1

Cellular Networks

Ajay R Mishra

COPYRIGHTED MATERIAL

1.1 Introduction

The cellular technology evolution has been going on since the late 1950s, though the first commercial systems came into being in the late 1970s and early 1980s. Here is a brief overview of the cellular technologies and the networks that made an impact on the development and the fast evolution of the mobile communications.

1.2 First Generation Cellular Networks

Since the late 1970s when the cellular era started, mobile communication has gone through an evolutionary change every decade in terms of technology and usage. Japan took the lead in the development of cellular technology, which resulted in the deployment of the first cellular networks in Tokyo. Within a couple of years Nordic Mobile Telephony (NMT) started cellular operations in Europe. Along with it, systems such as AMPS (Advanced Mobile Phone Service) started in the USA, while TACS (Total Access Communication System) started in the UK. These formed a part of what was called 'First Generation Mobile Systems', which catered for speech services and were based on analogue transmission techniques. The geographical area was divided into small sectors, each called a cell. Hence, the technology came to be known as cellular technology while the phones were called cell phones. All the systems that were initially developed were quite incompatible with each other. Each of these networks implemented their own standards. Facilities such as roaming within the continent were impossible and most countries had only one operator. The penetration was also low; e.g. penetration in Sweden was just 7 %, while countries like Portugal had a penetration of only 0.7 %. Handsets were also expensive, the minimum being more than $1000. Apart from higher costs and incompatibility with other cellular networks, first generation technology also had an inherent limitation in terms of channels, etc.

1.2.1 NMT (Nordic Mobile Telephony)

The NMT mobile phone system was created in 1981 as a response to the increasing congestion and heavy requirements of the ARP (auto radio puhelin, or car radio phone) mobile phone network. The technical principles of NMT were ready by 1973 and specifications for base stations were ready in 1977. It is based

Advanced Cellular Network Planning and Optimisation Edited by Ajay R Mishra
© 2007 John Wiley & Sons, Ltd

on analogue technology (first generation or 1G) and two variants exist: NMT 450 and NMT 900. The numbers indicate the frequency bands used. NMT 900 was introduced in 1986 because it carries more channels than the previous NMT 450 network. The NMT network has mainly been used in the Nordic countries, Baltic countries and Russia, but also in the Middle East and in Asia. NMT had automatic switching built into the standard from the beginning. Additionally, the NMT standard specified billing and roaming. The NMT specifications were free and open, allowing many companies to produce NMT hardware and pushing prices down. A disadvantage of the original NMT specification is that traffic was not encrypted. Thus, anyone willing to listen in would just have to buy a scanner and tune it to the correct frequency. As a result, some scanners have had the NMT bands 'deleted' so they could not be accessed. This is not particularly effective as it is not very difficult to obtain a scanner that does not have these restrictions; it is also possible to re-program a scanner so that the 'deleted' bands can be accessed. Later versions of the NMT specifications defined optional analogue encryption, which was based on two-band audio frequency inversion. If both the base station and the mobile station supported encryption, they could agree upon using it when initiating a phone call. Also, if two users had mobile stations supporting encryption, they could turn it on during conversation, even if the base stations did not support it. In this case audio would be encrypted all the way between the two mobile stations. While the encryption method was not at all as strong as encryption in newer digital phones, it did prevent casual listening with scanners. The cell sizes in an NMT network range from 2 km to 30 km. With smaller ranges the network can service more simultaneous callers; e.g. in a city the range can be kept short for better service. NMT used full duplex transmission, allowing for simultaneous receiving and transmission of voice. Car phone versions of NMT used transmission power of up to 6 watts and handsets up to 1 watt. Signalling between the base station and the mobile station was implemented using the same RF channel that was used for audio, and using the 1200 bps (bits per second) FFSK modem. This caused the periodic short noise bursts that were uniquely characteristic of NMT sound.

1.2.2 AMPS (Advanced Mobile Phone System)

The first cellular licences in the US were awarded in 1981, and the cellular services started in 1983 in Chicago and The Baltimore–Washington area using the AMPS. The AMPS was based on the FDMA (frequency division multiple access) technology, which allowed multiple users in a cell or cell sector. Initially, cell size was not fixed and an eight mile radius was used in urban areas and a twenty-five mile radius in rural areas. However, as the number of users began to increase, new cells were added. With the addition of every new cell, the frequency plan was to be re-done to be able to avoid interference related problems. This system not only had capacity related problems, but the security system was also poor. If you are able to get hold of another person's serial code, it would be possible to make illegal calls. Although efforts were made to address these problems, especially the ones related to capacity, the results were not sufficient and the industry started to look into other options, such as the next generation digital systems. The TACS was similar to the AMPS and operated in the 900 MHz frequency range.

1.3 Second Generation Cellular Networks

Due to the incompatibility of the various systems in place, the European commission started a series of discussions that tried to change the then existing telecommunication regulatory framework, leading to a more harmonised environment which resulted in the development of a common market for the telecommunication services and equipment. In the early 1990s, digital transmission technology came into force, bringing with it the next generation system, called the 'Second Generation Mobile System'. Digitisation means that the sound of the speaker's voice was processed in a way that imitated a human ear through techniques such as sampling and filtering. This made it possible for many more mobile users to be accommodated in the radio spectrum. Key 2G systems in this generation included GSM (Global

Systems for Mobile Communications), TDMA IS-136, CDMA IS-95, PDC (Personal Digital Cellular) and PHS (Personal Handy Phone System).

1.3.1 D-AMPS (Digital Advanced Mobile Phone System)

IS 54 and IS 136 (where IS stands for Interim Standard) are the second generation mobile systems that constitute the D-AMPS. This was the digital advancement of the then existing AMPS in America. TDMA (Time Division Multiple Access) was used as the air interface protocol. The D-AMPS used existing AMPS channels and allows for smooth transition between digital and analogue systems in the same area. Capacity was increased over the preceding analogue design by dividing each 30 kHz channel pair into three time slots and digitally compressing the voice data, yielding three times the call capacity in a single cell. A digital system also made calls more secure because analogue scanners could not access digital signals.

IS-136 added a number of features to the original IS-54 specification, including text messaging, circuit switched data (CSD) and an improved compression protocol. The short message service (SMS) and CSD were both available as part of the GSM protocol, and IS-136 implemented them in a nearly identical fashion. D-AMPS used the 800 and 900 MHz frequency bands – as does the AMPS – but each 30 kHz channel (created by FDMA) is further subdivided into three TDMA, which triples the channels available and the number of calls.

1.3.2 CDMA (Code Division Multiple Access)

CDMA has many variants in the cellular market. N-CDMA, i.e. Narrowband CDMA (or just CDMA), was developed by Qualcomm, known in the US as IS-95, and was a first generation technology. Its typical characteristic was high capacity and small cell radius. CDMAone (IS-95) is a second generation system, offering advantages such as an increase in capacity (almost 10 times that of the AMPS), improved quality and coverage, improved security system, etc. Enhancement of the CDMAone was IS-95B, also called 2.5G of CDMA technology, which combined the standards IS-95A, ANSI-J-STD-008 and TSB-74. Major advantages of this system include frequency diversity (i.e. frequency dependent transmission impairments have less effect on the signal), increased privacy as the spread spectrum is obtained by noise like signals, an interference limited system, etc., while some disadvantages of this system include the air interface, which is the most complicated, soft hand-off, which is more complicated than the ones used in the TDMA/ FDMA system, signals near to the receiver, which are received with less attenuation than the ones further from it, etc.

1.3.3 GSM (Global System for Mobile Communication)

GSM was first developed in the 1980s. From 1982 to 1985, in the GSM group (originally hosted by CEPT) discussions were held to decide between building an analogue or a digital system. After multiple field tests, etc., it was decided to build a digital system and a narrowband TDMA solution was chosen. The modulation scheme chosen was Gaussian minimum shift keying (GMSK). The technical fundamentals were ready by 1987 and by 1990 the first specification was produced. By 1991, GSM was the first commercially operated digital cellular system with Radiolinja in Finland. GSM is by far the most popular and widely implemented cellular system with more than a billion people using the system (by 2005). Features such as prepaid calling, international roaming, etc., enhanced the popularity of the system. Of course, this also led to the development of smaller and lighter handsets with many more features. The system became more user friendly with many services also provided apart from just making calls. These services included voice mail, SMS, call waiting, etc. SMS was a phenomenal success, with almost 15 billion SMS sent every month by the year 2000. The key advantage of GSM systems has been higher

digital voice quality and low cost alternatives to making calls, such as text messaging. The advantage for network operators has been the ability to deploy equipment from different vendors because the open standard allows easy interoperability.

The GSM system operates at various radio frequencies, with most them operating at 900 MHz and/or 1800 MHz. In the US and Canada, the operation is at 850 MHz and/or 1900 MHz. The uplink frequency band in the 900 MHz band is 935–960 MHz and the downlink frequency is 890–915 MHz. Thus, in both the uplink and downlink the band is 25MHz, which is subdivided into 124 carriers, each being 200 kHz apart. Each radio frequency channel contains eight speech channels. The cell radius in the GSM network varies depending upon the antenna height, antenna gains, propagation conditions, etc. These factors vary the cell size from a couple of hundred metres to a few kilometres. Due to this cell sizes are classified into four kinds in GSM networks; macro, micro, pico and umbrella, with macro cells being the biggest and pico and umbrella cells being the smallest.

System Architecture

A network mobile system has two major components: the fixed installed infrastructure (network) and the mobile subscribers, who use the services of the network. The fixed installed network can again be subdivided into three subnetworks: radio networks, mobile switching network and management network. These subnetworks are called subsystems. The respective three subsystems are:

- Base Station Subsystems (BSS);
- Switching and Management Subsystem (SMSS);
- Operation and Management Subsystems (OMSS).

Radio Network – Base Station Subsystem (BSS)

This comprises the Base Station Controller (BSC) and the Base Transceiver Station/Base Station (BTS/BS). The counterpart to a Mobile Station (MS) within a cellular network is the Base Transceiver Station, which is the mobile's interface to the network. A BTS is usually located in the centre of a cell. The BTS provides the radio channels for signalling and user data traffic in the cells. Besides the high frequency part (the transmitter and receiver component) it contains only a few components for signal and protocol processing. A BS has between 1 and 16 transceivers, each of which represents a separate radio frequency channel.

The main tasks of the BSC include:

- frequency administration;
- control of the BTS;
- exchange functions.

The hardware of the BSC may be located at the same site as the BTS, at its own stand-alone site, or at the site of the Mobile Switching Centre (MSC).

Mobile Switching Network

The Mobile Switching Subsystem (MSS) consists of Mobile Switching Centres and databases, which store the data required for routing and service provisions. The switching node of a mobile network is called the Mobile Switching Centre (MSC). It performs all the switching functions of a fixed network switching node, e.g. routing path search and signal routing. A public land mobile network can have several Mobile Switching Centres with each one being responsible for a part of the service area. The BSCs of a base subsystem are subordinated to a single MSC.

Dedicated Gateway MSC (GMSC)
This passes voice traffic between fixed networks and mobile networks. If the fixed network is unable to connect an incoming call to the local MSC, it routes the connection to the GMSC. This GMSC requests the routing information from the Home Location Register (HLR) and routes the connection to the local MSC in whose area the mobile station is currently staying. Connections to other mobile international networks are mostly routed over the International Switching Centre (ISC) of the respective country.

Home and Visitor Location Registers (HLR and VLR)
A given mobile network has several databases. Two functional units are defined for the synchronisation of registration of subscribers and their current location: a home location register (HLR) and the visitor location register (VLR). In general, there is one central HLR per public land mobile network (PLMN) and one VLR for each MSC.

Home Location Register (HLR)
The HLR stores the identity and user data of all the subscribers belonging to the area of the related GMSC. These are permanent data such as the International Mobile Subscriber Identity (IMSI) of an individual user, the user's phone number from the public network (not the same as IMSI), the authentication key, the subscribers permitted supplementary service and some temporary data. The temporary data on the Subscriber Identity Module (SIM) may include entries such as:

- the address of the current VLR;
- the number to which the calls may be forwarded;
- some transit parameters for authentication and ciphering.

Visitor Location Register (VLR)
The VLR stores the data of all mobile stations that are currently staying in the administrative area of the associated MSC. A VLR can be responsible for the areas of one or more MSCs. Mobile Stations are roaming freely and therefore, depending on their current location, they may be registered in one of the VLRs of their home network or in the VLR of a foreign network.

Operation and Maintenance Subsystem (OMSS)
The network operation is controlled and maintained by the Operation and Maintenance Subsystem (OMSS). Network control functions are monitored and initiated from an Operation and Maintenance Centre (OMC). The OMC has access to both the GMSC and BSC. Some of its functions are:

- administration and commercial operations (subscribers, end terminals, charging, statistics);
- security management;
- network configuration, operation, performance management;
- maintenance tasks.

The OMC configures the BTS via the BSC and allows the operator to check the attached components of the system.

User Authentication and Equipment Registration
Two additional databases are responsible for the various aspects of system security. They are based primarily on the verification of the equipment and subscriber identity; therefore, the databases serve for user authentication, identification and registration. Confidential data and keys are stored or generated in the Authentication Centre (AUC). The Equipment Identity Register (EIR) stores the serial numbers (supplied by the manufacturer) of the terminals (IMEI), which makes it possible to block service access for mobile stations reported as stolen.

Addresses and Identifiers

Mobile Station (MS)

These are pieces of equipment used by mobile subscribers for accessing the services. They consist of two major components: the Mobile Equipment (ME) and the Subscriber Identity Module (SIM). In addition to the equipment identifier the International Mobile Station Equipment Identity (IMEI) the mobile station has subscriber identification (IMSI and MSISDN, or the Mobile Subscriber ISDN Number) as subscriber dependent data.

Subscriber Identity Module (SIM)

The Subscriber Identity Module (SIM) provides mobile equipment with an identity. Certain subscriber parameters are stored on the SIM card, together with personal data used by the subscriber. The SIM card identifies the subscriber to the network. To protect the SIM card from improper use, the subscribers have to enter a 4-bit Personal Identification Number (PIN) before using the mobile. The PIN is stored on the card. If the wrong PIN is entered three times in a row, the card blocks itself and may only be unblocked with an 8-bit personal blocking key (PUK), also stored in the card.

International Mobile Station Equipment Identity (IMEI)

This serial number uniquely identifies mobile stations internationally. It is allocated by the equipment manufacturer and registered by the network operators who store them in the Equipment Identity Register (EIR). IMEI is a hierarchical address, containing the following parts:

- Type Approval Code (TAC): 6 decimal places, centrally assigned;
- Find Assembly Code (FAC): 6 decimal places, assigned by the manufacturer;
- Serial Number (SNR): 6 decimal places, assigned by the manufacturer;
- Spare (SP): 1 decimal place.

Hence, IMEI = TAC + FAC + SNR + SP.

International Mobile Subscriber Identity (IMSI)

While registering for service with a network operator, each subscriber receives a unique identifier, the International Mobile Subscriber Identity (IMSI), which is stored in the SIM. A mobile station can be operated if a SIM with a valid IMSI is inserted into equipment with a valid IMEI. The IMSI also consists of the following parts:

- Mobile Country Code (MCC): 3 decimal places, internationally standardised;
- Mobile Network Code (MNC): 2 decimal places, for unique identification of mobile networks across the country;
- Mobile Subscriber Identification Number (MSIN): maximum 10 places, identification number of the subscriber in his/her mobile home network.

Thus IMSI = MCC + MNC + MSIN and a maximum of 15 digits is used.

Mobile Subscriber ISDN Number (MSISDN)

The real telephone number of the MS is the Mobile Subscriber ISDN Number. It is assigned to the subscriber, such that an MS can have several MSISDNs depending on the SIM. The subscriber identity cannot be derived from the MSISDN unless the association of IMSI and MSISDN as stored in the HLR is known.

In addition to this a subscriber can hold several MSISDNs for selection of different services. Each MSISDN of a subscriber is reserved for a specific service (voice, data, fax, etc.). In order to realise this service, service specific resources need to be activated, which are done automatically during the setup of a connection. The MSISDN categories have the following structure:

- Country Code (CC): up to 3 decimal places;
- National Destination Code (NDC): typically 2–3 decimal places;
- Subscriber Number (SN): maximum 10 decimal places.

Thus, MSISDN = CC + NDC + SN.

Mobile Station Roaming Number (MSRN)

The Mobile Station Roaming Number (MSRN) is a temporary location dependent ISDN number. It is assigned by a locally responsible VLR to each MS in its area. Calls are routed by the MS using the MSRN. On request, the MSRN is passed from the HLR to the GMSC. The MSRN has the same structure as the MSISDN:

- Country Code (CC) of the visited network;
- National Destination Code (NDC) of the visited network;
- Subscriber Number (SN) in the current mobile network.

The components CC and NDC are determined by the visited network and depend on the current location. The SN is assigned by the current VLR and is unique within the mobile network. The assignment of an MSRN is done in such a way that the currently responsible switching node MSC in the visited network (CC + NDC) can be determined from the subscriber number, which allows routing decisions to be made.

The MSRN can be assigned in two ways by the VLR: either at each registration when the MS enters a new Location Area (LA) or each time when the HLR requests it for setting up a connection for the incoming calls to the mobile station. In the first case, the MSRN is also passed on from the VLR to the HLR, where it is stored for routing. In the case of an incoming call, the MSRN is first requested from the HLR of the MS. In this way the currently responsible MSC can be determined, and the call can be routed to this switching node. In the second case, the MSRN cannot be stored in the HLR, since it is only assigned at the time of the call setup. Therefore the address of the current VLR must be stored in the tables of the HLR. Once routing information is requested from the HLR, the HLR itself goes to the current VLR and uses a unique subscriber identification (IMSI and MSISDN) to request a valid MSRN. This allows further routing of the call.

Location Area Identity (LAI)

Each LA has its own identifier. The Location Area Identifier (LAI) is also structured hierarchically and is internationally unique. It consists of the following parts:

- Country Code (CC): 3 decimal digits;
- Mobile Country Code (MNC): 2 decimal places;
- Location Area Code (LAC): maximum 5 decimal places, or maximum twice 8 bits.

The LAI is broadcast regularly by the base station on the Broadcast Control Channel (BCCH). Thus, each cell is identified uniquely on the radio channel and each MS can determine its location through the LAI. If the LAI that is heard by the MS notices this LA change it requests the updating of its location information in the VLR and HLR (location update). The LAI is requested from the VLR if the connection for an incoming call has been routed to the current MSC using the MSRN. This determines the precise location of the MS where the mobile can be currently paged.

Temporary Mobile Subscriber Identity (TMSI)

The VLR being responsible for the current location of a subscriber can assign a Temporary Mobile Subscriber Identity (TMSI), which only has significance in the area handled by the VLR. It is used in place of the IMSI for the definite identification and addressing of the MS. Therefore nobody can

determine the identity of the subscriber by listening to the radio channel, since the TMSI is only assigned during the MS's presence in the area of one VLR, and can even be changed during this period (ID (identity) hopping). The MS stores the TMSI on the network side only in the VLR and it is not passed to the HLR.

Local Mobile Subscriber Identity (LMSI)

The VLR can assign an additional searching key to each MS within its area to accelerate database access, called the Local Mobile Subscriber Identity (LMSI). Each time messages are sent to the VLR concerning an MS, the LMSI is added, so the VLR can use the short searching key for transactions concerning this MS.

Mobile Call Origination and Termination

The case is considered where a person makes a call from a telephone connected to a public switched telephone network (PSTN) or ISDN, to a mobile subscriber going from city A to city B. The call will take place only if the subscriber's mobile is switched on. Assuming the mobile to be switched on, the MS searches for the cellular network by scanning the relevant frequency band for some control channel transmitted by a nearby MS. After location updating the MS accesses the network and acquires a unique serial number. Once an MS has successfully registered its location with the network it enters the idle mode, whereby it listens to the paging channels from the selected BS.

Since the subscriber is presently in city A the MS will have identified a BS in this area. The MS will notice that the signal begins to fall as it is moving from city A to city B and it will now look for a more appropriate BS to take over. When the MS identifies a more appropriate BS it examines its control channels to determine the location area to which it belongs. If it belongs to the same location area as the previous BS, the MS simply re-tunes to a paging channel on the new BS and continues to monitor this new channel for incoming paging calls. If the MS has moved between BSs in different location areas, then it performs a location update and informs the network of its new position. This process of transition between BSs while in the idle mode is termed the idle mode handover.

The entire process of the call is initiated by the person lifting the handset and dialing the number of the mobile subscriber. On receiving a number with the area code, the PSTN/ISDN network will route the call to the gateway switch of the mobile network and will also provide the telephone number of the mobile subscriber. The gateway switch then interrogates the mobile network's HLR to recover the subscriber's records.

Once the call arrives at the MSC, the MS is paged to alert it to the presence of an incoming call. A paging call is then issued from each BS in the location area in which the subscriber is registered. On receiving a paging call the MS responds by initiating the access procedure. The access procedure commences with the MS sending a message to the BS requesting a channel. The BS replies by sending the MS details of a dedicated channel and the MS re-tunes to this channel. A certain degree of handshaking occurs to ensure that the identity of the subscriber is correct.

Once the dedicated signalling channel is established, security procedures such as subscriber authentication, take place over this channel. Following this, the network allocates a dedicated speech channel and both the BS and MS re-tune to this channel and establish a connection. It can be seen that until this point is reached all processes are carried out autonomously by the MS and no interaction is required from the subscriber. It is only once all these processes are completed that the MS begins to ring.

The subscriber can now talk and the handover can take place between different BSs. Once the call has ended the call clear process initiates, which consists of a small exchange of signalling information ensuring that both the network and the MS know that the call has ended. The MS again returns to the idle mode and monitors the paging channel of its current cell.

Several cryptographic algorithms are used for GSM security, which include the features link user authentication, over-the-air voice privacy, etc. The security model of GSM, however, lacked some features such as authentication of the user to the network and not vice versa (a feature that came in the Universal Mobile Telecommunications System, or UMTS).

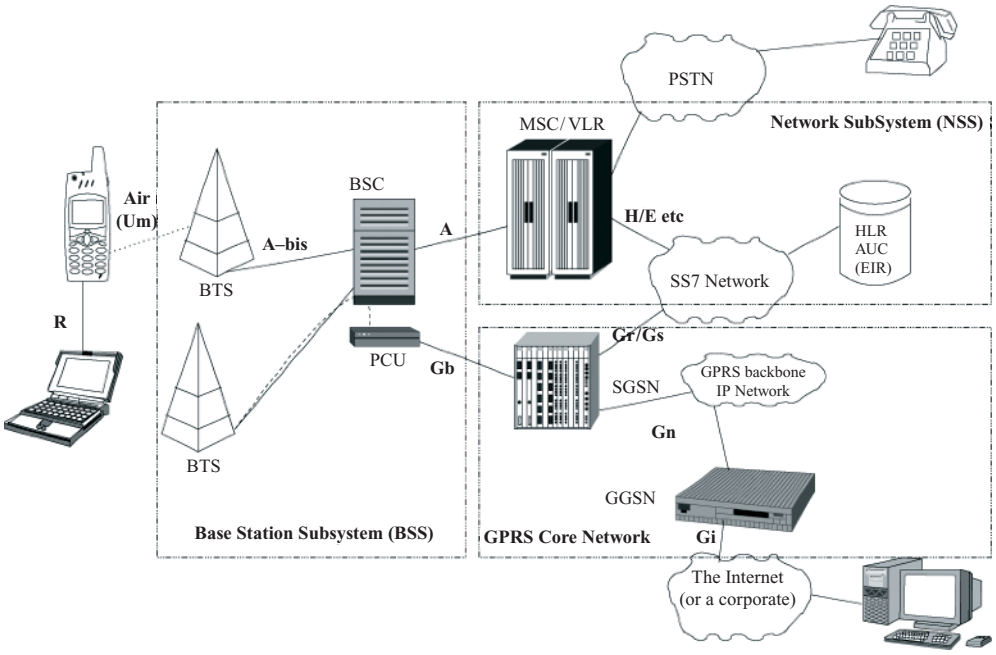

Figure 1.1 GSM and GPRS System

Limitations of 2G Networks

- *Low transfer rates*. The 2G networks are primarily designed to offer voice services to the subscribers. Thus the transfer rates offered by these networks are low. Though the rates vary across technologies, the average rate is of the order of tens of kilobits per second.
- *Low efficiency for packet switched services*. There is a demand for Internet access, not just at home or the office but also while roaming. Wireless Internet access with the 2G networks is not efficiently implemented.
- *Multiple standards*. With a multitude of competing standards in place, a user can roam in only those networks that support the same standard. This allows the user only limited roaming. Therefore the 2G network technology was semi-global in this respect.

1.3.4 GPRS (General Packet Radio Service)

GPRS is a nonvoice, i.e. data, value added service to the GSM network. This is done by overlaying a packet based air interface on the existing circuit switched GSM network (see Figure 1.1). In infrastructure terms, the operator just needs to add a couple of nodes and some software changes to upgrade the existing voice GSM system to voice plus data GPRS system. The voice traffic is circuit switched while data traffic is packet switched. Packet switching enables the resources to be used only when the subscriber is actually sending and receiving the data. This enables the radio resources to be used concurrently while being shared between multiple users. The amount of data that can be transferred is dependent upon the number of users. Theoretical maximum speeds of up to 171.2 kilobits per second (kbps) are achievable with GPRS using all eight timeslots at the same time. GPRS allows the interconnection between the network and the Internet. As there are the same protocols, the GPRS network can be viewed as a subnetwork of the Internet, with GPRS capable mobile phones being viewed as mobile hosts.

However, there are some limitations in the GPRS network, such as low speed (practical speed is much lower than theoretical speeds).

1.3.5 EDGE (Enhanced Data Rate for GSM Evolution)

The limitation of the GPRS network was eliminated to a certain extent by the introduction of the EDGE technology. EDGE works on TDMA and GSM systems. It is considered to be a subset of the GPRS as it can be installed on any system that has GPRS deployed on it. It is not an alternative to UMTS but a complimentary technology for it. In EDGE, 3G services can be given at a lower but similar data rate as UMTS, with the data rates going up to 500 kbps (theoretically). This is done by introducing a new modulation scheme 8-PSK (phase-shift keying) and will coexist with the GMSK that is used in GPRS. However, the major advantage is that existing GSM networks can be upgraded for the same, thus preventing huge costs needed to roll-out the 3G networks and at the same time giving services like 3G. General features of EDGE include enhanced throughput per timeslot (8.8–59.2 kbps/timeslot), modulation changes from GMSK to 8-PSK, decreased sensitivity of the 8-PSK signal and higher capacity and coverage. Though, not many changes in the hardware are required by EDGE, except for some hardware upgrades in the BTS and some software upgraded in the network.

However, the second generation system lacked capacity, global roaming and quality, not to mention the amount of data that could be sent. This all led to the industry working on a system that had more global reach (e.g. the user did not need to change phones when going to Japan or the US from SE Asia or Europe). This was the beginning of the evolution of third generation systems.

1.4 Third Generation Cellular Networks

The third generation cellular networks were developed with the aim of offering high speed data and multimedia connectivity to subscribers. The International Telecommunication Union (ITU) under the initiative IMT-2000 has defined 3G systems as being capable of supporting high speed data ranges of 144 kbps to greater than 2 Mbps. A few technologies are able to fulfil the International Mobile Telecommunications (IMT) standards, such as CDMA, UMTS and some variation of GSM such as EDGE.

1.4.1 CDMA2000

CDMA2000 has variants such as 1X, 1XEV-DO, 1XEV-DV and 3X. The 1XEV specification was developed by the Third Generation Partnership Project 2 (3GPP2), a partnership consisting of five telecommunications standards bodies: CWTS in China, ARIB and TTC in Japan, TTA in Korea and TIA in North America. It is also known as the High Rate Packet Data Air Interface Specification. It delivers 3G like services up to 140 kbps peak rate while occupying a very small amount of spectrum (1.25 MHz per carrier). 1XEV-DO, also called 1XEV Phase One, is an enhancement that puts voice and data on separate channels in order to provide data delivery at 2.4 Mbps. EV-DV, or 1XEV Phase Two promises data speeds ranging from 3 Mbps to 5 Mbps. However, CDMA2000 3 $\times$ is an ITU-approved, IMT-2000 (3G) standard. It is part of what the ITU has termed IMT-2000 CDMA MC. It uses a 5 MHz spectrum (3 $\times$ 1.25 MHz channels) to give speeds of around 2–4 Mbps.

1.4.2 UMTS

The Universal Mobile Telecommunications System (UMTS) is one of the third generation (3G) mobile phone technologies. It uses W-CDMA as the underlying standard. W-CDMA was developed by NTT DoCoMo as the air interface for their 3G network FOMA. Later it submitted the specification to the

International Telecommunication Union (ITU) as a candidate for the international 3G standard known as IMT-2000. The ITU eventually accepted W-CDMA as part of the IMT-2000 family of 3G standards. Later, W-CDMA was selected as the air interface for UMTS, the 3G successor to GSM. Some of the key features include the support to two basic modes FDD and TDD, variable transmission rates, intercell asynchronous operation, adaptive power control, increased coverage and capacity, etc. W-CDMA also uses the CDMA multiplexing technique, due to its advantages over other multiple access techniques such as TDMA. W-CDMA is merely the air interface as per the definition of IMT-2000, while UMTS is a complete stack of communication protocols designated for 3G global mobile telecommunications. UMTS uses a pair of 5 MHz channels, one in the 1900 MHz range for uplink and one in the 2100 MHz range for downlink. The specific frequency bands originally defined by the UMTS standard are 1885–2025 MHz for uplink and 2110–2200 MHz for downlink.

UMTS System Architecture

A UMTS network consists of three interacting domains: Core Network (CN), UMTS Terrestrial Radio Access Network (UTRAN) and User Equipment (UE). The UE or ME contains the mobile phone and the SIM (Subscriber Identity Module) card called USIM (Universal SIM). USIM contains member specific data and enables the authenticated entry of the subscriber into the network. This UMTS UE is capable of working in three modes: CS (circuit switched) mode, PS (packet switched) mode and CS/PS mode. In the CS mode the UE is connected only to the core network. In the PS mode, the UE is connected only to the PS domain (though CS services like VoIP (Voice over Internet Protocol) can still be offered), while in the CS/PS mode, the mobile is capable of working simultaneously to offer both CS and PS services.

The components of the Radio Access Network (RAN) are the Base Stations (BS) or Node B and Radio Network Controllers (RNCs). The major functions of the BS are closed loop power control, physical channel coding, modulation/demodulation, air interface transmissions/reception, error handling, etc., while major functions of the RNC are radio resource control/management, power control, channel allocation, admission control, ciphering, segmentation/reassembly, etc.

The main function of the Core Network (CN) is to provide switching, routing and transit for user traffic. The CN also contains the databases and network management functions. The basic CN architecture for UMTS is based on the GSM network with GPRS. All equipment has to be modified for UMTS operation and services. The CN is divided into the CS and PS domains.

Circuit switched elements are the Mobile Services Switching Centre (MSC), Visitor Location Register (VLR) and Gateway MSC. Packet switched elements are the Serving GPRS Support Node (SGSN) and the Gateway GPRS Support Node (GGSN). Network elements like EIR, HLR, VLR and AUC are shared by both domains. The Asynchronous Transfer Mode (ATM) is defined for UMTS core transmission. The ATM Adaptation Layer type 2 (AAL2) handles the circuit switched connection and the packet connection protocol AAL5 is designed for data delivery. A typical 3G network is shown in Figure 1.2.

UMTS QoS Classes

UMTS network services have different quality of service (QoS) classes for four types of traffic:

- conversational class (e.g. voice, video telephony, video gaming);
- streaming class (e.g. multimedia, video on demand);
- interactive class (e.g. web browsing, network gaming, database access);
- background class (e.g. email, SMS, downloading).

Conversational Class

The best examples of this class are voice traffic and real time data traffic such as video telephony, video gaming, etc. This traffic runs over CS bearers. The quality of this class is dependent totally on subscriber

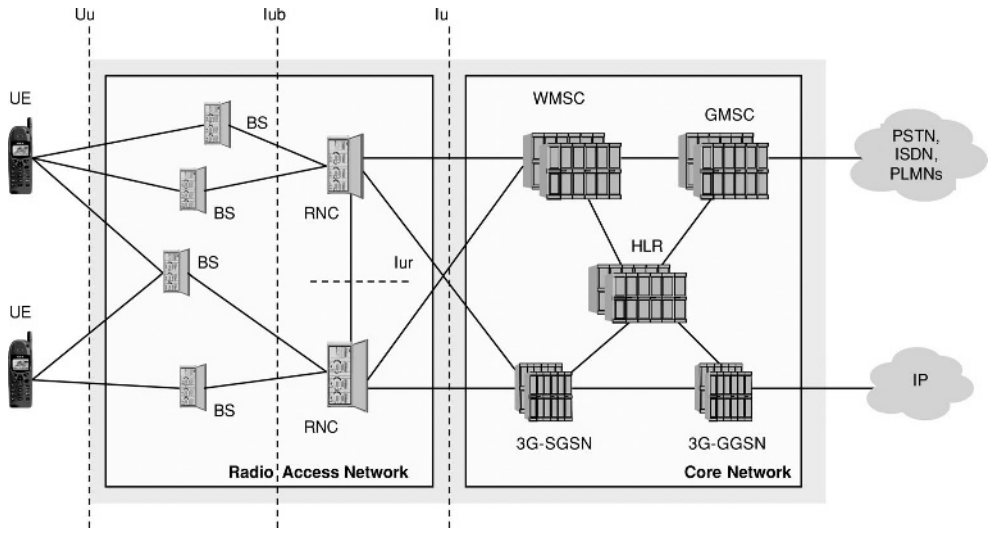

Figure 1.2 UMTS network

perception. The key aspect of this class is low end-to-end delays (e.g. less than 400 ms). For speech coding/decoding the adaptive multirate (AMR) technique will be used. Upon request, AMR coders can switch the bit rates every 20 ms of speech frame. Thus, during busy hours, bit rates can be lowered to offer higher capacity by sacrificing quality. Also, the coverage area of the cell can be increased by decreasing bit rates. Thus, this technique helps in balancing coverage, capacity and quality of the network.

Streaming Class

Multimedia, video on demand, etc., are examples of the streaming class. The data are transferred in a steady and continuous stream. How does this work? On the Internet, the display starts even when the entire file has not been downloaded. The delay in this class is higher than the conversational class.

Interactive Class

The Internet is a classical example of the interactive class. The subscriber requests the information from the server and waits for the information to arrive. Thus, delay is not the ster minimum under this class as the time to download also depends upon the number of subscribers logged on to the system and the system capacity itself. Another aspect of this service is that the transfer of data is transparent. Location based services and computer games are other examples of this class of service.

Background Class

Other applications such as SMS, fax, emails, etc., fall under the background class. Delay is the highest in this class of service. Also, the data transfer is not transparent as in the interactive class.

1.4.3 HSDPA in UMTS

High Speed Downlink Packet Access (HSDPA) is a packet based data service in the downlink having a transmission rate up to 8–10 Mbps over the 5 MHz bandwidth. This means that implementation of this technique will allow data speeds to increase to almost five times that of the most advanced Wideband Code Division Multiple Access (WCDMA) networks. Also, the base station capacity increased

by double. The system capacity and the user data rates are increased by implementation of HSDPA, which includes MIMO (Multiple Input Multiple Output), cell search, advanced receiver design, HARQ (Hybrid Automatic Request) and AMC (Adaptive Modulation and Coding). HSDPA is mainly intended for non-real-time traffic, but can also be used for traffic with tighter delay requirements (for more details refer to Appendix B).