

(19) World Intellectual Property  
Organization  
International Bureau



(43) International Publication Date  
19 February 2004 (19.02.2004)

PCT

(10) International Publication Number  
**WO 2004/015968 A1**

(51) International Patent Classification<sup>7</sup>: **H04M 3/16**

(21) International Application Number:  
PCT/US2003/025131

(22) International Filing Date: 11 August 2003 (11.08.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:  
60/403,158 13 August 2002 (13.08.2002) US

(71) Applicant (for all designated States except US): **THOMSON LICENSING S.A.** [FR/FR]; 46, Quai A. Le Gallo, F-92648 Boulogne (FR).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **VERMA, Shaily** [IN/IN]; A-305 "Glengate", Hiranandani Gardens, 76 Powai, Mumbai (IN). **WANG, Charles, Chuanming** [US/US]; 1504 Spearmint Circle, Jamison, PA 18929 (US). **ZHANG, Junbiao** [CN/US]; 1003 Sunny Slope Road, Bridgewater, NJ 08807 (US).

(74) Agents: **TRIPOLI, Joseph, S.** et al.; Thomson Licensing Inc., Two Independence Way, Suite #200, Princeton, NJ 08540 (US).

(81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

**Published:**

- with international search report
- before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments

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.

(54) Title: MOBILE TERMINAL IDENTITY PROTECTION THROUGH HOME LOCATION REGISTER MODIFICATION

(57) Abstract: Secure access by a mobile wireless terminal (14) of a wireless telephony network (10) is achieved by having a Home Location Register (30) store the terminal's temporary and permanent identities. Upon accessing the network following initial registration, the terminal sends a temporary identity to a Serving GPRS Support Node (SGSN) (201 and 202). If no serving node in the network knows the terminal, the terminal need not sent its permanent identity in clear as was previously required. Rather, the serving node need only query the HLR since the HLR can map the terminal's temporary identity to its permanent identity. In this way, the permanent identity of the mobile wireless terminal remains secure.



WO 2004/015968 A1

## **MOBILE TERMINAL IDENTITY PROTECTION THROUGH HOME LOCATION REGISTER MODIFICATION**

### **5 TECHNICAL FIELD**

This invention relates to a technique for protecting the identity of a mobile wireless terminal when accessing a wireless telephony network.

### **10 BACKGROUND ART**

Presently, users seeking wireless telephony service typically subscribe to one of many providers of such service. Today's wireless telephony service providers not only offer voice calling but also offer General Packet Radio Service (GPRS) to enable the exchange data packets via a mobile wireless terminal. While GPRS exists in many areas, data transmission rates typically do not exceed 56 Kbs and the cost to wireless network service providers to support this service remain high, making GPRS expensive. To provide enhanced data communications, efforts now exist to establish new standards for wireless telephony. One such effort is the proposed "Universal Mobile Telecommunications System (UMTS)" standard specified by the 3rd Generation Partnership Project (3GPP) for advanced packet radio service in wireless telephony networks. The UMTS standard proposes transmission rates as high as 2 Mbps, making such service more attractive to subscribers.

In accordance with the UMTS standard, a subscriber's mobile wireless terminal will transmit its permanent identity, typically referred to as an International Mobile Station Identity or IMSI, to the network upon initial registration. To maintain user identity confidentiality and untraceability, after initial registration, each subscriber receives from the wireless network a temporary identity called Packet Temporary Mobile Subscriber Identity (P-TMSI) kept in a Serving GPRS Support Node (SGSN) in the network. Upon each subsequent access of the wireless network, the mobile wireless terminal will send its P-TMSI. The SGSN serving that mobile wireless terminal maps the P-TMSI to the user's permanent identity (i.e., IMSI). In this way, the user avoids transmitting its IMSI. To reduce the risk of breaching the user's confidentiality, the network should not identify the user for a long period by means of the same

P-TMSI. Rather, the wireless telephony network should assign a new P-TMSI after some extended interval.

Despite efforts to protect the user's confidentiality via the P-TMSI, circumstances exist in present day wireless telephony networks that require the mobile wireless terminal to transmit its permanent identity (IMSI) after registration. For example, upon a new attachment to the wireless telephony network, the mobile wireless terminal could encounter an SGSN different than the one that served the terminal prior to detachment. Upon such a new attachment, the mobile wireless terminal will send its P-TMSI to the new SGSN. In turn, the new SGSN sends an Identification Request message to the old SGSN. If both the old and new SGSNs lack knowledge of the mobile wireless terminal, the new SGSN will send an Identity Request message to the terminal. The mobile wireless terminal must respond with its permanent Identity (IMSI) in clear text, breaching the confidentiality of the user's identity

Thus, there is need for a technique for protecting the user's identity during attachment to a wireless telephony network.

## BRIEF SUMMARY OF THE INVENTION

Briefly, in accordance with a preferred embodiment of the present principles, there is provided a method for enabling a mobile wireless terminal to securely access a wireless network, such as a wireless telephony network. The method commences upon receipt in the network of an access request from a mobile wireless terminal that had previously registered with the network. Thus, the access request made by the mobile wireless terminal will contain a temporary identity assigned to the terminal during each attach procedure. Upon receipt of the identity request, a query is launched to at least one serving node in the wireless network to identify the terminal. If no serving node in the wireless network recognizes the mobile wireless network, then a query is launched to a register (e.g., a Home Location Register), which stores the identity of each registered mobile wireless terminal previously attached to the network. In response, the register sends an identification response to the querying serving node to enable authentication of the user.

Maintaining mobile wireless terminal temporary identity information in the Home Location Register enables a serving node that does not recognize the terminal to query the

register. In this way, the mobile wireless terminal need not send its permanent identity when unrecognised by the serving node.

## BRIEF DESCRIPTION OF THE DRAWINGS

5

FIGURE 1 depicts a block schematic diagram of an illustrative embodiment of a wireless telephony network for practicing the principles of the present invention;

FIGURE 2 depicts a chart illustrating the steps of a prior art procedure whereby a mobile wireless terminal attaches itself to the network of FIG. 1; and

10

FIGURE 2 depicts a chart illustrating the steps of a procedure whereby a mobile wireless terminal attaches itself to the network of FIG. 1 in accordance with the present principles.

## DETAILED DESCRIPTION

15

FIGURE 1 depicts a block schematic diagram of a wireless telephony network 10 having an architecture as proposed in the UMTS 3GPP standard. The wireless telephony network 10 includes at least one, and preferably, a plurality of radio access networks, illustratively shown as radio access networks 12<sub>1</sub> and 12<sub>2</sub>. In the UMTS radio access networks comprising of a Node B and a Radio Network Controllers (RNC), the UMTS Node B, serves as the point of access for a mobile wireless terminal 14 seeking to connect with (attach itself to) the network 10. Radio Network Controllers (RNCs) 16<sub>1</sub> and 16<sub>2</sub> each control a separate one of the radio access networks 12<sub>1</sub> and 12<sub>2</sub>, respectively, for the purpose of allocating the necessary resources in each network.

20

25

Each of the RNCs 16<sub>1</sub> and 16<sub>2</sub> connects to a corresponding one of Serving GPRS Support Nodes (SGSNs) 20<sub>1</sub> and 20<sub>2</sub>, respectively, that comprise part of the core of the wireless telephony network 10. Each SGSN manages packet and voice services for the subscribers on a corresponding radio access network. Each SGSN has a link to a Gateway GPRS Node (GGSN) 22 that serves as an interface to the Internet 24 for packet service. In a similar fashion, the SGSN 20<sub>1</sub> connects to a Mobile Switching Center (MSC) 26 that interfaces to the Public Switched Telephone Network (PSTN) 28 for voice services. A similar MSC (not shown) interfaces the SGSN 20<sub>2</sub> to the PSTN 28.

30

Within the wireless telephony network 10, there exists at least one register (database) 30, typically known as the Home Location Register or HLR. The HLR 30 contains packet domain subscription data and location information that identifies which SGSN serves a particular subscriber. Each of the SGSNs 20<sub>1</sub> and 20<sub>2</sub> accesses the HLR 30 via a separate Gr interface, whereas the GGSN 22 accesses the HLR via a Gc interface. In accordance with the present principles, the HLR 30 stores the International Mobile Station Identity (IMSI) and a temporary identity (P-TMSI) for each mobile wireless terminal 14 previously attached to the wireless telephony network 10. Additionally, the HLR 30 stores the identity (i.e., the address) of each SGSN, the address of the SGSN currently attached to the mobile wireless terminal 14, as well as the address of the last visited SGSN if the terminal is currently detached. For a roaming mobile wireless terminal 14 not resident in the wireless telephony network 10, the HLR associated with that terminal will reside in a different wireless telephony network, accessible through the Internet 24 or a private line (not shown).

In order to better understand the advantage obtained by the attachment technique of the present principles, a description will first be provided of the current attachment technique depicted in FIG. 2. Upon moving from the coverage area of one radio access network to another, a mobile wireless terminal 14 makes an attachment request of the new SGSN serving the newly access radio access network during step 100 of FIG. 2. For purposes of illustration, assume that the mobile wireless terminal 14 seeks attachment through the radio access network 12<sub>2</sub> of Fig. 1. Thus, the mobile wireless terminal 14 initiates the attachment process by making the attachment request to the SGSN 20<sub>2</sub>, hereinafter referred to as the "new" SGSN. Should the new SGSN 20<sub>2</sub> have no identity information for the mobile wireless terminal 14, the new SGSN forwards the attachment request during step 102 of FIG. 2 to the "old" SGSN (e.g., SGSN 20<sub>1</sub> of FIG. 1). If the old SGSN 20<sub>1</sub> no longer retains any identity information for the mobile wireless terminal 14, the new SGSN will receive an identity response during step 103 of FIG. 2 indicating that the old SGSN lacks knowledge of the mobile wireless terminal 14.

Upon receiving an indication from the old SGSN 20<sub>1</sub> that mobile wireless terminal 14 remains unknown, the new SGSN 20<sub>2</sub> sends the mobile terminal an identity request during step 104 of FIG. 2. If unknown to both the SGSNs 20<sub>1</sub> and 20<sub>2</sub>, the mobile wireless terminal 14 cannot simply send its P-TMSI to identify itself. Instead, the mobile wireless terminal 14 must respond to the identity request by sending its permanent identity (i.e., its IMSI) in clear text

during step 105 of FIG. 2 to the new SGSN 20<sub>2</sub>. Sending the IMSI in clear text incurs the risk of interception and fraudulent misuse of the subscriber's identity.

After receiving the IMSI, the new SGSN 20<sub>2</sub> authenticates the mobile wireless terminal 14 by querying the HLR 30 of FIG. 1 during step 106 of FIG. 2. Upon receiving a positive authentication response from the HLR 30, the new SGSN 20<sub>2</sub> provides a positive verification response to the mobile wireless terminal 14 during step 107. Thereafter, the mobile wireless terminal 14 send an International Mobile Equipment Identity (IMEI) request to the new SGSN 20<sub>2</sub> during step 108 of FIG. 2 to initiate an update of the terminal's location, as well as to verify the status of the terminal. Following receipt of the IMEI check request, the new SGSN 20<sub>2</sub> queries an Equipment Identity Register 32 of FIG. 2 during step 109 to verify whether the mobile wireless terminal 14 is legitimate as opposed to having been stolen. Upon finding that mobile wireless terminal 14 legitimate during step 109, the new SGSN 20<sub>2</sub> sends a message to the HLR 30 during step 110 to update the location of the terminal.

In response to the terminal location update information, the HLR 30 sends a request to the old SGSN 20<sub>1</sub> during step 111 to cancel the location information stored therein for the mobile wireless terminal 14. The old SGSN 20<sub>1</sub> responds with a cancel location acknowledgement during step 112. During step 113, the HLR 30 inserts into the new SGSN 20<sub>2</sub> subscriber data associated with the mobile wireless terminal 14 that has now attached itself to this SGSN. The new SGSN 20<sub>2</sub> responds by an Insert Subscriber Data Acknowledgement message during step 114. After step 114, the HLR 30 responds to the new SGSN 20<sub>2</sub> with an Update Location Acknowledgement message during step 115 of FIG. 2.

In addition to updating the HLR 30, the new SGSN 20<sub>2</sub> also makes update request to a Visiting Location Register (VLR) (not shown) in the MSC 26 of FIG. 1 during step 116 since the new SGSN 20<sub>2</sub> is served by a different MSC than the old SGSN 20<sub>1</sub>. Upon receiving such a request, the new MSC/VLR 26 makes a request during step 117 to update the HLR 30. In turn, the HLR 30 sends a cancellation command during step 118 to the old MSC/VLR (designated as MSC 26' of FIG. 2) to indicate attachment of the mobile wireless terminal to the new SGSN 20<sub>2</sub>. The old MSC 26' of FIG. 2 responds with an Acknowledgement message during step 119.

Next, the HLR 30 inserts into the new MSC/VLR 26 updated subscriber data during step 120. The new MSC 26 responds with an Insert Subscriber Data Acknowledgement message during step 122. The new MSC/VLR 26 of FIG. 2 then sends a Location Update Acceptance message to the new SGSN 20<sub>2</sub> during step 123, triggering transmission of an Attach Acceptance

message from the new SGSN to the mobile wireless terminal 14 during step 124. The mobile wireless terminal 14 responds with an 'Attach Complete' message during step 125, followed by a TMSI Reallocation Complete Message from the new SGSN 20<sub>2</sub> to the new MSC/VLR 26 during step 126 to indicate completion of the task of reallocating the TMSI mapping from the old to the new SGSN.

The prior art attachment process of FIG. 2 incurs the disadvantage of requiring the mobile wireless terminal 14 transmit its IMSI in clear text when the old SGSN 20<sub>1</sub> and the new SGSN 20<sub>2</sub> both fail to recognize the terminal. The attachment technique of the present principles, best illustrated in FIG. 3, overcomes this disadvantage by storing subscriber identity information in the HLR 30. Storing such information in the HLR 30 enables identification of the mobile wireless terminal 14 in the event neither the old nor new SGSN recognizes the terminal. Referring to FIG. 3, the attachment technique of the present principles commences when the mobile wireless terminal 14 sends an 'Attach Request' message to the new SGSN 20<sub>2</sub> during step 200 following a transition of the terminal to the radio access network 12<sub>2</sub> of FIG. 1. Upon receipt of the 'Attach Request' message during step 200 of FIG. 3, the new SGSN 20<sub>2</sub> sends an Identity Request message to the old SGSN 20<sub>1</sub> during step 202 to identify the mobile wireless terminal 14. Absent knowledge of the mobile wireless terminal 14 having been attached, the old SGSN 20<sub>1</sub> will send the new SGSN 20<sub>1</sub> an Identity Response message during step 202 indicating an error.

In the past, when the old SGSN 20<sub>1</sub> lacked knowledge of a previous attachment of the mobile wireless terminal 14, the terminal needed to send its permanent identity in clear text to identify itself. To avoid this disadvantage, the present attachment method does not make a request of the mobile wireless terminal 14 under such circumstances. Rather, as depicted in FIG. 3, the new SGSN 20<sub>2</sub> sends an Identity Request message to the HLR register 30 during step 203 after receiving an error message during step 202. In accordance with the present principles, the HLR 30 stores the temporary identity (i.e., the P-TMSI) and permanent identity (IMSI) of each mobile wireless terminal 14 previously attached to the wireless telephony network 10. Thus, upon receipt of the Identity Request message during step 203, the HLR 30 provides the new SGSN 20<sub>2</sub> an Identity Response message during step 204. This message includes the IMSI of the mobile wireless terminal 14, and the associated authentication vectors needed to verify the terminal. During step 205, authentication of the mobile wireless terminal

14 occurs. Typically, such authentication occurs in the same manner as during steps 106-123 of FIG. 2.

Following authentication, the new SGSN 20<sub>2</sub> sends an Attach Acceptance message to the mobile wireless terminal 14 during step 206 of FIG. 3. In response, the mobile wireless terminal 14 sends an 'Attach Complete' acknowledgement message during step 207. During step 208, the new SGSN 20<sub>2</sub> can reallocate the P-TMSI by sending a P-TMSI reallocation command to the mobile wireless terminal 14. Upon completion of reallocation of the P-TMSI, the mobile wireless terminal 14 sends a P-TMSI reallocation complete acknowledgement to the new SGSN 20<sub>2</sub> during step 209.

The applicable GPRS and UMTS standards provide that the SGSN may reallocate the P-TMSI at any time. Such reallocation can occur during a P-TMSI Reallocation procedure, or as part of the 'Attach' or 'Routing Area Update' procedures. Updating the HLR 30 each time one of the SGSNs reallocates the P-TMSI could consume significant resources. Instead, HLR updating should be done upon receipt of a P-TMSI and P-TMSI signature from a SGSN only at the time of detachment, i.e. only at the time the last P-TMSI and P-TMSI signature are stored in the HLR 30. When a SGSN issues a new P-TMSI to a mobile wireless terminal 14 to replace the old P-TMSI, the SGSN waits for an acknowledgement before removing the old P-TMSI and using the new one.

In practice, the wireless telephony network 10 of FIG. 1 considers the old P-TMSI as invalid upon receipt of the P-TMSI Reallocation Complete acknowledgement message. If, for some reason, the SGSN receives no acknowledgement, and the mobile wireless terminal becomes detached, the SGSN will store both old and new P-TMSI for that terminal. Two proposed solutions address this problem:

#### Solution 1

##### The mobile wireless terminal 14 initiates detachment

To detach itself from the wireless telephony network 10 of FIG. 1, the mobile wireless terminal 14 sends a Detach Request message (Detach Type, P-TMSI, P-TMSI Signature, Switch Off) to its corresponding SGSN. In accordance with this proposed solution, the mobile wireless



terminal 14 will include its old P-TMSI in the Detach Request message. In this way, the SGSN will know which P-TMSI to store in the HLR 30.

The wireless telephony network 10 initiates detachment

5

To initiate detachment, the SGSN sends a Detach Request message to the mobile wireless terminal 14. In response, the mobile wireless terminal 14 sends a Detach Accept message to the SGSN. However, with a network-initiated detachment, no P-TMSI exchange occurs upon receipt of the request or acceptance messages to remove the P-TMSI ambiguity.

10 The UMTS 3GPP standard does not discuss P-TMSI reallocation and the possibility of a network-initiated detachment collision. Typically, the wireless telephony network 10 can wait until transmission of a P-TMSI Reallocation Completion acknowledgement message from the mobile wireless terminal 14 to the SGSN. The mobile wireless terminal 14 will then send the Detach Request message to the wireless telephony network 10 to avoid ambiguity when the  
15 terminal powers up again. In such an instance, the SGSN stores the new P-TMSI in the HLR 30.

Solution 2

20 Another proposed solution would require the SGSN to send both old and new P-TMSI to the HLR 30. Thus, at the time of attachment, the HLR 30, when queried by a new SGSN, can map whichever P-TMSI is sent by mobile wireless terminal 14 to the stored IMSI.

The foregoing describes a technique for protecting the identity of a mobile wireless terminal during attachment to a wireless telephony network.

## CLAIMS:

- 1           1.       A method for protecting the identity of a mobile wireless terminal during  
2 attachment to a wireless network, comprising the steps of:  
3           receiving in the network a request for access from a mobile wireless terminal previously  
4 registered with the network;  
5           querying at least one serving node in the wireless network to recognize the mobile  
6 wireless network in accordance with a temporary identity contained in the access request, but if  
7 no serving node recognizes the mobile wireless terminal, then  
8           launching a query from the one serving node to a register in the wireless network storing  
9 identity information of previously registered mobile wireless terminals to identify the mobile  
10 wireless from its temporary identity; and  
11           sending an identification response from register to the at least one serving node to  
12 identify the mobile wireless terminal.
- 1           2.       The method according to claim 1 further comprising the step of updating the  
2 register each time the temporary identity of the mobile wireless terminal is allocated (including  
3 allocation the very first time and reallocation).
- 1           3.       The method according to claim 1 further comprising the step of updating the register  
2 at detachment of the mobile wireless terminal from the wireless telephony network.
- 1           4.       The method according to claim 3 wherein the at least one serving node discards a  
2 stored temporary identity for the terminal upon receipt of a detachment request and an  
3 acknowledgement from the terminal.
- 1           5.       The method according to claim 4 further comprising the step of storing in the at  
2 least one serving node a temporary identity contained in the detachment request when the  
3 mobile wireless terminal initiates detachment.

1           6.       The method according to claim 3 further comprising the step of storing a new  
2 temporary identity for the mobile wireless terminal following temporary identity reallocation  
3 when the wireless telephony network initiates detachment of the mobile wireless terminal.

1           7.       The method according to claim 1 further comprising the step of storing both new  
2 and old temporary identities for the mobile wireless terminal in the register following a  
3 temporary identity reallocation.

1           8.       A wireless network for protecting the identity of a mobile wireless terminal  
2 during attachment, comprising:  
3           at least one serving node for receiving a request for access from a mobile wireless  
4 terminal previously registered with the network and for identifying the terminal in accordance  
5 with a temporary identity contained in the access request when the serving node has knowledge  
6 of the terminal; and  
7           a register in the wireless network storing identity information of previously registered  
8 mobile wireless terminals to identify the mobile wireless from its temporary identity in response  
9 to a query from the at least one serving node when the one node lacks knowledge of the  
10 terminal.

          9.       The network according to claim 8 wherein the register is updated each time the  
temporary identity of the mobile wireless terminal is allocated.

1           10.      The network according to claim 8 wherein the register undergoes updating at  
2 detachment of the mobile wireless terminal from the wireless telephony network.

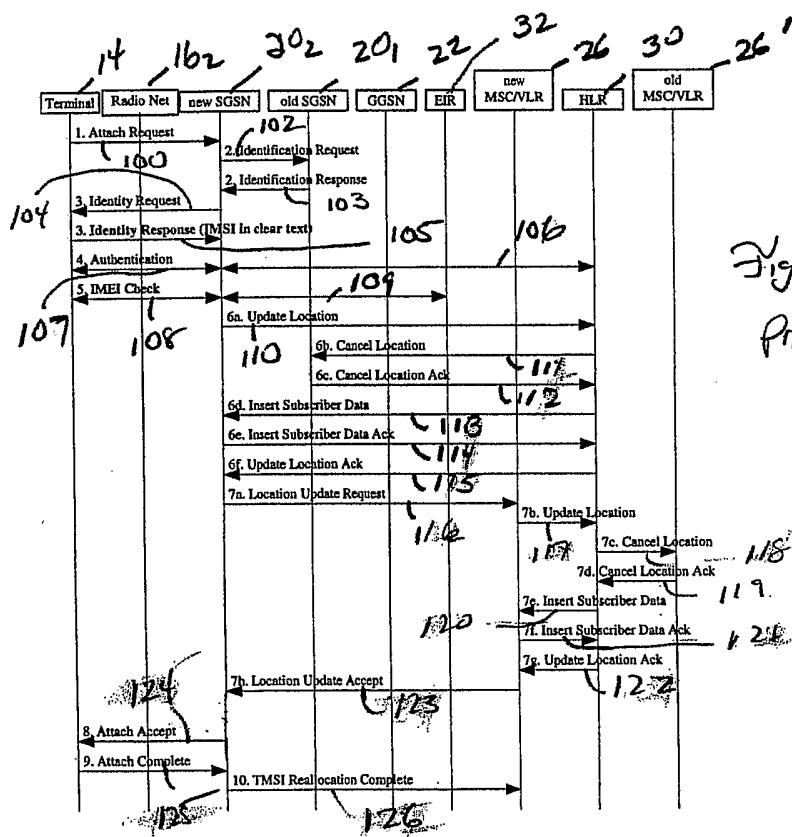
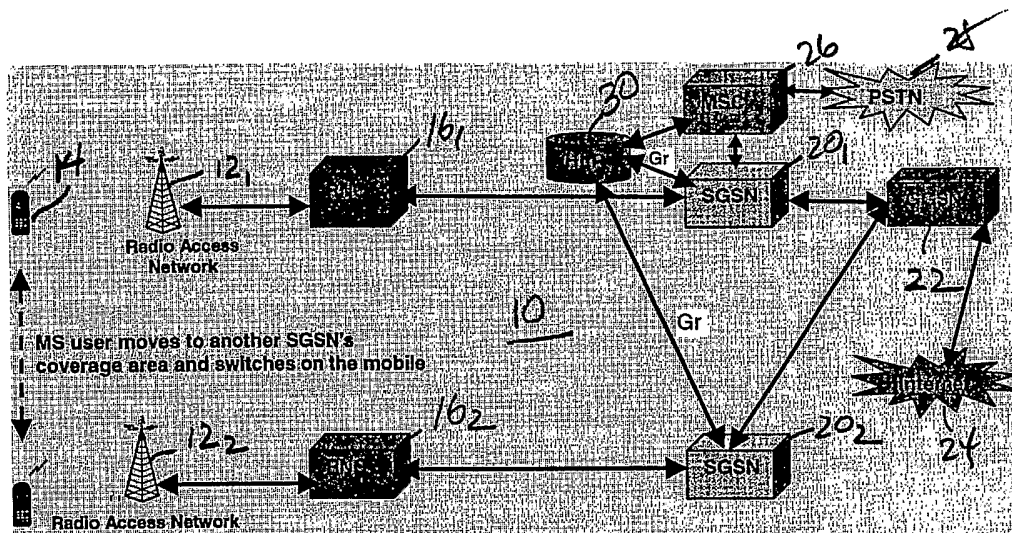
1           11.      The network according to claim 10 wherein the at least one serving node discards  
2 a stored temporary identity for the terminal upon receipt of a detachment request and an  
3 acknowledgement from the terminal.

1           12.      The network according to claim 11 wherein the at least one serving node stores a  
2 temporary identity contained in the detachment request when the mobile wireless terminal  
3 initiates detachment.

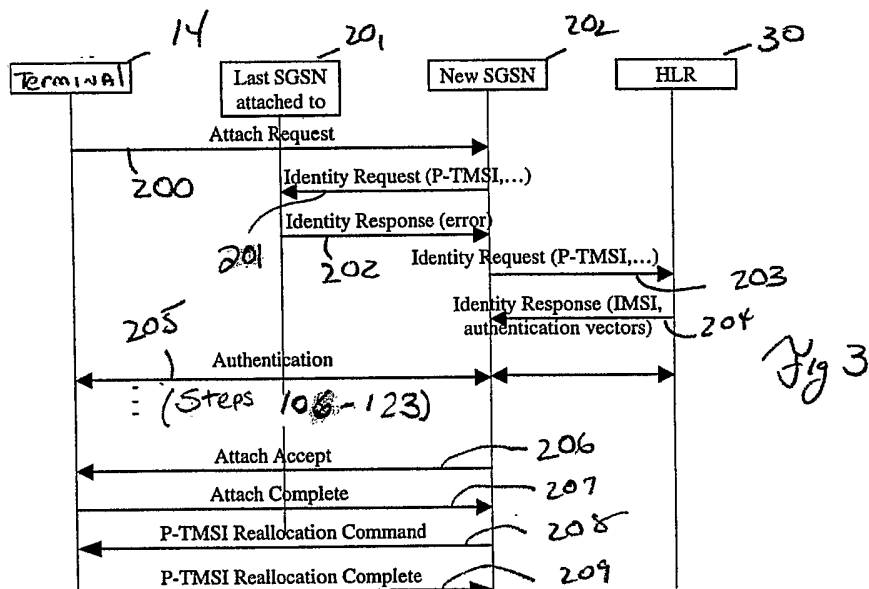
1           13.    The network according to claim 12 wherein the at least one serving node stores a  
2   new temporary identity for the mobile wireless terminal following temporary identity  
3   reallocation when the wireless telephony network initiates detachment of the mobile wireless  
4   terminal.

1           14.    The network according to claim 8 wherein the register stores both new and old  
2   temporary identities for the mobile wireless terminal following a temporary identity  
3   reallocation.

1/2



2/2



# INTERNATIONAL SEARCH REPORT

International application No.

PCT/US03/25131

## A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : H04M 3/16  
US CL : 455/410,411

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)  
U.S. :

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)  
East

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6, 167,279 A (CHANG ET AL.) 26 December 2000, column 4, line 63 - column 5, line 3.	1-14

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

☐ See patent family annex.

* Special categories of cited documents:	"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
"A" document defining the general state of the art which is not considered to be of particular relevance	"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
"E" earlier application or patent published on or after the international filing date	"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
"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)	"&" document member of the same patent family
"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	

Date of the actual completion of the international search

20 November 2003 (20.11.2003)

Date of mailing of the international search report

05 DEC 2003

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. (703)305-3230

Authorized officer

Huy Nguyen

Telephone No. 703-305-3283