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

(19) **World Intellectual Property Organization**
International Bureau

(43) **International Publication Date**
9 August 2007 (09.08.2007)

PCT

(10) **International Publication Number**
WO 2007/088344 A1

(51) **International Patent Classification:**
H04L 9/32 (2006.01) *H04Q 7/38* (2006.01)
H04L 29/06 (2006.01) *H04Q 7/34* (2006.01)

(21) **International Application Number:** PCT/GB2007/000309

(22) **International Filing Date:** 30 January 2007 (30.01.2007)

(25) **Filing Language:** English

(26) **Publication Language:** English

(30) **Priority Data:**
0601954.1 31 January 2006 (31.01.2006) GB

(71) **Applicant** *(for all designated States except US)*: **M.M.I. RESEARCH LIMITED** [GB/GB]; 5 Diary Walk, Hartley Wintney, Hampshire RG27 8XX (GB).

(72) **Inventors; and**
(75) **Inventors/Applicants** *(for US only)*: **MARTIN, Paul, Maxwell** [GB/GB]; M.M.I. Research Limited, 5 Diary Walk, Hartley Wintney, Hampshire RG27 8XX (GB). **DOLBY, Riki, Benjamin** [GB/GB]; M.M.I. Research Limited, 5 Diary Walk, Hartley Wintney, Hampshire RG27 8XX (GB).

(74) **Agents: RIBEIRO, James, Michael** et al.; Withers & Rogers LLP, Goldings House, 2 Hays Lane, London SE1 2HW (GB).

(81) **Designated States** *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, 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, LV, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 2007/088344 A1

(54) **Title:** ACQUIRING IDENTITY PARAMETER

(57) **Abstract:** A method of acquiring an identity parameter of a device registered with a network. The device is configured to respond to a set of integrity protected requests from the network only after the device has authenticated the network. The device is also configured to respond to a non-integrity protected identity request from the network without requiring authentication of the network. The method comprises transmitting a false cell broadcast which is not under the control of the network, the false cell broadcast including the non- integrity protected identity request; and receiving the identity parameter from the device in response to the identity request.

ACQUIRING IDENTITY PARAMETER

The present invention is concerned with a method and associated apparatus for acquiring an identity parameter of one or more mobile devices.

An IMSI Catcher is described in Hannes Federrath, Security in Mobile Communications: Protection in GSM networks, mobility management and multilateral security - Braunschweig; Wiesbaden: Vieweg, 1999, ISBN 3-528-05695-9. The IMSI Catcher behaves like a BTS and like an MS in relation to the "genuine" BTS of the network carrier. The IMSI Catcher transmits a signal on the BCH, which must be received more strongly by the MSs than the signal of the genuine BTS. The MSs continuously select the BTS that can be optimally reached and consequently they answer to the IMSI Catcher.

A method for identifying the user of a mobile telephone and for listening in to outgoing calls is described in EP-A-1051053. A Virtual Base Station (VBTS) obtains a Broadcast Allocation (BA) list of base stations, selects a base station from the BA list, and emulates the base station in order to acquire identity parameters (IMSI, IMEI) from the mobile telephone. EP-A-1051053 is concerned with obtaining the IMSI and IMEI of a single target device, in order to intercept the calls of the user.

The present invention provides a method of acquiring an identity parameter of a device registered with a network, the device being configured to respond to a set of integrity protected requests from the network only after the device has authenticated the network, the device also being configured to respond to a non-integrity protected identity request from the network without requiring authentication of the network, the method comprising transmitting a false cell broadcast which is not under the control of the network, the false cell broadcast including the non-integrity protected identity request; and receiving the identity parameter from the device in response to the identity request.

The invention is particularly suited for acquiring the parameter of a device registered with a Third Generation (3G) network which typically has a high level of authentication required.

An embodiment of the present invention will now be described with reference to the accompanying drawings, in which:

Figure 1 is a schematic diagram showing a 3G network including a User Equipment device (UE), and a Separately Introduced NodeB (SINodeB); and

Figure 2 shows the SINodeB in further detail.

Figure 1 shows a 3G network comprising three NodeBs 101-103 broadcasting to three cells by downlink transmissions 104-106 each having a unique downlink scrambling code. On moving into the vicinity of the three NodeBs, a User Equipment device (UE) 120 evaluates on which NodeB to camp.

The UE 120 is required to constantly re-evaluate the signals from cells around it. It does this to ensure that during a connection (data or voice) it is always communicating with the best (most appropriate) NodeB. However a 3G UE will spend most of its time when not transmitting voice or data traffic in an idle state. In this idle state the UE will monitor the strength of the serving NodeB and other neighbour NodeBs, and if the criteria specified by the network are met then it will perform a cell reselection converting one of the previous neighbour NodeBs into the new serving NodeB. If this new serving NodeB is in a different location or routing area then the UE must perform a location or routing area update procedure to inform the network of its new location. This is done so that the network will always have an idea of where the UE is in the network, so that in the event of an incoming call request to the UE the network can use the minimum amount of resources to request the UE to establish a signaling connection.

Each NodeB transmits broadcasted information that serves two main purposes. First, some of this information is transmitted using well know codes and data patterns that allow the UE to recognise that the Radio Frequency (RF) signal being received is actually a UMTS cell and also allows the UE to perform power measurements on the received signal. Second, descriptive information about the cell is broadcast. This system information is transmitted in the form of System Information Blocks (SIBS) which describe many parameters of the NodeB and provide enough information for the UE to identify the mobile network that the NodeB belongs to, and also to establish a signaling connection if it needs to.

Figure 2 shows a Separately Introduced NodeB (SINodeB) 100. The SINodeB 100 is configured to acquire an identity parameter from a UE registered with the 3G network of Figure 1. This is achieved by emulating a NodeB using a method specially adapted to the UMTS protocol, as described in further detail below.

The SINodeB 100 is typically a mobile device, which may be housed in a vehicle. In use, the SINodeB 100 is moved to an area, and operated to acquire identity parameters from one or more User Equipment devices (UEs) registered with the 3G network in that area. Alternatively the SINodeB 100 may be permanently located in an area of interest. In both cases, the SINodeB 100 effectively transmits a false cell broadcast which is not under the control of the 3G network providing coverage to that area.

In order to persuade the UE to move over to the SINodeB 100, certain criteria must be met. Primarily the transmission must be received at the UE with a higher signal strength. Even once the UE has made the decision that the SINodeB 100 is preferential it would normally be considered necessary to pass the UMTS security procedures in order to be able to gather any useful information or perform any useful tasks.

It is not necessary to exactly emulate all the configuration of an existing NodeB for it to be a suitable candidate for a UE to connect to. This makes the task of configuring the SINodeB 100 much simpler. The reason for this is that the broadcasted system information defines the configuration of the cell that is transmitting that data, and cells within the same network will have different configurations, so the UE always looks at the data from the current cell to determine the necessary information.

The key parameters in the false cell broadcast that need to be considered for changing are as follows:

- Cell Frequency
- Primary Scrambling code
- Mobile Country Code (MCC) [- which country this cell is in]
- Mobile Network Code (MNC) [- which network this cell belongs to]
- Location area code (LAC)
- Routing area code (RAC)
- Cell power
- SIB value tags [- Value tags are use by the UE to detect if SIB information has changed between reads of the SIBs]
- Contents of SIB18 and SIB11 for serving cell [- SIB 11 contains measurement control information to be use by the UE in idle mode / SIB 18 contains PLMN ids of neighbour cells to be considered in idle and connected mode]

The MCC and MNC must be the same as the serving cell for the UE to consider the SINodeB to be in the same network.

The Cell Frequency must be the same as the serving cell to make the process as easy as possible - interfrequency reselections have more complex criteria and processes.

There are several options for configuring the other parameters transmitted by the SINodeB:

1) Same LAC/RAC and Primary Scrambling code, different SIB value tags - This completely mimics the serving cell, and allows the SINodeB to actively grab the UE.

2) Different LAC/RAC and Primary Scrambling code - where Scrambling code is present in the SIB11 of the serving cell. This is mimicking a neighbour NodeB that the serving NodeB has been instructing the UE to perform measurements on - thus ensuring that the UE is trying to look for the SINodeB. This causes a UE to perform a cell reselection to the SINodeB if the SINodeB transmission is of sufficiently higher power than the serving NodeB. The amount by which the SINodeB needs to be a stronger signal is defined in SIB3 of the serving NodeB.

3) Different LAC/RAC and Scrambling code - no reference in SIBS of the serving NodeB.

Once a suitably strong and configured cell is being transmitted, the UEs in the target area will perform a cell reselection to the SINodeB and establish an RRC connection for the purpose of performing a location updating procedure. The location update is required because the LAC of the SINodeB is different from the old serving SINodeB. Once the RRC connection is established the SINodeB has the opportunity to perform other signaling procedures as desired.

The UMTS protocol is designed to enhance the security and identity protection features in GSM. To this end, authentication and integrity mechanisms are used in addition to the temporary identities found in GSM. These temporary identities avoid the frequent transmission of the identity of the IMSI and the IMEI, because once the network has assigned the phone a temporary identity then it maintains a mapping from that new identity to the IMSI.

Mechanisms exist to allow the network to interrogate a phone for its IMSI and IMEI and these are used for the first connection of a phone to the network or when an error has occurred and the network needs to re-establish the correct mapping between a temporary identity (such as a TMSI) and its associated real identity (such as an IMSI). In normal network operation almost all signaling between the UE and the network must be performed after the authentication procedure has been completed successfully and integrity has been enabled on the signaling connection. This makes the falsification or modification of signaling by a third party effectively impossible.

Unless a NodeB is provided with a mechanism to successfully pass the authentication and integrity procedures, then the UMTS protocols are designed that almost no useful communication can be achieved with the UE. However there are "gaps" in the UMTS protocols that allow the IMSI, IMEI and TMSI to be retrieved from the UE by the SINodeB 100 without requiring these security mechanisms.

These "gaps" are described in 3GPP TS 33.102 version 3.13.0 Release 1999, and in 3GPP TS 24.008 version 3.19.0 Release 1999. The relevant portions of these protocols will now be described.

3GPP TS 33.102 version 3.13.0 Release 1999

This protocol specifies in Section 6.5 that all signaling messages except the following shall be integrity protected:

HANDOVER TO UTRAN COMPLETE

PAGING TYPE 1

PUSCH CAPACITY REQUEST

PHYSICAL SHARED CHANNEL ALLOCATION

RRC CONNECTION REQUEST

RRC CONNECTION SETUP

RRC CONNECTION SETUP COMPLETE

RRC CONNECTION REJECT

RRC CONNECTION RELEASE (CCCH only)

SYSTEM INFORMATION (BROADCAST INFORMATION)

SYSTEM INFORMATION CHANGE INDICATION

Thus these messages cannot be integrity protected under any circumstances.

3GPP TS 24.008 version 3.19.0 Release 1999

This protocol specifies a list of messages which the UE can respond to, in certain circumstances, without first having integrity protected the network. Specifically, the protocol states the following:

Except the messages listed below, no layer 3 signalling messages shall be processed by the receiving MM and GMM entities or forwarded to the CM entities, unless the security mode control procedure is activated for that domain.

- MM messages:

- AUTHENTICATION REQUEST

- AUTHENTICATION REJECT

- IDENTITY REQUEST

- LOCATION UPDATING ACCEPT (at periodic location update with no change of location area or temporary identity)

- LOCATION UPDATING REJECT

- CM SERVICE ACCEPT, if the following two conditions apply:

- no other MM connection is established; and

- the CM SERVICE ACCEPT is the response to a CM SERVICE REQUEST with CM SERVICE

TYPE IE set to 'emergency call establishment'

- CM SERVICE REJECT

- ABORT

- GMM messages:

- AUTHENTICATION & CIPHERING REQUEST

- AUTHENTICATION & CIPHERING REJECT

- IDENTITY REQUEST

- ATTACH REJECT

- ROUTING AREA UPDATE ACCEPT (at periodic routing area update with no change of routing area or temporary identity)

- ROUTING AREA UPDATE REJECT

- SERVICE REJECT

- DETACH ACCEPT (for non power-off)

CC messages:

- all CC messages, if the following two conditions apply:

- no other MM connection is established; and

- the MM entity in the MS has received a CM SERVICE ACCEPT message with no ciphering or

integrity protection applied as response to a CM SERVICE REQUEST message, with CM SERVICE

TYPE set to 'Emergency call establishment' sent to the network.

Therefore an RRC Connection can be set up without requiring integrity protection, since the RRC connection messages are listed as not requiring integrity protection in 3GPP TS 33.102 version 3.13.0 Release 1999. After an RRC Connection has been established between the SINodeB and the UE, for the purpose of a location update procedure a series of MM Identity Requests are sent by the SINodeB 100 to retrieve the UE identification information. Again, the UE responds to these MM Identity Requests without requiring integrity protection because MM Identity Request is specified in the list given above in 3GPP TS 24.008 version 3.19.0 Release 1999.

Specifically, the series of messages between the UE and the SINodeB is as follows:

UE <-> SINodeB
-> RRC Connection Request
<- RRC Connection Setup
-> RRC Connection Setup Complete
-> MM Location Update Request
<- MM Identity Request (Requesting IMSI)
-> MM Identity Response (IMSI)
<- MM Identity Request (Requesting IMEI)
-> MM Identity Response (IMEI)
<- MM Identity Request (Requesting IMEISV)
-> MM Identity Response (IMEISV)
<- MM Identity Request (Requesting TMSI)
-> MM Identity Response (TMSI)

When the UE sends the MM Location Update Request, it also starts an LAC update timer. The SINodeB ignores this request. If the UE does not receive a valid response to the MM Location Update Request within a predetermined time, then the UE resends the MM Location Update Request. This process is repeated a few times and then the UE aborts the connection.

Thus by sending the series of three MMI Identity Requests straight after the RRC Connection is established, and before the UE aborts the connection, the SINodeB can receive the MM Identity Response messages from the UE without requiring integrity protection.

Once the identity information has been collected, the SINodeB rejects the location update request thus preventing the UE from repeatedly trying to camp on to the SINodeB.

CLAIMS

1. A method of acquiring an identity parameter of a device registered with a network, the device being configured to respond to a set of integrity protected requests from the network only after the device has authenticated the network, the device also being configured to respond to a non-integrity protected identity request from the network without requiring authentication of the network, the method comprising transmitting a false cell broadcast which is not under the control of the network, the false cell broadcast including the non-integrity protected identity request; and receiving the identity parameter from the device in response to the identity request.

2. A method according to claim 1 wherein the identity request is an identity request specified in a 3G network protocol.

3. A method according to claim 2 wherein the identity request is an identity request specified in a UMTS network protocol.

4. A method according to any preceding claim wherein the identity request is an MM identity request.

5. A method according to any preceding claim wherein the device has been assigned with a temporary identity parameter by a network with which the device is registered, and wherein the non-integrity protected identity request is intended for use when the network loses a mapping between the temporary identity parameter and a permanent identity parameter.

6. A method according to any preceding claim wherein the non-integrity protected identity request is intended for use when the device roams from an old network to a new network.

7. A method according to any preceding claim further comprising setting up a non-integrity protected connection with the mobile device.

8. A method according to claim 7 wherein the connection is an RRC connection.

9. A method according to any preceding claim further comprising moving a separately introduced device to an area; and operating the device to perform the method on a device registered with the network in that area.

10. A computer program product which, when run on one or more computers, causes the computer(s) to perform a method according to any preceding claim.

11. Apparatus configured to perform a method according to any of the preceding claims.

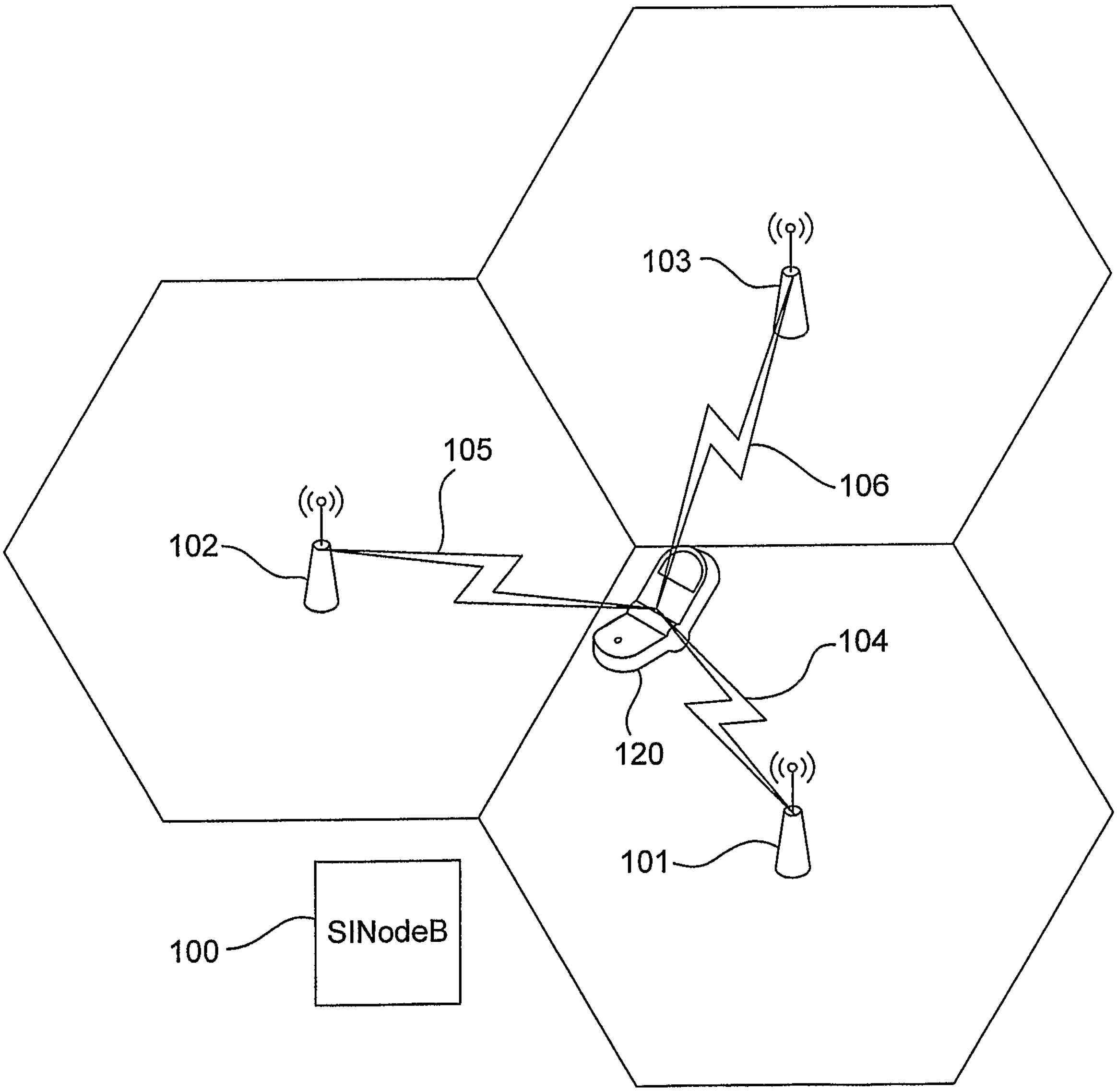

Figure 1

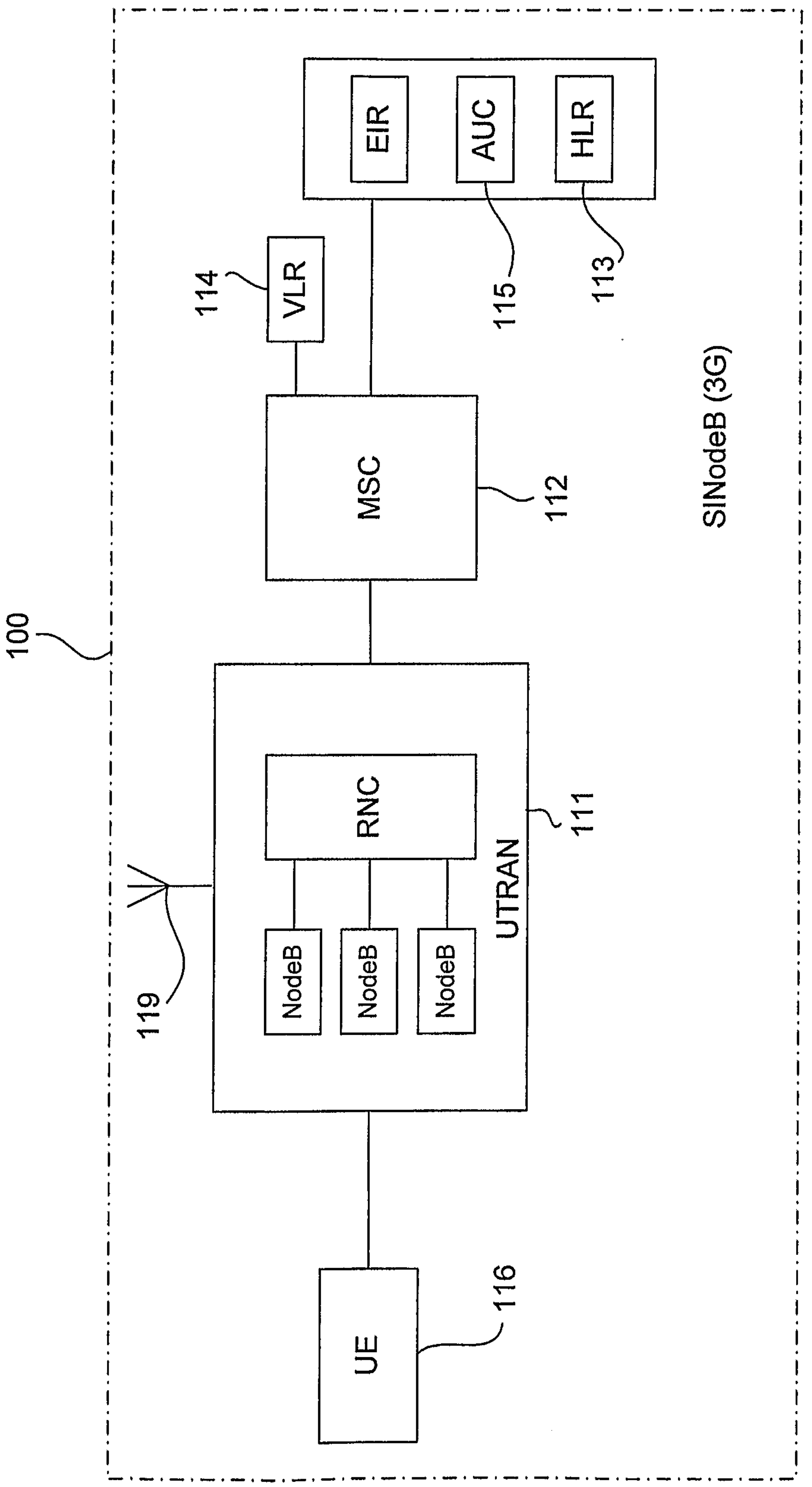
100
UE
116
119
NodeB
NodeB
NodeB
RNC
UTRAN
111
MSC
112
VLR
114
EIR
AUC
HLR
115
113
SINodeB (3G)

Figure 2

INTERNATIONAL SEARCH REPORT

International application No
PCT/GB2007/000309

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/32 H04L29/06 H04Q7/38 H04Q7/34

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)
H04L H04Q

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	"Digital cellular telecommunications system (Phase 2+)" ETSI STANDARDS, EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE, SOPHIA-ANTIPO, FR, vol. 3-CN1, no. V720, December 2005 (2005-12), XP014032487 ISSN: 0000-0001 cited in the application paragraph 2.2.2, 4.1.1.1, 4.1.1.1.1 and 4.1.2.1.1; par. 4.1.2.1 to 4.1.2.1.2 and 4.2.2; par. 4.3.1 to 4.3.2b, 4.3.2.5 to 4.3.2.6 and 4.3.3 to 4.3.3.2; par. 4.4.1, 4.4.4.1 to 4.4.4.4 and 4.4.4.7 ----- -/--	1-11

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

☒ 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 9 May 2007	Date of mailing of the international search report 16/05/2007
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Authorized officer Biyee, Nicole

2

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	FR 2 869 189 A1 (THALES SA [FR]) 21 October 2005 (2005-10-21) page 3, line 1 - page 4, line 12 page 6, line 25 - page 9, line 29 page 9, line 40 - page 10, line 6 -----	1-11
A	EP 1 051 053 A2 (ROHDE & SCHWARZ [DE]) 8 November 2000 (2000-11-08) cited in the application abstract paragraph [0001] - paragraph [0013] paragraph [0014] - paragraph [0024] -----	1-5,7-11
A	EP 1 199 903 A2 (ROHDE & SCHWARZ [DE]) 24 April 2002 (2002-04-24) abstract paragraph [0001] - paragraph [0005] -----	1,4,7-11
X,P	WO 2007/010223 A (M M I RES LTD [GB]; PRIDMORE ANDREW PAUL [GB]; MARTIN PAUL MAXWELL [GB) 25 January 2007 (2007-01-25) page 1, line 14 - page 5, line 28 page 7, line 10 - page 9, line 3 page 10, line 1 - page 17, line 19 -----	1-11

2

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/GB2007/000309

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
FR 2869189 A1	21-10-2005	EP 1747695 A1 WO 2005112497 A1	31-01-2007 24-11-2005
EP 1051053 A2	08-11-2000	DE 19920222 A1	09-11-2000
EP 1199903 A2	24-04-2002	AT 297104 T DE 10051129 A1 DK 1199903 T3 ES 2242687 T3	15-06-2005 18-04-2002 12-09-2005 16-11-2005
WO 2007010223 A	25-01-2007	NONE	