ESPRIT PROJECT EP28425

Broadband Integrated Satellite Network Traffic Evaluations

Deliverable 2.4

Mobile Network Characteristics

Status / Version : **DELIVERABLE / FINAL**
Date : **September 30, 1999**
Distribution : **Public**
Code : **BISANTE/DEL24**
Author (s) : **J-Y. Chiaramella (Ed.), C. Xenakis, H. Hlavacs**

Abstract : The goal of this deliverable is in the continuity of the other deliverables in WorkPackage 2, which is to provide the network characteristics which have an impact on the upper layers of applications, in this case for mobile networks.
For this, a survey of the most popular mobile networks in use today has been done, each one being analyzed for its individual characteristics.
A second phase was to address the modeling techniques we will follow in order to implement the models of the selected mobile networks.

The BISANTE Consortium consists of :

Thomson-CSF Communications	Partner	France
Netway	Partner	Austria
Solinet	Partner	Germany
University of Vienna	Associated Partner	Austria
University of Surrey	Associated Partner	United Kingdom
Institut National des Télécommunications (INT)	Associated Partner	France

TABLE OF CONTENTS

1. INTRODUCTION

As in the previous deliverables belonging to WorkPackage 2, the main topic of the present document is to identify the various characteristics of mobile networks that have an impact on the upper layers, meaning the various applications running on these networks, and, by extension, the network users.

No network is truly similar to another, but in the case of mobile networks, the differences between various technologies are perhaps even more pronounced than usual. For this reason, each kind of mobile network will be studied and characterized separately. As it would be pointless to try to list and examine each kind of mobile network ever designed, we will restrict ourselves to the most popular and widely used ones, namely :

- **WLANs** (or Wireless Local Area Networks) are designed to provide mobile communications over small areas, but in return allow for better performances. We will concentrate on the most well-known ones : the **802.11 standard** and the newer **HiperLAN** technology.

- As for terrestrial networks, where one finds both Local Area Networks and Wide Area Networks for communications over small and large areas respectively, some mobile networks are designed to allow transmissions over greater distances than those allowed by WLANs. As there are many types of networks in this category, we will sort them out according to their age, as outlined below :
  - First, we will examine the networks that compose the second generation (or the "current generation"), namely **DECT** and **GSM**
  - **GPRS**, both as it stands as a gateway between the second and third generation of mobile networks, and as it is the protocol we are more interested in in the course of the BISANTE project, will be detailed in a separate chapter
  - Last, we will present **UMTS**, which is the first mobile network belonging to the new third generation.

The goal of this deliverable is also not only to determine what characteristics do mobile network possess that have impact on upper layers, but also to determine how we will model them for in later parts of the project. For this reason, the last chapter will be describing the modeling techniques specific to mobile networks (such as roaming, handover, …) chosen for the BISANTE project. We have chosen to restrict ourselves to one case, namely the GPRS protocol, for the following reasons :

- it is the newer already specified mobile network
- as the standard has not be put into practice yet, there are no models associated
- it will be introduced within the already-existing GSM configuration
- it will integrate mobile & IP networks

This is why the last chapter, although describing modeling techniques that can be applied to other technologies, will be written specifically with the goal of modeling GPRS in mind.

2. WIRELESS LANS

Wireless LANs were originally introduced to solve four nagging problems : mobility, ad hoc networking, relocation, and an alternative to locations that are difficult to wire. A wireless LAN (WLAN) is a flexible data communication system implemented as an extension to, or as an alternative for, a wired LAN within a building or campus. Using electromagnetic waves, WLANs transmit and receive data over the air, minimizing the need for wired connections. Thus WLANs combine data connectivity with user mobility, and, through simplified configuration, enable movable LANs.

Over the last decade, WLANs have gained strong popularity in a number of vertical markets, including the health-care, retail, manufacturing, warehousing and academic arenas. These industries have profited from the productivity gains of using hand-held terminals and notebook computers to transmit real-time information to centralized host for processing. Today, WLANs are becoming more widely recognized as a general-purpose alternative for a broad range of business customers.

What are the applications for Wireless LANs ? With the advent of FDDI and Fast Ethernet, WLANs should not be considered rivals to wired LANs. Rather, WLANs augment wired LANs - providing the final few meters of connectivity between a backbone network and the in-building or a campus mobile user. The widespread strategic reliance on networking among competitive business and the meteoric growth of the Internet and online services are strong testimonies to the benefits of shared data and shared resources. With WLANs, users can access shared information without looking for a place to plug in, and network managers can set up or augment networks without installing or moving wires and cables. Wireless LANs offer the following advantages over traditional wired networks :

- **Improved productivity and service** by allowing people to access shared resources anywhere in their organization

- **Installation speed and simplicity**, as WLAN technology eliminate the need to pull cable through the walls and ceilings

- **Installation flexibility**, as wireless technology allow networks to go where wired networks cannot go

- **Reduced cost-of-ownership** : although the initial investment required for WLAN hardware can be higher than the cost of wired LAN hardware, overall installation expenses and life-cycle costs can be significantly lower.

- **Scalability** : Wireless LANs systems can be configured in a variety of topologies to meet the needs of specific applications and installations. Configurations can be easily changed and ranged from independents network suitable for a small number of users to full infrastructure networks of thousand of users that allow roaming on a large area.

2.1. WLANs : THE 802.11 STANDARD

In 1997, the IEEE released its 802.11 standard covering the field of wireless LANs communications. This standard is designed specifically so that WLANs stay compatible with the 802.3 standard (Ethernet). It consists of three main elements : the physical layer and medium access control specifications, and the power saving functionality.

2.1.1. THE 802.11 PHYSICAL LAYERS

The IEEE 802.11 standard specifies three different physical layers, each applying to a different kind of transmission technology. One layer applies baseband-infrared, the two others apply direct-sequence spread-spectrum, and frequency-hopping spread-spectrum for transmission. All 802.11 devices using one of these three technologies are required to operate at 1 Mbps data rate, with 2 Mbps as an option. the maximal size of a MSDU is 2312 bytes, before the MAC header and the physical preamble are added. There are several physical-layer dependent parameters that are relevant to the design of the MAC protocol. On one hand, there is the Rx/Tx (Receiver/Transmitter) turnaround time, that varies from :

- 0 µs (infrared),
- 10 µs (direct sequence),
- to 19 µs (frequency hopping).

Since this time is contained not only in the length of the interframe spaces but also in the length of the backoff slots in the contention window, it causes significantly different performance of the MAC protocol on top of the 3 physical layers. the backoff slottime for the three layers is defined as :

- 6 µs for infrared
- 20 µs for direct-sequence
- 50 µs for frequency-hopping

For each physical layer also differs the length of the physical preamble added to each packet. Infrared adds 92-112 timeslots of 250 ns + 32 bits, direct sequence 192 bit and frequency hopping 122 bit. This means that the resulting performance will be highly dependent on the type of applied physical media.

2.1.2. THE 802.11 MEDIUM ACCESS CONTROL LAYER (MAC LAYER)

The MAC layer specification for 802.11 has similarities to the 802.3 Ethernet wired line standard (which isn't very surprising, as WLANs are supposed to be compatible with wired Ethernet). The protocol for 802.11 uses a protocol scheme known as Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA).

The major difference with the CMSA/CD (Carrier Sense Multiple Access with Collision Detection) scheme used in 802.3 is that this protocol tries to avoid collisions instead of detecting them once they occurred. This is due to the specific nature of the medium, as it is far more difficult to detect collisions on radio waves than on links.

The MAC layer operates together with the physical layer by sampling the energy over the medium transmitting data. The physical layer uses a clear channel assessment (CCA) algorithm to determine if the channel is clear. This is accomplished by measuring the energy at the antenna and determining the strength of the received signal. If the received signal strength is below a specified threshold, the channel is declared clear and the MAC layer is given the clear channel status for data transmission. If the RF energy is above the threshold, data transmissions are deferred in accordance with the protocol rules. The standard provides another option for CCA that can be alone or with the signal measurement. Carrier sense can be used to determine if the channel is available. This technique is more selective sense since it verifies that the signal is the same carrier type as 802.11 transmitters.

The best method to use depends upon the levels of interference in the operating environment. The CSMA/CA protocol allows for options that can minimize collisions by using request to send (RTS), clear-to-send (CTS), data and acknowledge (ACK) transmission frames, in a sequential fashion. Communications is established when one of the wireless nodes sends a short message RTS frame. The RTS frame includes the destination and the length of message. The message duration is known as the network allocation vector (NAV). The NAV alerts all others in the medium, to back off for the duration of the transmission. The receiving station issues a CTS frame which echoes the senders address and the NAV. If the CTS frame is not received, it is assumed that a collision occurred and the RTS process starts over. After the data frame is received, an ACK frame is sent back verifying a successful data transmission.

A common limitation with wireless LAN systems is the "hidden node" problem. This can disrupt 40% or more of the communications in a highly loaded LAN environment. It occurs when there is a station in a service set that cannot detect the transmission of another station to detect that the media is busy. In Figure 1 below, stations A and B can communicate. However an obstruction prevents station C from receiving station A and it cannot determine when the channel is busy. Therefore both stations A and C could try to transmit at the same time to station B. The use of RTS, CTS, Data and ACK sequences helps to prevent the disruptions caused by this problem.

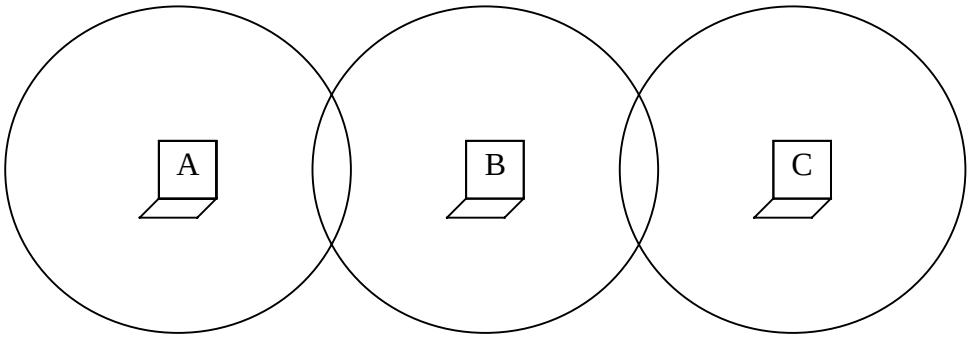

Figure 1 : Hidden Node Problem

Power management is supported at the MAC level for those applications requiring mobility under battery operation. Provisions are made in the protocol for the portable stations to go to low power "sleep" mode during a time interval defined by the base station.

2.1.3. WLANS TECHNOLOGIES

There are mainly three popular (and technically effective) technologies for WLAN; those are spread spectrum, infrared and microwave.

2.1.3.1.SPREAD SPECTRUM LANS

The most popular WLAN technology is spread spectrum radio. First commercially used in the mid-1980s, spread spectrum radio is highly secure, can operate under intense frequency jamming and provides good signal integrity. The name spread spectrum comes from the technique used which ‘’spreads’’ a signal over a portion of the radio spectrum. Therefore, it avoids concentrating power in a single narrow frequency band.

Spread spectrum has been assigned the so-called ISM (Industrial, Scientific, and Medical) bands of the electromagnetic spectrum. These bands regroup :

- 902 to 928 MHz
- 2.4 to 2.484 GHz

Spread spectrum is based on a digital coding technique in which the signal is ‘’spread’’ so that it sounds like noise, making interception difficult. The coding technique for its part permits the increase the number of bits transmitted and the expanse of the bandwidth used. Of course, the receiver must use the same spreading code as the sender to be able to correlate and reassemble all the data received into the original message.

With this spread of the signal’s power over a wide band of frequencies, not only is the signal more difficult to intercept, but it is also more resistant to electromagnetic interferences as well. Those noises include :

- **Interference** : disruption by external sources, such as the electromagnetic emissions of electronic devices, or internal sources (such as crosstalk)

- **Jamming** : disruption caused by a stronger signal, which overwhelms the weaker signal

- **Multipath** : the message is reflected by solid objects, which causes a distortion in the signal

- **Interception** : unauthorized users capture the signal in order to determine its contents

By assigning users different channels, restricting the signals to certain bandwidth limits, and limiting the modulation power used for transmitting, spread spectrum manages to avoid crosstalks for a large part - thus increasing overall transmission rate. Current spread spectrum LANs allow rates up to 6 Mbps.

Spread spectrum technology can be further divided into two subcases : Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS).

- **Direct Sequence Spread Spectrum (DSSS)**

DSSS avoids excessive power concentration by spreading the signal over a wider frequency band. Each bit of data is mapped into a pattern of ‘’chips’’ by the transmitter. The higher modulation rate is achieved by multiplying the digital signal with a chip sequence. The ratio of chips per bit is called the "spreading ratio". A high spreading ratio increases the resistance of the signal to interference. A low spreading ratio increases the net bandwidth available to a user. The rationale behind this technique is to realize that two different signals spread-coded each one with its unique spread code cannot have the same spectral characteristics. At the destination the chips are mapped back into a bit, recreating the original data. Transmitter and receiver must be synchronized to operate properly.

This particular kind of spread spectrum enables to build and operate several networks in the same location. By assigning a unique spreading code, all transmissions can use the same frequency band without interfering with each other. All signals that do not share the same spreading code as one particular signal will look like noise for it and will be filtered out.

As this spreading process lowers the signal’s power on each frequency, it may be assumed that it creates unreliable transmissions, as the signals would be more susceptible to electromagnetic noise. However, the processing gain of the despreading correlator recovers the loss in power when the signal is collapsed back down to the original data bandwidth.

In practice, DSSS spreading ratios are quite small. Virtually all manufacturers of 2.4 GHz products offer a spreading ratio of less than 20. The proposed IEEE 802.11 standard specifies a spreading ratio of 11. The FCC (Federal Communications Commission) requires that the spreading ratio must be greater than 10.

Several DSSS products in the market allow users to deploy more than one channel in the same area. They accomplish this by separating the 2.4 GHz band into several sub-bands, each of which contains an independent DSSS network (as explained above). Because DSSS truly spreads across the spectrum, the number of independent (i.e. non-overlapping) channels in the 2.4 GHz band is small. The maximum number of independent channels for any DSSS implementation on the market is three.

Generally, DSSS provides very good security and immunity to interference, and a transfer rate of around 2 Mbps in the 2.4 GHz ISM band. This can be increased for DSSS allows to ‘’stack’’ the cells on top of each other, thus netting the user a 6 Mbps data transfer ratio.

- **Frequency Hopping Spread Spectrum (FHSS) :**

FHSS spreads the signal by transmitting a short burst on one frequency, "hopping" to another frequency for another short burst and so on. The source and destination of a transmission must be synchronized so they are on the same frequency at the same time.

The hopping pattern (frequencies and order in which they are used) and dwell time (time at each frequency) are determined in accordance with a pseudo-random code sequence. They are restricted by most regulatory agencies. For example, the FCC requires that 75 or more frequencies be used and a maximum dwell time of 400 ms. If interference occurs on one frequency, then the data is retransmitted on a subsequent hop on another frequency.

All FHSS products on the market allow users to deploy more than one channel in the same area. They accomplish this by implementing separate channels on different, orthogonal, hopping sequences. Because there are a large number of possible sequences in the 2.4 GHz band, FHSS allows many non-overlapping channels to be deployed.

FHSS devices offer in comparison to DSSS a reduced range and a reduced data transfer rate of 1 Mbps, but they are cheaper and offer better noise-immunity characteristics.

2.1.3.2.INFRARED LANS

Infrared LANs (or IR LANs) use the wavelength band between 780 and 950 nm (nano-meters), which puts them between visible spectrum and microwaves (hence the 'infrared' name). This is due to the availability of cheap , reliable system components working for this band. The infrared signal from a compatible device goes to an access point where the infrared signal is translated into appropriate electrical signal.

There are two conventional ways to set up an IR LAN :

- the infrared transmissions can be **aimed** (directed IR LANs). This gives a good range of a couple of kilometer and can be used outdoors. It also offers the highest bandwidth and throughput.

- the other way is to transmit **omni-directionally** (non-directed IR LANs) and bounce the signals off of everything in every direction. Using this technique implies a loss of energy, which reduces coverage to 30 - 60 feet and the data rates as well, but it is an *area* coverage, which means that this system is generally more robust than directed IR LANs (because it is difficult to block all the light reflected from large surface areas).

These systems are not bandwidth limited and thus can achieve transmission speeds greater than the other systems. Infrared transmission operates in the light spectrum and does not require a license to operate, another attractive feature. IR LANs offer more resistance to electromagnetic noise than spread spectrum, which makes them admirably suited for use in very noisy environments (such as factory buildings).

However, IR LAN systems suffer from a number of drawbacks :

- the transmission spectrum is shared with the sun and other things such as fluorescent lights. If there is enough interference from other sources it can render the LAN useless (though using directional transceivers with special filters can offset this problem).

- IR systems require an unobstructed line of sight (LOS).

- IR signals cannot penetrate opaque objects. This means that walls, dividers, curtains, or even fog can obstruct the signal.

Current implementations of IR LANs yield performances that can match (or even exceed in some cases) the data rate of wired-based LANs, as transmission systems allowing 50 Mbps or

100 Mbps have already been demonstrated in controlled environments. However, for most applications in general conditions, slower data transfers are used.

The IrDA (Infrared Data Association) , which is an industry consortium developing infrared products for computer connectivity, has identified mainly three different data transmission rates : 115 Kbps, 1.15 Mbps and 4 Mbps.

2.1.3.3.MICROWAVE LANS

A microwave is a short radio wave that varies from 1 millimeter to 30 centimeters in length. Microwaves enjoy the possibility to pass through the ionosphere (which is not the case for longer radio waves that are either blocked or reflected). This makes them all the more suitable for long-range applications, as it allows them to communicate with satellites.

Two microwave configurations dominate the field today :

- **point-to-point** : those systems are designed for low and medium density communications.

- **point-to-multipoint** : those systems provide communications between a central node and remote data units. They provide backbone links, enabling less populated areas to be covered on a more economical basis.

They usually operate at less than 500 mW of power. They use narrow-band transmissions with single-frequency modulation and are set up mostly in the 5.8 GHz band. The big advantage to MW systems is higher throughput achieved because they do not have the overhead involved with spread spectrum systems.

Most frequently, the vendors of such microwave systems have to obtain a license for use of the channels in their frequency spectrum. Although this explains why microwave LANs are easily the most expensive WLANs on the market, it does make them almost interference-free, as only the licensed company has the right to use this frequency, thus eliminating all outside noise.

Please, note that the 802.11 standard does not cover this technology in its original form. Plans however are made to remedy to this.

2.2. ETSI RES 10 : HIPERLAN

2.2.1. HIPERLAN : A QUICK PRESENTATION

As we saw in the former section, ‘’classical WLANs’’ are usually restricted to data speeds of 6 Mbps or slower. This is far below the capacities of nowadays wired networks (with FDDI at 100 Mbps, and Ethernet coming now at 100 Mbps and even 1 Gbps), and, even if one considers that WLANs are not a concurrent to wired LANs but more a partner, it is definitely a drawback. However, there are so many advantages in wireless technology that constructors did not want to drop it, so they went on refining it to allow better capabilities. More

particularly, the ETSI (European Telecommunications Standard Institute) has set up in mid-1991 a new workgroup to look at it (identified as RES 10) to develop a standard that would be equal in performance to wired LANs such as Ethernet.

CEPT identified vacant spectrum at the 5 Ghz band. Prior, the 5.00-5.25 Ghz band was allocated worldwide to aviation authorities, but only the 5.00-5.15 Ghz spectrum was used. CEPT then allocated the remaining band, 5.15-5.25 Ghz, to HiperLAN on a secondary basis with its status as non-interference, non-protected band. Also, an extension from 5.25-5.3 Ghz is available in most countries.

The requirements of the standard are as follows :

- HiperLAN is rather short-ranged, with 50 meters at most
- designed to work with and without infrastructure (i.e. two stations can communicate directly if needed)
- it allows for low mobility, with a user's speed of 1.4 m/s at most
- it supports isochronous traffic : audio traffic, at 32 Kbps with a 10 ns latency, and video traffic, at 2 Mbps with a 100 ns latency
- it supports asynchronous traffic : data traffic, at 10 Mbps, with immediate access

2.2.2. THE LAYERED ARCHITECTURE OF HIPERLAN

The HiperLAN project has defined a system architecture as shown below (Figures 2 and 3). On top of the physical layer specification a separate sublayer has been integrated, containing the channel access mechanism. this mechanism is used by the different functional entities, offering different services.

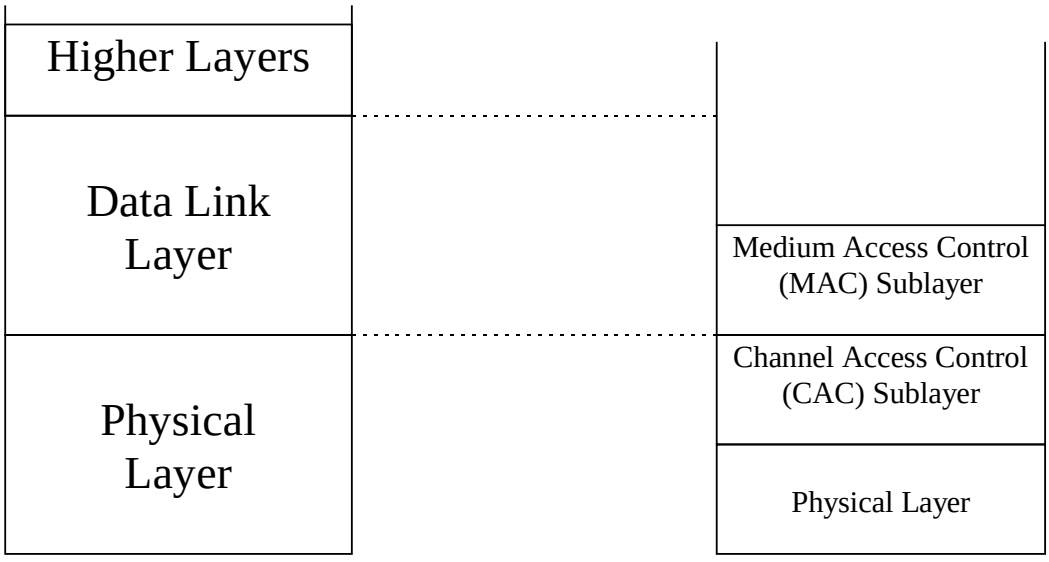

Figure 2 : Correspondence between the OSI and the HiperLAN Reference Models

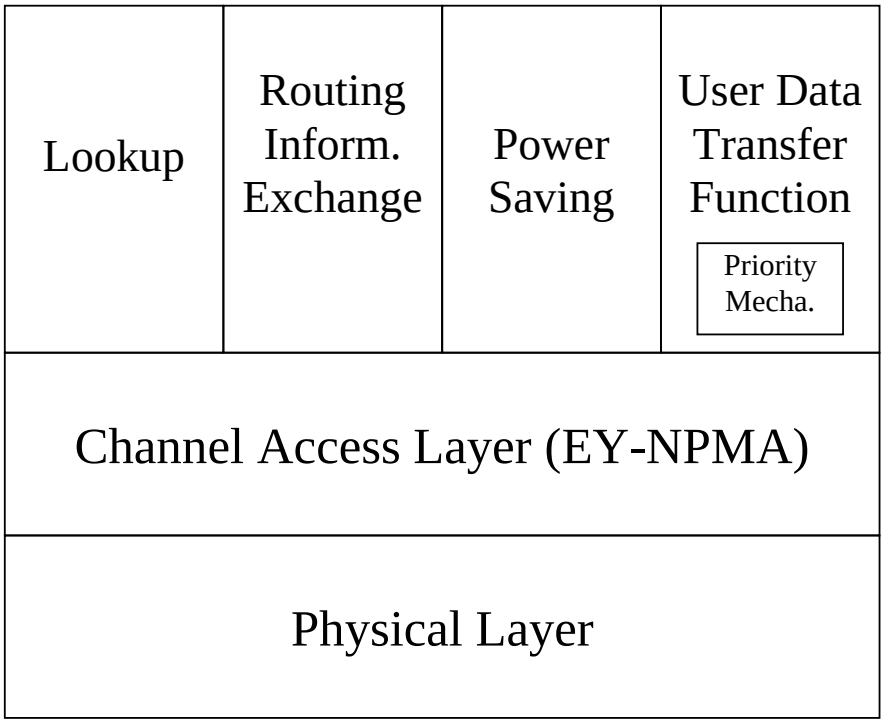

Figure 3 : Layer Architecture of the HiperLAN Reference Model

In order to be able to support forwarding of packets to stations outside of radio range of the sender with the help of supporting stations (i.e. forwarders), a routing information exchange functionality is present. A lookup functionality is added to enable collocated operation of distinct WLANs. Optional encryption/decryption may be used, but the mechanisms applied are not specified. 2 MAC-user priority classes are supported, that are mapped onto 5 channel priorities.

2.2.2.1.PHYSICAL LAYER

The physical layer allows a HiperLAN to select one of five independent channels within the allocated bandwidth. While channel one to three are license-free in any country, channel four and five are not globally available. The selection of a new channel and the changing of the carrier must not take more than 1 ms. The channel transmits data at two different data rates :

- a low data rate (1, 4706 Mbps) that is used to transmit acknowledgment packets and the packet header
- a high data rate (23, 5294 Mbps) to transmit the data packet itself.

As said above, it uses 5 channels sprayed along the 5.15-5.30 Ghz band. The Rx/Tx (Receiver/Transmitter) turnaround time is limited to < 5 μs. The physical layer adds to the MPDU the low rate header, 450 high rate bits for synchronization and training sequence and a variable number of bits for padding.

2.2.2.2.HIPERLAN LOOKUP

The HiperLAN look-up functionality is defined to explore the HiperLAN communication environment. The function allows to retrieve the HiperLAN identifier for a specific HiperLAN which is known by name. A new HiperLAN can be created by choosing a HiperLAN identifier which is not in current use in the communication environment. An already existing HiperLAN can be joined by just using its identifier. A HiperLAN is left by stop using its identifier. A HiperLAN is destroyed when no more entity uses its identifier.

2.2.2.3.PRIORITY CLASSES

Although the HiperLAN draft standard does not define different priority classes for the various traffic classes like multimedia or file transfer, it supports time bounded delivery of packets. this task is performed by assigning channel access priorities dynamically to the packets. The channel access priority depends on the normalized residual MSDU lifetime (or NRMT) and the user-assigned priority. the MAC-layer has to assign a lifetime to every data packet. The NRMT is the ratio of residual lifetime and the distance between source and destination (measured in hops). Thus the priority of each packet increases while its lifetime expires. In each access cycle, only packets with the same access priority compete for the channel since the access mechanism guarantees hierarchical independence of performance between packets with different channel access priorities. The table below shows how the access priority is defined.

NRMT (ms)	High User Defined Priority	Low User Defined Priority
< 10	0 (highest)	1
10 < NRMT < 20	1	2
20 < NRMT < 40	2	3
40 < NRMT < 80	3	4 (lowest)
> 80	4 (lowest)	4 (lowest)

Table 1 : Access Priority Classes

2.2.2.4.POWER SAVING

The HiperLAN draft standard supports power saving in two ways. First of all, the low rate header of each packet allows the receiver to determine whether it is the destination for the packet or not without using the equalizer. Thus, the equalizer is only used when necessary. Secondly, a node can save power by receiving packets only at prearranged moments instead of continuously. HiperLAN power concentration is achieved by an implicit bilateral agreement between a node conserving power (p-saver) and a node deferring transmissions (p-supporter). This agreement is defined by the declaration and transmission of active wake patterns.

2.2.2.5.HIPERLAN ACCESS MECHANISM

EY - NPMA (Elimination Yield - Non-preemptive Priority Multiple Access) is the preferred MAC protocol of HiperLAN. If offers a mechanism that requires a minimal number of Rx/Tx-turnarounds, while still resulting in a single winning station with high probability (97.8%). Features of this access scheme are :

- No preemption by frames with higher priority after the priority resolution possible
- Hierarchical independence of performance
- Fair contention resolution of frames with the same priority

The access mechanism is split into 3 phases : **Priority Resolution**, **Elimination** and **Yield** phases.

In the first phase, a station seeking access to the media transmits a burst for Priority Assertion Period (PAD) in the fitting priority slot (the Priority Detection period is divided in slots according to the number of priorities). If the channel was idle for p-1 priority slots, everybody else stands back from transmission. At least one station survives this phase.

In the second phase, every surviving station transmits bursts (Elimination Period - EP) and, after this, listens to the channel for an Elimination Survival Verification Period (ESVP). The burst length is individual for every station, bounded and defined by a certain discrete probability distribution. If a station sends a signal in the ESVP, then it stands back from transmission. At least one station survives after this phase.

In the yield phase, every surviving station listens to the channel (Yield Period - YP). The YP length is individual for every station (again bounded by a discrete probability distribution). If a station hears a signal, it stands back from transmission, else it transmits immediately the data frame after the yield period.

3. SECOND GENERATION MOBILE SYSTEMS

In this chapter, we will have a look at the most widely used networks in the field of mobile communications nowadays.

3.1. DECT

The DECT standard was initially conceived in the mid-1980s as a pan-European standard for domestic cordless phones. The objective of the new standard, proposed by CEPT (the Council of European PTTs), was to use digital radio technology to improve the performance of cordless phones in three important areas - speech quality, security against eavesdropping, and immunity from radio interference between nearby cordless phones.

By the time the DECT standard was finalized in 1992, and published by ETSI (European Telecommunications Standards Institute, the successor to CEPT), the scope of the standard had broadened beyond domestic cordless phones to include two additional application areas. One was business cordless telephones (the so-called cordless PBX or wireless PBX) and the other was as a cordless access system for subscribers to public telecom networks.

The DECT common interface standard has a layered structure and is contained in ETS 300 175, Parts 1 to 8. It is a comprehensive set of requirements, protocols and messages providing implementers with the ability to create network access profiles (protocol subsets) to be able to access virtually any type of telecommunications network.

Since 1993, DECT has been a mandatory standard throughout the European Union. Member countries have set aside radio frequencies in the 1.88-1.9GHz for DECT systems. The DECT standard has also been adopted for use in countries outside the EU. The latest information is that DECT is regarded as a standard in 26 countries, making it the most widely-used digital standard for cordless communications.

For this reason, the name of the DECT standard has been revised. In the original form, the letter 'E' stood for 'European'. Now, it denotes 'Enhanced'. So, today, DECT means ‘Digital Enhanced Cordless Telecommunications.’

3.1.1. CHARACTERISTICS

DECT is a digital radio access standard for single- and multiple-cell cordless communications. It is based on a multi-carrier TDMA (time division multiple access) technology. This is the same technology used in the main digital cellular standards, but the central difference is that cellular systems were developed for wide-area coverage, whereas the DECT standard was optimized for local coverage, with high densities of users. TDMA will be further described below

The standard specifies four layers of connectivity, plus other important functions. The four layers correspond approximately to layers 1-3 of the ISO Open Systems Interconnection (OSI) model, as follows:

1. Physical layer: Radio parameters such as frequency, timing and power values, bit and slot synchronization, and transmitter and receiver performance.

2. Medium Access Control layer: The establishment and release of connections between portable and fixed parts of the DECT system.

3. Data Link Control layer: Provides very reliable data links to the Network layer, for signaling, speech transmission, and circuit- and packet-switched data transmission.

4. Network layer: The main signaling layer, specifying message exchanges required for the establishment, maintenance and release of calls between portable and fixed elements of the network.

5. Other elements of the DECT standard cover equipment identities and addressing, security authentication procedures, speech coding and transmission, Public Access Profile and cryptographic algorithms.

The description of one particular function is described in a particular part of the DECT standard. Relationships between functionalities and parts are given in the table below :

Part	**Title**	**Description**
1	Overview	General introduction to the other parts of ETS 300 175
2	Physical Layer	Radio requirements of DECT, e.g. carrier frequency allocation, modulation method, transmission frame structure, transmitted power limits, spurious emission requirements, …
3	Medium Access Control layer	Description of procedures, messages, and protocols for radio resource management i.e. link set-up, channel selection, handover, link release and link quality maintenance, …
4	Data Link Control layer	Description of provisions to secure a reliable data link to the network layer
5	Network layer	Description of the signaling layer with call control and mobility management functions and protocols.
6	Identities and Addressing	Description of the portable and fixed part identities requirements for all DECT application environments.
7	Security aspects	Procedures to prevent eavesdropping, unauthorized access and fraudulent use.
8	Telephony	Telephony requirements for systems supporting the 3.1 kHz speech service to ensure proper interworking with public telecommunications networks. De-fines transmission levels, loudness ratings, sidetone levels, frequency response, echo control requirements etc.

Table 2 : DECT Functions Description

3.1.2. THE MC/TDMA/TDD PRINCIPLE

The DECT radio interface is based on the Multi Carrier, Time Division Multiple Access, Time Division Duplex (MC/TDMA/TDD) radio access methodology. Basic DECT frequency allocation uses 10 carrier frequencies (MC) in the 1880 to 1900 MHz range. The time spectrum for DECT is subdivided into timeframes repeating every 10 ms. Each frame consists of 24 timeslots each individually accessible (TDMA) that may be used for either transmission or reception. For the basic DECT speech service two timeslots - with 5 ms separation - are paired to provide bearer capacity for typically 32 Kbit/s (ADPCM G.726 coded speech) full duplex connections. To simplify implementations for basic DECT the 10 ms timeframe has been split in two halves (TDD); where the first 12 timeslots are used for FP transmissions (downlink) and the other 12 are used for PP transmissions (uplink). The TDMA structure allows up to 12 simultaneous basic DECT (full duplex) voice connections per transceiver providing a significant cost benefit when compared with technologies that can have only one link per transceiver (e.g. CT2). Due to the advanced radio protocol, DECT is able to offer widely varying bandwidths by combining multiple channels into a single bearer. For data transmission purposes error protected net throughput rates of n x 24 Kbit/s can be achieved, up to a maximum of 552 Kbit/s with full security as applied by the basic DECT standard.

The three **applications** for the DECT standard that have reached widespread commercial deployment so far are for home cordless phones, business cordless systems, and as a radio alternative to wired subscriber accesses in public fixed telecom networks, known as Wireless Local Loop (WLL).

- In a DECT home cordless phone, a typical DECT system consists of a phone handset and a base unit that contains the radio base station.

- In a DECT business cordless system, the core radio network is a number of radio base stations, all connected to a PBX through a radio exchange. A DECT business cordless system has an architecture that is similar in concept to a cellular mobile phone system, with a network of radio base stations so that users can walk around the premises, making and receiving calls. The cells in a DECT business cordless system are much smaller (pico-cells) than are used in a cellular network, which allow much higher user densities. DECT permits the highest user densities of any cordless system, up to 100,000 per square kilometer.

- In a DECT WLL system, the radio base station is located somewhere in the neighborhood, and each subscriber is equipped with a DECT transceiver unit into which a standard telephone can be plugged. Group 3 fax machines and data modems can also be used. A further development of this public network access concept is to equip subscribers with DECT digital cordless phones, to provide a limited degree of mobility in a local area. This solution is termed Cordless Terminal Mobility (CTM).

3.1.3. DECT STRENGTHS

- **High capacity**: The digital TDMA radio technology used in the DECT standard, with its low radio interference characteristics, allows business cordless systems to handle up to

100,000 users per square kilometer. This allows even the most densely-occupied office buildings and similar locations to be served.

- **High speech quality**: Speech is digitally encoded before transmission, using 32 Kbit/s ADPCM (Adaptive Differential Pulse Code Modulation) speech encoding. The resulting speech quality is as good as with an ordinary wired phone.

- **High security**: The DECT standard uses encryption techniques so that radio eavesdropping is virtually impossible.

- **Long battery life**: The radio technology uses discontinuous transmission, occupying only two out of the 16 timeslots, which reduces the load on the battery in the cordless phone. Standby and talk times of 45 hours and nine hours are commonly available in the latest DECT cordless phones.

- **Seamless handover of calls**: In a DECT business cordless system, as the user moves around from one pico-cell to another during a call, it is the phone rather than the radio network that initiates handover from cell to cell. A 'make-before-break' handover principle ensures that the handover is undetectable to the user.

- **Data as well as voice**: The DECT standard permits cordless data communications as well as voice, creating the possibility of cordless LANs (Local Area Networks) which could share capacity with cordless telephone systems.

- **Profiles for interworking**: Another feature of the DECT standard is that it has been developed with a number of different interconnection profiles so that a DECT system can be linked to other networks including GSM digital cellular networks, to provide integrated communications mobility.

- One of the most important profiles is the **GAP** (Generic Access Profile), which ensures that all DECT products from different manufacturers will be compatible. This promotes competition, and provides users with a wider range of DECT products to choose from.

3.2. GSM

GSM is the name of the European digital mobile telephone network. The first steps were done in 1982, when CEPT (Conference Europeenne des Administrations des Postes et des Telecommunications) founded the Groupe Special Mobile which initially gave GSM its name. After the foundation of the European standardization institute ETSI (European Telecommunication Standards Institute), GSM became an ETSI Technical Committee and was renamed to Global System for Mobile Communication, keeping GSM as its acronym. The standard drafted by GSM consists of about 130 single documents with over 5000 pages. The official start of GSM was in 1992, in late 1993 there were already more than one Million GSM subscribers, over 80% of then in Germany alone. Since then, more than 200 networks run GSM in over 100 countries , serving around 50 Million subscribers. The frequency bands used lie around 900, 1800 and 1900 MHz.

3.2.1. SYSTEM ARCHITECTURE

A GSM Public Land Mobile Network (PMLN) is cell based, i.e. the area covered by a cell phone company is divided into hexagons. In the middle of each hexagon, a Base Transceiver Station (BTS) serves all Mobile Stations (MS) that are currently inside this cell. Cells are further grouped into clusters of k (3,4,7) cells.

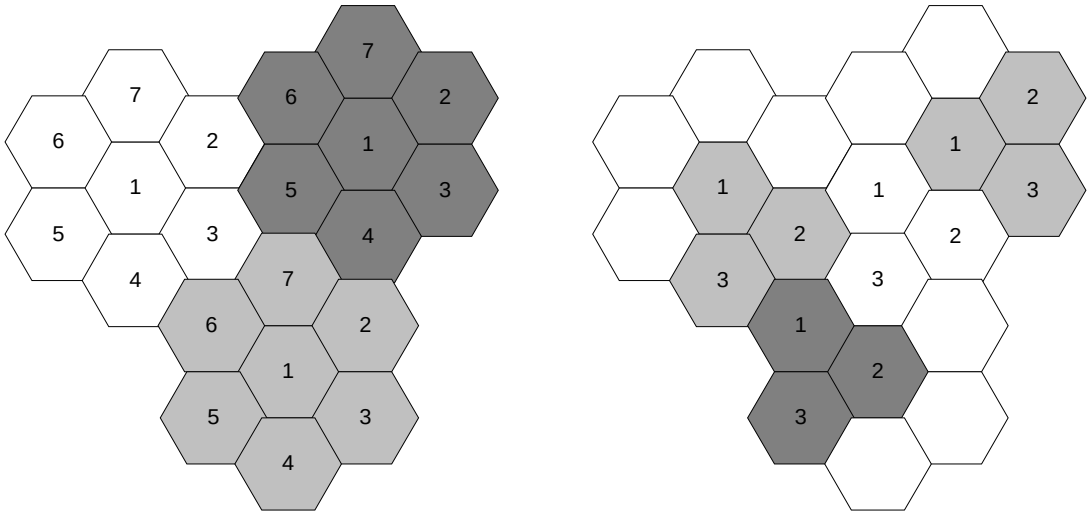

Figure 4 : Cells covering hexagonal areas.

In reality, cells are less likely to be of hexagon shape with exact the same size. Instead, cells will be of different sizes, smaller ones covering areas with high population density (cities), while larger ones will cover low density areas.

GSM can be divided into 3 subsystems:
1. Base Station Subsystem (BSS)
2. Network and Switching Subsystem (NSS)
3. Operation Subsystem (OSS)

The subsystems can be seen in the next figure:

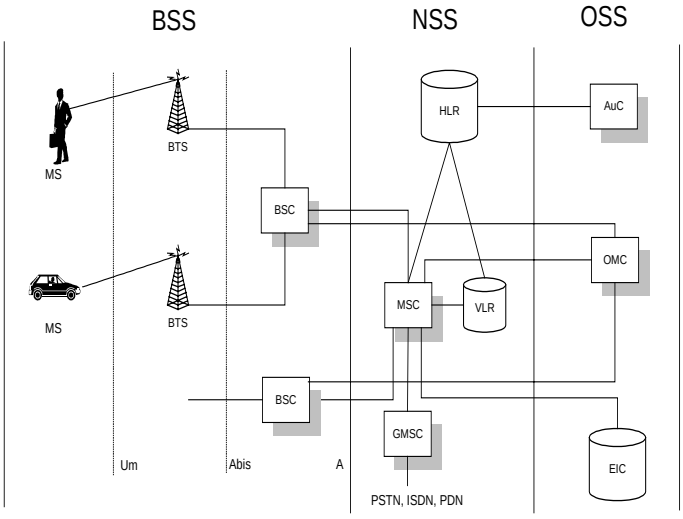

Figure 5 : GSM subsystems.

3.2.1.1.BASE STATION SUBSYSTEM (BSS)

Contains the radio components like Mobile Stations (MS), Base Transceiver Stations (BTS) and Base Station Controllers (BSC). Mobile stations can be cell phones and car phones, being installed at a fixed location and communicating always with the same BTS or travelling around and contacting a sequence of BTSs. BTS are little more than intelligent antennas that use error prediction and correction methods to insure reliable data connections. To make BTS as simple as possible, most of the protocol logic is put into BSCs, which serve several BTS. Here, more complex protocols like handovers from one cell to another, as well as frequency assignments are implemented. Mobile stations use radio links to talk to the BTS they are currently assigned to. From the BTS on, conventional terrestrial networks take over and route the data to their destination.

3.2.1.2.NETWORK AND SWITCHING SUBSYSTEM (NSS)

This subsystem is connects mobile stations to other mobile stations of the same network, as well as to other networks such as public phone networks (PSTN, ISDN, PDN, ...).

In this subsystem, Mobile Services Switching Centers (MSC) denote high performance ISDN switches, controlling several BSCs. MSCs create, maintain and delete connections via the Signaling System 7. They also control handovers between BSCs and MSCs. Furthermore, MSCs control supplementary services as known from ISDNs like conference calls, blocking certain numbers and so on. MSCs thus control a local area containing a certain number of BSCs. Beside its functions controlling BSC, BTS and MS, an MSC is also a full ISDN switching node. A GMSC a special MSC, connecting the PLMN with other networks (PSTN, ISDN, PDN, ...).
The Home Location Register (HLR) is a database storing all members of one cell phone company together with their ISDN phone number. Additionally, the HLR stores temporary data about these members, such as the current area they are in (their MS is in). The HLR is a central repository and has no direct control over MSCs.

With each MSC, one Visited Location Register (VLR) is associated. In this database, data about the MS that are currently inside the area covered by the MSC is stored. If a MS leaves this area, the data is removed from the VLR.

3.2.1.3.OPERATION SUBSYSTEM (OSS)

This subsystem is responsible for subscription management, network operation, maintenance and mobile equipment management, billing and so on.. The Operation and Maintenance Center (OMC) controls all network elements and guarantees best possible services. It is based on the Telecommunications Management Network (TMN), a hierarchical set of services developed by the ITU-T. The OMC manages subscribers, billing, controls the state of all network elements and creates statistical reports about the observed traffic.

The Authentication Center (AuC) contains all information necessary to safe data sent over the radio channels. Here, cryptographic keys and algorithms for authentication are stored.

Finally, the Equipment Identity Register (EIR) stores information of all subscribers and mobile equipment. In this database, three lists (white, black and gray) store identification numbers unique to all mobile terminals. The white list contains allowed terminals, the black contains unallowed terminals (e.g. stolen), and the gray contains with known bugs.

3.2.2. SUBSCRIBER AND EQUIPMENT IDENTIFICATION

In GSM, there is a strong distinction between subscribers (identified by their SIM) and the hardware they use for making phone calls. In order to identify both before and during GSM service allocation, several identification numbers exist and are stored at different locations. The following IDs are stored in the HLR:

1. International Mobile Subscriber Identity (IMSI): Permanent ID assigned to each GSM network subscriber.
2. International Mobile Subscriber ISDN Number (MSISDN): The ISDN number permanently assigned to each GSM subscriber.
3. Mobile Station Roaming Number (MSRN): Temporary ISDN number of a subscriber. This number is assigned by the local VLR each time, the subscriber enters its area. The MSRN is then sent to the HLR and GMSC.
4. The address of current VLR and MSC: Identify the area the subscriber is currently in, if available.
5. Local Mobile Subscriber Identity (if available): A short ID temporarily assigned to an active subscriber by an VLR and sent to the HLR.

The following IDs are stored temporarily at the VLR associated with the MSC that is currently controlling an active MS:

1. IMSI
2. MSISDN
3. MSRN
4. Location Area Identity (LAI): ID the Location Area (LA), where subscriber has connected to network.
5. Temporary Mobile Subscriber Identity (TMSI): Temporarily assigned to active MS in order to prevent the IMSI from being transmitted too often over radio. The TMSI is periodically changed during a call.

3.2.3. GSM SERVICES

Like in ISDN, there are three classes of services available in GSM:

- **Bearer Services**: Lower level services that enable the creation of reliable data transport connections. Bearer Services are used by higher levels for data transport. Transparent services (T) denote constant bitrate transport with changing bit error probabilities (Section 3.2.7.2). Non-transparent services (NT) activate additionally a special protocol (Radio Link Protocol, RLP) between MS and MSC that resend blocks with observed errors (Section 3.2.7.3).

Service	Structure	BS Nr.	Bitrate	Mode
Data	Asynchronous	21	300	T or NT
		22	1200	T or NT
		23	1200/75	T or NT
		24	2400	T or NT
		25	4800	T or NT
		26	9600	T or NT
Data	Synchronous	31	1200	T
		32	2400	T or NT
		33	4800	T or NT
		34	9600	T or NT
PAD	Asynchronous	41	300	T or NT
		42	1200	T or NT
		43	1200/75	T or NT
		44	2400	T or NT
		45	4800	T or NT
		46	9600	T or NT
Packet	Synchronous	51	2400	NT
		52	4800	NT
		53	9600	NT
Alternating Voice/Data		61	1300 or 9600	
Voice followed by Data		81	1300 or 9600	

Table 3 : Bearer Services

- **Teleservices**: Teleservices are well defined services within GSM and use bearer services for transport. They include services like voice, SMS and Message Handling Systems (MHS).

Category	TS Nr.	Service	Class
Voice	11	Phone	E1
	12	Emetgency	E1
Short Messages Services	21	Short Message Mobile Terminated, Point to Point	E3
	22	Short Message Mobile Originated, Point to Point	A
	23	Short Message Cell Broadcast	-
MHS access	31	Access to message handling systems	A
Videotext	41	Videotext Profile 1	A
	42	Videotext Profile 2	A
	43	Videotext Profile 3	A
Teletext	51	Teletext	A
Fax	61	Voice and Fax Group 3 alternating T/NT	E2/A

	62	Fax Group 3 T/NT	-

Table 4 : Teleservices

- **Supplementary services**: Supplementary services are defined similar to ISDN and are always associated with bearer services or teleservices by altering them or adding new functionality. Amongst them are, for instance, call forwarding and call restriction.

Category	Short Name	Service	Class
Call Offering	CFU	Call Forwarding Unconditional	E1
	CFB	Call Forwarding on Mobile Subscriber Busy	E1
	CFNRy	Call Forwarding on No Reply	E1
	CFNRc	Call Forwarding on Mobile Subscriber Not Reachable	E1
Call Restriction	BAOC	Barring of All Outgoing Calls	E1
	BOIC	Barring of Outgoing International Calls	E1
	BAIC	Barring of All Incoming Calls	E1
	BOIC-exHC	Barring of Outgoing International Calls except those to Home PLMN	A
	BIC-Roam	Barring of Incoming Calls when Roaming Outside the Home PLMN	A

Table 5 : Supplementary Services

Additionally, GSM defines the above services to be either essential (E) or additional (A). For E-services, three phases have been defined. E1-services must be implemented from 1991 on, E2 from 1994 and E3 from 1996 on. A-services are not compulsory but can be offered by the cell phone company.

3.2.4. RADIO CHANNEL MANAGEMENT (UM INTERFACE)

In this section, the radio channel management of the MS-BTS interface will be described.

The modulation of data to one specific radio frequency is done with the Gauss Minimum Shift Keying method (GMSK). GSM uses both Time Division Multiple Access (TDMA) and Frequency Division Multiple Access (FDMA) to enable the communication of several MS with one BTS.

3.2.4.1.PHYSICAL CHANNELS

For GSM, two bands of 25 MHz width each have been reserved. For sending from MS to BTS (Uplink), the band from 890 MHz to 915 MHz was defined, for sending data from BTS to MS (Downlink), the band from 935 MHz to 960 MHz was defined. Frequency multiplexing is done by dividing the available frequency bands into 124 FDM-channels, each being separated from its neighbors by a security strip of 200 kHz.

Each MS and BTS then may send data on one of these FDM-channels. To allow more than 124 MS per cell, each FDM-channel is then subdivided into 8 time slots and each MS is assigned one of these time slots for sending and receiving (TDMA).

Finally, to allow more than 124x8 senders in the GSM network, frequencies are reassigned, if there is enough distance between two senders. This is done in the following way: Each BTS is assigned a subset of the available 124 frequencies. No BTS in the same cluster (see Section 3.2.1) is assigned one of these frequencies. If there is one cell in one of the neighboring clusters that is sufficiently far apart, the frequencies may be reassigned.

Though both Uplink and Downlink use 8 time slots, there is a difference of 3 time slots between an Uplink time slot and a Downlink time slot with the same number. This allows MS to avoid duplex hardware for their antenna system.

For instance, a certain BTS may use channels 2 to 60. A contacting MS wishing to establish a call is assigned the second time slot in channel 4. Uplink data then will be sent in the second time slot on frequency 890.2 + 0.2 x (4-1) = 890.8 MHz. Downlink data will be sent in the second time slot on frequency 935.2 + 0.2 x (4-1) = 935.8 MHz. The difference of these frequencies will always be 45 MHz.

As certain frequencies and time slots are sometimes likely to produce series of errors, each BTS may additionally enable frequency hopping, thus reassigning a new FDM-channel to each MS for each new time slot. Errors will then be at the same (low) level for all MS at the same BTS.

In each time slot, data is transported in a burst. There are five different burst types:

1. Normal Burst (NB): In these bursts, normal traffic data and control information is transported.
2. Frequency Correction Burst (FB): This burst is used to synchronize frequencies.
3. Synchronization Burst (SB): This is done for time synchronization of MS with their BTS.
4. Dummy Burst (DB): This burst is sent from each BTS on a special FDM-channel (BCCH), in case no other information needs to be sent.
5. Access Burst (AB): Burst for random access on the RACH.

In order to guard bursts from their neighbors, additional guard times are added before and after each burst. 8 time slots are then collected into one TDMA-frame.

3.2.4.2.LOGICAL CHANNELS

The above described methods insure two physical channels between each MS and its BTS (Uplink and Downlink). In order to separate traffic/voice data from control information, the available time slots of each MS are further subdivided into logical channels. There is a large

number of logical channels, and rules exist that specify which logical channels can be open at the same time. Logical channels are grouped into two groups:

1. Traffic Channel (TCH) or mobile B-channel (Bm-channel): on this channel, user data like voice, data and fax is transported. The TCH can transport connection-oriented or packet-switched traffic.
2. Signaling channels or mobile D-channels (Dm-channels): these channels carry signaling information to establish, control and tear down connections.

The Bm-channels can further be subdivided into

1. Broadcast Channel: These are unidirectional, downlink only channels broadcasting information to all MS in the same cell.
2. Common Control Channel (CCCH): Unidirectional, up- or downlink, for channel access management like assigning channels to MS.
3. Dedicated Control Channel (DCCH): Bidirectional channel established either with an open traffic channel or as stand alone if requested by an MS.

Mapping logical channels to physical channels is done by first grouping either 26 or 51 TDMA-frames into 26-frame or 51-frame multiframes. One superframe then consists of 26 51-frame or 51 26-frame multiframes. Finally, a hyperframe consists of 2028 superframes. Within the GSM standard, rules then define, which time slots may be used for which logical channel within one 26-frame or 51-frame multiframe in a cyclic fashion.

3.2.5. GSM HANDOVER

One of the most important features of a cell-based mobile phone system is its ability to handover MS from one BTS to another, in case the MS leaves the BTS cell. This is done in four steps:

1. As the location of the MS can only be estimated within +-1000m due to a large error in the round-trip-delay, the *quality* of the connection to the current BTS and to its immediate neighbors is constantly measured (quality monitoring). The data is sent to the BSC.
2. If this quality drops below a certain margin, the BTS and MS will increase their field strength in steps of 2 dBm.
3. If the maximum field strength is reached and still the measured connection quality is below a certain level, whereas the there is a much better connection to one of the neighbors, the BSC sends a handover request to its MSC.
4. The MSC decides, whether the handover is carried out.
5. If a positive decision has been made, the MSC handles the handover and updates its VLR.

Measuring the connection quality is done twofold: First, the field strength of each downlink burst of the current BTS is measured by the MS. The average of 100 such bursts is then

computed and stored as the current RXLEV. Additionally, the MS measures the field strength of the logical channel BACCH of each of the BTS neighbors. This is done in the intervals between uplink and downlink communication with the current BTS. Secondly, the MS measures the channel quality of the traffic channel (logical channel TCH), which contains a set of fixed training bits. The parameter RXQUAL denotes the mean bit error in this sequence prior to error correction.

The current RXLEV, the best 6 neighbor RXLEVs and RXQUAL are then put into a Measurement Report and sent to the BSC.

Before generating a handover request, the following must be considered:

- Measurements must be averages over a minimum period of time. This inhibits handovers due to short term quality drops.
- Before generating a handover request, the BTS and MS have to increase their field strength.
- The BTS with best connection must be chosen as the new BTS.

For carrying out handovers, different scenarios exist:

- **Intra-Cell Handover:** The channel used is changed in one particular cell. The MS can be assigned either another FDM-channel or another time slot.
- **Inter-Cell/Intra-BSC Handover:** Here, the MS changes to a new BTS (by being assigned a new FDM-channel) handled by the same BSC.
- **Inter-BSC/Intra-MSC Handover:** The MS is assigned to a new BTS and BSC, the MSC is the same.
- **Inter-MSC Handover:** The MS is assigned a new BTS, BSC and MSC.

In the first two cases, the handover can be carried out by the BSC, if it is able to do so. If not, the MSC must handle the handover. The handover itself is carried out by sending a sequence of messages and will not be described here.

Ping-Pong handovers can be decreased by providing reasonable limits but cannot be avoided.

3.2.6. THE GSM PROTOCOL ARCHITECTURE

Like in ISDN, the GSM architecture can be roughly divided into three independent planes:

- User plane
- Control plane
- Management plane

The user plane defines a set of protocols to carry connection oriented voice and user data from one TE to the other. In the ISDN part of the GSM network, this is done over B-channels. At the radio interface, it is called Bm-channel.

The control plane defines a set of protocols for controlling these connections. This data is carried over D-channels (Dm-channels). As the D and Dm-channels will often have spare capacities, packet oriented data like SMS may also be transported over D and Dm-channels. At the radio interface Um, user plane data will be carried by the TCH logical channel, while signaling information will be carried over the remaining logical channels. All logical channels, however, will be finally multiplexed onto the physical channel.

3.2.7. USER DATA TRANSMISSION

For carrying user data, the path is divided roughly into two parts. In the first part, the MS communicates with the BSS over radio. This set of protocols is GSM specific. The BSS then communicates with the MSC over the A-interface. This is done in an ISDN-compatible manner. The Abis-interface between BTS and BSC in general is transparent to user data.

3.2.7.1. VOICE TRANSMISSION

GSM and ISDN use both different codecs and transmission rates. GSM generates data at 13 kbit/s, using the Regular Pulse Excitation-Long Term Prediction (RPE-LTP) codec. ISDN-B-channels work at 64 kbit/s and use ITU-T A-law coding, a non-uniformly spaced logarithmic codec. At one point in the transmission path, the two different streams have to be converted into each other. This is done in the Transcoding and Rate Adaption Unit (TRAU). On possible location of the TRAU is inside the BTS. In this case, the data leaving such a BTS will flow at 64 kbit/s into the adjacent BSC and beyond.

Another location can be between a BSC and an MSC. Here, the TRAU can be locate at the BSC or MSC. If it is located at the BSC, the BSC can multiplex four 13 kbit/s channels onto one ISDN-B-channel. As the TRAU depends on the radio link for synchronization, the remaining 3 kbit/s (16 = 13+3) are used to carry signaling information (inband signaling). This must also be done, if the TRAU is physically at the MSC.

Once the data is being transported inside an ISDN-B-channel, it will travel to its destination by using the ITU-T ISDN standard protocols G.703, G.705 and G.732.

3.2.7.2. TRANSPARENT DATA TRANSMISSION

As the transmission quality of radio signals can change drastically during one connection, the biterror probability despite FEC can vary between 10^{-2} and 10^{-5}. Transparent bearer services do not try to correct detected errors and rely on FEC only. The sender thus is guaranteed a constant bitrate and may send data at this rate without flow control, hence, for the sender, the underlying transport system is transparent. The TE though has to be aware of non-neglectable biterror probabilities.

3.2.7.3.NON-TRANSPARENT DATA TRANSMISSION

Another way of coping with detected biterrors is to resend the data-frame. In Non-Transparent bearer services, the Radio Link Protocol (RLP), is used. One part of this protocol is located in the MS, the other in the MSC. In this protocol, the data is cut into numbered frames of equal size, where each frame has to be acknowledged by the receiver (one acknowledge frame can acknowledge several data frames). In RLP, there are two different frame types:

- Information frames: carry the user data
- Control frames: carry control information for controlling the connection and sending acknowledgements.

By the special design of the frame header, information frames can also transport control information. If an error is detected inside an information frame, the receiver sends a resend command to the sender, either for this particular frame or all frames beginning from the erroneous frame.

Due to frame resends as a result of bad radio connections, the net bitrate of such a channel may change drastically and the sending TE must be flow-controlled in order to adapt to the available bitrate. This is done by the Non-Transparent Protocol (NTP), where the TE is connected to (generally over a V.24 interface). Hence for the sender, the transport system is not transparent anymore.

3.2.8. SIGNALING TRANSMISSION

For establishing, controlling and deleting connections, GSM nodes have to exchange signals with each other. The following interfaces are defined between the GSM nodes:

- MS-BTS: Um
- BTS-BSC: Abis
- BSC-MSC: A
- MSC-VLR: B
- MSC-HLR: C
- VLR-HLR: D
- MSC-MSC: E
- MSC-EIR: F
- VLR-VLR: G

The physical transportation of these signals is done via the physical channel in the Um interface, and over digital lines of either 2048 kbit/s or 64 kbit/s otherwise (ITU-T G.703, G.705, G.732).

3.2.8.1.THE GSM PROTOCOL LAYERS

The GSM protocol layers are designed to meet the ISO/OSI reference model.

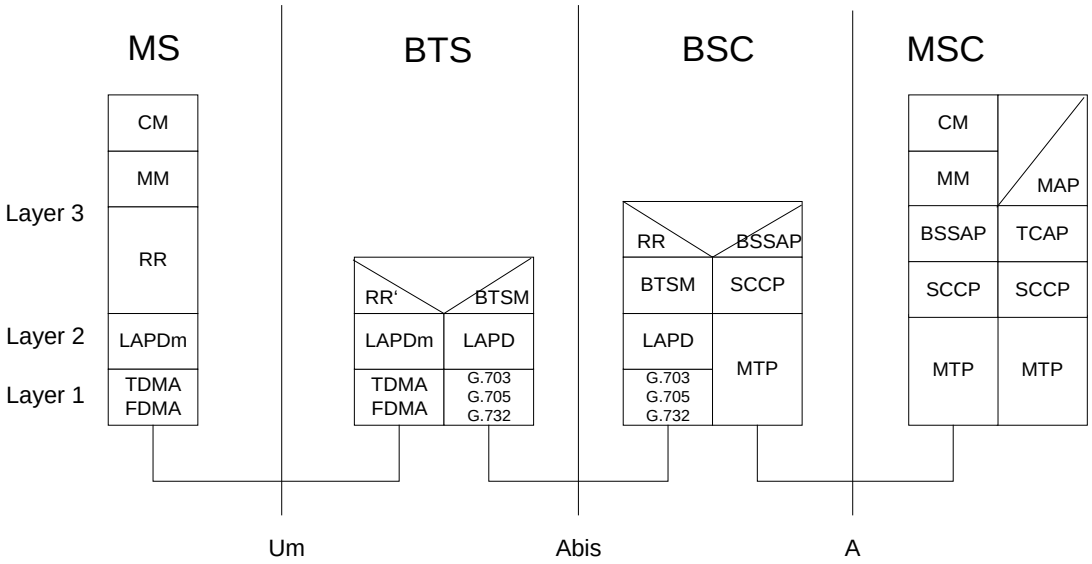

Figure 5 : GSM Protocol Layers

Lower layers provide their services to higher layers at Service Access Points (SAP). The following sections will describe briefly the protocols at the Um, Abis and A interfaces.

3.2.8.2.LAYER 2 PROTOCOLS

- **Link Access Procedure for the Dm-channel (LAPDm)** is a GSM specific layer 2 protocol to provide secure Dm-channels between MS and BTS for layer 3 protocols. LAPDm is similar to HDLC and works in two modes. Unacknowledged operation means sending UI-frames without acknowledgement. Flowcontrol and L2-error correction are not carried out. In acknowledged operation, data is transported in I-frames and must be acknowledged. Error correction by resending and flowcontrol are carried out.
- **Link Access Procedure for the D-channel (LAPD)** is layer 2 protocol to provide secure D-channels for ISDN.
- **Message Transfer Part (MTP)** is the standard ISDN message transport part for SS7. Generally, it includes the lower 3 layers of the ISDN network, i.e. it routes and transports signaling messages. As MM and CM need identifiable connections for signals, the Signaling Connection Control Part (SCCP) is inserted at layer 3.

3.2.8.3.LAYER 3 PROTOCOLS

- **Radio Resource Management (RR)** is a layer 3 protocol for creating, maintaining and deleting of radio link channels. RR´ defines a subset of RR. It is also responsible for

measuring the channel quality, controlling the radio field strength and synchronization, handover and data ciphering. An RR message contains a protocol discriminator for protocol identification, a transaction ID and a message type. The data itself is carried in a so-called Information Element (IE) of fixed or variable length (here, an additional Length Indicator (IE) is necessary).

- **Mobility Management (MM)** is a layer 3 protocol for supporting the mobility of a TE. MM procedures need a pre-established RR connection, i.e. a logical channel and a LAPDm connection. Signaling is carried out between the MS and the MSC, it is thus transparent to the BSS. For MM procedures, there are three categories. Common procedures can always be carried out independent of each other. Examples are TMSI reallocation, authentication, identity requests and IMSI detachments. Specific procedures are mutually exclusive, i.e. such a procedure cannot be carried out, as long as another one is executed. They are also mutually exclusive to MM-connections. Examples are location updates and IMSI attachments. Finally, mobility management procedures create, maintain and tear down MM connections. MM connections are created upon requests from the higher CM sublayer. Each CM instance is assigned its own MM connection.
- **Call Management (CM)** is a layer 3 protocol containing three subprotocols. Call Control (CC) creates, maintains and deletes calls. Several parallel calls can be established, thus for each call, one CC instance is created in the MS, and one in the MSC. CC instances communicate with each other via dedicated MM instances they own. The Short Message Service (SMS) is divided into the SMS Control Layer (SMS-CL) and the SMS Relay Layer (SMS-RL). They need previously established MM, RR and LAPDm connections. As the user data is packet oriented, they are marked SAPI=3 in the LAPDm layer. Finally, Supplementary Services (SS) provide an entry point to access the GSM supplementary services. Applications from upper layers may enter the CM vie the three Service Access Points (SAP) MNCC-SAP, MNSS-SAP and MNSMS-SAP. However, they can also bypass the CM by directly entering the MMREG-SAP of MM.
- **Signaling Connection Control Part (SCCP)** is a layer 3 SS7 protocol for establishing and maintaining identifiable control connections. At the A-interface, it offers connection-oriented and connectionless transport services.
- **Base Station System Application Part (BSSAP)** is a layer 3 protocol for signaling at the A interface, using services offered by the SCCP. It is further divided into three sub-parts. The Direct Transfer Application Part (DTAP) offers services for signaling between the MS and the MSC (CM,MM). Here, signals are transported transparently through the in-between BSS. DTAP signals only use connection oriented SCCP services. The Base Station System Management Application Part (BSSMAP) transports signals between an MSC and an BSC. These signals may concern single MS, physical channels of the radio link as well as global commands for the BSC resource management. BSSMAP procedures use connection-oriented and connectionless SCCP services. Finally, the Base Station System Operation and Maintenance Application Part (BSSOMAP) transports network management messages from the OMC over the MSC to a BSC.
- **Mobile Application Part (MAP)** is the GSM specific enhancement of SS7. It manages roaming functions like location registration/updating, IMSI attach/detach, handover, subscriber management, IMEI management, authentication and identification and SMS. For MAP, the special interfaces to other GSM network nodes are defined as stated in section 3.2.8.

4. GPRS : GATEWAY TO 3RD GENERATION

This section covers the presentation and characterization of the GPRS network protocol. As it is the only kind of mobile network that we plan to model and simulate, it is given more emphasis than the others.

4.1. INTRODUCTION

4.1.1. THE SCENE

The technological area of mobile and personal communications experiences an evolution in Europe and worldwide. The 1st Generation of cellular technologies introduced the analog mobile systems. The 2nd Generation, which is the current generation, introduced the digital mobile systems already available plus the mobile packet technologies, which are evolving. The most prominent representative of the 2nd Generation digital mobile systems is GSM, which gained worldwide acceptance and extraordinary market success. GSM provided so far circuit switched services. However, it is currently enhanced in order to provide high-speed packet switched services as well. The General Packet Radio Service (**GPRS)** is one kind of packet-switched data technology, which is being developed for GSM networks. This technology is expected to open the mobile world to a number of new applications. In fact it will enable what is usually referred as the mobile office. GPRS is expected to be implemented in the 1999-2000 time frame. A view of the anticipated GSM service evolution towards multimedia services is depicted in Table 6.

Data communications bit rate / Application	Single slot 9.6 kbit/s	Double slot 19.2 kbit/s	Multiple slot 76.8 kbit/s
Simultaneous voice & data	Half rate + 4.8 kbit/s	Full rate + 9.6 kbit/s	Full rate + 76.2 kbit/s
Hi/Fi music/ voice	Wireline quality with enhanced full rate coder	HiFi quality voice	HiFi quality voice and music
Multimedia/ video	Stills animations	Animations video	Video conferencing

Table 6 : GSM evolution towards multimedia services

The GSM MoU Association, representing 239 GSM network operators, telecommunications regulators and administrations from over 109 countries/areas of the world, has placed a high priority on developing its vision of future Third Generation Systems based on an evolution of the GSM platform.

During its recent plenary meeting, GSM MoU Association members agreed that GPRS would be a key link between GSM and the UMTS as many of the characteristics of GPRS (e.g. packet based, transport, new control) are very relevant for UMTS.

4.1.2. IMPORTANCE OF PACKET RADIO TECHNOLOGIES

The currently available digital mobile technologies provide circuit-switched services that require a dedicated radio channel even when no data is being sent. GPRS aims to provide actual packet-switched radio access for mobile GSM users. The main benefit is that it reserves radio resources only when there is something to send. The same radio resource is shared by all mobile stations (MSs) in a cell, providing effective use of the scarce resources.

The need for packet radio is based on the high burstiness of data applications. GPRS facilitates a variety of applications, such as teleworking, telemetry, train control systems, interactive data access, toll road charging systems, and Internet browsing using World Wide Web. In these cases, packet-switched access mechanisms are known to give better utilization of the transmission medium than circuit-switched ones due to statistical multiplexing.

From the user's viewpoint packetized transmission within GSM will be more convenient not only because of the new services that could be provided. In contrast to time-oriented charging applied for circuit-switched connections, packet-switched data services will allow charging depending on the amount of data transmitted and the quality of service negotiated. The primary interest of end users of a new wireless packet data service is that applications used to run within their fixed computer environment should be supported at moderate cost and without notable changes in operation.

In order to satisfy the increasing user requirements and to preserve competitiveness, one major concern of GSM Phase 2+ development, led by the European Telecommunications Standards Institute (ETSI), has been to specify a general packet radio service (GPRS) that accommodates data connections with high bandwidth efficiency.

The main intention of the specification of a GPRS has been to enlarge the limited range of existing GSM data services that offers data rates up to 9.6 kb/s only. In order to enable support of new data applications with a convenient quality of service, the GPRS concept foresees bit rates of nearly 170 kb/s that can be flexibly allocated according to actual user demands.

4.1.3. GPRS PRIMARY REQUIREMENTS

The primary requirements to be met by GPRS are as follows :

- **To enable new and existing applications to be attracted onto GSM :** To achieve this, the enhancement of GSM's functional and QoS parameters are vital goals. Applications, which could be attracted because packet mode data transmission is provided through GPRS, can be classified into horizontal and vertical markets. Requests for enhancements of the functional and performance capabilities of GSM have been received from the following markets:

Horizontal:	Wireless Personal Computers
	Mobile Offices
	Electronic Funds Transfer from Point of Sale
Vertical:	Road Transport Informatics
	Union International de Chemin de Fer (UIC)

Field Service Businesses
Fleet Management
Remote Telematics
Commodity/Supply Logistics

- **GPRS shall support both connectionless and connection oriented services**.

- **To offer a flexible service at low cost to the user :** In order to make the service as cost effective as possible, the impact upon existing investments in GSM architectural entities, their supporting protocols and deployment costs must be kept to a minimum.

- **To use scarce network resources as efficiently as possible**.

- **To support early introduction of GPRS services**, without compromise to eventual capacity and performance, through a phased program of definition and implementation.

4.1.4. GPRS CLASSIFICATION

GPRS shall provide packet mode transfer for applications that exhibit the following data traffic patterns :

- Frequent transmission of small volumes.

- Infrequent transmissions of small or medium volumes.

The PLMN Operator who offers GPRS shall be responsible for transferring data between the service access points at the fixed side and at the mobile side. The flow of data shall be possible in three scenarios :

- Packets sent from a mobile access point to a fixed network access point.

- Packets sent from a fixed network access point to a mobile access point.

- Packets sent from a mobile access point to a mobile access point via the GSM PLMN infrastructure. This does not exclude an implementation in which MO-MT packets are transferred using the previous two modes.

GPRS shall be distinguished from existing services in two ways :

- Firstly, it is required to efficiently use network resources for packet mode applications.

- Secondly, new mechanisms are required in order to provide highly standardized, feature-rich services, in which the Service Requesters can make the selection of the QoS parameters.

Other guidelines ruling GPRS deployment are as follows :

- GPRS shall not prevent the existing user's operation of GSM services.
- GPRS shall not be used as a basis for packetized speech.
- GPRS shall not be used as a basis for services that duplicate, in terms of performance and cost requirements, GSM services.

4.2. GPRS TECHNICAL DESCRIPTION

4.2.1. GPRS SERVICE DESCRIPTION

There are two categories of GPRS services :

- **Point to Point** (PTP) services,
- **Point to Multipoint** (PTM) services.

The PTP service provides a transmission of one or more packets between two users initiated by a service requester and received by a receiver.

There are two PTP services:

- PTP Connectionless Network Service (PTP-CLNS);
- PTP Connection Orientated Network Service (PTP-CONS).

The PTM service provides a transmission of packets between a service requester and a receiver group.

There are three PTM services:

- PTM Multicast (PTM-M);
- PTM Group Call (PTM-G);
- IP Multicast (IP-M).

For PTM-M and PTM-G the data transmission is restricted to the members of a receiver group currently located within a geographical area. The service requester specifies both the receiver group and the geographical area.

The geographical area addressing mechanism is not applicable to IP-M.

An invocation of the service request by a service requester is possible from the fixed and mobile access points Table 7 presents the relationship between service requests and the Service Requester/Receiver.

Service requester/receiver AP = Access Point (see note 1)	Types of service request			
	PTP-CONS and PTP-CLNS	**PTM-M**	**PTM-G**	**IP-M**
From fixed AP to mobile AP	Supported	Supported	Supported	Supported
From mobile AP to mobile AP (see note 3)	Supported	Supported	Supported	Supported
From mobile AP to fixed AP	Supported	Not applicable	Supported (limited, see note 2)	Supported
NOTE 1: Mobile bearer services access points are 2 and 4 from figure 2. Fixed bearer service access points are 7 and 8. NOTE 2: All PTM-G features may not be supported for fixed AP, e.g., paging. NOTE 3: It shall be possible to transfer data between two mobiles of the same operator without the use of non-GSM external data networks.				

Table 7 : Relationship of service request and service requester/receiver

4.2.2. NETWORK ARCHITECTURE

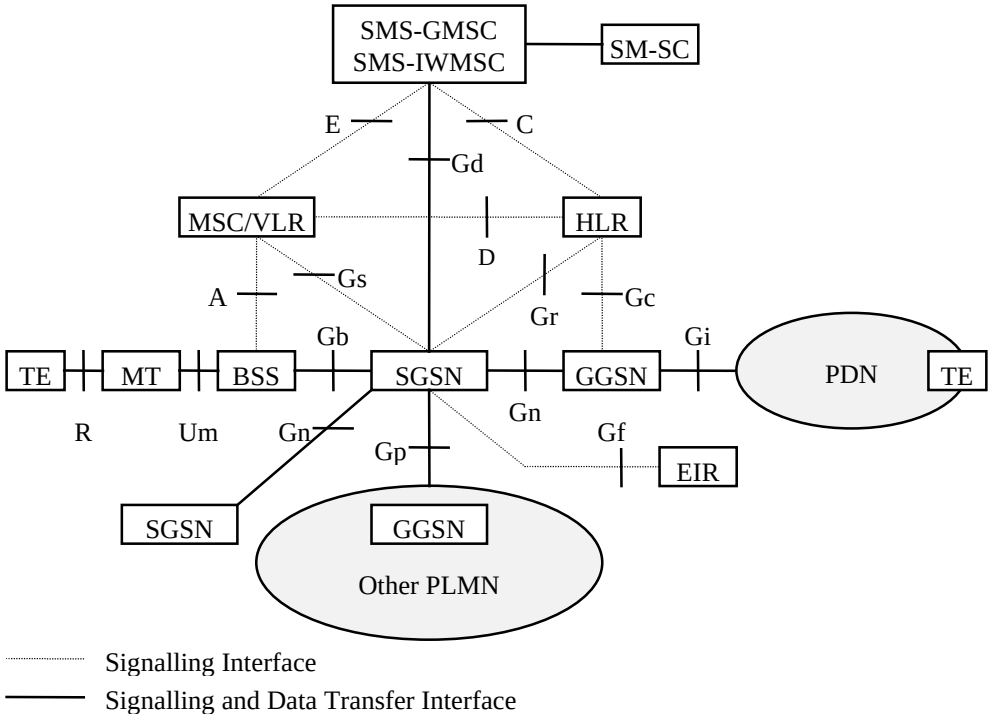

Figure 6 : GPRS Network Description

4.2.2.1. NETWORK INTERFACES

In the GSM-GPRS network topology the following interfaces are defined.

Gb Interface between an SGSN and a BSS.

Gc Interface between a GGSN and an HLR.

Gd Interface between an SMS-GMSC and an SGSN, and between an SMS-IWMSC and an SGSN.

Gf	Interface between an SGSN and an EIR.
Gi	Reference point between GPRS and an external packet data network.
Gn	Interface between two GSNs within the same PLMN.
Gp	Interface between two GSNs in different PLMNs. The Gp interface allows support of GPRS network services across areas served by the co-operating GPRS PLMNs.
Gr	Interface between an SGSN and an HLR.
Gs	Interface between an SGSN and an MSC/VLR.
Um	Interface between the mobile station (MS) and the GPRS fixed network part. The Um interface is the GPRS network interface for providing packet data services over the radio to the MS. The MT part of the MS is used to access the GPRS services through this interface.

4.2.2.2.NETWORK & SWITCHING SUBSYSTEM (NSS)

- **The Home Location Register (HLR) :**

This functional entity is a database in charge of the management of mobile subscribers. A PLMN may contain one or several HLRs: it depends on the number of mobile subscribers, on the capacity of the equipment and on the organization of the network. Two kinds of information are stored there:

- the subscription information;
- some location information enabling the charging and routing of calls towards the MSC where the MS is located (e.g. the MS Roaming Number, the VLR address, the MSC address and the Local MS Identity).

- **The Mobile-services Switching Center (MSC) :**

The Mobile-services Switching Center is an exchange which performs all the switching and signaling functions for mobile stations located in a geographical area designated as the MSC area. The main difference between a MSC and an exchange in a fixed network is that the MSC has to take into account the impact of the allocation of radio resources and the mobile nature of the subscribers and has to perform in addition, at least the following procedures:

- Procedures required for the location registration.
- Procedures required for handover.

- **The Visitor Location Register (VLR) :**

A mobile station roaming in an MSC area is controlled by the Visitor Location Register is in charge of this area. When a Mobile Station (MS) enters a new location area it starts a

registration procedure. The MSC in charge of that area notices this registration and transfers to the Visitor Location Register the identity of the location area where the MS is situated. If this MS is no yet registered the VLR and the HLR exchange information to allow the proper handling of calls involving the MS.

- **The Authentication Center (AuC) :**

The Authentication Center (AuC) is associated with an HLR, and stores an identity key for each mobile subscriber registered with the associated HLR. This key is used to generate:

- data which are used to authenticate the IMSI;
- a key used to cipher communication over the radio path between the mobile station and the network.

.
The AuC communicates only with its associated HLR over an interface denoted the H-interface.

- **The Equipment Identity Register (EIR) :**

This functional entity contains one or several databases which store(s) the IMEIs used in the GSM system. The mobile equipment may be classified as "white listed", "gray listed" and "black listed" and therefore may be stored in three separate lists. An IMEI may also be unknown to the EIR.

- **GPRS Support Nodes: GSN – SGSN :**

A GPRS Support Node (GSN) contains functionality required to support GPRS. In one PLMN, there may be more than one GSN.

The Gateway GPRS Support Node (GGSN) is the node that is accessed by the packet data network due to evaluation of the PDP address. It contains Routing information for attached GPRS users. The Routing information is used to tunnel PDUs to the MS's current point of attachment, i.e., the Serving GPRS Support Node. The GGSN may request location information from the HLR via the optional Gc interface. The GGSN is the first point of PDN interconnection with a GSM PLMN supporting GPRS (i.e., the Gi reference point is supported by the GGSN).
The Serving GPRS Support Node (SGSN) is the node that is serving the MS (i.e., the Gb interface is supported by the SGSN). At GPRS attach, the SGSN establishes a mobility management context containing information pertaining to e.g., mobility and security for the MS. At PDP Context Activation, the SGSN establishes a PDP context, to be used for Routing purposes, with the GGSN that the GPRS subscriber will be using.

The SGSN and GGSN functionality may be combined in the same physical node, or they may reside in different physical nodes. SGSN and GGSN contain IP routing functionality, and they may be interconnected with IP routers. When SGSN and GGSN are in different PLMNs, they are interconnected via the Gp interface. The Gp interface provides the functionality of the Gn interface, plus security functionality required for inter-PLMN communication. The security functionality is based on mutual agreements between operators.

The SGSN may send location information to the MSC/VLR via the optional Gs interface. The SGSN may receive paging requests from the MSC/VLR via the Gs interface.

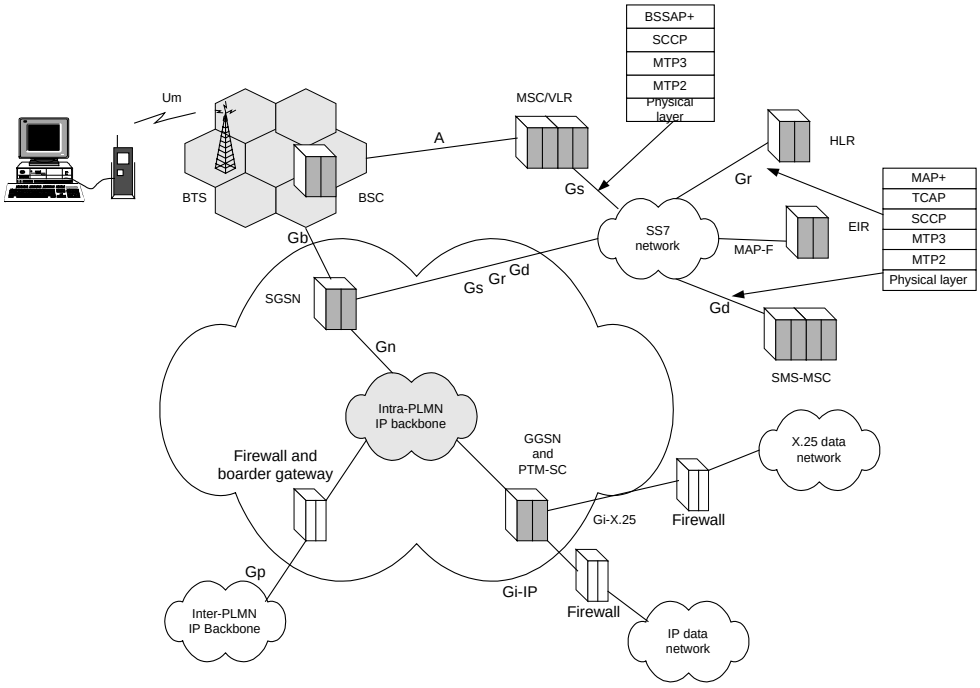

Figure 7 : GPRS Network Architecture

4.2.2.3.BASE STATION SUBSYSTEM (BSS)

The Base Station System (BSS) is the system of base station equipment (transceivers, controllers, etc.) which is viewed by the MSC through a single A-interface as being the entity responsible for communicating with Mobile Stations in a certain area. The radio equipment of a BSS may support one or more cells. A BSS may consist of one or more base stations, where an Abis-interface is implemented. The BSS consists of one Base Station Controller (BSC) and one or more Base Transceiver Station (BTS).

A Base Station Controller (BSC) is a network component in the PLMN with the functions for control of one or more BTS.

A Base Transceiver Station (BTS) is a network component, which serves one cell.

4.2.3. TRANSMISSION AND SIGNALING PLANES

4.2.3.1.TRANSMISSION PLANE

The transmission plane consists of a layered protocol structure providing user information transfer, along with associated information transfer control procedures (e.g., flow control, error detection, error correction and error recovery). The transmission plane independence of

the Network Subsystem (NSS) platform from the underlying radio interface is preserved via the Gb interface. The following transmission plane is used in GPRS:

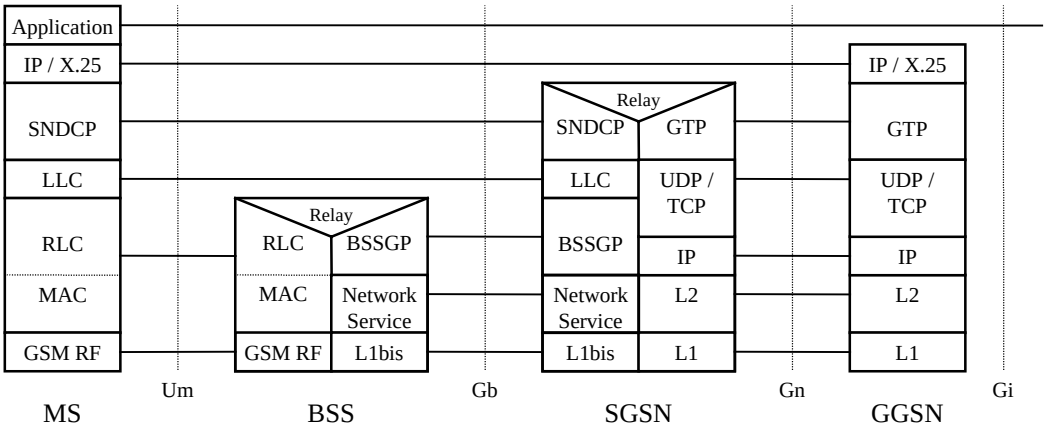

Figure 8 : Transmission Plane

- **GPRS Tunneling Protocol (GTP) :** This protocol tunnels user data and signaling between GPRS Support Nodes in the GPRS backbone network. All PTP PDP PDUs shall be encapsulated by the GPRS Tunneling Protocol. GTP shall provide mechanisms for flow control between GSNs.
- **TCP** carries GTP PDUs in the GPRS backbone network for protocols that need a reliable data link (e.g., X.25), and UDP carries GTP PDUs for protocols that do not need a reliable data link (e.g., IP). TCP provides flow control and protection against lost and corrupted GTP PDUs. UDP provides protection against corrupted GTP PDUs. TCP is defined in RFC 793. UDP is defined in RFC 768.
- **IP :** This is the GPRS backbone network protocol used for Routing user data and control signaling. The GPRS backbone network may initially be based on the IP version 4 protocol. Ultimately, IP version 6 shall be used. IP version 4 is defined in RFC 791.
- **Subnetwork Dependent Convergence Protocol (SNDCP) :** This transmission functionality map network-level characteristics onto the characteristics of the underlying network. SNDCP is specified in GSM 04.65.
- **Logical Link Control (LLC) :** This layer provides a highly reliable ciphered logical link. LLC shall be independent of the underlying radio interface protocols in order to allow introduction of alternative GPRS radio solutions with minimum changes to the NSS. LLC is specified in GSM 04.64.
- **Relay :** In the BSS, this function relays LLC PDUs between the Um and Gb interfaces. In the SGSN, this function relays PDP PDUs between the Gb and Gn interfaces.
- **Base Station System GPRS Protocol (BSSGP) :** This layer conveys Routing- and QoS-related information between BSS and SGSN. BSSGP does not perform error correction.
- **Network Service (NS) :** This layer transports BSSGP PDUs. NS is based on the Frame Relay connection between BSS and SGSN, and may be multi-hop and traverse a network of Frame Relay switching nodes.

- **RLC/MAC :** This layer contains two functions: The Radio Link Control function provides a radio-solution-dependent reliable link. The Medium Access Control function controls the access signaling (request and grant) procedures for the radio channel, and the mapping of LLC frames onto the GSM physical channel. RLC/MAC is defined in GSM 04.60 .
- **GSM RF :** As defined in GSM 05 series.

4.2.3.2.SIGNALING PLANE

The signaling plane consists of protocols for control and support of the transmission plane function :

- controlling the GPRS network access connections, such as attaching to and detaching from the GPRS network;
- controlling the attributes of an established network access connection, such as activation of a PDP address;
- controlling the Routing path of an established network connection in order to support user mobility;
- controlling the assignment of network resources to meet changing user demands; and
- providing supplementary services.

4.2.4. HIGH-LEVEL FUNCTIONS REQUIRED FOR GPRS

The following list gives the logical functions performed within the GPRS network. Several functional groupings (meta-functions) are defined which each encompasses a number of individual functions:

- Network Access Control Functions.
- Packet Routing and Transfer Functions.
- Mobility Management Functions.
- Logical Link Management Functions.
- Radio Resource Management Functions.
- Network Management Functions.

4.2.4.1.NETWORK ACCESS CONTROL FUNCTIONS

Network access is the means by which a user is connected to a telecommunication network in order to use the services and/or facilities of that network. An access protocol is a defined set of procedures that enables the user to employ the services and/or facilities of the network.

User network access may occur from either the mobile side or the fixed side of the GPRS network. The fixed network interface may support multiple access protocols to external data networks, for example X.25 or IP. The set of access protocols to be supported is determined by the PLMN operator.

Individual PLMN administrations may require specific access-control procedures in order to limit the set of users permitted to access the network, or to restrict the capabilities of individual users, for example by limiting the type of service available to an individual subscriber. Such access control procedures are beyond the scope of the GPRS specifications.

In addition to the standard PTP data transfer, GPRS may support anonymous access to the network. The service allows an MS to exchange data packets with a predefined host that can be addressed by the supported interworking protocols. Only a limited number of destination PDP addresses can be used within this service. IMSI or IMEI shall not be used when accessing the network thus guaranteeing a high level of anonymity. Therefore, no authentication and ciphering functionality is foreseen for anonymous access.

4.2.4.2.PACKET ROUTING AND TRANSFER FUNCTIONS

A route is an ordered list of nodes used for the transfer of messages within and between the PLMN(s). Each route consists of the originating node, zero or more relay nodes and the destination node. Routing is the process of determining and using, in accordance with a set of rules, the route for transmission of a message within and between the PLMN(s).

4.2.4.3.MOBILITY MANAGEMENT FUNCTIONS

The mobility management functions are used to keep track of the current location of an MS within the PLMN or within another PLMN.

4.2.4.4.LOGICAL LINK MANAGEMENT FUNCTIONS

Logical link management functions are concerned with the maintenance of a communication channel between an individual MS and the PLMN across the radio interface. These functions involve the co-ordination of link state information between the MS and the PLMN as well as the supervision of data transfer activity over the logical link.

4.2.4.5.RADIO RESOURCE MANAGEMENT FUNCTIONS

Radio resource management functions are concerned with the allocation and maintenance of radio communication paths. GSM radio resources is shared between the circuit mode (voice and data) services and the GPRS.

4.3. INTERWORKING

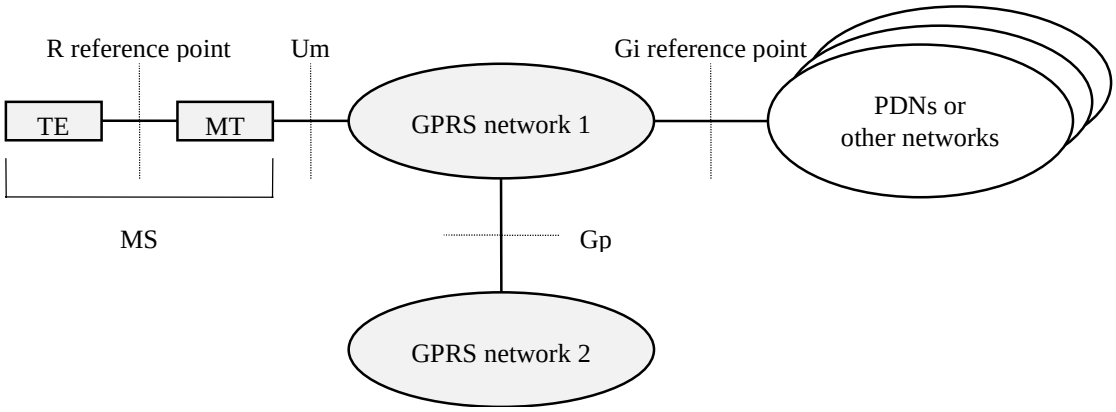

Figure 9 : GPRS Access Interfaces and Reference Points

Network interworking is required whenever a PLMN supporting GPRS and any other network are involved in the execution of a GPRS Service Request. With reference to Figure 10, interworking takes place through the Gi reference point and the Gp interface.

The GPRS internal mechanism for conveying the PDU through the GSM PLMN is managed by the GSM GPRS network operator and is not apparent to the data user. The use of this GSM data service may have an impact on and increase the transfer time normally found for a message when communicated through a fixed packet data network.

4.3.1. PSPDN INTERWORKING

GPRS shall support interworking with PSPDN networks. The interworking may be either direct or through a transit network (e.g., ISDN). GPRS shall support both X.121 and E.164 addresses.
GPRS shall provide support for X.25 virtual circuits and X.25 fast select. X.75 may be used for interworking with X.25 PDNs.

The GPRS TEs have addresses provided by the GSM PLMN GPRS service operator and belong to the GPRS service domain. The PSPDN TE sends data to the GPRS TE by use of the GSM PLMN GPRS DNIC (Data Network Identification Code) or equivalent that uniquely identifies the GPRS network.

There are two models for PSDN interworking :

- X.75 over the Gi reference point.

- X.25 over the Gi reference point with the DCE located within the PSDN and the DTE located within the TE of the GPRS PLMN.

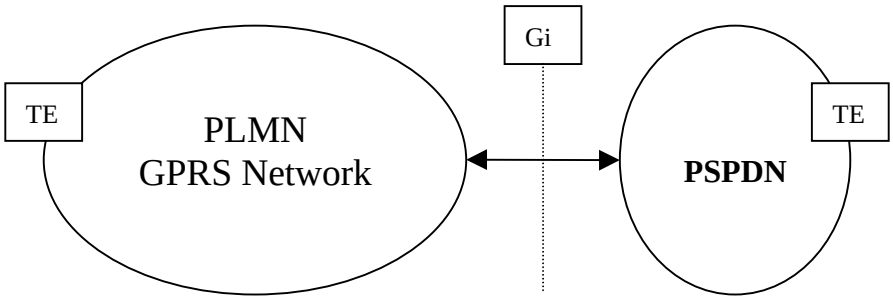

Figure 10 : X75 PSPDN Interworking at Gi reference point

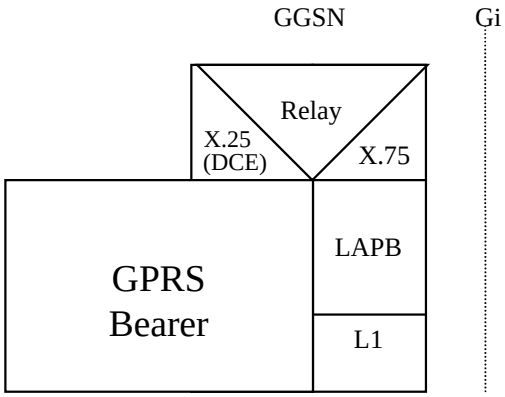

Figure 11 : The Protocol Stack for the X.75 Gi Referencing point

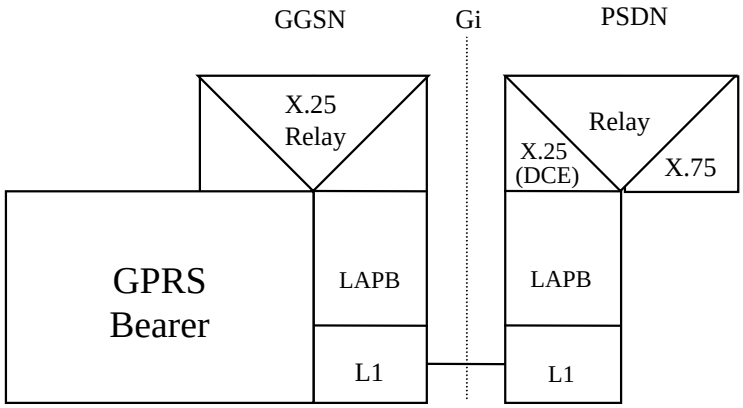

Figure 12: The Protocol Stack for the X.25 / Gi Referencing point

4.3.2. INTERNET (IP) INTERWORKING

GPRS support interworking with networks based on the Internet protocol (IP). GPRS provide compression of the total TCP/IP header when an IP-datagram is used within the context of a TCP connection.

In a similar way to the PSPDN X.25 case, the GSM PLMN GPRS service is an IP domain, and mobile terminals offered service by a GSM service provider are globally addressable through the network operator's addressing scheme.

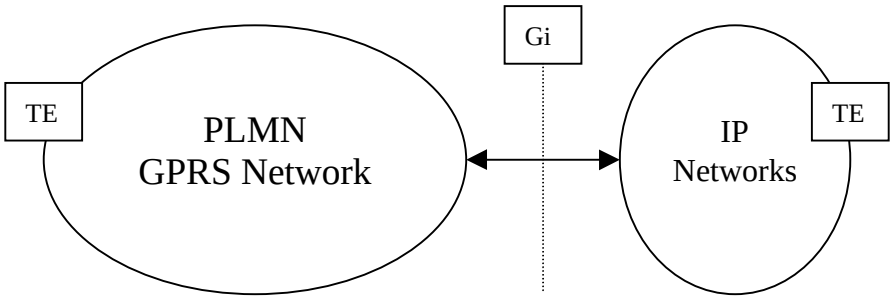

Figure 13: The Protocol Stack for IP Networks / Gi Referencing point

When interworking with the IP networks, GPRS can operate IPv4 or Ipv6. The interworking point with IP networks is at the Gi reference point.

The GGSN for interworking with the IP network is the access point of the GSM GPRS data network (see Figure 13). In this case the GPRS network will look like any other IP network or subnetwork.

Typically in the IP networks, the interworking with subnetworks is done via IP routers. The Gi reference point is between the GGSN and the external IP network. From the external IP network's point of view, the GGSN is seen as a normal IP router. The L2 and L1 layers are operator specific.

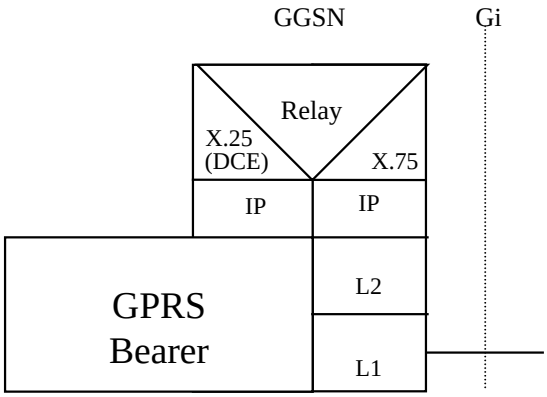

Figure 14 : The protocol stacks for the Gi IP reference point

Interworking with user defined ISPs and private/public IP networks is subject to interconnect agreements between the network operators.

A generic infrastructure supporting IP-interworking can include the following elements:

- The GPRS operator configures a firewall. In general, all applications that are using IP as the underlying protocol are supported, but the GPRS operator may restrict their usage.
- A Domain Name Server is managed by the GPRS or the external IP network operator.

From the GPRS network's point of view, the allocation of a dynamic IP address is done by the GGS. The GGSN may allocate these addresses by itself or use an external device such as a DHCP (Dynamic Host Configuration Protocol) server. This external device may be operated by an external organization such as an ISP or Intranet operator.

5. A PRESENTATION OF THIRD GENERATION MOBILE SYSTEMS

Now, we have studied the most important existing mobile network protocols, but a new generation of mobile systems is being designed currently. So far, it concerns only one protocol, still in the specification phase, that is called UMTS.

5.1. INTRODUCTION

At the beginning of the next century the mobile communication scene will be significantly different. Due to the global success of the GSM family, mobile communications will have reached the mass market status. On the demand side, the call for new and more sophisticated services and applications will increase. On the supply side, network operators and service providers will be looking for opportunities to distinguish themselves from their competitors.

5.2. UMTS GENERAL DESCRIPTION

The new generation of mobile technology would be necessary to cater for the challenges of the next century. The Universal Mobile Telecommunication System (UMTS) is the realization of a such a new generation, aimed for a world in which "Personal Services will be based on a combination of fixed and wireless/mobile services to form a seamless end-to-end service for the user". To bring this about will require at least:

- provision of a **unified presentation of services** to the user in wireless and wired environments;
- **mobile technology** that supports a very broad mix of communication services and applications;
- on-demand **flexible bandwidth allocation** and in a wide variety of applications;
- **standardization** that allows full roaming and interworking capability, where needed, but that is also responsive to proprietary, innovative and niche markets.

With UMTS providing the integral mobile access part to B-ISDN, telecommunications will make a major leap forward towards the provision of a technically integrated, comprehensive and consistent system of personal communications supported by both fixed and mobile terminals. As a result, mobile access networks will begin to offer services that have traditionally been provided by fixed networks, including wideband services up to 2 Mbit/s. UMTS however might also function as a stand-alone network implementation.

UMTS will be introduced in the public network environment as integral part of the future broadband infrastructure that is in the process of being deployed. It will be perceived as providing mobile access to the broadband infrastructure. UMTS will become a part of the public infrastructure, its use in restricted coverage environments is also supported (i.e. Wireless Local Loop access).It will integrate the satellite component mainly as a complement to its terrestrial coverage.

New UMTS applications will build on the UMTS system and may, or may not, require extra functionality of the system. The former case is an extension of the specified UMTS system. UMTS users will demand services that are competitive with the services of the dedicated first and second generation networks. Moreover they will expect that UMTS will bring 'made-to-measure' services for 'ready-made' prices. Users will expect UMTS to provide a solution for Quality of Service problems they possibly have as the result of saturation in the older systems.

5.2.1. SERVICE PROVISION

UMTS will be capable of providing services of high quality and integrity. The UMTS services will be compatible with services provided by B-ISDN, ISDN, PSTN and second generation mobile systems (GSM, DCS 1800, etc.). There will be complementary to, and consistent with, the services provided in the fixed environments. UMTS will be capable of providing telephony services of a quality that is at least comparable to the telephony services of the existing fixed and mobile networks. It will be capable of providing the basic telecommunication services underlying the following applications:

- telephony
- messaging
- transfer of documents containing text, images and voice annotation, e.g. facsimile group 4;
- transactional applications;
- applications related to transfer of (short) messages, including paging and voice mail;
- user guidance for service usage (e.g. directory services);
- video information transfer, either on-line or off-line (restricted by the available transmission capacity);
- file transfer;
- information retrieval applications, including multimedia;
- Advanced Transport Telematic applications.

UMTS will support multimedia services, in accordance with the following principles:

- dynamic bandwidth allocation;
- transfer mode independent of information type (where possible);
- decoupling of telecommunication service and network technology;
- point-to-point, multipoint, multicast, and broadcast communications.

The UMTS environment, due to its inherent features and characteristics, imposes specific requirements and constraints on the provision of multimedia services. Constraints originating from the radio path and mobility aspects will determine for a great extent the characteristics of the multimedia services in UMTS. Important aspects in this respect are:

- bandwidth;

- synchronization;
- handover.

UMTS will support a wide range of association services. These are divided into basic association services, which provide basic call and connection support, and supplementary association services, which provide features similar to the supplementary services in ISDN and GSM.

UMTS will allow services to be integrated or combined in a modular and flexible way. UMTS will specify its services as independent modules, without requiring a minimum interdependent set of services to be present at all times. UMTS will enable stand-alone implementations of one service.

5.2.2. SERVICE ACCESS

There will be a uniform procedure for accessing a UMTS service in all different environments and sub-networks. A UMTS user will only need one subscription to UMTS to access services all over the public part of UMTS (i.e. the collection of all public UMTS networks) and a UMTS user will be billed by only one provider. Also, a UMTS user will be identified by means of one identifier, which will be location and environment independent. UMTS will support access to different service providers. It will also support the concept of telecommunications session, i.e. after a session has been opened, UMTS will allow the user to invoke several calls in sequence without terminating the session.

UMTS will provide the facilities for a user to determine what type of communication is possible by examining or querying network capabilities, profiles or through negotiation. Values, network or service provider parameters and the capture and release of facilities may be requested or negotiated for.

5.2.3. MODULAR DECOMPOSITION OF UMTS

The modular decomposition of UMTS is done for two main reasons. First, because it introduces a key separation of concerns when existing networks are studied for re-use in UMTS. Second, the decomposition reveals some functional aspects. The three modular parts are: the *Access Network (AN)*, the *Backbone Network (BN)* and the *Service Network (SN)*. This decomposition is depicted in Figure 15.

The AN provides mainly radio related functions, that is, the basic transmission and local switching functionality required in order to enable access of the MT onto the fixed network resources over the radio interface. The BN provides the basic (fixed network) switching infrastructure and network resources, that is, the call and connection control needed by UMTS. Finally, the SN provides service and mobility control. It also provides for data storage and manipulation. Network Management is provided by a (at least logically) separate Management Network (UMTS TMN), which will not be further considered. The service, access and backbone networks can be thought of as *modular network parts* in order to be distinguished from complete *network systems* (like UMTS, GSM, DCS1800).

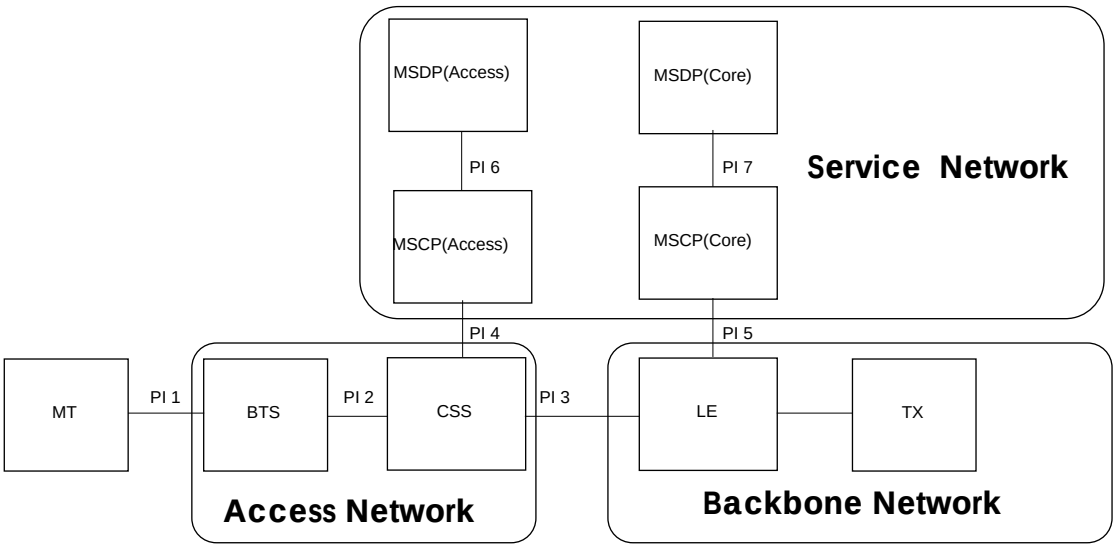

Figure 15: The UMTS Basic Modularity Model (BMM).

The UMTS Physical Entities are allocated in one of the identified networks. This decomposition will be referred as the UMTS Basic Modularity Model (BMM). The BMM is in reality a simplified Network Architecture, which will be used for the purposes of the study. The identified Physical Interfaces cater for the appropriate signaling transport (lower layer) functionality. The boundary between AN and SN is not always fixed. For example certain handover functions could be implemented in the AN as well as in the SN. Such issues will be resolved when the specific implementation options are considered. The PIs towards the management plane Network Entities are outside the scope of the study and have already been eliminated in Figure 15.

Taking the BMM (simplified NA) as a basis, we can focus only on the four remaining PIs. These are the Radio Interface (PI 1), the Backbone UNI (PI 3), the AN to SN Interface (PI 4) and the BN to SN interface (PI 5). These are the only relevant ones, since we are concentrating on the re-use of complete modularity network types.

6. MODELING MOBILE NETWORKS : SPECIFIC ASPECTS

Now we have examined the most important protocols in the mobile networking domain, we have to determine how we will model them, and how many of them will be modeled. As said in the introduction we have decided to limit ourselves just to one model, namely GPRS.

There are several reasons for this :

- GPRS is the newest developed mobile network, and, still fresh on the draft boards, hasn't been implemented yet. Obviously, people are working on the installation of new GPRS networks, but lacking any models suitable for simulation, this means that no reliable predictions can be done. The introduction of a reliable GPRS set of models should then prove important in this area
- GPRS is introduced within the GSM configuration, which means that already existing models can be used as basis for future development
- It will integrate IP networks on a mobile support, which is a major improvement on more traditional mobile network

6.1. MOBILE NETWORK MODELING

The relevant aspects of the Mobile networks to derive the signaling and data traffic are considered in the following paragraphs. These aspects are identified within the 2nd Generation Mobile networks that have provided a common basis for the mobility and traffic modeling activities. The 2nd Generation Mobile network framework identifies different user classes, services, geographical area types and environments. The following framework does not aim at completeness in the sense that all aspects are identified that possibly could influence the workload on the Mobile network, but aims at a practical approach to identify the most important aspects.

6.1.1. MOBILITY REFERENCE MODEL

The Mobility Reference Model consists of two parts. The first part describes the characteristics of the mobile user and the second part describes the effect of mobility on different signaling procedures.
The first part contains estimations for the density of users, average speed of users, penetration and user and terminal state probabilities. These data can be used as rough estimations if no real measurements of the geographical area are available.
The second part describes the effect of mobility on signaling by means of formulas that estimate the signaling rate of different procedures. Formulas to estimate the Location Updating and Handover signaling rates are provided.
The Mobility Reference Model thus enables us to estimate the triggering of different signaling flows in the Mobile network. To estimate the signaling load (e.g. Handover rates) the call behavior of the users, that is defined in the User Traffic Reference Model, needs to be taken into account.

6.1.1.1. USER CLASSES

The user classes that can be identified within the geographical area, are listed in Table 8.

User classes
Car passenger
Public transportation passenger
Pedestrian
Not moving

Table 8 : User classes.

The moving car passengers, public transportation passengers and pedestrians are assumed to be located in the outdoor environment. The not-moving people are assumed to be located in the indoor environment that could be a Business or Residential. Within the geographical area different geographical area types can be identified.

6.1.1.2.GEOGRAPHICAL AREA MODEL

The Geographical Area Model is a description of the geographical area for which an implementation of the Mobile network is considered. This description contains information that is specific for the geographical area and relevant for the implementation of the Mobile network in that area.
The information concerning the geographical area, that is required to determine the traffic impact on the Mobile network, is the *density* of users in different areas and the *crossing rate* at which these users enter or leave a particular area. The density and crossing rate of users has a direct impact on the signaling within the Mobile access network.
The following information concerning the geographical area is required:

- Density of potential Mobile users within the geographical area.
- The flow of users in the geographical area to derive the crossing rates.

The average number of incoming and outgoing pedestrians in an area are *estimated* by means of the density and average speed of pedestrians within the area. The rate of pedestrians crossing the area boundary can be estimated by means of the formulas:

$$\lambda_{ped}(MU) = L \cdot \frac{a_p}{b_p} \cdot \sigma_{MU} \cdot P_{ped} \cdot v_p \qquad (1)$$

Where,

λ_{ped}(MU): The pedestrian crossing rate (pedestrians/hour),
L: The perimeter of area *A* (km),
P_{ped}: The percentage of mobile users moving as pedestrians,
a_p: The percentage of the area A border length which corresponds to pedestrian crossings and pavements.
b_p: The percentage of the area around the border that is covered by pedestrian crossings and pavements.

σ_{MU}: The density of mobile users in the area around the borders (mobile users/Km^2),

v_p: The average pedestrian speed (Km/hour).

The crossing rates of cars and public transportation passengers are derived from the Vehicular Traffic Model, which provides detailed and accurate data. These are estimated according to equation (1).

Thus the car crossing rate will be:

$$\lambda_{car} = L \cdot \frac{a_c}{b_c} \cdot \sigma_{car} \cdot v_c \quad \text{(cars/hour)} \quad (2)$$

Where:

λ_{car}: The area A boundary, car crossing rate (cars/hour),

L: The perimeter of area *A* (km),

a_c: The percentage of the border length corresponding to streets.

b_c: The percentage of the area around the borders that is covered by streets,

σ_{car}: The car density around the border of area A (cars/Km^2).

v_c: The average car speed (Km/hour).

The Eq. (2) gives the estimation of the car crossing rate. However in mobile telecommunications we are interested in the car passenger crossing rate since car passengers are the possible users carrying a mobile terminal. For example, when a bus crosses the area boundary possibly more than one passenger carry a mobile terminal. The estimation of the car passenger crossing rate has to consider the car crossing rate and in addition the mean number of car passengers:

$$\lambda_{pas} = \lambda_{car} \cdot r_{pas} = L \cdot \frac{a_c}{b_c} \cdot \sigma_{pas} \cdot v_c \quad (3)$$

Where,

λ_{pas}: The crossing rate of car passengers (car passengers/hour),

σ_{pas}: The car passenger density in the area around the borders (car passengers/km^2),

r_{pas}: The mean number of passenger per car, i.e. $r_{pas}=\sigma_{pas}/\sigma_{car}$.

Since from the mobile telecommunications view point we are interested in the crossing rates of car passengers carrying a mobile terminal we are going to estimate the crossing rate of mobile users moving as car passengers:

$$\lambda_{pas}(MU) = L \cdot \frac{a_c}{b_c} \cdot \sigma_{pas} \cdot P_{MU} \cdot v_c \Rightarrow$$
$$\lambda_{pas}(MU) = L \cdot \frac{a_c}{b_c} \cdot \sigma_{MU} \cdot P_{pas} \cdot v_c \quad (4)$$

Where:

P_{MU}: The percentage of car passengers carrying a mobile terminal,

σ_{MU}: The density of mobile users in the area around the borders (mobile users/Km^2),

P_{pas}: The percentage of mobile users moving as car passengers.

6.1.1.3.LOCATION UPDATING

The Location Updating procedure is responsible for updating the location information of a mobile terminal. Location information is stored in a distributed data base and indicates a location area within which a mobile terminal roams. When a mobile terminal is called it is paged within the location area that the location information indicates. The output of paging phase is the cell area within which the called mobile terminal currently roams. Obviously location information should always be consistent so as to make all mobile terminals reachable. Therefore location updating procedure should be performed every time a mobile terminal moves from a location area to another.

Location updating takes place whenever a switched on mobile terminal changes location area. If P_{swn} is the probability that a mobile terminal is switched-on, then the location updating rate (λ_{lu}) referring to a given location area is:

$$\lambda_{lu} = P_{swn} \cdot \left[\lambda_{pas}(MU) + \lambda_{ped}(MU)\right] \qquad (5)$$

6.1.1.4.HANDOVER

Handover is the procedure responsible for supporting the service provision continuity to moving mobile terminals. When a busy mobile terminal moves from a cell area to another, then handover procedure is applied so as to establish a wireless connection between the terminal and the base station covering the new cell area. This happens because the wireless connection between the terminal and the base station of the originating cell becomes weak. Note that small size cells will increase the signaling requirements due to handover. As it can be noticed the rate of handovers related to a single cell area is in fact the cell border crossing rate of busy mobile terminals.

Handover takes place whenever a busy mobile terminal crosses a cell boundary. If T_c and T_p are the traffic per mobile terminal (in Erlangs) for cars and pedestrians respectively, then the handover rate (λ_{hr}) referring to a given cell area is:

$$\lambda_{hr} = \lambda_{pas}(MU) \cdot T_c + \lambda_{ped}(MU) \cdot T_p \qquad (6)$$

6.1.2. USER TRAFFIC REFERENCE MODEL

The User Traffic Reference Model describes the traffic characteristics of different services used by different user classes within different geographical areas during the busy hour. The parameters contained within the User Traffic Reference Model are:

- bhc: Average number of successful calls per service per user during the busy hour including both incoming and outgoing calls (calls/h.).
- dur : Average holding time of a call (sec.).
- vol : Average number of bytes of user information exchanged during a call.

pr : Service penetration rate indicating the percentage of users that is subscribed to the specific service.

From the User Traffic Reference Model the traffic requirements of the users can be derived. The user traffic requirements are input for the radio coverage model to determine the radio cell layout in the geographical area.
The traffic generated by user u in geographical area g expressed in number of equivalent telephony Erlang is calculated as:

$$ETE_{u,g} = \sum_{s} pr_{s,u,g} \cdot \frac{bhc_{s,u,g} \cdot dur_{s,u,g} \cdot band_{s}}{3600 \cdot band_{tele}} \quad (7)$$

Where:

$ETE_{u,g}$: Generated traffic in geographical area g by a user of class u (ETE/user).

$pr_{s,u,g}$: Service penetration rate of service s for user class u whiting geographical area g.

$bhc_{s,u,g}$: Average number of successful calls for service s per user of class u in geographical area g during the busy hour including both incoming and outgoing calls (calls/h.).

$dur_{s,u,g}$: Average holding time for a call of service s for user class u in geographical area g (sec.).

$band_{s}$: Bandwidth requirement of service s.

$band_{tele}$: Bandwidth requirement of plain telephone service.

6.1.3. RADIO COVERAGE MODEL

The radio coverage of the geographical area determines the coverage of the total service area by means of Micro and Macro cells. The radio coverage model determines the location and coverage area of the radio cells in the geographical area.
The actual cell planning of the 2nd generation mobile networks entail much detail and complexity that will be treated in the workload modeling methodology in a simplified way. The intention of the radio coverage activity is not to provide a detailed cell planning method, but to provide a simple but realistic cell layout that satisfies the traffic requirements of the expected user densities.
The Micro cells are applied within a city environment to cover areas with a high density of vehicle and pedestrian traffic. The Macro cells are used to provide wide area cellular coverage. It is assumed that the radio propagation requirements can be met within the range of coverage as listed in Table 9.

Radio cell	Geographical area	Range of coverage area
Macro cell	Metropolitan/Urban/ Suburban/Rural	Radius 1 - 20 km.
Micro cell	Metropolitan/Urban/ Suburban/Rural	Radius 100 – 1,000 m.

Table 9 : Geographical area and range of coverage areas of radio cells in GPRS

In the workload modeling methodology the actual coverage area of a radio cell is determined by the expected *traffic demand* provided that the coverage area stays within the range defined in Table 9. The traffic demand is determined by the expected user density and the traffic characteristics of the users. The expected number of users and their traffic characteristics limit the actual coverage area of a cell. The *traffic capacity* expresses the maximum amount of traffic a radio cells can support. Thus the radio coverage model determines the cell layout that satisfies the traffic demand in the geographical area.

6.1.4. NETWORK TOPOLOGY

The Network topology determines the interconnection of the Physical Entities of the Network Architecture. The Network topology defines the links between the Physical Entities allocated in the geographical area by the System Area dimensioning. As such the network topology also implicitly reflects the allocation of functionality in the network. The network topology may be implemented according to some network configuration pattern e.g. bus, ring or star configuration.
The Network topology can be evaluated taking into account the costs associated with different interconnection patterns and the resulting signaling flows.

6.1.5. MOBILE SIMULATION SCENARIO

Summarizing the analysis about Mobile Network Modeling, the parameters that determine a mobile simulation scenario will be presented. First the network topology of a proposed simulation scenario should be described. Then the following constant or variable values should be specified:

- The total number of network subscribers.
- The percentage of users are switched on
- The rate of Switch on/off per Mobile Station per day.
- Location area characteristics :
    - L: the perimeter of area A.
    - a_p:The percentage of the area A border length which corresponds to pedestrian crossings and pavements.
    - b_p:The percentage of area around the border that is covered by pedestrian crossings and pavements.
    - A_c:The percentage of the border length corresponding to streets.
    - B_c:The percentage of the area around the border that is covered by streets,
    - σ_{MU}:The density of mobile users in the area around the border (mobile users/Km^2),

- The percentage of moving users
    - The percentage of moving users moving as pedestrians.
    - The percentage of moving users moving car passenger.

- The average pedestrian user velocity
- The average car passenger user velocity

Using the above parameter values and the formulas presented in section 1.1.1, the mobility management traffic load that introduced in a mobile access network can be estimated.

From the user profile description can be derived the following parameters values:

- λ_{cs} the average number of "sessions" for service per user including both incoming and outgoing
  (sessions/h.).
- The service penetration rate (The percentage of service usage)
- The average amount of data transfer per call per service.

Using these parameter values and the formula presented in the User Traffic Model paragraph (see 1.1.2), the signaling traffic load and the user data traffic can be estimated.

6.1.5.1.PARAMETERS VALUES

The objective of the aforementioned parameter values is to define a potential simulation scenario. The network designer sets values to these parameters according to the simulation needs. However, reference values for these parameters have been published either from real measurements or from theoretical studies. In the following table, real measurements concerning car movements in Helsinki, which have been taken during the RACE project, are presented.

Urban	**Area Radius**	300 m	500 m	700 m
A_C	Mean Value Variance	0.06505 0.00896	0.05251 0.00562	0.04272 0.00444
B_C	Mean Value Variance	0.11156 0.2040	0.09708 0.00593	0.08348 0.00431
σ_{car}	Mean Value Variance	467.332 76.539	409.881 30.495	368.131 25.634
V_C	Mean Value Variance	30.0533 0.0170	29.45171 0.02085	28.1789 0.02060

Table 10: Mean value and variance of the parameters used by the theoretical formula for car crossing rate, in the case of an urban area (Helsinki).

6.2. GPRS SIMULATION SCENARIO CONFIGURATION

In the following figure, the configuration of the GPRS network that will be implemented for the BISANTE simulation prototype is presented.

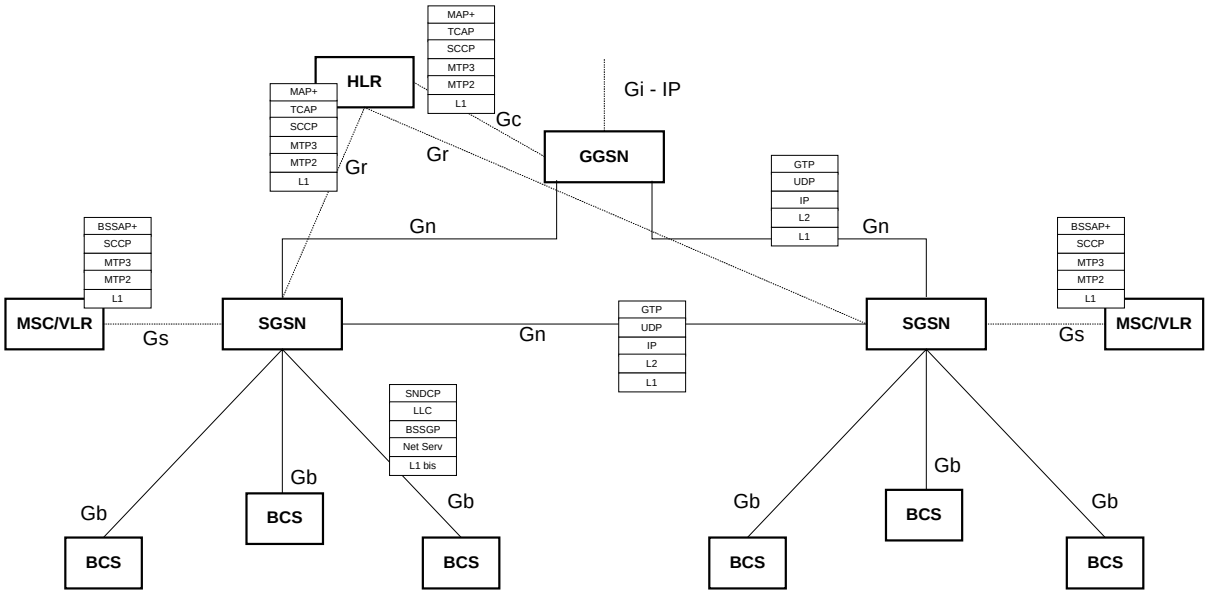

Figure 16: GPRS simulation scenario configuration

6.3. TRAFFIC SOURCES FOR GPRS

For the GPRS simulation scenario in the BISANTE prototype two kinds of traffic sources are going to be implemented:

- The payload traffic sources that will generate data traffic according to the applications which are supported by the GPRS network.

- The signaling traffic sources that will generate signaling traffic according to the signaling procedures which are defined in the GPRS network.

6.3.1. PAYLOAD TRAFFIC SOURCES

The payload traffic sources for the GPRS access network will be the same with the corresponding terrestrial traffic sources for terrestrial networks. The mobile and terrestrial traffic sources have the same structure and operation because if both users employ exactly the same applications, then these applications have the same characteristics. Of course, the radio bandwidth restrictions and Mobile Station limitations confine the variety of mobile applications. The services that will be supported by the GPRS network in the BISANTE prototype are www, Ftp, E-mail, Telnet and Audio-conference.

The profiles of the mobile users can be easily derived from the profiles of the terrestrial uses. The service penetrations are the same in both cases and some discrepancies are applied regarding the mobile simulation scenario.

6.3.2. SIGNALING TRAFFIC SOURCES

The signaling traffic sources for the GPRS access network will generate signaling message sequences according to the mobility management procedures and Packet Routing functions which are defined for the GPRS network. These message sequences are presented in the following paragraphs.

6.3.2.1.MOBILITY MANAGEMENT

The mobility management activities in a GPRS access network is described by three different Mobility Management (MM) states in Mobile Station (MS) and SGSN. These are:

- IDLE: The Mobile Station (MS) is not known by the network. Point to point data transfer is not possible. If the MS wants to send or receive data the MS have to perform a GPRS attach procedure.

- STANDBY: MS is known on the Routing area level and the MS informs the SGSN when changing Routing Areas. If a mobile originated data transfer is initiated the MS enter the READY state. The MS is possible to be paged from the network and when a mobile terminated data transfer is initiated the state is changed to READY.

- READY: MS is known on a cell level and the MS informs the SGSN when changing cells. Point to point data transfer may occur. In this state the Mobile Station may have radio resources.

The transitions between the different states are:

- IDLE to READY: GPRS Attach procedure is performed to establish a logical link between MS and SGSN.

- READY to STANDBY: The READY timer expire or the MS is forced to STANDBY.

- STANDBY to READY: PDU transmission is either a mobile originated data transfer or an answer to a paging message for a mobile terminated data transfer.

- READY to IDLE: GPRS Detach procedure.

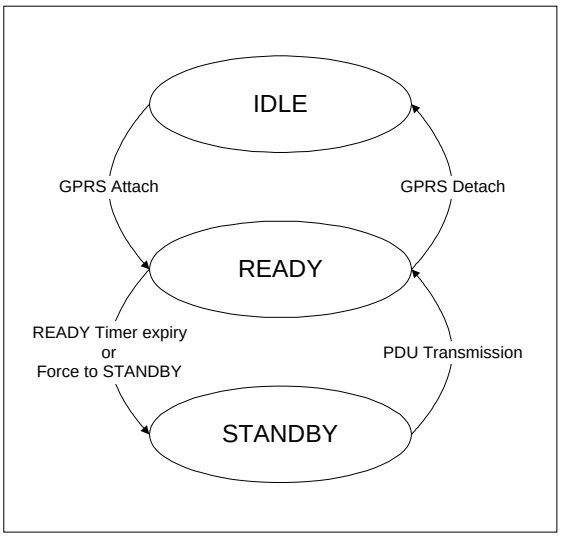

Figure 17: Mobility Management States of Mobile Station

6.3.2.1.1.GPRS ATTACH

In order to access the GPRS services, an MS shall first make its presence known to the network by performing a GPRS attach. This operation establishes a logical link between MS and SGSN. This procedure is related with the frequency that a GPRS subscriber opens his Mobile Stations. The rate that a GPRS attach procedure is performed, is the rate of switching-on per Mobile Station per day (see section 1.2.5).

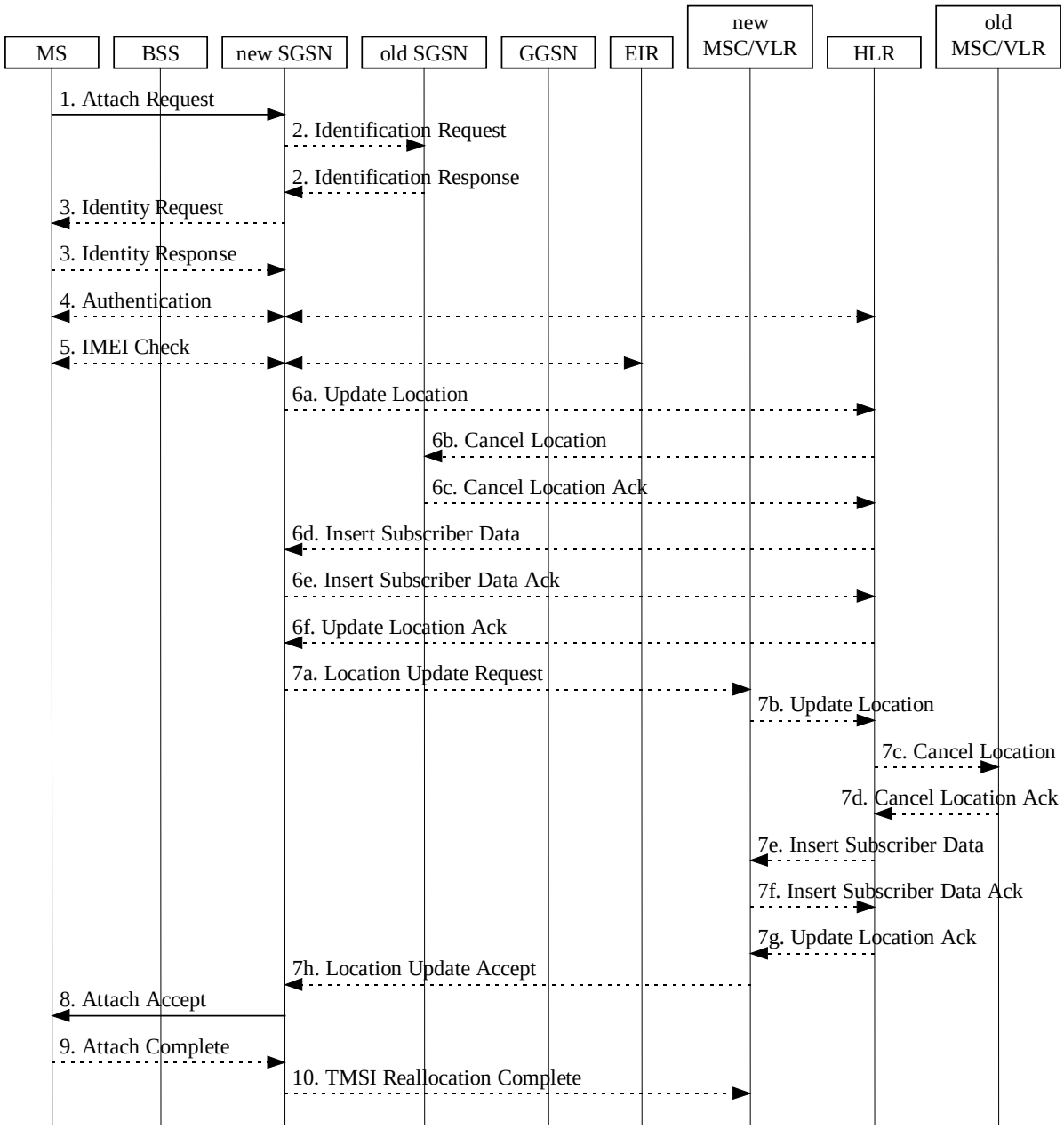

Figure 18: Combined GPRS / IMSI Attach Procedure

6.3.2.1.2.GPRS DETACH

The GPRS Detach function occurs when either the MS or the SGSN wants to detach the GPRS service. This procedure is related with the frequency that a GPRS subscriber closes his Mobile Stations. The rate that a GPRS detach procedure is performed, is the rate of switching-off per Mobile Station per day (see section 1.2.5).

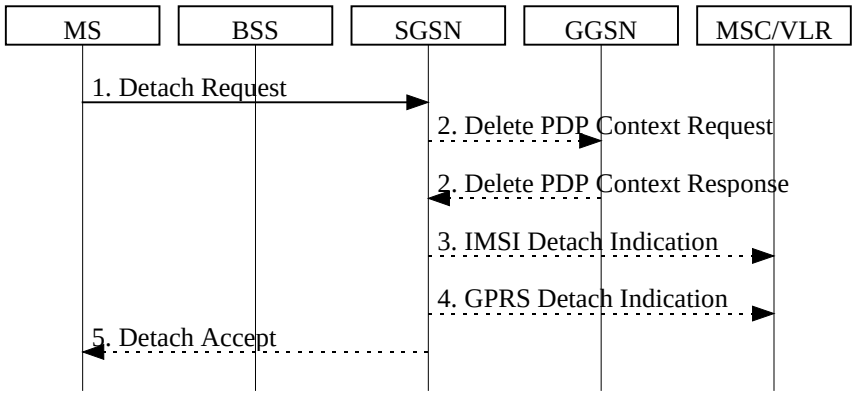

Figure 19: MS-Initiated Combined GPRS / IMSI Detach Procedure

6.3.2.1.3.CELL UPDATE AND ROUTING AREA UPDATE

The location management functions provide procedures for cell and routing area update. A routing area (RA) consists of one or more cells and is the area for paging. A routing area is equal to or a subset of a Location Area.

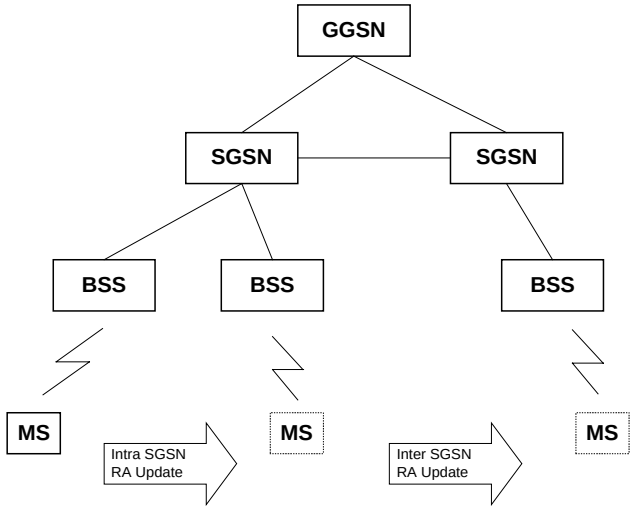

Figure 20: Intra & Inter SGSN Routing Area Update

- **Cell Update Procedure**

When an MS changes cells within a RA the MS performs a Cell Update by sending the identity to the SGSN and the BSS adds the Routing Area Identity.

- **Routing Area Procedure**

When an MS changes Routing area a Routing Area Update procedure is performed to inform the SGSN about the new RA.

If the change of RA takes place within a SGSN it is a Intra SGSN RA update and if the new RA is connected to a new SGSN it is an inter SGSN RA Update.

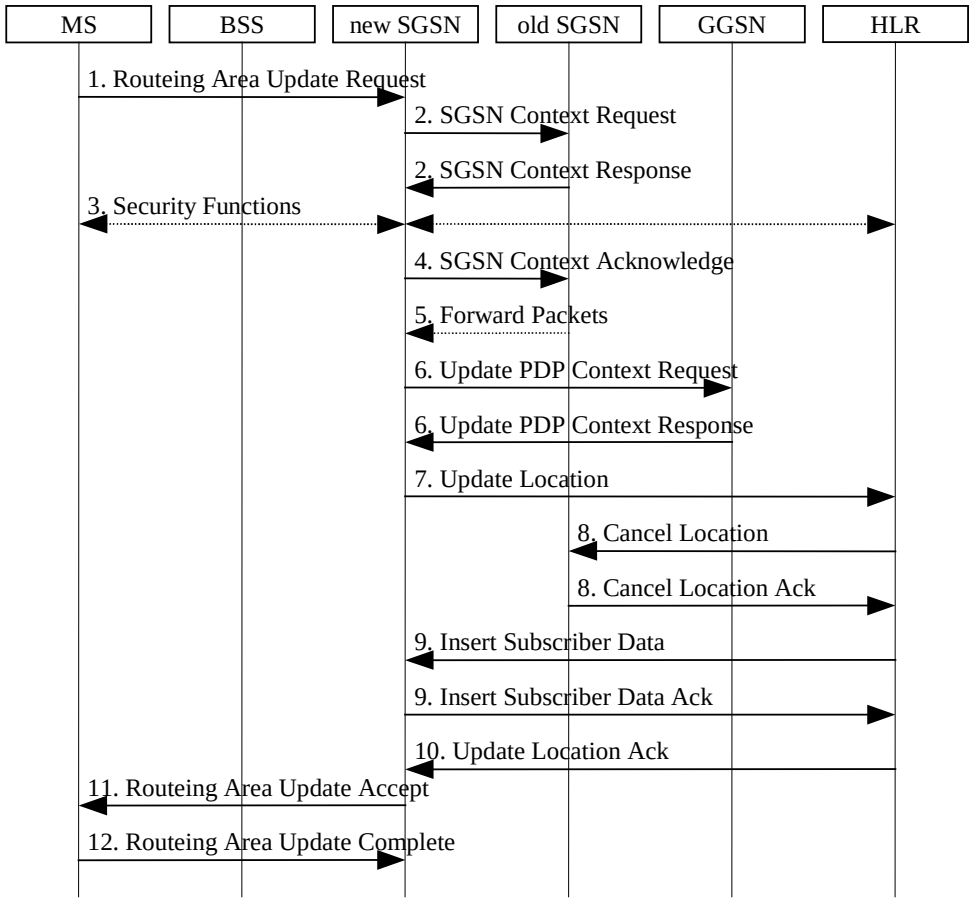

Figure 21: Inter SGSN Routing Area Update Procedure

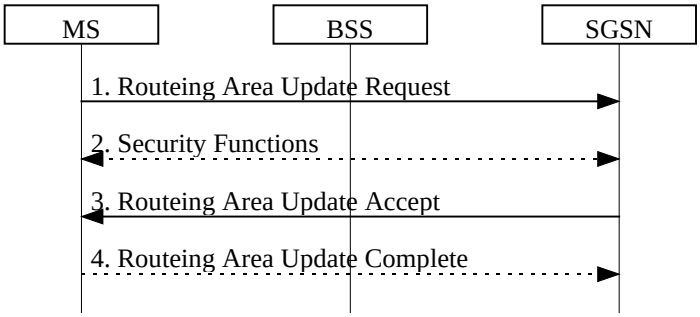

Figure 22: Intra SGSN Routing Area Update Procedure

In order to calculate the rate that the Intra SGSN RA procedure is performed in a given Area A that is covered by a unique BSS, we have to use the formula (5) (see section 1.2.5)of location update rate estimation.

$$\lambda_{lu} = P_{swn} \cdot \left[\lambda_{pas}(MU) + \lambda_{ped}(MU) \right]$$

From the above parameters the probability P_{swn} is known from the simulation scenario parameters. So, we have to estimate the rates of the pedestrians and passengers crossing the

borders of area's A. To be able to estimate the two rates, λ_{ped} λ_{pas}, it is necessary to have the values of:

L:	The perimeter of area *A* (km),
P_{ped}:	The percentage of mobile users moving as pedestrians,
a_p:	The percentage of the area A border length which corresponds to pedestrian crossings and pavements.
b_p:	The percentage of the area around the border that is covered by pedestrian crossings and pavements.
σ_{MU}:	The density of mobile users in area A (mobile users/Km^2),
v_p:	The average pedestrian speed (Km/hour).
a_c:	The percentage of the border length corresponding to streets.
b_c:	The percentage of area A covered by streets,
σ_{car}:	The car density around the border of area A (cars/Km^2).
v_c:	The average car speed (Km/hour).
P_{MU}:	The percentage of car passengers carrying a mobile terminal,
σ_{MU}:	The density of mobile users in area A (mobile users/Km^2),
P_{pas}:	The percentage of mobile users moving as car passengers.

Using the above estimation steps and defining an Area B that is covered by an SGSN, we can estimate the rate that the Inter SGSN RA Update procedure is performed in this area.

6.3.2.2.PACKET ROUTING

The packet data transfer in the GPRS access network is accomplished using the Packet Data Protocol PDP. The PDP has two states: The inactive state and the active state.

In the INACTIVE state no data can be transferred. The PDP context contains no routing or mapping information to process PDUs related to that PDP address. A changing location of a subscriber causes no update for the PDP context in INACTIVE state even if the subscriber is attached to the GPRS MM.

The MS initiates the movement from INACTIVE to ACTIVE state by initiating the PDP Context Activation procedure.

In the ACTIVE state, the PDP context for the PDP address in use is activated in MS, SGSN and GGSN. The PDP context contains mapping and routing information for transferring PDUs for that particular PDP address between MS and GGSN. The PDP state ACTIVE is permitted only when the mobility management state of the subscriber is STANDBY or READY.

An active PDP context for an MS is moved to INACTIVE state when the deactivation procedure is initiated.

All active PDP contexts for an MS are moved to INACTIVE state when the MM state changes to IDLE.

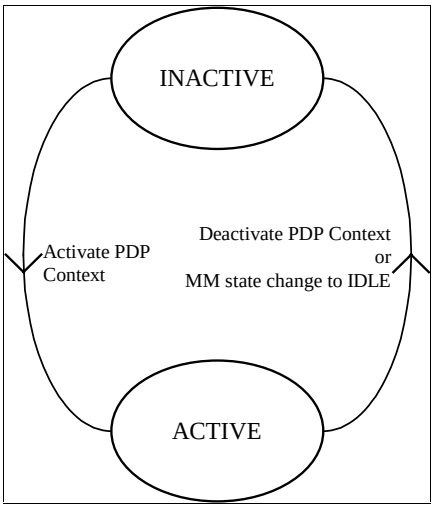

Figure 23: Functional PDP State Model

6.3.2.2.1.ACTIVATE PDP CONTEXT

When this procedure is performed, is activated the MS access to a Packet data network via the GGSN. The MS may be authenticated by the access provider.

The rate that an Activate PDP Context procedure is performed is related with the cumulative number of "sessions" are originated or terminated to the Mobile Station for all the services which are supported. If a GPRS subscriber uses a, b, c different services with

λ_{ca} the average number of "sessions" for service a per user (sessions/h.).
λ_{cb} the average number of "sessions" for service b per user (sessions/h.).
λ_{cc} the average number of "sessions" for service c per user (sessions/h.).

and with penetration

Pen_a Penetration of service a
Pen_b Penetration of service b
Pen_c Penetration of service c

The Rate of Activate PDP Context

$\lambda_{Act\_PDP\_Cntx} = (\lambda_{ca} * Pen_a) + (\lambda_{cb} * Pen_b) + (\lambda_{cc} * Pen_c)$

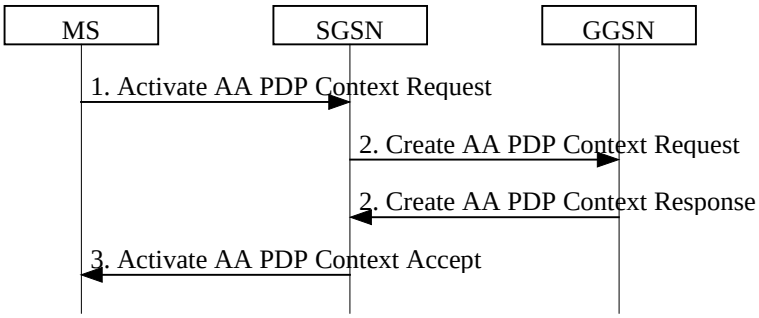

Figure 24: PDP Context Activation Procedure

6.3.2.2.2.DEACTIVATE PDP CONTEXT

This procedure terminates the access to a Packet Data Network. The rate that the Deactivate PDP Context is performed is the same with the rate of the Activate PDP Context procedure.

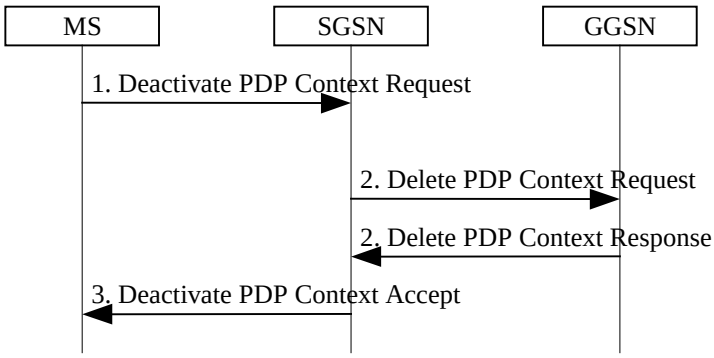

Figure 25: PDP Context Deactivation Initiated by MS Procedure

7. CONCLUSION

In this document, we have examined the most important mobile network protocols, and determine which of their characteristics should have impact on the upper layers, and more particularly, on the applications and users that started them. This survey has spanned the following range :

- Wireless LANs : 802.11 standard and the more recent HiperLAN
- Second generation of mobile networks : DECT and GSM
- The GPRS technology
- A presentation of the third generation of mobile networks with the UMTS protocol

Once this characterization work had been done, we had to think how to use them in our models. Although some mechanisms (e.g. queuing) can be modeled for mobile networks the same way they are modeled for other networks, mobile networks have still their own features that require adapted techniques. The features we identified include :

- The description of the population of users and their geographical repartition,
- The laws and formulas describing the traffic and moving of these users,
- How the users' mobility influence the network functionalities, and
- How this mobility influence also the topology of the network.

Once these characteristics were properly described, we provided means to calculate their impact on network performances.

We included also a short description of scenarios that will be used as basis for the development and testing of our models in the future. However, although we describe the modeling techniques and how they will be used to build the models of the network we selected, modeling per se is beyond the scope of this document, and will be treated in WorkPackage 3.

ANNEXE A : ABBREVIATIONS

ATM	Asynchronous Transfer Mode
AUC	Authentication Center
BCCH	Broadcast Control Channel
BG	Border Gateway
BSC	Base Station Controller
BSS	Base Station Subsystem
BSSAP	Base Station System Application Part
BSSAP+	Base Station System Application Part +
BSSGP	Base Station System GPRS Protocol
BSSMAP	Base Station System Management Application Part
BTS	Base Transceiving Station
BTSM	Base Transceiving Station Management
CA	Cell Allocation
CC	Call Control
CCCH	Common Control Channel
CCU	Channel Codec Unit
CGI	Cell Global Identification
CHAP	Challenge Handshake Authentication Protocol
CS	Circuit Switched
DCN	Data Communication Network
DHCP	Dynamic Host Configuration Protocol
DNIC	Data Network Identification Code
DNS	Domain Name System
DTAP	Direct Transfer Application Part
FDMA	Frequency Division Multiple Access
FEC	Forward Error Correction
GGSN	Gateway GPRS Support Node
GMM/SM	GPRS Mobility Management and Session Management
GMSC	Gateway MSC
GMSK	Gauss Minimum Shift Keying
GSC	GSM Speech Codec
GSN	GPRS Support Node
GTP	GPRS Tunneling Protocol
HDLC	High Level Data Link Control
HLR	Home Location Register
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISP	Internet Service Provider
LAI	Local Area ID
LAP	Link Access Procedure
LAPB	Link Access Protocol Balanced
LLC	Logical Link Control

LL-PDU	LLC PDU
MAC	Medium Access Control
MAP	Mobile Application Part
MCC	Mobile Country Code
MNC	Mobile Network Code
MM	Mobility Management
MS	Mobile Station
MSC	Mobile Switching Center
MSISDN	Mobile Station ISDN Number
MSRN	Mobile Station Roaming Number
MT	Mobile Terminal
MTP	Message Transfer Part
MTP2	Message Transfer Part layer 2
MTP3	Message Transfer Part layer 3
NGAF	Non-GPRS Alert Flag
NS	Network Service
NSAPI	Network layer Service Access Point Identifier
NSS	Network SubSystem
NTP	Non-Transparent Protocol
OMC	Operation and Management Center
PCM	Pulse Code Modulation
PCU	Packet Control Unit
PDCH	Packet Data CHannel
PDN	Packet Data Network
PDP	Packet Data Protocol, e.g., IP or X.25
PDU	Protocol Data Unit
PIN	Personal Identification Number
PLMN	Public Land Mobile Network
PNIC	Pseudo Network Identification Code
PSDN	Packet Switched Data Network
PSPDN	Packet Switched Public Data Network
PTM	Point To Multipoint
PTP	Point To Point
PVC	Permanent Virtual Circuit
RA	Routing Area
RAC	Routing Area Code
RAI	Routing Area Identity
RLC	Radio Link Control
RLP	Radio Link Protocol
RPE-LTP	Regular Pulse Excitation-Long Term Prediction
RR	Radio Resource Management
RRM	Radio Resource Management
SAP	Service Access Point
SCCP	Signaling Connection Control Part
SGSN	Serving GPRS Support Node
SIM	Subscriber Identity Module
SM	Short Message
SMS	Short Message Service
SM-SC	Short Message - Service Center
SMS-GMSC	Short Message Service Gateway MSC

SMS-IWMSC	Short Message Service Interworking MSC
SNDC	SubNetwork Dependent Convergence
SNDCP	SubNetwork Dependent Convergence Protocol
SN-PDU	SNDCP PDU
SS7	Signaling System Number 7
TCAP	Transaction Capabilities Application Part
TCH	Traffic Channel
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
TE	Terminal Equipment
TEI	Terminal Equipment Identifier
TETRA	Trans European Trunked Radio
TID	Tunnel Identifier
TLLI	Temporary Logical Link Identity
TMSI	Temporal Mobile Subscriber Identity
TRAU	Transcoder and Rate Adaptor Unit
UDP	User Datagram Protocol
VLR	Visited Location Register

ANNEXE B : BIBLIOGRAPHY

- **Wireless LANs :**

For a detailed list of references see: http://www.cis.ohio-state.edu/~jain/refs/wir_refs.htm

E. Prem, "*Wireless Local Area Networks*," Aug 97, http://www.cis.ohio-state.edu/~jain/cis788-97/wireless_lans

I. Brodsky, "*Wireless Computing*," Van Nostrand Reinhold, 1997.

R. A. Dayem, "*Mobile Data & Wireless LAN Technologies,*" Prentice-Hall, 1997

J. Ahmadi, et al, "*Design Issues in Wireless LANs,*"

J. of High Speed Networks, 1996, pp 87-104

R. LaMaire, et al, "*Wireless LANs and Mobile Networking: Standards and Future Directions,*" IEEE Communications Magazine, August 1996, pp. 86-94, http://www.comsoc.org/pubs/ci/comsoc/

- **DECT :**

ETS 300 175-1 to 175-8 : "Radio Equipment and Systems (RES); Digital European Cordless Telecommunications (DECT) "

- **GSM :**

Eberspächer, Jörg. *GSM, Global System for Mobile Communication*, Teubner Verlag, Stuttgart, 1997.

Mouly, Michel. *The GSM system for mobile communications*, Lassay-les-Châteaux, Europe Media Duplication, 1993.

Walke, Bernhard. *Mobilfunknetze und ihre Protokolle*, Teubner Verlag, Stuttgart, 1998.

Jan A. Audestad. *Network aspects of the GSM system*. In EUROCON 88, June 1988.

D. M. Balston. *The pan-European system: GSM*. In D. M. Balston and R.C.V. Macario, editors, Cellular Radio Systems. Artech House, Boston, 1993.

M. Feldmann and J. P. Rissen. *GSM network systems and overall system integration*. Electrical Communication, 2nd Quarter 1993.

Thomas Haug. *Overview of the GSM project*. In EUROCON 88, June 1988.

- **UMTS :**

Stanley Chia,"*The Universal Mobile Telecommunication System"*, IEEE Communication Magazine, Dec 1992

Joseph C. S. Cheung et all,"*Network Planning for Third–Generation Mobile Radio Systems"*, IEEE Communication Magazine, Nov 1994

Raymond Steele,"*The Evolution of Personal Communication"*, IEEE Personal Communications, Second Quarter 1994

Juha Rapeli,"*UMTS: Target, System Concept, and Standardization in a Global Framework"*, IEEE Personal Communication, Febr 1995

B.G. Marchent et al.: Integration of UMTS and BISDN protocols with utilisation of ATM for information transport. RACE Mobile Summit, Cascais, Portugal, November 1995.