21-07-2010	GB 2464261 A	14-04-2010
		US 2010087191 A1	08-04-2010
EP 1675420 A1	28-06-2006	EP 1829402 A1	05-09-2007
		WO 2006066942 A1	29-06-2006
US 2009069047 A1	12-03-2009	NONE	