US 20040087305A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2004/0087305 A1**

Jiang et al. (43) **Pub. Date: May 6, 2004**

(54) **METHOD AND SYSTEM FOR CELLULAR NETWORK TRAFFIC REDIRECTION**

(76) Inventors: **Yue Jun John Jiang**, Danville, CA (US); **Avnish Chauhan**, Cuperino, CA (US); **Subhabrata Biswas**, Mumbai (IN); **Bahadur Bhambhani**, Mumbai (IN); **Alex Rodrigues**, Mumbai (IN)

Correspondence Address:
Shemwell Gregory & Courtney LLP
Suite 201
4880 Stevens Creek Boulevard
San Jose, CA 95129 (US)

(21) Appl. No.: **10/635,804**

(22) Filed: **Aug. 5, 2003**

Related U.S. Application Data

(60) Provisional application No. 60/401,362, filed on Aug. 5, 2002.

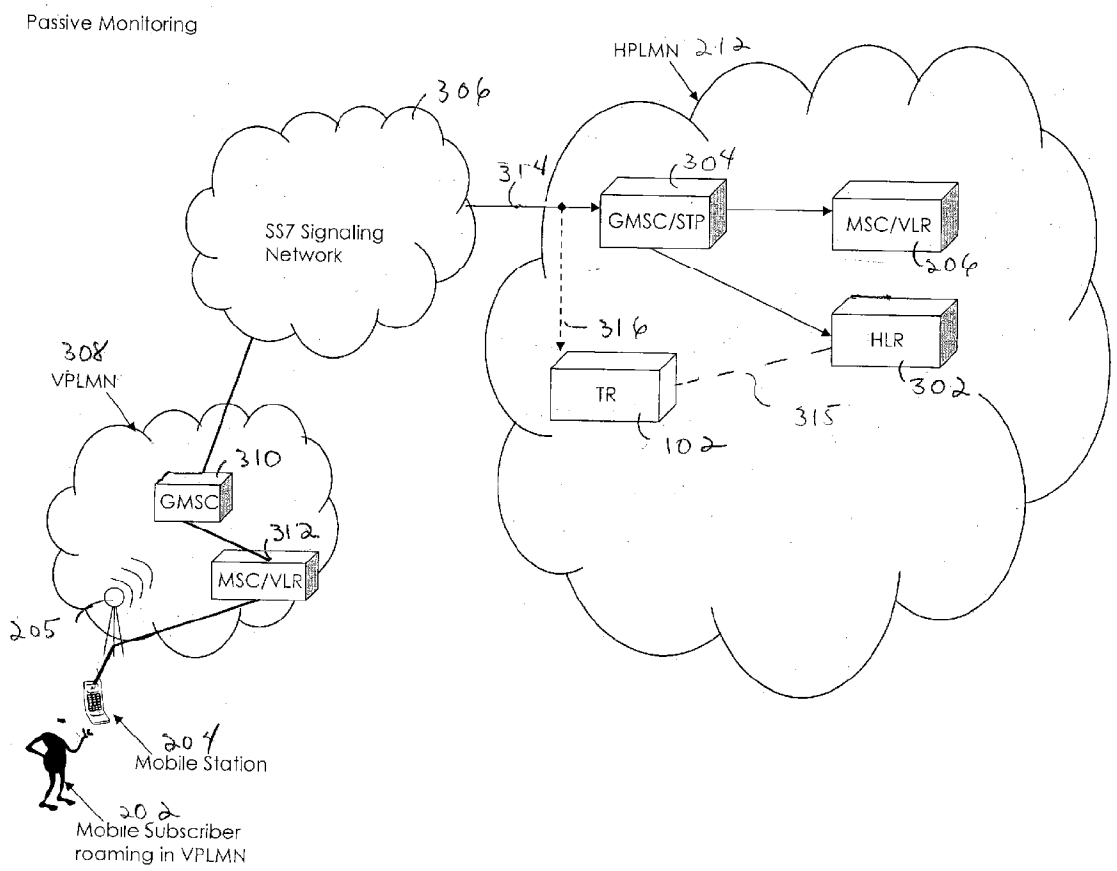
Publication Classification

(51) **Int. Cl.**[7] **H04Q 7/20**

(52) **U.S. Cl.** **455/432.1**; 455/436; 455/448

(57) **ABSTRACT**

A system and apparatus for redirecting wireless network traffic. Embodiments include determining when a roaming mobile station initiates a registration attempt with a non-preferred network and causing the roaming mobile station to initiate a registration attempt with a preferred network. Embodiments further include a traffic redirection network entity including a traffic redirection node, a traffic redirection application, and a traffic redirection probe.



APPLE 1039

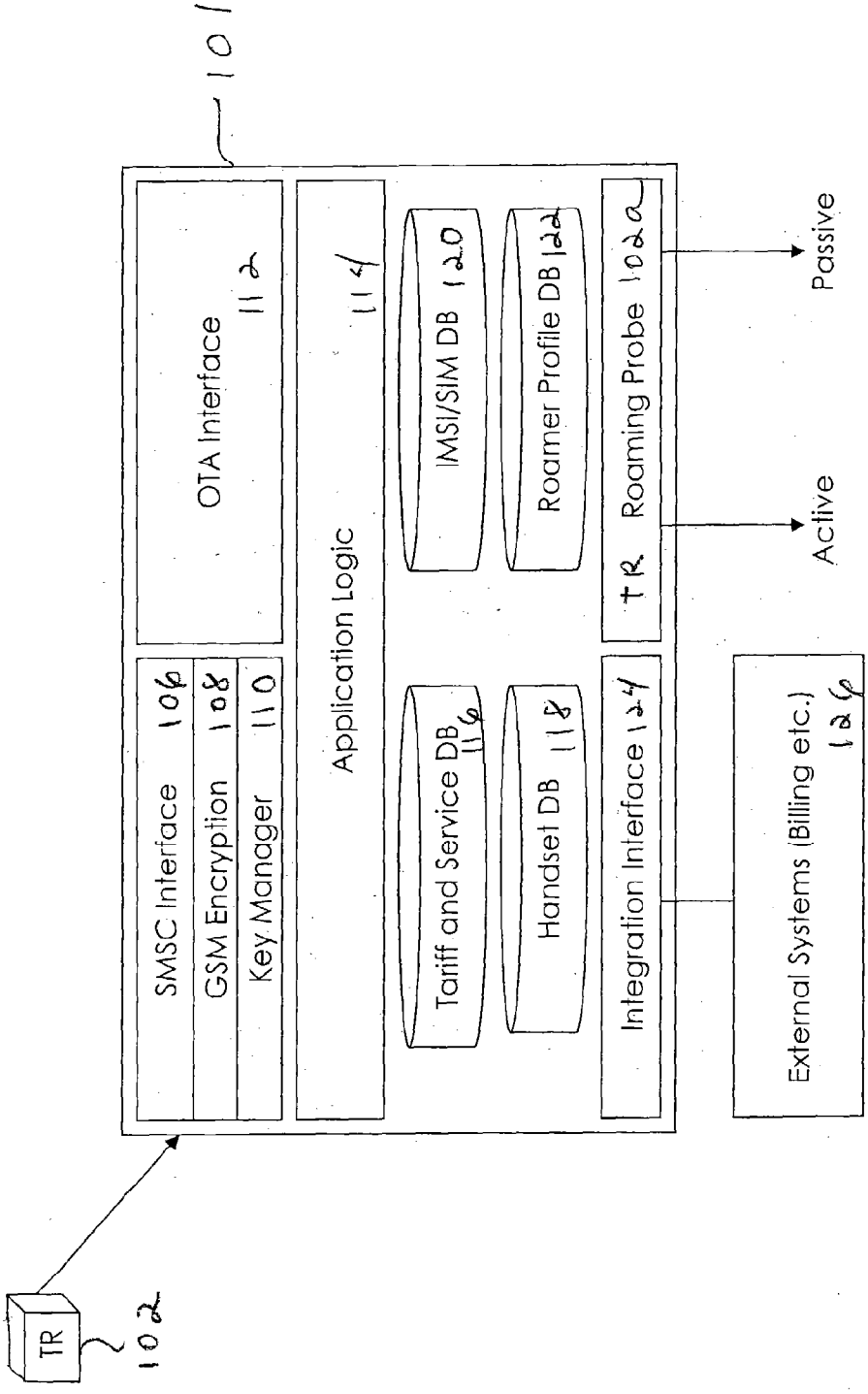
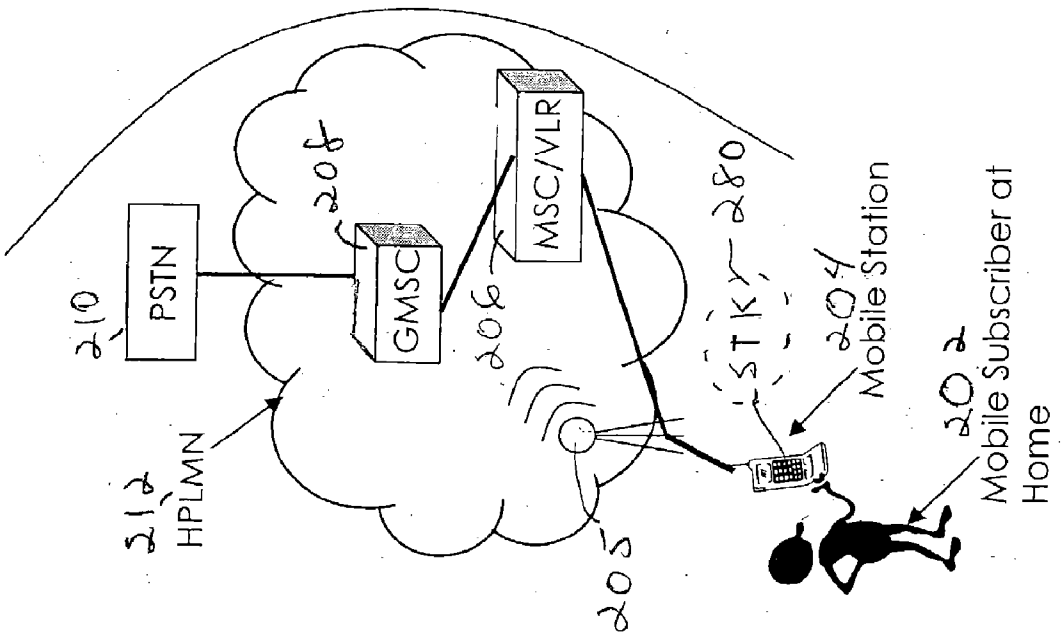

100
101
SMSC Interface 106
GSM Encryption 108
Key Manager 110
OTA Interface 112
Application Logic 114
IMSI/SIM DB 120
Roamer Profile DB 122
Tariff and Service DB 116
Handset DB 118
TR Roaming Probe 102a
Integration Interface 124
External Systems (Billing etc.) 126
Passive
Active
TR
102

Figure 1

Figure 2


210
PSTN
208
GMSC
MSC/VLR
206
STK
280
204
Mobile Station
202
Mobile Subscriber at Home
212
HPLMN
205

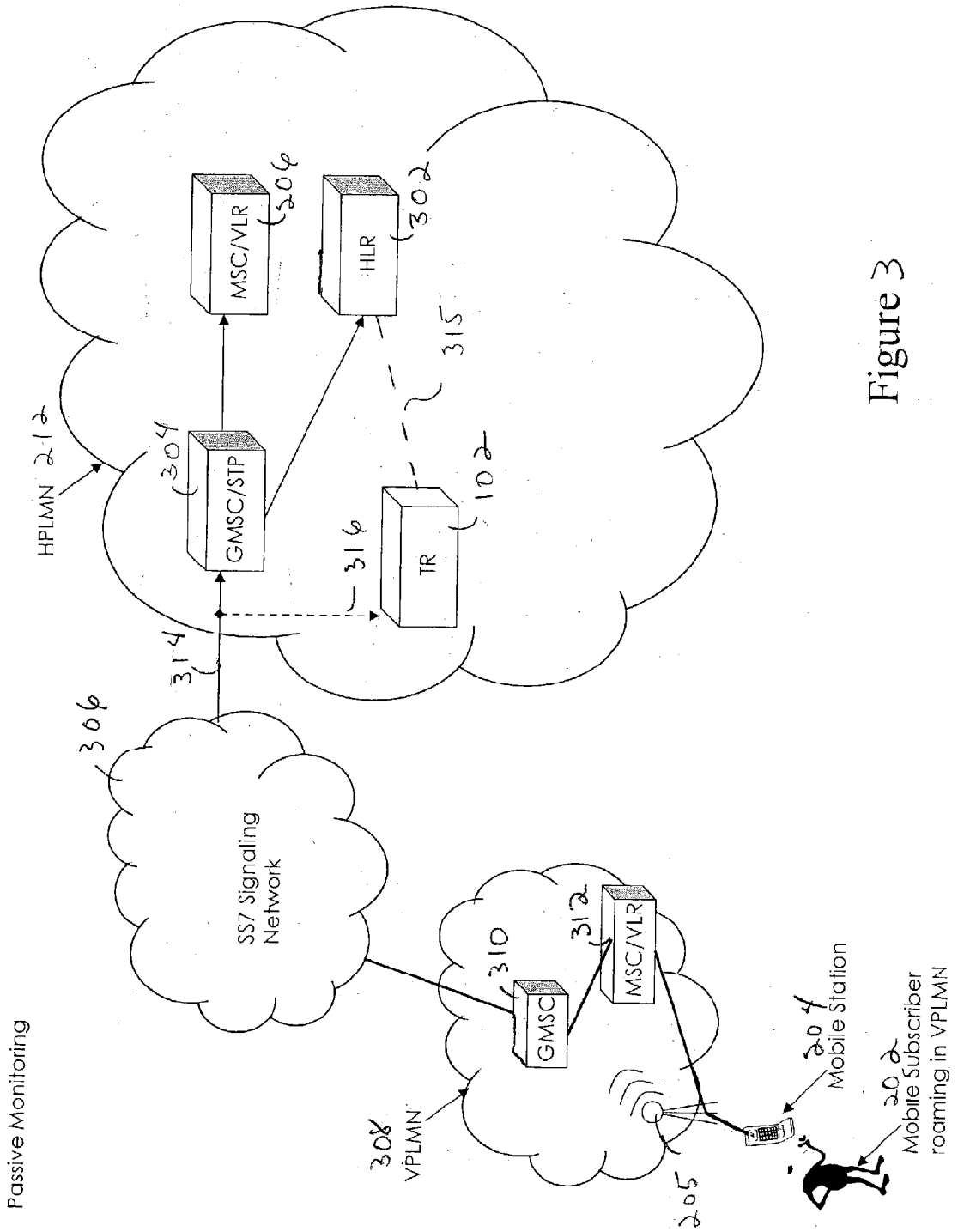

HPLMN 212
MSC/VLR
306
HLR
302
304
GMSC/STP
315
316
TR
102
314
306
SS7 Signaling Network
310
GMSC
312
MSC/VLR
308
VPLMN
205
204
Mobile Station
202
Mobile Subscriber roaming in VPLMN
Passive Monitoring

Figure 3

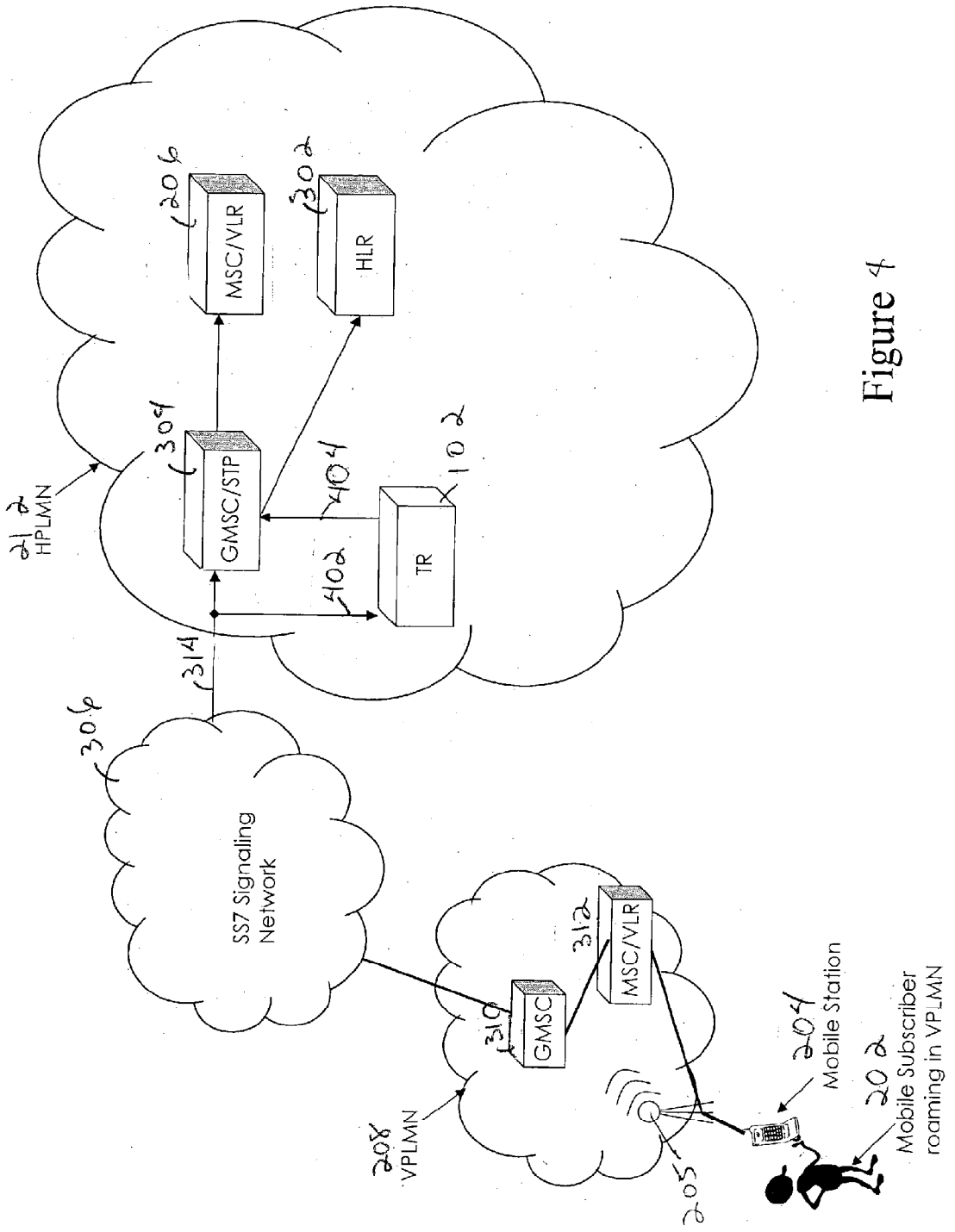

HPLMN
GMSC/STP
MSC/VLR
HLR
TR
SS7 Signaling Network
VPLMN
GMSC
MSC/VLR
Mobile Station
Mobile Subscriber roaming in VPLMN

Figure 4

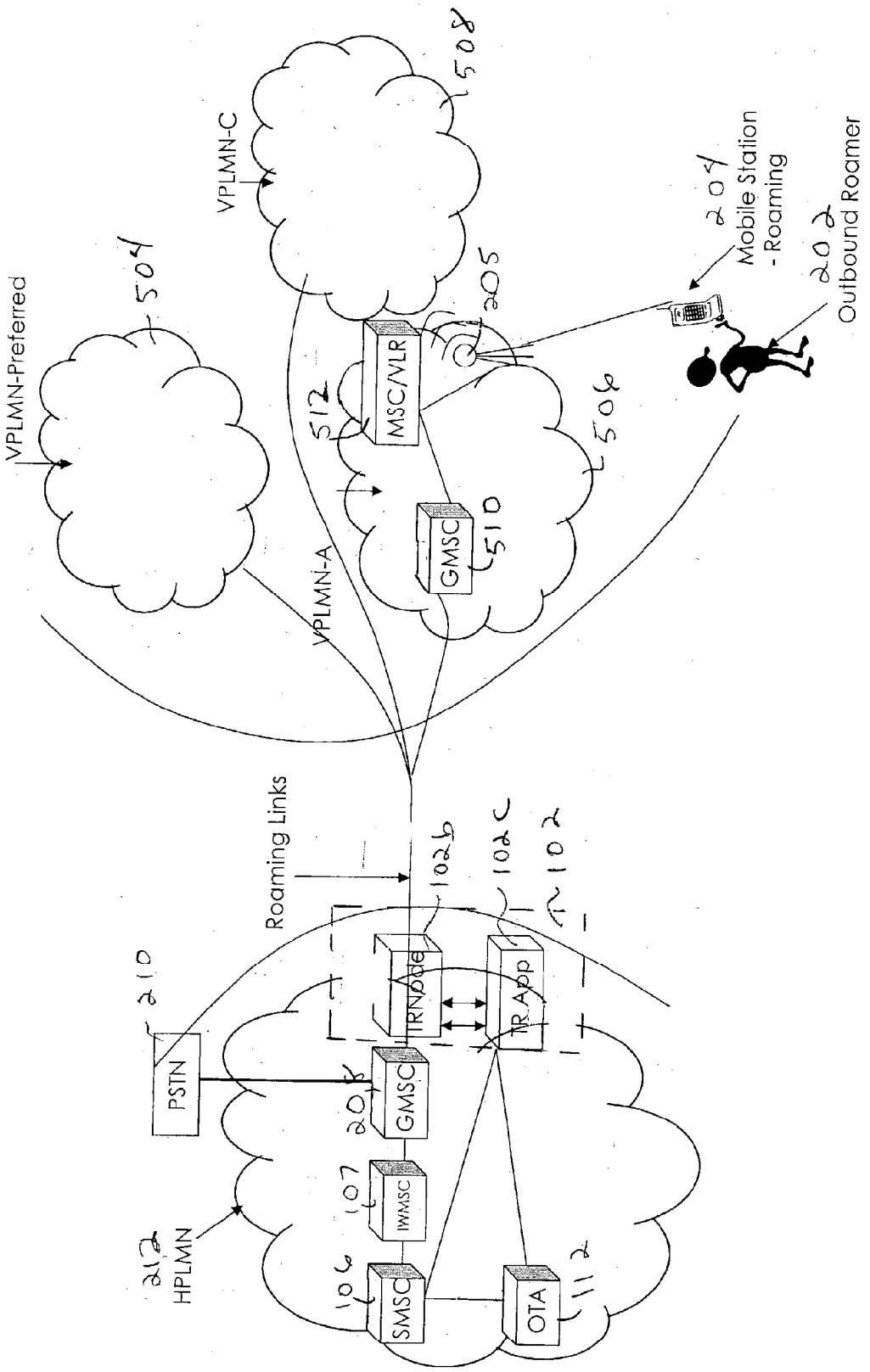

VPLMN-Preferred
504
VPLMN-C
508
VPLMN-A
MSC/VLR
512
GMSC
510
505
506
204
Mobile Station
- Roaming
202
Outbound Roamer
Roaming Links
1026
1024
102
IRN Node
IR App
210
PSTN
GMSC
208
107
IWMSC
106
SMSC
212
HPLMN
OTA
112

Figure 5

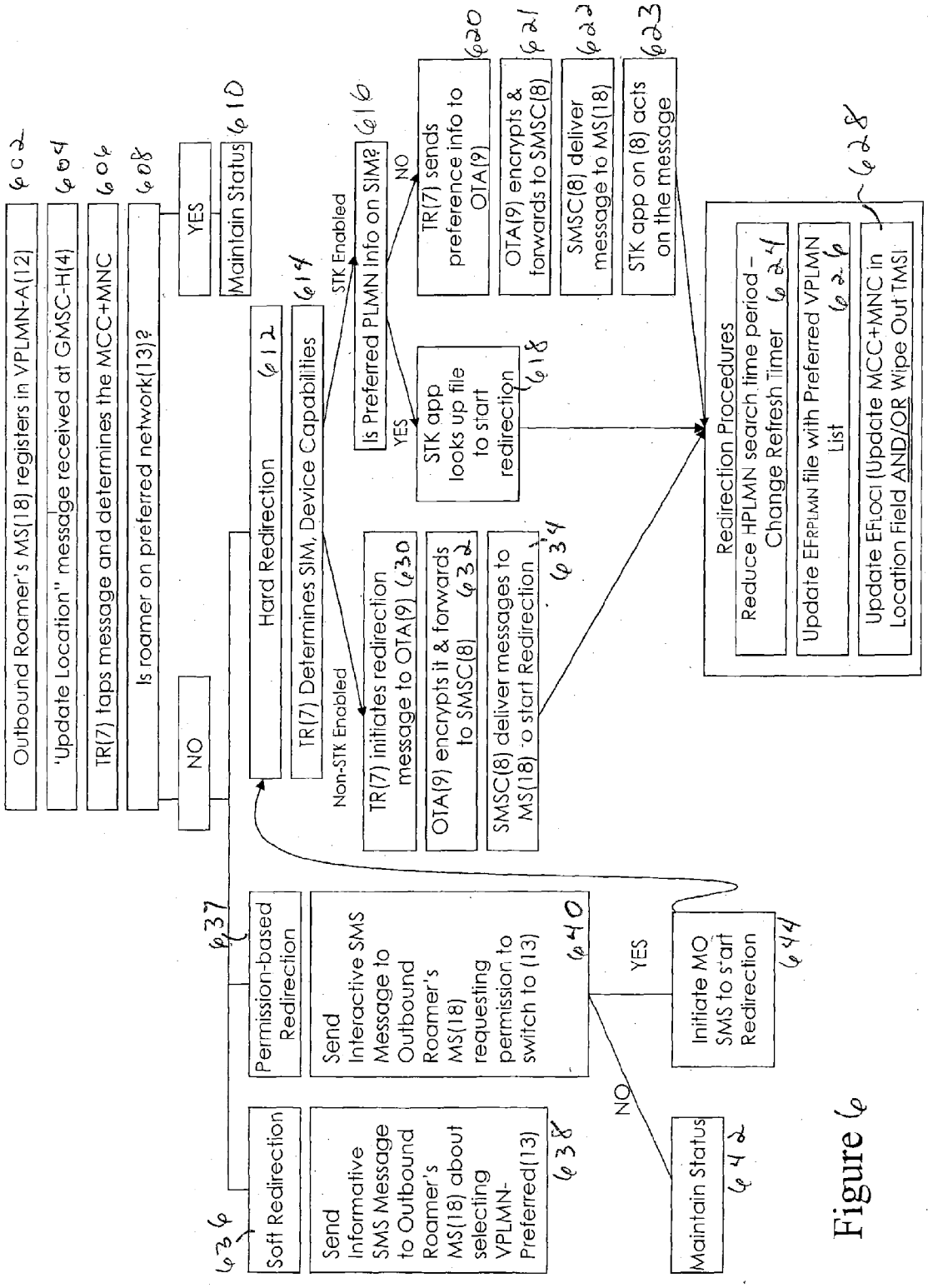

Outbound Roamer's MS(18) registers in VPLMN-A(12)
'Update Location" message received at GMSC-H(4)
TR(7) taps message and determines the MCC+MNC
Is roamer on preferred network(13)?
NO
YES
Maintain Status
Hard Redirection
TR(7) Determines SIM, Device Capabilities
Non-STK Enabled
STK Enabled
TR(7) initiates redirection message to OTA(9)
OTA(9) encrypts it & forwards to SMSC(8)
SMSC(8) deliver messages to MS(18) to start Redirection
Is Preferred PLMN info on SIM?
YES
NO
STK app looks up file to start redirection
TR(7) sends preference info to OTA(9)
OTA(9) encrypts & forwards to SMSC(8)
SMSC(8) deliver message to MS(18)
STK app on (8) acts on the message
Redirection Procedures
Reduce HPLMN search time period – Change Refresh Timer
Update EFFPLMN file with Preferred VPLMN List
Update EFLOCI (Update MCC+MNC in Location Field AND/OR Wipe Out TMSI
Soft Redirection
Permission-based Redirection
Send Informative SMS Message to Outbound Roamer's MS(18) about selecting VPLMN-Preferred(13)
Send Interactive SMS Message to Outbound Roamer's MS(18) requesting permission to switch to (13)
NO
YES
Maintain Status
Initiate MO SMS to start Redirection

Figure 6

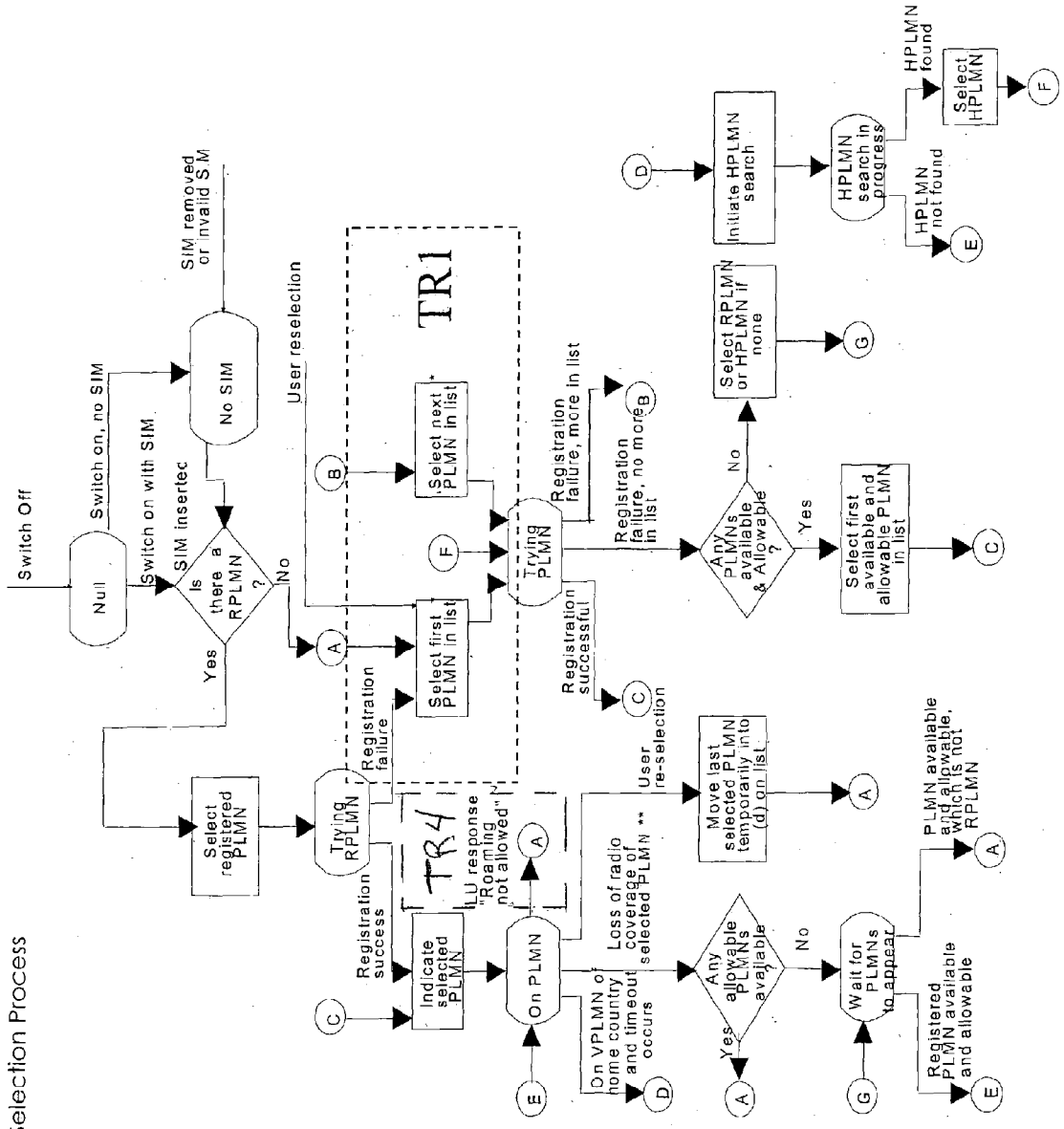

Automatic Network Selection Process
Switch Off
Null
Switch on, no SIM
Switch on with SIM
SIM inserted
Is there a RPLMN ?
Yes
No
No SIM
SIM removed or invalid SIM
User reselection
Select registered PLMN
Trying RPLMN
Registration failure
Select first PLMN in list
Select next PLMN in list
TR1
Registration success
Indicate selected PLMN
TR4
LU response "Roaming not allowed"
On PLMN
Loss of radio coverage of selected PLMN **
On VPLMN or home country and timeout occurs
Any allowable PLMNs available
Yes
No
Move last selected PLMN temporarily into (d) on list
User re-selection
Wait for PLMNs to appear
Registered PLMN available and allowable
PLMN available and allowable, which is not RPLMN
Trying PLMN
Registration successful
Registration failure, more in list
Registration failure, no more
Any PLMNs available & Allowable ?
Yes
No
Select first available and allowable PLMN in list
Select RPLMN or HPLMN if none
Initiate HPLMN search
HPLMN search in progress
HPLMN found
HPLMN not found
Select HPLMN

Figure 7

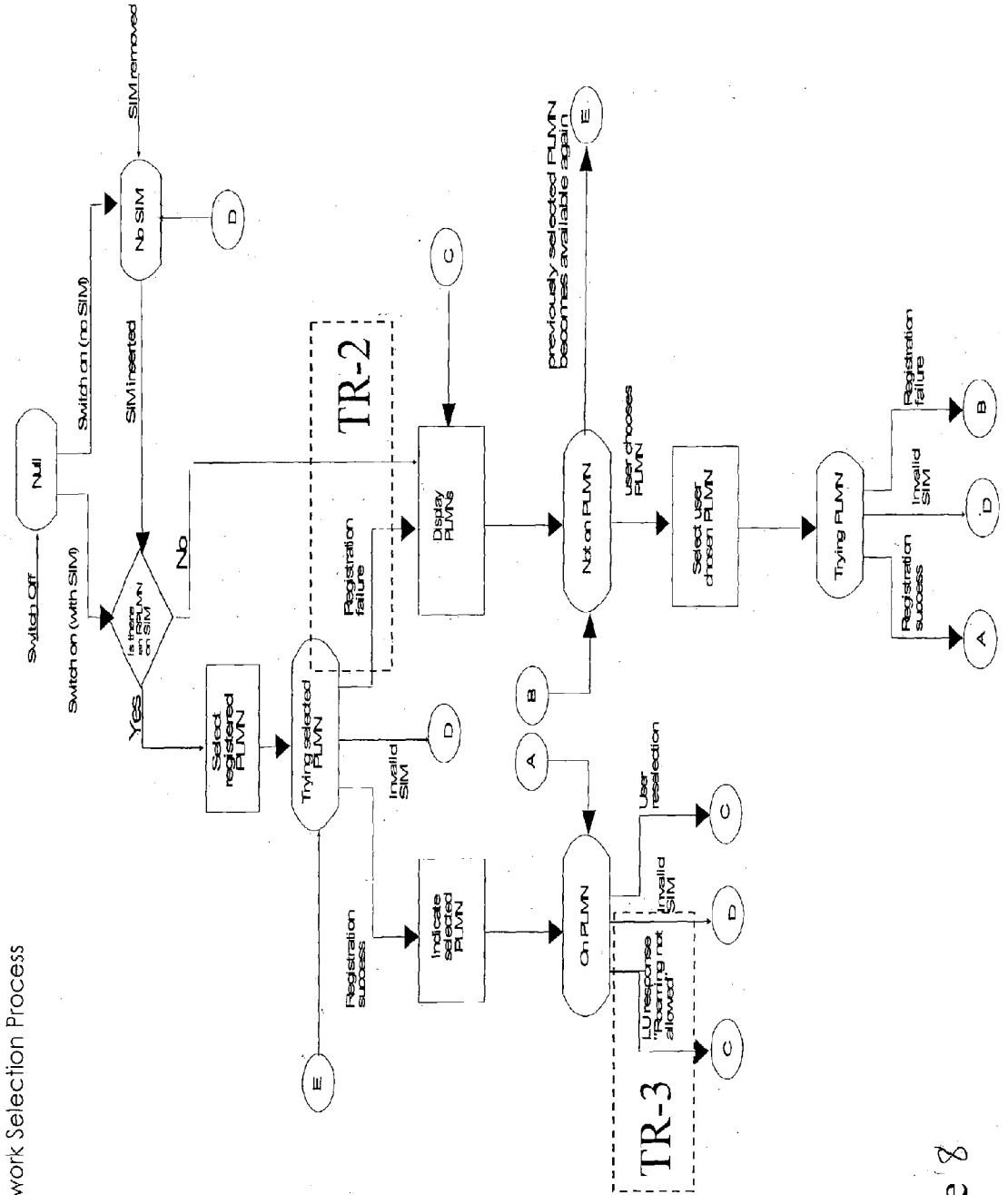

Manual Network Selection Process
Null
Switch Off
Switch on (with SIM)
Switch on (no SIM)
SIM removed
SIM inserted
No SIM
Is there an RPLMN on SIM
YES
No
Select registered PLMN
Trying selected PLMN
Registration failure
Registration success
Invalid SIM
Indicate selected PLMN
Display PLMNs
Not on PLMN
On PLMN
User reselection
LU response "Roaming not allowed"
previously selected PLMN becomes available again
User chooses PLMN
Select user chosen PLMN
Trying PLMN
TR-2
TR-3
A
B
C
D
E

Figure 8

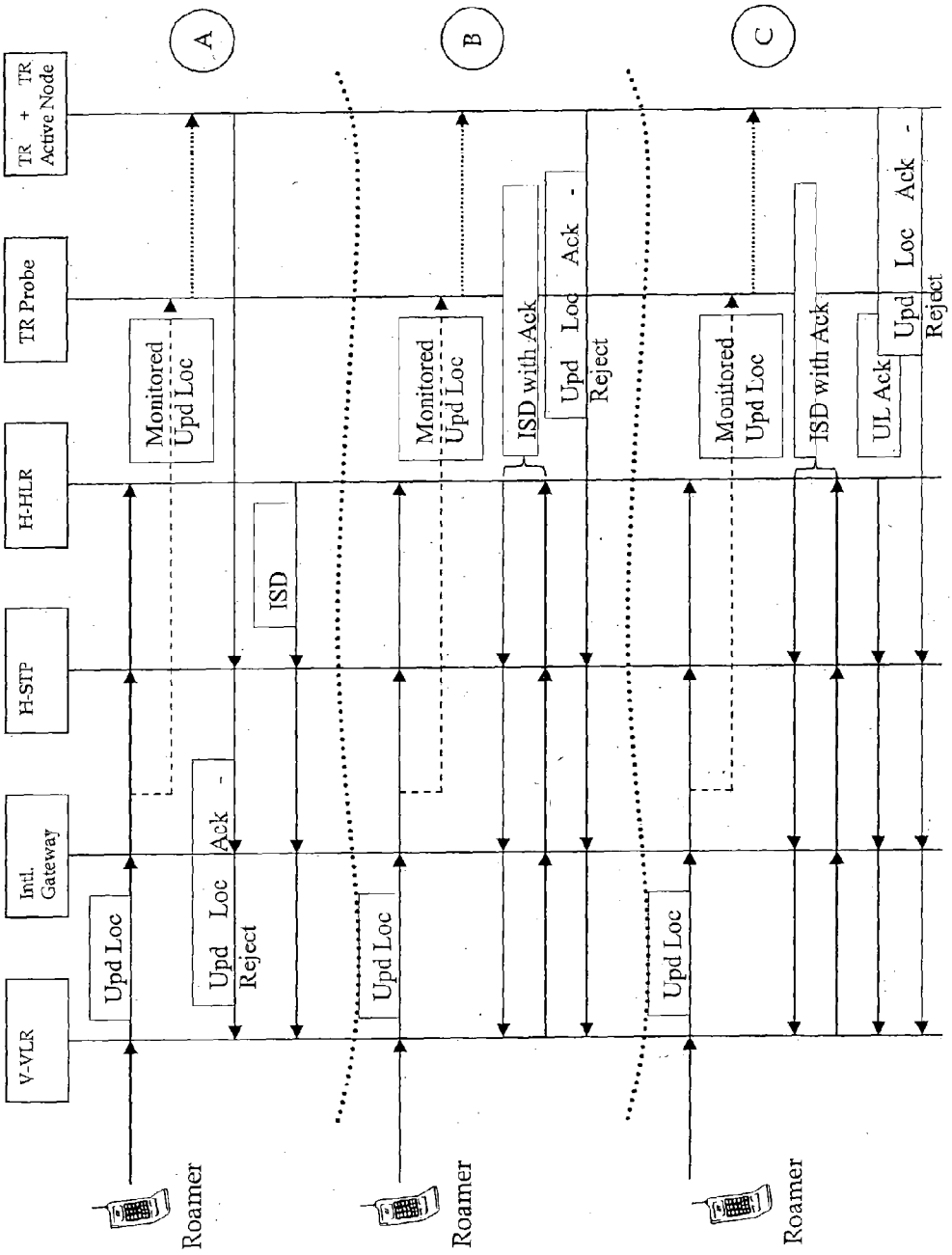

V-VLR
Intl. Gateway
H-STP
H-HLR
TR Probe
TR + TR Active Node
A
B
C
Upd Loc
Upd Loc Reject
Ack -
ISD
Monitored Upd Loc
ISD with Ack
Upd Loc Reject
Ack -
Monitored Upd Loc
ISD with Ack
UL Ack
Upd Loc Reject
Ack -
Roamer
Roamer
Roamer

Figure 9

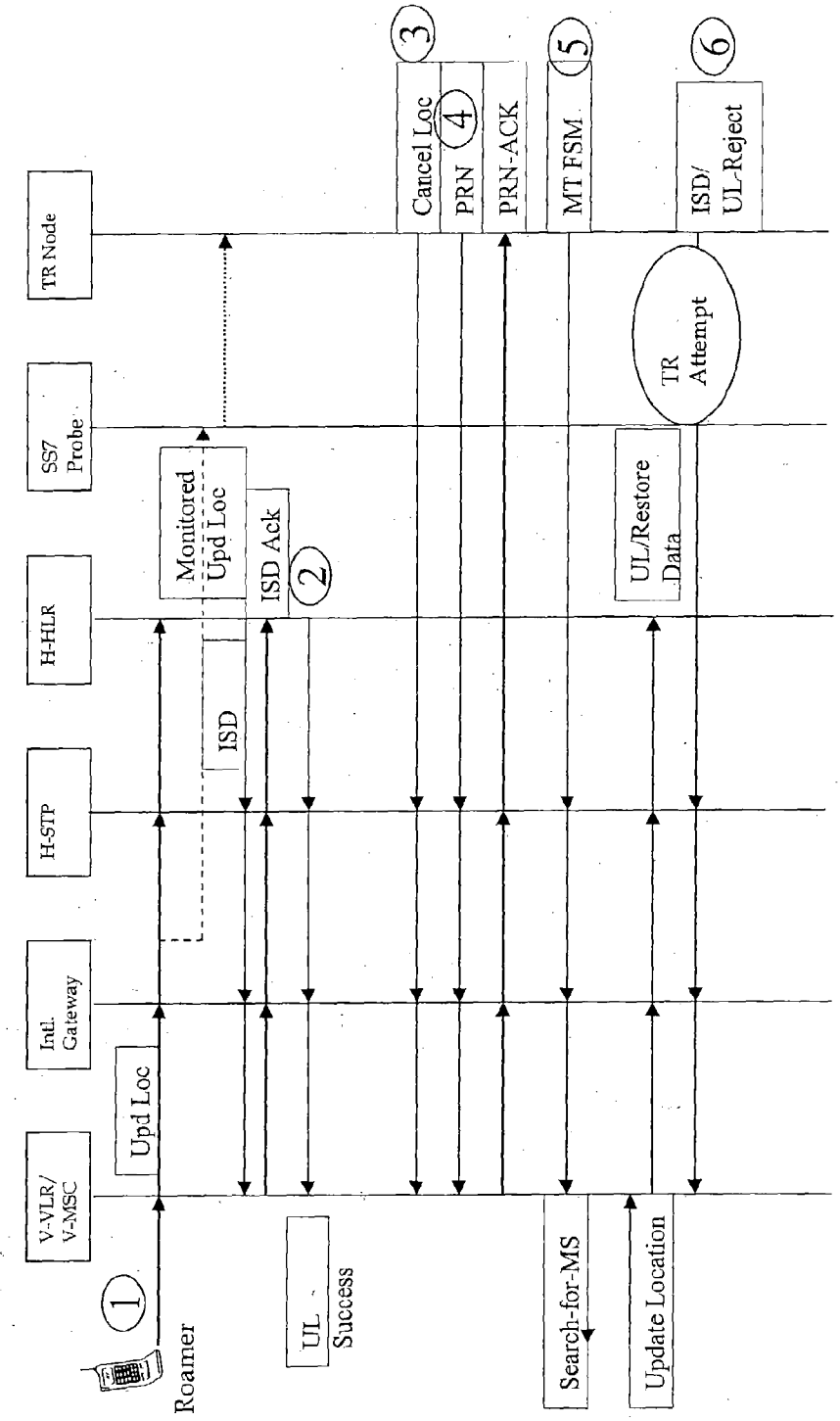

V-VLR/ V-MSC
Intl. Gateway
H-STP
H-HLR
SS7 Probe
TR Node
Roamer
Upd Loc
ISD
Monitored Upd Loc
ISD Ack
UL Success
Cancel Loc
PRN
PRN-ACK
MT FSM
Search-for-MS
Update Location
UL/Restore Data
TR Attempt
ISD/ UL-Reject
1
2
3
4
5
6

Figure 10

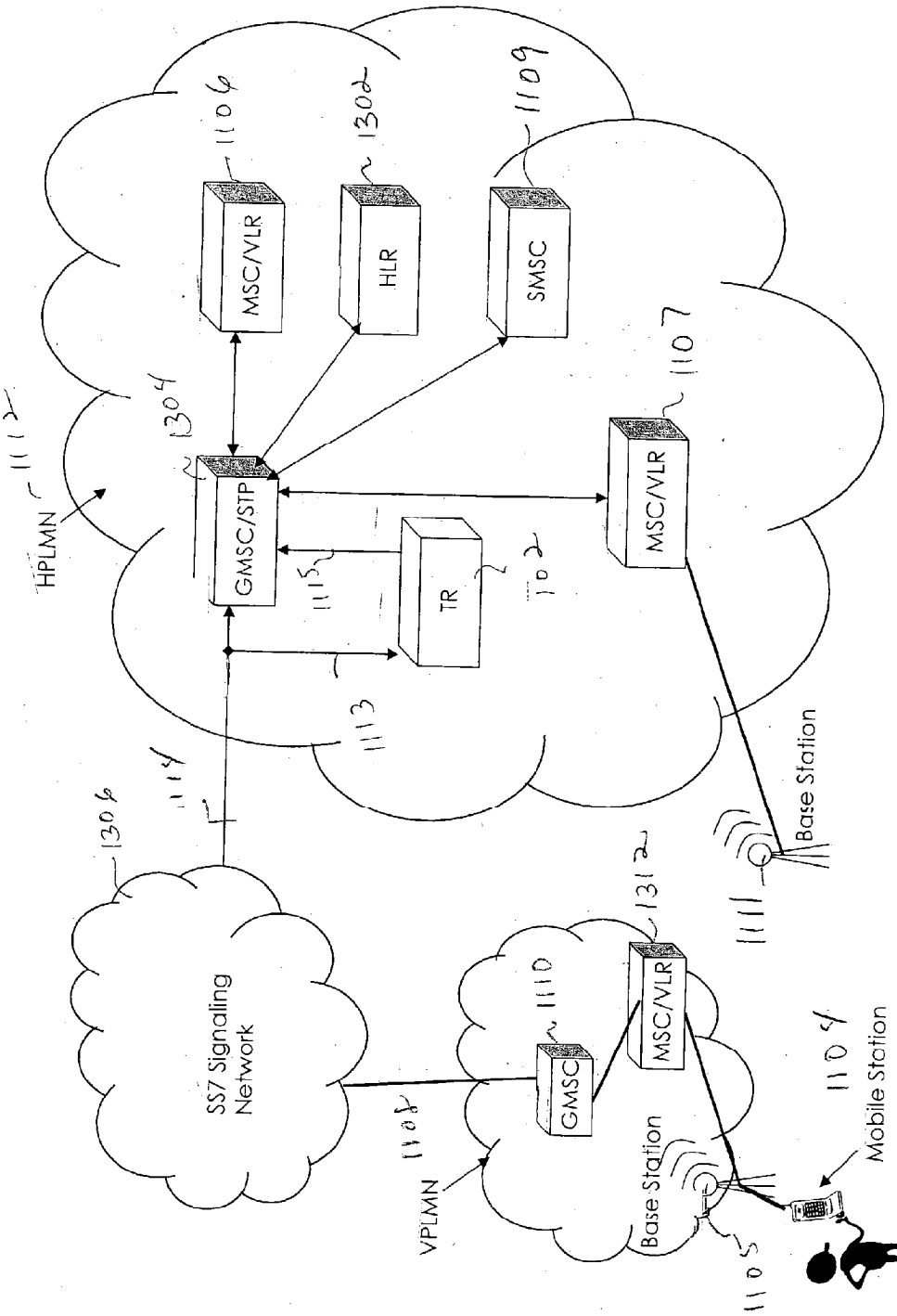

HPLMN
1112
1106
MSC/VLR
1302
HLR
1109
SMSC
1304
GMSC/STP
1115
TR
1102
1107
MSC/VLR
1113
1114
1306
Base Station
1111
SS7 Signaling Network
1312
1110
GMSC
MSC/VLR
1104
Mobile Station
1108
VPLMN
Base Station
1105
1103
Mobile Subscriber roaming in VPLMN

Figure 11

METHOD AND SYSTEM FOR CELLULAR NETWORK TRAFFIC REDIRECTION

RELATED APPLICATIONS

[0001] This application claims priority from U.S. Provisional Patent Applications Serial No. 60/401,362, entitled TRAFFIC REDIRECTION, filed Aug. 5, 2002.

TECHNICAL FIELD

[0002] The disclosed embodiments relate to methods and system for directing cellular network traffic.

BACKGROUND

[0003] There are many mobile or cellular network operators, or providers, in the world, often more than one in a single country. These network operators include, but are not limited to, operators who provide mobility services using GSM, GPRS, 3G, CDMA, TDMA, PHS, WCDMA, IDEN and WLL technology or their variants. These network operators provide voice and data services to their own subscribers and to subscribers from other networks. When the network operator provides service to a subscriber from a foreign country, it is referred to as "international roaming". When the network operator provides service to a subscriber from another network in the same country, it is referred to as "domestic roaming".

[0004] When the subscriber is registered in the network with which it has a direct billing relationship, the serving network is often referred to as the Home Public Mobile Network or HPMN. If the subscriber is in a network with which it does not have a direct billing relationship, the serving network is referred to as the Visited Public Mobile Network or VPMN, and the subscriber is referred to as an in-roamer by the VPMN. The same subscriber is referred to as an out-roamer by the HPMN. In such a case, the in-roamers are treated as temporary subscribers from a service availability perspective, while the billing for usage incurred by them is through inter-carrier settlements via the home network of the subscriber.

[0005] Various network operators have partnership agreements with each other that include more favorable roaming charges than non-partners receive. Partner networks are "preferred" networks for the network operator's subscriber to register with when roaming. Non-partner networks are "non-preferred" networks to the subscriber. Network operators can maximize their margins and the roamers can get more attractive roaming rates and services if roamers roam on their home mobile operator's preferred partner networks.

[0006] When "home" subscribers roam into visited networks, they may roam onto one, two or more VPMNs, any one at a time, based on various criteria. To better understand this, consider the cases when the handset can be in one of two modes: automatic network selection mode; or manual network selection mode.

[0007] In automatic mode, the handset automatically uses a set of rules to find the network to register with. The order of these rules may be handset vendor dependent; however, industry specifications state the order as:

[0008] 1. The last selected network (from EFLOCI on the SIM card);

[0009] 2. The home network if its available (based on MCC and MNC from IMSI);

[0010] 3. If the last registered network is not found, the handset tries to register on the list of networks from the Preferred PLMN List (EFPLMNSEL on SIM card) in priority order excluding the previously selected PLMN (the handset scans the GSM 900 frequency band before it scans the GSM 1800 frequency band);

[0011] 4. Other PLMN with a received signal level above −85 dBm in random order excluding the previously selected PLMN; and

[0012] 5. Any other PLMN excluding the previously selected PLMN in order of decreasing signal strength or alternatively the previously selected PLMN may be chosen ignoring its signal strength.

[0013] In manual mode, the handset shows a list of available networks to the user. The user selects one of them and the handset attempts registration onto that network. If the registration is not successful, the handset shows the list of networks to the user once again. In manual mode, the user has selected a particular network, so preferred VPMN selection from the HPMN perspective should not apply. However, a majority of current handsets are in automatic selection mode, and the HPMN is keen on controlling and/or influencing the roaming network chosen by its out-roamers. Also, since the HPMN would like to honor the manual selection mode, it has to identify the current settings on the handset. However, implementing a seamless mechanism to do this has been a challenge thus far.

[0014] Over the last few years, the revenues to network operators from home subscribers have consistently declined due to increased competition and resulting pricing pressures. On the other hand, revenues from roamers have consistently grown in the same period due to increased mobile penetration in local markets and an increase in travel. Moreover, roaming revenues are high-margin revenues that typically comprise between 8-25% of the total network operator revenues. Hence, protecting the existing roaming revenues and growing them further has become an important priority for the network operators worldwide.

[0015] Some operators also own networks in various countries. These operators would like to make sure their out-roamers stay within the group properties, or stay on preferred networks, in order to gain the best service experience even when roaming. They will also be able to offer geography based price plans (for example, a single rate all across Western Europe or South East Asia) to users who have subscribed to such plans. In addition, as new technologies keep rolling out, they can control the rollout schedule across their own properties and also make sure interoperability issues are taken care of. Keeping roaming subscribers on preferred networks gives the best service experience to the subscriber. However, current methods of controlling which network a subscriber registers on when roaming have disadvantages.

[0016] For example, a commonly-used method of attempting to prevent roaming subscribers from registering with non-preferred networks includes storing a list of preferred networks on a SIM in the subscriber's handset (a Preferred PLMN list). The list can be burned on the SIM or updated using Over-The-Air (OTA) messages. This list influences

the initial selection of the preferred network. However, due to various reasons (for example, the preferred network is not currently available or there is a temporary loss of coverage), the handset may also select a non-preferred network. The existing approach cannot control this situation and hence once the user is on a non-preferred network, he/she will remain there unless the non-preferred network loses the radio coverage. Even when the handset is powered off, the non-preferred network stays on the SIM card and on next power on it will be selected according to rules described herein. Thus, once the handset initiates an attempt to register on a non-preferred network, the network operator loses control of the roamer.

[0017] It would be advantageous for the network operator to retain some control over a roaming subscriber handset even when a handset has initiated a registration attempt with a non-preferred network for any reason, such as failure of the SIM network list to produce registration on a preferred network.

BRIEF DESCRIPTION OF THE FIGURES

[0018] In the drawings, the same or similar reference numbers identify similar elements or acts.

[0019] **FIG. 1** is a block diagram of an embodiment of a traffic redirection system.

[0020] **FIG. 2** is a block diagram of an embodiment of a traffic redirection system that shows one of the network operator's subscribers within the subscriber's home network.

[0021] **FIG. 3** is a block diagram of an embodiment of a traffic redirection system illustrating passive monitoring.

[0022] **FIG. 4** is a block diagram of an embodiment of a traffic redirection system illustrating active monitoring.

[0023] **FIG. 5** is a block diagram of an embodiment of a traffic redirection system illustrating Over-The-Air (OTA) based traffic redirection.

[0024] **FIG. 6** is a flow diagram of an embodiment of OTA traffic redirection.

[0025] **FIG. 7** is a flow diagram illustrating the interaction of an embodiment of traffic redirection with automatic network selection.

[0026] **FIG. 8** is a flow diagram illustrating the interaction of an embodiment of traffic redirection with manual network selection.

[0027] **FIG. 9** is a diagram of a call flow according to one traffic redirection embodiment.

[0028] **FIG. 10** is a diagram of a call flow according to one traffic redirection embodiment.

[0029] **FIG. 11** is a block diagram of an embodiment of a traffic redirection system with national or border roaming and traffic redirection.

DETAILED DESCRIPTION

[0030] A method and system are described for redirecting wireless network voice and data traffic under control of a network operator when a subscriber is roaming. Various embodiments of the invention include redirecting a handset when the handset has initiated a registration attempt with a non-preferred network. Various embodiments of the invention include redirecting a handset when the handset attempts to register with a non-preferred network. Various embodiments of the invention include redirecting a handset after the handset successfully registers with a non-preferred network. The embodiments described can be used as a complement to existing traffic redirection methods, such as preferred PLMN lists. More than one approach can be combined to enhance the user experience. The various traffic redirection methods described are transparent to the subscriber. An Appendix includes an explanation of numerous acronyms used herein and is included below for reference. Therefore, various acronyms used may not be spelled out in the body of the document.

[0031] Herein terms such as handset, subscriber, user, etc., may be used interchangeably to indicate an actor that is registering with a network. These terms are used for convenience, but in fact, the actor that registers with the network could be any combination of hardware and software capable of registering on a wireless network, e.g., a personal digital assistant (PDA) or personal computer (PC). The method and system described apply to any network entity that can register with one of several networks.

[0032] Embodiments described herein include OTA traffic redirection methods and "registration rejection" traffic redirection methods.

[0033] OTA methods include the following components: detecting the network the roamer is currently on; traffic redirection (TR) application logic deciding whether the roamer should be moved to a different (preferred) network; sending OTA messages to update certain files on the SIM card and then instructing the handset to refresh its cache; and sending OTA or SMS messages to the SIM toolkit application on the handset so that the application switches the roamer to a preferred network. In the final component just listed, the SIM toolkit application switches the roamer to a preferred network using one of two approaches: updating SIM card files and then instructing the handset to refresh its cache; or instructing the handset to select a particular network directly.

[0034] Registration rejection methods include the following components: detecting the network the roamer is currently on; the TR application logic deciding whether the registration process should be allowed to succeed or rejected; if the network is to be rejected, various approaches are taken to reject the Update Location with various error codes or to send a subscriber profile with information that makes the handset search for a new network; if a preferred network is not found, the TR application logic can decide that the user should be provided service on any available network, and hence registrations on non-preferred networks are also allowed to go through; a mechanism to initiate Update Location on demand is also provided, and this can be used to make the handset trigger an Update Location periodically; in some embodiments, it is determined whether the handset is in manual or automatic network selection mode; and it is also determined whether the handset is in midst of a voice or GPRS/MMS session.

[0035] Both the OTA approaches and the registration rejection approaches involve first detecting that the subscriber is roaming in another network. The two types of

approached also share various databases (to be described below) of information that is be used to make traffic redirection decisions.

[0036] **FIG. 1** is a block diagram of one embodiment of a traffic redirection system **100**. The system **100** includes network operator backend processes (or "backend") **101**, external systems **126**, and traffic redirection network (TR) element **102**. These elements are used by the network operator to provide wireless services to subscribers, such as cellular phone users. Subscribers buy services from the operator, including voice and data services that the user access with a phone, a PDA, a PC, or any device (not shown in this figure) that can communicate on a wireless network. The user device is generically referred to as a mobile station in the wireless network. For convenience herein, the mobile station will usually be referred to as a handset.

[0037] The network provider backend **101** includes an SMSC interface **106**, a GSM encryption element **108**, and a key manager **110**. The key manager has control over certain keys in the handset. For example, the handset may have an OTA key lock that prevents writing to the handset SIM without network operator permission. The network operator backend **101** further includes an OTA interface **112** for sending and receiving OTA messages, and application logic **114** for providing and controlling specific wireless services. The network operator backend **101** further includes various databases, including a tariff and service database **116**, a handset database **118**, an IMSI/SIM database **120**, and a roamer profile database **122**. Various databases are described in more detail below.

[0038] The network operator backend **101** further includes an integration interface for facilitating communication with other systems.

[0039] Traffic redirection elements of the system **100** include a traffic redirection (TR) network element **102**. The TR network element **102** includes a TR roaming probe **102***a*, and a TR node (not shown in this figure), and a TR application (not shown in this figure). Each of these is described in more detail below. The TR node, the TR application, and the TR roaming probe may or may not be physically co-located in various embodiments, but all are considered parts of the TR network element.

[0040] The TR roaming probe **102***a* monitors the handset in either a passive or active mode to determine such things as when the handset is attempting to register on a network and which network the handset is currently registered on.

[0041] **FIG. 2** is a diagram that shows one of the network operator's subscribers **202** within the subscriber's home network. The subscriber **202** is a "home" subscriber from the perspective of the network operator that owns the network operator backend **101**. The subscriber **202** has a mobile station or handset **204** which communicates over the wireless network with a home network or HPLMN **212** through a base station **205** and an MSC/VLR **206**. In the embodiment shown, there is a SIM toolkit application (STK) **280** resident on the handset **204**, and it will be described in more detail below. In further figures throughout this description, the handset **204** is shown without the STK **280**, which is optional. The handset **204**, whenever shown, may or may not include the STK **280**, and embodiments which include the STK **280** will be described accordingly. The HPLMN **212** communicates with a public switched telephone network (PSTN) **210** via a GMSC **208**.

[0042] Detecting Out-roamers: Passive Mode

[0043] A passive monitoring approach, according to an embodiment, includes monitoring the SS7 MAP signaling messages on the external signaling links between the operator STP/GMSC and the signaling provider. With reference to **FIG. 3**, the mobile subscriber **202** is roaming in a VPMN **308**. The VPMN **308** and the subscriber's HPMN **212** have a roaming relationship such that the HPMN **212** subscribers are allowed to get service on the VPMN **308**. When the roaming mobile subscriber's handset **204** registers on the network **308**, it initiates a registration process such that a VLR **312** sends a MAP Update Location message to an HLR **302** in the HPMN **212** of the roaming subscriber **202**. Passive monitoring includes using high impedance probes on a SS7 signaling link **314** between a GMSC/STP **304** of the HPMN **212** and a SS7 signaling network **306**. The high impedance ensures that the probing does not interfere with the regular information exchange between the VPMN **308** and the HPMN **212**. Alternatively, the link between the GMSC/STP **304** and the HLR **302** can be monitored. Any MAP messages can be monitored. In one embodiment, at least the following MAP messages are monitored:

[0044] MAP Update Location request and response;

[0045] MAP Cancel Location request and response; and

[0046] MAP Insert Subscriber Data request and response.

[0047] In some cases, the probes used to monitor the SS7 signaling link **314** may belong to a third party and the information exchanged with the TR network element **102** may use Files, Sockets, FTP, custom trigger etc. In yet other cases, a HPMN HLR **302** may initiate a trigger to an external application, such as the TR application or TR network element **102**, on every Update Location message, as shown by path **315**.

[0048] Detecting Out-roamers: Active Mode

[0049] In the active mode, the TR network element **102** includes a node in the signaling path **314** of the Update Location message between the VLR **312** in the VPMN **308** and the HLR **302** in the HPMN **212**. With reference to **FIG. 4**, the subscriber **202** is roaming in VPMN **308**. The VPMN **308** and the HPMN **212** have a roaming relationship such that HPMN **212** subscribers are allowed to get service on the VPMN **308**. When the roaming subscriber's handset **204** registers on the network **308**, it initiates a registration process such that the VLR **312** sends a MAP Update Location message on the SS7 signaling network **306** directed towards the HPLMN **212** of the subscriber **202**. In one embodiment, the TR network element **102** is in the signaling path **314** before the messages go to the HLR **302** and before the response from the HLR **302** goes back to the VLR **312** in the VPMN **308**.

[0050] Embodiments of the invention contemplate various approaches to routing the signaling messages via the TR network element **102** using links **402** and **404**. The following approaches are not meant to be an exhaustive list.

[0051] In one approach, the signaling provider routes all messages with a E.214 numbering plan type to the TR

network element **102** instead of to the network operator GMSC/STP **304**. The TR network element **102** internally routes the messages via the network operator GMSC/STP **304** and hence stays in the signaling path by acting as a specialized STP.

[**0052**] Alternatively, the network operator GMSC/STP **304** is configured such that if the Called Party address is an HLR **302** address (SSN=6) and the numbering plan type is E.214, the message gets routed via the TR network element **102**.

[**0053**] Another alternative is configuring the operator GMSC/STP **304** to send all the E.214 messages to the HLR **302**. However, in response to the to the Insert Subscriber Data message, if the Called Party Address is outside the operator's numbering plan and the Called SSN is a VLR **312** SSN (SSN=7), the messages are routed via the TR network element **102**. This achieves the same result as the second alternative listed above but limits the number of messages that go via the TR network element **102** since only messages meant for external networks need to be handled.

[**0054**] Yet another alternative is for the external signaling provider to send all Update Location messages using a non-zero Translation Type. The operator STP **304** routes all E.214 messages with a specific Translation Type (for example, TT=10) to the TR network element **102**. The TR network element **102** changes the TT to 0 and routes it back to the GMSC/STP **304** after which it is routed to the HLR **302**.

[**0055**] In some cases, the HLR **302** will initiate a trigger to an external application, such as the TR network **102** TR application, when it receives an Update Location message from the VPMN VLR **312**. In any case, the TR network element **102** has the capability to trigger the OTA message to the handset, timeout the message, send a reject message or even modify the information exchanged in the messages between the HLR **302** and the VLR **312**.

[**0056**] Information Databases

[**0057**] The network operator may chose to use various data elements in order to selectively redirect registration traffic. For example, pre-paid users may need to be redirected to a specific network while post-paid users are be redirected to another preferred network in the same country and coverage area. Even within these segments, the operator may have business rules to determine if the roamer is a GPRS/MMS subscriber or just a voice call user. Based on such service profile information, further preference for networks can be established. Some of the database entities that are envisaged by this patent application are listed below.

[**0058**] A Country and Network database contains a list of networks and the countries they are in. Each country can be selectively barred for registration rejection traffic redirection. If the country is barred, each of the networks in the country is also barred for registration rejection traffic redirection. If the country is not barred, it is possible to set the barred or not barred status on a per network basis. In addition, it is possible to specify if a particular network is an outbound roaming partner. Network-specific information contains roaming attributes that indicate, for example, whether pre-paid roaming is allowed on a network, whether GPRS roaming is available on a network, whether roaming minutes are agreed to for volume discounting, etc.

[**0059**] A Device Capabilities database contains a list of TAC and FAC codes for the various handsets in the market. This database also contains various attributes related to the handset capabilities. For example, the particular proactive SIM REFRESH modes supported, whether the handset is a GPRS handset, whether the handset updates EFLOC, on power-off, etc.

[**0060**] A subscriber Device Information database contains the subscriber's IMSI, MSISDN and particular device. When a particular traffic redirection approach has handset dependencies, this database can be used to select the appropriate approach to take in order to effect the traffic redirection.

[**0061**] A Roaming Partners Tariff database includes tariff information and typically also contain information regarding whether the roaming partner is part of a global or geographical tariff plan, whether charges are incurred per minute, or per second, or per six seconds, whether there is a minimum charge, etc.

[**0062**] A Roamer Profile database includes a "blacklist" database and a "white list" database. The white list database contains the IMSI values for subscribers for which registration rejection traffic redirection should be applied. If this list is activated, the traffic redirection works only for these specific IMSI values; remaining subscribers are not affected. Similarly the black list database contains a list of IMSI values for which the traffic redirection is never attempted. All SIM cards issued to roaming partners should be included in this database to assure intended traffic redirection.

[**0063**] A Subscription Identification databases includes information regarding pre-paid, post-paid, GPRS, and MMS subscribers. Pre-paid roamers are typically identified using a database that is populated by the operator. Similarly, the database has information on GPRS and MMS subscription. The ISD messages on the roaming links can be monitored to identify pre-paid roamers (for example, using CAMEL service mark and SCF address).

[**0064**] Other information related to decision making in the traffic redirection process includes: Barring Time, or the time during which traffic redirection should not be attempted; National TR, which is a flag to indicate whether traffic redirection should be attempted for national roaming; and System configuration data, such as OTA Server information, SMSC Configuration etc.

[**0065**] Some of these databases are shown in **FIG. 1**.

[**0066**] Over-The-Air (OTA) Traffic Redirection Approach

[**0067**] The OTA based traffic redirection involves interaction with the handset and SIM card capabilities. In one embodiment, files on the SIM card are updated, and the handset is instructed to refresh its cache and potentially do a new search for available networks.

[**0068**] **FIG. 5** is a diagram that helps illustrates embodiments of OTA traffic redirection. In **FIG. 5**, the subscriber **202** is away from the home network, HPLMN **212**. Several networks are available for the subscriber **202** to roam on, including VPLMN **504**, VPLMN **506**, and VPLMN **508**.

[**0069**] The HPLMN **212** communicates with the various VPLMNs through the TR node **102***b* of the TR network element **102** and international roaming links **514**. Elements

of the HPLMN **212** include the GMSC **208**, an IWMSC **107**, the SMSC interface **106**, and the OTA interface **112**.

[**0070**] Over-The-Air (OTA) Traffic Redirection Approach with Optional SIM Toolkit Application (STK)

[**0071**] As shown in **FIG. 2**, an STK application **280** may be installed on the SIM card in the roamer mobile station **204**. Certain SIM cards do not respond to OTA messages directly. One approach to communicating with such SIMs is placing an STK on the SIM to behave as a proxy or intermediary that can receive OTA messages and communicate appropriately with the SIM. Then instead of the network messaging directly updating the files on the SIM card and asking the SIM card to update its cache, all of that information is sent to the STK, which is directed to update the SIM for the network.

[**0072**] The STK application **280** registers for three Event Download messages—Location Status, Call Connected and Call Disconnected. Every time the Location Area changes, the Location Status event is downloaded to the STK application **280**. Similarly, for every MO and MT call, the Call Connected event is downloaded. When the call clears, the Call Disconnected event is downloaded to the STK application **280**.

[**0073**] The Call Connected and Disconnected events contain information on MO or MT calls. During a call, the roamer will not be switched to another network.

[**0074**] The Location Status event contains the following information:

[**0075**] Location Status—contains the current service state of the Mobile Station. Can have values Normal Service, Limited Service or No Service;

[**0076**] Location Information—is included only of service state is Normal Service;

[**0077**] Mobile Country Code (MCC) and Mobile Network Code (MNC); and

[**0078**] Location Area Code (LAC) and Cell Identity Value (Cell Id).

[**0079**] If the currently selected MCC and MNC are not the same as the home network (identified in GSM networks using the first few digits of IMSI), the SIM Toolkit Application detects that the user is roaming in the VPMN. It can then initiate mechanism to move the user to the preferred network by sending this information to the HPMN via SMS, USSD or a URL invocation (using WIB, for example). Additionally, if the handset and SIM support the RUN AT service, the RUN AT+COPS command can also be invoked.

[**0080**] Using an STK provides an additional capability. The STK allows a RUN AT command to be issued over the network, for example, by the TR network entity. A Run AT command allows the STK to directly command the handset, for example, to change from a current network to another specified network. Traffic redirection approaches involving STKs and the Run AT command will be explained more fully below.

[**0081**] **FIG. 6** is a flow diagram of an embodiment of OTA traffic redirection, which will now be described with reference to **FIG. 5** and **6**,

[**0082**] As shown in block **602**, the roaming mobile station **204** registers on VPLMN **506** via the base station **205** and an MSC/VLR **512**. An "Update Location" message is then generated by the MSC/VLR **512** at **604**.

[**0083**] The TR network element **102** monitors the external roaming links **514** for "Update Location" messages. Monitoring can be done actively or passively, as previously described, depending on the operator requirements. If monitoring is passive, the TR node **102***b* of the TR element **102** is a passive probe. If the VPMN information is gleaned from the signaling path, then the TR node **102***b* of the TR element **102** is an active SS7 element and SCCP relay.

[**0084**] As soon as TR network element **102** taps the "Update Location" message at **606**, it determines the MCC and MNC codes from this message, which enables it to identify the country and the VPLMN on which its roaming mobile station **204** has registered. At **608**, using the various databases including the preferred partner list database, the TR network element **102** determines if the current VPLMN is a preferred network.

[**0085**] If the current VPLMN is a preferred partner network, no further action is taken, and the status is maintained, as shown at **610**. If the current VPLMN is not a preferred partner network, then the TR network element **102** initiates a redirection process. Depending on several factors, such as the choice of operator-HPLMN and associated business rules, the TR network element **102** initiates one of several traffic redirection processes.

[**0086**] Referring first to soft redirection **636**, the TR network element **102** sends a SMS message to the roaming mobile station **204** via the SMSC **106**, informing the outbound roamer **202** that she would benefit from economical roaming rates and value-added services if she manually switches to the HPLMN **212** preferred partner network, VPLMN-Preferred **504**. This is shown at **638**. This message can further provide short steps on how the user **202** can manually switch to the preferred network **504**. Additionally, the TR network element **102** can personalize these steps for the specific device **204**, by using its handset capabilities database. The user **202** may follow the suggested steps and switch to the VPLMN-Preferred network **504**.

[**0087**] In the case of permission based redirection **637**, the TR network element **102** sends an interactive SMS message **640** to the roaming mobile station **204** via the SMSC **106**, informing the outbound roamer **202** of the benefits of switching to the preferred VPLMN-preferred network **504**. This interactive message further gives the roamer an option to respond with a "Y" or "N" to this request. If the roamer **202** responds with "N", then no action is taken, the status does not change, as shown at **642**, and the roamer **202** continues on the VPLMN-A network **506**. If the roamer **202** responds with "Y", then the TR network element **102** initiates the redirection process at **604**. From this point, the process is similar to hard redirection, as described below.

[**0088**] In the case of hard redirection **612**, the TR network element **102** looks up the SIM/Device capabilities database to determine if the roaming mobile station **204** is STK enabled or not, as shown at **614**. Alternatively (not shown), the OTA server can also be used to query the SIM for contents of the EF_{PHASE} (GSM Phase Information file). The value determines the phase of the SIM. A value of 00

indicates Phase 1 SIM while a value of 02 indicates Phase 2 SIM. Any other value of 03 or higher indicates that at the very minimum Phase 2 capabilities are supported.

[0089] If the mobile station **204** is non-STK enabled, then the TR network element **102** initiates a redirection message with the necessary data to the OTA server **112** at **630**. The OTA server **112** encrypts this message at **632** and forwards it to the SMSC **106** for delivery to the roaming mobile station **204** at **634**.

[0090] If the mobile station **204** is STK-enabled, then the TR network element **102** determines at **616** whether preferred PLMN information is available on the mobile station **204** SIM. If the preferred PLMN information is not available, the TR network element **102** sends preference information to the SIM at **620**. The OTA server **112** encrypts the information and sends it to the SMSC **106** at **621**. The SMSC **106** delivers a message to the mobile station **204** at **622**, and at **623** the STK application **280** acts on the message.

[0091] If the preferred PLMN information is available, the STK application on the mobile station **204** looks up the preferred PLMN information file and begins redirection at **618**.

[0092] Redirection includes using the OTA server **112** is to update certain SIM card files. As shown at **624**, the SIM files are updated to reduce an HPLMN search timer period in EF_{HPLMN} from a default value to a value "01" as specified in ETSI GSM 11.11. This specifies that the mobile station will search for the HPMN after 6 minutes. If the redirection attempt is not successful (within next 6+delta minutes), redirection will be re-attempted for a configurable number of times. If the attempt is still not successful or if the mobile station switched to the preferred network, the search period specified in EF_{HPLMN} will be restored to the default value at the discretion of the HPMN. This search time reduction may be required on some handsets to trigger a search for the HPLMN and in the process force an Update Location procedure as defined in ETSI GSM 2.11, 4.08, 3.22 and 3G TS 23.122.

[0093] As shown at **626**, the $EF_{PLMNSEL}$ file (PLMN Selector file) is updated with a list of preferred partners. The preferred partners can be derived based on application logic (group network, partner network, favorable inter-operator tariff (IOT) rates, network offering services most used by the out-roamer, roaming traffic commitments etc.). The most preferred network should be the first network in the list followed by the next preferred partner etc. The information stored is essentially the MCC and MNC code for the networks in that geographic area.

[0094] For some SIM cards, it is necessary to delete the information stored in EF_{BCCH} (Broadcast Control Channels) or to read it and re-order some of the cell information such that the cells are arranged in decreasing priority order of the preferred networks (most preferred network cell is ordered first). The BCCH information is derived from the System Information 2 message and the Neighbor Cells Description Information Element as specified in ETSI GSM 4.08, 11.11 and 3G TS 23.122.

[0095] As shown at **628**, the EF_{LOCI} (Location Information File) is updated with the following information:

[0096] set MCC and MNC in LAI to the most preferred network; and

[0097] for some SIM and handset combinations, erase the Temporary Mobile Subscriber Identity) TMSI value.

[0098] For some SIM and handsets combinations, the Location Update Status field is set to "Not Updated". This forces an Update Location to the MCC and MNC set in the Location Area Identifier (LAI) field.

[0099] For some SIM and handset combinations, the EF_{F-PLMN} is set to the currently selected non-preferred network.

[0100] If the mobile station **204** detects these changes automatically, it performs a new Update Location on the MCC and MNC updated by the TR network element **102**. In other cases, the handset should be instructed to refresh its cache. This is performed using an OTA initiated REFRESH, a SIM toolkit application initiated proactive REFRESH command, or a WIB REFRESH (if the SIM card supports it).

[0101] If the signal strength from the preferred network is strong enough, the mobile station **204** will be able to successfully register.

[0102] This completes the redirection procedure and the roaming mobile station **204** is switched to the VPLMN-Preferred network **504**.

[0103] RUN AT Command Based Traffic Redirection

[0104] This section describes an alternative to the previously described OTA approach for traffic redirection. If the handset is letter class "b" compliant (which means it supports the RUN AT proactive SIM command) and if the RUN AT service (service number 42 in EF_{SST} on the SIM card) is activated and allocated, then a SIM toolkit application or WIB application can issue a RUN AT+COPS command to select a specific network. On some SIM cards, it may also be possible to use proprietary mechanisms to invoke the RUN AT command via the OTA server.

[0105] Registration Rejection Traffic Redirection

[0106] Embodiments of registration rejection traffic redirection involve rejecting the first round of Update Location messages when the handset is trying to register on the VPMN, so that the handset starts searching for a new network. Various ways to achieve this are described below.

[0107] Registration Rejection Traffic Redirection—Aborting the Update Location Transaction

[0108] Referring again to **FIG. 4**, note that in a passive monitoring mode, the link **402** is a monitored link while the link **404** is an active link into the SS7 network **306**. In an active mode, both links **402** and **404** are active links into the SS7 network, and the TR network element **102** is the signaling path. When the mobile station **204** registers in the VLPMN **208**, the VLR **312** first requests authentication information from the HPLMN **212** of the roamer **202**. This is to make sure that the roamer **202** is an authentic subscriber and is allowed to get service on the registration rejection on a roaming relationship between the VPLMN **208** and the HPLMN **212**. This authentication request is in the form of a MAP message that is sent on the SS7 signaling link **314**. The specific MAP message depends on the MAP version being supported, but is typically one of SEND AUTHENTICATION INFO, or SEND PARAMETERS. Once the response from the HLR **302** is received by the VLR **312**, the MSC **312** accepts the Update Location message from the mobile

station **204** and routes it to the HLR **302** in HPLMN **212** via the inter-operator SS7 signaling link **314**.

[**0109**] The TR network element **102** detects the Update Location Request, and if the subscriber is on a non-preferred network, it sends an Update Location End response on the SS7 link **314** with a message such as cause System Failure, Unexpected Data Value or Data Missing. The Global Title of the sending entity does not make a difference and it could either be the same as the HLR **302** or a different one.

[**0110**] The transaction can be aborted at the TCAP layer. In order to do this, the dialog of the original transaction is used and the Update Location End response message is sent on the SS7 link **314** to the VLR **312**.

[**0111**] Each of the processes described above can be performed using passive monitoring or by being in signaling path (active monitoring). The TR node **102***b* uses a valid Global Title and Point Code to inject these messages into the SS7 network **306**.

[**0112**] The handset **204** tries the Update Location on the same network a few more times. This attempt count is equal to the value of the ATTEMPT COUNTER (recommended as 4 in GSM specifications). If there are as many consecutive failures, the handset **204** searches for a new PLMN. In effect, it goes to the box marked as TR1 in **FIG. 7** (Automatic network selection mode) or the box marked as TR2 in **FIG. 8** (Manual network selection mode). **FIGS. 7 and 8** are diagrams showing and automatic network selection process and a manual network selection process, respectively per the specification 3G TS 23.122 Version 3.1.0 Release 199 (ETSI TS 123 122 V3.1.0 2000-01). As referred to herein, **FIGS. 7 and 8** show how various embodiments interact with the specified processes.

[**0113**] The Update Location message is routed to the HLR **302** in the HPMN **212** of the roamer. The TR roaming probe **102***a* monitors the MAP messages on the international roaming links. The TR application **102***c* of the TR network element **102** receives the Update Location event since it has previously registered with the probe for this event notification.

[**0114**] The TR application **102***c* checks its database information and decides if a traffic redirection has to be attempted. For example, if the roamer has registered on a non-preferred VPMN, the traffic redirection application may decide to perform some actions. Other, more specific logic can also be programmed to identify a candidate for traffic redirection. For example, preferred networks for pre-paid and post-paid users, or for GPRS and non-GPRS users may be different influencing whether to redirect.

[**0115**] The traffic redirection application rejects the "first round" of Location Updates and thereby force the handset to search for the next available PLMN (in automatic roaming network selection mode) or try the same PLMN after a brief delay (in manual roaming network selection mode, or if only one network is available in automatic roaming mode). The "first round" of Update Location is "rejected" by jamming the transaction. In one embodiment, jamming the transaction involves sending a spurious MAP End Update Location message with a configurable user error. In one embodiment, the user error is one of System Failure (local value 34), Data Missing (local value 35) or Unexpected Data Value (local value 36).

[**0116**] Other possible values include Unknown Subscriber (local value 1), and Roaming Not Allowed (local value 8). These values, however, can cause various significant events. For example, Unknown subscriber translates to "IMSI not known in HLR" on the radio interface and this marks the SIM as an invalid SIM. The handset stops further PLMN search unless the SIM is removed and reinserted or the handset is powered off and on. "Roaming Not Allowed" puts the PLMN in the Forbidden PLMN file (EF_{FPLMN}) in non-volatile memory on the SIM card and the network cannot be selected unless removed by an OTA operation, STK application, or manual network selection. This value is probably not useful unless the partner network in VPMN country has national coverage or there is a roaming relationship with at-least three operators in the visited country.

[**0117**] The HLR has to send at least one and in many cases two or three Insert Subscriber Data messages to the VLR. Therefore, its transaction time would be greater than that taken by the TR application **102***c* to send the End Update Location. In most cases, there are two ISD messages for post-paid and three ISD messages for most pre-paid subscribers. The time between receiving an Update Location to sending an End Update Location is between 2-3 seconds. Referring to **FIG. 9**, the three call flow cases (A), (B) and (C) should be evaluated in this context. If the VLR sees an End Update Location message from the TR application **102***c* before it sees one from the HLR, it will abort the transaction and reject subsequent messages (including any pending ISD or End UL from HLR). This is shown in call flow (A).

[**0118**] It is also possible for the HLR manages to send the ISD message; however the TR application **102***c* Update Location Reject message arrives before the UL Ack from the HLR, and the Update Location transaction is aborted. This case is shown in call flow (B).

[**0119**] Call flow (C) shows the case in which the HLR manages to successfully send its data and close the transaction before the TR application **102***c* message reaches the VLR. In this case, the second End Update Location from the TR application **102***c* will be rejected and the out-roamer will manage to register successfully on the non-preferred network.

[**0120**] In each of call flows A, B, and C if the roamer handset is in manual mode, it will retry the Update Location on the same network automatically or show the list of available networks to the roamer to choose from. If the handset was in automatic roaming mode, it will try to register on another PLMN if one is available. Else, it will reattempt an Update Location on the same network.

[**0121**] In one embodiment, the TR network element introduces random event based delays before trying to abort the transaction. The delays help "hide" the Traffic Redirection attempts from VPMN since the UL attempts will get blocked at different levels—sometimes before the first ISD; sometimes after the first ISD. In some cases, no traffic redirection attempt will be made. Additional information elements like Subscription class (enterprise, consumer), average spending etc. can also be used to make these decisions.

[**0122**] The timers that define how long the mobile station waits before reattempting the Update Location are defined in GSM 04.08. According to those specifications, the mobile station waits 15 seconds (the value of timer T3211) after receiving an Update Location reject or an abort at the TCAP layer of the transaction.

[0123] Registration Rejection Traffic Redirection—Aborting the Send Authentication Information Transaction

[0124] Referring again to **FIG. 4**, in a passive monitoring mode, link **402** is a monitored link while link **404** is an active link into the SS7 network **306**. In an active mode, the TR network element **102** is in an active signaling path and the signals are carried by the active SS7 links **402** and **404**.

[0125] When the mobile station **204** registers in the VLPMN **308**, the VLR **312** first requests authentication information from the HLPMN **212** of the roamer **202**. This is to make sure that the roamer is an authentic subscriber and is allowed to get service on the registration rejection on roaming relationship between the VLPMN **208** and the HLPMN **212**. This authentication request is in the form of a MAP message that is sent on the SS7 signaling link **314**. The specific MAP message depends on the MAP version being supported but is one of SEND AUTHENTICATION INFO, or SEND PARAMETERS.

[0126] The TR network element **102** detects the Send Authentication Info or Send Parameters message and if the subscriber is on a non-preferred network, it sends the End response on the SS7 link **314** with a cause System Failure, Unexpected Data Value or Data Missing message. The Global Title of the sending entity does not make a difference and it could either be the same as the HLR **302** or a different one.

[0127] In order to abort the transaction at the TCAP layer, the original transaction is used, and the End response is sent on the SS7 link **314** to the VLR **312**.

[0128] Each of the above can be performed using passive monitoring or active monitoring. This case is similar to the Update Location Abort case described earlier; however, it makes sense to do this while in the active signaling path since the transaction time is much smaller than that of the Update Location. The TR node **102***b* needs a valid Global Title and Point Code in order to inject these messages into the SS7 network **306**.

[0129] The handset **204** tries to authenticate itself on the same network a few more times. This attempt count is equal to the value of the ATTEMPT COUNTER (recommended as 4 in GSM specifications). If there are as many consecutive failures, the handset searches for a new PLMN. In essence it goes to the box marked as TR1 in **FIG. 7** (Automatic network selection mode) or the box marked as TR2 in **FIG. 8** (Manual network selection mode).

[0130] Registration Rejection Traffic Redirection—Timing Out the Response to Send Authentication Information Message

[0131] This case is similar to Aborting the Send Authentication Information message. The difference is that instead of aborting the transaction, the TR node **102***b* of the TR network element **102** does not send any response to the VLR **312**. This forces the mobile station **204** to rescan the network as per procedures described in **FIGS. 7 and 8**.

[0132] Registration Rejection Traffic Redirection—Timing Out the Response to Update Location Message

[0133] This case is similar to timing out the Send Authentication Information message. The difference is that Send Authentication Information is allowed to go through but the Update Location is not. The TR network element **102** does not send any response to the VLR **312**. This forces the mobile station **204** to rescan the network as per procedures described in **FIGS. 7 and 8**.

[0134] Registration Rejection Traffic Redirection—Modifying the Insert Subscriber Data Message with "Roaming Restriction Due to Unsupported Feature"

[0135] Referring again to **FIG. 4**, this approach is effective when the TR network element **102** is in the active signaling path **404**. On receipt of an Update Location request from the VLR **312**, the TR network element **102** can send or modify the framed Insert Subscriber Data Message from the HLR **302** to the VLR **312** with the flag "Roaming Restriction due to unsupported feature". Subsequently, the Update Location transaction is allowed to complete normally. This allows the registration to succeed in the VLR **312**, but the VLR **312** sends a "Roaming not allowed in this Location Area" code to the mobile station **204** via the MSC **312**. When the mobile station **204** receives this response code, it starts searching for a new PLMN. This is shown in block TR3 of **FIG. 8** and block TR4 of **FIG. 7**. If no PLMN is found, the mobile station **204** stays on the current VLR/MSC **312** area and only allows emergency calls to go through.

[0136] Unlike the "Forbidden PLMN" information which is in non-volatile storage on the SIM card, this information is stored on the handset memory and is erased when the subscriber roams into a different location area of the same network, switches the phone off, manually selects the network again, or the restriction is removed from the VLR. Specifications also recommend that this list be erased every 12 or 24 hours.

[0137] If the handset is in automatic mode and another network is available, the handset will attempt registration on that network quickly. The TR network element **102** recognizes this and allows/rejects the registration again. However, if the handset is in manual mode or no network was available in automatic mode, it will not attempt a registration quickly. In such a case, the TR network element **102** withdraws the roaming restriction using MAP DELETE SUBSCRIBER DATA (ref GSM 09.02). Therefore, subsequent registrations will be allowed.

[0138] Handling Special Cases

[0139] Special handling is required in certain cases for both international and national roaming. These require certain variations to the approaches described before, and take care of situations such as, for example:

- [0140] identifying whether the out-roamer is in the middle of a call or a GPRS/MMS session;
- [0141] invoking the Update Location on demand so that an attempt to move the out-roamer from a non-preferred network to a preferred network can be made;
- [0142] identifying whether the out-roamer handset is in manual or automatic network selection mode; and
- [0143] identifying an exact location area for national roaming in which coverage may have to be provided on a more restrictive geographical basis.

[0144] These cases are discussed in the following sections. In addition, mechanisms to handle VLR and HLR failures and GPRS sessions in progress are also described.

[0145] Identifying a Roamer within a MO or MT call: SIM Toolkit Approach

[0146] The SIM Toolkit application registers for Event Download on Call Connected and Call Disconnected events. On a MO or MT call, these events are delivered to the SIM toolkit application. The application can hence make sure that it performs the traffic redirection when the mobile station is in idle mode.

[0147] Identifying a Roamer within a MO or MT call: Update Location Reject Approach

[0148] As per specifications, an Update Location is sent only in the following cases:

[0149] a) mobile station requests an Update Location at registration;

[0150] b) mobile station requests an Update Location due to expiration of Periodic Update Location Timer;

[0151] c) the GSM subscriber moves between two VLR areas. If a VLR handles more than one MSC, then the UL is sent when the subscriber moves to another MSC handled by the second VLR. However, if the subscriber moves between MSC handled by the first VLR, no Update Location is sent;

[0152] d) the GSM subscriber moves between two different networks. In this case, the call drops today. However, there are some operators (few and far between) who have arrangements to hand-over the call between their networks; and

[0153] e) in the case of VLR or HLR failure: if the VLR fails, it invokes a Restore Data to which the HLR responds with Insert Subscriber Data. If HLR fails, it sends a Reset Data message to which the VLR responds with Restore Data.

[0154] The GSM specification (ETSI TS 100 527; GSM 03.09 v7.0.0) also provides information on the call handover procedures. If the subscriber is in midst of a call, an Update Location is not sent to the HPMN for cases b) and c). For case d), if the call is dropped, a new registration process in the second network initiates an Update Location transaction. If the network just hands over the call to another MSC, no new UL is sent. This happens because the original VLR/MSC still retains call control and just the radio part is handed over. The second VLR gets the subscriber information from the earlier VLR.

[0155] Since the Traffic Redirection network element blocks the Update Location messages, this implies that if the subscriber is in the midst of a call, there will be no location update and hence there will be no affect on Quality of Service to the subscriber.

[0156] Identifying Manual/Automatic Network Selection Mode: SIM Toolkit Approach

[0157] If the SIM has RUN AT service (service number 42 in EF_{SST}) activated and allocated and the handset supports the RUN AT proactive SIM command (as most letter class "b" handsets do), the SIM Toolkit application can issue the RUN AT+COPS? in order to detect the handset mode.

[0158] Identifying Manual/Automatic Network Selection Mode: Update Location Reject Approach

[0159] This approach heuristically detects the handset mode from the SS7 signaling. If the TR network element detects more than four Update Location transactions on the same network, it assumes that the handset is in manual network selection mode. This is because the ATTEMPT COUNTER value is specified to be four.

[0160] Another mechanism to detect the manual network selection mode is detecting when the handset does not perform a new Update Location on a different network within 20 seconds of the previous Update Location that was rejected.

[0161] Initiating Update Location on Demand From HPMN

[0162] There can also be situations where the HPMN will want more active control on the outbound roamer. Normally the Update Locations are received when the roamer moves from one VLR to another, or when they switch VPMNs. However,,if the roamer remains static in a VLR area (which could handle multiple MSC), no Update Location will be sent unless triggered by the Periodic Location Update Timer (with a random value typically in hours).

[0163] The TR network element can initiate an Update Location from the mobile even when the roamer does not move. With reference to **FIG. 10**, the roamer initiates an Update Location from the VLR to the HLR. This is identified by step 1. Subsequently the HLR sends the Insert Subscriber Data message and the Location Registration is complete. However, since this roamer is on a non-preferred network, the HPMN may want to move the subscriber to the preferred network at some point in time (nighttime, for example). In one embodiment, this is accomplished by sending a MAP-CANCEL-Location message to the VLR. This is identified in Step 3. This marks the record as deleted in the VPMN VLR. Next, the TR network element sends a MAP Provide Roaming Number message to the same VPMN VLR to which the Cancel Location was sent earlier in Step 3. The specifications (GSM 09.02 Fault Recovery section 19.3) state that on receipt of a PRN message for an IMSI which does not exist, the VLR will create a dummy record for the IMSI, mark the "Confirmed in HLR Flag" as "Not Confirmed" and also mark the "Confirmed by Radio contact Flag" as "Not confirmed". The VLR will also return the MSRN number to the requester. The PRN transaction is identified as Step 4. On receipt of an incoming call or SMS, the VLR instructs the MSC to page the IMSI in all its location areas. This paging establishes radio contact and when successful, forces the mobile to initiate a fresh Update Location/Restore Data procedure. This forces the HLR to resend the subscriber profile via the ISD message. The monitoring probe can now follow the original TR approach of Rejecting Update Location. These steps are marked as Steps 5 and 6.

[0164] Handling MAP_RESTORE_DATA during VLR Failure

[0165] When the VLR starts its recovery procedure after a failure, it marks the "Confirmed in HLR" flag as "Not Confirmed". Subsequently, when the VLR receives incoming calls or SMS for IMSI for which the status is not set to "Confirmed", it will initiate a Restore Data or Update

Location message to the HLR. The SS7 monitoring probe and the TR application **102***c* will see a big surge in messages. The TR network element will try to move as many out-roamers to partner networks as it can. However, if there is more traffic than can be handled by the TR network element, this does not create a problem since in the worst case, some roamers will continue to be on the non-preferred network until they perform a new Update Location by virtue of moving, or Periodic Location Updating (PLU) Timer, or as a result of induced Update Location as described previously.

[**0166**] Handling MAP_RESTORE_DATA during HLR Failure

[**0167**] When the HLR starts its recovery procedure after a failure, it sends a MAP_RESET_DATA message with leading indicators of IMSI values handled by it. This causes the VLR to mark the "Confirmed in HLR" flag to "Not Confirmed". Subsequent PRN requests and incoming/outgoing calls will initiate Restore Data/Update Location from the VLR to the HLR. For both the approaches just discussed above, depending on business logic, these restoration attempts could be treated as potential TR candidates (since the partner network has anyways lost information!) or left alone. This may impose a short peak load on the probes and TR network element; however that load is short lived and in the worst case, some mobiles will not undergo the TR treatment. There will be no other side effect.

[**0168**] Handling Active GPRS Subscribers

[**0169**] There should not be any affect on GPRS roaming subscribers since those updates are normally independent of the normal Update Location and performed using MAP_UPDATE_GPRS_LOCATION from SGSN to HLR (ref GSM 09.02 and GSM 04.08).

[**0170**] National Roaming

[**0171**] Some special handling may be required to handle the case of national roaming. As an example, in the international case, the TR network element is interested in which country the handset is in. In the national case, roaming can occur among many networks in large countries like the United States and Canada. In the national case, the TR network entity is interested in the current Location Area of the handset. This is due to the fact that in some areas, both the HPMN and VPMN may offer service while in other areas only the VPMN may offer service. In some countries, the HPMN may also want to bar their subscriber from using a particular VPMN in some specific regions. Note that in such cases, the decision of which network to keep the roamer on cannot be determined just by looking at the VLR address in the Update Location transaction. Finer granularity at a cell-id or Location Area level is required.

[**0172**] **FIG. 11** illustrates a case in which the mobile subscriber **1102** could potentially get coverage from the VPLMN **1108** base station **1105**, and the HPLMN **1112** base station **1111**). The HPLMN **1112** operator might want to allow the mobile station **1104** to roam onto VPLMN **1108** in some areas and in other areas either deny the service or try to proactively move the roamer to the HPLMN **1112** coverage area. In such a case, the granularity may be the Cell-id. Note that each base station has multiple cells and the cell-id is not sent to the HPLMN **1112** in the Update Location transaction.

[**0173**] In one embodiment the mechanism of doing this includes selective redirection. The TR network entity stays in the SS7 signaling path **1114** and manipulate the Update Location transaction. Again with reference to **FIG. 11**, the mobile subscriber **1102** is roaming in VPLMN **1108**, and initiates the registration process on the network. The Update Location message is routed from the VPLMN **1108** to HPLMN **1112** where the message is routed via the TR network element **102** to the HLR **1302**. The HLR **1302** sends the subscriber profile to the VLR **1312** using the Insert Subscriber Data message. This message is routed via the TR network element **102**. TR network element **102** modifies the Subscriber Status in the message to "Operator Determined Barring". This allows the mobile station **1104** to register, but does not allow the subscriber **1102** to make or receive any calls. Immediately afterwards the TR network element **102** sends a MAP Provide Subscriber Information message to the VLR **1312**. The VLR **1312** returns the cell-id of the mobile station **1104** gathered during the Update Location Area transaction. Based on this cell-id information, the HPLMN **1112** may decide if it wants the roamer to register on this network (for example, when HPLMN **1112** does not offer service in that specific region) or search for another network (for example, if the roamer is in or close to an area where the HPLMN **1112** also offers service).

[**0174**] Should the subscriber be denied service, the TR network element **102** issues a MAP Cancel Location command to the VLR **1312** and subsequently sends a MAP Forward MT-SMS message using SMS protocol id **40** to force the mobile station **1104** to acknowledge the SMS without showing the content to the subscriber **1102**. In some cases, the instead of sending the SMS using a MAP command, The SMS can be sent via the HPMN SMSC **1109**. This forces the VLR **1312** to issue a Search MS command to the MSC/VLR **1312** and hence establish radio contact with the mobile station **1104**.

[**0175**] An alternative is to send a MAP Provide Roaming Number request to the VLR **1312**. Because the roamer record was previously cancelled using Cancel Location, the VLR **1312** creates a dummy record; allocates a MSRN, and sets the status of the dummy record as "Confirmed in HLR" and "Not confirmed by radio contact". On a subsequent incoming call, this results in a MAP Restore Data message from the VLR **1312** to the HLR **1302** to retrieve the, profile. The TR network element **102** sends the Insert Subscriber Data message with "Roaming restriction due to unsupported feature" in order to make the mobile station **1104** search for a new network. In this case if the subscriber **1102** moves and the mobile station **1104** sees the HP LMN **1112** cell-id covered by base station **1111**, then the mobile station attempts registration on the HP LMN **1112** and this is allowed to go through.

[**0176**] If the subscriber should be provided service in the original location area covered by VPMN **1108** base station **1105**, a similar approach is followed except that the "Roaming Restriction due to unsupported feature" flag is not set and the Subscriber Status flag is also not modified. This allows the subscriber to register properly and get service.

[**0177**] Note that for national roaming, it is recommended that the EF_{HPLMN} value on the SIM card be set to 1. This will make the handset search for the HPLMN every 6 minutes. Hence if a subscriber was granted service in a VPLMN and

subsequently moves to another area where the HPLMN also has coverage, the maximum time before the HPLMN is selected will be 6 minutes.

[0178] In addition, some operators may chose to not use Cancel Location in the approach mentioned above; however they may send a Standalone Insert Subscriber Data message and abort it. This approach has similar end result with the advantage that existing calls in progress will not be affected.

[0179] Application Using the Traffic Redirection Embodiments

[0180] Various applications can be built on top of the core technology to redirect users onto a specific network. Some of these are as follows:

[0181] Application Using the Traffic Redirection Embodiments: Border Roaming Gateway

[0182] In many countries, especially with land borders, there is coverage from networks of the bordering countries. A similar situation arises in national roaming case when within a country, the HPMN and the VPMN offer roaming in some overlapping coverage areas. In such a case, the people at the border continuously "hop-on" and "hop-off" the HPLMN network. The approach of rejecting the Update Location on the roaming network and bringing them back onto the HPLMN network can save lot of money for the mobile operators and also provide good customer service to their subscribers since the subscribers do not have to pay roaming charges.

[0183] Application Using the Traffic Redirection Embodiments: Menu/SMS Based User Permission for TR

[0184] Mobile operators can offer various kinds of Menu based services to the roamers in order to select the correct network. Some of these selections can be influenced by:

[0185] providing information to the roamer on the roaming tariff applicable on various roaming partner networks, billing pulse duration, minimum charges etc.;

[0186] providing information to the roamer on who is the partner network in that country and what services do the various networks offer. For example, network 1 may offer only voice roaming but network 2 may offer voice and GPRS; and

[0187] providing information on partner networks in the country and on which user could earn rewards etc.

What is claimed is:

1. A method for controlling wireless network traffic, comprising:

determining when a roaming mobile station initiates a registration attempt with a non-preferred network; and

causing the roaming mobile station to initiate a registration attempt with a preferred network.

2. The method of claim 1, further comprising determining what network the mobile station is currently registered with.

3. The method of claim 1, further comprising preventing the mobile station from succeeding in the registration attempt with the non-preferred network.

4. The method of claim 1, wherein the registration attempt with the non-preferred network is completed, the method further comprising:

determining that the mobile station is registered with a non-preferred network; and

periodically causing the mobile station to reinitiate a registration attempt with a preferred network.

5. The method of claim 1, further comprising:

determining whether the mobile station should be moved to another network; and

updating files on the mobile station, including a preferred provider list.

6. The method of claim 1, further comprising:

determining whether the registration attempt with a non-preferred network is allowed to succeed;

if the registration attempt is not allowed to succeed, rejecting the attempt.

7. The method of claim 6, wherein rejecting the attempt comprises sending a recognized transaction to the mobile station that aborts the attempt.

8. The method of claim 6, wherein rejecting the attempt comprises causing a transaction time out.

9. The method of claim 6, wherein rejecting the attempt comprises modifying a message to restrict roaming by the mobile station.

10. The method of claim 1, further comprising determining whether a roaming mobile station is engaged in a voice or data session.

11. The method of claim 1, further comprising determining whether a roaming mobile station is in an automatic network selection mode or a manual network selection mode.

12. The method of claim 1, further comprising invoking an Update Location message on demand.

13. A method for directing a network entity to a particular network, comprising:

detecting a roaming network entity is registering with a visited network;

detecting the visited network is a non-preferred network; and

initiating a redirection message to the network entity that causes the network entity to search for a preferred network.

14. The method of claim 13, wherein detecting the roaming network entity is registering with a visited network includes tapping a message and determining at least a mobile country code (MCC) and a mobile network code (MNC).

15. The method of claim 14, wherein the message is an Update Location message.

16. The method of claim 13, further comprising:

sending the redirection message to an over-the-air (OTA) server;

encrypting the message; and

forwarding the message to a short message service center (SMSC).

17. The method of claim 13, further comprising:

determining whether the network entity includes a Subscriber Identity Module (SIM) toolkit application (STK); and

if the network entity includes an STK, initiating redirection with the STK.

18. The method of claim 13, further comprising:

if the network entity includes an STK, determining whether a Public Land Mobile Network (PLMN) list is on the SIM; and

if not, forwarding a PLMN list to the SIM.

19. The method of claim 13, further comprising:

in response to the message, initiating redirection procedures; and

updating information on the SIM, including

a home PLMN search time period;

a PLMN selector file; and

a location information file.

20. The method of claim 13, further comprising, in response to the message, issuing a RUN AT+COPS command to select a specific network.

21. A system for directing wireless network traffic, comprising:

a network operator backend, including an OTA interface; and

a traffic redirection network entity, wherein the traffic redirection entity communicates with a mobile station to direct registration with a particular network when the mobile station attempts registration with a non-preferred network.

22. The system of claim 21, wherein the traffic redirection network entity comprises a traffic redirection node, a traffic redirection roaming probe, and a traffic redirection application.

23. The system of claim 22, wherein, in a passive mode, the traffic redirection network entity monitors a signaling link between a home network and an SS7 signaling network to determine a network the mobile station is currently registered with.

24. The system of claim 22, wherein, in an active mode, the traffic redirection node is in a signaling path **314** between a visited location register in a visited network and a home location register in a home network that determines a network the mobile station is currently registered with.

25. The system of claim 22, wherein, in an active mode, the traffic redirection node is in a signaling path **314** between a visited location register in a visited network and a home location register in a home network.

* * * * *