ELSEVIER

Computer Networks 34 (2000) 763–779

COMPUTER NETWORKS

www.elsevier.com/locate/comnet

Understanding GPRS: the GSM packet radio service

Brahim Ghribi, Luigi Logrippo *

Telecommunications Software Engineering Research Group, School of Information Technology and Engineering, University of Ottawa, Ottawa, Ont., Canada K1N 6N5

Abstract

The general packet radio service (GPRS), a data extension of the mobile telephony standard GSM is emerging as the first true packet-switched architecture to allow mobile subscribers to benefit from high-speed transmission rates and run data applications from their mobile terminals. A high-level description of the GPRS system is given with emphasis on services and architectural aspects.

Keywords: Mobile telephony; Mobile data communications; GSM; GPRS; Packet radio; Telecommunications

Nomenclature

ANSI	American National Standards Institute
APN	access point name
AuC	authentication center
BSCs	base station controllers
BSS	base station subservice
BTS	base transceiver stations
CDMA	code division multiple access
CLNS	connectionless network service
CONS	connection oriented network service
EDGE	enhanced data rates for GSM evolution
EIR	equipment identity register
ETSI	European Telecommunications Standards Institute
GGSN	gateway GPRS support node
GMM/SM	GPRS mobility management and session management
GPRS	GPRS packet radio service
GSM	global system for mobile communications
GSN	GPRS support node
GTP	GPRS tunneling protocol
HLR	home location register
HSCSD	high-speed circuit-switched data
IMSI	International Mobile Subscriber Id
IMT 2000	International Mobile Telecommunications 2000
IP	Internet protocol
IPsec	Internet protocol security
LA	location area
LLC	logical link control
MAC	medium access control
MO	mobile originated
MS	mobile station
MT	mobile terminal, mobile terminated
MSC	message switching center
NSS	network switching subsystem

* Corresponding author.
E-mail addresses: brahim.ghribi@alcatel.fr (B. Ghribi), luigi.logrippo@site.uottawa.ca (L. Logrippo).

1389-1286/00/$ - see front matter
PII: S1389-1286(00)00127-4

NSAP	network service access point
NSAPI	network service access point identifier
PCU	packet control unit
PIN	personal identification number
PDN	packet data network
PDP	packet data protocol
PDU	protocol data unit, packet data units
PLMN	public land mobile network
PTP	point-to-point
PTM	point-to-multipoint
RA	routeing area
RF	radio frequency
RLC	radio link control
SAP	service access point
SGSN	serving GPRS support node
SNDCP	subnetwork dependent convergence protocol
TDMA	time division multiple access
TE	terminal equipment
TID	tunnel identifier
TLLI	temporary logical link identity
UMTS	universal mobile telecommunications systems
VLR	visitor location register
WCDMA	wideband CDMA
3GPP	third generation partnership project

1. Introduction

In the past few years, fixed networks have witnessed a tremendous growth in data traffic due in good part to the increasing popularity of the Internet. Consequently new data applications are emerging and are reaching the general public. At the same time the market is witnessing a remarkable explosion of cellular and mobile technologies leading to demand that data applications become available to mobile users.

Global system for mobile communications (GSM) [1] is the European standard for cellular communications developed by the European Telecommunications Standards Institute (ETSI). Throughout Europe and the rest of the world (including North America), GSM has been widely adopted. It has already been implemented in over 100 countries [2]. The most important service in GSM is voice telephony. Voice is digitally encoded and carried by the GSM network as a digital stream in a circuit-switched mode.

GSM offers data services already but they have been constrained by the use of circuit-switched data channels over the air interface allowing a maximum bit rate of 14.4 kbit/s. For this reason, the GSM standard has continued its natural evolution to accommodate the requirement for higher bit rates. The high-speed circuit-switched data (HSCSD) are one solution that address this requirement by allocating more time slots per subscriber and thus better rates. It remains however insufficient for bursty data applications such as Web browsing. Moreover, HSCSD rely on circuit-switching techniques making it unattractive for subscribers who want to be charged based on the volume of the data traffic they actually use rather than on the duration of the connection. In turn, service providers need effective means to share the scarce radio resources between more subscribers. In a circuit-switched mode, a channel is allocated to a single user for the duration of the connection. This exclusive access to radio resources is not necessary for data applications with the use of packet switched techniques.

GPRS stands out as one major development in the GSM standard that benefits from packet switched techniques to provide mobile subscribers with the much needed high bit rates for bursty data transmissions. It is possible theoretically for GPRS subscribers to use several time slots (packet data channels) simultaneously reaching a bit rate of about 170 kbit/s. Volume-based charging is possible because channels are allocated to users only when packets are to be sent or received. Bursty data applications make it possible to balance more efficiently the network resources between users because the provider can use transmission gaps for other subscriber activities.

This paper aims to provide a comprehensive yet simple overview of the GPRS system from the user's and from the architectural perspectives. It addresses itself particularly to people who have some knowledge of the GSM system, however it tries to be self-contained as far as possible. This paper is based on the GPRS service description documents stage 1 [3] and stage 2 [4] proposed by ETSI. Additional information on GPRS can be found in [5,6].

2. GPRS services

GPRS services are defined to fall in one of two categories: point-to-point (PTP) and point-to-multipoint (PTM) services. Some of the GPRS services are not likely to be provided by network operators during early deployment of GPRS due in part to the phased development of the standard. Market demand is another factor affecting the decision of the operators regarding which services to offer first.

2.1. PTP services

GPRS will support applications based on IP. Applications based on the connection oriented network protocols are also defined to be supported. The X.25 protocol was initially mentioned but has been dropped in recent standard developments. Table 1 illustrates the general description of the PTP services and some possible applications.

2.2. PTM services

The PTM services provide the subscribers with the capability to send data to multiple destinations within one single service request. Table 2 shows a general description of these services and some possible applications. With the exception of point-to-multipoint multicast (PTM-M) services, groups must be defined and members are required to join an ongoing call to become participants. A point-to-multipoint group (PTM-G) call is usually restricted to members located within a specific geographical area. An IP-multicast (IP-M) call is on the other hand independent of the geographical area of the participants and can be internal to the network or distributed across the internet.

PTM services are de-emphasized in this paper because the main effort revolves around IP-based PTP services in current GPRS standard releases. Some work is being done however in the PTM services area and concerns IP-multicast.

3. Basic overview of the GSM network

In order to understand the GPRS network architecture, some fundamental GSM terminology is necessary. This section describes some of the main components of the GSM network (Fig. 1). The GSM PLMN is divided into two major subsystems: the base station subsystem (BSS), and the network switching subsystem (NSS). A GSM subscriber requires a terminal called mobile station (MS) to connect to the network using the radio interface (Um).

Table 1
Point-to-point (PTP) GPRS services

Service	Description	Applications
PTP-CONS Point-to-point connection oriented network service	• Bursty transactive or interactive applications • A logical relation is established between users • Multiple packets are sent between a single source and a single destination	Credit card validations Electronic monitoring Telnet applications Data base access and information retrieval
PTP-CLNS Point-to-point connectionless network service	• Datagram type service for bursty applications • No logical link required between users • Packets are sent between a single source and a single destination • Each packet is independent of its predecessor and successor	Electronic mail Internet's World Wide Web

Table 2
Point-to-multipoint (PTM) GPRS services

Service	Description	Applications
Point-to-multipoint multicast (PTM-M)	• Messages are transmitted to a specific geographical area and optionally to a specified group within that area • The recipients are anonymous • Delivery time is scheduled • Uni-directional transmission	News Weather and traffic reports
Point-to-multipoint group call (PTM-G)	• Messages are transmitted to a specific group within a specific geographical area • Group members must join the PTM-G call to become participants • Delivery in real time • Uni-directional, bi-directional and multi-directional transmissions	Conferencing services
IP multicast (IP-M)	• Messages are transmitted to a specified group • Group members must join the IP-M call to become participants • Delivery in real time • Multi-directional transmission	Live multimedia transmissions Corporate messages to employees

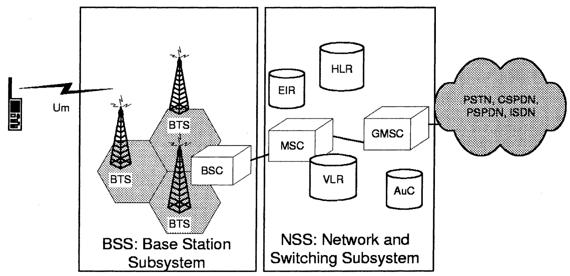


Fig. 1. GSM network architecture.

3.1. The network switching subsystem

The NSS is responsible for call control, service control and subscriber mobility management functions.

3.1.1. Home location register (HLR)

The HLR is a database used to store and manage permanent data of subscribers such as service profiles, location information, and activity status.

3.1.2. Mobile switching center (MSC)

The MSC is responsible for telephony switching functions of the network. It also performs authentication to verify the user's identity and to ensure the confidentiality of the calls. The authentication center (AuC) provides the necessary parameters to the MSC to perform the authentication procedure. The AuC is shown as a separate logical entity but is generally integrated with the HLR. The equipment identity register (EIR) is on the other hand a database that contains information about the identity of the mobile equipment. It prevents calls from unauthorized, or stolen MSs.

3.1.3. Visitor location register (VLR)

The VLR is a database used to store temporary information about the subscribers and is needed by the MSC in order to service visiting subscribers. The MSC and VLR are commonly integrated into one single physical node and the term MSC/VLR is used instead. When a subscriber enters a new MSC area, a copy of all the necessary information is downloaded from the HLR into the VLR. The VLR keeps this information, so that calls of the subscriber can be processed without having to interrogate the HLR (which can be in another PLMN) each time. The temporary information is cleared when the mobile station roams out of the service area.

3.1.4. Gateway mobile switching center (GMSC)

A GMSC is an MSC that serves as a gateway node to external networks, such as ISDN or wireline networks.

3.2. The base station subsystem

The BSS performs radio-related functions. It consists of base transceiver stations (BTSs) and base station controllers (BSCs).

3.2.1. Base transceiver station

The BTS handles the radio interface to the MS. It consists of radio equipment (transceivers and antennas) required to service each cell in the network.

3.2.2. Base station controller

The BSC provides the control functions and physical links between the MSC and the BTS. A number of BSCs are served by one MSC while several BTSs can be controlled by one BSC.

The reader is referred to [1] for a more substantial description of GSM network components. We focus in what follows on the GPRS network architecture and functionality.

4. GPRS architectural aspects

GPRS is considered as a service or feature of GSM. It was designed by ETSI to be implemented over the existing infrastructure of GSM without interfering with the already existing services. The aim is quick GPRS deployment with minor impact on existing GSM PLMN components. Fig. 2 illustrates the logical architecture of a GSM network supporting GPRS. The impact of GPRS introduction over the GSM network subsystems and the requirements for special GPRS terminals are described next.

4.1. The GPRS terminals

GPRS and GSM systems provide inter-working and sharing of resources dynamically between users. For this reason, three types of terminals have been defined: a class-A MS can carry a circuit-switched and a packet switched connection simultaneously enabling the subscriber to initiate or receive a voice call without interrupting a data transmission or reception activity. This type of terminal probably will not be available when GPRS is initially deployed due to its complexity and high cost. An MS of class-B is able to connect to both GSM and GPRS at the same time but an incoming voice call requires GPRS data transactions in progress to be suspended for the duration of the call. GPRS data transactions can then resume at the end of the voice call. Finally, a class-C MS allows subscribers to access one service type only at a given time in an exclusive manner.

The GPRS MS has two components: a mobile terminal (MT) which is typically a handset used to access the radio interface as a radio modem, and a terminal equipment (TE) which is typically a

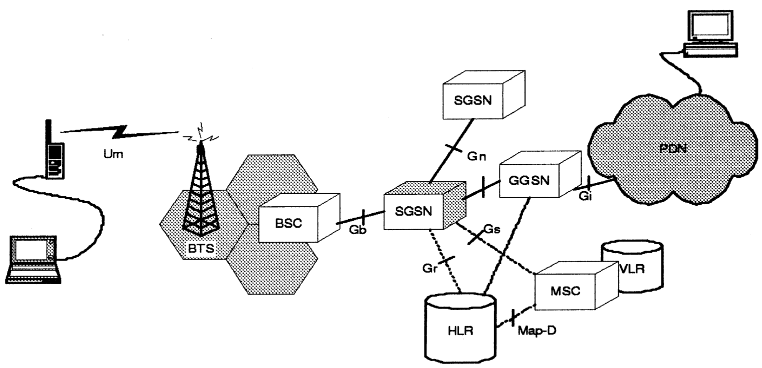


Fig. 2. Logical architecture of GPRS network.

laptop or a personal digital assistant (PDA). GPRS MSs will also come as one unit combining the functionalities of an MT and a TE.

4.2. GPRS BSS

GPRS has minor impact on the existing GSM BSS making it easy to reuse existing component and links without major modifications. This is possible because GPRS uses the same frequency bands and hopping techniques, the same TDMA frame structure, the same radio modulation and burst structure as GSM.

A new functional component called packet control unit (PCU) was added to the BSS in the GPRS standard to support the handling of data packets. The PCU (not shown in Fig. 2) is placed logically between the BSS and the GPRS NSS. Unlike the voice circuit connections however, connections in GPRS have to be established and released between the BSS and the MS only when data need to be transported over the air interface. Therefore, ETSI has defined new procedures to adapt such connections.

4.3. GPRS NSS

The GPRS NSS can be viewed as an overlay network ensuring the link between mobile users and data networks. GPRS introduces a new functional element to the GSM infrastructure (Fig. 2): GPRS support node (GSN) which can be either a serving-GSN (SGSN) or a gateway-GSN (GGSN). This addition is necessary for the GSM network in order to support packet data services. The network is generally divided into several service areas controlled by separate SGSNs. Only one SGSN serves an MS at a given time provided it is located in its service area. The SGSN is primarily responsible for keeping track of the MSs it serves, and for access control to data services. The GGSN on the other hand provides the interface to external packet data networks (PDNs). The SGSN is connected to the BSS by frame relay and to possibly several GGSNs via a GPRS backbone network. The HLR database is updated to contain GPRS subscriber information. Adaptations to an existing MSC/VLR are not required but the GPRS standard suggests some enhancements to coordinate between the SGSN and the MSC/VLR if the optional interface between the two is to be supported.

Several interfaces have been introduced in GPRS to define entity-to-entity interactions. For instance, the *Gb* interface is required between the BSC and the SGSN. Two GSNs communicate through a *Gn* interface, and the SGSN sends queries and receives subscriber information to/from the HLR through the *Gr* interface. The *Gs* interface between the SGSN and the MSC/VLR was left optional while the *Gi* interface which connects a GGSN to a PDN was not specified in the standard to allow implementation preferences.

As mentioned, GPRS standard activities focused mainly on PTP connections to IP PDNs at the *Gi* interface. An example of such IP PDN can be a corporate Intranet where access is restricted to authenticated corporate employees allowing them to access for instance the corporate web and mail servers. Another example is connectivity to an Internet service provider (ISP) offering Internet access and related services.

4.4. Transmission/signaling planes in GPRS

A layered protocol structure is adopted for the transmission and signaling planes in GPRS (Fig. 3). The subnetwork dependent convergence protocol (SNDCP) serves as a mapping of the characteristics of the underlying network such as IP. Mobility management functionality is supported by the GPRS mobility management (GMM) and session management (SM) layers. The logical link control (LLC) layer provides a logical link between the MS and the SGSN and manages reliable transmission while at the same time supporting point-to-point and point-to-multipoint addressing. The radio link control (RLC), medium access control (MAC), and GSM RF (radio frequency) layers control the radio link, the allocation of physical channels and radio frequency. LLC PDUs (packet data units) between the MS and the SGSN are relayed at the BSS. The base station system GPRS protocol (BSSGP) layer handles routing and QoS between the BSS and the SGSN. The GPRS tunneling protocol (GTP) is the

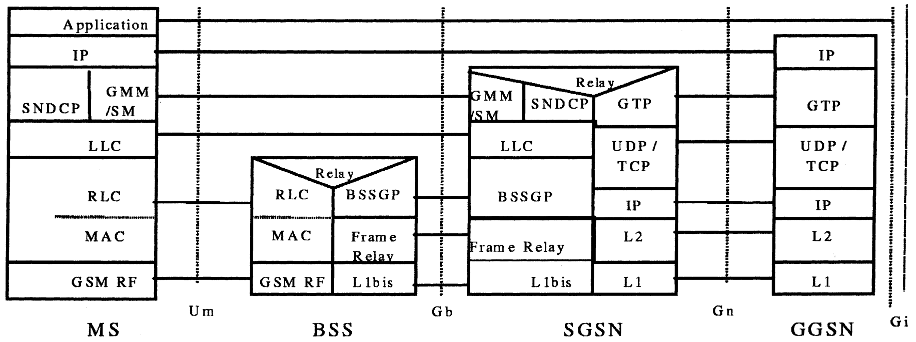


Fig. 3. GPRS transmission/signalling planes from MS to GGSN.

basis for tunnel signaling and user PDUS between the SGSN and GGSN. We do not describe the rest of the layers of Fig. 3 because they are already well known.

5. Security in GPRS

Security is an important issue in mobile networks and has gained a special attention in the GSM world. GPRS provides a security function similar to that of GSM. It is responsible for authentication and service request validation to prevent unauthorized service usage. User confidentiality is also protected using temporary identification during connections to the GPRS network. Finally, user data are protected using ciphering techniques.

5.1. Authentication in GPRS

Authentication in cellular systems often means the use of a PIN code as a means of identification. Such method is not very secure since it is possible in a radio environment to capture the PIN and therefore to break the confidentiality of the subscriber. Especially dangerous is the fact that this PIN is assigned once at subscription and therefore it can be captured in many ways. The GSM/GPRS approach addresses this problem by varying the access code for every connection. A secret parameter *Ki* specific to the user is used to compute a shared value using an operator-dependent one-way (trap-door) algorithm. Fig. 4 shows the

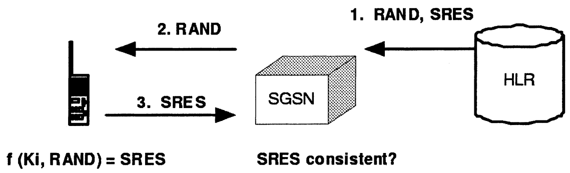


Fig. 4. The GPRS authentication computation.

authentication computation using the parameter *Ki* which is never transmitted via the air interface. The sequence of the figure is triggered when the MS requests to attach to the GPRS network or may be requested by the SGSN if the MS is roaming. The MS is issued a new random number *RAND* whenever authentication is required. The MS computes the value SRES (signed result) using *Ki* and *RAND* and forwards it back to the SGSN for comparison. The authentication procedure in GPRS is executed from the SGSN instead of the MSC/VLR as in GSM.

5.2. Ciphering in GPRS

Ciphering between the MS and SGSN starts only after the MS is authenticated. Similarly, a secret ciphering key *Kc* is used at the MS and the SGSN to encrypt the exchange of messages. The ciphering scope is from the MS to the SGSN while in GSM it is from the MS to the BSS. This is done to simplify the key management since cell selection by the MS can occur frequently and therefore packets may travel via different BTSs. In GSM however, a single logical channel is used between the MS and the BTS at each given time. Also, by extending the scope of ciphering in GPRS, ciphering algorithms can be changed without updating every element of the BSS. Alternatively, radio elements can be upgraded or replaced without modifying the ciphering mechanism.

5.3. Security in the GPRS backbone

Authentication of subscribers in GPRS is performed by the SGSN, and the scope of ciphering is between the MS and the SGSN. The GPRS standard has left to the implementation the requirements for security beyond the SGSN and GGSN. For instance, an IP-based GPRS backbone can ensure security using IP security protocol (IPsec) [7] which groups a set of mechanisms used to protect traffic at the IP level. Secured services offered by IPsec are integrity in connectionless mode, authentication of data origin, and protection of data confidentiality. IPsec is interesting because it provides security of data at the network level rather than at the application or physical levels.

An operator can ensure security in the GPRS backbone by relying on several options such as the following:

- installing firewalls at the *Gi* reference point (between a GGSN and an external data network),
- using border gateways when interfacing to other GPRS networks,
- improving the backbone network protection by using some security products such as IPsec for an IP-based backbone as mentioned above, and
- using some packet filtering mechanisms.

6. Mobility management in GPRS

Mobility management is the means by which a mobile network such as GPRS can keep track of the mobile subscriber location while connected to the network. To understand mobility management in GPRS, the reader needs to understand the following concepts:

- GPRS service areas,
- GPRS network access,
- GPRS mobility management states,
- GPRS procedures required to keep track of individual MSs.

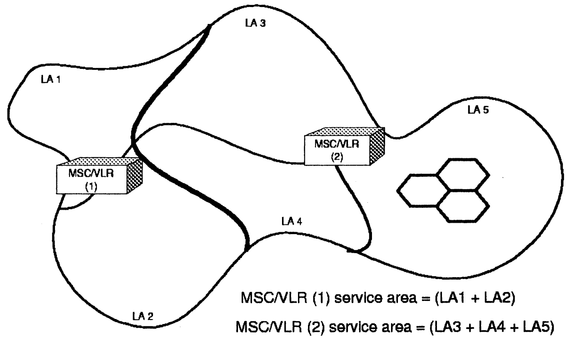


Fig. 5. GSM network service areas.

6.1. GPRS service areas

In GSM, the network is divided into several MSC/VLR service areas. Each MSC/VLR spans over a group of location areas (LAs) which are sets of cells. Fig. 5 illustrates a simplified example of the GSM network service areas. The network is shown to be divided into five LAs and two MSC/VLR service areas. The thick line in the figure is used to show the separation between the two service areas.

In GPRS on the other hand, a group of cells is called a routeing [1] area (RA). The SGSN controls a service area containing several RAs. There may not be a direct mapping between SGSN and MSC/VLR service areas but an RA is a subset of one, and only one, LA. GPRS has chosen a different layout from GSM (i.e., RAs instead of LAs) to allow for signaling and paging over geographically smaller areas and thus, a better optimization of radio resources. One possible implementation of GPRS in the existing GSM network of Fig. 5 is shown in Fig. 6. The example suggests three SGSN service areas to span over 11 RAs. The reader should be aware that the example is simplified to illustrate the difference between GSM and GPRS service areas. In a real network implementation, the layout is decided by the operator of the network.

[1] Note the unusual spelling: the GPRS standard uses it to distinguish between the generic concept of *routing* and the concept of *routeing* described in this section.

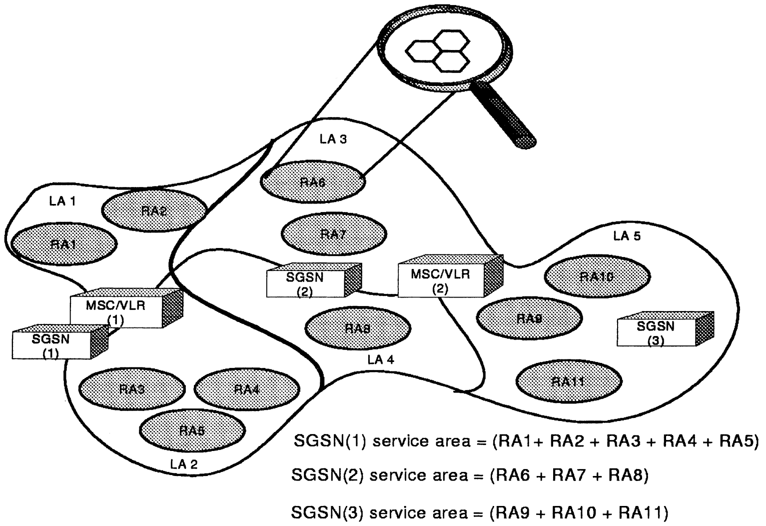


Fig. 6. GPRS network service areas.

6.2. Accessing the GPRS network

An MS can connect to the GPRS network by requesting a GPRS *attach* procedure. The outcome is the establishment of a logical link between the MS and a single SGSN and the creation of a mobility management context. The logical link is uniquely defined by the identifier temporary logical link identifier (TLLI) and is used subsequently in messages exchanged between the MS and SGSN. This identifier is changed when the MS is served by a new SGSN.

6.3. Mobility management states

The MS in GSM can be in one of two states: *Idle* or *Dedicated.* A channel allocation is held for the MS exclusively when it is in *Dedicated* mode due to the nature of circuit- switched connections. When the connection is released, the MS returns to *Idle* mode. A GPRS MS on the other hand can share radio channels with other subscribers connected to the network. For this reason, the MS is defined to have three possible states: *Idle*, *Ready*, and *Standby* (Fig. 7).

6.3.1. Idle state

An MS in the *Idle* state is not traceable and can only receive PTM-M transmissions such as general

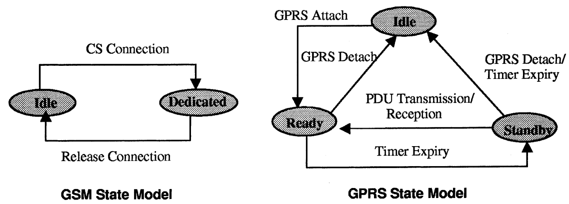


Fig. 7. GSM and GPRS functional state models.

broadcast events destined to a specific geographical area. The MS needs to perform the attach procedure in order to connect to the GPRS network and become reachable.

6.3.2. Ready state

Data are sent or received in this state. The MS informs the SGSN when it changes cells. The MS may explicitly request (or can be forced by the network) to detach in which case it moves to *Idle*. A timer monitors the *Ready* state and upon its expiry, the MS is put on *Standby*. The timer insures that resources are not wasted by an inactive MS.

6.3.3. Standby state

A connected MS which is inactive is put in the *Standby* state. Moving back to *Ready* can be triggered by sending data or signaling information from the MS to the SGSN. Upon arrival of data destined to the MS, the SGSN pages the latter and a response to the page moves the MS back to the *Ready* state. The MS may wish (or can be forced by the network) to terminate the connection by requesting to *detach* in which case it returns to *Idle*. A timer is used by the SGSN to monitor the tracking of the MS, and when it expires, the MS is detached and is considered unreachable.

6.4. Keeping track of the MS

Location management is the means by which the GPRS network keeps track of the MS location. Within a GPRS network, three types of location management procedures are described (Fig. 8):

- *Cell update* is the means by which an MS informs the network of its current cell location.
- *Intra-SGSN routeing update* is the procedure used when an MS changes RA and remains serviced by the same SGSN.

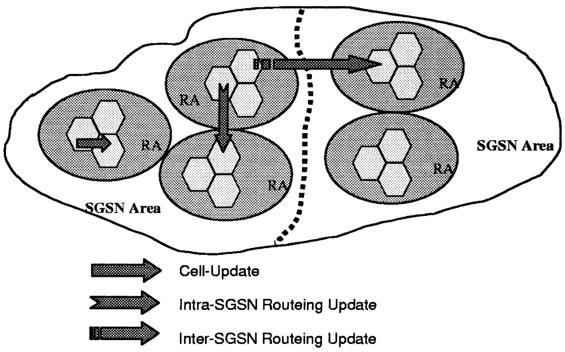


Fig. 8. GPRS location management procedures.

- *Inter-SGSN routeing update* is the procedure used when the entry of an MS to a new RA triggers a change of SGSN service area.

When roaming agreements between different network operators exist, an MS that enters a new network performs a routeing update procedure provided that this is allowed by the implementation. Otherwise, the MS is forced to the Idle state. In early GPRS implementations, the latter case is most likely to occur.

The location management procedures depend on the current state of the MS (Table 3). An Idle MS does not perform any updates. An MS in Standby performs routeing area updates only and does not inform the SGSN of its cell changes. The SGSN needs to know the cell changes only when the MS is in the Ready state. This is done in two ways: when the new cell is within the same RA, a cell update takes place. Alternatively when the new cell is within a new RA, then a routeing update procedure is performed instead. The BSS usually adds the cell identifier to the routeing update request and this will be used by the SGSN to derive the new RA identity. Also, even if the MS does not change RA, it is requested that an RA update be done periodically.

The MS detects that it has entered a new cell or new RA by listening periodically to special control channels that broadcast general information such as the identities of the cell, the RA, the LA, and of the network.

From the MS point of view, inter and intra-SGSN updates are transparent and the request is the same. The SGSN on the other hand is able to detect whether the MS is new in its service area or

Table 3
Location management and mobility management states

	Cell updates	Intra-SGSN routeing updates	Inter-SGSN routeing updates
Idle	No The MS is aware of cell changes locally	No	No
Standby	No	Yes if the new cell belongs to a new RA but remains within the same SGSN service area	Yes if the new cell belongs to a new RA that is within a new SGSN service area
Ready	Yes if new cell is within the same RA	Yes if the new cell belongs to a new RA but remains within the same SGSN service area	Yes if the new cell belongs to a new RA that is within a new SGSN service area

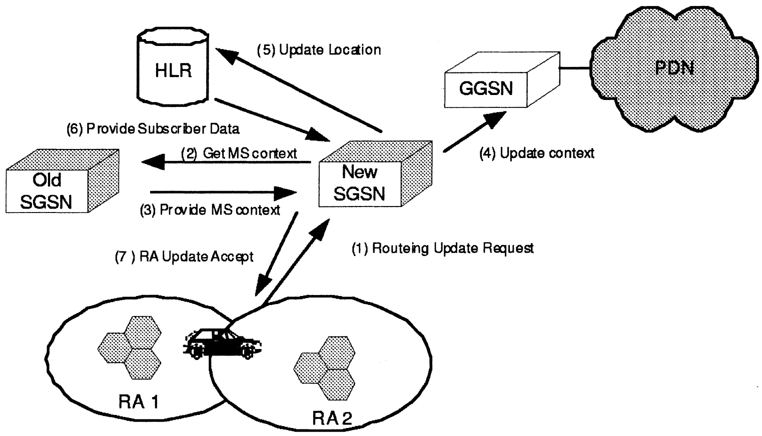


Fig. 9. Inter-SGSN routeing update procedure (simplified).

if it is already a serviced MS switching RAs. The MS includes the parameter *old RA* in the routeing update request when it enters a new RA. By looking at this parameter, the SGSN can conclude whether the old RA is in its service area or not. If it is the case, the SGSN performs a simple intra-SGSN routeing update procedure and does not need to inform the GGSN and the HLR about the new location of the MS. An old RA outside the scope of the SGSN implies that the MS must have been served by another SGSN and an inter-SGSN routeing update procedure is required (Fig. 9). We simplified the signals exchanged by removing the acknowledgments and details related to the security functions which may be requested by the new SGSN in order to authenticate the MS. The old SGSN provides the new SGSN with the context information which describes the current activities of the MS. The new SGSN is responsible for informing the GGSNs and the HLR (which could be in another service area) of the new MS location. Finally, the HLR needs to provide the subscriber's information to the new SGSN.

7. End-to-end packet routing

We described in the previous sections how an MS can access the GPRS network and how mobility management procedures are used to keep track of its location. To use data services via the GPRS network, specific procedures for packet data networks access and data routing are performed and are discussed in this section.

Once an MS is attached, it can request to activate one or more packet data protocol (PDP) contexts which specify the packet data networks (PDNs) it wants to access. In other words, the MS asks the SGSN to create routing paths or "tunnels" to the external data networks. A PDP context activation procedure is initiated for each required PDP session. The activation procedure can be triggered by the MS (MS initiated) or by an incoming request from a PDN (network requested). A PDP context refers to the parameters required to transfer packets between the MS and the PDN via a GGSN. These parameters are specific to each PDP context and include routing information and the quality of service (QoS) profile.

7.1. PDP context activation procedure

The MS specifies its network service access point and the access point name (APN) of the PDN it wants to connect to. The APN specifies the target PDN network identifier such as "intranet.company-name.com" and the operator domain name such as "operatorname.country.gprs". The SGSN identifies the corresponding GGSN and makes it aware of the MS. A two-way point-to-point path or a "tunnel", is uniquely identified by a tunnel identifier (TID) and is established

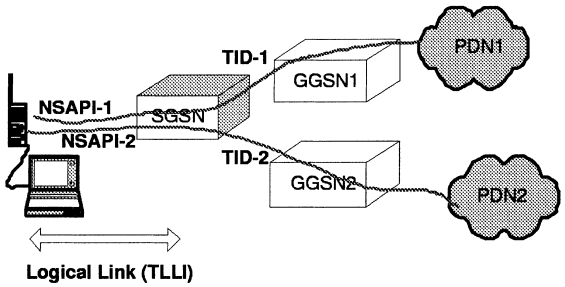


Fig. 10. A MS with PDP contexts active.

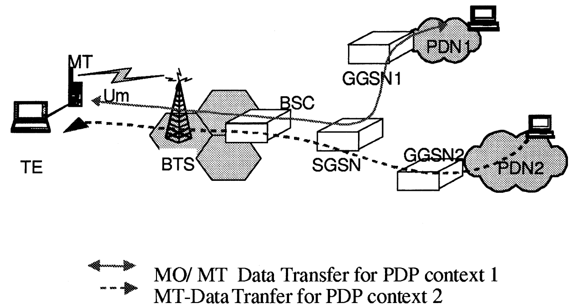


Fig. 11. End-to-end packet switching for a MS in the home network.

between the SGSN and the GGSN. Tunneling is the means by which all encapsulated packets are transferred from the point of encapsulation to the point of decapsulation. In this case, the SGSN and GGSN are the two end-points of the tunnel.

At the MS side, a PDP context is identified by a network service access point identifier (NSAPI). The MS uses the appropriate NSAPI for subsequent data transfers to identify a PDN. On the other hand, the SGSN and GGSN use the TID to identify transfers with respect to a specific MS. Fig. 10 illustrates an example of an MS with two PDP contexts activated. The MS uses NSAPI-1 for its data transfers with PDN1. The corresponding tunnel is identified by TID-1. Similarly, NSAPI-2 is used by the MS to connect to PDN2. The tunnel identifier in this case is TID-2.

Depending on the GPRS implementation, an MS can be assigned static or dynamic addresses. For instance, the operator can assign a permanent (static) PDP address to the MS or choose to assign a different address for each PDP context activated dynamically. Also, a visited network may assign dynamically an address to the MS for each PDP context activated.

7.2. Packet switching in GPRS

Once the MS has attached, data activities can proceed with a PDN provided that a PDP session has been established with the PDN in question. GPRS data are encapsulated and tunneled between the MS and the PDNs transparently through the GPRS network. Sub-network dependent convergence protocol (SNDCP) provides compression and segmentation mechanisms and ensures the transfer of data packets between the MS and the SGSN. GTP (GPRS tunneling protocol) manages tunneling of user packets between the SGSN and the GGSN. Data can also be transferred in a protected mode and monitored by retransmission protocols.

For a given active PDP context, data transfer can be mobile-originated (MO) or mobile-terminated (MT). The activation of the PDP context can be however MS-initiated or network requested and the transfer mode is independent of this fact.

MO packets are forwarded by the SGSN to the appropriate GGSN through the established GTP tunnel. The GGSN then delivers the packets to the PDN. For MT transmissions, when the GGSN receives data packets for the MS, it identifies the SGSN that is currently serving it, and tunnels the packets. The SGSN then delivers the packets to the MS in the appropriate cell. When the MS is in Standby, if it is paged in the appropriate RA and it responds to the page, it moves to the Ready state in order to receive the packets.

Fig. 11 illustrates an example of data routing for two active PDP contexts.

7.3. Data routing for a mobile MS

As a result of mobility, GPRS requires a mechanism to continue forwarding the packets to the MS when it enters a new SGSN service area. In GPRS, a buffering mechanism controlled by a timer in the old SGSN is used. This is how it works: as soon as the old SGSN responds to the new SGSN with the MS context information, it starts a timer and starts tunneling buffered PDUs received from the GGSN to the new SGSN. The old SGSN stops forwarding packets to the new SGSN when the timer expires. The new SGSN buffers the packets received until the inter-SGSN routeing update procedure is completed and then delivers them.

When the MS is roaming in a visited PLMN, it can still access GPRS services, perform mobility management functions, activate PDP contexts, and send and receive packets under the following conditions:

- roaming agreements exist between the home PLMN and the visited PLMN,
- the subscription allows for the requested services in the visited PLMN,
- the presence of a border gateway between the home and the visited PLMNs to ensure the transport of signaling and data between both PLMNs.

8. GSM/GPRS service interactions

GPRS has a special network mode of operation (Mode I) allowing mobility management coordination between GSM and GPRS through the Gs interface. Interactions between GSM and GPRS services imply the need for interactions between the SGSN and the MSC/VLR and for the optional Gs interface between the two to be supported. An association is maintained between the SGSN and the MSC/VLR that are currently serving the MS so paging for circuit-switched calls can be achieved via the SGSN when the MS is camped on the packet side. The SGSN is identified by a number that is communicated to the MSC/VLR during a mobility management update procedure. Similarly, the VLR is identified by a number that is derived from the RA identifier by the SGSN using a mapping table. The SGSN has to keep track of the VLR number while the latter stores the MS class and the SGSN number.

Among the benefits of such association is the economy of radio resources. For instance, when an MS is already attached to the GPRS network (GPRS attached), it can request to attach to the GSM network (*IMSI-attach*) via the SGSN. A combined *GPRS/IMSI attach* is also possible and will be issued via the SGSN which initiates the association with the MSC/VLR. GSM location update procedures and paging for circuit-switched calls can be accomplished via the SGSN. The association is updated every time the MS changes SGSN or MSC/VLR service areas and is removed at GPRS or IMSI detach.

8.1. Co-ordination of location area and routeing area updates

The MS monitors the RA and LA every time it enters a new cell. If the MS is both GPRS and IMSI attached and the LA is changed, then it may use the RA update request to include the LA change. The SGSN forwards the LA update to the MSC/VLR.

In the example shown in Fig. 12 and explained in Table 4, an MS moves from LA2 and crosses LA4 to finally reach LA5. During this transition, the MS has actually covered RA3, RA4, RA8, and RA11. Assuming that the MS is of class A or B and is in GSM Idle state, several possible location management procedures are required and are described in Table 4. Note that in GSM, no LA updates are performed during the dedicated state.

Another possible scenario not shown in Table 4 is the case of combined Intra-SGSN RA/LA update. This occurs when the MS switches MSC/VLR but remains within the service area of the same SGSN. In this case a new association between the new MSC/VLR and the SGSN is created and the old association with the old MSC/VLR is removed. Note that the illustration of Fig. 12 does not consider such scenario for simplicity but some networks may support it.

8.2. Circuit-switched paging via the SGSN

By maintaining the association between MSC/VLR and SGSN, the MSC can page the MS for incoming circuit-switched calls via the SGSN (Fig. 13). Paging via the SGSN is more efficient because the SGSN will page in either a cell or a routeing area which is always contained in a GSM location area. The MS needs to listen therefore to only one paging channel, and the paging area is

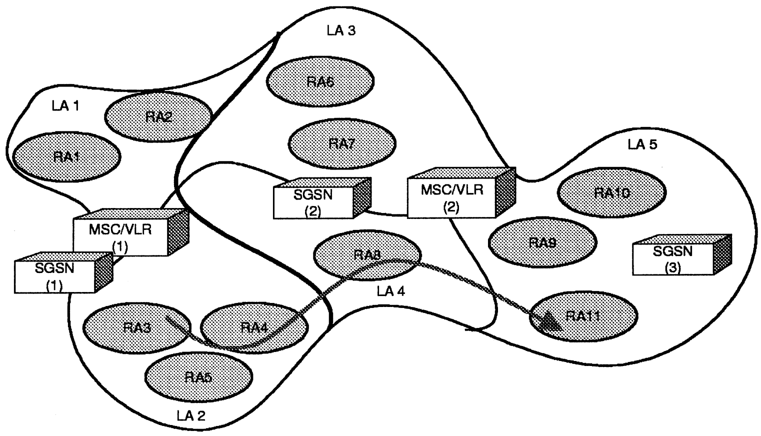


Fig. 12. Location area and routeing area updates.

Table 4
Examples of location management procedures

MS connection	RA3 to RA4 (within LA2)	RA4 to RA8 (LA2 to LA4)	Within RA8 (within LA4)	RA8 to RA11 (LA4 to LA5)
GPRS-attached only (MS GPRS-Standby or Ready)	Intra-SGSN routeing area update MS remains serviced by SGSN(1)	Inter-SGSN routeing area update Control is handed over from SGSN(1) to SGSN(2)	Cell updates only if the MS is in GPRS-Ready state	Inter-SGSN routeing area update Control is handed over from SGSN(2) to SGSN(3)
GPRS/IMSI-attached (MS GSM-Idle) (MS GPRS-Standby or Ready)	Same as for GPRS-attached only Association between SGSN(1) and MSC/VLR (1) is unaffected	Combined inter-SGSN RA/LA update Create new association between MSC/VLR(2) and SGSN(2) and clear old association between MSC/VLR(1) and SGSN(1)	Same as for GPRS-attached only	Combined inter-SGSN RA/LA update Create new association between MSC/VLR(2) and SGSN(3) and clear old association between MSC/VLR(2) and SGSN(2)

optimized. One important detail to keep in mind is that the MS can be already engaged in a GPRS data transaction which may require extra handling depending on the class of the MS.

8.3. The special case of class-B MS

As mentioned, a class-A MS can engage in GPRS and GSM calls simultaneously which means that it can continue receiving packets while carrying a GSM voice call. Class-B on the other hand is a special case since it can be both IMSI/GPRS attached but can only service one of them at a time. In the case where the MS is already engaged in a GPRS data transaction, an incoming GSM call requires the GPRS packet activity to be suspended until the voice call is terminated.

8.4. Point-to-point short message service (SMS)

GPRS is also defined to support the GSM SMS service. The idea is to allow GPRS attached mobiles to send and receive short messages via the SGSN and over the GPRS radio channels. This feature aims to further optimize the use of radio resources and to give operators more flexibility in terms of SMS delivery. An additional interface (Gd interface) has been defined for the purpose of SMS support and connects the SGSN to SMS gateway nodes.

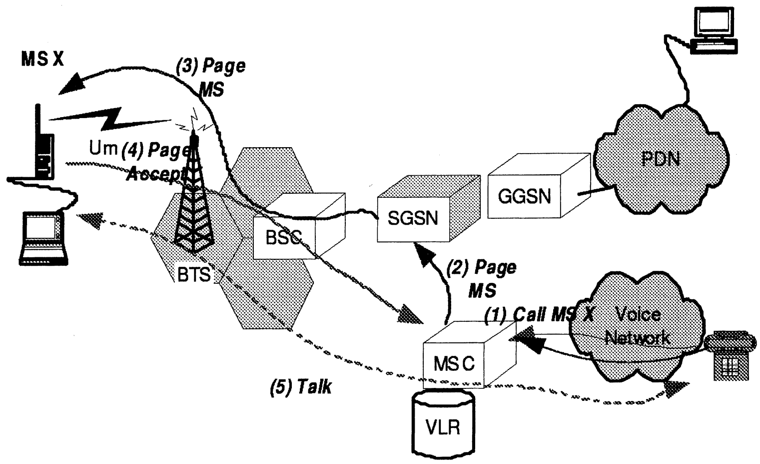


Fig. 13. Circuit-switched page via the SGSN.

9. Limitations of GPRS

Despite its potential, GPRS remains constrained by the following limitations:

- GPRS transmission rates are much lower than in theory. To achieve the theoretical maximum of about 170 kbit/s would require allocating eight time slots to a single user which is not likely to be allowed by network operators. Even if this maximum allocation was allowed, the GPRS terminals may be constrained by the number of time slots they can handle.
- GPRS relies on packet switching which means that data packets can traverse different routes and then be reassembled in their final destination leading to potential transit delays affecting the QoS.
- GPRS relies also on re-transmission and data integrity protocols to ensure that data packets transmitted over the radio air interface are not lost or corrupted. This can affect even further the transit delay problem.
- GPRS allows the specification of QoS profiles using service precedence, delay, reliability, mean and peak throughput. Although these attributes are signaled in the protocols and are negotiated between the network and the MS, no procedures are defined to provide QoS differentiation between services. This causes a lack of uniformity with respect to QoS between manufacturers and potentially between operators. This issue is being addressed in later standard efforts.
- Although it is possible theoretically to specify a high QoS profile, traffic over radio imposes severe constraints on the QoS.
- The protocols between the BSS and the SGSN support mainly asynchronous data transfer applications making it a challenge to implement real-time interactive traffic.

10. Evolution to third generation wireless communications

GPRS is a stepping stone towards third generation wireless communications. Its deployment provides the means to create new services, and to reach markets that were not easily accessible in the past. For instance, it will be possible to introduce Internet access via GPRS in areas where a fixed telephony network infrastructure is not existent or scarce. However standardization committees are aware of the limitations of GPRS and are working on defining a set of standards to build a migration path towards third generation systems. The main activities in this direction are:

- Enhanced data rates for GSM evolution (EDGE). This standard is still evolving and it introduces a new modulation technique for the transmission of packets over the air interface.

While GPRS is based on a modulation technique known as Gaussian minimum-shift keying (GMSK), EDGE is based on a new modulation method called eighth phase shift keying (8PSK). It will allow a much higher bit rate of up to 384 kbit/s. The combination of EDGE and GPRS leads to what is called E-GPRS for enhanced GPRS and will result in a much improved use of the radio resources. The benefit of EDGE is that it will have minor impact on the network structure and therefore it can be introduced quickly to existing networks.

- GPRS-136. The GPRS standard is evolving to be deployed not only in mobile networks that are based on GSM, but also to inter-work with the North American IS-136 time division multiple access (TDMA) standard. GPRS-136 is the TDMA packet data standard that adopts GPRS to reuse most of the existing network components (the NSS part). A gateway MSC/VLR is required to connect the GPRS network (the SGSN) to the ANSI-41 mobile switching network (ANSI-41 MSC/VLR). EDGE was chosen to allow for high-speed TDMA. The deployment of GPRS in a high-speed TDMA network is called GPRS-136HS.
- Universal mobile telecommunications system (UMTS) is the European version of International Mobile Telecommunications 2000 (IMT 2000). This is the core of third generation (3G) systems and is developed under the auspices of ETSI and 3GPP. It builds on GSM and GPRS technology to offer a global wireless standard for personal multimedia applications. The air interface has been completely reworked and a new BSS technology is introduced, based on wideband CDMA (WCDMA). The UMTS BSS will be connected to an enhanced GSM/GPRS network via the *Iu* interface which is being defined. Theoretically, UMTS will support high-speed packet data up to 2 mbit/s.

11. Summary

This paper presents an overview of GPRS and covers most of the key architectural and functional aspects. Although GPRS is intended to support a multitude of services including point-to-multipoint, the emphasis was on point-to-point IP services reflecting current GPRS standard releases. GPRS limitations and the main standardization activities towards third generations wireless telecommunications systems were enumerated as concluding topics for the paper.

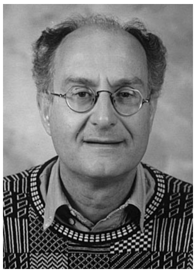
Acknowledgements

We are grateful to Motorola Canada and to NSERC for partial funding of this research, and to Laurent Andriantsiferana for many useful discussions.

References

[1] M. Mouly, M.B. Pautet, The GSM System for Mobile Communications, Palaiseau, France, 1992.
[2] J. Rapeli, Standardization for global mobile communications in the 21st century, European Telecommunications Standardization and the Information Society, The State of the Art, ETSI, 1995, pp. 176–185.
[3] ETSI, GSM 02.60 Digital Cellular Telecommunications System (Phase 2+): General Packet Radio Service, Service Description Stage 1.
[4] ETSI, GSM 03.60 Digital Cellular Telecommunications System (Phase 2+); General Packet Radio Service, Service Description Stage 2.
[5] S. Buckingham, Data on GPRS, Mobile Lifestreams Limited, 1999.
[6] C. Scholefield, Evolving GSM data services, IEEE 6th Int. Conference on Universal Personal Communications, October 1997, pp. 888–892.
[7] A. Randall, K. Stephen, Security Architecture of the Internet Protocol, Internet Request for Comments, RFC 2401.

Brahim Ghribi received his Bachelor and Master degrees in Computer Science from the University of Ottawa respectively in 1990 and 1992. From 1992 to 1996 he worked as a software engineer with Computing Devices Canada. From 1996 to 1998, he was a research associate in the Telecommunications Software Engineering Research Group of the University of Ottawa. Since 1999, he has been with Alcatel France as a Telecommunication Systems Engineer working on Packet Radio Services for GSM and UMTS. He is an active member in the standardization process towards third generation mobile telecommunication services and architectures.



Luigi Logrippo received his "laurea" from the University of Rome (Italy) in 1961. Until 1967, he worked with Olivetti, Olivetti-Bull, General Electric, and Siemens as a programmer and systems analyst. From 1967 to 1969 he was a Research Associate at the Insititute for Computer Studies, University of Manitoba, where he obtained a M.Sc. in Computer Science in 1969. He then obtained a Ph.D. in Computer Science at the University of Waterloo in 1974. Since 1973, he has been with the Computer Science Department of the University of Ottawa, where he is a Professor and has been Chair for two terms. His current research interests are in the area of telecommunications software engineering: specification, verification, formal development from specifications, and testing. The main application area studied is telephony (including mobile telephony) with its services. He has participated in the design of the specification language LOTOS and is pursuing research on its applications and extensions.