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

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2574578 A1 2006/02/02

(21) 2 574 578

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(86) Date de dépôt PCT/PCT Filing Date: 2005/07/20
(87) Date publication PCT/PCT Publication Date: 2006/02/02
(85) Entrée phase nationale/National Entry: 2007/01/19
(86) N° demande PCT/PCT Application No.: US 2005/025810
(87) N° publication PCT/PCT Publication No.: 2006/012381
(30) Priorité/Priority: 2004/07/20 (US60/589,821)

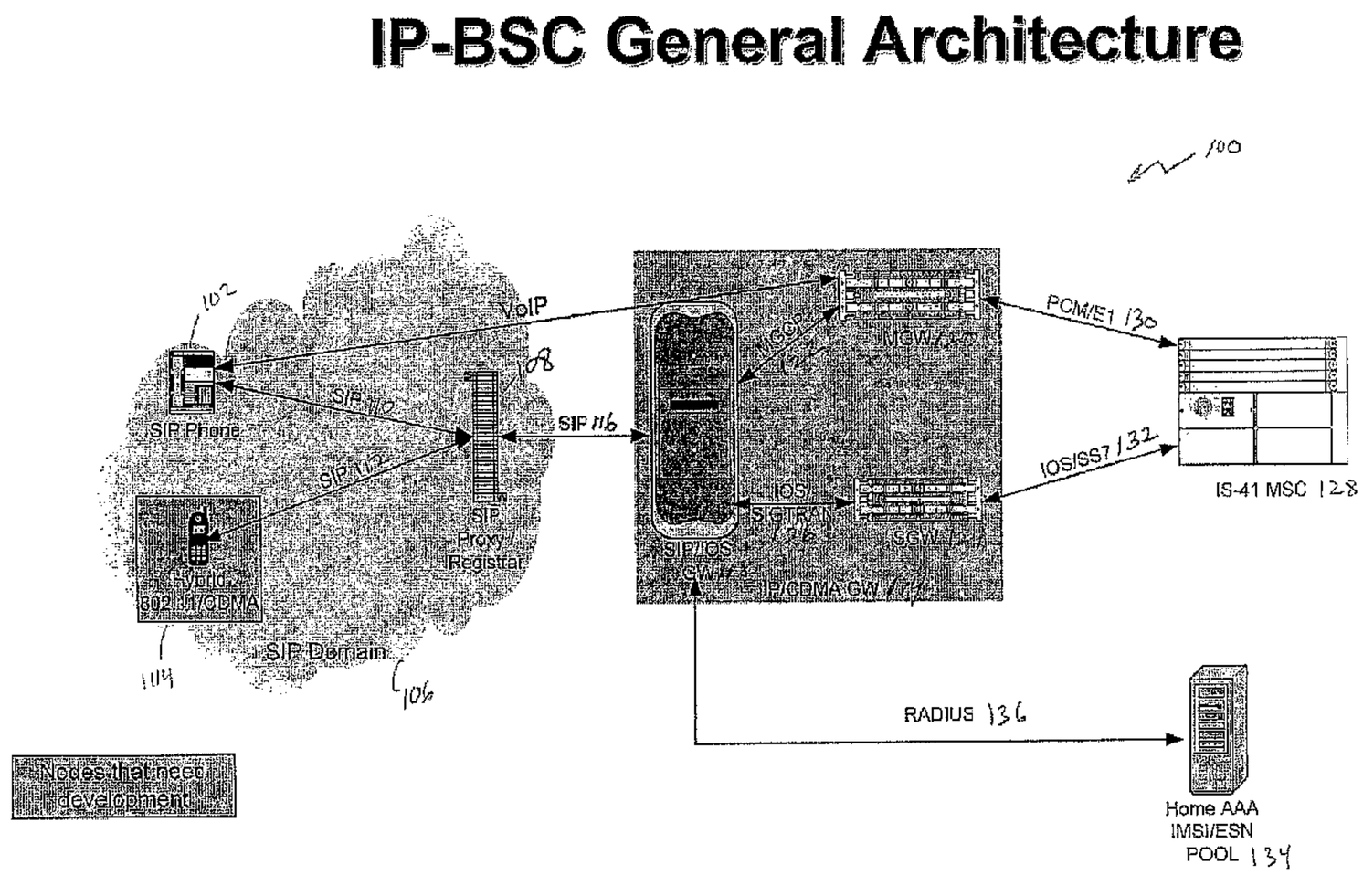
(51) Cl.Int./Int.Cl. *H04L 12/28* (2006.01),
H04Q 7/38 (2006.01)

(71) Demandeur/Applicant:
QUALCOMM INCORPORATED, US

(72) Inventeurs/Inventors:
ZREIQ, SAMER, IL;
ERUCHIMOVITCH, BARUCH, IL

(74) Agent: SMART & BIGGAR

(54) Titre : TRANSFERT ENTRE UN RESEAU SIP ET UN SYSTEME DE COMMUNICATION CELLULAIRE
(54) Title: HANDOFF BETWEEN A SIP NETWORK AND A CELLULAR COMMUNICATION SYSTEM



(57) Abrégé/Abstract:
Handoff between a wireless SIP network and a cellular communication system is provided. A system is designed to provide nomadic cellular services including voice to a SIP-enabled device.

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
2 February 2006 (02.02.2006)

PCT

(10) International Publication Number
WO 2006/012381 A1

(51) International Patent Classification[7]: H04L 12/28, H04Q 7/38

(21) International Application Number: PCT/US2005/025810

(22) International Filing Date: 20 July 2005 (20.07.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/589,821 20 July 2004 (20.07.2004) US

(71) Applicant *(for all designated States except US)*: **QUALCOMM Incorporated** [US/US]; 5775 Morehouse Drive, San Diego, California 92121 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **ZREIQ, Samer** [IL/IL]; 205 Ha Yam Road, 34890 Haifa (IL). **ERUCHIMOVITCH, Baruch** [IL/IL]; 68 Hatichon, 32293 Haifa (IL).

(74) Agents: **WADSWORTH, Philip R.** et al.; 5775 Morehouse Drive, San Diego, California 92121 (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, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

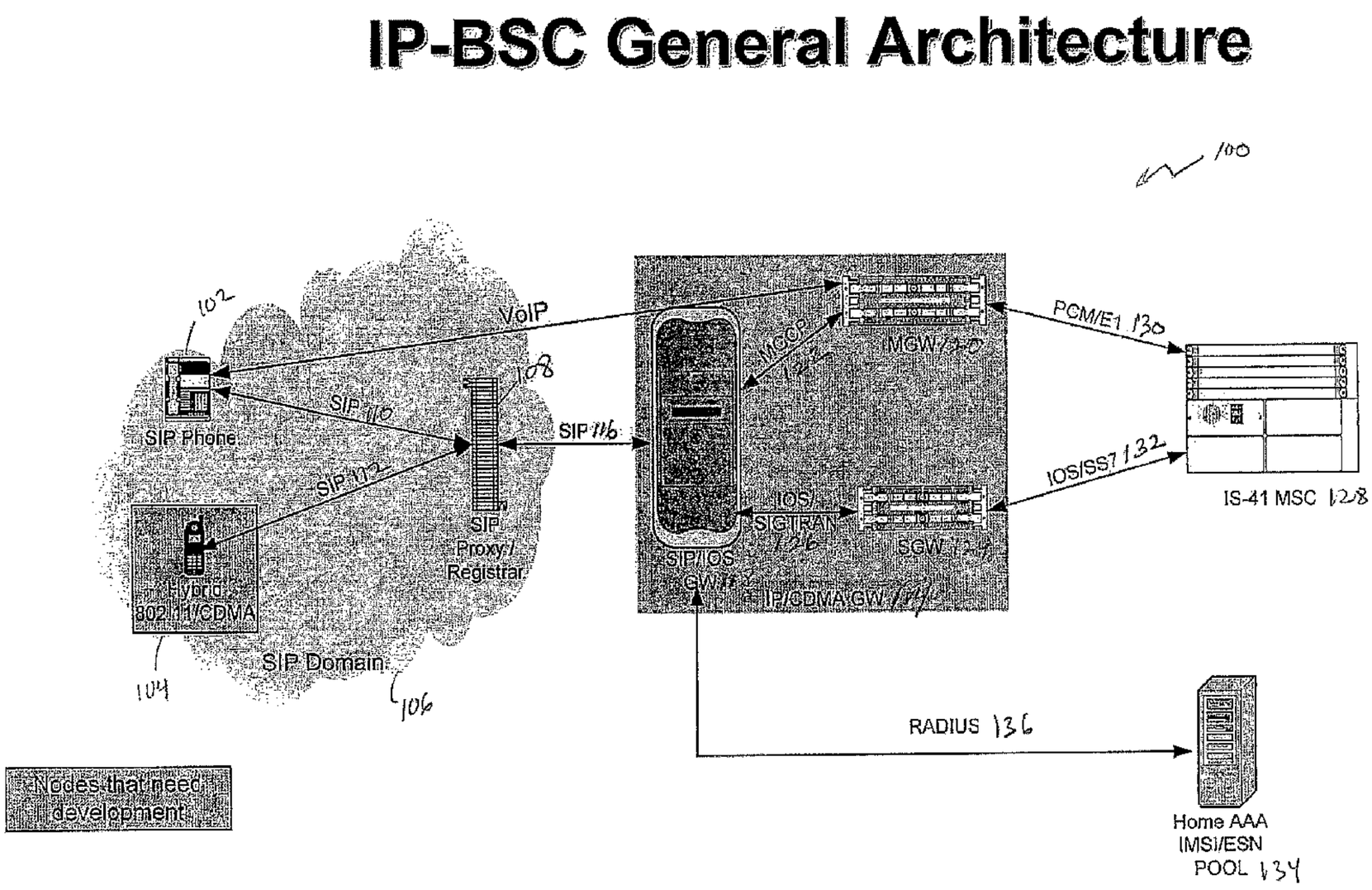
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, 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).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations 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, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR,*

[Continued on next page]

(54) Title: HANDOFF BETWEEN A SIP NETWORK AND A CELLULAR COMMUNICATION SYSTEM



(57) Abstract: Handoff between a wireless SIP network and a cellular communication system is provided. A system is designed to provide nomadic cellular services including voice to a SIP-enabled device.

WO 2006/012381 A1

GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii)) for all designations*

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

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

HANDOFF BETWEEN A SIP NETWORK AND A CELLULAR COMMUNICATION SYSTEM

Claim of Priority under 35 U.S.C. §119

[0001] The present Application for Patent claims priority to Provisional Application No. 60/589,821 entitled "AUTHENTICATION OF AN IP-ONLY DEVICE INTO A CDMA NETWORK" filed July 20, 2004, and assigned to the assignee hereof and hereby expressly incorporated by reference herein.

BACKGROUND

Field

[0002] This invention generally relates to wireless communications. More particularly, the invention relates to handoff between a session initiation protocol (SIP) network and a cellular communication system.

Background

[0003] Table 1 summarizes acronyms and abbreviations.

Table 1: Acronyms and abbreviations

AP	Access Point
AKEY	Authentication Key
BS	Base Station
CDMA	Code Division Multiple Access
CFSCNM	Candidate Frequency Search Control Message
CFSRSM	Candidate Frequency Search Response Message
CFSRQM	Candidate Frequency Search Request Message
ESN	Electronic Serial Number
EVRC	Enhanced Variable Rate Codec
FA	Foreign Agent
FFS	For Further Study
GPS	Global Positioning System
GW	Gateway
HLR	Home Location Register
HW	Hardware
IETF	Internet Engineering Task Force

IMSI	International Mobile Subscriber Identity
IOS	Inter Operability Specifications or Server
IP	Internet Protocol
LAN	Local Area Network
MAC	Medium Access Control
MAD	Mobile Addressed message
MGW	Media Gateway
MIB	Management Information Base
MIN	Mobile Identification Number
MIP	Mobile Internet Protocol
MO	Mobile Originated
MS	Mobile Station
MSC	Mobile Switching Center
MT	Mobile Terminated
NGLAN	Next Generation LAN
OAM	Operation Administration Management
OAM&P	Operation Administration Management & Provisioning
OCS	Obiwan Cellular Server
PPP	Point to Point Protocol
QoS	Quality of Service
RFC	Request For Comments
RLP	Radio Link Protocol
SGW	Signaling Gateway
SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol
SS	Supplementary Service
SS7	Signaling System #7
SW	Software
TCH	Traffic Channel
TCP	Transport Control Protocol
UDP	User Datagram Protocol
VoIP	Voice Over IP
VOPS	Voice Optimized Power Save
WAN	Wide Area Network
WSS	Wireless Soft Switch

[0004] SIP-only devices do not have a cellular identity and cannot be granted cellular access without a cellular identity. Thus, there is a need for internetworking SIP-only devices with a cellular network.

[0005] One solution has been to statically allocate a cellular identity to every SIP-only device that is planned to have access to a cellular network. This is none standard solution requires changes to the standard SIP protocol in the SIP devices.

[0006] In another solution, when a SIP device calls a cellular device, the call can be routed through the public telephony network (PSTN) and in the PSTN the call is routed to a cellular network. This solution introduces extra signaling and traffic overhead which affects the voice quality of the calls. It also introduces extra charges since the call is routed through the PSTN and PSTN operators charge for the call.

[0007] Thus, there is a need for a solution that does not require changes to the standard SIP protocol and that does not involve extra signaling and traffic overhead.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] FIG. 1 is a general system architecture in accordance with an embodiment;

[0009] FIG. 2 shows a handoff call flow in accordance with an embodiment;

[0010] FIG. 3 shows an interaction between a serving mobile station and a candidate base station in accordance with an embodiment;

[0011] FIG. 4 shows a mobile originated call setup in accordance with an embodiment;

[0012] FIG. 5 shows a mobile terminated call set up in accordance with an embodiment;

[0013] FIG. 6 shows a sequence of events for the handoff procedure;

[0014] FIG. 7 shows a mobile originated SMS (no call) in accordance with an embodiment;

[0015] FIG. 8 shows a mobile terminated SMS (no call) in accordance with an embodiment;

[0016] FIG. 9 shows a mobile originated SMS (during calls) in accordance with an embodiment; and

[0017] FIG. 10 shows a mobile terminated SMS (during calls) in accordance with an embodiment.

DESCRIPTION

[0018] In an embodiment, handoff between a SIP network and a cellular communication system is provided.

[0019] In an embodiment, a wireless unit is a Session Initiation Protocol (SIP) device. A wireless unit can also be called a subscriber station, subscriber unit, mobile station, mobile, remote station, remote terminal, access terminal, user terminal, user agent, or user equipment. A wireless unit may be a personal digital assistant (PDA), a handheld device having wireless connection capability, or other processing device connected to a wireless modem.

Architecture

[0020] In accordance with an embodiment, an IP (SIP) network is coupled to a cellular (CDMA) network using a special base station (or Gateway), referred to as an SIP/IOS gateway.

[0021] Hybrid cellular mobile devices (that support SIP as well), can be granted service in the IP network, while the SIP/IOS GW translates between SIP and CDMA protocols and passes the messages between the two networks. Such hybrid devices have cellular numbers (IMSI and ESN) as well as security parameters that enable the cellular network to authenticate these devices.

[0022] In this solution, SIP-only devices are presented as "real" cellular devices to the cellular network. When such a device accesses the cellular network, the SIP/IOS GW along with an AAA server will assign a cellular identity (IMSI, ESN and security parameters) to that device, and pass the cellular identity to the cellular network.

[0023] A general system architecture in accordance with an embodiment is shown in Figure 1. Figure 1 presents an overall view of an IP-BSC interworking architecture 100 in accordance with an embodiment. These enabling functionalities include the reuse of CDMA subscription, system selection, single authentication mechanism, call routing and service access, as well as end user charging.

[0024] A SIP phone 102 and a hybrid 802.11/CDMA phone 104 are shown in a SIP domain 106 communicating wirelessly with an SIP proxy/registrar 108 via SIP 110, 112. The SIP phone 102 is also configured to communicate with a Media Gateway 120 via voice over Internet Protocol (VoIP). Next Generation LAN (NGLAN) is another name to describe a SIP network 106 that is coupled to a cellular operator.

[0025] The SIP proxy/registrar 108 communicates wirelessly with an IP/CDMA gateway 114 via SIP 116. In particular, the SIP proxy/registrar communicates wirelessly with an SIP/IOS gateway 118 of the IP/CDMA gateway 114.

[0026] The SIP/IOS gateway 118 communicates with a Media Gateway 120 via MGCP 122 in accordance with an embodiment. The SIP/IOS gateway 118 communicates with a Signaling Gateway 124 via IOS/SIGTRAN 126. The SIP/IOS gateway 118 communicates with a Home AAA IMSI/ESN pool 134 via RADIUS 136.

[0027] The Media Gateway 120 communicates with an IS-41 MSC 128 via PCM/E1 130 in accordance with an embodiment. The Signaling Gateway 124 communicates with an IS-41 MSC 128 via IOS/SS7 132. It would be apparent to those skilled in the art that the MSC 128 may be another kind of CDMA MSC and is not limited to an IS-41 MSC.

[0028] When a SIP user logs into the system with a SIP-only device 102, the AAA 134 authenticates the user's account by the user name and password. The GW 114 and AAA 134 may allocate static cellular identities to certain SIP users (VIP users for example) at the login/registration time, and may dynamically allocate cellular identities to other SIP users when the users attempt to make a call to the cellular network, in accordance with an embodiment.

[0029] When static IDs are allocated to certain users, mobile terminated call (from the cellular network) can be managed to these users using their static cellular numbers.

[0030] In accordance with an embodiment, a SIP provider (that can be an enterprise for example) may purchase a "service package" form the cellular operator that contains a defined number of cellular identities. The cellular operator configures the AAA 134 with the user accounts that are served by the SIP operator and will be granted access to the cellular network. The AAA 134 will also be configured with the cellular identities that will be allocated to the SIP users (dynamically or statically, as mentioned above). The AAA server 134 logs SIP accounts activities to be supplied by the cellular operator to the SIP operator for billing purposes.

Handoff

[0031] In an embodiment, a cellular number works on either a CDMA network or an NGLAN. The core network is smart enough to deliver service either on the NGLAN or on the CDMA network.

[0032] In an embodiment, handoffs occur in idle mode or an active mode. In idle mode as the mobile moves between networks, the core network knows how to get to the mobile. Active mode supports NGLAN to CDMA handoffs.

[0033] In an embodiment, there are two numbers for the two networks. There is a number for the CDMA network and a number for the NGLAN. Both the NGLAN and CDMA networks can be monitored simultaneously.

[0034] NGLAN service is delivered using NGLAN. In an embodiment, an outgoing service is configured to use a preferred access.

[0035] In an embodiment, IDs are allocated dynamically for native IP devices in the CDMA domain. IMSI and ESN are allocated from a pool managed by a central server, such as a Home AAA server 134, to every native IP device when attempting to originate a call to a CDMA device. IDs are also allocated to SIP calls. Multiple calls from the same originator are available. Originators are identified by their SIP URL and SIP Call-ID.

[0036] In an embodiment, IDs are allocated statically for native IP devices in the CDMA domain. IMSI and ESN are allocated for every device (or part of the devices) in the IP domain when registering in the SIP domain. IP devices are identified by their SIP URL. Multiple calls from the SIP device to the CDMA network are not available.

[0037] It would be apparent to those skilled in the art that SIP can be exchanged with any other signaling protocol.

[0038] No changes to an 802.11 PHY or MAC layers are needed to implement SIP to CDMA handoffs. Billing records are consistent with cellular. AKEY, ESN and IMSI are used for authentication. RADIUS is for data authentication.

[0039] The look and feel of SMS integration and supplementary services support are preserved. There is seamless service availability due to simultaneous monitoring of networks, the SIP network and the CDMA network.

[0040] In an embodiment, handoff trigger and target selection are supported. In an embodiment, handoff occurs within 80 seconds and the target of a handoff is determined in 20 milliseconds.

[0041] In an embodiment, sleep modes between 802.11 and CDMA are coordinated.

[0042] Figure 2 shows a handoff call flow 200 in accordance with an embodiment. Figure 2 shows a call on SIP 252 and a call on CDMA 1x 254. An mobile station (MS) 256, a source base station (BS) 258, a mobile switching center (MSC) 260, and a target BS 262 are only shown.

[0043] The MS 256 sends a message to the source BS 258 indicating that the MS 256 is out of coverage 201. Then, handoff handshaking 201a occurs between the MS 256 and the source BS 258.

[0044] The source BS 258 sends a handoff required message 202 to the MSC 260. The MSC 260 sends a handoff request message 203 to the target BS 262. The target BS 262 does a traffic channel (TCH) setup 204.

[0045] Null forward traffic frames 205 are sent from the target BS 262 to the MS 256. A handoff request acknowledgment 206 is sent from the target BS 262 to the MSC 260. A handoff command 207 is sent from the MSC 260 to the source BS 258. An update handoff direction message (UHDM) 208 is sent from the source BS 258 to the MS 256. An MS acknowledgement order 209 is sent from the MS 256 to the source BS 258. A handoff commenced message 210 is sent from the source BS 258 to the MSC 260. The MS 256 tunes 211 to 1x in accordance with an embodiment. Reverse traffic frames 212 are sent from the MS 256 to the target BS 262.

[0046] The MS 256 sends a handoff completion message (HCM) 213 to the target BS 262. The target BS 262 sends a handoff complete 214 to the MSC 260. The MSC 260 sends a clear command 215 to the source BS 258. The source BS sends a clear complete 216 to the MSC 260.

[0047] Figure 3 shows an interaction during handoff handshaking between a serving MS and a candidate base station in accordance with an embodiment. A search parameters message (CFSRQM) 201 is sent from a BS to an MS 222. An acceptance message (CFSRSM) 202 is sent from the MS 222 to a candidate base station 220.

[0048] The CFSRQM is a Candidate Frequency Search Request Message where the base station informs the MS about:

- Candidate Frequency Neighbor List (CFNL)
- Candidate Frequency Search Set (CFSS), a subset of CFNL
- Frequency band and channel number
- Search period for periodic search
- Thresholds (MS Rx power and total pilot E_c/I_0, etc.)
- Can specify a search for AMPS (other formats can be added)
- Optionally, can synchronize timing between MS and BS

[0049] The CFSRQM can also start a search.

[0050] The CFSRSM is a Candidate Frequency Response Message wherein the MS replies to the CFSRQM:

- Dead time to search entire CFSS (forward and reverse)
- Dead time per visit to candidate frequency (forward and reverse)

[0051] Dead time can be specified in frames in one embodiment or in 1.25 ms slots in another embodiment.

[0052] A search order (CFSCNM) does not need to be sent from a BS to the serving MS 222. The CFSCNM is a Candidate Frequency Search Control Message to start and stop searches (periodic or single). The serving MS 222 communicates with candidate base stations 220.

[0053] The serving MS 222 sends a report (CFSRPM) to candidate base stations 220. CFSRPM is a Candidate Frequency Search Report Message, wherein the MS reports to a BS on the serving frequency:

- MS Rx power on candidate frequency
- Pilots above add threshold (T_Add)
- Sent in periodic search only if total E_c/I_0 of candidate frequency search set is above threshold
- All pilot measurements have to be made within 0.8 seconds of the report.

[0054] A General Handoff Direction Message (GHDM) is sent the serving MS 222, the GHDM including flags to specify procedure upon hard handoff (HHO) failure.

Call Setup

[0055] Figure 4 shows a mobile originated call setup in accordance with an embodiment.

[0056] Figure 5 shows a mobile terminated call set up in accordance with an embodiment.

[0057] Figure 6 shows a registration procedure in accordance with an embodiment.

SMS

[0058] For hybrid devices that support SMS, SMS messages are tunneled in SIP extended messages. For native SIP devices, the IP/CDMA gateway is used as an SMS proxy. The IP/CDMA gateway handles the SMS protocol and sends text in SIP messages.

[0059] Figure 7 shows a mobile originated SMS (no call) in accordance with an embodiment.

[0060] Figure 8 shows a mobile terminated SMS (no call) in accordance with an embodiment.

[0061] Figure 9 shows a mobile originated SMS (during calls) in accordance with an embodiment.

[0062] Figure 10 shows a mobile terminated SMS (during calls) in accordance with an embodiment.

[0063] In an embodiment, the SIP/IOS gateway is a special kind of BSC that supports the Standard Inter Operability Specifications (IOS) 4.2 A1 and A2 interfaces, for example. The SIP/IOS gateway is deployed in the operator's network and provides the support for a client in a wireless unit to provide cellular services.

[0064] The SIP/IOS gateway is responsible of translating between SIP and IOS protocols. It functions as a SIP Server for the wireless unit and as a CDMA BSC for the MSC. A SIP Registrar is used to register users in the SIP/WLAN domain. The SIP Registrar maintains the translation between IMSI/ESN and the IP address for each user in the SIP/WLAN domain.

[0065] The media gateway (MGW) and the signaling gateway (SGW) are controlled by the SIP/IOS gateway and are used to communicate with the MSC using A1/SS7/T1/E1 for signaling and over A2/T1/E1 for voice transfer. The Signaling Gateway translates between SIGTRAN (IP) and SS7, and the Media Gateway includes vocoders, and it translates between EVRC/RTP and PCM/T1/E1.

[0066] The network includes an MSC (Soft-Switch) to provide services to wireless terminals in SIP/WLAN mode. This MSC supports standard IOS A1 and A2 interfaces towards the MGW. This MSC is also connected to an IS-41 network for handoffs to the CDMA radio network.

[0067] In an embodiment, the SIP/IOS gateway 118 (with the SGW) 204 translates between SIP/IOS and IOS/SS7 protocols.

Subscription Management

[0068] Primarily the cellular subscription will be used to manage services. This implies that the cellular ESN and IMSI along with AKEY will be used.

[0069] A SIP capable terminal, when operating in the WLAN environment, will use SIP for call processing signaling. It will tunnel the cellular subscription using SIP signaling infrastructure.

[0070] In an embodiment, the IP/CDMA GW 114 will store the mapping between an internet address (TCP/IP address and port or UDP/IP address and port) and the cellular subscription in persistent redundant storage.

Handoff trigger

[0071] Handoff occurs when the quality of the link between the wireless terminal and the SIP/IOS GW 118 is unsuitable. Note that a trigger does not always result in a handoff. The handoff outcome depends on the search stage.

[0072] Search: The wireless terminal will search for new access points (APs), and will select the AP with the strongest signal strength. An access point is a base station or a gateway.

[0073] Handoff will be initiated if this AP is better than the current AP by more than a hysteresis level. (This is to prevent a ping-pong effect). Note that part of the search stage may occur before the handoff trigger, through the construction of a candidate AP list (in cooperation with a database at the IP/CDMA GW).

[0074] Completion: The wireless terminal sets up a connection with the new AP. This includes 802.11 authentication, 802.11 association and higher layer functions.

[0075] Inter-AP handoff is mobile controlled as in 802.11 systems (as opposed to the mobile assisted handoff that is commonly used in cellular handovers).

[0076] A step in handoff is the generation of a handoff trigger that essentially says that the quality of the current link is unsuitable. Based on the handoff trigger, handoff is executed to a CDMA network or to another AP. The handoff execution itself depends on a list of candidate AP's that is maintained at the wireless terminal. The final step in handoff is the execution of handoff, which involves the setup of a new voice path, and the termination of the old voice path.

[0077] Handoff Execution

[0078] Talk Mode Handoff Execution: Based on entries for each candidate, the candidate AP list is sorted. If the signal strength of the AP on top of the list is sufficient, handoff is attempted to the AP on top of the list. If handoff fails, the wireless terminal tries to link with the next AP on the candidate list, and continues this process until a timer expires, or a maximum number of handoff attempts have been made.

[0079] Idle Mode Handoff Execution

[0080] The wireless terminal exits the 802.11 power save mode, and scans all channels valid for the operating regulatory domain to construct a candidate AP list, and sorts the list according to the rules given in **Error! Reference source not found.**. If handoff fails, the wireless terminal tries to link with the next AP on the candidate list, and continues this process until a timer expires, or a maximum number of handoff attempts have been made. The wireless terminal sends a keep alive upon completing every handoff. This keep alive includes the time taken for handoff completion, and is used by the IP/CDMA GW to refresh its database. After handoff is complete (successful exchange of messages with the IP/CDMA GW), the wireless terminal switches back to 802.11 power save mode. The exact mechanism for handoff depends on the level of security implemented in a WLAN deployment.

[0081] Handoff with no security

[0082] First consider the simplest case, where no security settings or only WEP security settings are used. For these simple cases the process of handoff comprises the following steps

[0083] Send authentication request, get authentication response. This is the stage where the WEP key, if assigned, is used. A wireless terminal gets the WEP key from the IP/CDMA GW database or a local database at the wireless terminal.

[0084] Send association request, get association response.

[0085] Use inter-AP protocol to inform old AP to remove wireless terminal from its list

[0086] Use SNAP to inform the switch at the AP subnet to send packets for wireless terminal to the new AP

[0087] Handoff with security

[0088] Security is implemented using the 802.1x standard that specifies the operation of EAP (extended authentication protocol) over 802 networks.

[0089] 802.11 to 1x Handoff in Voice Mode

[0090] An active state handoff features a handoff from 802.11 operation mode to native 1xRTT mode.

[0091] Deciding between inter-AP and CDMA handoffs

[0092] When the current AP has low signal strength, we need to decide whether to handoff to a CDMA network or WLAN. For example, in a home WLAN (with only one AP), attempting to handoff to an alternate AP will result in additional delay, and handoff to a CDMA network is attempted as soon as the WLAN link degrades in accordance with an embodiment. On the other hand, in an enterprise deployment, there are likely to be many AP's and handoff to an alternate AP should be attempted before handoff to a CDMA network is attempted.

[0093] In case scanning performed during the call (or before the call began) indicates that no other AP's are available, the decision between WLAN and CDMA is clear, and handoff must be to CDMA. However, when other AP's are present, we need to decide whether to handoff to WLAN or CDMA. This decision is important because:

- Handoff to WLAN maximizes free spectrum usage
- Handoff to WLAN may cause excess delay if a new IP address needs to be obtained or if WLAN deployment results in excessive delay.

[0094] The IP/CDMA GW database helps the wireless terminal decide if handoff should be to WLAN or CDMA. Talk mode WLAN to CDMA handoff is attempted if there is a trigger for WLAN to CDMA handoff, or if there is no reliability level 4 AP with signal strength above a threshold.

[0095] WLAN to CDMA Handoff Basics

[0096] Prior to the handoff, the user terminal employs a SIP over IP over 802.11 protocol stack in the signaling plain, as well as a VoIP stack in the traffic plain. After the handoff procedure is completed, the user terminal employs a native IS-2000 1xRTT signaling protocol stack in the signaling plain, as well as a native IS-2000 1xRTT voice processing at the traffic plain.

[0097] The target CDMA BTS, target CDMA BSC and target IS-41 MSC are standard components. The IP/CDMA GW interaction with the IS-41 MSC throughout the handoff procedure complies with the IS-41 and IOS specifications. Development is only allowed and required at the IP/CDMA GW and at the user terminal.

[0098] During a voice call in 802.11 operation mode, the wireless terminal should monitor both networks (802.11, CDMA). If the reception power of the 802.11 falls below a certain threshold, the wireless terminal should report the reception power of both networks to the IP/CDMA GW. The IP/CDMA GW may then invoke intersystem handoff procedure to CDMA. Hence, this handoff procedure is mobile assisted. As part

of this procedure, the IP/CDMA GW should forward the Handover Command that is received from the IS-41 MSC to the user terminal. The user terminal should then terminate its operation in 802.11 operation mode, tune to 1xRTT mode, kick start its CDMA protocol stack into Active mode and perform the standard CDMA handoff sequence together with the target base station.

[0099] Handoff from WLAN to CDMA can occur in two cases: when there is a trigger for WLAN to CDMA handoff, or when inter-AP handoff fails, resulting in a request for handoff to a CDMA network.

[00100] The trigger for WLAN to CDMA handoff is generated when any of the following conditions are met.

- No packets are received on the downlink for Handoff_Timeout_Threshold
- The fraction of missed packets on the downstream exceeds Handoff_PacketLoss_Threshold.

[00101] Separate RF chain and firmware will be used by the user terminal for each operation mode (802.11, CDMA). During an 802.11 call, the user terminal should periodically monitor both the 802.11 and the CDMA networks, using the separated hardware. The wireless terminal should attempt to acquire the Pilot Channel of a CDMA system. Following the first Pilot channel acquisition, the wireless terminal should also acquire the associated Synch and Paging channels, to obtain timing information, SID and NID pair, Neighbor List message and the BASE_ID for the CDMA system. Subsequently, the wireless terminal should remain in a reduced flavor of the CDMA Idle state with Slot Cycle Index zero and perform idle mode handoffs to the neighbor cells when needed. The wireless terminal should maintain a list of the 4 strongest Pilot channels received and their associated PN offset, receive power and BASE_ID.

[00102] The IP/CDMA GW may reside in a distant location than the target CDMA cell for the handoff. As a result and unlike native CDMA, the IP/CDMA GW is unable to determine the unique identification of the target CDMA cell, based on PN offset alone. The wireless terminal should therefore acquire the Paging channel of the target cell and obtain the BASE_ID from the System Parameters message. To reuse standard CDMA design and implementation, the wireless terminal should remain in the flavor of the idle state mentioned above. This may cause a small waste of battery consumption, but simplifies the implementation significantly.

[00103] WHAT IS CLAIMED IS:

CLAIMS

1. A method of assigning a cellular identity to a session initiation protocol (SIP) device, comprising:

determining whether a device is a SIP device;

authenticating the SIP device; and

assigning a cellular identity to the SIP device based on the authenticating.

2. A method of wireless communication from a session initiation protocol (SIP) device to a CDMA network, comprising:

determining whether a device is a SIP device;

authenticating the SIP device;

assigning a cellular identity to the SIP-only device based on the authenticating; and

tunneling SIP text within SMS messages.

3. A method of handoff from a session initiation protocol (SIP) network to a CDMA network for a wireless terminal, comprising:

determining whether a device is a SIP device;

authenticating the SIP device;

assigning a cellular identity to the SIP device based on the authenticating;

determining a handoff trigger has been triggered based in part on quality of a wireless terminal link; and

tunneling SIP text within SMS messages.

4. A wireless terminal, comprising:

means for determining whether a device is a SIP device;

means for authenticating the SIP device;

means for assigning a cellular identity to the SIP device based on the authenticating;

means for determining a handoff trigger has been triggered based in part on quality of a wireless terminal link; and

means for tunneling SIP text within SMS messages.

5. Computer readable media embodying a program of instructions executable by a program to perform a method of handoff from a session initiation protocol (SIP) network to a CDMA network for a wireless terminal, comprising:

determining whether a device is a SIP device;

authenticating the SIP device;

assigning a cellular identity to the SIP device based on the authenticating;

determining a handoff trigger has been triggered based in part on quality of a wireless terminal link; and

tunneling SIP text within SMS messages.

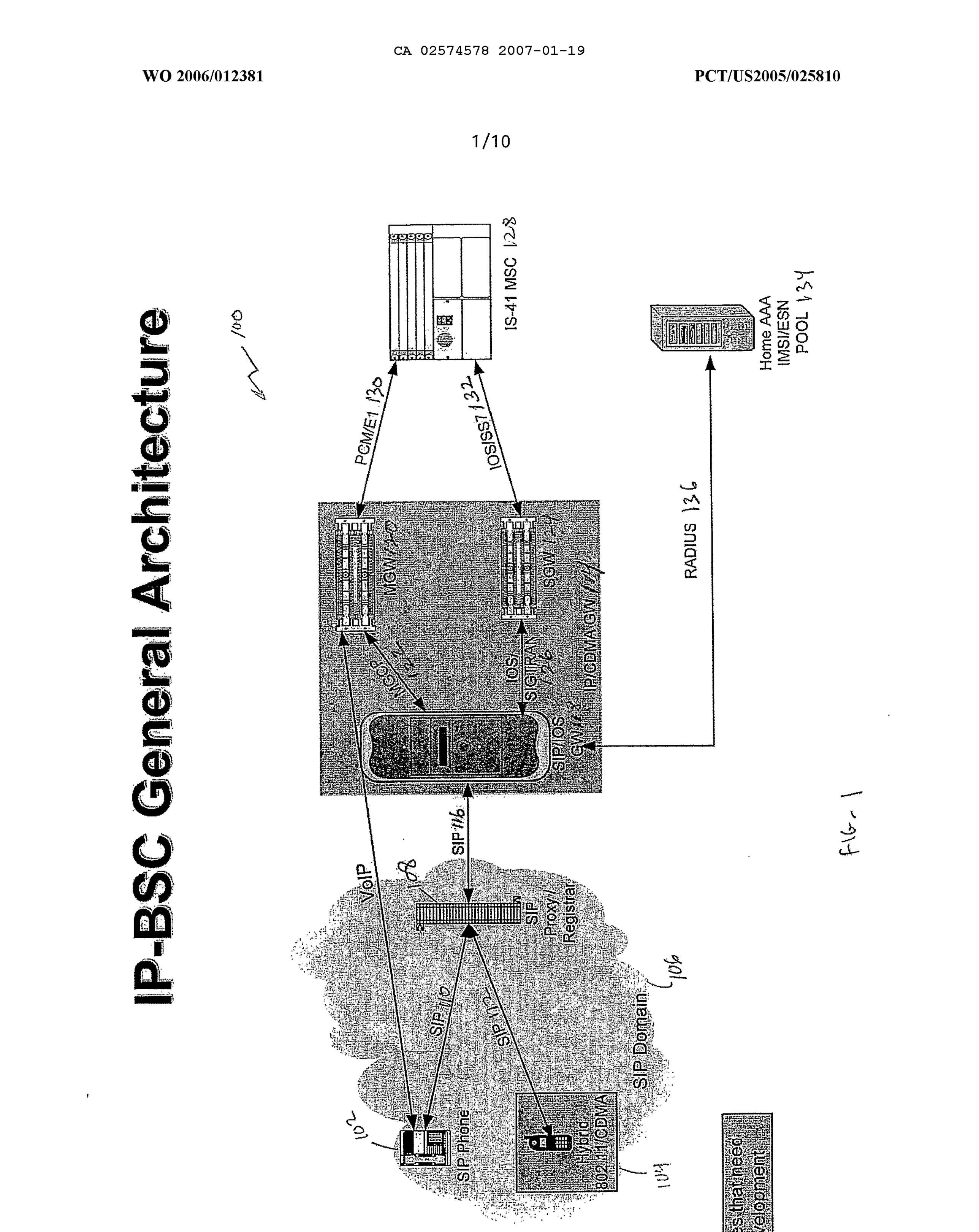

IP-BSC General Architecture
100
IS-41 MSC 128
PCM/E1 130
IOS/SS7 132
MGW 120
SGW 124
IP/CBMA GW 122
IOS/ SIGTRAN 126
SIP/IOS GW
RADIUS 136
Home AAA
IMSI/ESN
POOL 138
SIP 116
VoIP
108
SIP Proxy/ Registrar
SIP Domain
106
SIP 110
SIP 112
SIP Phone
102
Hybrid 802.11/CDMA
104
Nodes that need development

Fig. 1

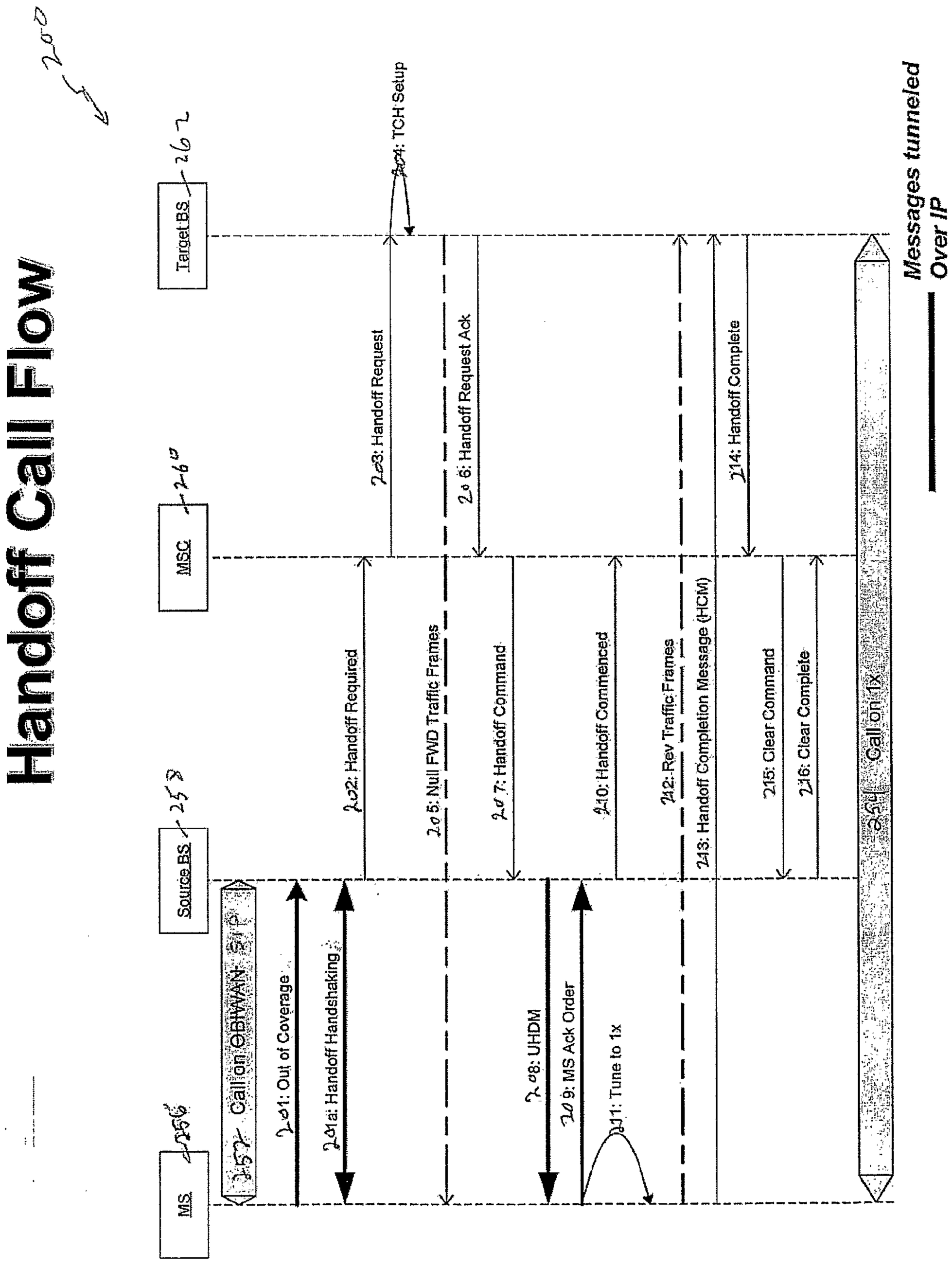

Handoff Call Flow
MS
Source BS
MSC
Target BS
Call on CDMA
Call on OBIWAN
Call on 1x
Messages tunneled Over IP
201: Out of Coverage
201a: Handoff Handshaking
202: Handoff Required
203: Handoff Request
204: TCH Setup
205: Null FWD Traffic Frames
206: Handoff Request Ack
207: Handoff Command
208: UHDM
209: MS Ack Order
210: Handoff Commenced
211: Tune to 1x
212: Rev Traffic Frames
213: Handoff Completion Message (HCM)
214: Handoff Complete
215: Clear Command
216: Clear Complete

FIG. 2

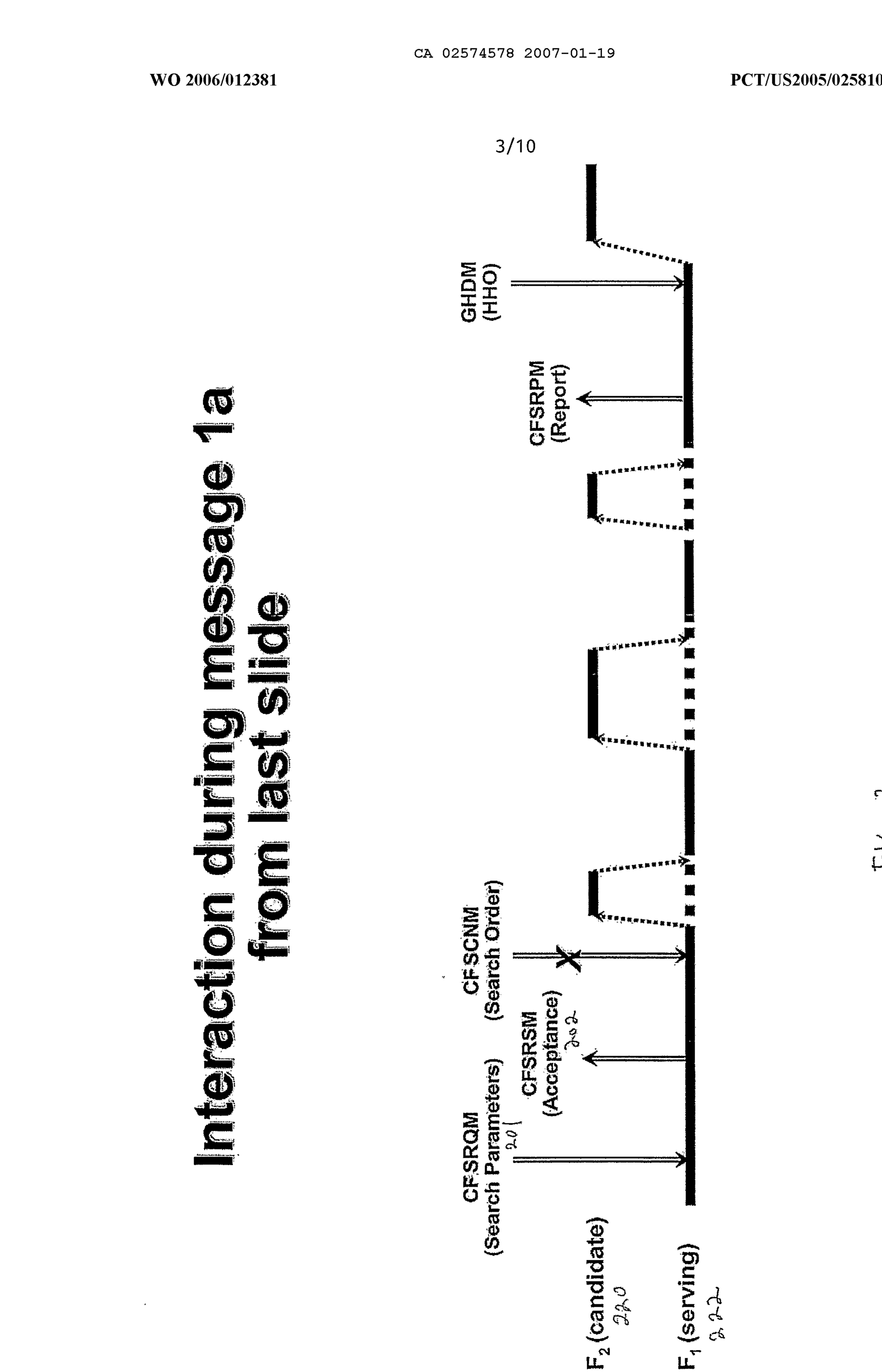
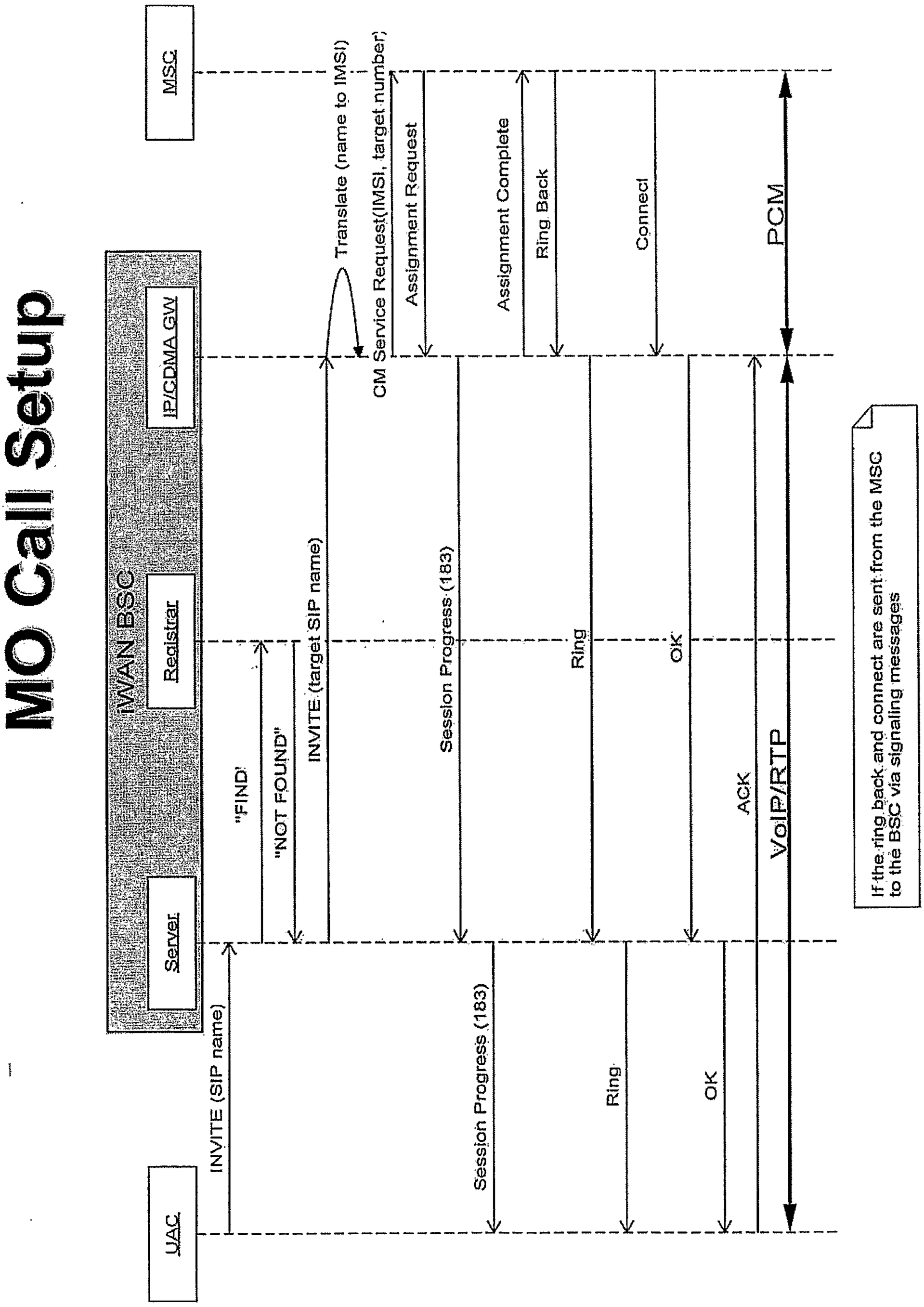

Interaction during message 1a
from last slide
GHDM
(HHO)
CFSRPM
(Report)
CFSCNM
(Search Order)
CFSRSM
(Acceptance)
202
CFSRQM
(Search Parameters)
201
F2 (candidate)
220
F1 (serving)
222

Fig. 2


MO Call Setup
UAC
Server
iWAN BSC
Registrar
IP/CDMA GW
MSC
INVITE (SIP name)
"FIND"
"NOT FOUND"
INVITE (target SIP name)
Translate (name to IMSI)
CM Service Request(IMSI, target number)
Assignment Request
Session Progress (183)
Ring
OK
ACK
VoIP/RTP
Assignment Complete
Ring Back
Connect
PCM
If the ring back and connect are sent from the MSC to the BSC via signaling messages

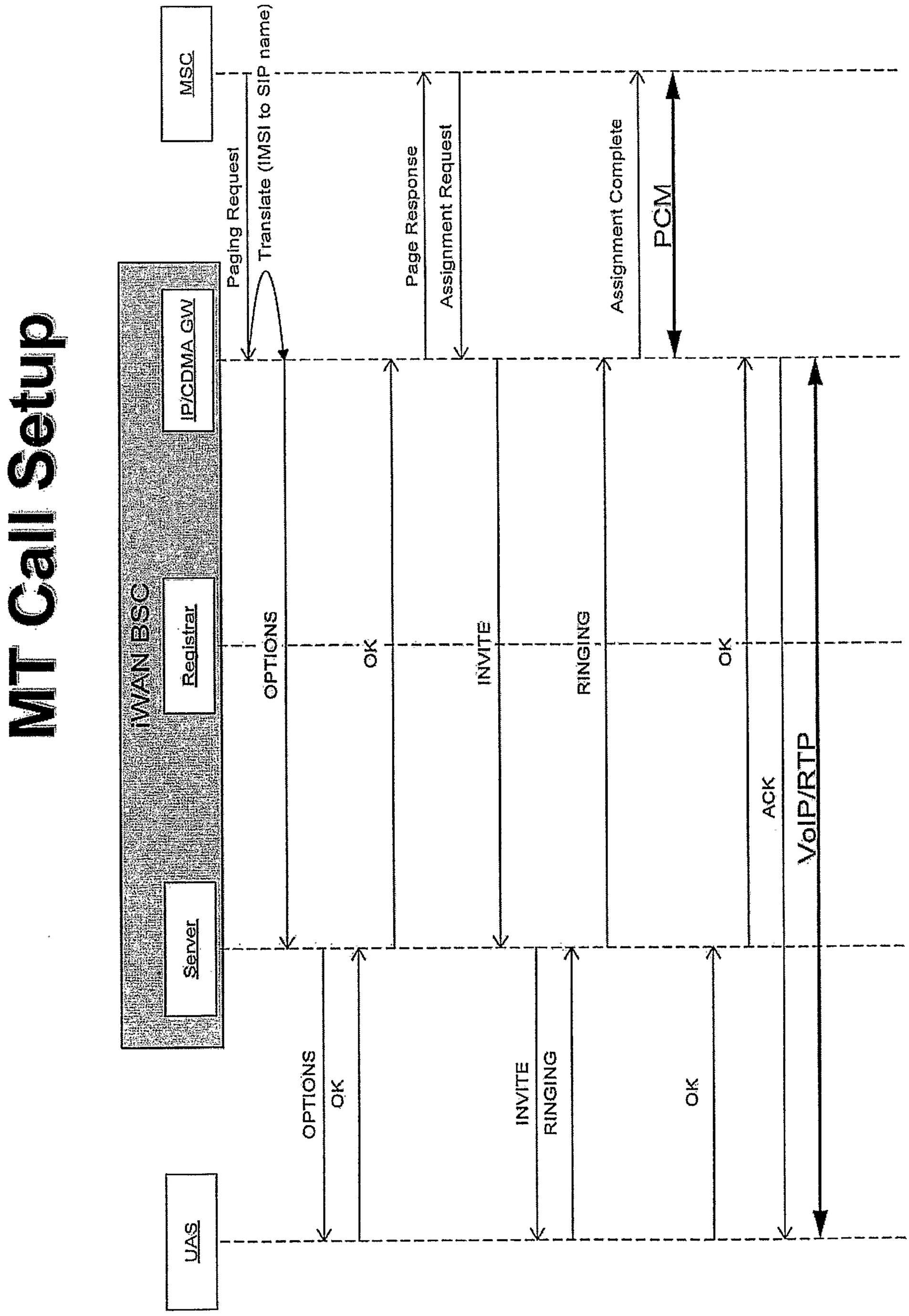

MT Call Setup
MSC
IP/CDMA GW
iWAN BSC
Registrar
Server
UAS
Paging Request
Translate (IMSI to SIP name)
Page Response
Assignment Request
Assignment Complete
PCM
OPTIONS
OK
INVITE
RINGING
OK
ACK
VoIP/RTP
OPTIONS
OK
INVITE
RINGING
OK

FIG. 5

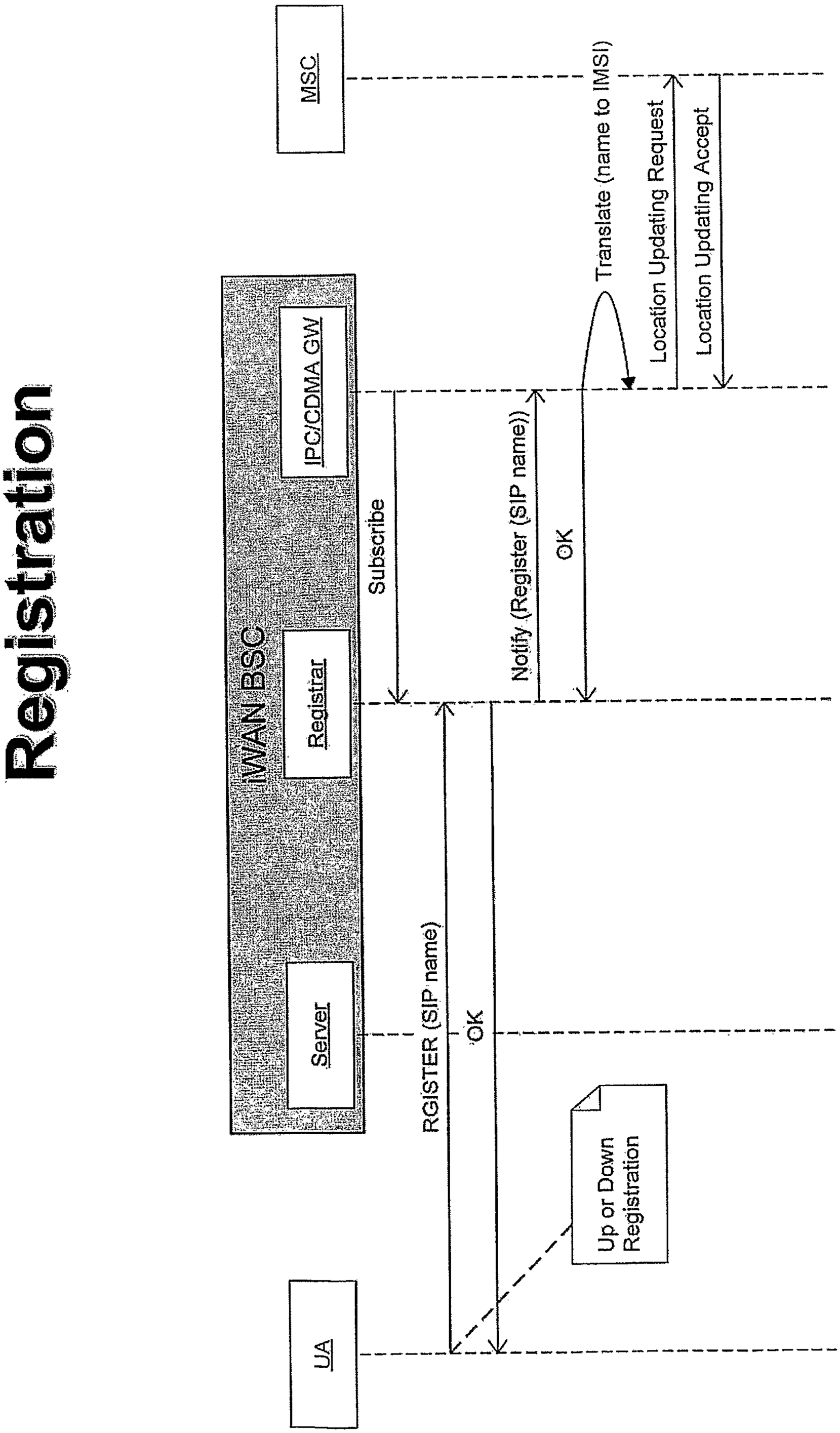

Registration
MSC
IWAN BSC
IPC/CDMA GW
Registrar
Server
UA
Subscribe
Notify (Register (SIP name))
OK
Translate (name to IMSI)
Location Updating Request
Location Updating Accept
RGISTER (SIP name)
OK
Up or Down Registration

FIG. 6

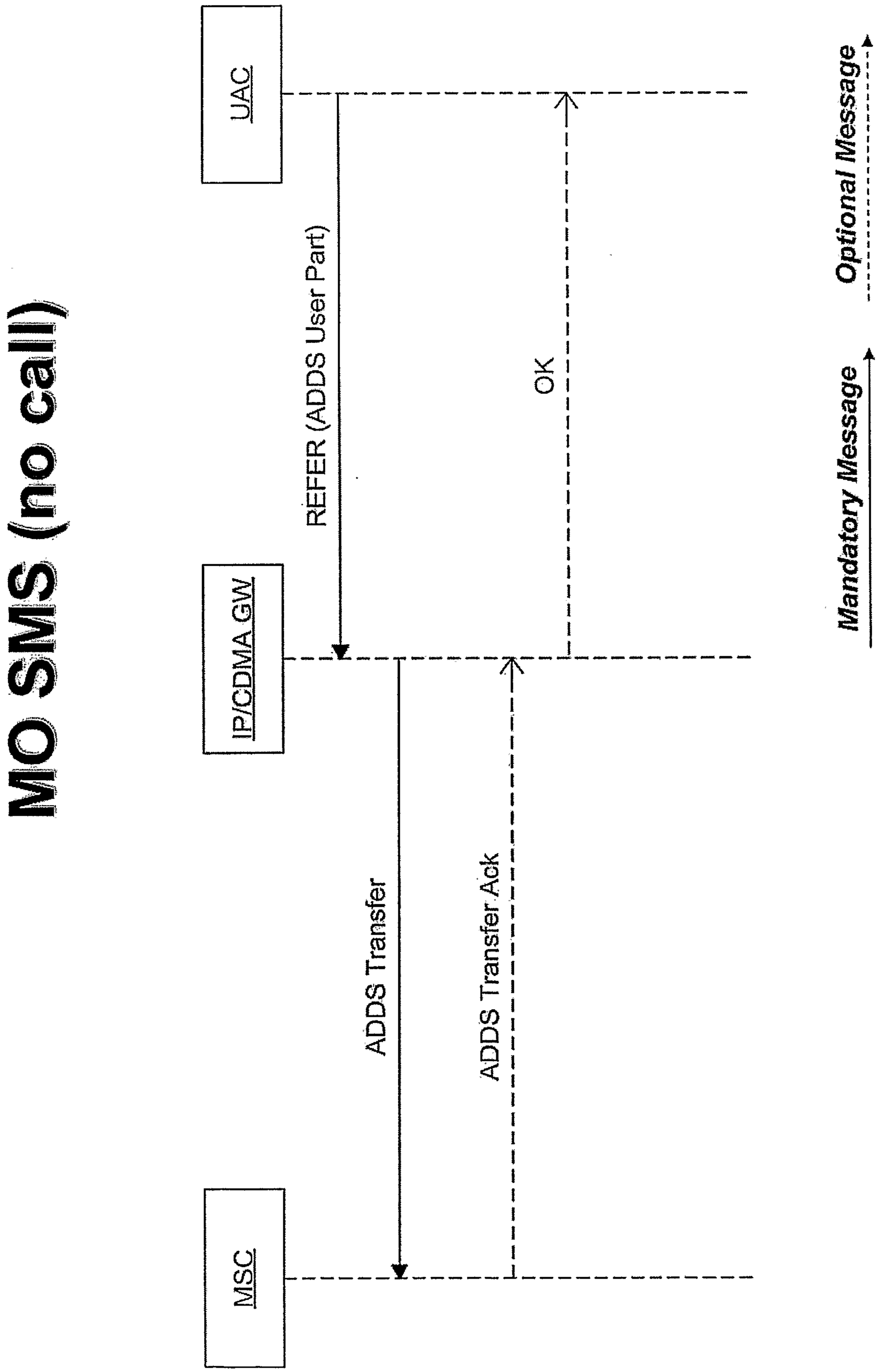

MO SMS (no call)
UAC
IP/CDMA GW
MSC
REFER (ADDS User Part)
OK
ADDS Transfer
ADDS Transfer Ack
Mandatory Message
Optional Message

FIG. 7

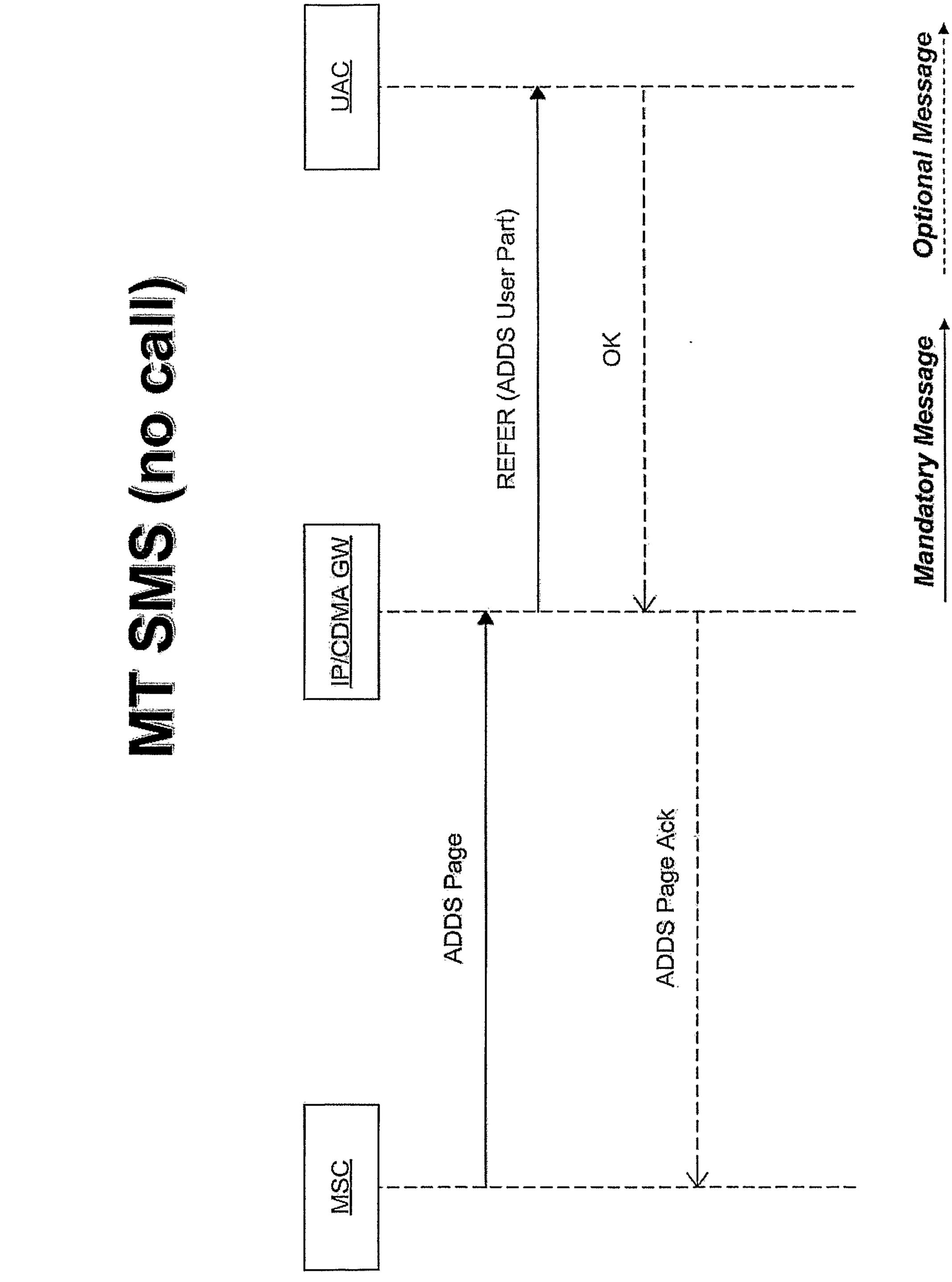

MT SMS (no call)
UAC
IP/CDMA GW
MSC
REFER (ADDS User Part)
OK
ADDS Page
ADDS Page Ack
Mandatory Message
Optional Message

Fig. 8

MO SMS (during calls)

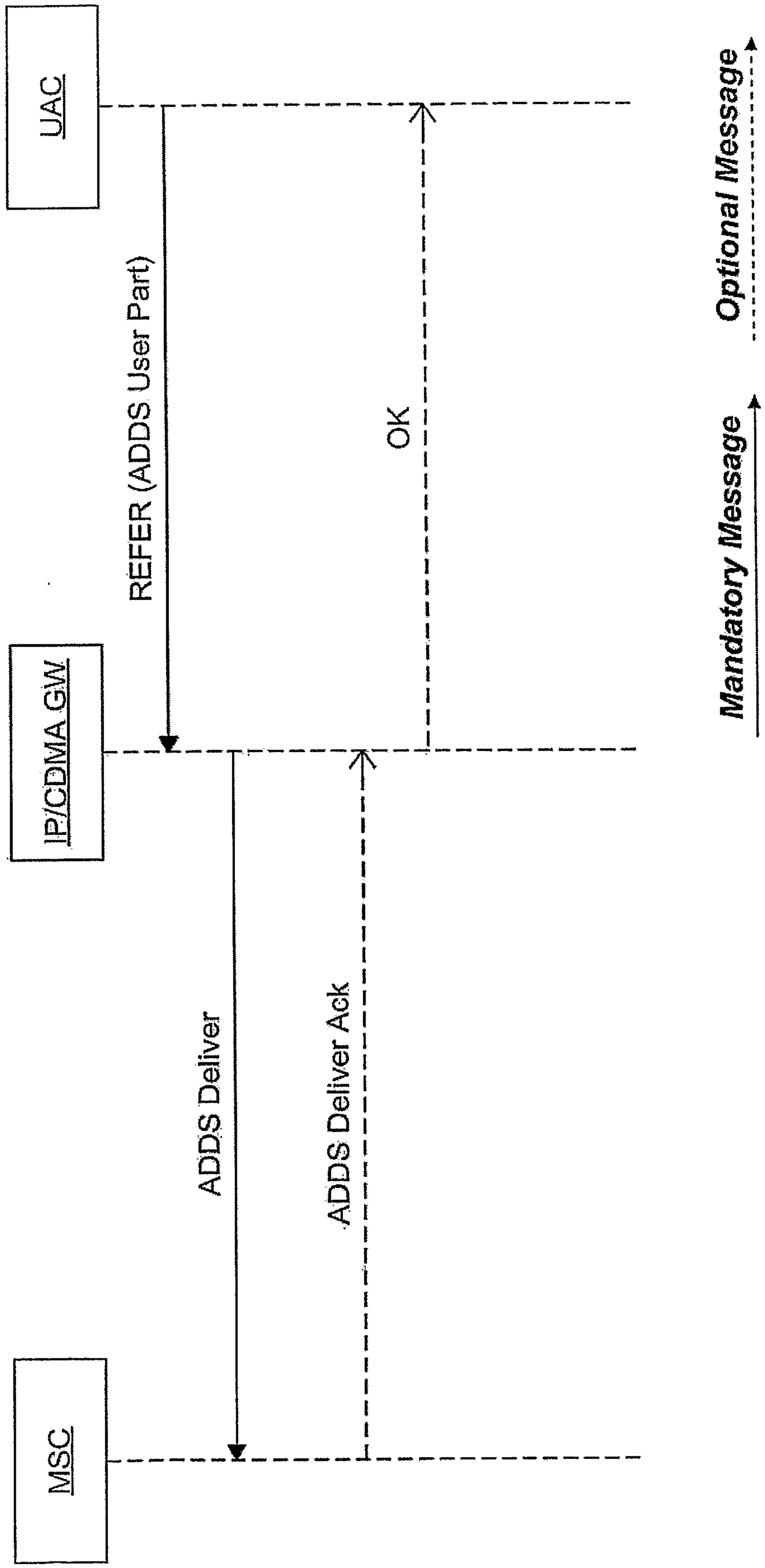


Fig. 9

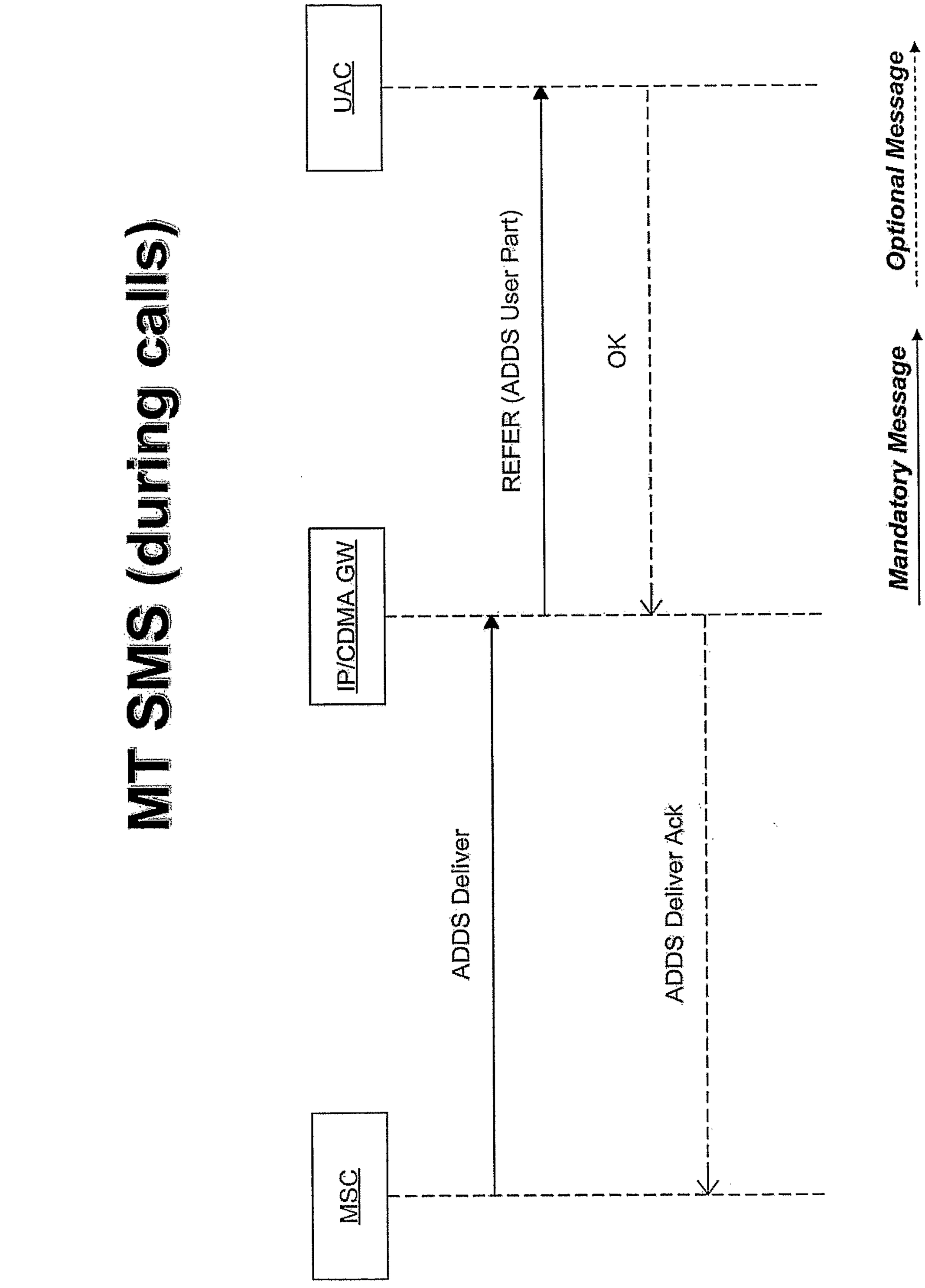

MT SMS (during calls)
UAC
IP/CDMA GW
MSC
REFER (ADDS User Part)
OK
ADDS Deliver
ADDS Deliver Ack
Mandatory Message
Optional Message

FIG. 10

IP-BSC General Architecture

