METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT FOR COUNTERING ANTI-TRAFFIC REDIRECTION

Related Applications

[0001]This application claims priority from United States Provisional Patent Application Serial No. 60/662,031 entitled "Method and Apparatus for Defense Against Defense Against Network Traffic Redirection", filed March 14, 2005 and this application is related to United States Patent Application entitled "Method And System For Cellular Network Traffic Redirection" Application No. 10/635,804 filed on August 05, 2003, claiming priority from August 05, 2002. Both of those patent applications in their entirety are incorporated herein by this reference.

BACKGROUND

Field of the Invention

[0002]The present invention relates to traffic redirection in a wireless network. More particularly the invention discloses a method, system and program product to counter anti-traffic redirection mechanisms.

Background of the Technology

[0003]Wireless communication networks have become an integral part of today's digital lifestyle. The necessity and the desire to remain connected at all points of time has resulted in wireless operators expanding their networks to almost all conceivable parts of the world.

[0004]Different standards and protocols have been adopted in the industry, depending upon the users' requirement and the preference of the operators in a particular geographical location. Some of the popular technologies that are present in this domain include GSM, GPRS, 3G, CDMA, WCDMA, TDMA, WLL, WiFi, WiMax and VoIP. All of these technologies have their merits and shortcomings and provide a gamut of voice based and data based services. A network operator may be providing one or more of voice/data service using one or a combination of the aforementioned technologies.

[0005]In order to prevent monopoly of a service provider, various geographical zones are allotted to one or more network operators. These operators usually provide competitive services in their zone. A particular network operator may be present in more than one geographical zone. In order to provide seamless service to a subscriber, the network operators not only cater to the subscribers directly registered with them but also to their subscribers from other zones and/or the subscribers of other network operators with whom they have a "roaming" agreement. Often, those roaming arrangements are bilateral, such that the subscribers of each geographically diverse operator are enabled to receive roaming service within the zone of the other operator. The network with which the subscriber has a direct relationship is called the subscriber's Home Network. Any other network in which the user may roam is called the Visiting Network. The subscriber is referred to as an outbound roamer from the perspective of the Home Network and an inbound roamer from the perspective of the Visited Network.

[0006]As mentioned above, at any given geographical location, there maybe more than one network operator providing one or more kinds of service. The home network of the roaming user may prefer one visited network over another, or may want to allocate varying percentages of their outbound roamers' traffic to different operators. Various factors such as commercial terms, quality of service, range of service and the like would dictate such a preference or roaming distribution. Under ideal scenario the home network would make all possible efforts to ensure that its outbound roamers register to the visited network operator that it prefers in that case.

[0007]Traffic Redirection (TR) or Steering of Roaming (SoR) is a method by which the home network operators use the messages exchanged in a Mobile Application Part (MAP) based signaling scheme so as to steer their subscribers to attempt connection with the preferred network/s according to some logics or distribution. The term preferred network is used herein, to refer either static preferences of one network over another or dynamic preference of one network over another based on some logics or distribution (e.g. subscriber profiles, the visiting country, current distribution of outbound roamers in the country).

[0008]Due to the magnitude of revenues generated through inbound roaming, operators are always motivated to capture the maximum amount possible of inbound roaming traffic. Billboards and advertisements at airports and borders, and the

competition among operators to install the most powerful transmitters at those locations bear witness to that. With the advent of Steering of Roaming, operators today are motivated to disrupt traffic redirection attempts and try to cause inbound roamers to register automatically with their networks. This not only results in loss of revenues to the home network operator but also may not provide the subscriber the best quality and range of services as desired by the home network operator.

[0009]There is a need in the art for a method and system that counters the anti-traffic redirection attempts and steers roamers back to the preferred networks.

BRIEF DESCRIPTION OF THE FIGURES

[0010]In the drawings, the same or similar reference numbers identify similar elements or acts.

[0011]FIGURE 1 is a block diagram of an embodiment of the anti-anti-Traffic Redirection system.

[0012]FIGURE 2 is a flowchart illustrating the method for countering an anti-TR approach, as per some embodiments of the invention.

[0013]FIGURE 3 shows the signal flow for countering an anti-TR approach that fakes manual mode of the handset or fakes the scenario of being the only network available.

[0014]FIGURE 4 shows the signal flow for countering an anti-TR approach that fakes the presence of a special handset.

[0015]FIGURE 5 shows the signal flow for countering a GLR based anti-TR.

DETAILED DESCRIPTION

[0016]A method for detecting the anti-TR mechanism and redirecting the roamer to a preferred network is disclosed. The method detects the presence of an anti-TR solution by observing one or more registration messages exchanged by a visiting network and a home network. The method includes steps to steer the roamer to reattempt connection with the preferred networks by sending appropriate registration response messages in response to the observed registration messages.

[0017]The invention also discloses a system for detecting the anti-TR mechanism and redirecting the roamer to a preferred network. The system includes a probing block to observe the registration messages exchanged between the Home Network

and the Visiting Network. The system further includes a detection block to detect the presence of an anti-TR mechanism deployed at the visiting network, based on the registration messages as observed by the probing block. The invention also provides for a redirection module that attempts to redirect the roamer to attempt reconnection with a preferred visiting network.

[0018]Various embodiments are disclosed herein, which counter the various approaches that an anti-TR mechanism may take so as to fail the TR mechanism of the home network.

[0019]A computer program product for realising the aforementioned method is also claimed herein.

[0020]The following description provides specific details for a thorough understanding and an enabling description for various embodiments of Anti-Traffic Redirection Countering System (ATRCS). However, one skilled in the art will understand that the ATRCS may be practiced without these details. In other instances, well-known structures and functions have not been shown or described in detail to avoid unnecessarily obscuring the description of the embodiments of the ATRCS. The headings provided herein are for illustrative purposes only and do not affect the scope or meaning of the claimed invention. An Appendix includes an explanation of numerous acronyms used herein and is included below for reference. Therefore, the acronyms used may not be spelled out in the body of the document.

[0021]The invention would now be described with reference to the accompanying figures. Although the invention is being described with GSM as the underlying technology and focus, the inventive concept is equally applicable in other wireless technologies such as CDMA, WCDMA, WiFi, WiFiMax, VoIP etc. In context of a cell-based GSM network, the home network has been referred to as Home Public Mobile Network (HPMN) and the visiting network has been referred to as Visiting Public Mobile Network (VPMN). Furthermore the HPMN and VPMN may both have more than one network operators wherein the HPMN may prefer certain VPMN network operators to the others. The terms HPMN/ HPMN network / HPMN network operator and VPMN / VPMN network / VPMN network operator have been used interchangeably throughout this specification and their intended meaning is driven by the context in which they have been used. The term subscriber is used herein to indicate a user that registers with a network. The subscriber that registers with a network can be any combination of hardware and software capable of registering on

a wireless network, e.g., a personal digital assistant (PDA) or a personal computer (PC).

[0022]The methods and system disclosed herein use the Mobile Application Part (MAP)-signaling messages exchanged between the VPMN and the HPMN to detect any anti-TR solutions deployed by the visiting network and thereafter steer the roamer to attempt reconnection with the preferred network.

[0023]FIGURE 1 illustrates a block diagram of a system in accordance with an embodiment of the present invention. System comprises a HPMN 102 communicating with VPMNs 104 and 106 via a SS7 interface 108. Although the embodiment is described illustrating communication between one HPMN and two VPMNs, a number of VPMNs may be communicating with HPMN 102. Out of these VPMNs, some may be the preferred VPMNs of HPMN. In this illustrative embodiment, VPMN 106 is the preferred VPMN and VPMN 104 is the non-preferred VPMN that has deployed an anti-TR solution. HPMN 102 comprises an anti-anti-TR block 110, an HPMN Roaming Signal Transfer Point (STP) 112, and an HPMN HLR 114. Anti-anti-TR block 110 and HPMN HLR 114 are coupled to HPMN Roaming STP 112. Anti-anti-TR block comprises of three modules, a probing block 110a, a detecting block 110b and a redirecting block 110c. The functions of these blocks has been discussed in detail below. These blocks are logical blocks and may be present as one single entity or may be formed by one or more logical/physical entities. System further comprises an international STP 116, corresponding with HPMN 102, to route the signals to another international STP 118 that corresponds with VPMNs 104 and 106. VPMN 104 comprises a VPMN STP 120 coupled to a VPMN VLR/VMSC 122. VPMN 106 and other VPMNs would also have a similar structure (not shown in this diagram). HPMN Roaming STP 112 communicates with VPMN STP 120 and VPMN STP 124 via international STP 116, SS7 interface 106 and international STP 118. The aforesaid embodiment is described using the blocks pertinent to the invention, however various other blocks may be present in HPMN and VPMNs.

[0024]In accordance with one embodiment of the invention, the HPMN 102 may deploy a TR solution so as to steer its outbound roamers to its preferred VPMNs 106. In order to counter this TR, the non-preferred VPMNs 104 may deploy anti-TR solutions that would try to pull the inbound roamers on to their networks. The anti-TR solution is deployed in the VPMN 104 network either by monitoring the roaming MAP

transactions and injecting spurious messages or by intercepting the roaming MAP transactions and faking interactions as if from the roaming handset or the real VPMN VLR.

[0025]The invention discloses two possible modes of operation of the anti-anti-TR solution i.e. the monitoring approach and the in-signaling approach.

Monitoring Approach

[0026]In an embodiment of the invention, anti-anti-TR module 110 detects the anti-TR attempt by monitoring passively the exchange of at least one registration message between HPMN 102 and VPMN 104. In one embodiment of the invention, probing block 110a observes the registration messages exchanged between HPMN 102 and VPMN 104. The detecting block 110b detects an anti-TR attempt, by observing the type and frequency (explained in detail below) of messages exchanged between HPMN 102 and VPMN 104. In one embodiment of the invention, at least one registration message is a Location Update (LUP) message.

In-signaling Approach

[0027]In another embodiment of the invention, anti-anti-TR module 110 detects an anti-TR attempt by actively monitoring the signaling between HPMN 102 and VPMN 104. The anti-anti-TR block actively monitors the exchange of at least one registration message between HPMN 102 and VPMN 104. Active monitoring is hereinafter referred interchangeably as in-signaling mode. In the in-signaling mode the anti-anti-TR block 110 is deployed on roaming SS7 path by configuring HPMN's 102 roaming STP 112 to route roaming SCCP traffic through anti-anti-TR module 110.

[0028]It will apparent to a person skilled in the art, that different routing methods can be used without affecting the working of the system or method as disclosed herein.

[0029]FIGURE 1 depicts both the monitoring based and in-signaling path based anti-anti-TR architecture. In the case of monitoring-based anti-anti-TR solution, there will be an additional tapping of international roaming links between HPMN and international signal carriers. In the case of in-signaling path based anti-anti-TR solution, roaming SS7 messages from any VPMN are redirected thru the anti-anti-TR block 110 by the HPMN Roaming STP 112. Whatever deployment option is chosen, the anti-anti-TR detection mechanism will receive an outbound roamer's Location

update transaction between VPMN 104, 106 and HPMN 102. In both cases however, the anti-anti-TR block 110 will inject or modify MAP transactions on outbound roamers.

[0030]If the roamer still succeeded to register on the non-preferred VPMN network after a HPMN anti-anti-TR solution, then HPMN 102 can deduce the failure of the HPMN TR/anti-anti-TR solution and the success of the VPMN anti-TR solution. If the roamer failed to register on the VPMN network 104 after the anti-anti-TR solution, then HPMN 102 can deduce the success of the HPMN TR/anti-anti-TR solution and the failure of the VPMN anti-TR solution.

[0031]Based on these deductions and subsequent success or failure of HPMN TR/anti-anti-TR, HPMN 102 can produce all kinds of reports such as signaling load overhead, TR/anti-anti-TR success/failure, percentage of redirected outbound roaming traffic etc.

[0032]The anti-TR solution deployed by VPMN 104, may take one or more approaches. We now explain each of these approaches and how the instant invention's anti-anti-TR solution counters each of these approaches.

Fake Manual Mode or No-Coverage Detection Defense

[0033]A basic idea for implementing an anti-TR solution at a VPMN is to fool the HPMN TR to think that the handset is operating in manual mode or the VPMN is the only network in coverage. This is achieved by repeatedly sending a location update on the same network location despite more than 4 location update rejections from the HPMN TR already.

[0034]Since TR should not try to reject registration of devices in a manual selection or if the VPMN is the only network in coverage, recognition of this mode of an outbound roaming device is important. To avoid bad customer experience, the current TR solution deduces the manual mode or VPMN-only coverage if the outbound roamer's location update from the same VMSC/VLR of the VPMN comes back the fifth time despite rejected the previous 4 times consecutively. This makes it easier for the anti-TR solution of a VPMN operator to fake the manual mode or VPMN-only coverage on behalf of the inbound roaming device.

[0035]However the anti-TR solution generally cannot hold for a long time to respond to the registration of an inbound roaming device. This is because the handset might move to another network or try another registration anyway if its registration attempt

is timed out. The anti-TR solution also cannot easily select some random or configurable intervals to fake new location update since inter-location update intervals are very unpredictable. These intervals not only vary among different handset types, but also can have a small range even for the same handset type. It is also possible that inter network location update intervals can vary between different operators/networks. Furthermore, inter network location update intervals might also vary among different handset types but also can have a small range even for the same handset type. The most likely scenario for an anti-TR solution to do by a VPMN, after suspecting the response to the first location update from the device is a TR attempt, is to fairly rapidly fire one or more location update in succession, on the same VMSC/VLR on behalf of the inbound roaming device at the VPMN.

[0036]For example, if the anti-TR solution fires 3 more location updates after the first TR reject, then the total TR rejects will be 4. The handset will then try another location update on the same location; the HPMN TR solution will allow the location update. For another example, if the anti-TR solution fires one more location update after the first reject, then the total TR rejects will be 2 at the moment. The handset will then try 3 more location updates on the same location. The HPMN TR solution will allow the last location update normally.

[0037]To counter such a tactic, the anti-anti-TR solution keeps the original TR mechanism of deducing the manual mode or VPMN-only coverage but does not count a location update that comes within a configurable threshold time interval, for example within 15 seconds, after a previous location update is rejected.

[0038]FIGURE 2 illustrates some countering approaches for an anti-TR solution deployed by non-preferred VPMN 104. Figure 2 shows these approaches in conjunction with each other. However these individual approaches may be implemented in isolation or in any combination alongwith other approaches for anti-anti-TR.

[0039]As mentioned before the anti-anti-TR block 110 receives LUP messages by either monitoring the SS7 link between the Roaming STP 112 and International STP 116 or by the redirected messages from roaming STP 112. The LUP messages from a particular IMSI are received at step 201. At 202 it is checked if the LUP message for the same IMSI from the same VMSC/VLR 122 is received within a configurable threshold time interval. If it is found so 203 then HPMN 102 does not increment the LUP reject counter 204 but sends a LUP reject 205. If the LUP is received after the

threshold time either HPMN 102 may acknowledge the same or may opt to check for other anti-TR approaches 206.

[0040]The anti-anti-TR block 110 can detect if the interval between location updates of the same outbound IMSI is shorter than the configurable threshold time interval. When a new location update comes within such a configurable threshold time interval, the TR rejection to the location update is not counted in the rejection counter. In this way, even though the anti-anti-TR enhanced HPMN TR might have received 5 consecutive Location Update attempts from the same IMSI on the same VMSC/VLR 122, it will not treat the roaming device in manual mode and will continue to reject the LUP when some of the inter-LUP attempts come within the configurable threshold time interval.

[0041]In an exemplary embodiment of the invention, the configurable threshold time interval may be changed periodically.

[0042]In a further embodiment of the invention, anti-anti-TR block 110 may statistically change the configurable threshold time interval over a period of time. This statistical calculation may be based on the frequency of LUPs received from various VMSC/VLR. Such a solution provides robustness against anti-TR solution detecting the configurable threshold time interval.

[0043]FIGURE 3 shows the exchange of signals for the aforementioned scenario. At 301 a mobile station / handset initiates registration with a non-preferred VPMN 104. Thereafter VPMN 104 sends a LUP 302 to HPMN 102. Since HPMN has deployed a TR solution, it refuses the update and sends a LUP reject message 303. The anti-TR solution of VPMN 104 detects the TR 304 and sends 3 more LUP messages 305 from same IMSI/VLR or may set the Calling Party Address (CgPA) as VLR. The number of LUP messages sent would depend upon the threshold number after which HPMN 102 would accept the LUP. However, since VPMN 104 cannot hold on to the mobile station for long as the roamer may initiate a new location LUP manually in the mean time, therefore VPMN 104 sends further LUP messages in quick succession. Upon receipt of a consecutive LUP message from same VMSC/VLR, anti-anti-TR block 110 would check if it has come within the configurable threshold time interval. If it has, then anti-TR would be detected 306 and LUP rejection error would be sent 307, without incrementing the LUP rejection counter. This way the mobile station would effectively be reinitiating the registration process in a normal manner 308 despite of anti-TR solution intercepting in between.

[0044]This anti-anti-TR solution works in both the in-signaling path mode of TR and the monitoring mode of TR.

Special Handset Detection and Defense

[0045]Another approach taken by an anti-TR solution is to fool HPMN 102 to think that the handset/mobile station is special, by extending the interval between location updates on the same VPMN 104 VLR/VMSC 122 of the same network or by extending the interval between location updates between networks. Normally to avoid bad customer experience, the HPMN 102 will allow subsequent location update to succeed.

[0046]To defend against this anti-TR tactic, the HPMN 102 anti-anti-TR block 110 on receipt of an LUP from an IMSI/VLR 201, would check if it is received after a threshold time period after the last LUP 207. This threshold time period is a configurable extended time period up to which HPMN 102 would wait without assuming the mobile station to be a special handset and therefore issue an LUP ack. For example this configurable extended time period may be about 2 (or more) times of the normal interval (e.g. 30secs, configured by the anti-anti-TR solution) between location updates. If the LUP is received within the extended time period, anti-anti-TR 110 would still reject the LUP. However to avoid bad customer experience, HPMN 102 will only wait for this extended interval for a configurable number (e.g. 1) of times, in general, less than 2 times. Therefore once it is determined 208 that the LUP is received within the configurable extended time interval, it is checked if the extended time interval has been exercised more than the configurable number of times 209. If yes 211, then a LUP ack is sent 212 to VPMN 104. If no 210, then a LUP reject is sent 205 and the extended time interval counter is incremented by one (not shown in figure).

[0047]FIGURE 4 shows the exchange of signals for the aforementioned scenario. At 401 the mobile station initiates registration with VPMN 104 and VPMN 104 sends LUP (with IMSI and VLR information) message 402 to HPMN 102. Since HPMN 102 deploys TR, it rejects the LUP received 403 from a non-preferred VPMN 104. This way VPMN 104 detects the presence of a TR solution 404. Thereafter anti-TR block of VPMN 104 drops LUP messages from same IMSI for 'n' number of times 405 and follows it up by sending a LUP message 406 thereby extending the period between two consecutive LUPs so as to fool HPMN 102 to treat the mobile station as special

handset. However because of the aforementioned algorithm HPMN 102 still sends a reject message 408 to VPMN 104. . This way the mobile station would effectively be reinitiating the registration process in a normal manner 409 despite of anti-TR solution intercepting in between.

[0048]This anti-anti-TR solution works in both the in-signaling path mode of TR and the monitoring mode of TR.

Detect and Defense against a GLR-based anti-TR Solution

[0049]Another basic idea of anti-TR is to avoid subsequent location update between VPMN 104 and HPMN 102 by using a Global Location Register (GLR) to store the first location update profile in the VPMN network. In this way, if by any chance that the roamer succeeded in registering at VPMN 104 despite the HPMN's TR attempt, the GLR can avoid the onslaught of HPMN 102 TR in subsequent location update by the roamer at the same VPMN 104.

[0050]In order to detect the use of GLR as an anti-TR solution, HPMN's 102 anti-anti-TR solution 110 would check if a first successful location update of an outbound roamer on VPMN 104 is followed by a subsequent location update for the same IMSI on same VPMN 104 or any other VPMN, within a configurable time interval 213, for example 10 minutes. HPMN 102 also checks if similar non-receipt of LUPs has been happening for many subscribers 216 on a particular VPMN 104. The number of subscribers for checking this condition may either be a fixed number, which in a very watchful mode maybe 1 i.e. even if one subscriber does not update the location within the configurable time interval then a corrective action would be taken. However a more rational approach may be more calculative, in which the number of subscribers to be checked maybe a ratio of the total number of subscribers registered with the particular VPMN 104. If the above two conditions are not satisfied i.e. subsequent LUPs have been received 214 and even if they have not been received from few IMSI 217, then HPMN 102 assumes no GLR based anti-TR solution deployed. However, if it is found that subsequent LUPs have not been received within the configurable time 215 and the same has been happening for a number of subscribers 219 then HPMN 102 would send a Cancel Location message 219 to IMSI.

[0051]After the detection of GLR based anti-TR solution, the anti-anti-TR solution will wait for a configurable interval (for example 10 minutes) to issue a MAP Cancel-

Location each time a location update at the VPMN (found out to be deploying GLR based anti-TR) from an outbound roaming device is successful. Note that the Home Location Register (HLR) of the roaming device still has the real VPMN VLR/VMSC entry. In this way, for any Mobile Originated (MO)-activity with the VPMN, the handset will be forced to make a new location update on the VPMN. For any Mobile Terminate (MT) call to an outbound roamer, the HPMN HLR will issue MAP PRN to the outbound roamer's real VLR, which returns the MSRN. If the VPMN VLR entry of the roamer is empty, the VPMN VLR will issue a MAP RestoreData to HPMN HLR. The anti-anti-TR solution will wait for a configurable interval to issue another MAP Cancel-Location on the outbound roamer to the VPMN VLR after the RestoreData. For any MT SMS to an outbound roamer, the HPMN HLR will return the outbound roamer's real VPMN VMSC to the originating SMSC. The originating SMSC will then send the message to the real VPMN VMSC. If the VPMN VLR entry is empty, the SMSC will receive an error ack and can then report the delivery status to the roamer's HPMN HLR for future delivery.

[0052]FIGURE 5 shows the exchange of signals for the aforementioned scenario. At 501 a roaming mobile station registers with VPMN 104. VPMN 104 sends a LUP message 501 to HPMN 102. The location Update profile of the roamer sent by HPMN 102 is stored by VPMN at GLR 503. Thereafter for very subsequent LUP from IMSI, VPMN 104 would use the stored profile to acknowledge. Upon discovering that no subsequent LUPs have been received from an IMSI after a successful LUP and a similar occurrence for a number of IMSIs on same VPMN 104, HPMN 102 deduces that a GLR based anti-TR solution has been deployed 504. It then sends a Cancel Location message 505, 506 to the IMSI who have not been updated for a long period of time on VPMN 104 having GLR based anti-TR solution.

[0053]This anti-anti-TR solution works in both the in-signaling path mode of TR and the monitoring mode of TR.

[0054]We would now explain certain approaches to anti-TR that would work in the in-signaling mode only:

Roaming Restricted

[0055]In a TR mechanism employing in-signaling approach, a Roaming Restricted error code can also be used is response to a LUP message. Although this temporarily, puts the network location area as forbidden in the handset, it results in a

faster network reselection. To defend against this TR, the anti-TR solution can perform just TCAP abort or just TCAP reject the Roaming Restricted in the MAP ISD message with unexpected data value or unsupported service etc in ISD ACK.

[0056]To counter against this anti-TR tactic, whenever the ISD RR is not honored due to a suspecting anti-TR attempt, the anti-anti-TR solution will continue to attempt ISD (RR) for a configurable number of times before trying an alternative TR tactic unless the VPMN is genuinely recognized as a RR non-supporting network. If it is detected that some of the ISD ack messages from the same VPMN contain RR whereas others do not, then in may be inferred that an anti-TR solution is deployed by the VPMN.

Roaming Not Allowed

[0057]In a TR mechanism employing in-signaling approach, a Roaming Not Allowed error code can also be used in response to a LUP message. Although this puts the network as forbidden in the SIM of a handset, it results in a faster network reselection. To defend against this TR, the anti-TR solution can just drop the LUP ack/error message and immediately issues another LUP message on the same transaction of the first LUP message that got the LUP error of Roaming Not Allowed. In this way, the HPMN TR may deduce that the handset has manually selected the same not allowed network again and could have allowed the registration to be successful.

[0058]To counter against this anti-TR tactic, the in-signal-path anti-anti-TR solution will continue to issue RNA to a location update if it comes back within a configurable interval (for example 20 seconds) of the previous location update that got rejected with the RNA error.

Defense against an Anti-TR solution to OTA/SIM approach

[0059]In order to defend against a HPMN 102 deploying OTA based TR mechanism, a VPMN 104 simplistically blocks all the OTA messages from HPMN 102 to its outbound roamers.

[0060]So as to counter the above, in one embodiment of the invention, HPMN 102 would respond by sending RNA error code in the LUP response to a LUP request from an outbound roamer registered/attempting registration with VPMN 104 deploying anti-TR solution to OTA/SIM approach. Once the roamer registers with an

alternate network, HPMN 102 can then send OTA messages, steering it to the preferred VPMN 106.

[0061]The methods discussed above have the advantage that they are robust against the anti-TR solutions deployed by the VPMN. Since the anti-anti-TR solution as explained herein works by observing the type and frequency of the registration messages exchanged between the HPMN and the VPMN, and is not focused on countering any particular approach/logic that may have been implemented by the anti-TR solution, therefore it would be difficult to apply a logic to counter the anti-anti-TR mechanism as disclosed herein.

[0062]A computer usable medium claimed herein includes computer usable program code, which when executed counters the anti-TR solution as deployed by the VPMN. The anti-TR attempt is detected by observing exchange of at least one registration message between the VPMN and the HPMN. The computer usable medium further includes computer usable program code for redirecting the roamer to attempt reconnection with a preferred network.

[0063]The components of Anti-Traffic Redirection Countering System (ATRCS) described above include any combination of computing components and devices operating together. The components of the ATRCS can also be components or subsystems within a larger computer system or network. The ATRCS components can also be coupled with any number of other components (not shown), for example other buses, controllers, memory devices, and data input/output devices, in any number of combinations. In addition any number or combination of other processor-based components may be carrying out the functions of the ATRCS.

[0064]It should be noted that the various components disclosed herein may be described using computer aided design tools and/or expressed (or represented), as data and/or instructions embodied in various computer-readable media, in terms of their behavioral, register transfer, logic component, transistor, layout geometries, and/or other characteristics. Computer-readable media in which such formatted data and/or instructions may be embodied include, but are not limited to, non-volatile storage media in various forms (e.g., optical, magnetic or semiconductor storage media) and carrier waves that may be used to transfer such formatted data and/or instructions through wireless, optical, or wired signaling media or any combination thereof.

[0065]Unless the context clearly requires otherwise, throughout the description and the claims, the words "comprise," "comprising," and the like are to be construed in an inclusive sense as opposed to an exclusive or exhaustive sense; that is to say, in a sense of "including, but not limited to." Words using the singular or plural number also include the plural or singular number respectively. Additionally, the words "herein," "hereunder," "above," "below," and words of similar import refer to this application as a whole and not to any particular portions of this application. When the word "or" is used in reference to a list of two or more items, that word covers all of the following interpretations of the word: any of the items in the list, all of the items in the list and any combination of the items in the list.

[0066]The above description of illustrated embodiments of the ATRCS is not intended to be exhaustive or to limit the ATRCS to the precise form disclosed. While specific embodiments of, and examples for, the ATRCS are described herein for illustrative purposes, various equivalent modifications are possible within the scope of the ATRCS, as those skilled in the art will recognize. The teachings of the ATRCS provided herein can be applied to other processing systems and methods. They may not be limited to the systems and methods described above.

[0067]The elements and acts of the various embodiments described above can be combined to provide further embodiments. These and other changes can be made to the ATRCS in light of the above detailed description.

Other Variations

[0068]Provided above for the edification of those of ordinary skill in the art, and not as a limitation on the scope of the invention, are detailed illustrations of a scheme for countering anti-TR between VPMN and HPMN of the roaming mobile station. Numerous variations and modifications within the spirit of the present invention will of course occur to those of ordinary skill in the art in view of the embodiments that have been disclosed. For example the present invention is implemented primarily from the point of view of GSM mobile networks as described in the embodiments. However, notwithstanding, the present invention may also be effectively implemented on CDMA, 3G, WCDMA, GPRS, WiFi, WiMAX, VOIP etc., or any other network of common carrier telecommunications in which end users are normally configured to operate within a "home" network to which they normally subscribe, but have the capability of also operating on other neighboring networks, which may even be across international borders.

[0069]The examples under the present invention Anti-Traffic Redirection Countering System (ATRCS) detailed in the illustrative examples contained herein are described using terms and constructs drawn largely from GSM mobile telephony infrastructure. But use of these examples should not be interpreted to limiting the invention to those media. Anti-Traffic Redirection Countering System – a method for countering anti-TR between VPMN and HPMN of the roaming mobile station in a manner that is agnostic to the capabilities of the visited or non-accustomed network can be of use and provided through any type of telecommunications medium, including without limitation: (i) any mobile telephony network including without limitation GSM, 3GSM, 3G, CDMA, WCDMA or GPRS, satellite phones or other mobile telephone networks or systems; (ii) any so-called WiFi apparatus normally used in a home or subscribed network, but also configured for use on a visited or non-home or non-accustomed network, including apparatus not dedicated to telecommunications such as personal computers, Palm-type or Windows Mobile devices,; (iii) an entertainment console platform such as Sony Playstation, PSP or other apparatus that are capable of sending and receiving telecommunications over home or non-home networks, or even (iv) fixed-line devices made for receiving communications, but capable of deployment in numerous locations while preserving a persistent subscriber id such as the eye2eye devices from Dlink; or telecommunications equipment meant for voice over IP communications such as those provided by Vonage or Packet8.

[0070]In describing certain embodiments of the ATRCS under the present invention, this specification follows the path of a telecommunications call from a calling party to a called party. For the avoidance of doubt, that call can be for a normal voice call, in which the subscriber telecommunications equipment is also capable of visual, audiovisual or motion-picture display. Alternatively, those devices or calls can be for text, video, pictures or other communicated data.

Technical references

GSM 902 on MAP specification
Digital cellular telecommunications system (Phase 2+)
Mobile Application Part (MAP) Specification
(3GPP TS 09.02 version 7.9.0 Release 1998)

Q71X SCCP
Q70X MTP
Q77X TCAP
GSM 1111 SIM and Mobile Interface
GSM 1114 SIM Toolkit
IR 7320 Steering of Roaming
GSM 348 Security and OTA,
GSM 31048 Security and OTA,
GSM 23119 Gateway Location Register,
GSM 408 Mobile Radio Interface Network Layer
GSM 23122 Mobile Station Procedure
GSM 24008 Mobile Radio Interface Network Layer
GSM22011 Service Accessibility
GSM25304 Idle Mode Selection
GSM29010 Error Network Mapping
GSM 29002 MAP Protocol

APPENDIX

Acronym	Description
3G	Third generation of mobile
BSC	Base Station Controller
BCSM	Basic Call State Model
CAMEL	Customized Application for Mobile Enhanced Logic
CDMA	Code Division Multiplexed Access
CLI	Calling Line Identification
CAP	Camel Application Part
CSI	Camel Subscription Information
GMSC	Gateway MSC
GLR	Gateway Location Register
GPRS	General Packet Radio System
GSM	Global System for Mobile
GSM SSF	GSM Service Switching Function
HLR	Home Location Register
HPLMN	Home Public Land Mobile Network
HPMN	Home Public Mobile Network
IMSI	International Mobile Subscriber Identity
IN	Intelligent Network
INAP	Intelligent Network Application Part
IDP	Initial DP IN/CAP message
ISUP	ISDN User Part
MAP	Mobile Application Part
MCC	Mobile Country Code
MCC	Mobile Country Code
MNC	Mobile Network Code
MO	Mobile Originated
MSC	Mobile Switching Center
MSISDN	Mobile Subscriber ISDN Number
MSRN	Mobile Subscriber Roaming Number
MT	Mobile Terminated
NDC	National Dialing Code
ODB	Operator Determined Barring
OTA	Over The Air
O-CSI	Originating CAMEL Subscription Information
PRN	Provide Roaming Number
RNA	Roaming Not Available
RR	Roaming Restricted
SIM	Subscriber Identification Module
SRI	Send Routing Information
SS	Supplementary Services
SS7	Signaling System 7
STP	Signal Transfer Point
TCAP	Transaction Capabilities Application Part

T-CSI	Terminating CAMEL Service Information
VAS	Value Added Service
VLR	Visited Location Register
VMSC	Visited Mobile Switching Center
VPLMN	Visited Public Land Mobile Network
VPMN	Visited Public Mobile Network

CLAIMS

I claim:

1. A method for countering an anti-traffic redirection of a roaming mobile station in a Visiting Public Mobile Network (VPMN) by a Home Public Mobile Network (HPMN), the method comprising the steps of:
   - detecting a forced connection of the roaming mobile station to a non-preferred VPMN by observing exchange of at least one registration message between the VPMN and the HPMN, and
   - steering the roaming mobile station to reinitiate a registration attempt with a preferred VPMN.

2. The method of claim 1, wherein detecting the forced connection comprises passively monitoring the exchange of registration messages between the VPMN and the HPMN.

3. The method of claim 1, wherein detecting the forced connection comprises actively monitoring the exchange of registration messages between the VPMN and the HPMN.

4. The method of claim 1, wherein detecting the forced connection comprises checking a number of LUP messages received within a configurable threshold time interval.

5. The method of claim 4, wherein steering the roaming mobile station comprises sending a Location Update Reject registration message in response to a predefined number of LUP messages received within the configurable threshold time interval.

6. The method of claim 5, wherein the predefined number of LUP messages is one or more.
7. The method of claim 5, wherein the configurable threshold time interval is 15 seconds.

8. The method of claim 4, further comprising the step of statistically configuring the threshold time interval based on the number of LUP messages received within the configurable threshold time interval.

9. The method of claim 1, wherein detecting the forced connection comprises checking for a time gap between two consecutive LUP messages.

10. The method of claim 9, wherein steering the roaming mobile station comprises sending a Location Update Reject message in response to the two consecutive LUP messages received after a gap of a configurable extended time interval.

11. The method of claim 10, wherein the configurable extended time interval is 2 times a configurable threshold time interval.

12. The method of claim 10, wherein the configurable extended time interval is 30 seconds.

13. The method of claim 10, wherein sending the Location Update Reject message is executed only a predetermined number of times.

14. The method of claim 13, wherein the predetermined number is within the range of 1 to 2.

15. The method of claim 1, wherein detecting the forced connection comprises checking for a Location Update (LUP) message received subsequent to a successful registration, within a configurable time interval and for a threshold number of outbound roamers registered with the same VPMN.

16. The method of claim 15, wherein the configurable time interval is 10 minutes.

17. The method of claim 15, wherein the threshold number of outbound roamers is at least one.

18. The method of claim 15, wherein the threshold number of outbound roamers is calculated as a percentage of total outbound roamers registered with the VPMN.

19. The method of claim 1, wherein steering the roaming mobile station comprises sending a MAP-Cancel Location message after a configurable time interval subsequent to issuing a LUP ack to a VPMN.

20. The method of claim 19, wherein the configurable time interval is 10 minutes.

21. The method of claim 1, wherein steering the roaming mobile station comprises sending a MAP-Cancel Location after a configurable time interval subsequent to receiving a MAP RestoreData from a VPMN.

22. The method of claim 21, wherein the configurable time interval is 10 minutes.

23. The method of claim 1, wherein, steering the roaming mobile station comprises sending ISD (RR) for a configurable number of times in response to an ISD ACK with System Failure, Unexpected Data Value and Missing Data.

24. The method of claim 1, wherein detecting the forced connection comprises checking for a Location Update (LUP) message received within a configurable time interval subsequent to a RNA message for a particular mobile station on a particular VPMN.

25. The method as claimed in claim 24, wherein steering the roaming mobile station comprises sending a RNA message, in response to the LUP message received within the configurable time period of sending the last RNA message to the mobile station attempting registration with the VPMN.

26. The method of claim 24, wherein the configurable time period is 20 seconds.

27. The method of claim 1, wherein, steering the roaming mobile station comprises sending a RNA error code in response to a location update request from a VPMN which has disabled OTA messages from the HPMN.

28. A system for countering an anti-traffic redirection of a roaming mobile station in a Visiting Public Mobile Network (VPMN) by a Home Public Mobile Network (HPMN), the system comprising of:
    - a probing block for observing at least one registration message exchanged between the VPMN and the HPMN,
    - a detecting block for detecting a forced connection of the mobile roaming station to a non-preferred VPMN, and
    - a redirection block for steering the roaming mobile station to reinitiate a registration attempt with a preferred VPMN.

29. The system of claim 28, wherein the VPMN and the HPMN are a part of a wireless network.

30. The system of claim 29, wherein the wireless network includes GSM, GPRS, 3G, CDMA, WCDMA, TDMA, WLL, WiFi, WiMax and VoIP networks.

31. The system of claim 28, wherein the probing block intercepts a signaling link between the HPMN and an international STP.

32. The system of claim 31, wherein the probing block passively monitors the registration messages exchanged between the VPMN and the HPMN.

33. The system of claim 28, wherein the probing block is coupled to the HPMN Roaming STP.

34. The system of claim 33, wherein the probing block actively monitors the registration messages exchanged between the VPMN and the HPMN.

35. The system of claim 28, wherein the probing block monitors the registration messages exchanged between a VPMN and a HPMN STP.

36. A computer program product comprising a computer readable medium including a computer readable program code for countering an anti-traffic redirection of a roaming mobile station in a Visiting Public Mobile Network (VPMN) by a Home Public Mobile Network (HPMN), the computer program product comprising:
    - computer readable program code configured for detecting a possible forced connection of the roaming mobile station to a non-preferred VPMN by observing at least one registration message exchanged between the VPMN and the HPMN, and
    - computer readable program code configured for steering the roaming mobile station to reinitiate a registration attempt with a preferred VPMN.

37. The computer program product of claim 36, comprising computer readable program code configured for passively monitoring the registration messages exchanged between the VPMN and the HPMN.

38. The computer program product of claim 36, comprising computer readable program code configured for actively monitoring the registration messages exchanged between the VPMN and the HPMN.

39. The computer program product of claim 36, comprising computer readable program code configured for checking the number of LUP messages received within a configurable threshold time interval.

40. The computer program product of claim 36, comprising computer readable program code configured for sending a Location Update Reject registration message in response to a predefined number of LUP messages received within the configurable threshold time interval.

41. The computer program product of claim 36, comprising computer readable program code for statistically configuring the threshold time interval on the

basis of the number of LUP messages received within the configurable threshold time interval.

42. The computer program product of claim 36 comprising computer readable program code configured for checking for a time gap between two consecutive LUP messages.

43. The computer program product of claim 36, comprising computer readable program code configured for sending a Location Update Reject message in response to two consecutive LUP messages received after a gap of a configurable extended time interval.

44. The computer program product of claim 36, comprising computer readable program code configured for checking for a Location Update (LUP) message received subsequent to a successful Location Update, within a configurable time interval and for a threshold number of outbound roamers registered on the same VPMN.

45. The computer program product of claim 36, comprising computer readable program code configured for sending a MAP-Cancel Location after a configurable time interval subsequent to issuing a LUP ack to a VPMN.

46. The computer program product of claim 36, comprising computer readable program code configured for sending a MAP-Cancel Location after a configurable time interval subsequent to receiving a MAP RestoreData from a VPMN.

47. The computer program product of claim 36, comprising computer readable program code configured for sending ISD (RR) for a configurable number of times in response to an ISD ACK with System Failure, Unexpected Data Value, RNA and Missing Data.

48. The computer program product of claim 36, comprising computer readable program code configured for checking for a Location Update (LUP) message

received within a configurable time interval subsequent to a RNA message for a particular mobile station on a particular VPMN.

49. The computer program product of claim 36, comprising computer readable program code configured for sending a RNA message, in response to the LUP message received within the configurable time period of sending the last RNA message to the mobile station attempting registration with the VPMN.

50. The computer program product of claim 36, comprising computer readable program code configured for sending a RNA error code in response to a location update request from a VPMN.