BSc in Computer Engineering
CMP4204
Wireless Technologies

Lecture 10

Cellular Mobile

3G and UMTS

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

This page is intentionally blank

1. Introduction

From the days of 2G Global System for Mobile Communications (GSM) and CdmaOne there has been a demand for data services and with the rise of the Internet of Things (IoT) and Machine to Machine (M2M) communication the focus has moved from voice to data services, speed quality and low latency. Two technologies are key to this change Orthogonal Frequency Division Multiplexing (OFDM) and Multiple-Input Multiple-Output (MIMO) Antenna.

1.1 Orthogonal Frequency Division Multiplexing (OFDM)

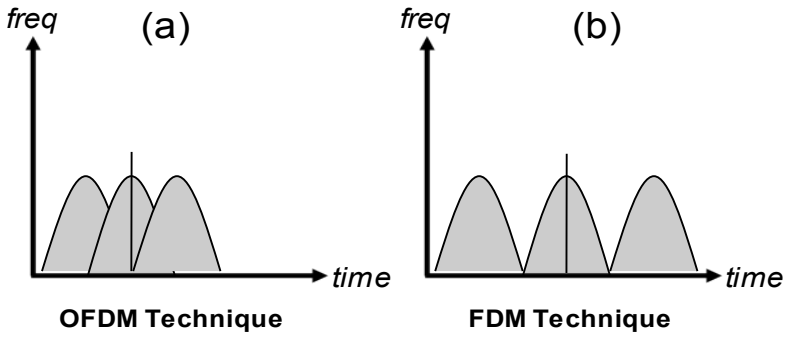

Illustration 1: OFDM Technique

OFDM is a particular form of Frequency Division Multiplex (FDM) where a datastream is transmitted over a number of low rate subcarriers. Unlike FDM instead of having the channels non overlapping as shown in Illustration 1 (b) OFDM makes more efficient use of spectrum by over-lapping the channels. This can only be achieved by reducing crosstalk between the carriers using a precise mathematical relationship between the frequencies, an orthogonal relationship. The sub-carrier frequencies are chosen so that the sub-carriers are orthogonal to each other, meaning that cross-talk between the sub-channels is eliminated and inter-carrier guard bands are not required.

To use OFDM the data to be transmitted is broken down into several streams that are broadcast simultaneously, on different frequencies, to a receiver that collects and reassembles them which makes it less susceptible to multipath and other radio interference.

This greatly simplifies the design of both the transmitter and the receiver; unlike conventional FDM, a separate filter for each sub-channel is not required. Each sub-carrier is modulated with a conventional modulation scheme such as QAM at a low symbol rate, maintaining data rates similar to conventional single-carrier modulation schemes in the same bandwidth.

The primary advantage of OFDM over single-carrier schemes is its ability to cope with severe channel conditions — for example, attenuation of high frequencies at a long copper wire, narrowband interference and frequency-selective fading due to multipath without complex equalisation filters. Channel equalisation is simplified because OFDM may be viewed as using many slowly-modulated narrowband signals rather than one

rapidly-modulated wideband signal. Low symbol rate makes the use of a guard interval between symbols affordable, making it possible to handle time-spreading and eliminate Inter Symbol Interference (ISI).

OFDM has developed into a popular scheme for wideband digital communication systems.

1.1.1 Summary of advantages

- Can easily adapt to severe channel conditions without complex equalisation
- Robust against narrow-band co-channel interference
- Robust against ISI and fading caused by multipath propagation
- High spectral efficiency
- Efficient implementation using Fast Fourier Transform (FFT)
- Low sensitivity to time synchronisation errors
- Tuned sub-channel receiver filters are not required (unlike conventional FDM)
- Facilitates Single Frequency Networks, i.e. transmitter macro-diversity.

1.2 Multiple-Input Multiple-Output (MIMO) Antenna

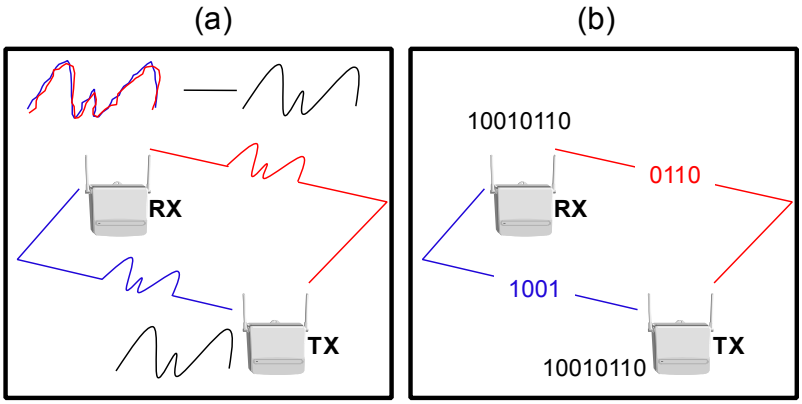

Illustration 2: MIMO

A MIMO antenna array is a set of antenna's at both ends of a link. The reasons for doing this are varied and a number of modes have evolved giving performance enhancements such as transmit-receive diversity and spatial multiplexing.

Diversity refers to the use of multiple antennas to increase the probability of a high quality signal path between the sender and the receiver. Referring to Illustration 2 (a) the transmitted signal follows multiple paths to the receiver with elements arriving at slightly out of phase from each other. The receiver can apply advanced signal processing algorithms to combine the different versions of the received signals to maximise Signal to Noise Ratio (SNR).

As can be seen from the diagram Illustration 2 (b) Spatial Division Multiplexing (SDM) allows the sender to transmit different portions of the user data on multiple paths in parallel to increase capacity.

2. Mobile Evolution

Mobile generations typically refer to non–backward-compatible cellular standards following requirements stated by International Telecommunication Union (ITU) Radiocommunication Sector (ITU-R), such as International Mobile Telecommunications (IMT) 2000 (IMT-2000) for 3G and IMT-Advanced for 4G.

Analogue 1G systems evolved into GSM and CdmaOne. The standard evolved so quickly to more than 170 countries and provided for over 60% of all 2G mobile subscribers worldwide. Data rates started to rise with 2.5G General Packet Radio Service (GPRS) to 172.2 kb/s and even further with Enhanced Data rates for GSM Evolution (EDGE) and EDGE Evolution to a maximum of 473 kb/s.

2.1 3G and Universal Mobile Telecommunications System (UMTS)

In 2000 the next generation of mobile wireless was released for operators who had chosen the GSM path at 2G. This started with Release '99 which offered separate 384 kb/s packet switched service from the 64kb/s circuit switched voice channel as well as location services and tandem free operation which allowed for improvements in voice quality on mobile to mobile calls by avoiding conversions to G.711 PCM. Another improvement 3G brought was the MultiMedia Messaging Service (MMS) as an enhancement to the popular Short Message Service (SMS) on 2G allowing the transfer of other that simple text. 3G also introduced the IP Multimedia Services (IMS), this created a pathway to All-IP to be realised in LTE.

Over time other improvements brought greater speeds and features.

- High-Speed Downlink Packet Access (HSDPA) improved downlink speeds up to 99.3 Mb/s.
- High-Speed Uplink Packet Access (HSUPA) improved uplink speeds up to 5.8 Mb/s which allow new over the top data services like Voice over IP (VoIP).
- Evolved High Speed Packet Access (HSPA+) improved on this further by increasing the downlink up to 84 Mb/s and up to 10.8 Mb/s in the uplink using 2x2 MIMO and higher order 64 QAM modulation

2.2 4G and the Evolved Packet Core (EPC)

In 2008 the first Long Term Evolution (LTE) release came from the 3GPP. LTE dropped the circuit switched channel in favour of a simplified All-IP model. LTE makes more use of MIMO and OFDM as used in WiFi.

3. Revised Radio Spectrum for 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. Compare this to the chart in lecture 08 notes.

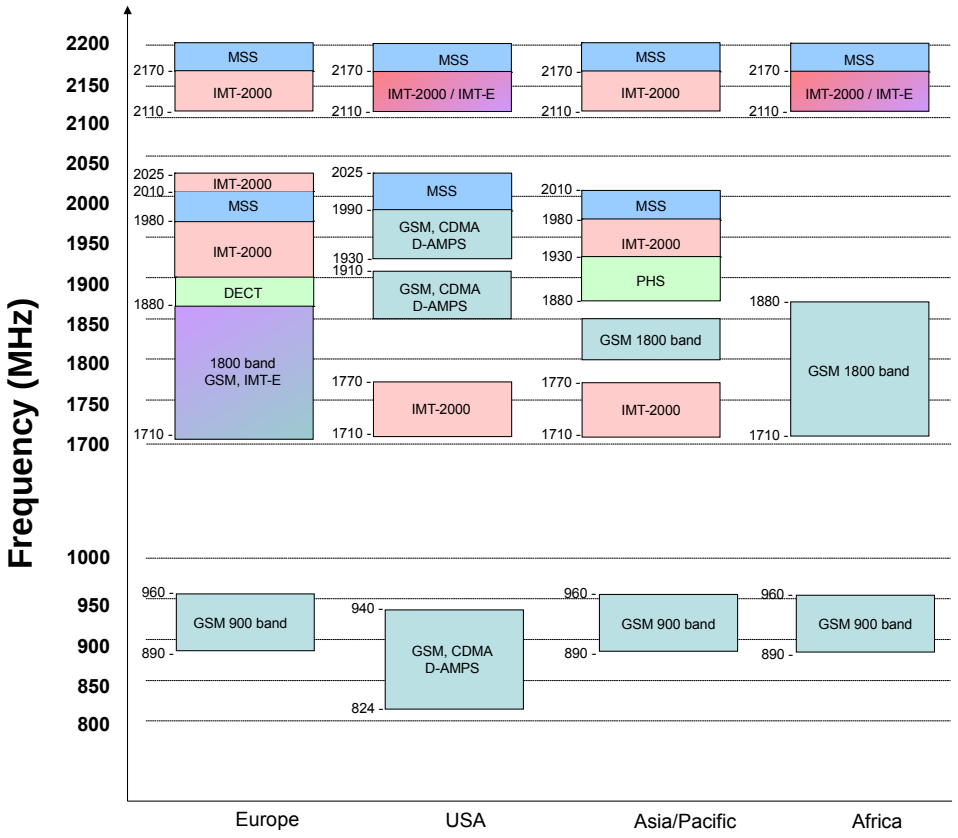

Illustration 3: Spectrum allocation

3.1 3G/3.5G

IMT-2000 is the global standard for third generation (3G) wireless communications. While the concept of a global 3G standard was admirable it is impractical for a number of reasons.

- Radio spectrum availability for IMT-2000 is not standard from country to country.
- GSM Operators want to reuse GPRS investment.
- As it is agreed that IMT-2000 should be CDMA based the existing cdmaOne operators required an upgrade path to reuse existing infrastructure.

As a result of this two groups formed to drive different flavours of IMT-2000 while maintaining the overall goals and aims of the umbrella standard.

- 3rd Generation Partnership Project (3GPP).
- 3rd Generation Partnership Project 2 (3GPP2).

3.2 4G

IMT-Advanced are the ITU requirements issued in 2008 for systems to be called 4G. These standards were a follow on from the IMT-2000 that heralded 3G in 2000. LTE standards from the 3GPP offering a bit rate of up to 100 Mb/s downlink and 50 Mb/s uplink with a 20 MHz channel and MIMO antennas and an all-IP core.

4. 3rd Generation Partnership Projects

4.1.1 3rd Generation Partnership Project (3GPP)

The 3GPP was created to produce globally applicable Technical Specifications and Technical Reports for a 3rd Generation Mobile System based on evolved GSM core networks and the radio access technologies that they support. For both Frequency Division Duplex (FDD) and Time Division Duplex (TDD) modes. The scope also includes the maintenance and development of GSM Technical Specifications and Technical Reports including GPRS and EDGE. The 3GPP are evolving the set of 3G standards called Universal Mobile Telephone System (UMTS). To date we have seen Release 99 and Release 4 and Release 5. UMTS offers the following advantages over 2G systems:

- Higher speech quality.
- Data rates of 2Mb/s, though initial releases will likely be lower than this.
- UMTS is a real global system, comprising both terrestrial and satellite components.
- Consistent service environment even when roaming via Virtual Home Environment (VHE).

4.1.2 3rd Generation Partnership Project Two (3GPP2)

ANSI/TIA/EIA-41 is a US core-network standard developed to support roaming between different cellular systems. The 3GPP2 was created by US and Asian interests to evolve 3G standards for ANSI/TIA/EIA-41 based carriers. The partners are Association of Radio Industries and Businesses (ARIB) and the Telecommunication Technology Committee (TTC) in Japan, China Wireless Telecommunication Standard (CWTS) in China, Telecommunications Technology Association (TTA) in Korea and the Telecommunications Industry Association (TIA) in North America.

The 3GPP2 standards are evolved from the cdmaOne 2G standard. Cdma2000 has already been implemented to several networks as an evolutionary step from cdmaOne as cdma2000 provides full backward compatibility with IS-95B. Cdma2000 is not constrained to only the IMT-2000 band, but operators can also overlay cdma2000 1x system, which supports 144 kb/s now and data rates up to 307 kb/s in the future, on top of their existing cdmaOne network.

4.1.3 ITU-R M.1457 – The 5 3Gs

As a result of these 3GPP groups work ITU-R M.1457 specifies five types of 3G radio interfaces:

- UMTS
  - IMT-2000 Code Division Multiple Access (CDMA) Direct Spread, also known as UTRA FDD. This is commonly known as Wideband CDMA (WCDMA).
  - IMT-2000 CDMA TDD, also known as UTRA TDD and Time Division Synchronous CDMA (TD-SCDMA).
- Cdma2000
  - IMT-2000 CDMA Multi-carrier, also known as Cdma2000 (3X) developed by 3GPP2. IMT-2000 CDMA2000 includes 1X components, like cdma2000 1X EV-DO.
- IMT-2000 TDMA Single Carrier, also known as UWC-136 (Edge) supported by Universal Wireless Communications Consortium (UWCC), replaced by 3G Americas in 2001.
- IMT-2000 Digital Enhanced Cordless Telecommunications (DECT) supported by DECT Forum.

5. Universal Mobile Telecommunications System (UMTS)

Universal Mobile Telecommunications System (UMTS) is one of the third-generation (3G) cell phone technologies. Currently, the most common form uses Wideband CDMA (W-CDMA) as the underlying air interface, is standardised by the 3GPP, and is the European answer to the ITU IMT-2000 requirements for 3G cellular radio systems.

To differentiate UMTS from competing network technologies, UMTS is sometimes marketed as 3GSM, emphasising the combination of the 3G nature of the technology and the GSM standard which it was designed to succeed.

UMTS, using W-CDMA, supports up to 14.0 Mb/s data transfer rates in theory (with HSDPA), although at the moment users in deployed networks can expect a transfer rate of up to 384 kb/s for Release 99 (R99) handsets, and 3.6 Mb/s for HSDPA handsets in the downlink connection. This is still much greater than the 9.6 kb/s of a single GSM error-corrected circuit switched data channel or 14.4 kb/s for cdmaOne, and offers access to the Internet and other data services on mobile devices.

5.1 UMTS Network

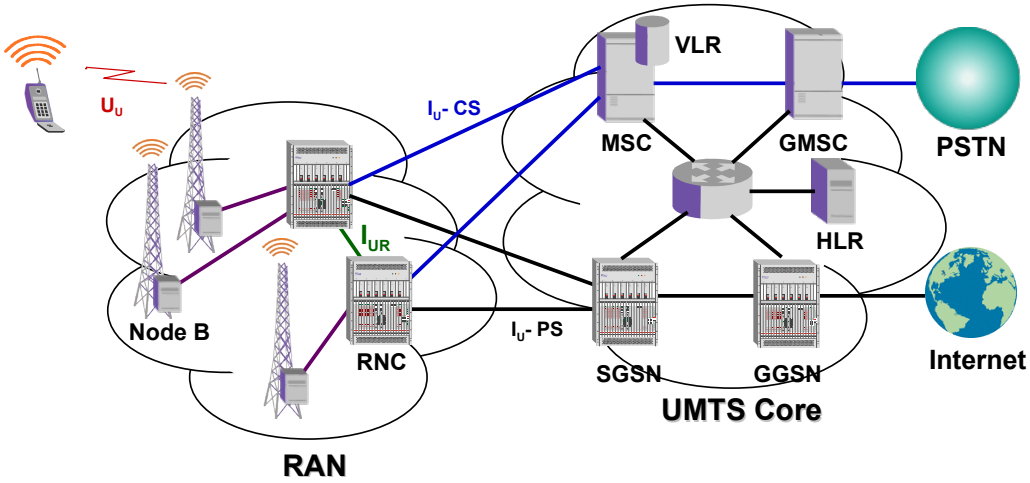

Illustration 4: UMTS network

UMTS Terrestrial Radio Access Network (UTRAN) has two separate flavours.

- Universal Terrestrial Radio Access (UTRA) Frequency Division Duplex (FDD).
- UTRA Time Division Duplex (TDD).

5.1.1 UTRA Frequency Division Duplex (FDD)

UTRA FDD uses a combination of FDD and CDMA. UTRA FDD is the 3G air interface mode currently being deployed by network operators in Europe and Japan to provide wide area access. The world's first commercial network was launched in Japan at the beginning of October 2001 and followed in December 2001 in Europe on the Isle of Man. UTRA FDD requires the allocation of two frequency bands:

- Uplink (UL).
- Downlink (DL).

It has the advantage of being able to transmit and receive at the same time. Furthermore, the size of the cell is not limited by propagation delays like in TDD because of the absence of time slots and guard periods, which also makes the timing synchronisation between base and mobiles less critical than TDD. Because it transmits and receive at the same time, FDD radio units need duplexers in order to separate the incoming and outgoing signals at the antenna. Duplexers are made of filters which increase the complexity and cost of the hardware. FDD does not allocate efficiently the available bandwidth for all types of services. A typical example is that of Internet Access where traffic patterns are small upstream bandwidth with large downstream bandwidth (i.e. like ADSL on wireline).

- Frequency band:
  - 1920 MHz -1980 MHz.
  - 2110 MHz - 2170 MHz FDD UL and DL.
- Minimum frequency band required: ~ 2 x 5 Mhz.

5.1.2 UTRA Time Division Duplex (TDD)

UTRA TDD uses a combined TDD and CDMA. Release 99 of the 3GPP specifications specified UTRA TDD with a chip rate of 3.84 Mcps operating in a 5MHz bandwidth to align with the UTRA FDD mode. In Release 4 of the 3GPP UMTS specifications, a second option was added to the UTRA TDD mode, the 1.28 Mcps option operating in a bandwidth of 1.6MHz. This harmonised UMTS with TD-SCDMA, another member of the IMT-2000 family of 3G standards, developed in China.

The UTRA TDD air interface mode deployments in Europe were as a complement to UTRA FDD by providing high density local area access. This is a consequence of the requirement for co-ordination of FDD and TDD network planning due to the particular UMTS frequency allocations. In other parts of the world, for example in China, where these network planning constraints do not exist, TDD can be deployed as a wide area access system.

UTRA TDD operates in the unpaired spectrum as UTRA FDD requires an UL and a DL so it uses the paired spectrum.

- Frequency band:
  - 1900 MHz -1920 MHz and 2010 MHz - 2025 MHz TDD Unpaired.
  - Channel spacing is 5 MHz and raster is 200 kHz.
  - Tx and Rx are not separated in frequency, but by guard period.
- Minimum frequency band required:
  - ~ 5 MHz with 3.84 Mcps.
  - ~ 1.6 MHz with 1.28 Mcps.

5.1.3 Time Division Synchronous CDMA (TD-SCDMA)

TD-SCDMA was proposed by CWTS group and approved by the ITU in 1999 and technology is being developed by the Chinese Academy of Telecommunications Technology and Siemens.

TD-SCDMA uses the TDD mode, which transmits uplink traffic (traffic from the mobile terminal to the base station) and downlink traffic (traffic from the base station to the terminal) in the same frame in different time slots.

TD-SCDMA was incorporated into UMTS UTRA TDD from Release 4 of the 3GPP UMTS specifications.

- Frequency band:
  - 2010 MHz - 2025 MHz in China.
- Minimum frequency band required:
  - 1.6 MHz.

5.2 UMTS Radio Access Network (RAN)

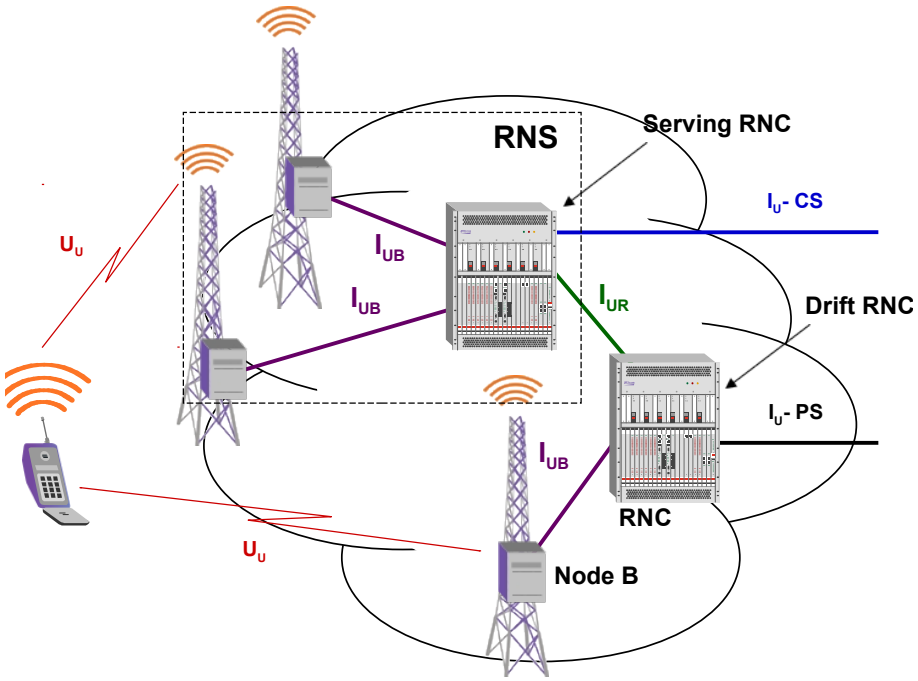

Illustration 5: UMTS Radio Access Network (RAN)

5.2.1 NodeB

The NodeB is the function within the UMTS network that provides the physical radio link between the Mobile Station (MS) and the network. Along with the transmission and reception of data across the radio interface the NodeB also applies the codes that are necessary to describe channels in a CDMA system.

5.2.2 Radio Network Sub-system / Radio Network Controller (RNC)

From the NodeB, perspective there is one Controlling RNC, where it's I_{UB} interface terminates. The Controlling RNC also exerts Admission Control for new mobiles or services attempting to use the NodeB. A Controlling RNC plus its NodeBs are called a Radio Network Subsystem (RNS).

From the Core Network point of view, the Serving RNC terminates the I_U for this MS. The Serving RNC also exerts Admission Control for new mobiles or services attempting to use the Core Network over its I_U interface. Admission Control ensures that mobiles are only allocated radio resources (bandwidth and signal/noise ratio) up to what the network has available.

Drift RNCs are RNCs who have NodeBs which also have a U_U interface to the MS. One or more Drift RNCs communicate with the Serving RNC via the I_{UR} interface where the signals can be combined to create a stronger signal. This mechanism also acts in the Soft handover process because the Drift RNC can become the Serving RNC as the MS moves further into its NodeB's sphere of influence.

5.3 UMTS Core Network

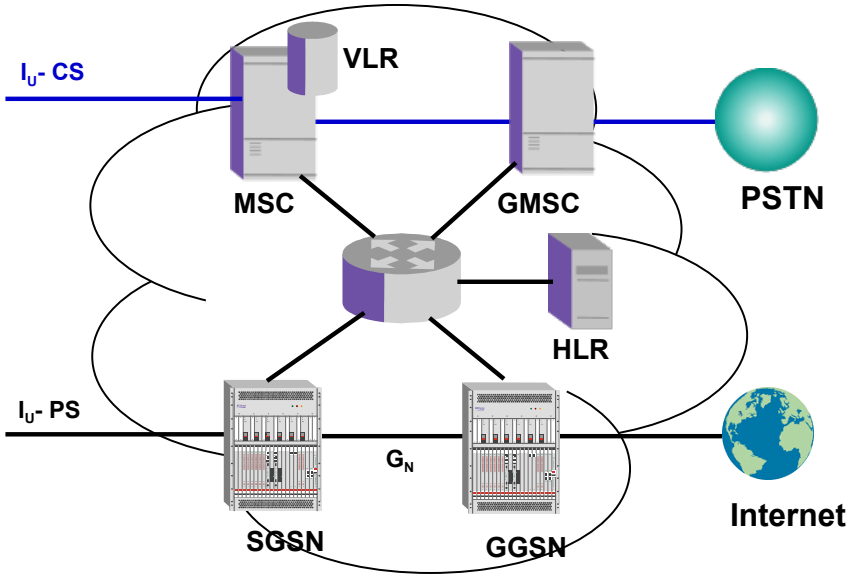

Illustration 6: UMTS core network

5.3.1 I_U Interface

I_U is the open Interface connecting UTRAN to Core Network (CN). I_U has two different instances:

- I_U CS for connecting UTRAN to Circuit switched (CS) CN.
- I_U PS to connect UTRAN to Packet Switched (PS) CN.

The function of I_U includes split responsibility and services towards CN which is provided by UTRAN, handles time alignments, error control, initialisation etc.

5.3.2 G_N Interface

The G_N interface is the GPRS interface located between the GPRS Support Nodes (GSN).

5.3.3 Mobile Switching Centre (MSC) / Visitor Location Register (VLR)

The RNCs are connected to a Mobile Switching Centre (MSC) to handle voice calls via I_U PS. The MSC is a telecommunication exchange which has a VLR database containing all subscriber data required for call handling and mobility management for mobile subscribers currently located in the area controlled by the MSC/VLR.

5.3.4 Gateway Mobile Switching Centre (GMSC)

The GMSC provides a gateway function to the Public Switched Telephone Network (PSTN). It terminates the PSTN signalling and traffic formats and converts this to protocols employed in mobile networks. For mobile terminated calls, it interacts with the Home Location Register (HLR) to obtain routing information.

5.3.5 Serving GPRS Support Node (SGSN)

The SGSN tracks the location of an individual MS and performs security functions and access control for packet services. It interfaces to the RNCs via the I_U CS Interface.

5.3.6 Gateway GPRS Support Node (GGSN)

The 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.

5.3.7 Home Location Register (HLR)

The HLR is a database within the Home Network of the MS. It provides routing information for terminated MS calls and SMS. It is also responsible for the maintenance of user subscription information. This is distributed to the relevant VLR or SGSN.

5.3.8 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.

5.4 UMTS Packet Services

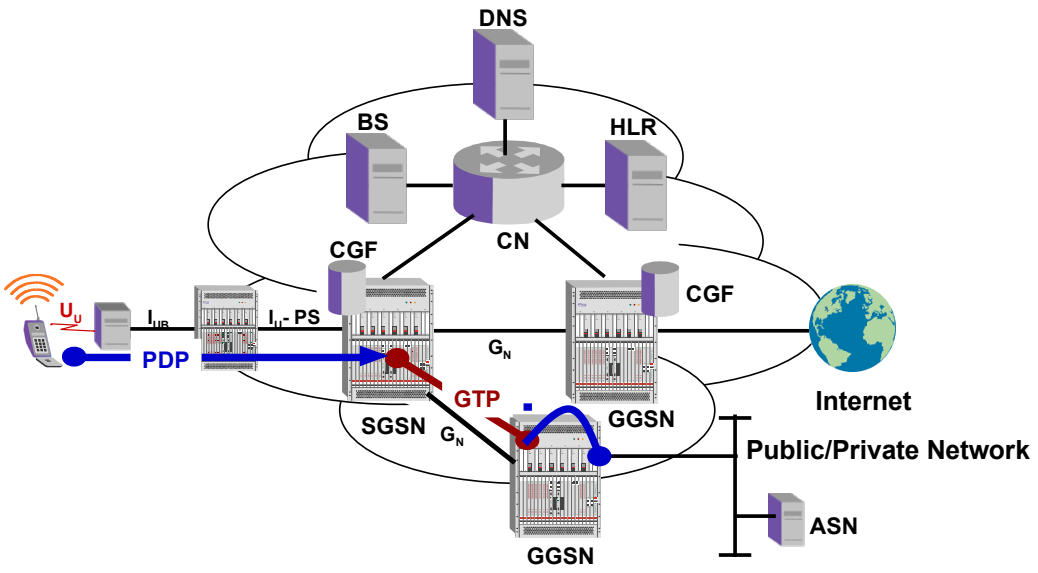

Illustration 7: UMTS packet connection

For a packet data connection in UMTS the process previously described for GPRS is more or less identical as UMTS implements the GPRS Core for packet services.

A Packet Data protocol (PDP) Context is established from the MS to the SGSN.

The SGSN establishes a GPRS Tunnelling Protocol (GTP) tunnel with the selected 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. Layer 2 Tunnelling Protocol (L2TP) to an L2TP Network Server (LNS) on a corporate network.

5.5 High-Speed Downlink Packet Access (HSDPA)

HSDPA is a 3G mobile telephony communications protocol which allows UMTS networks to have higher data transfer speeds and capacity. Current HSDPA deployments support down-link speeds of 1.8, 3.6, 7.2 and 14.4 Mb/s. The networks are then to be upgraded to Evolved HSPA (HSPA+), which provides speeds of 42 Mb/s downlink in its first release.

5.6 High Speed Uplink Packet Access (HSUPA)

The second major upgrade process is to upgrade the uplink by adding a new transport channel called the Enhanced Dedicated Channel (E-DCH). An enhanced uplink created opportunities for a number of new applications including VoIP, uploading pictures and sending large e-mail messages. The enhanced uplink increases the data rate up to 5.8 Mb/s) and also reduces latency.

5.7 Evolved High-Speed Packet Access (HSPA+)

HSPA+ provides extensions to the existing HSPA definitions and is therefore backward-compatible. It provides data rates up to 84 Mb/s in the downlink and 10.8 Mb/s in the uplink with 2x2 MIMO technologies and a higher order 64QAM modulation. With Dual Cell technology, these can be doubled.

6. Cdma2000

Cdma2000 is a hybrid 2.5G / 3G protocol of mobile telecommunications standards that use CDMA, a multiple access scheme for digital radio, to send voice, data, and signalling data (such as a dialled telephone number) between mobile phones and cell sites. Cdma2000 is considered a 2.5G protocol in 1xRTT and a 3G protocol in EVDO.

As described earlier in this section CDMA permits many simultaneous transmitters on the same frequency channel, unlike TDMA, used in GSM and D-AMPS, and FDMA, used in AMPS (US 1G). Since more phones can be served by fewer cell sites, CDMA based standards have a significant economic advantage over TDMA or FDMA based standards. Cdma2000 remains compatible with the older cdmaOne.

The Cdma2000 standards Cdma2000 1xRTT, Cdma2000 EV-DO, and Cdma2000 EV-DV are approved radio interfaces for the ITU's IMT-2000 standard and a direct successor to 2G CDMA, IS-95 (cdmaOne). Cdma2000 is standardised by 3GPP2.

Cdma2000 is an incompatible competitor of the other major 3G standard UMTS. It is defined to operate at 450 MHz, 700 MHz, 800 MHz, 900 MHz, 1700 MHz, 1800 MHz, 1900 MHz, and 2100 MHz.

Below are the different types of Cdma2000, in order of increasing complexity:

- Cdma2000 1x Radio Transmission Technology (RTT), 1xRTT
  - Cdma2000 1xRTT, the core Cdma2000 wireless air interface standard, is also known as 1x, 1xRTT, and IS-2000. The designation "1x", meaning "1 times Radio Transmission Technology", indicates the same RF bandwidth as IS-95 cdmaOne.
  - A duplex pair of 1.25 MHz radio channels. This contrasts with 3xRTT, which uses channels 3 times as wide (3.75 MHz) channels.
  - 1xRTT almost doubles the capacity of IS-95 by adding 64 more traffic channels to the forward link, orthogonal to (in quadrature with) the original set of 64.
  - Although capable of higher data rates, most deployments are limited to a peak of 144 kb/s.
  - 1xRTT officially qualifies as 3G technology, but it is considered by some to be a 2.5G (or sometimes 2.75G) technology. This allows it to be deployed in 2G spectrum in some countries that limit 3G systems to certain bands.
- Cdma2000 3xRTT
  - Cdma2000 3xRTT (EV-DO Rev. B) utilises a pair of 3.75 MHz radio channels (i.e., 3 X 1.25 MHz) to achieve higher data rates. The 3x version of Cdma2000 is sometimes referred to as Multi-Carrier (MC). The 3x version of Cdma2000 has not been deployed and is not under development at present.

- Cdma2000 EV-DO
  - EVolution-Data Only.
- Cdma2000 EV-DV
  - EVolution-Data/Voice.
  - Cdma2000 was implemented to several networks as an evolutionary step from cdmaOne as cdma2000 provides full backward compatibility with IS-95B.

6.1 Cdma2000 Network

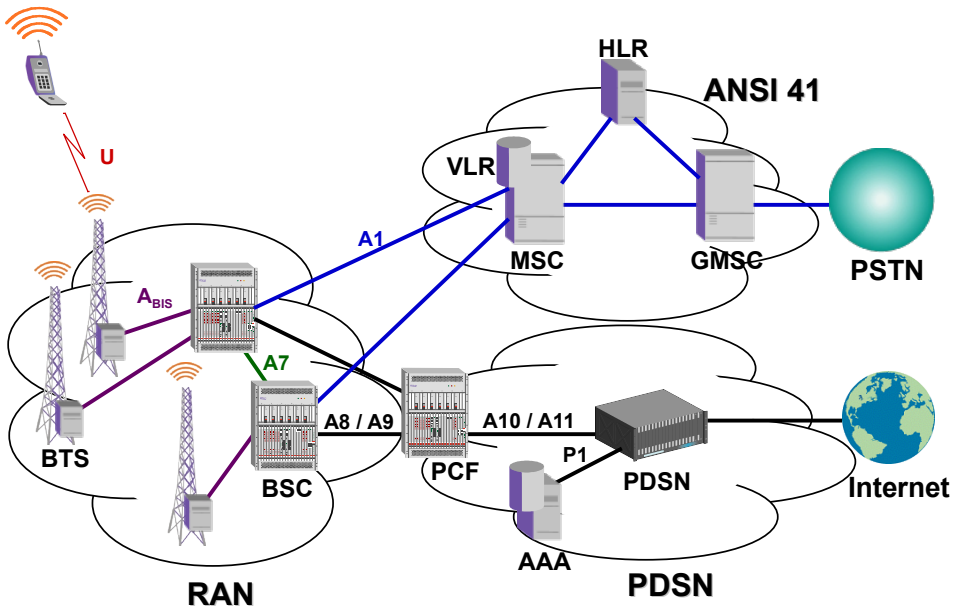

Illustration 8: Cdma2000 network

cdma2000 is not constrained to only the IMT-2000 band, but operators can also overlay a cdma2000 1x system, which supports 144 kb/s now and data rates up to 307 kb/s in the future, on top of their existing cdmaOne network.

- Frequency band: Any existing band.
- Minimum frequency band required:
  - 1x: 2 x 1.25 MHz.
  - 3x: 2 x 3.75 MHz.
- The network consists of 3 main groups:
  - RAN.
  - Packet Data Switching Network (PDSN).
  - ANSI-41 Voice Network.

6.2 Cdma2000 Radio Access Network (RAN)

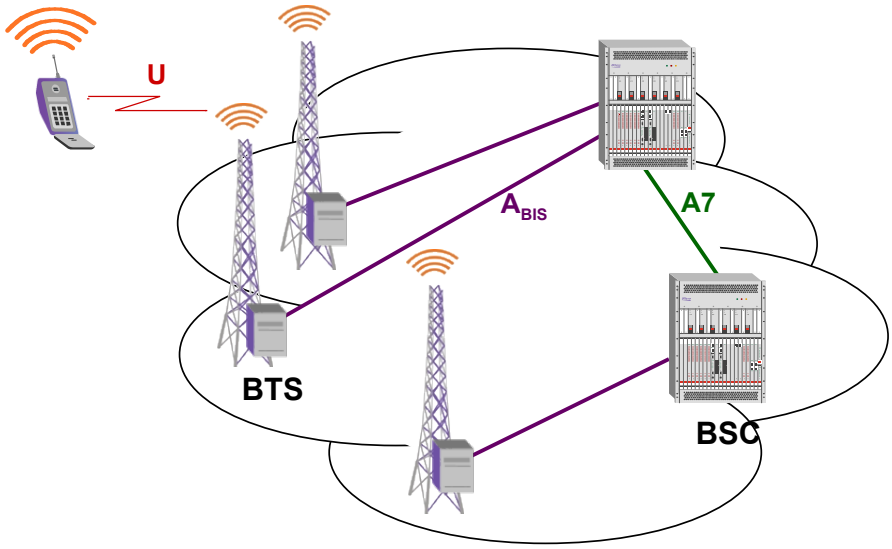

Illustration 9: Cdma2000 Radio Access Network (RAN)

6.2.1 Base Transceiver Station (BTS)

The Cdma2000 RAN consists of a Base Transceiver Station (BTS) which handles the air interface to the Mobile Station (MS). BTS units fulfil the same function as the NodeB in UMTS.

6.2.2 Base Station Controller (BSC) / Packet Control Function (PCF)

The BSC and PCF may reside in the same physical unit. These aggregate the BTS unit traffic and are responsible for the exchange of messages towards the MSC (Mobile Switching Centre) and the BTS. Traffic and signalling transferred between the MSC and MS (Mobile Station) will usually pass transparently through a BSC. The BSC also switches traffic destined for the PDSN to the PCF function which sends the traffic to the PDSN over a Mobile IP (MIP) tunnel in the A10 interface. This tunnel uses Generic Routing Encapsulation (GRE) format.

6.3 Cdma2000 ANSI-41

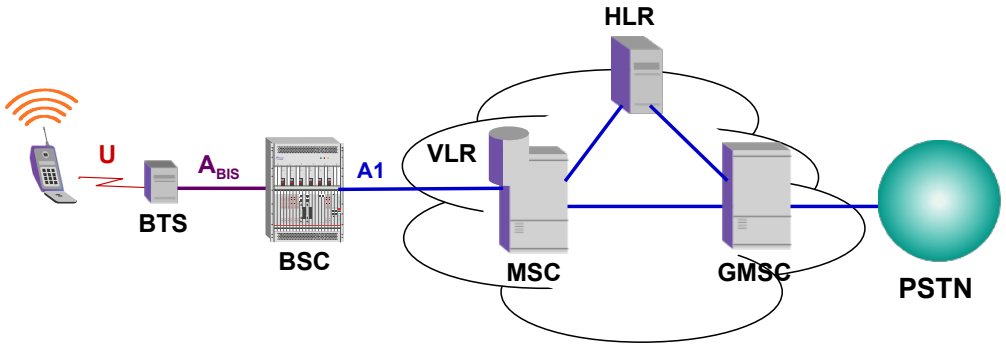

Illustration 10: Cdma2000 ANSI-41

ANSI-41 is a standard for identifying and authenticating users, and routing calls on mobile phone networks. The standard also defines how users are identified and calls are routed when roaming across different networks.

ANSI-41 is the standard used by AMPS (US analogue), D-AMPS IS-136 (TDMA) IS-95 cdmaOne and IS-2000 Cdma2000 CDMA networks.

6.3.1 Mobile Switching Centre (MSC)

The BSCs are connected to a MSC to handle voice calls. The MSC is a telecommunication exchange which has a VLR database containing all subscriber data required for call handling and mobility management for mobile subscribers currently located in the area controlled by the MSC/VLR. The A1 interface carries signalling information between the Call Control and Mobility Management functions of the MSC and the call control component of the BSC.

6.3.2 Home Location Register (HLR)

When the MSC/VLR does not have information on a subscriber it consults the HLR database of the subscriber. The HLR provides routing information for MT (Mobile Terminated) calls and SMS (Short Message Service). It is also responsible for the maintenance of user subscription information. This is distributed to the relevant VLR (Visitor Location Register).

6.3.3 Gateway Mobile Switching Centre (GMSC)

The GMSC provides a mediation function with the PSTN. It terminates the PSTN signalling and traffic formats and converts this to protocols employed in mobile networks. For mobile terminated calls, it interacts with the HLR to obtain routing information.

6.4 Cdma2000 PDSN with Simple IP

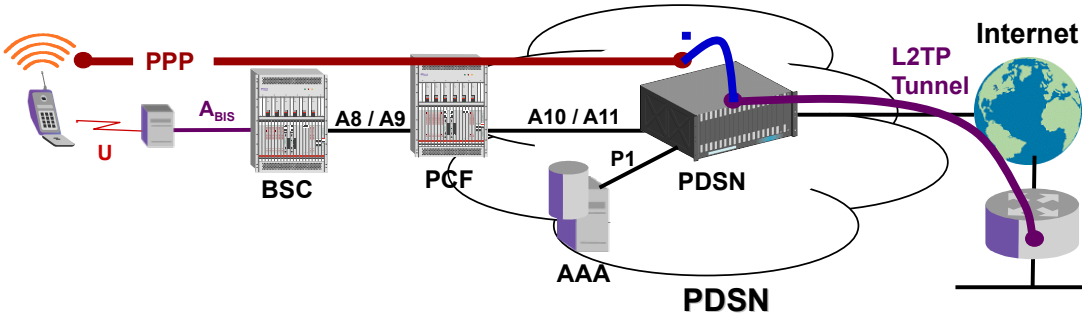

Illustration 11: Cdma2000 PSDN with simple IP

6.4.1 Packet Data Serving Node (PDSN)

The PDSN is responsible for the establishment, maintenance and termination of a Point to Point Protocol (PPP) session towards the MS. The PDSN tunnel switches incoming MIP connections to their final termination point using L2TP. The authentication and endpoint destination of the L2TP tunnel is determined by a Authentication, Authorisation and Accounting (AAA) RADIUS Server. The AAA RADIUS Server may have to consult a remote 'home' AAA RADIUS Server or the remote tunnel terminator may also need to authenticate the incoming tunnel as a further line of authorisation.

6.4.2 Data Call flow - Simple IP

The MS roams onto a new network and wishes to make a data connection. It sends a request to the BSC which forwards the request to the PDSN. The MS negotiates a PPP connection to the PDSN in a GRE tunnel (A10 Interface) and in the negotiation hands off its ID and security data to the PDSN. The PDSN uses this data to create a RADIUS Access Request. If the AAA RADIUS Server authenticates the user the and the AAA RADIUS Server returns an L2TP Tunnel end-point then the PPP connection is tunnelled to an LNS. The LNS Terminates the PPP connection so the MS receives its IP address from the remote network.

6.5 Cdma2000 PDSN with Mobile IP

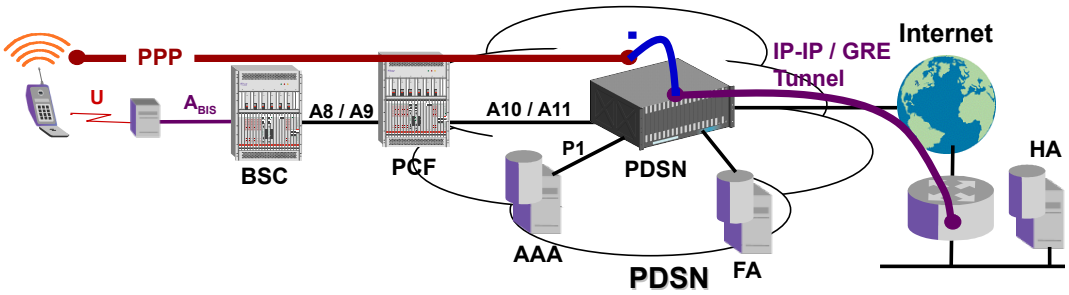

Illustration 12: Cdma2000 PDSN with Mobile IP

6.5.1 Data Call flow - Mobile IP

The MS roams onto a new network and wishes to make a data connection. It sends a request to the BSC. The BSC forwards the request to the PDSN. The MS negotiates a PPP connection to the PDSN in a GRE tunnel (A10 Interface) and in the negotiation hands off its ID and security data to the PDSN. The PDSN uses this data to create a RADIUS Access Request. If the AAA RADIUS Server authenticates the user the PPP connection is established. Once PPP is complete, the PDSN and MS go through the Agent Advertisement (AA) phase. The purpose of the PDSN sending AA is for the Mobile to discover the Foreign Agent (FA) and obtain a Care of Address (CoA) IP address.

The next step is the FA Challenge (FAC); this is the procedure by which the MIP registration is authenticated at the PDSN using Home Agent (HA) AAA RADIUS Server (HAAA). The PDSN sends a challenge during Agent Advertisement and the MIP Mobile Node (MN) sends back a response for this challenge in MIP registration. A RADIUS access request is built using this information and Authenticated at the HAAA. Once MIP registration has been successfully completed, an IP tunnel is created between the HA and the PDSN. IP traffic can now travel from the HA to the CoA via the tunnel and then on to the MN. The tunnelling schemes supported are IP in IP and GRE.

Typically tunnelling only applies from the Calling Station (CS) via the HA through the tunnel to the PDSN CoA and on the MN. Traffic from the MN to the CS can route directly from MN/PDSN to the CS without passing through the tunnel. This is called triangular routing. One problem with triangular routing is Firewalls that expect a two way conversation to start and end at the same set of IP addresses. To overcome this problem a tunnel must also be built from the CoA to the HA, this is called Reverse Tunnelling.

7. Self-test Quiz

1. Briefly describe each of the following:
   - EDGE
   - HSPDA
   - HSPA+
   - HSUPA.
2. Describe the difference between UTRA FDD and UTRA TDD and explain how each is used.