Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2632454 A1 2007/07/12

(21) 2 632 454

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(86) Date de dépôt PCT/PCT Filing Date: 2006/11/13
(87) Date publication PCT/PCT Publication Date: 2007/07/12
(85) Entrée phase nationale/National Entry: 2008/06/05
(86) N° demande PCT/PCT Application No.: US 2006/043960
(87) N° publication PCT/PCT Publication No.: 2007/078430
(30) Priorité/Priority: 2005/12/15 (US11/300,695)

(51) Cl.Int./Int.Cl. *H04L 29/06* (2006.01)

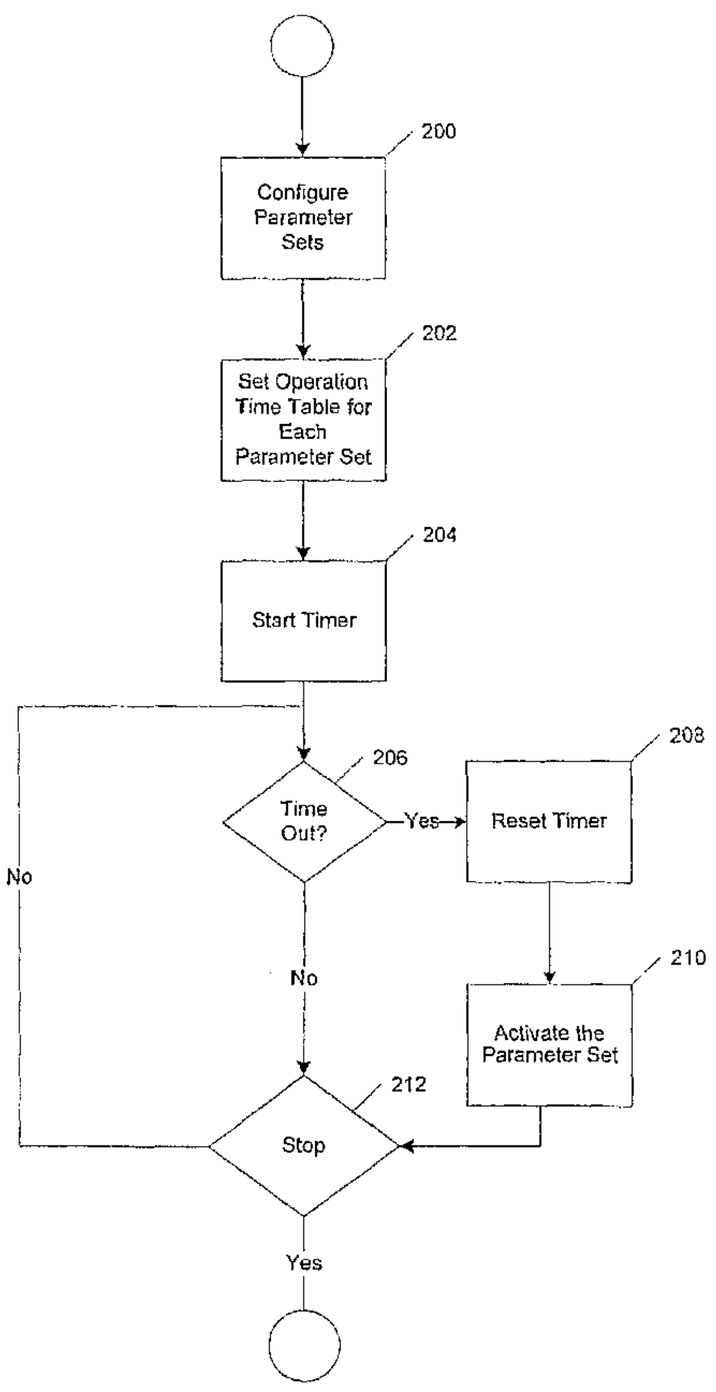
(71) Demandeur/Applicant:
AT&T MOBILITY II LLC, US

(72) Inventeurs/Inventors:
LEE, BO, US;
EASLEY, SCOTT, US;
TAYLOR, RICKIE T., US;
ANDERSSON, FREDRIK, US

(74) Agent: OYEN WIGGS GREEN & MUTALA LLP

(54) Titre : PROCEDES ET APPAREIL POUR LA CONFIGURATION DYNAMIQUE D'AUTHENTIFICATION REALISANT L'AJUSTEMENT DE CONFIGURATION D'AUTHENTIFICATION DANS UN RESEAU

(54) Title: METHODS AND APPARATUS FOR DYNAMIC AUTHENTICATION CONFIGURATION THAT ADJUST AUTHENTICATION CONFIGURATION IN A NETWORK



(57) Abrégé/Abstract:
A method of dynamic authentication configuration that adjust authentication configuration according to traffic patterns within a system, such as a cellular communications network. In a network, mobile devices are authenticated based on various events, such

(21) 2 632 454

(13) A1

(57) Abrégé(suite)/Abstract(continued):
as an attach, location update, originated call, etc. According to a first embodiment, one or more authentication configuration profiles is defined for a VLR/SGSN and a time schedule/table to automatically update the authentication configurations based on a time. Accordingly, the number authentications for a particular VLR is reduced as signaling traffic increases, and vice versa. In another exemplary embodiment, an HLR monitors system level traffic load to command each VLR and SGSN to change the authentication configurations. Authentication operations are preferably configured on per node and per traffic pattern basis.

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

REVISED VERSION

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 July 2007 (12.07.2007)

PCT

(10) International Publication Number
WO 2007/078430 A1

(51) International Patent Classification:
H04L 29/06 (2006.01)

(21) International Application Number:
PCT/US2006/043960

(22) International Filing Date:
13 November 2006 (13.11.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/300,695 15 December 2005 (15.12.2005) US

(71) Applicant *(for all designated States except US)*: **CINGULAR WIRELESS, II, LLC** [US/US]; 5565 Glenridge Connector, Suite 1700, Atlanta, GA 30342 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **LEE, Bo** [US/US]; 310 Milton Oaks Circle, Alpharetta, GA 30022 (US). **EASLEY, Scott** [US/US]; 5460 Oakrun Circle, Cumming, GA 30040 (US). **TAYLOR, Rickie, T.** [US/US]; 2 North Eckerson Lane, Spring Valley, NY 10977 (US). **ANDERSSON, Fredrik** [SE/US]; 3633 Edwards Drive, Plano, TX 75025 (US).

(74) Agent: **JACKSON, Thomas, H.**; BANNER & WITCOFF, LTD., 1001 G. Street, N.W., 11Th Floor, Washington, DC 20001-4597 (US).

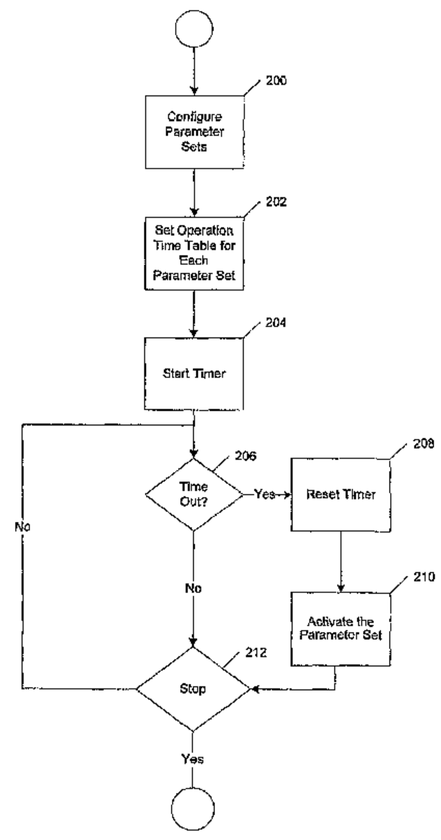
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR,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

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

Published:
— *with international search report*

[Continued on next page]

(54) Title: METHODS AND APPARATUS FOR DYNAMIC AUTHENTICATION CONFIGURATION THAT ADJUST AUTHENTICATION CONFIGURATION IN A NETWORK



(57) Abstract: A method of dynamic authentication configuration that adjust authentication configuration according to traffic patterns within a system, such as a cellular communications network. In a network, mobile devices are authenticated based on various events, such as an attach, location update, originated call, etc. According to a first embodiment, one or more authentication configuration profiles is defined for a VLR/SGSN and a time schedule/table to automatically update the authentication configurations based on a time. Accordingly, the number authentications for a particular VLR is reduced as signaling traffic increases, and vice versa. In another exemplary embodiment, an HLR monitors system level traffic load to command each VLR and SGSN to change the authentication configurations. Authentication operations are preferably configured on per node and per traffic pattern basis.

WO 2007/078430 A1

WO 2007/078430 A1

(88) **Date of publication of the revised international search report:** 14 February 2008

(15) **Information about Correction:** see Notice of 14 February 2008

METHODS AND APPARATUS FOR DYNAMIC AUTHENTICATION CONFIGURATION THAT ADJUST AUTHENTICATION CONFIGURATION IN A NETWORK

FIELD OF THE INVENTION

[01] The present invention is directed to configuring network authentication. In particular, the present invention is directed to a system for providing dynamic authentication configuration information to determine how and when a device is authenticated by the network.

BACKGROUND OF THE INVENTION

[02] Published United States Patent Application US2005/166263 of Nanopoulus et al. of 28 July 2005 discloses an authentication configuration for a computer network. In the Nanopoulus et al. computer network, personal identification numbers (PIN's) or passwords are provided with information from information tokens. An authentication token at time t provides data corresponding to a response At(c). A token output for time t is an input to a has function whose evaluation is compared to a stored record for a computer to gain network access. Consequently, in the art of computer networks, a system and method of providing an authentication configuration having a time variable and as described in Nanopoulus et al. are known.

[03] Global system for mobile communication (GSM) is one of the most widely wireless access systems in today's fast growing communication systems. GSM provides circuit-switched data services to subscribers, such as mobile telephone or computer users. General Packet Radio Service (GPRS), which is an extension to GSM technology, introduces packet switching to GSM networks. GPRS uses a packet-based wireless communication technology to transfer high and low speed data and signaling in an efficient manner. GPRS optimizes the use of network and radio resources, thus enabling the cost effective and efficient use of GSM network resources for packet mode applications.

[04] Authenticating a subscriber's mobile station/handset is desirable because it helps to prevent fraudulent use of an operator's network. However, authentication of mobile stations uses network resources and may create a high system load at peak times. The authentication traffic, however, does not produce any revenue for the operator. Thus, it would be desirable if authentication configuration could be dynamically changed based on call volume, times of day, etc., while maintaining an acceptable level of security.

SUMMARY OF THE INVENTION

[05] A method of dynamic authentication configuration that adjust authentication configuration according to traffic patterns within a system, such as a cellular communications network. In a network, mobile devices are authenticated based on various events, such as an attach, location update, originated call, etc. According to a first embodiment, one or more authentication configuration profiles is defined for a VLR/SGSN and a time schedule/table to automatically update the authentication configurations based on a time. Accordingly, the number of authentications for a particular VLR is reduced as signaling traffic increases, and vice versa. In another exemplary embodiment, an HLR monitors system level traffic load to command each VLR and SGSN to change the authentication configurations. Authentication operations are preferably configured on per node and per traffic pattern basis. In yet another embodiment, authentication is performed on a class of service to which a particular customer may subscribe.

VLR/SGSN and a time schedule/table to automatically update the authentication configurations based on a time. Accordingly, the number authentications for a particular VLR is reduced as signaling traffic increases, and vice versa. In another exemplary embodiment, an HLR monitors system level traffic load to command each VLR and SGSN to change the authentication configurations. Authentication operations are preferably configured on per node and per traffic pattern basis. In yet another embodiment, authentication is performed on a class of service to which a particular customer may subscribe.

[0005] These and other features of the invention will be described in greater detail below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0006] Fig. 1 is an overview of an exemplary wireless communication environment;

[0007] Fig. 2 illustrates an authentication procedure where a Visitor Location Register (VLR) /Serving GPRS Support Node (SGSN) request and receive authentication vectors from an HLR;

[0008] Fig. 3 illustrates an authentication procedure where the VLR /SGSN do not request and receive authentication vectors from Home Location Register (HLR);

[0009] Fig. 4 is a flowchart of exemplary processes performed in accordance with an embodiment of present invention;

[0010] Figs. 5 and 6 are exemplary messages passed between an HLR and a VLR /SGSN;

[0011] Fig. 7 is a flowchart of exemplary processes performed in accordance with another embodiment of present invention; and

[0012] Figs. 8 and 9 are flowcharts of exemplary processes performed to implement authentication classes to provide classes of service.

DETAILED DESCRIPTION OF ILLUSTRATIVE EMBODIMENTS

[0013] Fig. 1 shows a GSM/GPRS network architecture 100 the includes a GSM core network 101 and a GPRS network 130. The GSM core network 101 includes a Mobile Station (MS) 102, at least one Base Transceiver Station (BTS) 104 and a Base Station Controller (BSC) 106. The MS 102 is physical equipment or Mobile Equipment (ME), such as a mobile phone or a laptop computer that is used by mobile subscribers,

with a Subscriber identity Module (SIM). The SIM includes an International Mobile Subscriber Identity (IMSI), which is a unique identifier of a subscriber. The BTS 104 is physical equipment, such as a radio tower, that enables a radio interface to communicate with the MS. Each BTS may serve more than one MS. The BSC 106 manages radio resources, including the BTS. The BSC may be connected to several BTSs. The BSC and BTS components, in combination, are generally referred to as a base station (BSS) or radio access network (RAN) 103.

[0014] The GSM core network 101 also includes a Mobile Switching Center (MSC) 108, a Gateway Mobile Switching Center (GMSC) 110, a Home Location Register (HLR) 112, Visitor Location Register (VLR) 114, an Authentication Center (AuC) 118, and an Equipment Identity Register (EIR) 116. The MSC 108 performs a switching function for the network. The MSC also performs other functions, such as registration, authentication, location updating, handovers, and call routing. The GMSC 110 provides a gateway between the GSM network and other networks, such as an Integrated Services Digital Network (ISDN) or Public Switched Telephone Networks (PSTNs) 120. In other words, the GMSC 110 provides interworking functionality with external networks.

[0015] The HLR 112 is a database that contains administrative information regarding each subscriber registered in a corresponding GSM network. The HLR 112 also contains the current location of each MS. The VLR 114 is a database that contains selected administrative information from the HLR 112. The VLR 114 contains information necessary for call control and provision of subscribed services for each MS currently located in a geographical area controlled by the VLR 114. The HLR 112 and the VLR 114, together with the MSC 108, provide the call routing and roaming capabilities of GSM. The VLR 114 may reside on the same platform as the MSC 108 or the GMSC 110 or a call server. The AuC 116 provides the parameters needed for authentication and encryption functions. Such parameters allow verification of a subscriber's identity. The EIR 118 stores security-sensitive information about the mobile equipment.

[0016] Location services (LCS) are provided by a Gateway Mobile Location Center (GMLC) 111 and/or a Serving Mobile Location Center (SMLC) 113. The GMLC 111 may request routing information from the HLR 112 and send positioning requests to either the Visited Mobile Switching Centre (VMSC, not shown), a Serving GPRS

Support Node (SGSN 132) or MSC 108, and receives final location estimates from the corresponding entity.

[0017] The SMLC 113 is either a separate network element or an integrated functionality in the BSC 106. The SMLC manages the overall coordination and scheduling of resources required for the location of a MS 102. The SMLC 1113 also calculates the final location estimate and estimates the achieved accuracy. The SMLC 113 may control a number of Location Measurement Unit (LMU) for the purpose of obtaining radio interface measurements to locate or help locate MS subscribers in the area that it serves.

[0018] To gain access to GSM services, such as speech, data, and short message service (SMS), the MS first registers with the network to indicate its current location by performing a location update and IMSI attach procedure. The MS 102 sends a location update including its current location information to the MSC 108/VLR 114, via the BTS 104 and the BSC 106. The location information is then sent to the MS's HLR 112. The HLR 112 is updated with the location information received from the MSC108/VLR 114. The location update also is performed when the MS moves to a new location area. Typically, the location update is periodically performed to update the database as location updating events occur.

[0019] The GPRS network 130 is logically implemented on the GSM core network architecture by introducing two packet-switching network nodes, the serving GPRS support node (SGSN) 132 and a Gateway GPRS support node (GGSN) 134. The SGSN 132 is at the same hierarchical level as the MSC 108 in the GSM network. The SGSN 132 controls the connection between the GPRS network and the MS 102. The SGSN 132 also keeps track of individual MS's locations and security functions and access controls. The GGSN 134 provides a gateway between the GPRS network and a public packet network (PDN) or other IP networks 136. That is, the GGSN provides interworking functionality with external networks, and sets up a logical link to the MS through the SGSN 132. When packet-switched data leaves the GPRS network, it is transferred to an external TCP-IP network 136, such as an X.25 network or the Internet. In order to access GPRS services, the MS first attaches itself to the GPRS network by performing an attach procedure. The MS then activates a packet data protocol (PDP) context, thus activating a packet communication session between the MS, the SGSN 132, arc the GGSN.

[0020] In a GSM/GPRS network, GPRS services and GSM services can be used in parallel. The MS can operate in one three classes: class A, class B, and class C. A class A MS can attach to the network for both GPRS services and GSM services simultaneously. A class A MS also supports simultaneous operation of GPRS services and GSM services. For example, class A mobiles can receive GSM voice/data/SMS calls and GPRS data calls at the same time.

[0021] A class B MS can attach to the network for both GPRS services and GSM services simultaneously. However, a class B MS does not support simultaneous operation of the GPRS services and GSM services. That is, a class B MS can only use one of the two services at a given time.

[0022] A class C MS can attach for only one of the GPRS services and GSM services at a time. Simultaneous attachment and operation of GPRS services and GSM services is not possible with a class C MS.

[0023] A GPRS network 130 can be designed to operate in three network operation modes (NOM1, NOM2 and NOM3). A network operation modes of a GPRS network is indicated by a parameter in system information messages transmitted within a cell. The system information messages dictates a MS where to listen for paging messages and how signal towards the network. The network operation mode represents the capabilities of the GPRS network. In a NOM1 network, a MS can receive pages from a circuit switched domain (voice call) when engaged in a data call. The MS can suspend the data call or take both simultaneously, depending on the ability of the MS, In a NOM2 network, a MS may not received pages from a circuit switched domain when engaged in a data call, since the MS is receiving data and is not listening to a paging channel In a NOM3 network, a MS can monitor pages for a circuit switched network while received data and vise versa.

[0024] Figs. 2-3 illustrate exemplary authentication processes used in GSM and Universal Mobile Telecommunications Systems (UMTS). Authentication can be selectively invoked with predefined occurrences for specific traffic events through parameter settings. Such events include: International Mobile Subscriber Identity (IMSI) attachments, location updates, routing area updates, normal calls, and bearer service requests, etc., as configured by the network operator. Once specified, these parameter settings are applicable to all subscribers served by a VLR 114 or a SGSN 132.

[0025] As shown in Fig 2, for authentication following the first attach, a VLR 114 or a SGSN 132 requests one to five authentication vectors from the HLR 112. As

shown in Fig. 3, if the VLR 114 and the SGSN 132 is configured to request more than one vector and to use all of the authentication vectors, they will not need to request and receive new authentication vectors from the HLR 112 until there are no unused vectors remaining.

[0026] Authentication provides protection to wireless network by providing secure wireless services. The description of authentication described above is applicable to GSM/GPRS/UMTS systems. However, as noted above, authentication will also increase signaling traffic, which consumes network resources. Conventionally, most authentication procedures are invoked by statically configured thresholds. During busy hours, non-revenue generating authentication processes compete with other revenue generating traffic handling processes. During non-busy hours, authentication processes generally consume idling network resources and do not compete with traffic handling processes.

[0027] The present invention improves upon handling of authentication to improve an operator's return on operations while minimizing fraud and the impact to network capacity. For greatest effectiveness, authentication operations are preferably configured on per node and per traffic pattern basis. In particular, solutions that adjust authentication configuration according to traffic patterns within a system provide an advantageous solution. A first exemplary embodiment allows operator to define an authentication configuration profile for each VLR 114 and SGSN 132 and a time schedule/table for each node to automatically update the authentication configurations. Another exemplary embodiment enables the HLR 112 to monitor system level traffic load to command each VLR 114 and SGSN 132 to change the authentication configurations.

[0028] Referring to Fig. 4, the first embodiment provides that sets of authentication parameters that are predefined for low signaling traffic, medium signaling traffic and high signaling traffic (200). The exemplary Parameter Sets are shown in Tables 1 and 2 below. An exemplary time table is predefined for each VLR 114 and SGSN 132 where the sets are active (202).

	Time 1 (Off Peak 1)	Time 2 (Peak 1)	Time 3 (Off Peak 2)	Time 4 (Peak 2)
Time Variable	(8:00pm – 6:00am)	(6:00am – 10:00am)	(10:00am – 3:00pm)	(3:00pm – 8:00pm)
Parameter Set	1	2	1	2

Time Table 1

[0029] Each segment in the time table is associated with a set of the predefined parameters as shown in Tables 1 and 2. For example, the low signaling traffic time period is associated with Parameter Set 1; the medium signaling traffic period is associated with Parameter Set 2; and the high signaling traffic period is associated with Parameter Set 3.

[0030] A timer is started (204) and after it times-out (206) it is reset (208) and the appropriate parameter set for the time period is activated (210). As such, the set of parameters is automatically activated when its operation time arrives. Next, it is determined if the process should stop (212). If so, the process stops; otherwise it returns to (206) to wait for the timer time-out.

Parameter Set 1		Parameter Set 2		Parameter Set 3	
Traffic Event	Threshold for Event Counter	Traffic Event	Threshold for Event Counter	Traffic Event	Threshold for Event Counter
Attach	1	Attach	1	Attach	1
Normal Location Update	20	Normal Location Update	50	Normal Location Update	0
Periodic Location Update	20	Periodic Location Update	250	Periodic Location Update	0
Mobile-Originated Call	20	Mobile-Originated Call	50	Mobile-Originated Call	0
Mobile-Originated SMS	20	Mobile-Originated SMS	0	Mobile-Originated SMS	0
Mobile-Terminated Call	20	Mobile-Terminated Call	50	Mobile-Terminated Call	0
Mobile-Terminated SMS	20	Mobile-Terminated SMS	0	Mobile-Terminated SMS	0
Mobile-Terminated USSD	20	Mobile-Terminated USSD	0	Mobile-Terminated USSD	0
Mobile Location Service	20	Mobile Location Service	0	Mobile Location Service	0
Supplementary Service Operation	20	Supplementary Service Operation	0	Supplementary Service Operation	0

Table 1 - Parameter Set for VLR 114

Parameter Set 1		Parameter Set 2		Parameter Set 3	
Traffic Event	Threshold for Event Counter	Traffic Event	Threshold for Event Counter	Traffic Event	Threshold for Event Counter
Attach	1	Attach	1	Attach	1
Normal RA Update	30	Normal RA Update	70	Normal RA Update	0
Periodic RA Update	30	Periodic RA Update	250	Periodic RA Update	0
Mobile-Originated PDP Context Activation	30	Mobile-Originated PDP Context Activation	50	Mobile-Originated PDP Context Activation	0
Mobile-Originated PDP Context Deactivation	30	Mobile-Originated PDP Context Deactivation	70	Mobile-Originated PDP Context Deactivation	0
Mobile-Initiated PDP Modification	30	Mobile-Initiated PDP Modification	70	Mobile-Initiated PDP Modification	0
Mobile-Originated SMS	30	Mobile-Originated SMS	70	Mobile-Originated SMS	0
Mobile-Terminated SMS	30	Mobile-Terminated SMS	70	Mobile-Terminated SMS	0
GPRS Detach	30	GPRS Detach	0	GPRS Detach	0

Table 2 - Parameter Set for SGSN 132

[0031] The first embodiment above can be advantageously implemented in conventional GSM networks 100 without any changes to existing protocols. Each network operator may implement the Parameter Sets in a manner suitable for that operator at time periods that reflect signaling loads in systems on a local, regional or national basis.

[0032] Referring to Figs. 5-7 and Tables 1 and 2, a second embodiment also provides sets of authentication parameters for low signaling traffic, medium signaling traffic, and high signaling traffic. In this embodiment, the HLR 112 monitors traffic events from VLRs 114 (in the MSC 108/VLR 114, call sever, etc.) and SGSNs 132 to control the authentication parameters. The HLR 112 uses thresholds to determine signaling traffic load status to direct VLRs 114 and SGSNs 132 to change an authentication parameter set according to signaling traffic load.

[0033] For the HLR 112 and VLR 114 or SGSN 132 to exchange info for updating authentication parameter sets, a pair of MAP messages, such as those shown in Figs. 5 and 6 may be used for the interfaces between HLR 112/VLR 114 and HLR 112/SGSN 132. Thus, the second embodiment may require a change to conventional GSM networks 100 to implement the messaging protocol.

[0034] The message components from HLR 112 (Fig. 5) include the node (VLR 114 and SGSN 132) identity, instruction identity, and identity for the authentication parameter. It is preferable for HLR 112 to direct each VLR 114 or SGSN 132 individually. After a VLR 114 or SGSN 132 receives the direction from the serving HLR 112, the VLR 114 or SGSN 132 makes the new set of authentication parameters effective in a predefined time. The acknowledge message (Fig. 6) components from VLR 114 and SGSN 132 to the HLR 112 include HLR 112 identity and instruction identity that indicates success or failure and an error code associated with the parameter set.

[0035] Turning to Fig. 7, there is flow chart of the exemplary processes performed by this embodiment. Initially, the parameter sets and load thresholds are configured (216). In non-busy hours, the authentication parameters may be set to include more traffic events and to be invoked more frequently. In busy hours, the authentication parameters may be set to include less traffic events and to be invoked less frequently. When the signaling load on HLR 112 is very high, the authentication parameters may be set to include the least traffic events and to be invoked the least frequently.

[0036] Weights are configured for a load formula, which is used to determine a signaling load (218). Next, a time period for monitoring the signaling load is set in the HLR 112 (220). The dynamic automatic authentication configuration mechanism to adjust parameter sets is then enabled (222). A timer is started, that after a time-out period, is reset and a snapshot of the signaling load is taken (224-228).

[0037] To assess the signaling traffic load, the HLR 112 may weigh events impacting capacity (228). For example:

Signaling load = weight1 * Average CPU Utilization + weight2 * SRI causing PRN + weight3 * Location Update Requests + weight4 * LU Requests (No ISD 3GPP SC) + weight5 * CISS Requests + weight6 * SMS Routing Requests + weight 7 * Report SM Delivery Requests + weight8 * Ready For SM Requests + weight9 * USSD Requests and Indications + weight10 * Standby Requests + weight10 * Send Routing Info for LCS Requests + weight11 * Message Diversions + weight12 * ATSI Requests + weight13 * ATMod Requests.

[0038] The above traffic events are understood by those of ordinary skill in the art and it is appreciated that fewer or greater numbers of events may be weighted to arrive at a signaling load. The weights may be determined through empirical tests, analysis, etc., and adjusted to compensate for actual performance.

[0039] A set of thresholds are used to assess low signaling traffic, medium signaling traffic, high signaling traffic, and very high signaling traffic, to which the signaling load is compared (230). If the signaling load exceeds a higher threshold (232), the VLR 114/SGSN 132 is informed that it should move to a higher load parameter set (238). The VLR 114/SGSN 132 is sent a message, such as that in Fig. 5 and the parameters are changed to the appropriate higher Parameter Set (240, 242). A timer may be used in the VLR 114/SGSN 132 to make the new authentication Parameter Set effective. The VLR 114/SGSN 132 acknowledges the change by returning an acknowledgement such as that in Fig. 6 (244).

[0040] If at 232 the signaling traffic does not exceed the higher threshold, it is determine if it exceeds (i.e., is lower than) a lower threshold (234). If so, the VLR 114/SGSN 132 is informed that it should move to a lower load parameter set (236). The VLR 114/SGSN 132 is sent a message and the parameters are changed to the appropriate lower Parameter Set (240, 242). A timer may be used in the VLR 114/SGSN 132 to make the new authentication Parameter Set effective. The VLR 114/SGSN 132 acknowledges the change by returning a acknowledgement message (244).

[0041] In addition to applying the various Parameter Sets based on signaling load, the Parameter Sets may be applied to classes of service. For example, a customer may require a high level of authentication for mobile devices associated with the customer. Accordingly, Parameter Set 1, for example, may be applied to all of the customer's mobile devices at all times, whereas, other customers may have Parameter Set 3 applied to their devices due to signaling traffic, etc. Implementing this alternative will ensure that customer's devices are authenticated prior and during use to further secure the data being communicated thereby, thus allaying fears of unauthorized use or tampering.

[0042] Figs. 8 and 9 and an exemplary Time Table 2 illustrate classes of service in accordance with the present invention. Referring to Fig. 8, a first implementation adds the sets of authentication parameters for low signaling traffic, medium signaling traffic and high signaling traffic (Tables 1 and 2) to a subscriber profile (250). Time Table 2 is predefined for each VLR 114 and SGSN 132 where the sets are active and for each authentication class (252, 254).

	Time 1 (Off Peak 1)	Time 2 (Peak 1)	Time 3 (Off Peak 2)	Time 4 (Peak 2)
Time Variable	(8:00pm – 6:00am)	(6:00am – 10:00am)	(10:00am – 3:00pm)	(3:00pm – 8:00pm)

AuthClass1	Parameter Set 1	Parameter Set 1	Parameter Set 1	Parameter Set 1
AuthClass2	Parameter Set 2	Parameter Set 2	Parameter Set 2	Parameter Set 2
AuthClass3	Parameter Set 3	Parameter Set 3	Parameter Set 3	Parameter Set 3
AuthClass4	Parameter Set 1	Parameter Set 2	Parameter Set 1	Parameter Set 2
AuthClass5	Parameter Set 1	Parameter Set 3	Parameter Set 1	Parameter Set 3
AuthClass6	Parameter Set 2	Parameter Set 3	Parameter Set 2	Parameter Set 3

Time Table 2

[0043] A timer is started for each authentication class (256) and after any time for any authentication class times-out (258) it is reset (260) and the appropriate parameter set for the time period and authentication class is activated (262). As such, the set of parameters is automatically activated when its operation time arrives. Next, it is determined if the process should stop (264). If so, the process stops; otherwise it returns to (258) to wait for a timer to time-out.

[0044] Turning to Fig. 9, there is flow chart of the exemplary processes performed by another class of service embodiment. Initially, the parameter sets, load thresholds and authentication classes are configured (266). Weights are configured for a load formula for each authentication class, which is used to determine a signaling load (268). Next, a time period for monitoring the signaling load is set in the HLR 112 (270). The automatic mechanism to adjust parameter sets for authentication classes is then enabled (272). A timer is started for each monitored authentication class. After a time-out period for each class, each timer is reset and a snapshot of the signaling load is taken (274, 276).

[0045] To assess the signaling traffic load, the HLR 112 may weigh events impacting capacity (278) using weights such as those defined above with regard to Fig. 7. A set of thresholds are used to assess low signaling traffic, medium signaling traffic, high signaling traffic, and very high signaling traffic, to which the signaling load for the authentication class is compared (280). If the signaling load exceeds a higher threshold (282), the VLR 114/SGSN 132 is informed that it should move to a higher load parameter set (288). The VLR 114/SGSN 132 is sent a message, such as that in Fig. 5 and the parameters are changed to the appropriate higher Parameter Set (290, 292). A timer may be used in the VLR 114/SGSN 132 to make the new authentication Parameter Set effective. The VLR 114/SGSN 132 acknowledges the change by returning an acknowledgement such as that in Fig. 6 (294).

[0046] If at 282 the signaling traffic does not exceed the higher threshold, it is determine if it exceeds (i.e., is lower than) a lower threshold (284). If so, the VLR 114/SGSN 132 is informed that it should move to a lower load parameter set (286). The

VLR 114/SGSN 132 is sent a message and the parameters are changed to the appropriate lower Parameter Set (290, 292). A timer may be used in the VLR 114/SGSN 132 to make the new authentication Parameter Set effective. The VLR 114/SGSN 132 acknowledges the change by returning a acknowledgement message (294).

[0047] While the present invention has been described in connection with the preferred embodiments of the various Figs., it is to be understood that other similar embodiments may be used or modifications and additions may be made to the described embodiment for performing the same function of the present invention without deviating therefrom. For example, one skilled in the art will recognize that the present invention as described in the present application may apply to any environment (e.g., GSM/GPRS/UMTS, etc.), whether wired or wireless, and may be applied to any number of such devices connected via a communications network and interacting across the network. Therefore, the present invention should not be limited to any single embodiment, but rather should be construed in breadth and scope in accordance with the appended claims.

What is claimed:

1. A method of providing dynamic authentication configuration in a network, comprising: defining sets of authentication parameters; defining segments of time that are associated with particular ones of said sets of authentication parameters; and applying a particular one of said sets of authentication parameters based on a comparison of a current time to said segments of time

CHARACTERIZED BY

defining a signaling traffic load (224-228; 276,278), said sets of authentication parameters being based on the defined signaling traffic load.

2. The method of claim 1,

FURTHER CHARACTERIZED BY

said defining sets of authentication parameters comprising defining parameter sets for low signaling traffic, medium signaling traffic and high signaling traffic (FIG's 5-7; FIG. 8).

3. The method of claim 1,

FURTHER CHARACTERIZED BY

defining traffic events within said sets of authentication parameters (FIG.'s 2-3); and defining thresholds for event counters associated with said traffic events (Table 1, 2).

4. The method of claim 3,

FURTHER CHARACTERIZED BY

setting first thresholds (230, 280) for a first set associated with low signaling traffic to authenticate based on a first number of traffic events; and setting second thresholds (230, 280) for a second set associated with a higher amount of signaling traffic to authenticate based on a second number of traffic events less than said first number of traffic events.

5. The method of claim 1,

FURTHER CHARACTERIZED BY

providing said sets of authentication parameters to a cellular telecommunications network (FIG. 1); and applying said sets of authentication parameters to at least one of a Visitor Location Register (VLR 114) or a Serving GPRS Support Node (SGSN 132).

6. A method of providing dynamic authentication configuration in a network, comprising:

defining sets of authentication parameters

CHARACTERIZED BY

monitoring traffic events (Tables 1 and 2);

determining a signaling traffic load (200) based on said traffic events; and

applying a predefined set of authentication parameters based on said signaling load (Tables 1 and 2).

7. The method of claim 6,

FURTHER CHARACTERIZED BY

said sets of authentication parameters comprising sets of authentication parameters for low signaling traffic, medium signaling traffic, and high signaling traffic (200).

8. The method of claim 6,

FURTHER CHARACTERIZED BY

communicating a message from a database (HLR 112) to a registerer of devices (VLR 114; SGSN 132) attempting to authenticate with said network (FIG. 1) to inform said registerer that it should change sets.

9. The method of claim 8,

FURTHER CHARACTERIZED BY

said message being communicated to a specific registerer and including flags (FIG. 5) to activate or deactivate said sets of authentication parameters.

10. The method of claim 9,

FURTHER CHARACTERIZED BY

communicating an acknowledgement (FIG. 6) to said database.

11. The method of claim 6,

FURTHER CHARACTERIZED BY

comparing said signaling traffic load to a higher threshold (232) and a lower threshold (234) to determine which of said sets of authentication parameters should be applied.

12. The method of claim 6,

FURTHER CHARACTERIZED BY

determining said signaling traffic load based on a weighted sum (228) of said traffic events.

13. The method of claim 12,

FURTHER CHARACTERIZED BY

said network (FIG. 1) comprising a cellular telecommunications network and said traffic events comprising at least one of: CPU Utilization, SRI causing PRN, Location Update Requests, CISS Requests, SMS Routing Requests, Report SM Delivery Requests, Ready For SM Request, USSD Requests and Indications, Standby Requests, Send Routing Info for LCS Requests, Message Diversions, ATSI Requests and ATMod Requests.

14. The method of claim 6,

FURTHER CHARACTERIZED BY

providing said sets of authentication parameters (200; 216; 266) to a cellular telecommunications network (FIG. 1); and applying said sets of authentication parameters to

at least one of a Visitor Location Register (VLR 114) or a Serving GPRS Support Node (SGSN 132).

15. The method of claim 6,

FURTHER CHARACTERIZED BY

defining classes of services (268) within said network; and applying said sets of authentication parameters (272) differently to each defined class of service.

16. A cellular telecommunications network comprising: a home location register (HLR); a visitor location register (VLR); and a Serving GPRS Support Node (SGSN)

CHARACTERIZED BY

one of said visitor location register (114) and said Serving GPRS Support Node (132) comprising memory for storing defined sets of authentication parameters for predetermined signaling loads (230; 280) and one of said visitor location register and said Serving GPRS Support Node applying a particular set (242; 292) based on a determined signaling load within said cellular telecommunications network.

17. The network of claim 16,

CHARACTERIZED BY

one of said visitor location register (114) and said Serving GPRS Support Node (132) applying said particular set based on a time period selected according to signaling traffic load (FIG. 4; 7; 8; 9).

18. The network of claim 16,

CHARACTERIZED BY

one of said visitor location register (114) and said Serving GPRS Support Node (132) applying said particular set based on a comparison of said signaling load to a threshold (230; 280).

19. The network of claim 18,

FURTHER CHARACTERIZED BY

said at least one of said VLR (114) and said SGSN (132) receiving a message (FIG. 5) to apply said particular set.

20. The network of claim 16, wherein classes of services are defined within said cellular telecommunications network,

CHARACTERIZED BY

one of said visitor location register (114) and said Serving GPRS Support Node (132) applying said sets of authentication parameters differently (FIG. 9) for each defined class of service.

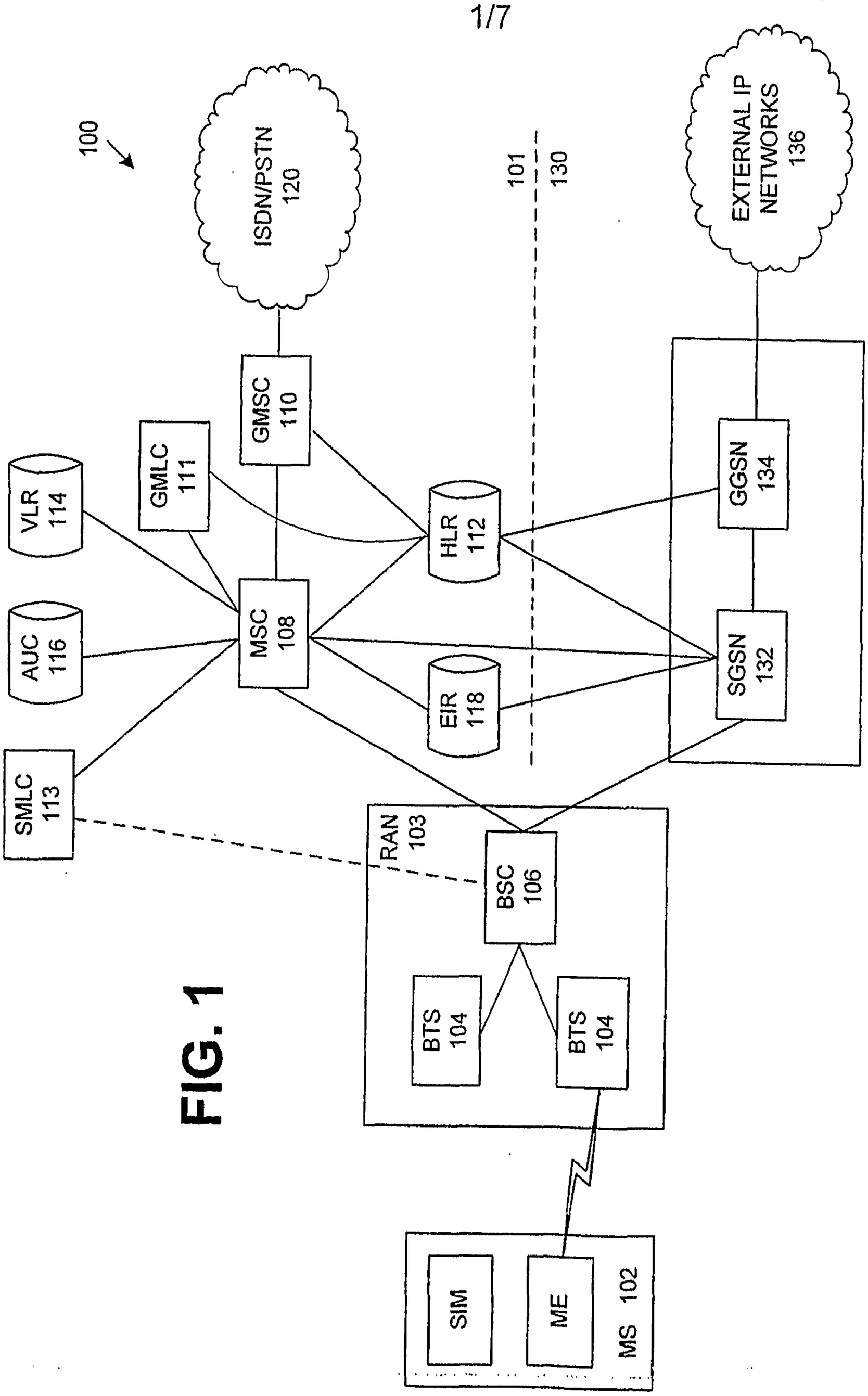

100
ISDN/PSTN 120
101
130
EXTERNAL IP NETWORKS 136
GMSC 110
GMLC 111
VLR 114
HLR 112
GGSN 134
AUC 116
MSC 108
EIR 118
SGSN 132
SMLC 113
RAN 103
BSC 106
BTS 104
BTS 104
SIM
ME
MS 102

FIG. 1

Fig. 2

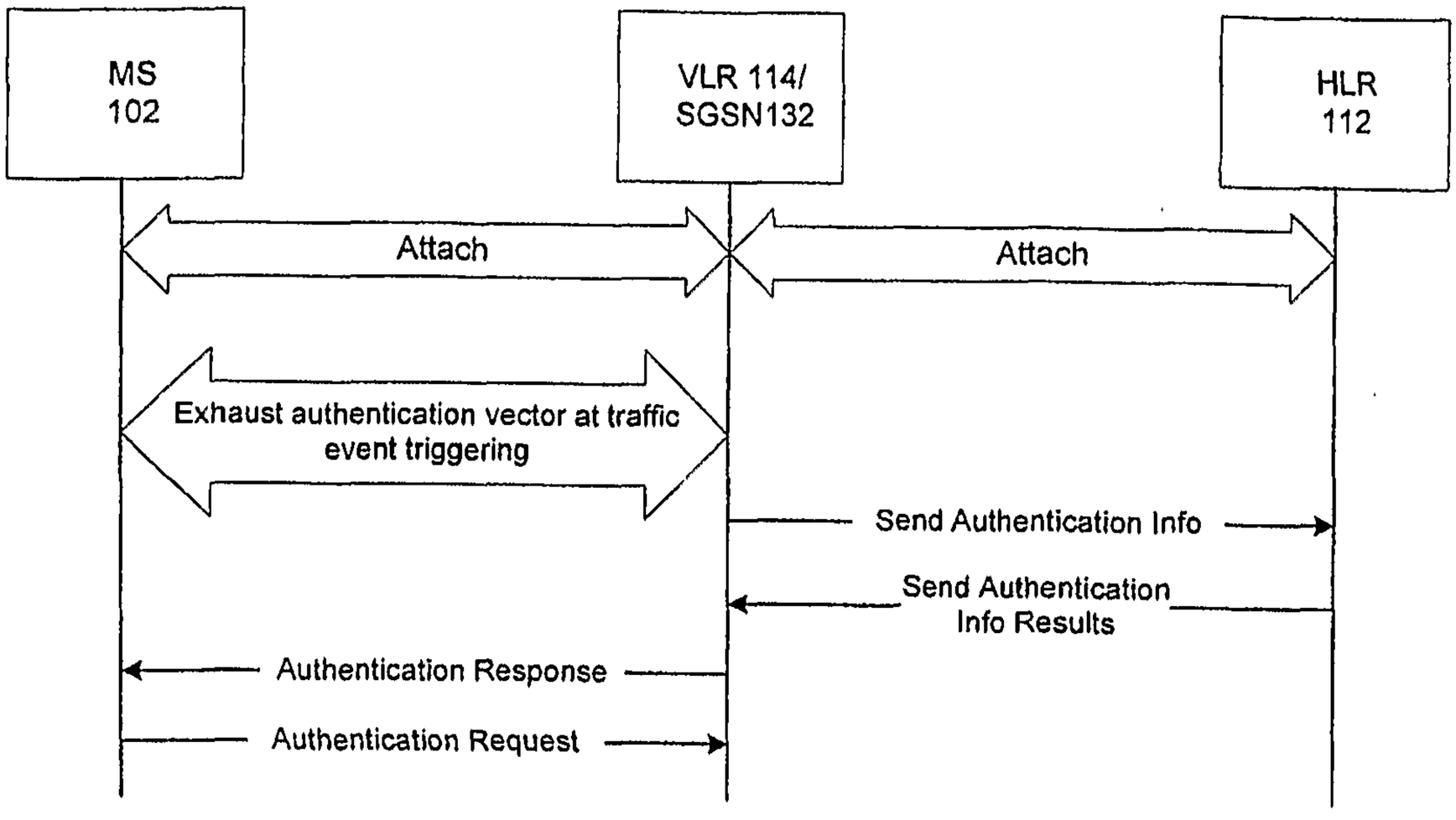

MS
102
VLR 114/
SGSN132
HLR
112
Attach
Attach
Exhaust authentication vector at traffic event triggering
Send Authentication Info
Send Authentication Info Results
Authentication Response
Authentication Request

Fig. 3

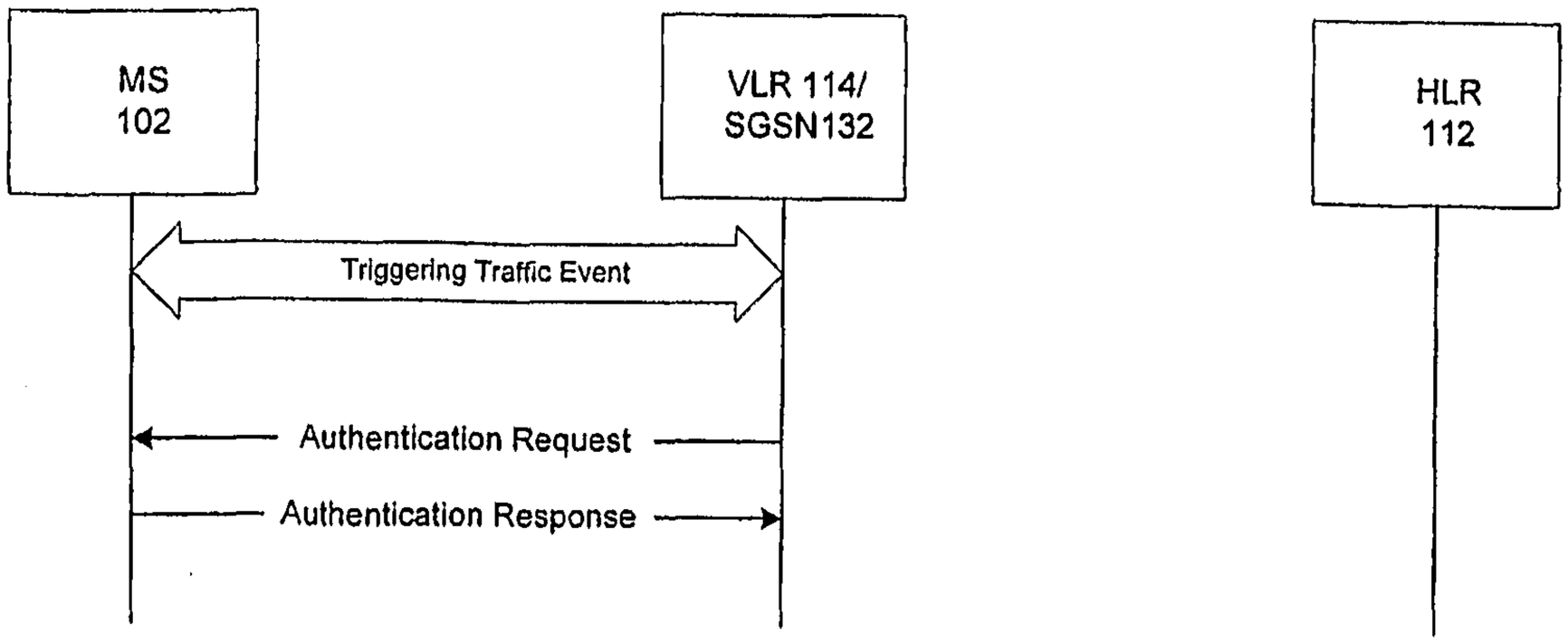

MS
102
VLR 114/
SGSN132
HLR
112
Triggering Traffic Event
Authentication Request
Authentication Response

Fig. 4

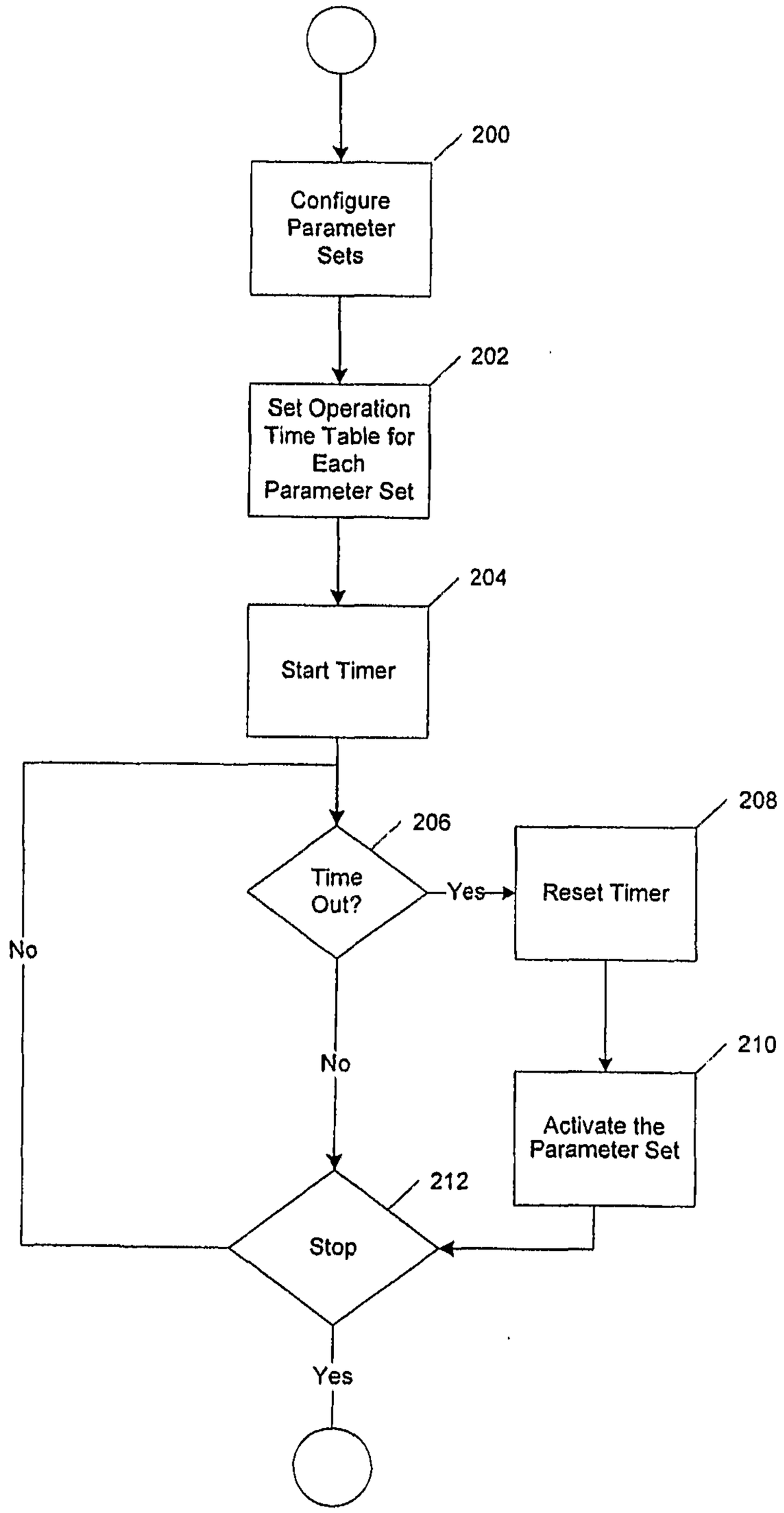

200
Configure Parameter Sets
202
Set Operation Time Table for Each Parameter Set
204
Start Timer
206
Time Out?
Yes
208
Reset Timer
No
No
210
Activate the Parameter Set
212
Stop
Yes

Fig. 5

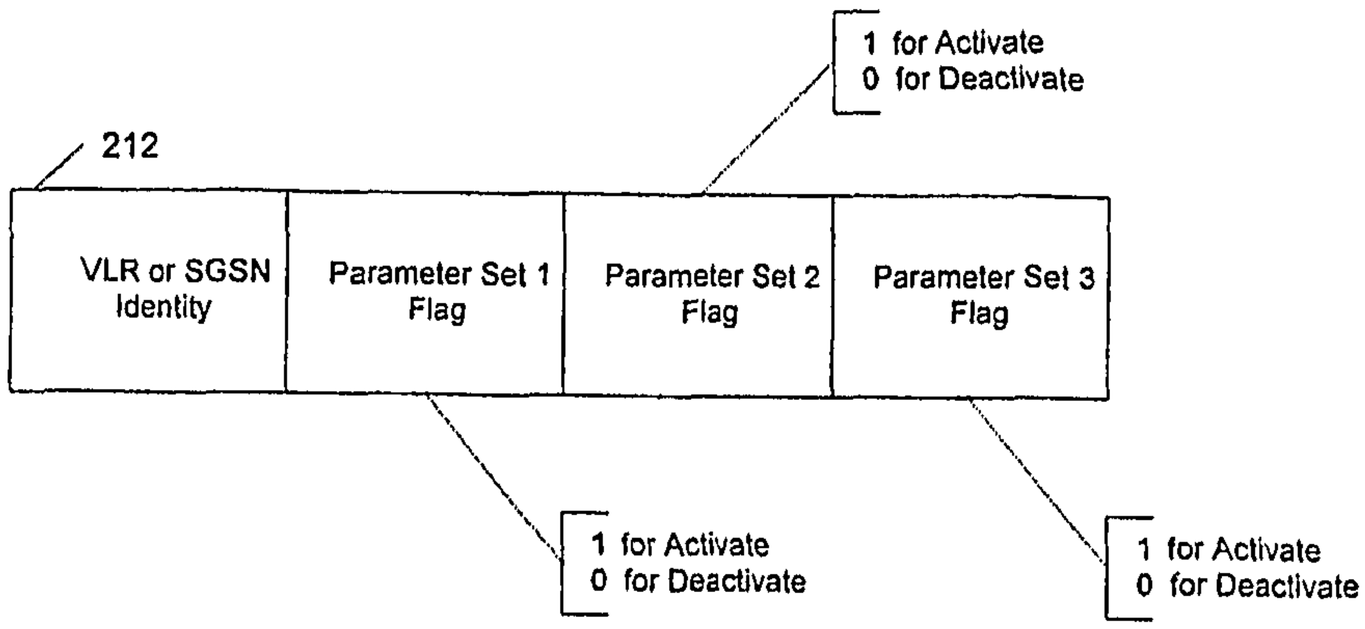

212
1 for Activate
0 for Deactivate
VLR or SGSN Identity
Parameter Set 1 Flag
Parameter Set 2 Flag
Parameter Set 3 Flag
1 for Activate
0 for Deactivate
1 for Activate
0 for Deactivate

Fig. 6

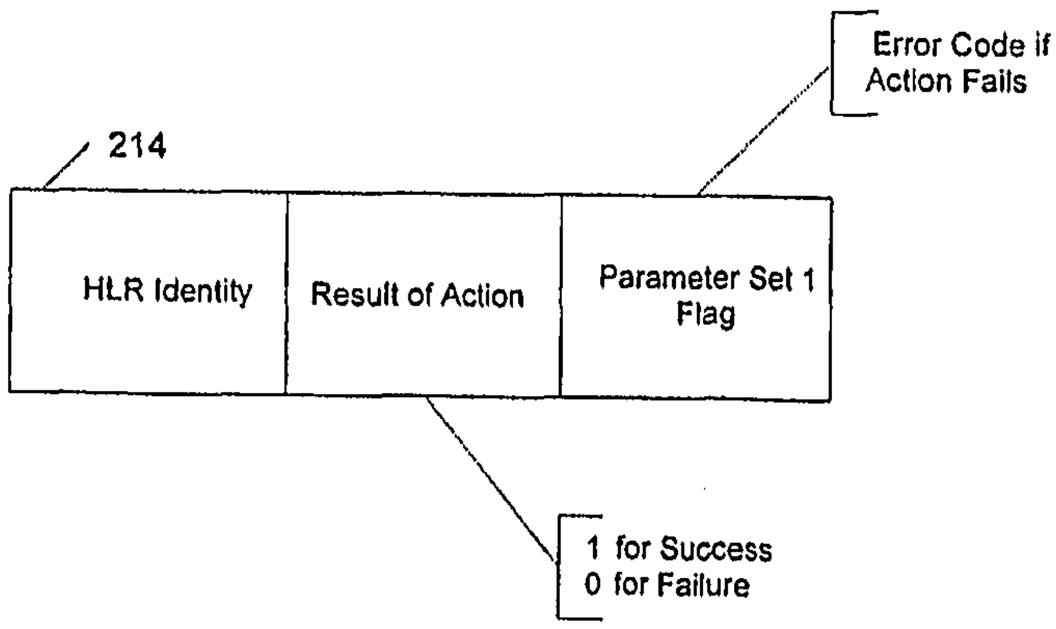

Error Code if Action Fails
214
HLR Identity
Result of Action
Parameter Set 1 Flag
1 for Success
0 for Failure

Fig. 7

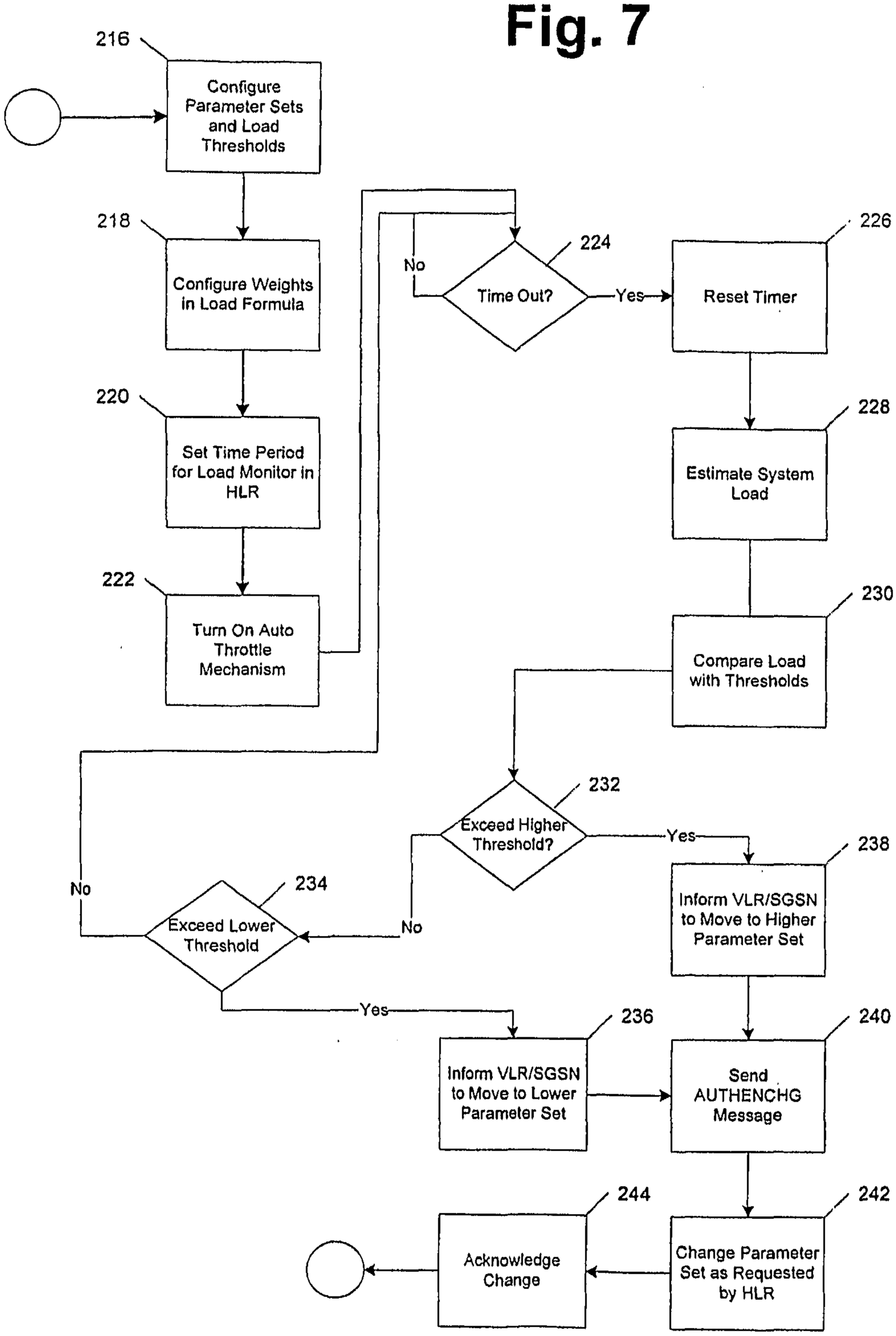
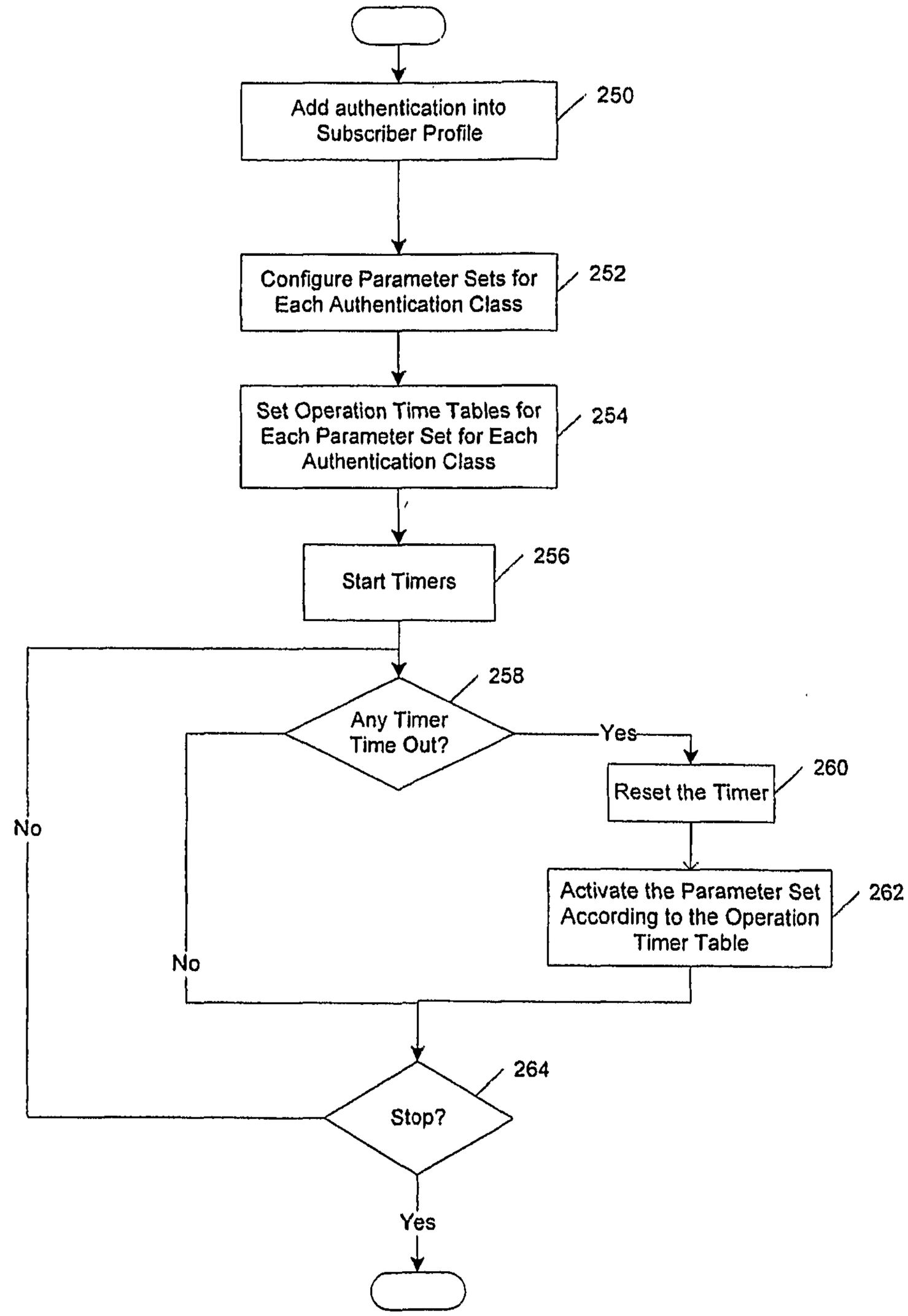

216
Configure Parameter Sets and Load Thresholds
218
Configure Weights in Load Formula
220
Set Time Period for Load Monitor in HLR
222
Turn On Auto Throttle Mechanism
224
Time Out?
No
Yes
226
Reset Timer
228
Estimate System Load
230
Compare Load with Thresholds
232
Exceed Higher Threshold?
Yes
238
Inform VLR/SGSN to Move to Higher Parameter Set
234
Exceed Lower Threshold
No
No
Yes
236
Inform VLR/SGSN to Move to Lower Parameter Set
240
Send AUTHENCHG Message
242
Change Parameter Set as Requested by HLR
244
Acknowledge Change

Fig. 8


Add authentication into Subscriber Profile
250
Configure Parameter Sets for Each Authentication Class
252
Set Operation Time Tables for Each Parameter Set for Each Authentication Class
254
Start Timers
256
Any Timer Time Out?
258
Yes
Reset the Timer
260
Activate the Parameter Set According to the Operation Timer Table
262
No
No
Stop?
264
Yes

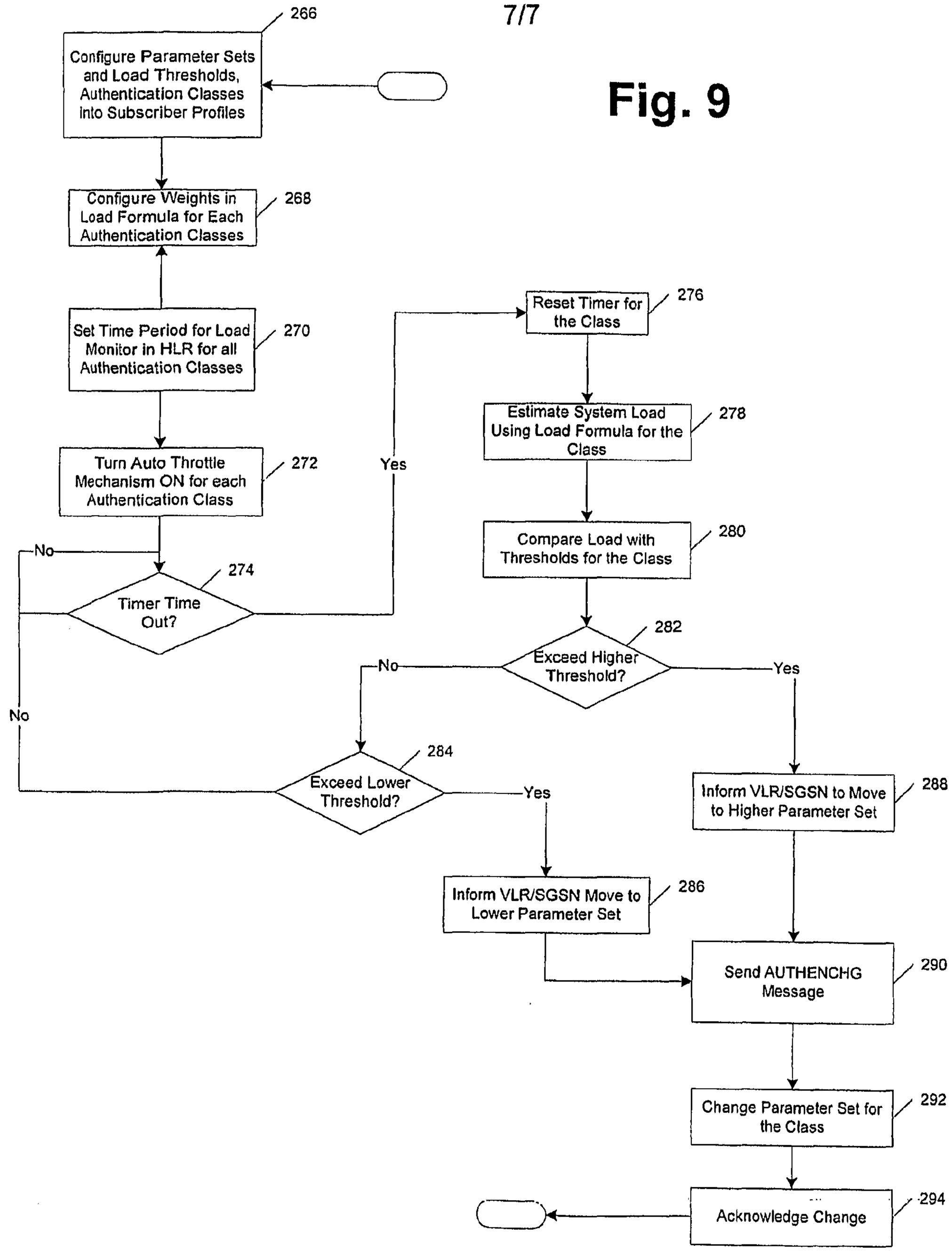
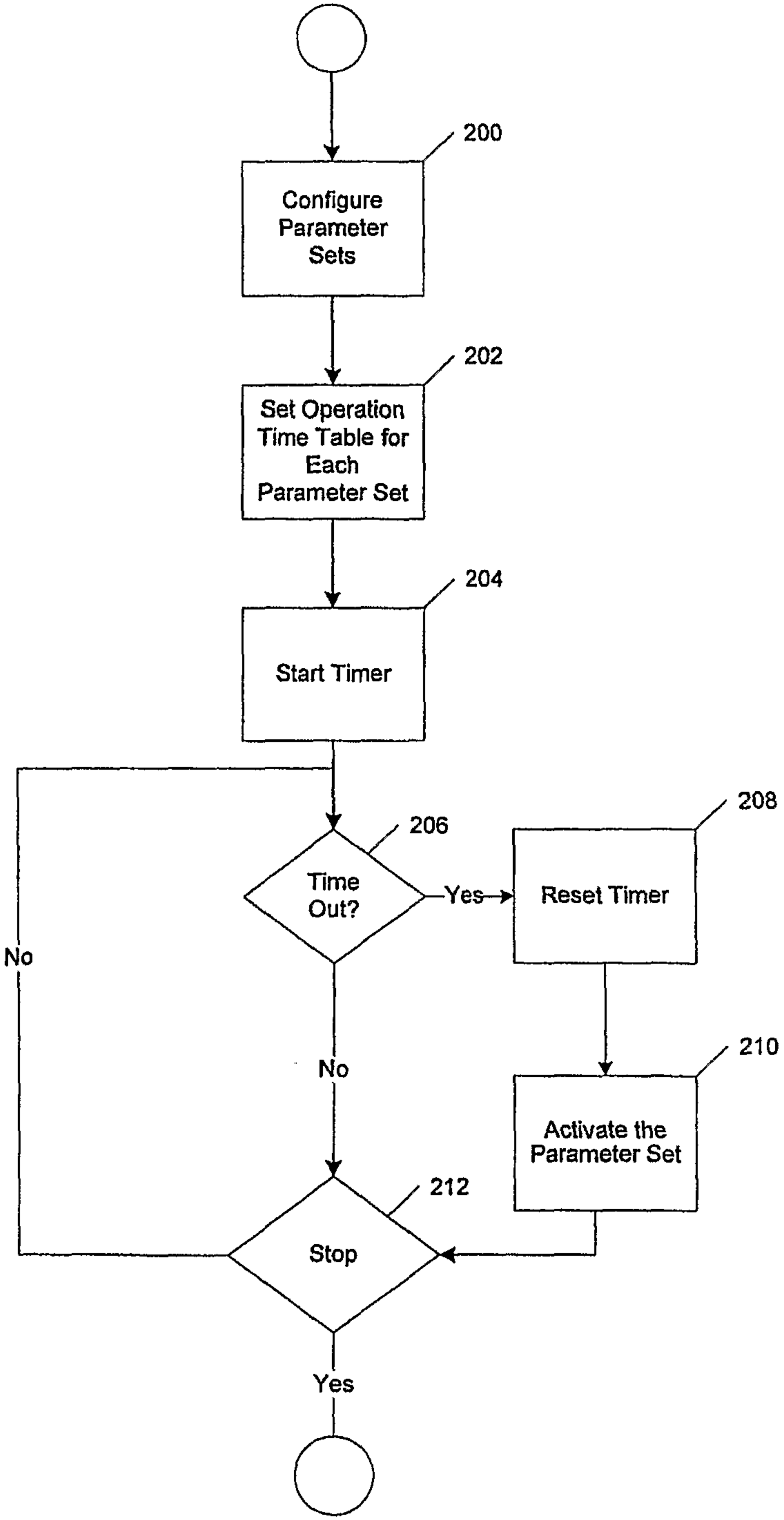

266
Configure Parameter Sets and Load Thresholds, Authentication Classes into Subscriber Profiles
Configure Weights in Load Formula for Each Authentication Classes
268
Set Time Period for Load Monitor in HLR for all Authentication Classes
270
Turn Auto Throttle Mechanism ON for each Authentication Class
272
No
Timer Time Out?
274
No
Yes
Reset Timer for the Class
276
Estimate System Load Using Load Formula for the Class
278
Compare Load with Thresholds for the Class
280
Exceed Higher Threshold?
282
No
Yes
Exceed Lower Threshold?
284
Yes
Inform VLR/SGSN Move to Lower Parameter Set
286
Inform VLR/SGSN to Move to Higher Parameter Set
288
Send AUTHENCHG Message
290
Change Parameter Set for the Class
292
Acknowledge Change
294

Fig. 9


200
Configure Parameter Sets
202
Set Operation Time Table for Each Parameter Set
204
Start Timer
206
Time Out?
Yes
208
Reset Timer
210
Activate the Parameter Set
No
No
212
Stop
Yes