BSc in Computer Engineering
CMP4204
Wireless Technologies

Lecture 08

2G, GSM, CDMA and GPRS Cellular Mobile

Eng Diarmuid O'Briain, CEng, CISSP

Department of Electrical and Computer Engineering,
College of Engineering, Design, Art and Technology,
Makerere University

Table of Contents

Illustration Index

1. Multiple Access Methods

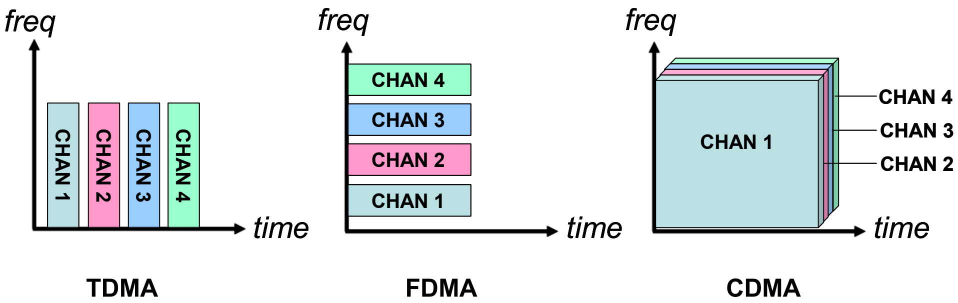


Illustration 1: Multiple access methods

Illustration 1 shows the three main multiple access methods.

The first diagram demonstrates division of channels by time. Each channel is allotted a period of time where the complete portion of the spectrum is available to it, this is Time Division Multiple Access (TDMA).

In the second diagram division of the portion of spectrum is by frequency, each channel is allocated a portion of the available frequency range on a constant basis. This is Frequency Division Multiple Access (FDMA).

Code Division Multiple Access (CDMA) means each channel has all the available portion of bandwidth all of the time. How can that be ? Well each channel is separated from each other by the application of a code. Receiving devices listen for the coded traffic for it and ignores all other traffic on the channel as noise. It is this method of Access the remainder of this document will concentrate.

1.1 Global System for Mobile Communications (GSM)

The access method chosen for Global System for Mobile Communications (GSM) is a combination of Time and Frequency Division Multiple Access (TDMA/FDMA). The FDMA part involves the division by frequency of the (maximum) 25 MHz bandwidth into 124 carrier frequencies spaced 200 kHz apart. One or more carrier frequencies are assigned to each base station. Each of these carrier frequencies is then divided in time, using a TDMA scheme.

1.2 CDMA2000 and CdmaOne

CdmaOne was the first mobile system to employ CDMA Spread Spectrum standardised as Interim Standard 95 (IS-95) in the USA. It was supplanted by IS-2000 or CDMA2000 which is also a CDMA-based standard.

2. Spread Spectrum

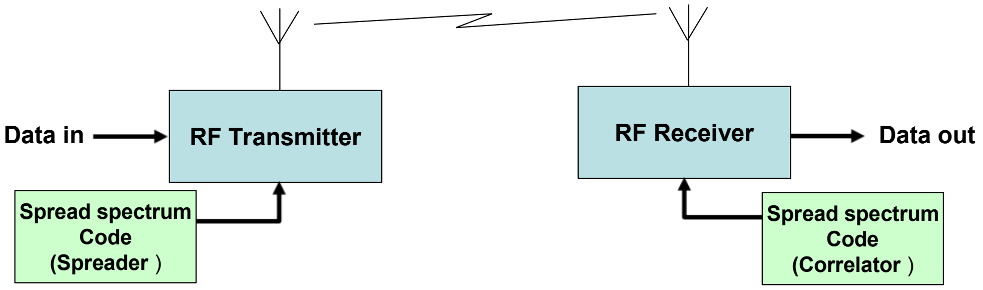

Data in
RF Transmitter
Spread spectrum Code (Spreader)
RF Receiver
Data out
Spread spectrum Code (Correlator)

Illustration 2: Spread spectrum

Spread spectrum uses wide band signals which are noise like in nature. Spread spectrum signals use codes that run many times the information bandwidth or data rate. These special "Spreading" codes are called "Pseudo Random" or "Pseudo Noise" codes. They are called "Pseudo" because they are not real Gaussian noise.

Spread spectrum transmitters use similar transmit power levels to narrow band transmitters but because spread spectrum signal bandwidth is so wide, they transmit at a much lower overall spectral power density (Watts/Hertz), than narrowband transmitters whose frequency spectrum is obviously much more narrow. This lower transmitted power density characteristic means that spread and narrow band signals can occupy the same band, with little or no interference.

Because of the noise like characteristic of spread spectrum signals they have a number of advantages over narrow band signals:

- Hard to detect.
- Harder to jam.

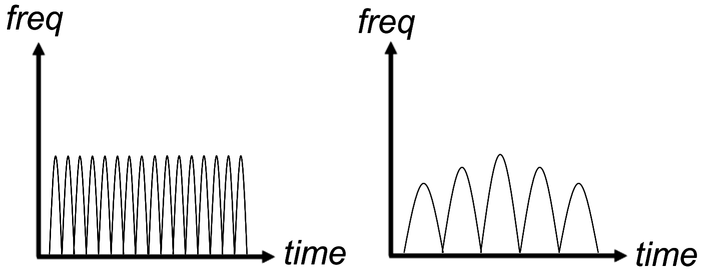
2.1 Spread spectrum characteristics

A spread spectrum signal will meet the following criteria:

- The transmitted signal bandwidth is much greater than the information bandwidth.
- Some function other than the information being transmitted is employed to determine the resultant transmitted bandwidth.

To apply spread spectrum, simply inject the corresponding spread spectrum code somewhere in the transmitting chain before the antenna. (That injection is called the spreading operation.) The effect is to diffuse the information in a larger bandwidth. Conversely, you can remove the spread spectrum code (dispreading operation) at a point in the receive chain before data retrieval. The effect of a dispreading operation is to reconstitute the information in its original bandwidth. Obviously, the same code must be known in advance at both ends of the transmission channel.

2.2 Spread spectrum methods



Frequency Hopping **Direct Sequence (DS)**

Illustration 3: Spread spectrum methods

Spread spectrum systems transmit an RF signal bandwidth as wide as 20 to 250 times the bandwidth of the information being sent. Some spread spectrum systems have employed RF bandwidths 1000 times their information bandwidth.

Spread spectrum systems fall under three general types:

- Frequency hopping.
- Direct sequence.
- Hybrid.

2.2.1 Frequency Hopping

In a frequency hopping system the transmitter hops from frequency to frequency over a wide band. The specific order of these hops is a function of a code sequence, and the hopping rate is a function of the information rate. The transmitted spectrum of a frequency hopping signal is demonstrated in the figure. The transmitter output is flat over the band of frequencies used with the bandwidth of a frequency hopping signal:

- $w * F$ slots
    - where w is the bandwidth of each hop channel.

2.2.2 Direct Sequence

Direct sequence spread spectrum systems have a high speed code sequence, along with the basic information being sent, to modulate their RF carrier. The high speed code sequence is used directly to modulate the carrier, thereby directly setting the transmitted RF bandwidth. Binary code sequences as short as 11 bits or as long as (289 – 1) have been employed for this purpose, at code rates from under a bit per second to several hundred megabits per second. The main lobe of this spectrum has a bandwidth twice the clock rate of the modulating code. The side lobes have a bandwidth equal to the code's clock rate.

2.3 CDMA Spreading

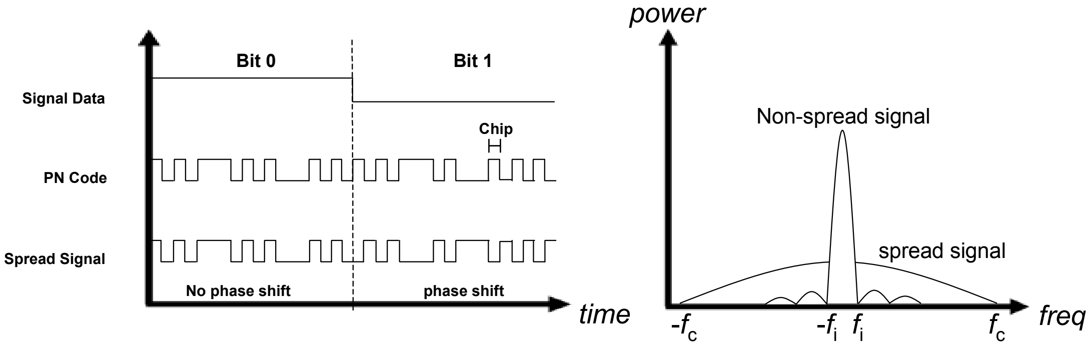


Illustration 4: CDMA Spreading

CDMA makes use of this spread spectrum technique, using spreading codes, which spreads the baseband data before transmission. The Spreader function generates a pseudo noise code (PN). This code has the following properties:

- It must be deterministic so the receiving station can independently generate the code to match that used by the transmitting station.
- It must appear random to a listener without prior knowledge of the code. It has the apparent properties of sampled white noise.
- The cross-correlation between any two codes must be small.
- The code must have a long period before the code repeats itself.

The pseudo noise codes bit rate is known as the chipping rate or chipping frequency (fc) while the signal data is known as the information rate (fi). The signal data modulates the pseudo noise code as is demonstrated in the first diagram above. The second diagram demonstrates the process of frequency spreading. The bandwidth of a digital signal is twice its bit rate. The bandwidths of the information data (fi) and the PN code are shown together. The bandwidth of the combination of the two is approximately the bandwidth of the PN code.

So: $fc + fi \approx fc \text{ as } fc >> fi$

The resultant coded signal next modulates an RF carrier for transmission using Quadrature Phase Shift Keying (QPSK). QPSK uses four different states to encode each symbol. The four states are phase shifts of the carrier spaced 90° apart. By convention, the phase shifts are 45°, 135°, 225°, and 315° degrees. Since there are four possible states used to encode binary information, each state represents two bits. This two bit “word” is called a symbol.

2.4 CDMA Gain

Processing Gain (*Gp*) is the theoretical system gain that results from the spreading effect. This gain is also known as the Spreading Factor and is given by:

- $Gp = fc / fi$

This high gain gives the system the following advantages:

- Interference rejection: the ability of the system to reject interference is directly proportional to *Gp*.
- System capacity: the capacity of the system is directly proportional to *Gp*.

So the higher the PN code bit rate which means the greater the available bandwidth, the better the system performance. Spreading Factor is the ratio of the chips (i.e. 3.8 Mchips/s) to the baseband information rate. These Spreading factors vary typically from 4 to 512.

So for example:

- $Gp = 3.8\ Mchips/s / 15\ K\ Symbols/s = 3800000 / 15000 = 253$

This spreading process gain can also be expressed in *dB*s.

- $10log(253) = 24dB$ gain.

2.5 Power Control

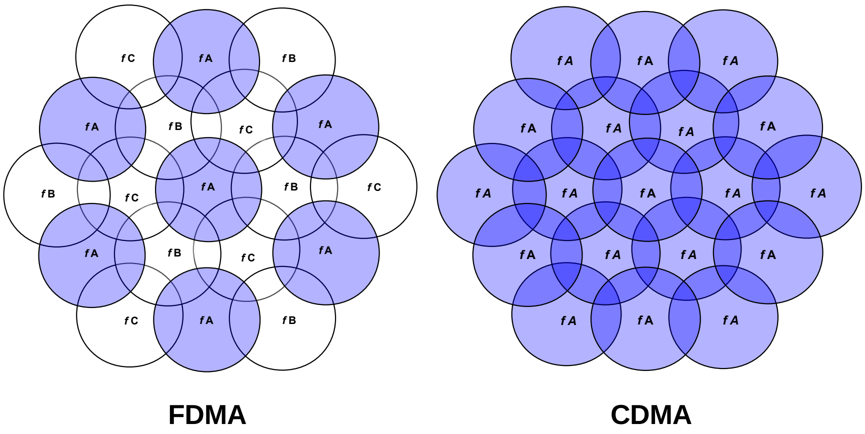
CDMA is interference limited multiple access system. All users transmit on the same frequency; internal interference generated by the system is the most significant factor in determining system capacity and call quality. The transmit power for each user must be reduced to limit interference, however, the power should be enough to maintain the required energy per bit to noise power spectral density ratio *Eb/No* (SNR ratio) for a satisfactory call quality. Maximum capacity is achieved when *Eb/No* of every user is at the minimum level needed for the acceptable channel performance. As the Mobile Station (MS) moves around, the RF environment continuously changes due to fast and slow fading, external interference, shadowing, and other factors. The aim of the dynamic power control is to limit transmitted power on both the links while maintaining link quality under all conditions. Additional advantages are longer mobile battery life.

2.6 Multipath and Rake Receivers

CDMA units use rake receivers. These are essentially a set of several correlators. Each correlator in a rake receiver is called a rake receiver finger. The base station combines the outputs of its rake receiver fingers. Typically mobile receivers have 3 rake receiver fingers and base station receivers had 4 or 5 depending on the equipment manufacturer. There are two primary methods used to combine the Rake-receiver finger outputs:

- One method weights each output equally and is, therefore, called equal-gain combining.
- The second method uses the data to estimate weights which maximise the Signal-to-Noise Ratio (SNR) of the combined output. This technique is known as maximal-ratio combining. In practice, it is not unusual for both combining techniques to perform about the same.

2.7 Handover



FDMA CDMA

Illustration 5: Handover

In FDMA systems cells must be separated by other frequencies so that cell areas of the same frequency do not interconnect. TDMA employs a similar mechanism using time as the separator. In Illustration 5 FDMA diagram it can be seen that Frequency A cells are separated from each other by other cells with frequency B or C. This necessitates a hard handover mechanism. Hard handover means that the MS must break the connection in the cell it is leaving before making a connection in the new cell it is entering. Hard handover can be seamless or non-seamless. Seamless hard handover means that the handover is not perceptible to the user. A handover that requires a change of the carrier frequency is always performed as hard handover.

As all cells in CDMA use the same frequency, it is possible to make the connection to the new cell before leaving the current cell. This is known as a "*make-before-break*" or "*soft*" handover. Soft handovers require less power, which reduces interference and increases capacity. "*Softer*" handover is a special case of soft handover where the radio links that are added and removed belong to the same cell node. The cell node entity is called a Node-B.

3. Mobile Evolution

Individual countries operated different analogue mobile systems termed first generation mobile (1G). The European Union countries in particular saw the need for a pan-European mobile network that would cross borders and had the vision to oversee an evolution to a second generation (2G) digital technology called GSM. GSM was designed from the start to be an open, non-proprietary system to promote the pan-European vision. One of its great strengths was the international roaming capability giving Europeans a seamless mobile experience. The standard evolved quickly and today more than 170 countries enjoy the benefits of GMS. GSM provides for over 60% of all 2G mobile subscribers worldwide. GSM satellite roaming has further extended the service where terrestrial coverage does not exist.

3.1 2G, GSM and CdmaOne

GSM is different from 1G systems in that it uses digital technology and Time Division Multiple Access (TDMA) transmission. Voice is digitally encoded prior to transmission and decoded at the receiving end.

Other 2G standards to evolve were:

- Digital Advanced Mobile Phone Service (D-AMPS) in the USA. This is another TDMA transmission system in the 800 and 900 Megahertz (MHz) spectrum.
- cdmaOne was a further advancement of 2G in the USA. This system which arrived in the 1993 is the first mobile system to use CDMA Spread spectrum technology. This technology permits more channels per band than TDMA systems.

Another step forward with 2G was the introduction of services:

- Short Messaging Service (SMS) – Short text mobile to mobile service.
- Wireless application protocol (WAP) and i-mode – are protocols which permit Internet Access on wireless devices. WAP is predominant in Europe and i-mode in Japan. The main difference is in the markup language where WAP used WML and i-mode uses Compact HTML (cHTML).

3.2 2.5G and General Packet Radio Service (GPRS)

2.5G networks are the enhanced versions of 2G networks which offer data as well as voice. Typically 2.5G systems offer data rates up to about 144kb/s.

- ***General Packet Radio Service (GPRS)***
  - GPRS is an overlaying packet based air interface on the existing circuit switched GSM network offering up to 172.2 kb/s data transfer rate.
  - GPRS is used as an add-on to TDMA based cellular systems like GSM.
- ***Enhanced Data rates for GSM Evolution (EDGE)***
  - This is a further step towards 3G for GSM Carriers. It allowed allow existing GSM operators to offer advanced mobile services such as the downloading of video and music clips, full multimedia messaging, high-speed colour Internet access and e-mail on the move.

4. Radio Spectrum and IMT-2000

Changes in technology and the requirement for more and more spectrum is a major problem for the communication regulators. Here is a simplified spectrum allocation chart to give some idea of the various bands involved and the difficult problem for those in charge of spectrum management.

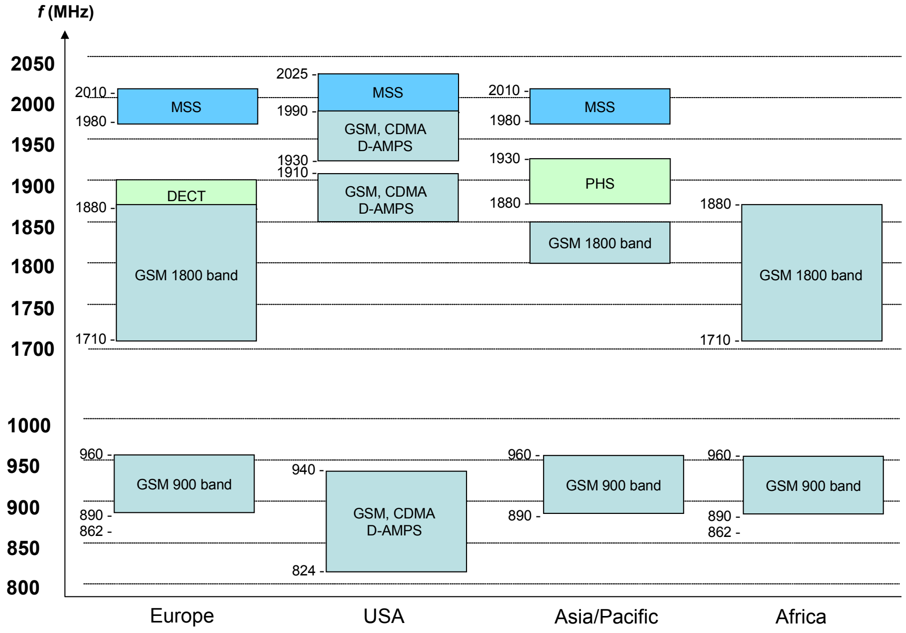


Illustration 6: 2G Spectrum allocation

4.1 2G/2.5G

In the GSM world, the two main bands used are the 900 and 1800 bands, however, in the US where GSM had to compete with AMPS (1G), D-AMPS and cdmaOne GSM operates in the 850 and 1900 bands. IS-95 cdmaOne is in the main a US 2.5G standard that has some traction in ASIA and the rest of the America’s. It is being supplanted by IS-2000 (CDMA2000). IS-136 Digital AMPS is a competing TDMA technology to cdmaOne that is US only.

5. Global System for Mobile communications (GSM)

Global System for Mobile communications / Groupe Spécial Mobile (GSM) has been the most popular standard for mobile phones in the world (82%) though it is now transitioning to Universal Mobile Telecommunications System (UMTS) sometimes called 3GSM. GSM is used by over 2 billion people across more than 212 countries. International roaming very common between mobile phone operators, enabling subscribers to use their phones as they travel. GSM differs from its predecessors in that both signalling and speech channels are digital call quality, and it is thus considered a second generation (2G) mobile phone system.

The key advantage of GSM systems to consumers has been better voice quality and low-cost alternatives to making calls, such as the Short message service (SMS).

Newer versions of the standard were backward-compatible with the original GSM phones. For example, Release '97 of the standard added packet data capabilities, by means of General Packet Radio Service (GPRS). Release '99 introduced higher speed data transmission using Enhanced Data Rates for GSM Evolution (EDGE). These enhancements have been generally branded 2.5G.

6. GSM Network

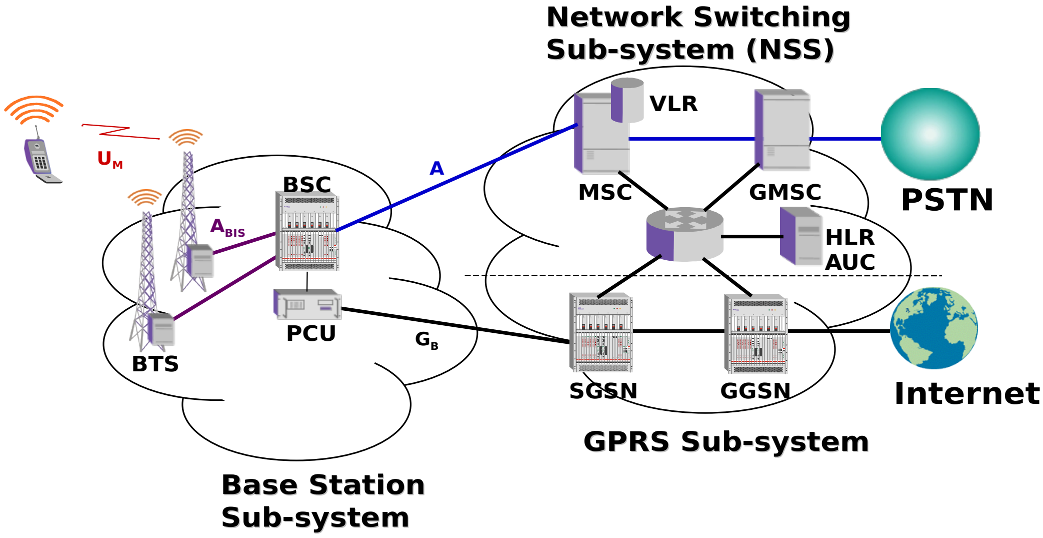


Illustration 7: GSM Network

The GSM network can be subdivided into 3 general areas, the Base Station Sub-system (BSS), the Network Switching Sub-system (NSS) and the General Packet Radio Services (GPRS) Sub-system.

6.1 Base Station Sub-system (BSS)

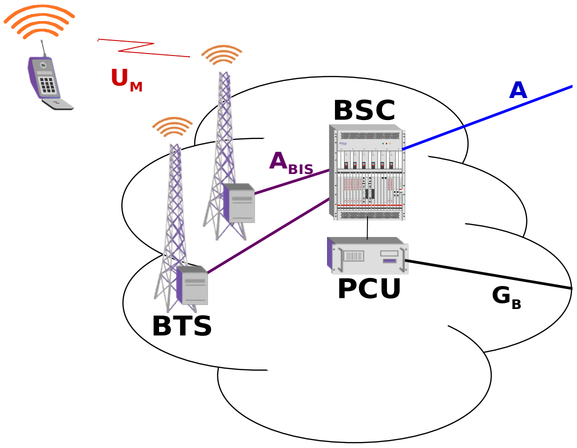


Illustration 8: Base Station Sub-system (BSS)

The Base Station Subsystem (BSS) is the section that handles traffic and signalling between a mobile phone and the Network Switching Subsystem. The BSS carries out transcoding of speech channels, allocation of radio channels to mobile phones, paging, quality management of transmission and reception over the Air interface and many other tasks related to the radio network.

6.2 The Base Transceiver Station (BTS)

The Base Transceiver Station (BTS) function is the transmission and reception of radio signals. It consists of transceivers, antennas, and equipment for encrypting and decrypting communications with the Base Station Controller (BSC). Typically a BTS for anything other than a picocell will have several transceivers (TRX) which allow it to serve several different frequencies and different sectors of the cell (in the case of sectorised base stations). A BTS is controlled by a parent BSC.

There are four different cell sizes in a GSM network, macro, micro, pico and umbrella cells. The coverage area of each cell varies according to the implementation environment. Macro cells can be regarded as cells where the base station antenna is installed on a mast or a building above average roof top level. Micro cells are cells whose antenna height is under average roof top level; they are typically used in urban areas. Picocells are small cells whose coverage diameter is a few dozen metres; they are mainly used indoors. Umbrella cells are used to cover shadowed regions of smaller cells and fill in gaps in coverage between those cells.

6.2.1 Sectorisation

By using directional antennas on a base station, each pointing in different directions, it is possible to sectorise the base station so that several different cells are served from the same location. Typically these directional antennas have a beamwidth of 65° to 85°. This increases the traffic capacity of the base station while not greatly increasing the interference caused to neighbouring cells. Typically two or three antennas are used per sector, at spacing of ten or more wavelengths apart. This allows the mobile provider to overcome the effects of fading due to physical phenomena such as multipath reception. Some amplification of the received signal as it leaves the antenna is often used to preserve the balance between uplink and downlink signal.

6.2.2 GSM Channels

There are a number of GSM System Bands, GSM-450, GSM-850, GSM-900, GSM-1800, GSM-1900. Here the two major bands used in Europe, Africa and Asia are considered. The bands are broken into two sets of 25 MHz bands split into 124 pairs of frequency duplex channels with 120 kHz carrier spacing.

One or more sets are assigned to each TRX in the BTS.

- GSM-900 system, two frequency bands:
  - 124 Channels (1 – 124)
  - 890 - 915 MHz for the uplink (direction MS to BS)
  - 935 - 960 MHz for the downlink (direction BS to MS).
- GSM-1800 system, two frequency bands:
  - 374 Channels (512 – 885)
  - 1710 - 1785 MHz for the uplink (direction MS to BS)
  - 1805 - 1880 MHz for the downlink (direction BS to MS).

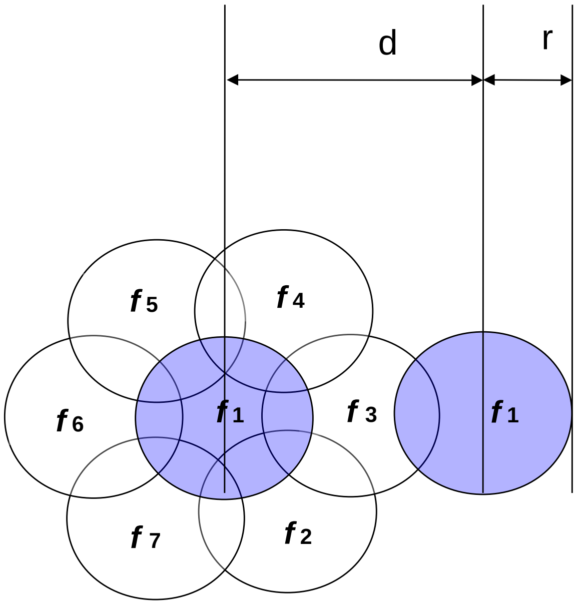


Illustration 9: GSM frequency separation

Seven sets of frequencies are sufficient to cover an arbitrarily large area, providing that the repeat-distance ‘d’ is larger than twice the maximum radius ‘r’ covered by each transmitter.

6.2.3 TDMA Frame Structure

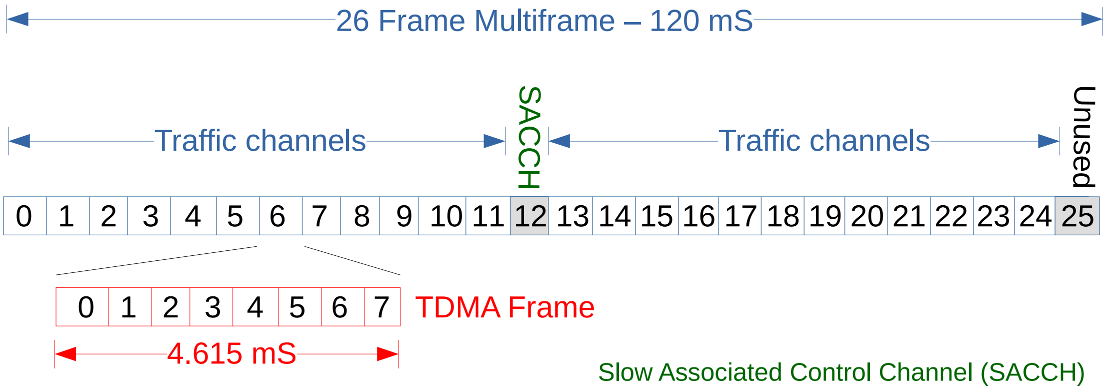


Illustration 10: TDMA frame structure

The individual radio channels are divided into frames which consist of a single 200 kHz radio channel divided into 26 TDMA timeslots. Each TDMA Timeslot is further subdivided into 8 bursts with each burst assigned to a single user. In this way multiple users can use the same RF channel. Each GSM Terminal is therefore only transmitting for 1/8 of the time 4.615/8 = 0.577 mS of each timeslot.

On the GSM Terminal traffic channels for uplink and downlink are separated by at least 3 bursts of time to ensure that it doesn't have to transmit and receive at the same time.

6.3 Base Station Controller (BSC)

The Base Station Controller (BSC) provides, the intelligence behind the BTSs. A BSC will have 10s or even 100s of BTSs under its control. The BSC handles allocation of radio channels, receives measurements from the mobile phones, controls handovers from BTS to BTS. A key function of the BSC is to act as a concentrator where many different low capacity connections to BTSs (with relatively low utilisation) become reduced to a smaller number of connections towards the Mobile Switching Centre (MSC). Overall, this means that networks are often structured to have many BSCs distributed into regions near their BTSs which are then connected to large centralised MSC sites.

6.3.1 Transcoder and Rate Adaptation Unit (TRAU)

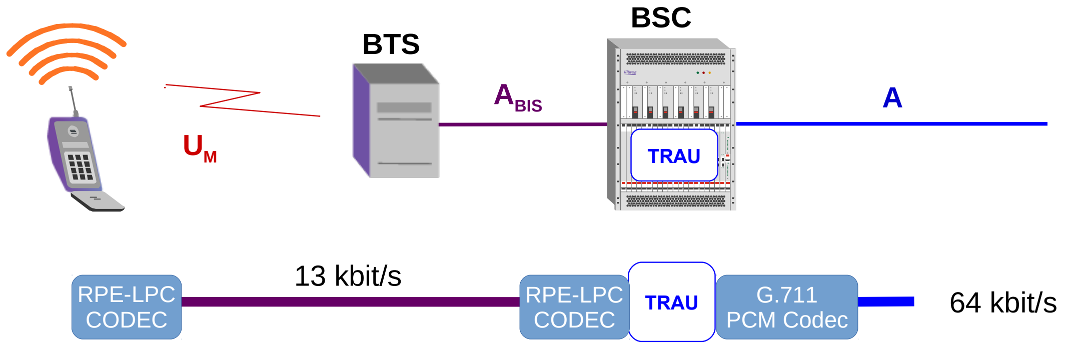


Illustration 11: Transcoder and Rate Adaptation Unit (TRAU)

Transcoding is the function of converting the voice channel coding between the GSM Regular Pulse Excited-Long Term Prediction (RPE-LPC) coder and PCM (G.711 A-law or μ-law). Since the PCM coding is 64 kb/s and the GSM coding is 13 kb/s, this also involves a buffering function so that PCM 8-bit words can be recoded to construct GSM 20 ms traffic blocks, to compress voice channels from the 64 kb/s PCM standard to the 13 kb/s rate used on the air interface. Some networks use 32 kb/s ADPCM on the terrestrial side of the network instead of 64 kb/s PCM and the TRAU converts accordingly. When the traffic is not voice but data such as fax or email, the TRAU enables its Rate Adaptation Unit function to give compatibility between the BSS data rates and the MSC capability.

6.4 Packet Control Unit

The Packet Control Unit (PCU) is a late addition to the GSM standard. It performs some of the processing tasks of the BSC, but for packet data. The allocation of channels between voice and data is controlled by the base station, but once a channel is allocated to the PCU, the PCU takes full control over that channel.

The PCU can be built into the base station, built into the BSC or even, in some architectures, it can be at the SGSN site.

6.5 BSS interfaces

- **U$_M$**
  - The air interface between the MS and the BTS. This interface conducts call control, measurement reporting, Handover, Power control, Authentication, Authorisation, Location Update etc.. Traffic and Signalling are sent in bursts of 0.577 mS at intervals of 4.615 mS, to form data blocks each 20 mS.
- **A$_{BIS}$**
  - The interface between the Base Transceiver Station and Base Station Controller. Generally carried by a E1 TDM circuit. Uses TDM subchannels for traffic (TCH), LAPD protocol for BTS supervision and telecom signalling, and carries synchronisation from the BSC to the BTS and MS.
- **A**
  - The interface between the BSC and Mobile Switching Centre. It is used for carrying Traffic channels and the Base Station System Application Part (BSSAP) of the SS7 stack. Although there are usually transcoding units between BSC and MSC, the signalling communication takes place between these two ending points and the transcoder unit doesn't touch the SS7 information, only the voice or circuit switched (CS) data are transcoded or rate adapted.
- **G$_B$**
  - Connects the BSS to the Serving GPRS Support Node (SGSN) in the GPRS Core Network.

6.6 Network Switching Station Subsystem (NSS)

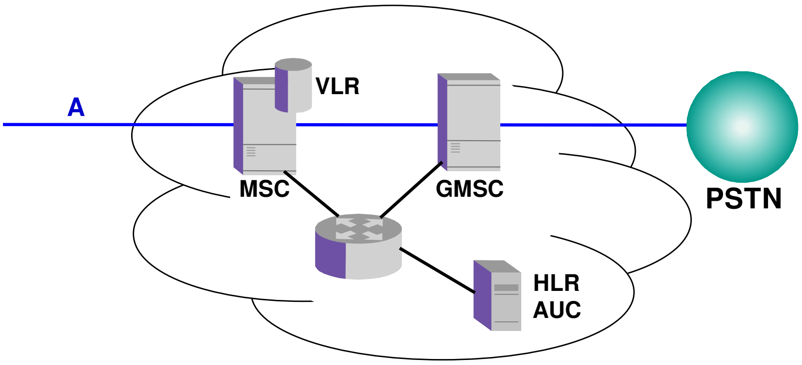


Illustration 12: Network Switching Station Subsystem (NSS)

Network Switching Subsystem (NSS) is the component of a GSM system that carries out switching functions and manages the communications between mobile phones and the Public Switched Telephone Network (PSTN). It allows mobile phones to communicate with each other and telephones in the wider telecommunications network. The architecture closely resembles a telephone exchange, but there are additional functions which are needed because the phones are not fixed in one location. Each of these functions handle different aspects of mobility management and are described in more detail below.

The NSS, also referred to as the GSM core network refers to the circuit-switched core network, used for traditional GSM services such as voice calls, SMS, and Circuit Switched Data calls.

6.7 Mobile Switching Centre (MSC)

The Mobile Switching Centre (MSC) is in effect a telephone exchange which provides circuit-switched calling, mobility management, and GSM services to the mobile phones roaming within the area that it serves. This means voice, data and fax services, as well as SMS and call divert. This is also termed the visited MSC as it is the MSC where a customer is currently located. The VLR associated with this MSC will have the subscriber's data in it.

6.7.1 Visitor Location Register (VLR)

The Visitor Location Register (VLR) is a temporary database of the subscribers who have roamed into the particular area which it serves. Each Base Station in the network is served by exactly one VLR, hence a subscriber cannot be present in more than one VLR at a time.

The data stored in the VLR has either been received from the HLR, or collected from the MS. In practice, for performance reasons, most vendors integrate the VLR directly to the MSC and, where this is not done, the VLR is very tightly linked with the MSC via a proprietary interface.

6.8 Gateway MSC (GMSC)

Gateway MSC is the MSC that determines which visited MSC the subscriber who is being called is currently located. It also interfaces with the Public Switched Telephone Network. All mobile to mobile calls and PSTN to mobile calls are routed through a GMSC. Depending upon network design the term is only valid in the context of one call since any MSC may provide both the gateway function and the visited MSC function or in some designs, dedicated high capacity MSCs which do not have any BSS connected to them. These MSCs will then be the Gateway MSC for many of the calls they handle.

6.9 Home Location Register (HLR)

The Home Location Register (HLR) is a central database that contains details of each mobile phone subscriber that is authorised to use the GSM core network. There is one logical HLR per Public Land Mobile Network (PLMN), although there may be multiple physical platforms. The HLR stores details of every Subscriber Identity Module (SIM) card issued by the mobile phone operator. The HLR data is stored for as long as a subscriber remains with the mobile provider.

6.9.1 Subscriber Identity Module (SIM)

Illustration 13: SIM Cards

Subscriber Identity Module (SIM) is part of a removable smart card for mobile cellular telephony devices such as mobile computers and mobile phones. SIM cards securely store the International Mobile Subscriber Identity (IMSI) used to identify a subscriber. The SIM card allows users to change phones by simply removing the SIM card from one mobile phone and inserting it into another mobile phone or broadband telephony device.

The SIM cards IMSI is the primary key to each HLR record. The next important items of data associated with the SIM is the Mobile Subscriber International ISDN Number (MSISDN). The MSISDN is defined by the E.164 numbering plan, the telephone numbering plan used by mobile phones to make and receive calls. The primary MSISDN is the number used for making and receiving voice calls and SMS, but it is possible for a SIM to have other secondary MSISDNs associated with it for fax and data calls. Examples of other data stored in the HLR against an IMSI record is:

- GSM services that the subscriber has requested or been given.
- GPRS settings to allow the subscriber to access packet services.
- Current Location of subscriber (VLR and SGSN).
- Call divert settings applicable for each associated MSISDN.

6.9.2 International Mobile Subscriber Identity (IMSI)

The IMSI is derived from the following steps.

The IMSI example: 011256705446743

Mobile Network Code (MNC): 011

Mobile Country Code (MCC): 256

Mobile Subscriber Identity Number (MSIN): 705446743

6.9.3 Authentication Centre (AuC)

The Authentication Centre (AuC) is a function to authenticate each SIM card that attempts to connect to the GSM core network (typically when the phone is powered on). Once the authentication is successful, the HLR is allowed to manage the SIM and services. An encryption key is also generated that is subsequently used to encrypt all wireless communications (voice, SMS, etc.) between the mobile phone and the GSM core network.

If the authentication fails, then no services are possible from that particular combination of SIM card and mobile phone operator attempted.

7. General Packet Radio Services (GPRS) Sub-system

The General Packet Radio Services (GPRS) Sub-system is an overlay architecture on the GSM core network to provide packet-switched data services and is sometimes known as the GPRS core network. This allows mobile phones to have access to services such as:

- Wireless Application Protocol (WAP).
- Multimedia Messaging Service (MMS).
- Internet access.

GPRS provides mobility management, session management and transport for Internet Protocol packet services in both GSM and as you will see later in Wideband Code Division Multiple Access (WCDMA) networks. The core network also provides support for other additional functions such as charging and lawful interception.

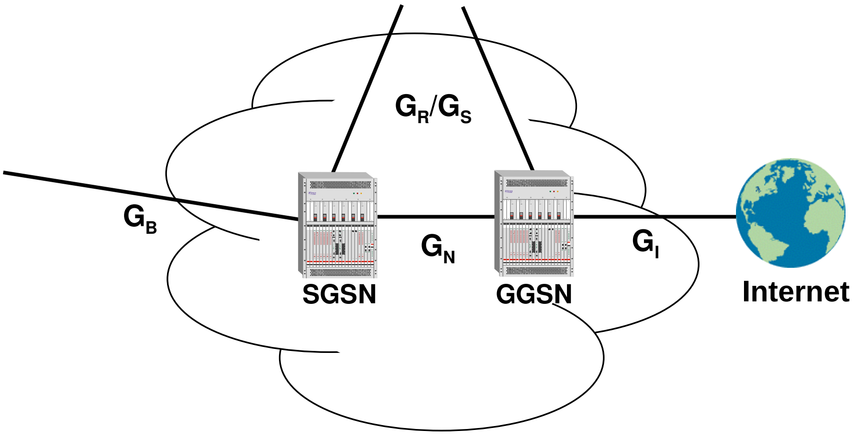


Illustration 14: General Packet Radio Services (GPRS)

7.1 Serving GPRS Support Node (SGSN)

The Serving GPRS Support Node (SGSN) tracks the location of an individual MS and performs security functions and access control for packet services. It interfaces to the BSSs via the G_B Interface, this is typically over Frame Relay.

7.2 Gateway GPRS Support Node (GGSN)

The Gateway GPRS Support Node (GGSN) provides a gateway routing function for the GPRS network. To external packet data networks the GGSN performs the task of an IP router. It also provides Firewall and filtering functionality, to protect the integrity of the GPRS core network. Billing functionality is also associated with the GGSN. The GGSN interfaces to the SGSN via the G_N Interface.

7.3 Charging Gateway Function (CGF)

The CGF consolidates filters and optimises Call Detail Record (CDR) prior to their transmission to the Billing Platform. This function can be distributed within the SGSN and GGSN or centralised.

7.4 GPRS Data Call

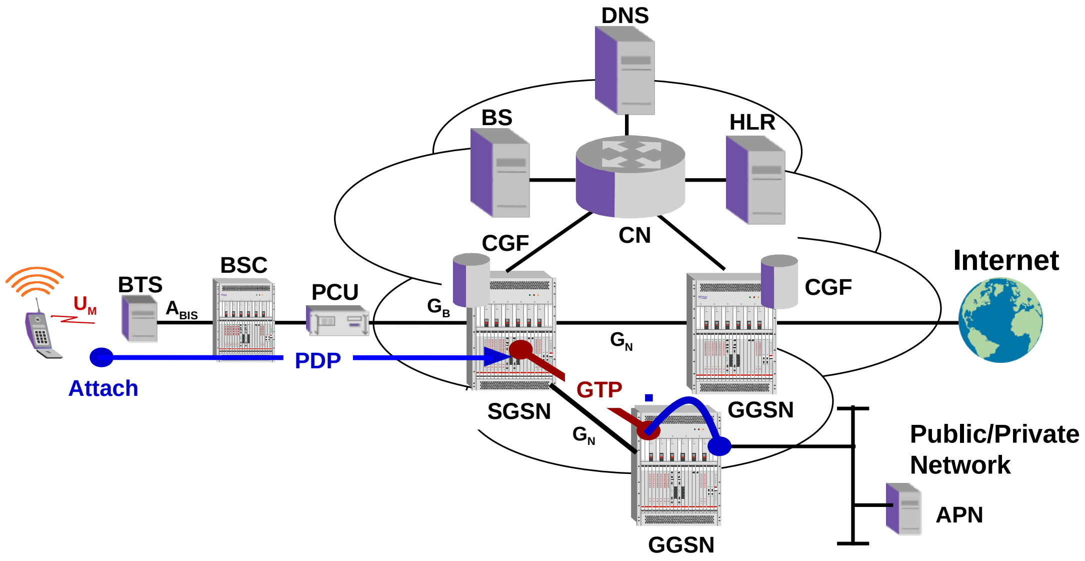


Illustration 15: GPRS data call

For a packet data connection in GPRS a Packet Data Protocol (PDP) Context is established from the MS to the SGSN. The PDP context is a data structure present on both the SGSN and the GGSN which contains the subscriber's session information when the subscriber has an active session. When a mobile wants to use GPRS, it must first attach and then activate a PDP context. This allocates a PDP context data structure in the SGSN that the subscriber is currently visiting and the GGSN serving the subscribers access point.

The SGSN looks for a suitable GGSN to provide the service based on the Access Point Name (APN) supplied by the MS (i.e. makerere.mnc011.mcc256.gprs) which points to an Abstract Syntax Notation One (ASN.1). The APN provides routing information for SGSN and GGSN. The APN consists of two parts:

- The Network ID identifies the external service requested.
- The Operator ID which specifies routing information i.e. Host/Domain.

Once a GGSN has been selected the SGSN establishes a GPRS Tunnelling Protocol (GTP) tunnel with the GGSN and the GGSN associates the tunnel with the interface to the external network providing the service. The interface on the GGSN could be a tunnel to a tunnel terminator on another network. i.e. L2TP to an LNS on a corporate network.

7.5 Packet Data protocol (PDP)

In order for the user to be able to transfer data, a Packet Data Protocol (PDP) Context must be activated in the MS, SGSN and GGSN. The user initiates this procedure, which is similar to logging on to the required destination network. The context defines aspects such as:

- Routing.
- QoS (Quality of Service).
- Security.
- Billing.

As GPRS supports IPv4 (IP version 4), IPv6 (IP version 6) or X.25 the PDP address can conforms directly to the standard addressing scheme of the respective network layer protocol used. The PDP Context has a PDP Type indication of what type of protocol is to be used by the mobile. The user initiates the logging on process, using an application on the workstation or MS. The MS requests sufficient radio resources to support the Context Activation procedure. Once the radio resources are allocated, the MS sends the Activate PDP context request to the SGSN. This signalling message includes key information about:

- User's IP address if fixed.
- The QoS requested for this context.
- The APN of the external network to which connectivity is requested.

After receiving the Activate PDP context message, the SGSN checks the user's subscription record to establish whether the request is valid. If the request is valid, the SGSN sends a query containing the requested APN to the DNS server. The DNS server uses the APN to determine and return the IP address of at least one GGSN that will provide the required connectivity to the external network. The SGSN uses the GGSN IP address to request a GTP tunnel to the GGSN. Upon receiving this request the GGSN completes the establishment of the tunnel and returns an IP address to be conveyed to the MS. The GGSN associates the tunnel with the required external network connection.

Once this procedure is completed, a virtual connection is established between the MS and the GGSN. The GGSN also has an association between the tunnel and the physical interface to the external network. Data transfer can now take place between the MS and the external network.

7.6 GPRS Tunnelling Protocol (GTP)

GTP is employed on the GN interface in order to tunnel user data between different GSN (GPRS Support Node). Version 0 of the protocol supports both signalling and user data under one generic header. It can be used with UDP (User Datagram Protocol) or TCP (Transmission Control Protocol) on the registered port 3386. GTP version 1 is used only on UDP. The GTP control plane (GTP-C) uses port 2123 and the GTP user plane (GTP-U) uses port 2152. GTP-C messages are exchanged between GSN elements i.e. the SGSN and the GGSN. These messages are used to:

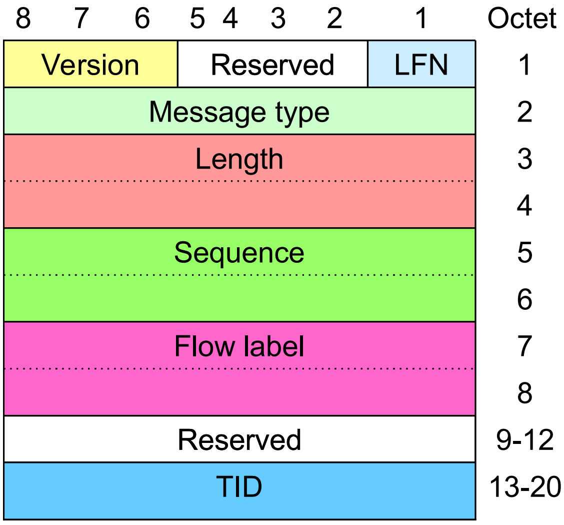
- Transfer GSN capability information between GSN elements.
- Creates, updates and teardown GTP tunnels.
- Manage the path.

GTP-U messages are exchanged between GSN elements and RNC elements in a path. These messages are used to:

- Carry user data packets.
- Signalling messages for path management.
- Signalling messages for error indication.

GTP has an optional charging protocol. GPRS nodes generate Call Detail Records (CDR) which can be collected by the Charging Gateway Function (CGF).

7.6.1 GTP Header



8	7	6	5	4	3	2	1	Octet
Version			Reserved				LFN	1
Message type								2
Length								3
								4
Sequence								5
								6
Flow label								7
								8
Reserved								9-12
TID								13-20

Illustration 16: GTP header

The GTP header is a fixed format 16 octet header used for all GTP messages.

- **Version**
    - Set to 0 to indicate the first version of GTP.
- **LLC Frame Number**
    - LLC frame number. Flag indicating whether the LLC frame number is included or not, set to 0 in signalling messages.
- **Message type**
    - Indicates the type of GTP message. In signalling messages, it is set to the unique value that is used for each type of signalling message.
- **Length**
    - Indicates the length in octets of the GTP message (G-PDU). In signalling messages, this is the length, in octets, of the signalling message including the GTP header.
- **Sequence number**
    - A transaction identity for signalling messages and an increasing sequence number for tunnelled T-PDUs.
- **Flow label**
    - Identifies a GTP flow any lost or un ordered packets.
    - In signalling Path Management messages and Location Management messages, the flow label is not used and is set to 0.
- **TID**
    - The Tunnel Identifier that points out MM and PDP contexts in the destination GSN. In signalling messages, it is set to 0 in all V Management messages, Location Management messages and Mobility Management messages.

7.7 Charging Gateway Function (CGF)

The CGF consolidates filters and optimises CDR (Call Detail Record) prior to their transmission to the Billing Platform. This function can be distributed within the SGSN and GGSN or centralised.

8. 2G Enhancements

8.1 Enhanced Data Rates for GSM Evolution (EDGE)

Enhanced Data rates for GSM Evolution (EDGE) or Enhanced GPRS (EGPRS), is a digital mobile phone technology that allows increased data transmission rates and improved data transmission reliability. Although technically a 3G network technology, it is generally classified as the unofficial standard 2.75G, due to its slower network speed. EDGE has been introduced into GSM networks around the world since 2003.

EDGE can be used for any packet switched application, such as an Internet connection. High-speed data applications such as video services and other multimedia benefit from EGPRS' increased data capacity. EDGE Circuit Switched is a possible future development.

EDGE can carry data speeds up to 236.8 kb/s for 4 timeslots (theoretical maximum is 473.6 kb/s for 8 timeslots) in packet mode.

8.2 EDGE Evolution

EDGE Evolution improves on EDGE in a number of ways. Latencies are reduced by lowering the Transmission Time Interval by half (from 20 mS to 10 mS). Bit rates are increased up to 1 Mb/s peak speed and latencies down to 100 mS using dual carriers, higher symbol rate and higher-order modulation (16QAM and 32QAM instead of 8-PSK), and turbo codes to improve error correction. And finally signal quality is improved using dual antennas. An EDGE Evolution terminal or network can support some of these improvements, or roll them out in stages.

9. Self-test Quiz

1. Describe the following multiple access methods:
   - TDMA
   - FDMA
   - CDMA.
2. With the aid of a diagram describe spread spectrum.
3. Describe the elements of a GSM Network Switching Sub-system (NSS).
4. On GSM networks what is the function of a TRAU.
5. With the aid of a diagram describe the steps of a GPRS Data Call.
6. Briefly describe the improvements brough by each of the following:
   - EDGE
   - EDGE Evolution.

This page is intentionally blank