SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE
www.sathyabama.ac.in

SCHOOL OF ELECTRICAL AND ELECTRONICS

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

UNIT – I – Wireless Communication –SEC1404

I. INTRODUCTION

UNIT 1 OVERVIEW OF WIRELESS COMMUNICATION

History of wireless communication - Spectrum allocation for wireless communication - Standard bodies for wireless communication - Evolution of wireless communication starting from 1G to 5G - Cellular system concepts - Circuit switched and Packet switched cellular systems - architecture and operation of cellular systems - Frequency reuse - Channel Assignment(Fixed ,Dynamic, Hybrid).Flat fading and frequency selective fading - Diversity techniques (time, frequency, space) - PCS network architecture - Handoff - inter BS handoff-Inter system handoff - Hard handoff and soft handoff.

HISTORY OF WIRELESS COMMUNICATION

The history of Wireless Communications started with the understanding or magnetic and electric properties observed during the early days by the Chinese, Greek and Roman cultures and experiments carried out in the 17th and 18th centuries.

1807 – French mathematician Jean Baptiste Joseph Fourier discovered Fourier’s theorem

1820 – Danish physicist Hans Christian Orsted discovered the electromagnetic field caused by electric current. The French physicist Dominique Francois Jean Arago showed that a wire became a magnet when current flowed through it. French mathematician and physicist Andre-Marie Ampere discovered electrodynamics and proposed an Electromagnetic Telegraph.

1831 – British scientist Michael Faraday discovered electromagnetic induction and predicted existence of electromagnetic waves.

1834 – American inventor Samuel Finley Breese Morse invented the code for telegraphy named after him.

1847 – German physiologist and physicist Hermann Ludwig Ferdinand von Helmholtz suggested electrical oscillation

1853 – William Thomson (Lord Kelvin) calculated the period, damping and intensity as a function of the capacity, self-inductance and resistance of an oscillatory circuit.

1857 – Feddersen verified experimentally the resonant frequency of a tuned circuit as suggested by Helmholtz in 1847.

1864 – Scottish mathematician and physicist James Clerk Maxwell formulated the electromagnetic theory of light and developed the general equations of the electromagnetic field. He formulated 20 equations that were later simplified into the 4 basic equations we use today.

1866 - American dentist Dr. Mahlon Loomis described and demonstrated a wireless transmission system which he patented in 1866. Loomis demonstrated the transmission of signals between two mountains, a distance of 22 km.

1882 – American physicist, Amos Emerson Dolbear, was granted a patent for a wireless transmission system using an induction coil, microphone and telephone receiver and battery. Nathan Stubblefield transmitted audio signals without wires.

1883 – Irish physicist and chemist George Francis FitzGerald published a formula for the power radiated by a small loop antenna.

1884 – German physicist Heinrich Rudolf Hertz wrote Maxwell's equations in scalar form by discarding the concept of aether reducing it from 20 to 12 equations.

1885 – Thomas Edison patented a system of wireless communication by electrostatic induction.

1886 – Heaviside introduced impedance as the ratio of voltage over current. Hertz started his work to demonstrate the existence of radio waves and published his results in 1888.

1887 – English physicist Oliver Joseph Lodge discovered Sympathetic Resonance (standing waves) in wires.

1888 – Hertz produced, transmitted, and received electromagnetic waves (5 m to 50 cm) using reflectors to concentrate the beam. Hertz also discovered the principle for Radar. Heaviside wrote Maxwell's equations in vector form – the four equations we use today. Italian Galileo Farrari and Croatian-American Nilola Tesla independently produced rotating fields using 2-phase currents. Austrian engineer Ernst Lecher established the relation between frequency, wire length, velocity of propagation and the electrical constants of the wire.

1890 – Lecher used standing waves produced in parallel wires to measure frequency. Tesla introduced high frequency currents in therapeutics as he observed that current of high frequency could raise the temperature of living tissue. Tesla also patented his Tesla Coil which was used later in every spark gap generator to produce high frequency signals. Heinrich Rubens and R. Titter made a

sensitive bolometer which measured the intensity of electromagnetic waves by means of the heat generated in a thin wire.

1893 – English physicist Joseph John Thomson published the first theoretical analysis of electric oscillations within a conducting cylindrical cavity of finite length suggesting the possibility of wave propagation in hollow pipes (waveguides). Hertz conducted experiments of EM shielding and for coaxial configuration.

1895 – Marconi transmitted and received a coded message at a distance of 1.75 miles near his home in Bologna, Italy. Indian physicist, Sir Jagadis Chunder Bose generated and detected wireless signals and produced many devices such as waveguides, horn antennas, microwave reflectors and more.

1897 – Marconi demonstrated a radio transmission to a tugboat over an 18 mile path over the English Channel. The first wireless company, Wireless Telegraph and Signal Company was founded – they bought most of Marconi's patents. Lord Rayleigh suggests EM wave propagation in waveguides and analysis of propagation through dielectrically filled waveguides. Lodge patented various types of antennas.

1899 – Marconi sent the first international wireless message from Dover, England to Wimereux, France.

1900 – Tesla obtained patents on System of Transmission of Electrical Energy which the US recognized as the first patents on Radio. Tesla is the first person to describe a system of determining the location of an object using radio waves – Radar.

1902 – Fessenden patented the Heterodyne receiver. American Cornelius D. Ehret filed patents covering the transmission and reception of coded signals or speech (Frequency Modulation – FM). Poulsen was the first to develop the CW transmitter.

1903 – Marconi established a transmission station in South Wellfleet, MA – the dedication included exchanges of greetings between American President Theodore Roosevelt and British King Edward VII. G.

1904 – Frank J. Sprague developed the idea of the printed circuit. W. Pickard filed a patent application for a crystal detector where a thin wire was in contact with silicon. It was the central component in early radio receivers called crystal radios. J. C. Bose was granted a patent on point contact diodes that were used for many years as detectors in the industry. Fleming suggested the rectifying action of the vacuum-tube diode for detecting high

frequency oscillation – the first practical radio tube.

1905 – Fessenden invented the superheterodyne circuit.

1906 – Lee de Forest patented the general principle of omni-range using a rotating radio beam keyed to identify the sector forming 360 degree sweep of the beam. He also invented the three-electrode valve or vacuum tube triode that was instrumental in the development of transcontinental telephony in 1913. Poulsen transmitted music by wireless using an arc transmitter with 1 kW of input power and a 200 feet high antenna that was heard 300 miles away.

1909 – Marconi and Braun shared the Nobel Prize for Physics for their contributions to the physics of electric oscillations and radiotelegraphy.

1911 – Von Lieben and Eugen Riesz developed a cascade amplifier. Hugo Germsback, an American novelist, envisaged the concept of pulse radar in one of his works where he proposed the use of a pulsating polarized wave, the reflection of which was detected by an actinoscope.

1911 – Engineers start to realize that the triode can also be used for transmitter and oscillator – the three-electrode vacuum tube was included in designs for telephone repeaters in several countries.

1912 – G. A. Campbell developed guided wave filters. Sinding and Larsen transmitted TV by wireless using 3 channels. The Institute of Radio Engineers was formed in the US.

1914 – The German physicist Walter Schottky discovered the effect of electric field on the rate of electron emission from thermionic-emitters named after him. Fleming discovered the atmospheric refraction and its importance in the transmission of EM waves around the Earth. Carl R. Englund was the first to develop the equation of a modulated wave (AM) and also discovered the frequencies related to sidebands. Frequency modulation of a carrier was proposed to accommodate more channels within the available bandwidths.

1915 – Schottky stated work on the space-charge-grid tube and a screen grid tube or Tetrode that achieved good amplification by placing a screen grid between the grid and the anode.

1916 – Leon m Brillouin and Georges A. Beauvais patented the R-C coupled amplifier. F. Adcock used open vertically spaced aerials for direction finding in aircraft and granted British patent.

1918 – Armstrong invented the Superheterodyne Radio Receiver using 8 valves – most receivers still use this design today. Langmuir patented the feedback amplifier. E. H. O Shaughnessy development of direction finding was one of the key weapons in England during WWI – Bellini-Tosi aerials were installed around the coast to locate transmission from ships and aircrafts. Louis Alan Hazeltime invented the neutrodyne circuit with tuned RF amplifier with neutralization.

1919 – Marconi-Osram company developed the U-5 twin-anode full-wave rectifier. Joseph Slepian filed a patent application for a vacuum tube electron multiplier. Sir Robert Alexander Watson-Watt patented a device for radiolocation by means of short-wave radio waves – the forerunner of the Radar system.

1921 - E. S. Purington made the all-electric frequency modulator. A.W. Hull invented the Magnetron oscillator operating at 30 kHz and output power of 8 kW and 69 percent efficiency. E. H. Colpitt and O. B. Blackwell developed modulation of an audio frequency carrier by signals of lower audio frequency for carrying telephony over wires. S. Butterworth published a classic paper on HF resistance of single coil considering skin and proximity effect.

1922 – Walter Guiton Cady invented the piezoelectric (Quartz) crystal oscillator. The BBC broadcasts is first news program.

1923 – The decibel (1/10th of a bel, after A. G. Bell, inventor of the telephone) was used to express the loss in a telephone cable. H. W. Nichols developed point-to-point communication using single side-band communication. D.C Prince analyzed Class A and Class C amplifiers. Scottish engineer Antoine Logie Barid built and patented the first practical TV. Watson-Watt perfected the radiolocation device by displaying radio information on a cathode ray oscilloscope telling the radar operator the direction, distance and velocity of the target. Ralph Vinton Lyon Hartley showed that the amount of information that can be transmitted at a given time is proportional to the bandwidth of the communication channel. H. Flurschein filed a patent on radio warning system for use on vehicles.

1924 – J.R. Carson showed that energy absorbed by a receiver is directly proportional to its bandwidth and extended Lorentz's reciprocity theory to EM fields to antenna terminals. Lloyd Espenschied invented the first radio altimeter. The mobile telephone was invented by Bell Telephone Company and introduced to NYC police cars.

1925 – First conference on frequency allocation was held in Geneva. Joseph Tykocinski-Tykociner demonstrated that the

characteristics of a full size antenna can be replaced with sufficient accuracy from measurements made on a small short wave in the rage of 3 to 6 m.

1926 – L.E. Lilienfield patented the theory of the Field-Effect Transistor. Japanese engineers Hidetsugu Yagi and Shintaro Uda developed the Yagi antenna, a row of aerials consisting of one active antenna and twenty undriven members as a wave canal. Hulsenback and Company patented identification of buried objects using CW radar.

1927 – R. V. Hartley developed the mathematical theory of communications. Harold Stephen Black of Bell Laboratories conceived the negative feedback amplifier. A. de Hass studied fading and independently developed diversity reception system.

1928 – Baird conducted the first transatlantic TV broadcast and built the first color TV. Nyquist published a classic paper on the theory of signal transmission in telegraphy. He developed the criteria for the correct reception of telegraph signals transmitted over dispersive channels in the absence of noise. C.S. Franklin patented the coaxial cable in England to be used as an antenna feeder.

1929 – L. Cohen proposed circuit tuning by wave resonance (resonant transmission line) and its application to radio reception. H.A. Affel and L. Espenscheid of AT&T/Bell Labs created the concept of coaxial cable for a FDMA multi-channel telephony system. K. Okabe made a breakthrough in cm-waves when operating his slotted-anode magnetron (5.35 GHz). Hans Erich Hollmann patented the idea of a reflex klystron with his double-grid retarding-field tube. W.H. Martin proposed the Decibel as a transmission unit.

1931 – H. diamond and F. W. Dunmore conceived a radio beacon and receiving system for blind landing of aircraft. H. E. Hollmann built and operated the first decimeter transmitter and receiver at the Heinrich Hertz Institute. He called the device the magnetron.

1932 – The word Telecommunication was coined and the International Telecommunications Union (ITU) was formed. George C. Southworth and J. F. Hargreaves developed the circular waveguide. Karl Jansky accidentally discovered radio noise coming from outer space giving birth to radio astronomy. R. Darbord developed the UHF Antenna with parabolic reflector.

1933 – Armstrong demonstrated Frequency Modulation (FM) and proposed FM radio in 1936. C.E. Cleeton and N. H. Williams made a 30 GHZ CW oscillator using a split-anode magnetron.

1934 – The Federal Communications Commission (FTC) was created in the US. W.L. Everitt obtained the optimum operating conditions for Class C amplifiers. F. E. Terman demonstrated a transmission line as a resonant circuit. German physicist Oskar Ernst Heil applied for a patent on technology relating electrical amplifiers and other control arrangements that was the theoretical invention of capacitive current control in FETs.

1935 – C. J. Frank of Boonton Radio Corp demonstrated Q-meter at the fall meeting of IRE – the ratio of reactance to resistance of a coil as its "Quality Factor" was first suggested about 1926. A French TV transmitter was installed on top of the Eiffel Tower. Watson-Watt developed and patented the first practical radar for use in the detection of airplanes in England. H. E. Hollmann filed a patent for the multi-cavity magnetron (granted in 1938).

1936 – H. W. Doherty developed a new high efficiency power amplifier for modulated waves, Doherty amplifier, at Bell Labs. English engineer Paul Eisler devised the Printed Circuit. N. H. Jack patented the semi-rigid coaxial cable using thin soft copper tube as the outer conductor. Harold Wheeler used two flat copper strips side by side to make a low loss transmission line that could be rolled to save space. H. T. Friis and A. C. Beck invented the horn reflector antenna with dual polarization.

1937 – Grote Rober constructed the first radio telescope. W. R. Blair patented the first anti-aircraft fire control radar. Russell H. Varian and his brother Sigurd Varian along with William Hansen developed the reflex Klystron. Alex H. Reeves invented pulse-code modulation for digital encoding of speech signals.

1938 – E. L. Chaffee determined the optimum load for Class B amplifiers. IRE published standards on transmitters, receivers and antennas. Claude Elwood Shannon recognized the parallels between Boolean algebra and the functioning of electrical switching systems. W. R. Hewlett developed the Wien-bridge (RC) oscillator. P. H Smith at RCA developed the well known Smith Chart. N. E. Lindenblad of RCA developed a coaxial horn antenna. John Turton Randall and Albert Boot developed the cavity magnetron that becomes the central components to radar systems.

1941 – W. C. Godwin developed the direct-coupled push-pull amplifier with inverse feedback. Siemens & Halske made the Ge diode – R. S. Ohl made the Si junction diode. Sidney Warner realized a two-way police FM radio.

1943 – H. J. Finden developed the frequency synthesizer. Austrian engineer Rudolf Kompfner developed the traveling wave tube. C.

K. Chang developed frequency modulation of RC oscillators. C. F. Edwards developed microwave mixers. H. T. Friis developed noise figures of radio receivers.

1944 – Harold Goldberg suggested pulse frequency position modulation. E. C Quackenbush of Amphenol developed the VHF coaxial connectors. Paul Neil of Bell Labs developed Type N connectors. Maurice Deloraine, P. R. Adams and D. H. Ranson applied for patents covering switching by pulse displacement a principle later defined as time-slot interchange – Thus, Time-Division Multiplexing (TDMA) was invented. Radio Research Lab developed radar countermeasures (jamming) in the 25 MHz to 6 GHz range.

1946 – S. L. Ackerman and G. Rappaport developed a radio control systems for guided missiles. E. M. Williams developed the radio frequency spectrum analyzer.

1947 – G. E. Mueller and W. A. Tyrrel developed the dielectric rod antenna. John D. Kraus invented the helical antenna. W. Tyrell proposed hybrid circuits for microwaves, H. E. Kallaman constructed the VSWR indictor meter.

1948 – W. H. Branttain, J. Bardeen and W. Shockley of Bell Labs built the junction transistor. E. L. Ginzton and others developed distributed wideband amplifier using pentodes in parallel. Shannon laid out the theoretical foundations of digital communications in a paper entitled "A Mathematical Theory of Communication." Paine described the BALUN.

1949 – E. J. Barlow published the principle of operation of Doppler Radar.

1950- J. M. Janssen developed the sampling oscilloscope.

1951- Charles Hard Townes published the principle of the MASER (Microwave Amplification by Stimulated Emission of Radiation). The Laboratoire Central des Telecommunications in Paris developed the first model of a time-division multiplex system connecting subscriber line by electronic gates handling amplitude modulated pulses.

1952 – C. L. Hogan demonstrated a microwave circulator.

1955 – R. H. DuHamel and D. E. IsBelll develop the log periodic antenna. John R. Pierce proposed using satellites for communications. Sony marketed the first transistor radio.

1957 – Soviet Union launched Sputnik I that transmitted telemetry signals for about 5 months. German physicist Herbert Kroemer

originated the concept of the heterostructure bipolar transistor (HBT).

1958 – Robert Noyce (Intel) and Jack Kilby (TI) produced the first Si integrated circuit (IC).

1962 – G. Robert-Pierre Marie patented the wide band slot antenna. S. R. Hofstein and F. P. Heiman developed MOS IC.

1963 – W. S. Mortley and J. H. Rowen developed surface acoustic wave (SAW) devices. John B. Gunn of IBM demonstrated microwave oscillations in GaAs and InP diodes. The Institute of Electrical and Electronic Engineers (IEEE) was formed by merging the IRE and AIEE.

1964 – R. L. Johnson, B. C. De Loach and B. G. Cohen developed the IMPATT diode oscillator. COMSAT and INTELSAT started launching a series of communications satellites that were the building blocks in the global network of international communications satellites.

1969 – The first digital radio-relay system went into operation in Japan using 2 GHz operating frequency. ARPANET was launched (precursor to Internet).

1971 – Statek began manufacturing and marketing quartz oscillators that were made using their patented photolithographic process.

1978 – AT&T Bell Labs started testing a mobile telephone system based on cells.

1980 – CW performance of GaAs MESFET reached 10 W at 10 GHz. ATLAS I EM pulse simulator was built for testing large aircraft – it was the largest wooden structure in the world (400 x 105 x 75 m).

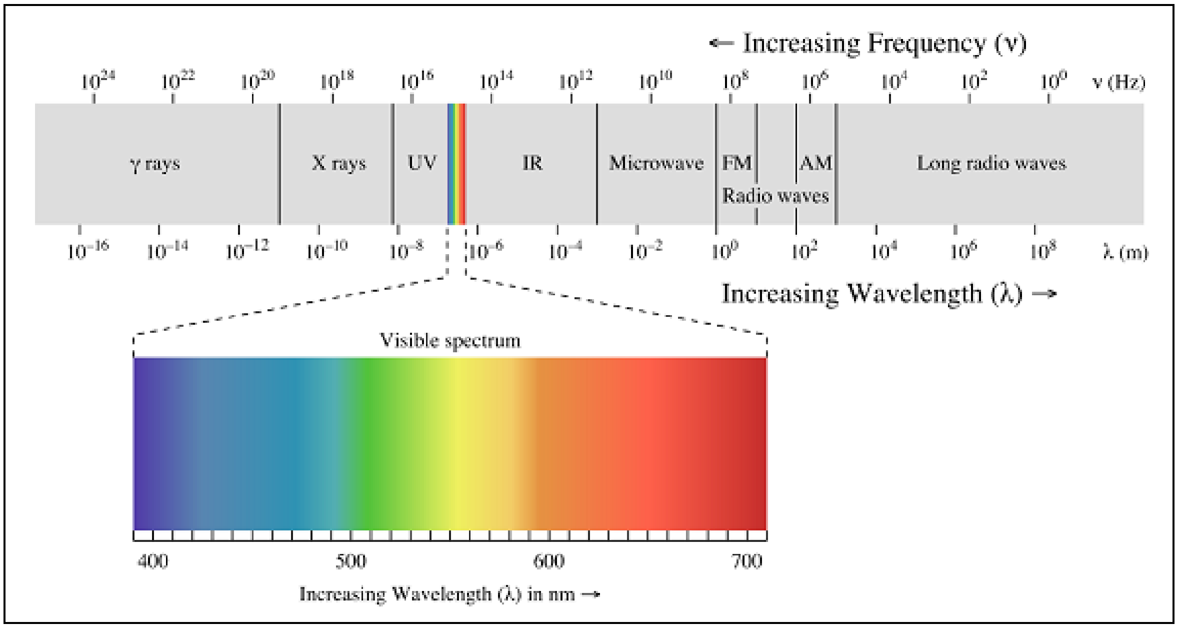
1989 – F. Laleari invented the broadband notch antenna

1990 – WWW was developed

Electromagnetic Spectrum

Wireless communication is based on the principle of broadcast and reception of electromagnetic waves. These waves can be characterized by their frequency (f) and their wavelength (λ) lambda.

A pictorial representation of the electromagnetic spectrum is given in the following figure.



Low Frequency bands

Low Frequency bands comprise of the radio, microwave, infrared and visible portions of the spectrum. They can be used for information transmission by modulating the amplitude, frequency or phase of the waves.

High Frequency bands

High Frequency bands comprise of X-rays and Gamma rays. Theoretically, these waves are better for information propagation. However, these waves are not used practically because of difficulty in modulation and the waves are harmful to living beings. In addition, high frequency waves do not propagate well through buildings.

Frequency Bands and their Uses

The following table depicts the frequency bands and its uses −

Band Name	Frequency	Wavelength	Applications
Extremely Low Frequency (ELF)	30 Hz to 300 Hz	10,000 to 1,000 KM	Power line frequencies
Voice Frequency (VF)	300 Hz to 3 KHz	1,000 to 100 KM	Telephone Communications

Very Low Frequency (VLF)	3 KHz to 30 KHz	100 to 10 KM	Marine Communications
Low Frequency (LF)	30 KHz to 300 KHz	10 to 1 KM	Marine Communications
Medium Frequency (MF)	300 KHz to 3 MHz	1000 to 100 m	AM Broadcasting
High Frequency (HF)	3 MHz to 30 MHz	100 to 10 m	Long distance aircraft/ship Communications
Very High Frequency(VHF)	30 MHz to 300 MHz	10 to 1 m	FM Broadcasting
Ultra High Frequency (UHF)	300 MHz to 3 GHz	100 to 10 cm	Cellular Telephone
Super High Frequency (SHF)	3 GHz to 30 GHz	10 to 1 cm	Satellite Communications, Microwave links
Extremely High Frequency (EHF)	30 GHz to 300 GHz	10 to 1 mm	Wireless local loop
Infrared	300 GHz to 400 THz	1 mm to 770 nm	Consumer Electronics
Visible Light	400 THz to 900 THz	770 nm to 330 nm	Optical Communications

Spectrum Allocation

Since the electromagnetic spectrum is a common resource, which is open for access by anyone, several national and international agreements have been drawn regarding the usage of the different frequency bands within the spectrum. The individual national governments allocate spectrum for applications such as AM/FM radio broadcasting, television broadcasting, mobile telephony, military communication, and government usage.

Worldwide, an agency of the International Telecommunications Union Radio Communication **(ITU-R)** Bureau called World Administrative Radio Conference **(WARC)** tries to coordinate the spectrum allocation by the various national governments, so that communication devices that can work in multiple countries can be manufactured.

WIRELESS COMMUNICATION STANDARDS

TIA (Telecommunication Industry Association)

With accreditation from ANSI (American National Standards Institute), The Telecommunications Industry Association or TIA develops standards based on consensus. Twelve of TIA's engineering committees are dedicatedly working on developing standards for radio, satellite and mobile communication.

ETSI (European Telecommunications Standards Institute)

The ETSI or the European Telecommunications Standards Institute is another well known organization that greatly contributes to the evolution of cellular technologies. It is a non-profit organization in Europe and its standards are widely accepted across the world. GSm has been standardized under ETSI.

ITU (International Telecommunications Union)

The International Telecommunication Union or the ITU, which was originally called the International Telegraph Union, is a committee under the United Nations Organization and is committed to resolving issues related to Information and communication technologies. The global radio spectrum usage is regulated by the ITU. It is also responsible for promoting co-operation and harmonious interoperation between countries, ensuring there is no encroachment on spectrums, satellite orbits etc. ITU assists various organizations all over the world in developing their technical standards.

Apart from the internationally important standard bodies mentioned above, there are a few regional standards that are of importance. A few of them are listed below:

ARIB/TTC (Association of Radio Industries and Business/ Telecommunication Technology Committee) – Japan

The Association of Radio Industries and Businesses, abbreviated to ARIB is a centre for devising means for effective usage of the radio spectrum. ARIB is a standardization agency of Japan; however it has been active in contributing to Global standards and 3GPP.

TTA (Telecommunications Technology Association) – South Korea

Telecommunications Technology Association or the TTA aims at the standardization if information and communication technologies. It is a non-profit and non-government organization. Based in South Korea, this organization provides testing and certification services for Information and Communication Technology products.

CWTS (Chinese Wireless Telecommunication Standard) – China

The China Wireless Telecom standards commonly called the CWTS, is responsible for defining, producing and maintaining the telecommunication standards within China. It is a non-profit organization with the aim of creating effective telecom standards to meet the increasing growth and demand of wireless technologies in China.

TEC (Telecommunications Engineering Center) – India

The Telecommunication Engineering Centre or TEC is a committee under the Ministry of Communication and Informaion Technology. Govt. of India. The purpose of this committee is to develop standards and specifications for telecom products services and networks within India.

EVOLUTION FROM 1G TO 5G

1G Technology

1G refers to the first generation of wireless mobile communication where analog signals were used to transmit data. It was introduced in the US in early 1980s and designed exclusively for voice communication. Some characteristics of 1G communication are −

- **Speeds up to 2.4 kbps**
- **Poor voice quality**
- **Large phones with limited battery life**
- **No data security**

2G Technology

2G refers to the second generation of mobile telephony which used digital signals for the first time. It was launched in Finland in 1991 and used GSM technology. Some prominent characteristics of 2G communication are −

- **Data speeds up to 64 kbps**

- **Text and multimedia messaging possible**
- **Better quality than 1G**

When GPRS technology was introduced, it enabled web browsing, e-mail services and fast upload/download speeds. 2G with GPRS is also referred as 2.5G, a step short of next mobile generation.

3G Technology

Third generation (3G) of mobile telephony began with the start of the new millennium and offered major advancement over previous generations. Some of the characteristics of this generation are −

- **Data speeds of 144 kbps to 2 Mbps**
- **High speed web browsing**
- **Running web based applications like video conferencing, multimedia e-mails, etc.**
- **Fast and easy transfer of audio and video files**
- **3D gaming**

Every coin has two sides. Here are some downsides of 3G technology −

- **Expensive mobile phones**
- **High infrastructure costs like licensing fees and mobile towers**
- **Trained personnel required for infrastructure set up**

The intermediate generation, 3.5G grouped together dissimilar mobile telephony and data technologies and paved way for the next generation of mobile communication.

4G Technology

Keeping up the trend of a new mobile generation every decade, fourth generation (4G) of mobile communication was introduced in 2011. Its major characteristics are −

- **Speeds of 100 Mbps to 1 Gbps**
- **Mobile web access**
- **High definition mobile TV**
- **Cloud computing**
- **IP telephony**

1G and 2G

There never was something called as 1G at first. It basically was a network with only voice call capabilities and only got the name 1G after 2G was put to use. During the 2G era, that lasted for quite a while from 1980's to 2003, there were quite a few advancements made within the spectrum itself such as GSM, GPRS and EDGE.

- **GSM: Short for *Global Systems for Mobile Communication e*nabled data transfer on top of voice communication at speeds that are seen as a joke today (30-35 kbps). It played a critical role in the evolution as mobile technology as right about the time it was being used mobile phone connectivity and popularity exploded.**

- **GPRS: *General Packet Radio Service* operated on the similar 2G technology as GSM with a few refinements with gave it higher data speeds (110 kbps)**

- **EDGE: *Enhanced Data rates for GSM Evolution* introduced in 2003 was somewhat known to be 2.9G or 3G due to its significant advancements over GPRS and GSM. It offered high speeds of 135 kbps and continues to be used on many mobile networks even today as is satisfies the basic needs of both carriers and users in various parts of the world.**

3G

This was a big revolution in terms of technological advancement for network and data transmission. 3G had and has speed capabilities of up to 2 mbps. It enabled smartphones to provide faster communication, send/receive large emails and texts, provide fast web browsing, video streaming and more security amongst others. It was widely based on CDMA2000 (Code-division multiple access) and EDGE technologies. Now you might wonder why EDGE? Well, because EDGE was so advanced it was able to provide enough capabilities to be considered as 3G. CDMA2000, on the other hand, operated on similar key concepts but did it better. It enabled multiple channels to communicate at one same thus improvising on the over speed and connectivity.

4G

The 4G standard sets several requirements for mobile networks

including mandating the use of Internet Protocol (IP) for data traffic and minimum data rates of 100 Mbps. [LifeWire] which was a huge jump from the 2 mbps for 3G. It is often referred to as MAGIC

- **M – Mobile multimedia**

- **A – Anytime anywhere**

- **G – Global mobility support**

- **I – Integrated wireless solution**

- **C – Customized personal service**

It is not much to do with the technology it uses but rather than the requirements set forth by International Telecommunication Union's Radio communication Sector (ITU-R). These standards are known as International Mobile Telecommunications-Advanced (IMT-

Advanced). The list of standards is quite complicated and thus were a barrier in fast adoption of the 4G spectrum.

Soon after 4G, 4G LTE was introduced. LTE stands for Long Term Evolution and it isn't as much a technology as it is the path followed to achieve 4G speeds. It was a complete redesign and simplification of 3G network architecture, resulting in a significant reduction in transfer latency and thus, increasing efficiency and speeds on the network.

5G

It is still quite in its early stages and the the technology likely to appear in the market only by 2020 at the earliest. Goals for future 5G include significantly faster speeds (a minimum of 1 Gbps and perhaps up to 10 Gbps) plus lower power requirements to better support huge numbers of new Internet of Things (IoT) devices. It will have capabilities to provide faster dialing speeds, multiple device connectivity, higher data speeds just to name a few.

1.1 BASIC CELLULAR SYSTEMS

There are two basic cellular systems; one is the circuit-switched system and the otheris the packet- switched system.Circuit-Switched Systems In a circuit-switched system, each traffic channel is dedicated to a user until its cell is terminated. We can further distinguish two circuit-switched systems: one for an analog system and one for a digitalsystem.

1.1.1 ANALOG SYSTEM

A basic analog cellular system1–3 consists of three subsystems: a mobile unit, a cell site, and a mobile telephone switching office (MTSO), as Fig. 1.1 shows, with connections to link the three subsystems.

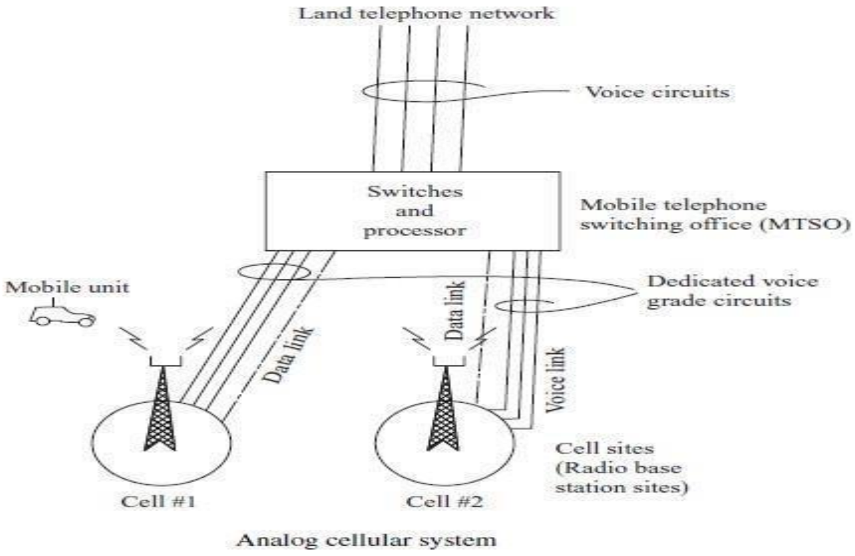


Figure 1.1 Analog Circuit switched system

Basic Components:

1. **Mobile units. A mobile telephone unit contains a control unit, a transceiver, and an antenna system.**

2. **Cell site. The cell site provides interface between the MTSO and the mobile units. It has acontrol unit, radio cabinets, antennas, a power plant, and data terminals.**

3. **MTSO. The switching office, the central coordinating element for all cell sites, contains the cellular processor and cellular switch. It interfaces with telephone company zone offices, controls call processing, provides operation and maintenance, and handles billing activities.**

4. **Connections. The radio and high-speed data links connect the three subsystems. Each mobile unit can only use one channel at a time for its communication link. But the channel isnot fixed; it can be any one in the entire band assigned by the serving area, with each site having multichannel capabilities that can connect simultaneously to many mobile units.**

The MTSO is the heart of the analog cellular mobile system. Its processor provides central coordination and cellular administration. The cellular switch, which can be either analog or digital, switches calls to connect mobile subscribers to other mobile subscribers and to the nationwide telephone network. It uses voice trunks similar to telephone company interoffice voice trunks. It also contains data links providing supervision links between the processor and the switch and between the cell sites and the processor. The radio link carries the voice and signaling between the mobile unit and the cell site. The high-speed data links cannot be transmitted over the standard telephone trunks and therefore must use either microwave links or T-carriers (wire lines). Microwave radio links or T-carriers carry both voice and data between cell site and the MTSO.

1.1.2 DIGITAL SYSTEMS

A Basic Digital System consists of four elements: 1. Mobile Station 2. Base Transceiver Station (BTS) 3. Base Station Controller (BSC) 4. Switching Subsystems, as shown in Fig. 1.2.

1. **MS: It consists of two parts, mobile equipment (ME) and subscriber identify module (SIM). SIM contains all subscriber-specific data stored on the MS side.**
2. **BTS: Besides having the same function as the analog BTS, it has the Transcoder/Rate Adapter Unit (TRAU), which carries out coding and decoding as well as rate adaptation in case data rate varies.**
3. **BSC: A new element in digital systems that performs the Radio Resource (RR) management for the cells under its control. BSC also handles handovers, power management time and frequency synchronization, and frequency reallocation among BTSs.**
4. **Switching subsystems: Main components of Switching Subsystem is as follows:**

a. **MSC: The main function of MSC is to coordinate the setup of calls between MSand PSTN users.**

b. **VLR (Visitor Location Register): A database of all mobiles roaming in the MSC'sarea of control.**

c. **HLR (Home Location Register):A centralized database of all subscribersregistered in a Public Land Mobile Network (PLMN).**

d. **AUC (Authentication Center): Provides HLR with authenticationparameters and ciphering keys that are used for security purposes.**

e. **EIR (Equipment Identity Register): A database for storing all registeredmobile equipment numbers.**

f. **EC (Echo Canceller): Used on the PSTN side of the MSC for all voice circuits.**

g. XC (Transcoder): Usually installs in each BTS. But for the cost reason, it can beinstalled in BSC or MSC.

h. OMC (Operational and Maintenance Center): This function resided in analogMSC but became a separated entity in digital systems

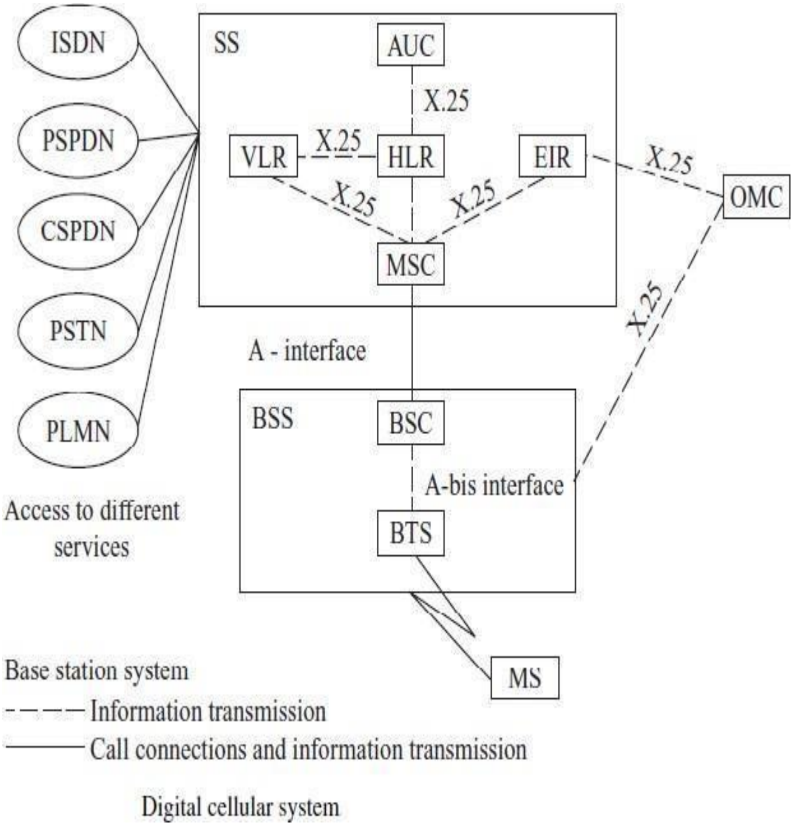


Figure 1.2 Digital Cellular System

1.1.3 PACKET SWITCHED SYSTEM

A cellular packet-switched system has six elements as follows:

1. **MS (Mobile Station)**
2. **Node B**
3. **RNC (Radio Network Controller)**
4. **SGSN (Service GPRS Support Node)**
5. **GGSN (Gateway GPRS Support Node)**
6. **CGF (Changing Gateway Function)**

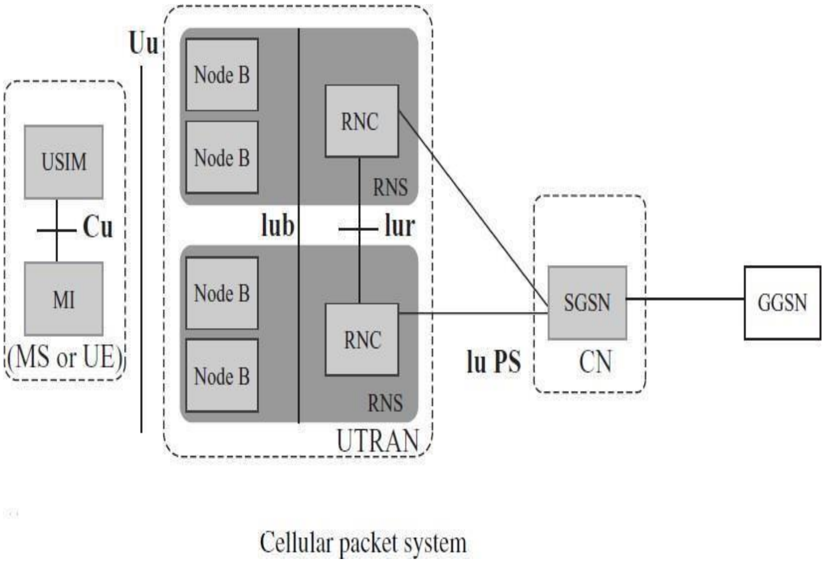


Figure 1.3 Packet Switched System

- **MS: Provides the voice and packet data services. It is also called UE (User Equipment).**

- **Node B: The name for base station in GSM.**

- **RNC (Radio Network Controller): Controls the radio resources of the Node Bs that are connected to it. Its function is similar to BSC. A device PCU (Packet Control Unit)converts the data stream into packet format.**

- **SGSN (Service GPRS Support Node): Analogous to MSC/VLR in the circuit-switched system. This includes mobility management, security, and access control functions. Itinterfaces to HLR.**

- **GGSN (Gateway GPRS Support Node): The point of interface with external packet data networks such as the Internet.**

- **CGF (Changing Gateway Function): Mainly for billing.**

- ***RNS (Radio Network Subsystem):* It consists of RNC and Node B. UTRAN consists oftwo or more RNS.**

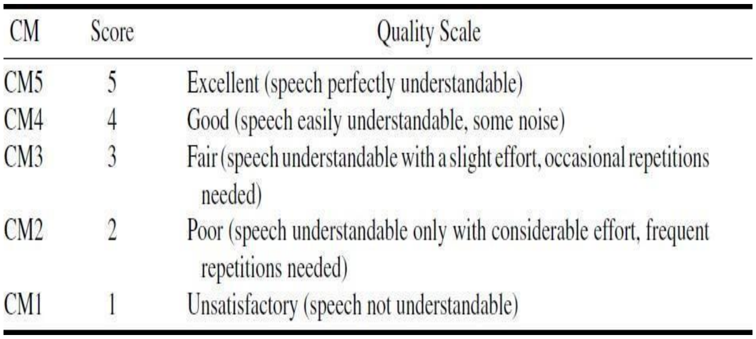
1.2 PERFORMANCE CRITERIA

- **Main components of Performance criteria are as follows:**
- **Voice Quality**
- **Data Quality**
- **Picture/Vision Quality**
- **Service Quality**
- **Special Features**

1. Voice Quality

Voice quality is very hard to judge without subjective tests for users' opinions. In this technical area, engineers cannot decide how to build a system without knowing the voice quality that will satisfy the users. In military communications, the situation differs: armed forces personnel must use the assigned equipment.

- **CM: For any given commercial communications system, the voice quality will be based on the following criterion: a set value *x* at which *y* percent of customers rate the system voice quality (from transmitter to receiver) as good or excellent; the toptwo circuit merits (CM) of the five listed below.**



CM	Score	Quality Scale
CM5	5	Excellent (speech perfectly understandable)
CM4	4	Good (speech easily understandable, some noise)
CM3	3	Fair (speech understandable with a slight effort, occasional repetitions needed)
CM2	2	Poor (speech understandable only with considerable effort, frequent repetitions needed)
CM1	1	Unsatisfactory (speech not understandable)

- **MOS: As the percentage of customers choosing CM4 and CM5 increases, thecost of building the system rises.**

- **The average of the CM scores obtained from all the listeners is called mean opinion score (MOS). Usually, the toll-quality voice is around MOS ≥4.**

- **DRT (Diagnostic Rhyme Test): An ANSI standardized method used for evaluation of intelligibility. It is a subjective test method. Listeners are required to choose which word of a rhyming pair they perceived. The words differ only in their leading consonant. The word pairs have been chosen such that six binary attributes of speech intelligibility are measured in their present and absent states. This attribute profile provides a diagnostic capability to the test.**

2. Data Quality:

There are several ways to measure the data quality such as bit error rate, chip error rate, symbol error rate, and frame error rate. The chip error rate and symbol error rate are measuring the quality of data along the transmission path. The frame error rate and the bit error rate are measuring the quality of data at the throughput.

3. Picture/Vision Quality

There are color acuity, depth perception, flicker perception, motion perception, noise perception, and visual acuity. The percentage of pixel (picture element) loss rate can be characterized in vertical resolution loss and horizontal resolution loss of a pixel.

4. Service Quality

Three items are required for service quality.

Coverage: The system should serve an area as large as possible. With radio coverage, however, because of irregular terrain configurations, it is usually not practical to cover 100 percent of the area for two reasons:

a. The transmitted power would have to be very high to illuminate weak spots with sufficient reception, a significant added cost factor.

b. The higher the transmitted power, the harder it becomes to control interference. Therefore, systems usually try to cover 90 percent of an area in flat terrain and 75 percent of an area in hilly terrain. The combined voice quality and coverage criteria in AMPS

Required grade of service: For a normal start-up system, the grade of service is specified for a blocking probability of .02 for initiating calls at the busy hour. This is an average value. However, the blocking probability at each cell site will be different. At the busy hour, near freeways, automobile traffic is usually heavy, so the blocking probability at certain cell sites may be higher than 2 percent, especially when car accidents occur. To decrease the blocking probability requires a good system plan anda sufficient number of radio channel.

Number of dropped calls*:* During Q calls in an hour, if a call is dropped and Q−1 calls are completed, then the call drop rate is 1/Q. This drop rate must be kept low. A high drop rate could be caused by either coverage problems or handoff problems related to inadequate channel availability or weak reception.

5. Special Features

A system would like to provide as many special features as

- **Call Forwarding**
- **call waiting**
- **voice stored (VSR) box**
- **automatic roaming**
- **short message service (SMS)**
- **multimedia service (MMS)**
- **push-to-talk (PTT)**
- **Navigation services.**

1.3 UNIQUENESS OF MOBILE RADIO ENVIRONMENTThe Propagation Attenuation

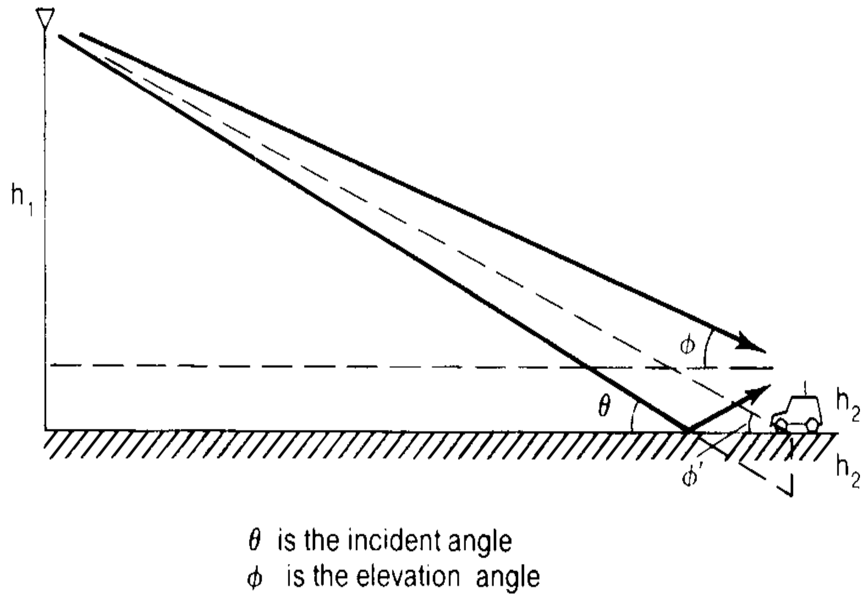


Figure 1.4 Mobile Radio Transmission Model

In general, the propagation path loss increases not only with frequency but also with distance. If the antenna height at the cell site is 30 to 100 m and at the mobile unit about 3 m above the ground, and the distance between the cell site and the mobile unit is usually 2 km or more, then the incident angles of both the direct wave and the reflected wave are very small, as Fig. 2.4 shows. The incident angle of the direct wave is 91, and the incident angle of the reflected wave is 02. 01 is also called the elevation angle. The propagation path loss would be 40 dB/dec,4 where "dec" is an abbreviation of decade, i.e., a period of 10. This means that a 40-dB loss at a signal receiver will be observed by the mobile unit as it moves from 1 to 10 km. Therefore C is inversely proportional to R ^{4}

$$C \alpha R^{-4} = \alpha R^{-4}$$

where C = received carrier power R = distance measured from the transmitter to the receiver α = constant

1.3.1 Model of Transmission Medium

A mobile radio signal r(t), illustrated in Fig. 2.6, can be artificially characterized5 by two components m(t) and r0(t) based on natural physical phenomena. r (t) = m(t)ro(t) The component m(t) is called local mean, long-term fading, or lognormal fading and its variation is due to the terrain contour between the base station and the mobile unit. The factor r0 is called multipath fading, short-term fading, or Rayleigh fading and its variation is due to the waves reflected from the surrounding buildings and other structures.

1.3.2 Mobile Fading Characteristics

Rayleigh fading is also called multipath fading in the mobile radio environment. Whenthese multipath waves bounce back and forth due to the buildings and houses, they form many standing-wave pairs in space. Those standing-wave pairs are summed together and become an irregular wave-fading structure. When a mobile unit is standing still, its receiver only receives a signal strength at that spot, so a constant signal is observed. When the mobile unitis moving, the fading structure of the wave in the space

is received. It is a multipath fading. The recorded fading becomes fast as the vehicle moves faster

1.4 OPERATIONS OF CELLULAR SYSTEM

- **Mobile unit initialization**
  - — **Scan and select strongest set up control channel**
  - — **Automatically selected BS antenna of cell**
    - • **Usually but not always nearest (propagation anomalies)**
  - — **Handshake to identify user and register location**
  - — **Scan repeated to allow for movement**
    - • **Change of cell**
  - — **Mobile unit monitors for pages (see below)**
- **Mobile originated call**
  - — **Check set up channel is free**
    - • **Monitor forward channel (from BS) and wait for idle**

— **Send number on pre-selected channel**

- **Paging**

— **MTSO attempts to connect to mobile unit**

— **Paging message sent to BSs depending on called mobile number**

— **Paging signal transmitted on set up channel**

- **Call blocking**

— **During mobile-initiated call stage, if all traffic channels busy, mobile tries again**

— **After number of fails, busy tone returned**

- **Call termination**

— **User hangs up**

— **MTSO informed**

— **Traffic channels at two BSs released**

- **Call drop**

— **BS cannot maintain required signal strength**

— **Traffic channel dropped and MTSO informed**

— **Calls to/from fixed MTSO connects to PSTN**

— **MTSO can connect mobile user and fixed subscriber via PSTN**

— **MTSO can connect to remote MTSO via PSTN or via dedicated lines**

— **Can connect mobile user in its area and remote mobile user**

1.5 CONCEPT OF FREQUENCY RESUSE SCHEMES

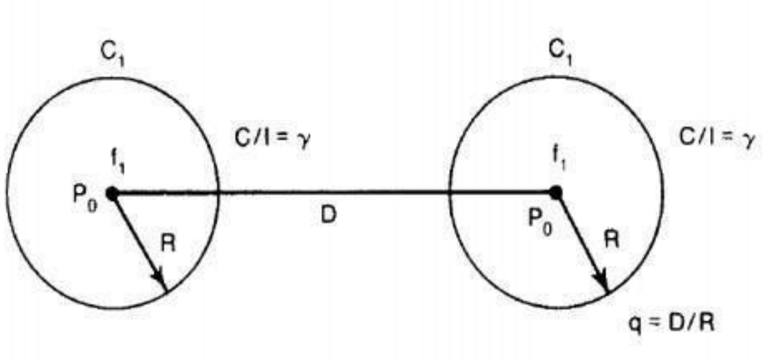


Figure 1.5 The ratio D/R

— **_N_ cells all using same number of frequencies**

— **_K_ total number of frequencies used in systems**

— **Each cell has _K/N_ frequencies**

— Advanced Mobile Phone Service (AMPS) *K*=395, *N*=7 giving 57 frequenciesper cell on average

- D = minimum distance between centers of cells that use the same band offrequencies (called co-channels)
- R = radius of a cell
- d = distance between centers of adjacent cells (d = R)
- N = number of cells in repetitious pattern

— Reuse factor

— Each cell in pattern uses unique band of frequencies

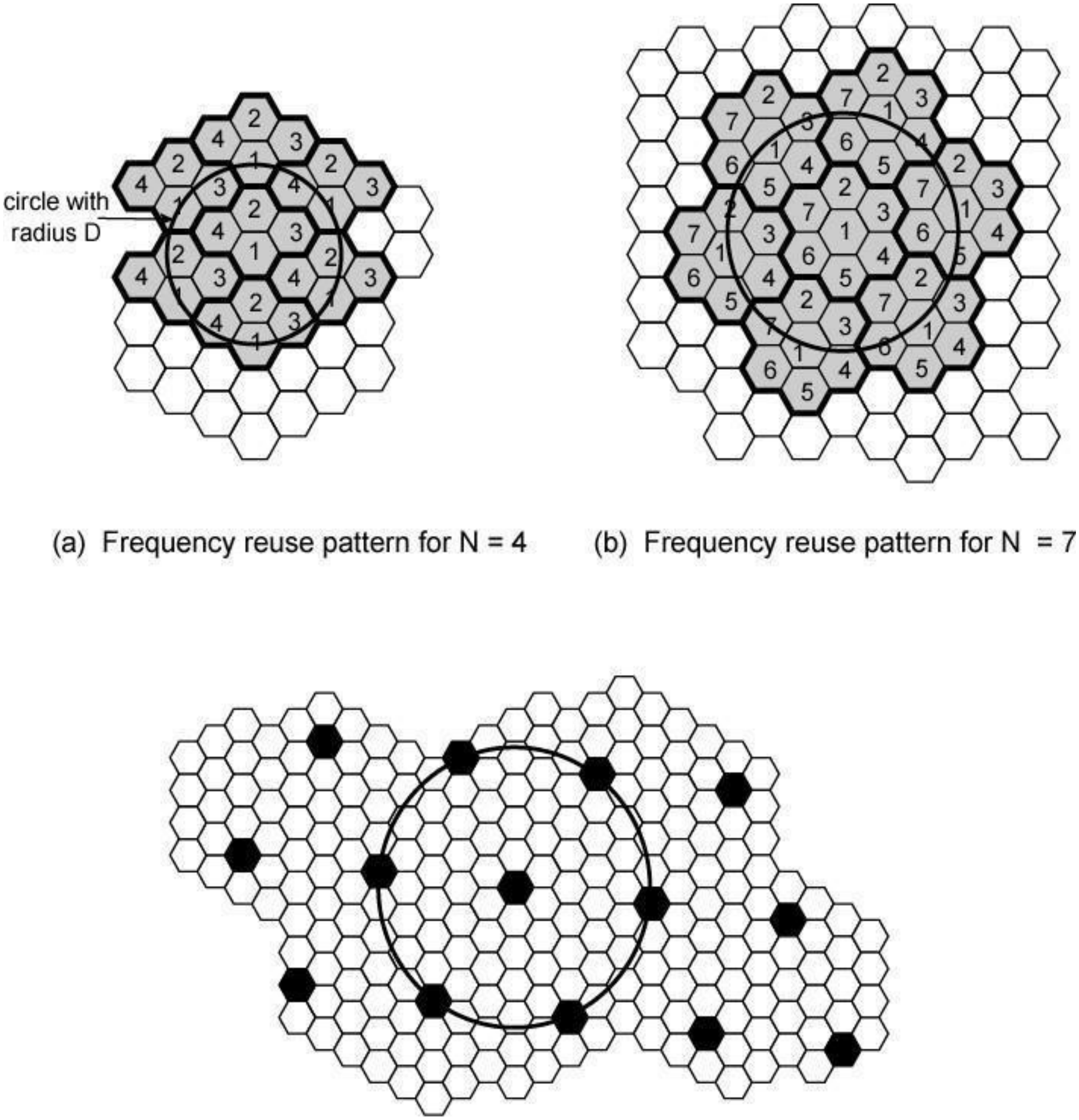
- Hexagonal cell pattern, following values of N possible

— N = I^2 + J^2 + (I x J), I, J = 0, 1, 2, 3, …

- Possible values of N are 1, 3, 4, 7, 9, 12, 13, 16, 19, 21, …

A radio channel consists of a pair of frequencies, one for each direction of transmission that is used for full-duplex operation. A particular radio channel, say F1, used in one geographic zone as named it a cell, say C1, with a coverage radius R can be used in another cell with the same coverage radius at a distance D away. Frequency reuse is the core concept of the cellular mobile radio system. In this frequency reuse system, users in different geographic locations (different cells) may simultaneously use the same frequency channel. The frequency reuse system can drastically increase the spectrum efficiency, but if the system is not properly designed, serious interference may occur. Interference due to the common use of the same channel is called cochannel interferenceand is our major concern in the concept of frequency reuse.

Same frequency assigned in two different geographic areas, such as AM or FM radio stations using the same frequency in different cities. 2. Same frequency repeatedly used in a same general area in one system2—the scheme is used in cellular systems. There aremany co channel cells in the system. The total frequency spectrum allocation is divided into K frequency reuse patterns as shown in figure 1.5, for K = 4, 7, 12, and 19.



(a) Frequency reuse pattern for N = 4

(b) Frequency reuse pattern for N = 7

(c) Black cells indicate a frequency reuse for N = 19

Figure 1.6 N-cell reuse pattern

1.6 CO-CHANNEL INTERFERENCE REDUCTION FACTOR

Reusing an identical frequency channel in different cells is limited by cochannel interference between cells, and the co-channel interference can become a major problem. Here we would like to find the minimum frequency reuse distance in order to reduce this cochannel interference. Assume that the size of all cells is roughly the same. The cell size is determined by the coverage area of the signal strength in each cell. As long as the cell size is fixed, cochannel interference is independent of the transmitted power of each cell. It means that the received threshold level at the mobile unit is adjusted to the size of the cell. Actually, cochannel interference is a function of a parameter q defined as

$q = D / R$

The parameter q is the co-channel interference reduction factor. When the ratio q increases, co- channel interference decreases. Furthermore, the separation D is a function of KI and C/I,

$D = f(KI, C/I)$

where KI is the number of co-channel interfering cells in the first tier and C/I is the received carrier-to-interference ratio at the desired mobile receiver

In a fully equipped hexagonal-shaped cellular system, there are always six cochannel interfering cells in the first tier, as shown in Fig. 1.6; that is, KI = 6. The maximum number of KI in the first tier can be shown as six (i.e., $2\pi D/D \approx 6$). Cochannel interference can be experienced both at the cell site and at mobile units in the center cell. If the interference is much greater, then the carrier-to-interference ratio C/I at the mobile units caused by the six interfering sites is (on the average) the same as the C/I received at the center cell site caused by interfering mobile units in the six cells. According to both the reciprocity theorem and the statistical summation of radio propagation, the two C/I values can be very close. Assume that the local noise is much less than the interference level and can be neglected. C/I then can be expressed, as

$$\frac{C}{I} = \frac{R^{-\gamma}}{6 \cdot D^{-\gamma}} = \frac{1}{6 \cdot q^{-\gamma}} = \frac{q^{\gamma}}{6}$$

where γ is a propagation path-loss slope5 determined by the actual terrain environment. In a mobile radio medium, γ usually is assumed to be 4. K_I is the number of cochannel interfering cells and is equal to 6 in a fully developed system, as shown in Fig. 1.6. The six cochannel interfering cells in the second tier cause weaker interference than those in the first tier.

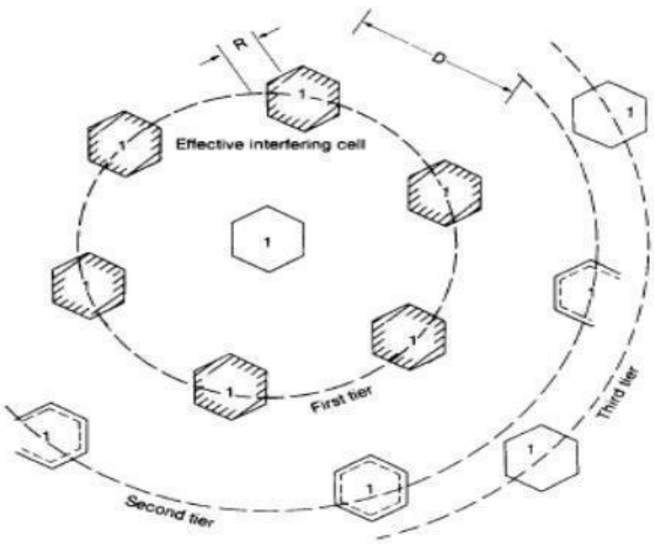


Figure 1.7 Six effective interfering cell of cell 1

1.6.1 DESIRED C/I FROM A NORMAL CASE IN A OMNI DIRECTIONAL ANTENNA SYSTEM

There are two cases to be considered: (1) the signal and cochannel interference received by the mobile unit and (2) the signal and cochannel interference received by the cell site.

Both cases are shown in Fig. 1.7. Nm, and Nb are the local noises at the mobile unit and the cell site, respectively. Usually, Nm and Nb are small and can be neglected as compared with the interference level. As long as the received carrier-to-interference ratios at both the mobile unit and the cell site are the same, the system is called a balanced system. In a balanced system, we can choose either one of the two cases to analyze the system

requirement; the results from one case are the same for the others.

Assume that all Dk are the same for simplicity, as shown in Fig. 1.7; then D = Dk , and q = qk , and

$$\frac{C}{I} = \frac{R^{-\gamma}}{6D^{-\gamma}} = \frac{q^{\gamma}}{6}$$

Thus $q^{\gamma} = 6\frac{C}{I}$ **and** $q = \left(6\frac{C}{I}\right)^{1/\gamma}$

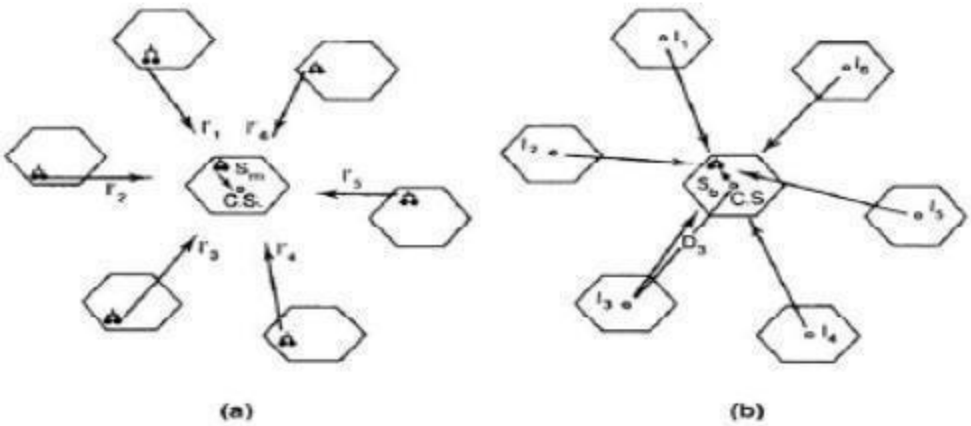


Figure 1.8 Co channel interference from six interferers, (a) Receiving at the cell site; (b) receiving at the mobile unit.

The value of C/I is based on the required system performance and the specified value of γ is based on the terrain environment. With given values of C/I and γ , the cochannel interference reduction factor q can be determined. Normal cellular practice is to specify C/I to be 18 dB or higher based on subjective tests. Because a C/I of 18 dB is measured by the acceptance of voice quality from present cellular mobile receivers, this acceptance implies that both mobile radio multipath fading and cochannel interference become ineffective at that level. The path-loss slope γ is equal to about 4 in a mobile radio environment.

q = D/R = (6 × 63.1)$^{1/4}$ = 4.41

The 90th percentile of the total covered area would be achieved by increasing the transmitted power at each cell; increasing the same amount of transmitted power in each

cell does not affect the result. This is because q is not a function of transmitted

power. The factor q can be related to the finite set of cells K in a hexagonal-shaped cellular system by

$$q = \overset{\Delta}{=} \sqrt{3K}$$

Substituting q yields K = 7

This indicates that a seven-cell reuse pattern is needed for a C/I of 18 dB. The seven- cell reuse pattern is shown in Fig. 1.7. Based on q = D/R, the determination of D can be reached by choosing a radius R. The greater the value of q, the lower the cochannel interference. The value q may not be large enough to maintain a carrier-to-interference ratioof 18 dB. This is particularly true in the worst case.

1.7 CELL SPLITTING

The motivation behind implementing a cellular mobile system is to improve the utilization of spectrum efficiency.19 The frequency reuse scheme is one concept, and cell splitting is another concept. When traffic density starts to build up and the frequency channels Fi in each cell Ci cannot provide enough mobile calls, the original cell can be split into smaller cells. Usually the new radius is one-half the original radius. There are two waysof splitting.

New cell radius = old cell radius/2 New cell area = old cell area/4

Let each new cell carry the same maximum traffic load of the old cell; then, inNew

theory, traffic load/Unit area= 4 × traffic load/unit area

There are two kinds of cell-splitting techniques:
Permanent splitting. The installation of every new split cell has to be planned ahead of time; the number of channels, the transmitted power, the assigned frequencies, the choosing of the cell-site selection, and the traffic load consideration should all be considered. When ready, the actual service cut-over should be set at the lowest traffic point, usually at midnight on a
weekend. Hopefully, only a few calls will be dropped because of this cut-over, assuming that the downtime of the system is within 2 h.

Dynamic splitting. This scheme is based on using the allocated spectrum efficiency in real time. The algorithm for dynamically splitting cell sites is a tedious job, as we cannot afford to have one single cell unused during cell splitting at heavy traffic hours.

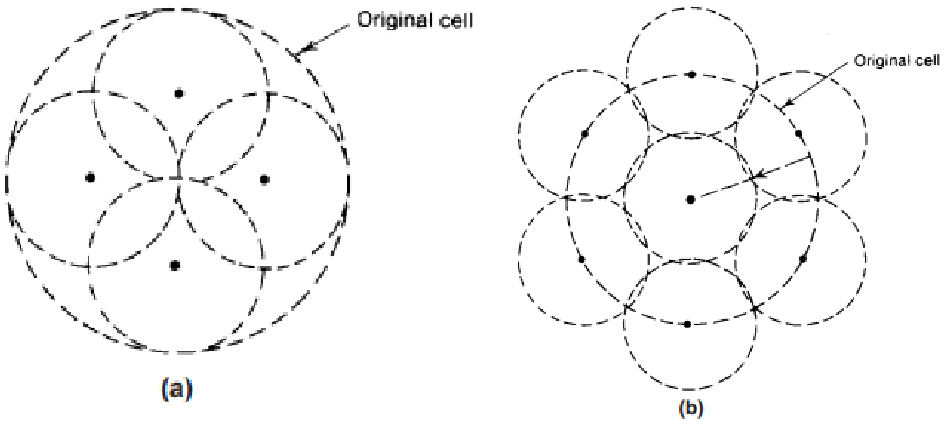
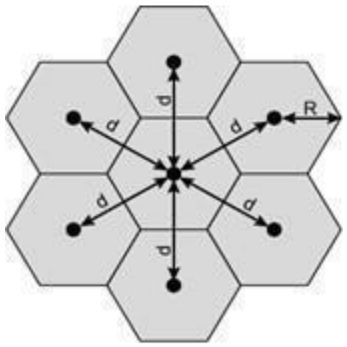


Figure 1.9 Cell Splitting

1.8 Shape of Cells



- **Hexagon**
  - **Provides equidistant antennas**
  - **Radius defined as radius of circum-circle**
- **Distance from center to vertex equals length of side**
  - **Distance between centers of cells radius *R* is**
  - **Not always precise hexagons**
- **Topographical limitations**
- **Local signal propagation conditions**

- **Location of antennas**

1.9 CONSIDERATION OF THE COMPONENTS OF CELLULAR SYSTEM

The elements of cellular mobile radio system design have been mentioned in the previous sections. Here we must also consider the components of cellular systems, such as mobile radios,antennas, cell-site, base-station controller, and MTSO. They would affect our system design if we do not choose the right one. The general view of the cellular system is shown in Fig. 1.5. Even though the EIA (Electronic Industries Association) and the FCC have specified standards for radio equipment at the cell sites and the mobile sites, we still need to be concerned about that equipment. The issues affecting choice of antennas, switching equipment, and data links are briefly described here

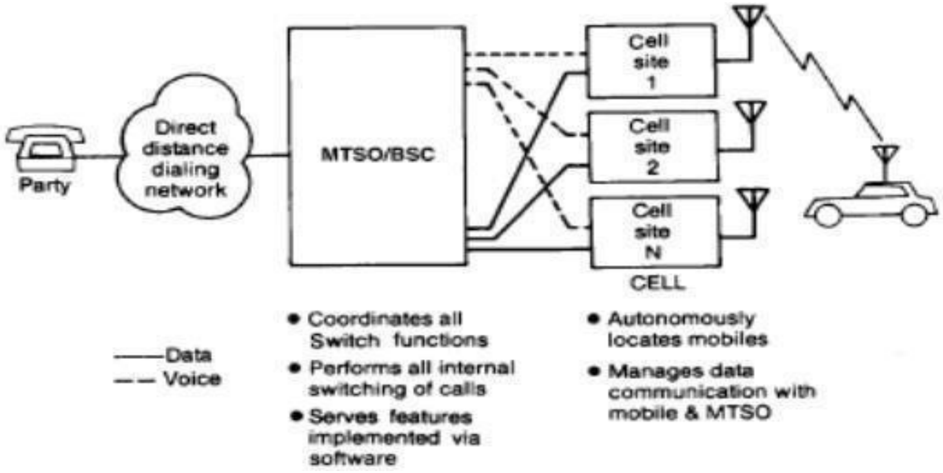

Party
Direct distance dialing network
MTSO/BSC
Cell site 1
Cell site 2
Cell site N
CELL
—— Data
— — Voice
• Coordinates all Switch functions
• Performs all internal switching of calls
• Serves features implemented via software
• Autonomously locates mobiles
• Manages data communication with mobile & MTSO

Figure 1.10 Components of Cellular System

Antennas: Antenna pattern, antenna gain, antenna tilting, and antenna height6 all affect the cellular system design. The antenna pattern can be omnidirectional, directional, or any shape in both the vertical and the horizon planes. Antenna gain compensates for the transmitted power. Different antenna patterns and antenna gains at the cell site and at the mobile units would affect the system performance and so must be considered in the system design. The antenna patterns seen in cellular systems are different from the patterns seen in free space. If a mobile unit travels around a cell site in areas with many buildings, the omnidirectional antenna will not duplicate the omnipattern.

In addtion, if the front-to-back ratio of a directional antenna is found to be 20 dB in free

space, it will be only 10 dB at the cell site. An explanation for these phenomena is given in Chapter 8.

Antenna tilting can reduce the interference to the neighboring cells and enhance the weak spotsin the cell. Also, the height of the cell-site antenna can affect the area and shape of the coveragein the system.

Switching Equipment: The capacity of switching equipment in cellular systems is not based on the number of switch ports but on the capacity of the processor associated with the switches. In a big cellular system, this processor should be large. Also, because cellular systems are unlike other systems, it is important to consider when the switching equipment would reach the maximum capacity. The service life of the switching equipment is not determined by the life cycle of the equipment but by how long it takes to reach its full capacity. If the switching equipment is designed in modules, or as distributed switches, more modules can be added to increase the capacity of the equipment. For decentralized systems, digital switches may be more suitable. Thefuture trend seems to be the utilization of system handoff. This means that switching equipmentcan link to other switching equipment so that a call can be carried from one system to another system without the call being dropped.

Data Links: The data links are shown in Fig.1.5. Although they are not directly affected by the cellular system, they are important in the system. Each data link can carry multiple channel data (10 kbps data transmitted per channel) from the cell site to the MTSO. This fast-speed data transmission cannot be passed through a regular telephone line. Therefore, data bank devices are needed. They can be multiplexed, many-data channels passing through a wideband T-carrierwire line or going through a microwave radio link where the frequency is much higher than 850 MHz. Leasing T1-carrier wire lines through telephone companies can be costly. Although the use of microwaves may be a long- term money saver, the availability of the microwave link has to be considered and is described

1.10 Frequency Management and Channel Assignment

Achieving optimum system capacity with a limited frequency spectrum is one of the main researchissues in cellular communications. In a cellular system, frequency management and channel assignment are essential in order to achieve the basic objectives of spectrum utilization as well as adaptability to traffic density.

Depending upon the system parameters, the allocated frequency spectrum is divided into a number of frequency channels. These available frequency channels are then divided into the subsetsthat can be assigned to each cell. Different strategies are followed for the assignment of these channel sets to cells. Fixed channel assignment (FCA) technique and dynamic channel allocation techniques are covered in detail. Frequency management includes operations such as designation of set-up and voice channels, numbering the channels, and grouping voice channels into subsets.

The main objective of channel-assignment is to stabilize the fluctuations in the probability of callblockage over the entire coverage area of a cellular network over a period of time. The channel assignment does the allocation of specific channels to cell sites and mobile units. It can be done in two ways:

o **Short-term assignment, where one channel assignment per call ishandled by mobile telephone switching office (MTSO).**

o **Long-term assignment, where a fixed channel set consisting of one or more subsets areassigned to cell site on a long-term basis.**

Each channel consists of two frequency channel bandwidths (mobile transmit/uplink or reverse channel and cell-site transmit/downlink or forward channel) to allow duplex operation. These two channel bandwidths must be separated in frequency in order to avoid interference. The frequencyseparation between the uplink and downlink channels is termed as channel spacing (or) duplex spacing. In the present 800 MHz band cellular system, the separation between the mobile transmitand the cell- site transmit is specified as 45 MHz.

The total channels available are 832 in number. However, most mobile units and systems are still operating on 666 channels. The arrangement of 666 frequency channels in block A and block B systems, each containing 333 channels. Out of these 333 available channels in each system, 312 channels are used for voice communication and 21 channels are used for controlling the system. These 21 channels are called as control channels or set-up channels. Therefore, a total of 42 channelsare used for controlling the system.

Channel Allocation

Channel allocation deals with the allocation of channels to cells in a cellular network. Once the channels are allocated, cells may then allow users within the cell to communicate via the available channels. Channels in a wireless communication system typically consist of time

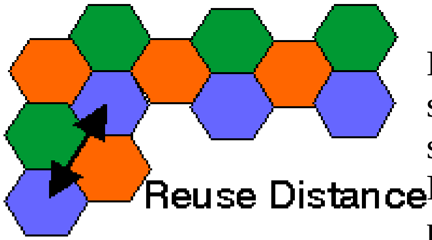
slots, frequency bands and/or CDMA pseudo noise sequences, but in an abstract sense, they can represent any generic transmission resource. There are three major categories for assigning these channels to cells (or base-stations). They are

- **Fixed Channel Allocation,**
- **Dynamic Channel Allocation and**
- **Hybrid Channel Allocation which is a combination of the first two methods.**

1.10.1 Fixed channel assignment

In FCA, each cell assigns its own frequency channel to the mobile subscribers within its cell. Channel assignment is primarily based on causing least co-channel and adjacent channel interference in the cellular system. The channel assignment for each voice call is determined by MTSO on a short- term basis. In a FCA, the set-up and voice channels are usually assigned to thecell site for relatively long periods. Channels in a channel set are usually 21 channels apart and must meet minimum frequency spacing requirements of a multi-channel transmitter combiner. Channels are usually numbered in order of increasing frequency. Regardless of the number of channels in a channel set,the highest channel set is frequency adjacent to the lowest channel set.

Fixed Channel Allocation



Fixed Channel Allocation (FCA) systems allocate specific channels to specific cells. This allocation is static and can not be changed. For efficient operation, FCA systems typically allocate channels in a manner that maximizes frequency reuse. Thus, in a FCA system, the distance between cells using the same channel is the minimum reuse distance for that system. The problem with FCA systems is quite simple and occurs whenever the offered traffic to a network of base stations is not uniform. Consider a case in which two adjacent cells are allocated *N* channels each. There clearly can be situations in which one cell has a need for *N*+*k* channels while the adjacent cell only requires *N*-*m* channels (for positive integers *k* and *m*). In such a case, *k* users in the first cell would be blocked from making calls while *m* channels in the second cell would go unused. Clearly in this situation of non-uniform spatial offered traffic, the available channels are not being used efficiently. FCA has been implemented on a widespread level to date.

The following are the advantages of FCA:

- **Fixed parameters (power, frequency) for transceivers.**
- **Good performance under uniform- and/or high-traffic loads as cells independently decidetheir channel allocation decisions.**
- **If each cell is allocated to a pre-determined set of voice channels then the call is *blocked* andall the channels are occupied.**

Borrowing strategy: A cell is allowed to borrow channels from neighbouring cell if all of its own channels are occupied. Mobile switching centre (MSC) supervises the borrowing procedure to ensure no disrupting calls or interference with any of the calls in progress in the donor cell.

1.10.2 Dynamic channel assignment

In dynamic channel assignment (DCA), the central common pool maintains all the available channels. Channels are assigned dynamically as new requests for radio resource (for a fresh originating call or handoff of existing call) arrive in the system. This also implies that when the use of assigned channel is completed, the channel currently in use is returned to the central pool.

In order to achieve optimum system capacity with limited frequency spectrum, many DCA schemes have been proposed to allocate the channels more efficiently. In a cellular system, a mobile subscriber moves from one cell to another and continuation of communication link is ensured with suitable handoff mechanism. This demands for additional and flexible radio resources utilization. However, because a limited frequency band is allocated for cellular communication, there is an upper limit to the maximum number of channels, thereby restricting the number of available channels that can be assigned to each cell. Another way is non-uniform FCA based on the amount of traffic expected to be served in different cells as per the statistical traffic data.

Dynamic Channel Allocation

Dynamic Channel Allocation (DCA) attempts to alleviate the problem mentioned for FCA systems when offered traffic is non-uniform. In DCA systems, no set relationship exists between channels and cells. Instead, channels are part of a pool of resources. Whenever a channel is needed by a cell, the channel is allocated under the constraint that frequency reuse requirements can not be violated. There are two problems that typically occur with DCA based systems.

- First, DCA methods typically have a degree of randomness associated with them and this leads to the fact that frequency reuse is often not maximized unlike the case for FCA systems in which cells using the same channel are separated by the minimum reuse distance.
- Secondly, DCA methods often involve complex algorithms for deciding which available channel is most efficient. These algorithms can be very computationally intensive and may require large computing resources in order to be real-time.

The following are the advantages of DCA:

- **No fixed channels are assigned to each cell.**
- **Out of the available channels, any channel can be assigned to any cellon need basis.**
- **The serving base station (BS) requests a channel from the MSC whenever a**
- **call request is made.**

Hybrid Channel Allocation Schemes

The third category of channel allocation methods includes all systems that are hybrids of fixed and dynamic channel allocation systems. Several methods have been presented that fall within this category and in addition, a great deal of comparison has been made with corresponding simulations and analyses [Cox, Elnoubi, Jiang, Katzela, Yue, Zhang]. We will present several of the more developed hybrid methods below.

Channel Borrowing is one of the most straightforward hybrid allocation schemes. Here, channels are assigned to cells just as in fixed allocation schemes. If a cell needs a channel in excess of the channels previously assigned to it, that cell may borrow a channel from one of its neighboring cells given that a channel is available and use of this channel won't violate frequency reuse requirements. Note that since every channel has a predetermined relationship with a specific cell, channel borrowing (without the extensions mentioned below) is often categorized as a subclass of fixed allocation schemes. The major problem with channel borrowing is that when a cell borrows a channel from a neighboring cell, other nearby cells are prohibited from using the borrowed channel because of co-channel interference. This can lead to increased call blocking over time. To reduce this call blocking penalty, algorithms are necessary to ensure that the channels are borrowed from the most available neighboring cells; i.e., the neighboring cells with the most unassigned channels.

Two extensions of the channel borrowing approach are **Borrowing with Channel Ordering** (BCO) and **Borrowing with Directional Channel Locking** (BDCL).

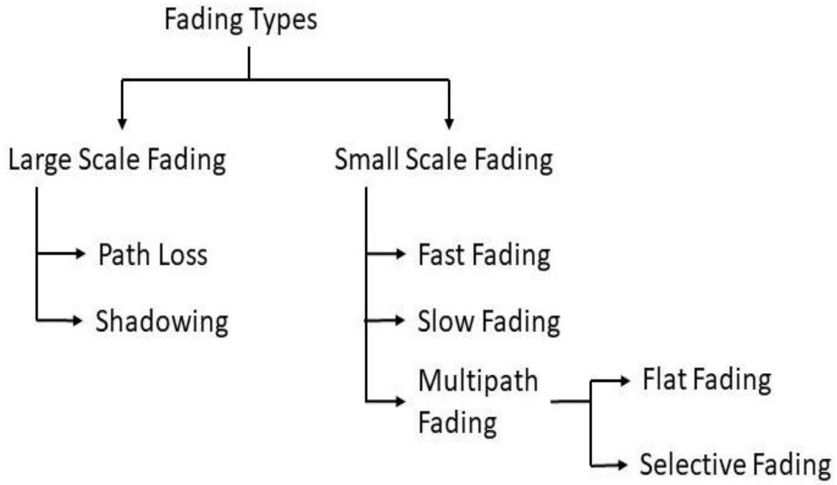
- Borrowing with Channel Locking was designed as an improvement over the simpler Channel Borrowing approach as described above [Elnoubi]. BCO systems have two distinctive characteristics [Elnoubi]:

1 The ratio of fixed to dynamic channels varies with traffic load.
2 Nominal channels are ordered such that the first nominal channel of a cell has the highest priority of being applied to a call within the cell.

The last nominal channel is most likely to be borrowed by neighboring channels. Once a channel is borrowed, that channel is locked in the co-channel cells within the reuse distance of the cell in question. To be "locked" means that a channel can not be used or borrowed. From a frequency reuse standpoint, in a BCO system, a channel may be borrowed only if it is free in the neighboring cochannel cells. This criteria is often too strict.

- In Borrowing with Directional Channel Locking, borrowed channels are only locked in nearby cells that are affected by the borrowing. This differs from the BCO scheme in which a borrowed channel is locked in every cell within the reuse distance. The benefit of BDCL is that more channels are available in the presence of borrowing and subsequent call blocking is reduced. A disadvantage of BDCL is that the statement "borrowed channels are only locked in nearby cells that are affected by the borrowing" requires a clear understanding of the term "affected." This may require microscopic analysis of the area in which the cellular system will be located. Ideally, a system can be general enough that detailed analysis of specific propagation measurements is not necessary for implementation.

Fading is a phenomenon that occurs due to varying parameters and conditions of the channel during wireless propagation. To better understand and eliminate the adverse effects of fading, it is divided into various types. Let us take a look into them in detail.



The figure above shows the different types of fading and the sub-categories. We have tried to elaborate on each type of fading below and provide information on how do they affect wave propagation.

1. Large Scale Fading: This refers to the attenuation of signal power due to obstacles between the transmitter and receiver. It also covers the attenuation and fluctuations of signal when the signal is transmitted over a long distance (usually in kilometres).

- **Path Loss: It refers to the attenuation when a signal is transmitted over large distances. Wireless signals spread as they propagate through the medium and as the distance increases, the energy per unit area starts decreasing.This is a fundamental loss that is independent of the type of transmitter and medium. Although, we can minimize its effects by increasing the capture area/dimension of the receiver. The figure below shows the radiation pattern and spread of the signal transmitted from the antenna.**

- **Shadowing: This refers to the loss in signal power due to the obstructions in the path of propagation. There are a few ways in which shadowing effects can minimize signal loss. One that is most effective, is to have a Line-Of-Sight propagation.**

Shadowing losses also depend on the frequency of the EM wave. As we know, EM Waves can penetrate through various surfaces but at the cost of loss in power i.e signal attenuation. The losses depend on the type of the surface and frequency of the signal. Generally, the penetration power of a signal is inversely proportional to the frequency of the signal.

2. Small Scale Fading: This refers to the fluctuations in signal strength and phase over short distance and small duration of time. It is also called Rayleigh Fading. Small Scale Fading affects almost all forms of wireless communication and overcoming them is a necessity to increase efficiency and decrease error.

- **Fast Fading: It occurs mainly due to reflections for surfaces and movement of transmitter or receiver. High doppler spread is observed in the fast fading with Doppler bandwidth comparable to or greater than the bandwidth of the signal and the channel variations are as fast or faster than the signal variations. It causes linear distortions in the shape of the baseband signal and**

creates Inter Symbol Interference (ISI). One way to remove ISI is adaptive equalization.

- **Slow Fading: It occurs mainly due to shadowing where large buildings or geographical structures obstruct the LOS. Low doppler spread is observed in Slow Fading with the doppler bandwidth being smaller compared to the bandwidth of the signal and the channel variations are slow relative to the signal variations. It results in reduction of SNR which can be overcome using error correction techniques and receiver diversity techniques.**
- **Multipath Fading: It occurs when a signal reaches the receiver from various path i.e. when multipath propagation takes place. Multipath fading can affect all ranges of frequencies starting from low frequency to microwave and beyond. It affects both the amplitude and the phase of the signal causing phase distortions and ISI. Multipath fading can affect signal transmission in two ways:**

○ **Flat Fading: In flat fading, all frequency components get affected almost equally. Flat multipath fading causes the amplitude to fluctuate over a period of time.**

○ **Selective Fading: Selective Fading or Selective Frequency Fading refers to multipath fading when the selected frequency component of the signal is affected. It means selected frequencies will have increased error and attenuation as compared to other frequency components of the same signal. This can be overcome by techniques such as OFDM which spreads the data across the frequency components of the signal to reduce data loss.**

DIVERSITY

Diversity is the use of multiple channels to increase the signal to noise ratio in the presence of random fading losses. The idea of diversity is “don’t put all of your eggs in one basket”.

For fading channels, we know that there is a finite probability that a signal power will fall below any given fade margin. For a Rayleigh channel, we showed that to have the signal above the required SNR 99% of the time, we needed to include a fade margin of 18.9 dB. This is a big "loss" in our link budget. For example, if we didn't need to include the fade margin in the link budget, we could multiply the path length by a factor of 1018.9/20 ≈ 10 (in free space); or increase the number of bits per symbol in the modulation significantly higher so that we can achieve higher bit rate for the same bandwidth.

There are several physical means to achieve multiple channels, and to get those channels to be nearly independent. Each has its advantages and disadvantages.

Space Diversity Space diversity at a receiver is the use of mul- tiple antennas across space. Because multipath fading changes quickly over space, the signal amplitude received on the different antennas can have a low correlation coefficient. The low correlation typically comes at separation distances of more than λ/2, where λ is the carrier wavelength. The Jakes model (equal power from all angles) says that the correlation coefficient at λ/2 is exactly zero; however, in reality, this is not true. The actual angular power profile (multi- path power vs. angle) determines the actual correlation coefficient. In general, we either accept that the correlation coefficient is not perfectly zero, or we separate the antennas further than λ/2. What is λ/2 at typical carrier frequencies. The problems with space diversity are most importantly that for consumer radios, want them to be small; and multiple antennas means that the device will be larger. This is fine when space is not a big concern – for base stations, or for laptops and access points. Another problem is, in general, a receiver with multiple antennas must have one RF chain (downconverter, LNA, filter) per antenna. An exception is that a receiver can use a

scanning combiner, which has an RF switch that scans between antennas, and switches when the SNR goes low.

The benefits of space diversity are that no additional signal needs to be transmitted, and no additional bandwidth is required. Space diversity could be used at a transmitter, by changing the transmit antenna until the receiver SNR is high enough. However, this requires some closed loop control, and so is less common. MIMO is a kind of space diversity and multipath diversity, that is more beneficial than simple diversity method. The multiple antennas don't need to have the same gain pattern.

Polarization Diversity Polarization diversity is the use of two antennas with different polarizations. We know that reflection coefficients are different for horizontal and vertically polarized components of the signal. Scattered and diffracted signal amplitudes and phases also are different for opposite polarizations. Thus, can consider one polarized signal, which is the sum of the amplitudes and phases of many reflected, scattered, and diffracted signals, to be nearly uncorrelated with the other polarized signal.

The advantages of polarization diversity is that the two anten- nas don't need to be spaced λ/2 apart, so polarization diversity can possibly be done on a mobile device. It may be combined with space diversity so to further reduce the correlation coefficient between the signal received at two antennas. Polarization diversity, like space diversity, doesn't require any additional bandwidth or signal transmission from the transmitter.

The disadvantages are simply that there can be only two chan- nels – vertical and horizontal (or equivalently, right-hand and left-hand circular) polarizations. It may require two receiver RF chains (again, unless a scanning combiner is used).

Frequency Diversity Frequency diversity uses multiple transmissions on different center frequencies. This doesn’t typically mean transmitting exactly the same thing on multiple different bands (which would require multiple times more bandwidth!). Frequency division multiplexing (FDM) or orthogonal FDM (OFDM) are the typical examples, which divide the data into N different bands. Error correction coding is used so that some percent of errors can be corrected, so if a certain percent of the bands experience deep fades, and all of that data is lost, the data can still be recovered during de- coding. Frequency bands in FDM or OFDM are typically somewhat correlated – each band needs to be in frequency flat fading so that equalization does not need to be used – but this means that bands right next to each other still have some positive fading correlation. FHSS is another frequency diversity example. FHSS may ex- perience deep fades (and interference) on some center frequencies among its hopping set, but it is unlikely to lose more than a percentage of its data. It also uses error correction coding.

Frequency diversity methods can also be set to control which frequency bands/ channels the transmitter uses, to remove the bands that are in deep fades. Again, this requires closed loop control.

Advantages of frequency diversity are that only one antenna, and one RF chain, is needed. A disadvantage is that, because some of the transmit power is used to send data in bands that are in deep fades, the power efficiency is less compared to space diversity, in which the transmitter sends all of its power in one channel.

Multipath diversity Multipath diversity is the capturing of multipath signals into independent channels. In DS-SS, a rake receiver achieves multipath diversity by isolating multipath components separately from each other based on their differing time delays. If one time delay group fades, another time delay group may not fade. These “fingers” of the rake receiver do not require

different RF chains (an advantage compared to space diversity) and benefit most when the multipath channel is the worst, for example, in urban areas, or in mountain canyons. The disadvantage of DS-SS is the large frequency band required – for example, 20 MHz for 802.11b, or 1.25 MHz for IS-95 (cellular CDMA). There is also significant computational complexity in the receiver, although standard ICs now exist to do this computation for these common commercial devices.

Time Diversity Time diversity is the use of a changing channel (due to motion of the TX or RX) at different times. For example, one might send the same data at multiple different times, but this would require multiple times the transmit power, and reduce the data rate possible on one channel. This incurs additional latency (delay). However, it is used in almost all common commercial systems in the form of "interleaving". Interleaving takes an incoming coded bitstream and spreads the bits across a transmitted packet in a known pattern. In the receiver, the inverse interleaving operation is performed. This way, a burst of (multiple sequential) coded bit errors caused by the channel are spread across the packet by the interleaver. Error correction codes are more effective when errors are not grouped together (recall our block coding and decoding – we assumed at most one error per 6 or 7 received coded bits). In general, coding methods correct a few out of each group of coded bits received, but not more.

Interleaving's only disadvantage is additional latency – need to receive the entire block of coded bits before they can be put in order and decoded (and then converted into an audio signal, for example). For different applications, latency requirements are different. Voice communications are typically the most latency-sensitive, and even cell phone voice data is interleaved.

The disadvantage is that temporal correlation can be very long for most applications, even for vehicular communications. Packet retransmissions (e.g., TCP) can be viewed as time diversity.

PCS ARCHITECTURE

Personal communications services (PCS) refers to a wide variety of wireless access and personal mobility services provided through a small terminal, with the goal of enabling communications at any time, at any place, and in any form.PCS technologies have grown rapidly in the telecommunications industry.

PCS architecture has mainly 3 types of Interfaces

Um interface The "air" or radio interface standard that is used for exchanges between a mobile (ME) and a base station (BTS / BSC). For signalling, a modified version of the ISDN LAPD, known as LAPDm is used.

Abis interface This is a BSS internal interface linking the BSC and a BTS, and it has not been totally standardised. The Abis interface allows control of the radio equipment and radio frequency allocation in the BTS.

A interface The A interface is used to provide communication between the BSS and the MSC.

PCS architecture divides into to 3 subsystem i.e.Base Station Subsystem(BSS),Network Switching Subsystem (NSS) and Operation and Support Subsystem (OSS)

Mobile station

PCS use mobile stations (MSs) to communicate with the base stations (BSs) in a PCS network. MS is also referred to as handset, mobile phone, subscriber unit, or portable. Mobile stations (MS),

mobile equipment (ME) or as they are most widely known, cell or mobile phones are the section of a GSM cellular network. In recent years their size has fallen dramatically while the level of functionality has greatly increased. There are a number of elements to the cell phone, although the two main elements are the main hardware and the SIM. It contains a number known as the International Mobile Equipment Identity (IMEI). This is installed in the phone at manufacture and “cannot” be changed. It is accessed by the network during registration to check whether the equipment has been reported as stolen.

The SIM or Subscriber Identity Module contains the information that provides the identity of the user to the network. It contains are variety of information including a number known as the International Mobile Subscriber Identity (IMSI).

Base Station Subsystem (BSS)

The Base Station Subsystem (BSS) section of the GSM network architecture that is fundamentally associated with communicating with the mobiles on the network. It consists of two elements:

Base Transceiver Station (BTS): The BTS used in a GSM network comprises the radio transmitter receivers, and their associated antennas that transmit and receive to directly communicate with the mobiles. The BTS is the defining element for each cell. The BTS communicates with the mobiles and the interface between the two is known as the Um interface with its associated protocols.

Base Station Controller (BSC): The BSC forms the next stage back into the GSM network. It controls a group of BTSs, and is often co-located with one of the BTSs in its group. It manages the radio resources and controls items such as handover within the

group of BTSs, allocates channels and the like. It communicates with the BTSs over what is termed the Abis interface.

Network Switching Subsystem (NSS)

The GSM system architecture contains a variety of different elements, and is often termed the core network. It provides the main control and interfacing for the whole mobile network. The major elements within the core network include:

Mobile Services Switching Centre (MSC): The main element within the core network area of the overall GSM network architecture is the Mobile switching Services Centre (MSC). The MSC acts like a normal switching node within a PSTN or ISDN, but also provides additional functionality to enable the requirements of a mobile user to be supported. These include registration, authentication, call location, inter-MSC handovers and call routing to a mobile subscriber. It also provides an interface to the PSTN so that calls can be routed from the mobile network to a phone connected to a landline. Interfaces to other MSCs are provided to enable calls to be made to mobiles on different networks.

Home Location Register (HLR): This database contains all the administrative information about each subscriber along with their last known location. In this way, the GSM network is able to route calls to the relevant base station for the MS. When a user switches on their phone, the phone registers with the network and from this it is possible to determine which BTS it communicates with so that incoming calls can be routed appropriately. Even when the phone is not active (but switched on) it re-registers periodically to ensure that the network (HLR) is aware of its latest position. There is one

HLR per network, although it may be distributed across various sub-centres to for operational reasons.

Visitor Location Register (VLR): This contains selected information from the HLR that enables the selected services for the individual subscriber to be provided. The VLR can be implemented as a separate entity, but it is commonly realised as an integral part of the MSC, rather than a separate entity. In this way access is made faster and more convenient.

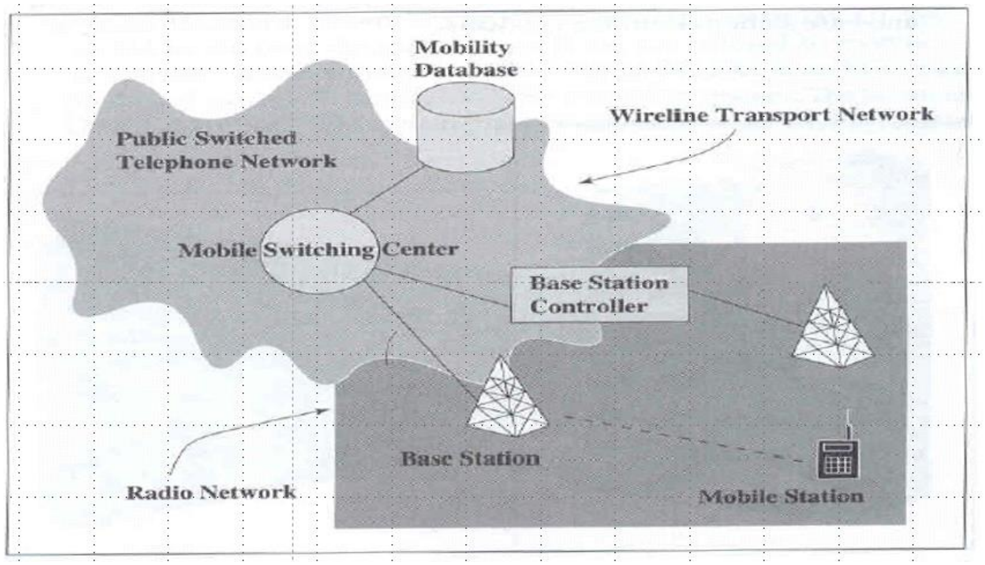
Equipment Identity Register (EIR): The EIR is the entity that decides whether a given mobile equipment may be allowed onto the network. Each mobile equipment has a number known as the International Mobile Equipment Identity. This number, as mentioned above, is installed in the equipment and is checked by the network during registration. Dependent upon the information held in the EIR, the mobile may be allocated one of three states – allowed onto the network, barred access, or monitored in case its problems.

Authentication Centre (AuC): The AuC is a protected database that contains the secret key also contained in the user's SIM card. It is used for authentication and for ciphering on the radio channel.

Gateway Mobile Switching Centre (GMSC): The GMSC is the point to which a ME terminating call is initially routed, without any knowledge of the MS's location. The GMSC is thus in charge of obtaining the MSRN (Mobile Station Roaming Number) from the HLR based on the MSISDN (Mobile Station ISDN number, the "directory number" of a MS) and routing the call to the correct visited MSC. The "MSC" part of the term GMSC is misleading, since the gateway operation does not require any linking to an MSC.

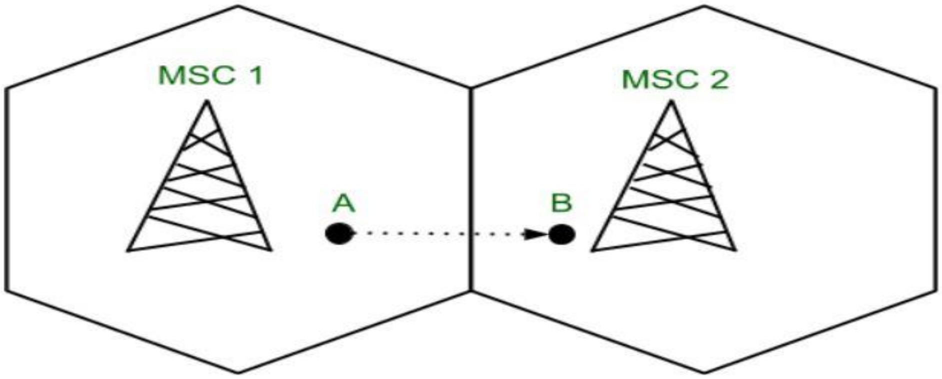
Operation and Support Subsystem (OSS)

The OSS or operation support subsystem is an element within the overall GSM network architecture that is connected to components of the NSS and the BSC. It is used to control and monitor the overall GSM network and it is also used to control the traffic load of the BSS. It must be noted that as the number of BS increases with the scaling of the subscriber population some of the maintenance tasks are transferred to the BTS, allowing savings in the cost of ownership of the system.



HAND OFF

In cellular telecommunications, the terms handover or handoff refers to the process of transferring ongoing call or data connectivity from one Base Station to other Base Station. When a mobile moves into the different cell while the conversation is in progress then the MSC (Mobile Switching Center) transfer the call to a new channel belonging to the new Base Station.



When a mobile user A moves from one cell to another cell then BSC 1 signal strength loses for the mobile User A and the signal strength of BSC 2 increases and thus ongoing calls or data connectivity for mobile user goes on without interrupting.

Types of Handoff:

1.11 Handoff in Cellular Systems

Handoff refers to a process of transferring an ongoing call or data session from one channel connected to the core network to another. The channel change due to handoff may be through a time slot, frequency band, code word, or combination of these for time- division multiple access (TDMA), frequency-division multiple access (FDMA), code- division multiple access (CDMA), or a hybrid scheme. Handoff is also called as 'Handover'.

Reasons for a Handoff to be conducted:

- **To avoid call termination when the phone is moving away from the area covered by one celland entering the area covered by another cell.**
- **When the capacity for connecting new calls of a given cell is used up.**
- **When there is interference in the channels due to the different phones using the samechannel in different cells.**
- **When the user behaviors change**

1.11.1 Types of Handoffs:-

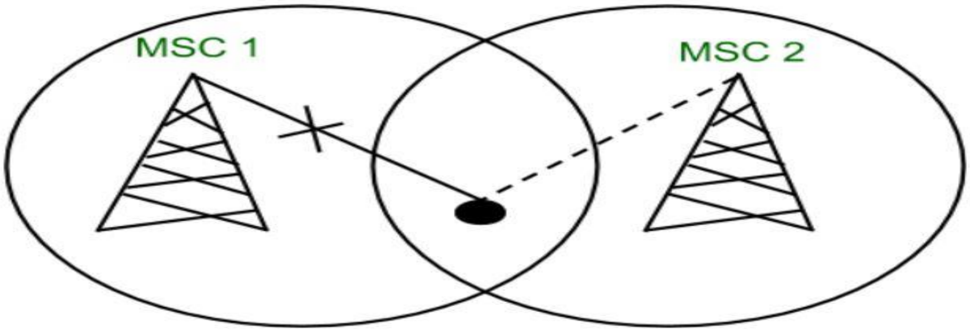
Handoffs are classified into two categories – ***hard and soft handoffs*****, which are further**

divided among themselves.

Hard handoff:

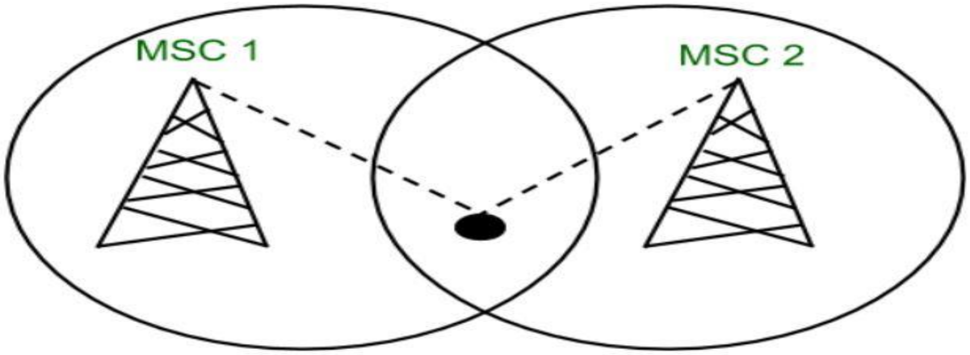
A hard handoff is essentially a "*break before make*" connection. Here the link to the prior base station is terminated before or as the user is transferred to the new cell's base station. This means thatthe mobile is linked to no more than one base station at a given time. A hard handoff occurs when users experience an interruption during the handover process caused by frequency shifting. A hard handoff is perceived by network engineers as event during the call. These are intended to be instantaneous in order to minimize the disruption of the call. Hard handoff can be further divided asintra and inter-cell handoffs.

Intra and inter-cell handoffs: In intra-cell handoff the source and target are one and the same cell andonly the used channel is changed during the handoff. The purpose of intra-cell handoff is to change achannel, which may be interfered, or fading with a new clearer or less fading channel. In inter-cell handoff the source and the target are different cells (even if they are on the same cell site). The purpose of the inter-cell handoff is to maintain the call as the subscriber is moving out of the area of the source cell and entering the area of the target cell. When there is an actual break in the connectivity while switching from one Base Station to another Base Station. There is no burden on the Base Station and MSC because the switching takes place so quickly that it can hardly be noticed by the users. The connection quality is not that good. Hard Handoff adopted the 'break before make' policy.



Soft handoff:

Soft handoff is also called as Mobile Directed Handoff as they are directed by the mobile telephones. Soft handoff is the ability to select between the instantaneous received signals from different base stations. Here the channel in the source cell is retained and used for a while in parallel with the channel in the target cell. In this the connection to the target is established before the connection to thesource is broken, hence this is called *"make-before-break"*. Soft handoffs can be classified as Multiwaysand softer handoffs. In Soft Handoff, at least one of the links is kept when radio signals are added or removed to the Base Station. Soft Handoff adopted the 'make before break' policy. Soft Handoff is more costly than Hard Handoff


MSC 1
MSC 2

- **Multiways and softer handoffs: A soft handoff which involves using connections to more than two cells is a multiways handoff. When a call is in a state of soft handoff the signal of the best of all used channels can be utilized for the call at a given moment or all the signalscan be combined to produce a clear signal, this type is called softer handoff.**

1.11.2 Types of handoff protocols:

There are four basic types of handoff protocols which help in providing continuous and QOS-guaranteed service. Namely:

- **Network-controlled handoff (NCHO)**
- **Mobile-assisted handoff (MAHO)**
- **Soft handoff (SHO) and**
- **Mobile-controlled handoff (MCHO)**

NCHO is a centralized handoff protocol, in which the network makes handoff decision based on measurements of the signal quality of mobile station (MS) at a number of based stations (BS). Sometimes the network sets up a bridge connection between the old and new BSs and thus minimizes the duration of handoff. This type of handoff is not suitable for a rapidly changing environment and a high density of users due to the associated delay.

An MAHO protocol distributes the handoff decision process. The MS makes measurements, and the MSC makes decisions.

SHO is a "make before break" connection. SHO is often used in conjunction with MAHO. Rather than immediately terminating the connection between a MS and a BS, the connection to the old BS is not broken until a connection to the new BS is made.

In MCHO, the MS is completely in control of the handoff process. This type of hand off has a short reaction time and is suitable for microcellular systems. A MS keeps on measuring signal strength from all the surround base stations. If the MS find that there is a new BS who has a stronger signal than that of an old BS, it may consider to handoff from the old BS to the new BS given a certain signal threshold is reached.

INTER BS HANDOFF

- **The new and the old BSs are connected to <u>the same MSC</u>.**
- **Assume that the need for handoff is detected by the MS; the following actions are taken:**

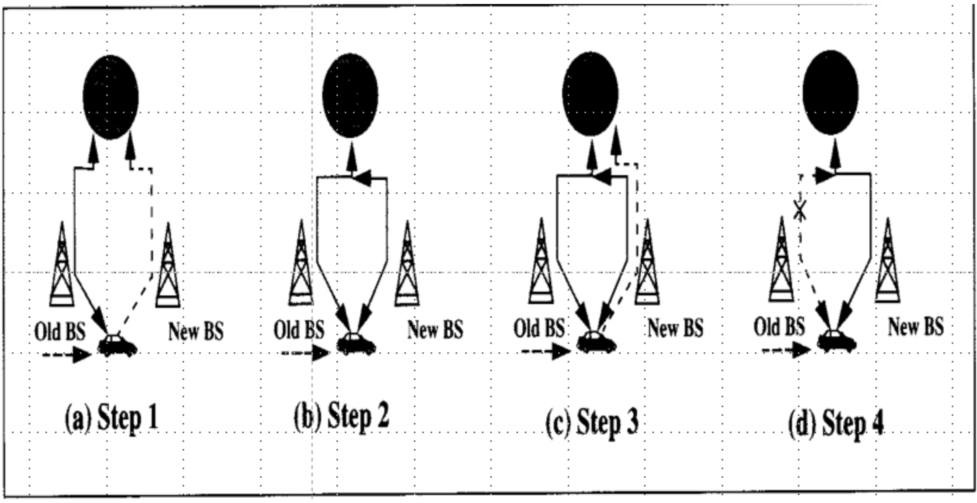
– 1. The MS momentarily suspends conversation and initiates the handoff procedure by signaling on an idle (currently free) channel in the new BS. Then it resumes the conversation on the old BS.

– 2. Upon receipt of the signal, the MSC transfers the encryption information to the selected idle channel of the new BS and sets up the new conversation path to the MS through that channel. The switch bridges the new path with the old path and informs the MS to transfer from the old channel to the new channel.

– 3. After the MS has been transferred to the new BS, it signals the network, and resumes conversation using the new channel.

– 4. Upon receipt of the handoff completion signal, the network removes the bridge from the path and releases resources associated with the old channel.

– This handoff procedure is used with the mobile-controlled handoff strategy



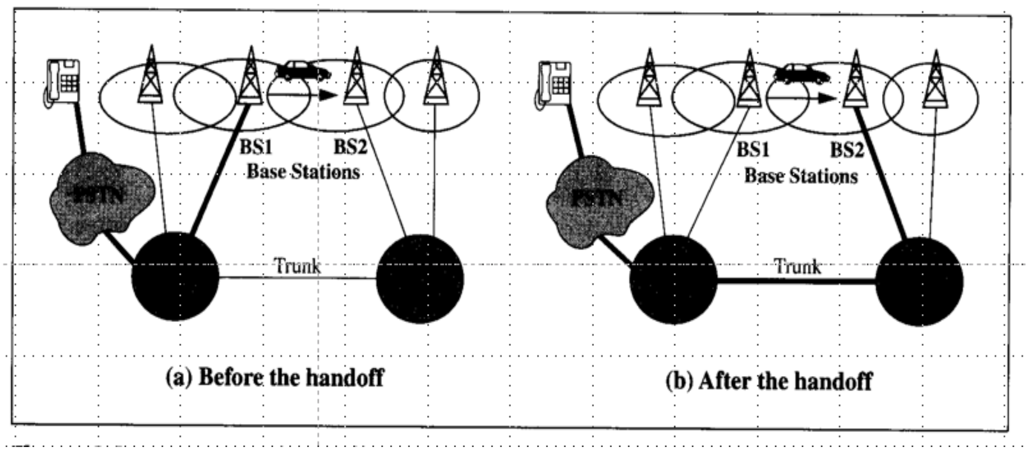
- For the **network-controlled handoff strategy**, all handoff signaling messages are exchanged between the MS and the old BS though the failing link.
- The whole process must be completed as quickly as possible, to ensure that the new link is established before the old link fails
- If the new BS does not have an idle channel, the handoff call may be dropped (or forced to terminate).
- The **forced termination probability** is an important criterion in the performance evaluation of a PCS network.
- Forced termination of an ongoing call is considered less desirable than blocking a new call attempt.
- Most PCS networks handle a handoff in the same manner as a new call attempt. That is, if no channel is available, the handoff is **blocked** and the call is held on the current channel in the old cell until the call is completed or when the failing link is no longer available.
- This is referred to as the **non-prioritized scheme**.

INTER SYSTEM HANDOFF

In intersystem handoff, the new and old BSs are connected to two **different MSCs**.

We trace the intersystem handoff procedure of IS-41, where network-controlled handoff (**NCHO**) is assumed.

In this figure, a communicating mobile user moves out of the BS served by MSC A and enters the area covered by MSC B.



(a) Before the handoff (b) After the handoff

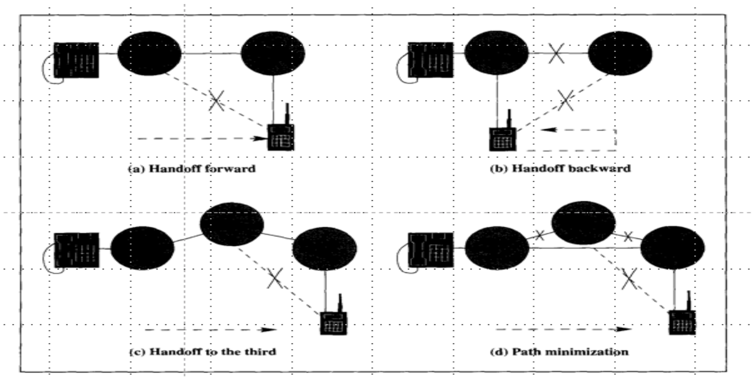
- **Intersystem handoff requires the following steps:**

Step 1. MSC A requests MSC B to perform handoff measurements on the call in progress. MSC B then selects a candidate BS2, BS2, and interrogates it for signal quality parameters on the call in progress. B returns the signal quality parameter values, along with other relevant information, to MSC A.

Step 2. MSC A checks if the MS has made too many handoffs recently (this is to avoid, for example, numerous handoffs between BS1 and BS2 a where the MS is moving within the overlapped area) or if intersystem trunks are not available. If so, MSC A exits the procedure. Otherwise, MSC A asks MSC B to set up a voice channel. Assuming that a voice channel is available in BS2, MSC B instructs MSC A to start the radio link transfer.

Step 3. MSC A sends the MS a handoff order. The MS synchronizes to BS2. After the MS is connected to BS2, MSC B informs MSC A that the handoff is successful. MSC A then connects the call path (trunk) to MSC B and completes the handoff procedure.

- **In this intersystem handoff process, MSC A is referred to as the anchor MSC, and is always in the call path before and after the handoff, as illustrated in the four cases in Figure.**
- **This anchor approach is used in all existing mobile phone networks because the re-establishment of a new call path (without involving MSC A) between MS and the new MSC would require extra trunk release/setup operations in PSTN, which is not available or is not cost-effective.**
- **If the MS moves back to MSC A again, the connection between MSC A and MSC B is removed (handoff backward).**
- **If the MS moves to the third MSC C, then MSC B will be in the call path (handoff to third).**
- **That is, the link between MSC B and MSC A is disconnected, and MSC C connects to MSC A directly.**
- **This process is called path minimization**
-



(a) Handoff forward

(b) Handoff backward

(c) Handoff to the third

(d) Path minimization

Question bank

PART A

1 Draw the cell structure

2 Define handoff

3 What are the two types of switching techniques

4 Define hard handoff

5 Define soft handoff

6 List the features of 5G

7 Compare 1G and 2G

8 Sketch the electromagnetic spectrum

9 List the types of channel assignment

10 Define fading

11 Compare flat and frequency selective fading

12 What are the various diversity techniques?

13 Define uplink and downlink

14 Differentiate inter system and inter BS handoff

15 List out few wireless communication standards

PART B

1 Discuss the History of Wireless communication

2 Compare and Contrast the Evolution from 1G to 5G

3 Explain the cellular system concepts

4 Discuss in detail the various channel assignment strategies

5 Explain the various diversity techniques

6 Explain hard and soft handoff

7 Distinguish inter BS and inter system handoff

TEXT / REFERENCE BOOKS

1. Andreas F. Molisch, “Wireless Communications”, 2n d Edition, John Wiley & Sons Ltd, 2011.

2. William C.Y. Lee., "Wireless & Cellular Telecommunications", 3rd edition, McGraw Hill.2006.

3. Yibing Lin, "Wireless & mobile Network architecture", Wiley 2002.

4. Tao Jiang, Lingyang Song and Van Zhang, “Orthogonal Frequency Division Multiple Access Fundamentals and Applications” Taylor and Francis Group, 2010.

5. Yong Soo Cho, Jaekwon Kim, Won Young Yang and Chung G. Kang, “MIMO-OFDM Wireless Communications with MATLAB”, John Wiley & Sons (Asia) Pvt. Ltd, 2010.

SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE
www.sathyabama.ac.in

SCHOOL OF ELECTRICAL AND ELECTRONICS
DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

UNIT – II – 2G AND B2G SYSTEMS – SEC1404

Global System for Mobile communications (GSM) - Functional architecture of GSM - Common control channels - Dedicated control channels -Location tracking and call setup - GSM location update - Short Message Service (SMS) -Network architecture of SMS - Protocol hierarchy of SMS.Evolving from GSM to General Packet Radio Service (GPRS) - Functional groups of GPRS - Architecture of GPRS - Interfaces of GPRS

GSM

GSM Architecture

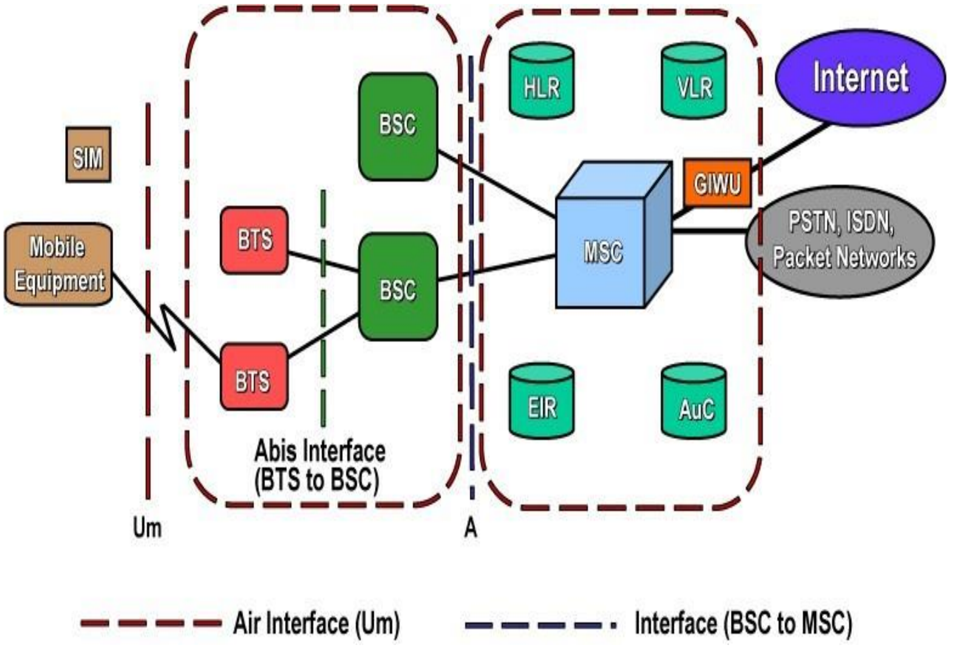
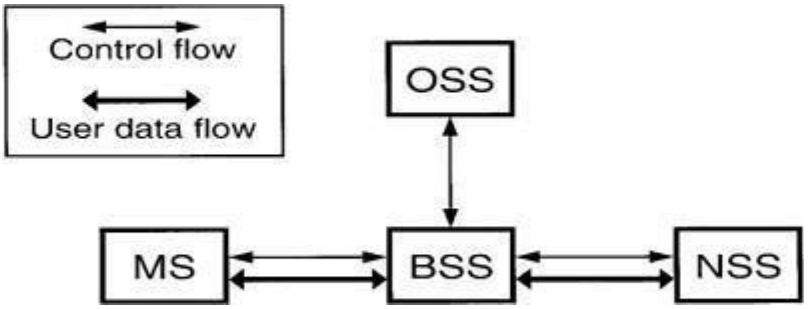


Figure 2.1 GSM

GSM Figure 2.1 consists of many subsystems, such as the mobile station (MS), the base station sub system (BSS), the network and switching subsystem (NSS), and the operation subsystem(OSS).



The external environment of BSS

The Mobile Station: The MS may be a stand-alone piece of equipment for certain services or support the connection of external terminals, such as the interface fora personal computer or fax. The MS includes mobile equipment (ME) and a subscriber identity module (SIM). ME does not need to be personally assigned to one subscriber. The SIM is a subscriber module which stores all the subscriber- related information. When a subscriber's SIM is inserted into the ME of an MS, that MS belongs to the subscriber, and the call is delivered to that MS. The ME is not associated with a called number it is linked to the SIM. In this case, any ME can be used by a subscriber when the SIMis inserted in the ME.

Base Station Subsystem: The BSS connects to the MS through a radio interface and also connects to the NSS. The BSS consists of a base transceiver station (BTS) located at the antenna site and a base station controller (BSC) that may control several BTSs. The BTS consistsof radio transmission and reception equipment similar to the ME in an MS.

A transcoder/rate adaption unit (TRAU) carries out encoding and speech decoding and rate adaptation for transmitting data. As a subpart of the BTS, the TRAU may be sited away from the BTS, usually at the MSC. In this case, the low transmission rate of speech code channels allows more compressed transmission between the BTS and the TRAU, which is sited at the MSC. GSM uses the open system interconnection (OSI). There are three common interfaces based on OSI (Fig. 3.1.): a common radio interface, called air interface, between the MS and BTS, an interface A between the MSC and BSC, and an A-bis interface between the BTS and BSC. With these common interfaces, the system operator can purchase the product of manufacturing company A to interface with the product of

manufacturing company B. The difference between interface and protocol is that an interface represents the point of contact between two adjacent entities (equipment or systems) and a protocol provides information flowsthrough the interface.

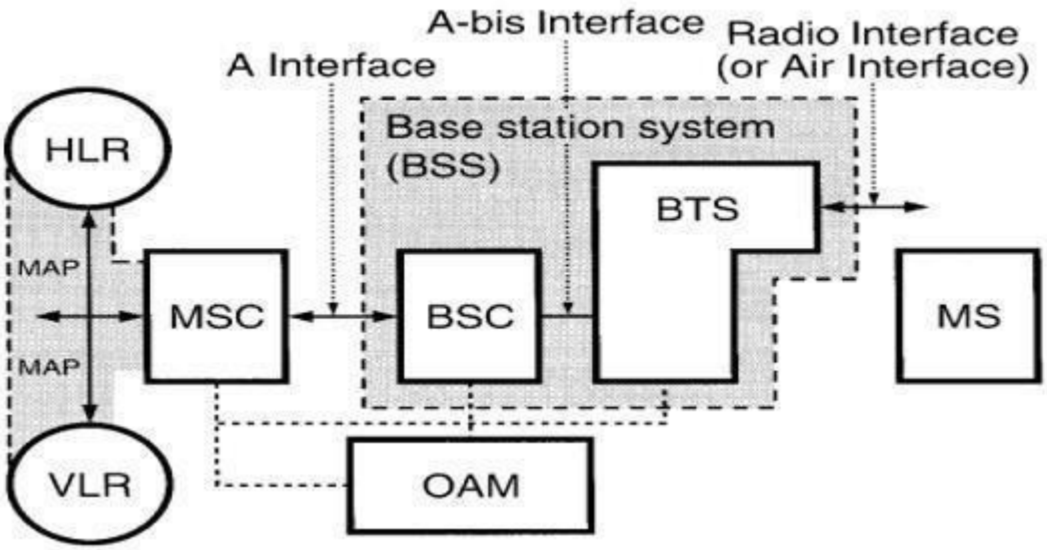


Figure 2.2 The functional architecture and principal interfaces

For example, Figure 2.2 the GSM radio interface is the transit point for information flow pertaining toseveral protocols.

Network and Switching Subsystem: NSS (see Fig. 3.2.) in GSM uses an intelligent network(IN). The IN's attributes will be described later. A signaling NSS includes the main switching functions of GSM. NSS manages the communication between GSM users and other telecommunications users. NSS management consists of:

Mobile service switching center (MSC): Coordinates call set-up to and from GSM users. An MSC controls several BSCs.

Interworking function (IWF): A gateway for MSC to interface with external networks for communication with users outside GSM, such as packet-switched public data network (PSPDN)or circuit-switched public data network (CSPDN).The role of the IWF depends on the type of userdata and the network to which it interfaces.

Home location register (HLR): Consists of a stand-alone computer without switching capabilities, a database which contains subscriber information, and information related to

the subscriber's current location, but not the actual location of the subscriber. A subdivision of HLR is the authentication center (AUC). The AUC manages the security data for subscriber authentication. Another sub-division of HLR is the equipment identity register (EIR) which stores the data of mobile equipment (ME) or ME-related data.

Visitor location register (VLR): Links to one or more MSCs, temporarily storing subscription data currently served by its corresponding MSC, and holding more detailed data thanthe HLR.

For example, the VLR holds more current subscriber location information than the locationinformation at the HLR.

Gateway MSC (GMSC): In order to set up a requested call, the call is initially routed to a gateway MSC, which finds the correct HLR by knowing the directory number of the GSM subscriber. The GMSC has an interface with the external network for gatewaying, and the networkalso operates the full Signaling System 7 (SS7) signaling between NSS machines.

Signaling transfer point (STP): Is an aspect of the NSS function as a stand-alone node or in the same equipment as the MSC. STP optimizes the cost of the signaling transport among MSC/VLR, GMSC, and HLR. As mentioned earlier, NSS uses an intelligent network. It separates the central data base (HLR) from the switches (MSC) and uses STP to transport signaling among MSC and HLR.

Operation Subsystem: There are three areas of OSS, as shown in Fig.. 2.3 and 2.4(network operation and maintenance functions, (2) subscription management, including charging andbilling, and (3)mobile equipment management. These tasks require interaction between some or all of the infrastructure equipment. OSS is implemented in any existing network.

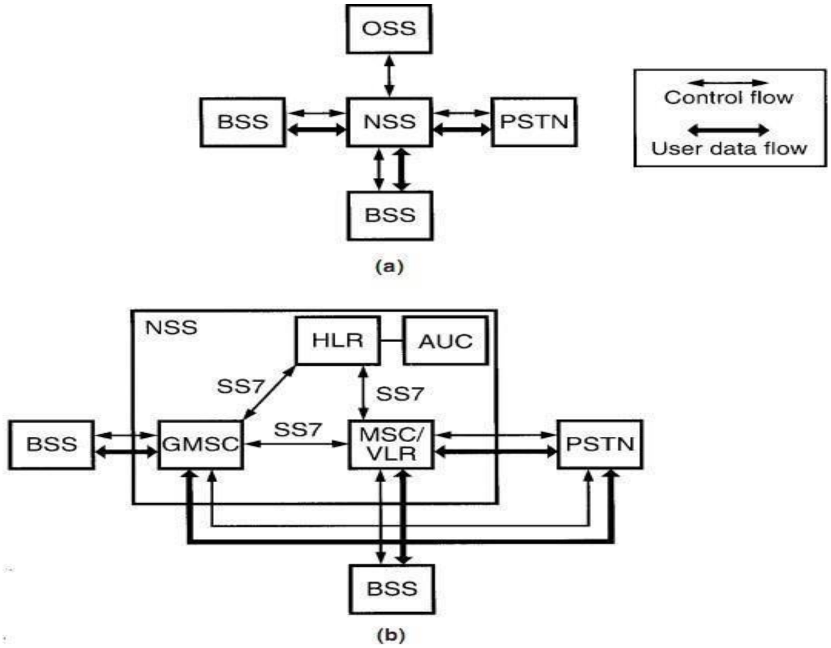


Figure 2.3 NSS and its environment (a) the external environment; (b) the internal structure

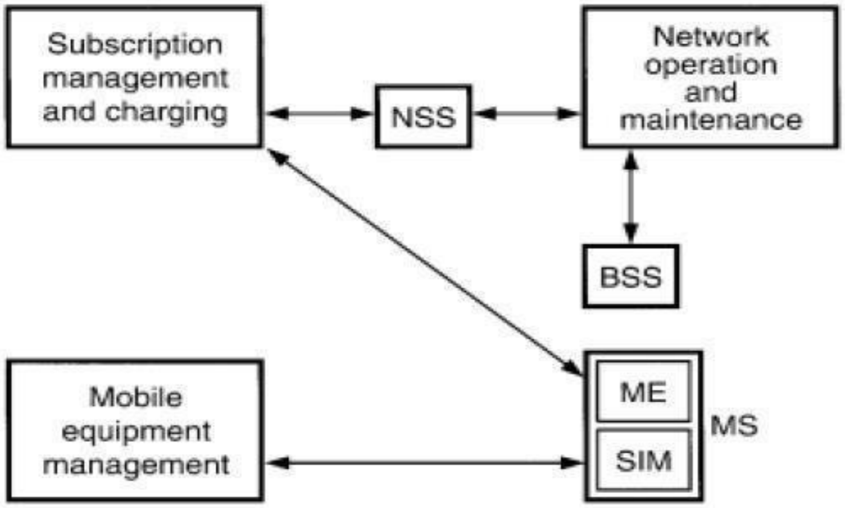

Subscription management and charging
NSS
Network operation and maintenance
BSS
Mobile equipment management
ME
SIM
MS

Figure 2.4 OSS organization

GSM Channel Structure: The services offered to users have four radio transmission modes, three data modes, and a speech mode. The radio transmission modes use the physicalchannels.

Physical Channels: There are three kinds of physical channels, also called traffic channels (TCHs):

i. **TCH/F (full rate): Transmits a speech code of 13 kbps or three data-mode rates, 12, 6, and 3.6 kbps.**

ii. **TCH/H (half rate): Transmits a speech code of 7 kbps or two data modes, 6 and 3.6 kbps.**

iii. **TCH/8 (one-eighth rate): Used for low-rate signaling channels, common channels, and data channels.**

Logic channels:

1. **Common channels: All the common channels are embedded in different traffic channels. Theyare grouped by the same cycle (51 × 8 BP), where BP stands for burst period (i.e., time slot), which is 577 µs.**

2. **Downlink common channels: There are five downlink unidirectional channels, sharedor grouped by a TCH.**

- **Frequency correction channel (FCCH) repeats once every 51×8 BPs; used to identifya beacon frequency.**
- **Synchronization channel (SCH) follows each FCCH slot by 8 BPs.**
- **Broadcast control channel (BCCH) is broadcast regularly in each cell and received by all themobile stations in the idle mode.**
- **Paging and access grant channel (PAGCH) is used for the incoming call received at the mobile station. The access grant channel is answered from the base station and allocates achannel during the access procedure of setting up a call.**
- **Call broadcast channel (CBCH). Each cell broadcasts a short message for 2s from the network to the mobile station in idle mode. Half a downlink TCH/8 is used, and special CBCH design constraints exist because of the need for sending two channels (CBCH and BCCH) in parallel. The mobile station (MS) finds the FCCH burst, then looks for an SCHburst on the same frequency to achieve synchronization. The MS then receives BCCH on several time slots and selects a proper cell, remaining for a period in the idle mode.**

3. **Uplink common channels: The random-access channel (RACH) is the only common uplink channel. RACH is the channel that the mobile station chooses to access the**

calls. There are tworates: RACH/F (full rate, one time slot every 8 BP), and RACH/H (half rate, using 23 time slotsin the 51 × 8 BP cycle, where 8 BP cycle [i.e. a frame] is 4.615ms).

4. Signaling channels: All the signaling channels have chosen one of the physical channels andthe logical channels names are based on their logical functions:

5. Slow Associated Control Channel (SACCH): A slow-rate TCH used for signaling transport and used for non urgent procedures, mainly handover decisions. It uses one-eighth rate. The TCH/F is always allocated with SACCH. This combined TCH and SACCH is denoted TACH/F. SACCH occupies 1 time slot (0.577 ms) in every 26 frames (4.615ms × 26). The time organizationof a TACH/F is shown in Fig.2.5

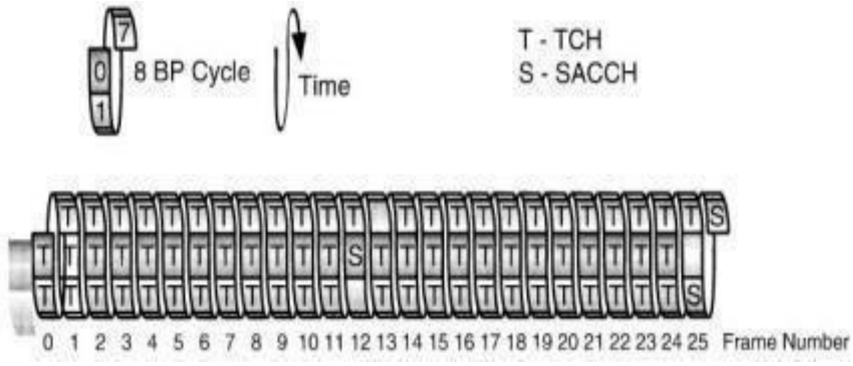

7
0
1
8 BP Cycle
Time
T - TCH
S - SACCH
T
S
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 Frame Number

Figure 2.5 Time organization of TACH/F6.

6. Fast Associated Control Channel (FACCH): Indicates cell establishment,authenticates subscribers, or commands a handover.

7. Stand-alone Dedicated Control Channel (SDCCH): Occasionally the connection between amobile station and the network is used solely for passing signaling information and not for calls.This connection may be at the user's demand or for other management operations such asupdating the unit's location. It operates at a very low rate and uses a TCH/8 channel. Radio slotsare allocated to users only when call penetration is needed. There are two modes, dedicated andidle. The mode used depends on the uplink and the downlink. In GSM terminology, the downlinkis the signal transmitted from the base

station to the mobile station, and the uplink is the signal transmitted in the opposite direction.

8. Voice/data channels: Each time slot of a voice channel contains 260 bits per block. The entire block contains 316 bits. Each time slot of a data channel contains 120 or 240 bits per block.

The different modes of GSM channel are as follows

1. Channel mode: Because of the precious value of the radio spectrum, individualusers cannot have their own TCH at all times.

2. Dedicated mode: Uses TCH during call establishment and uses SACCH to performlocation updating in the dedicated mode. TCH and SACCH are dedicated channels for both

uplink and downlink channels.

3. Idle mode: During non call activities, the five downlink channels are in the idle mode: FCCH; SCH; BCCH, which is broadcasting regularly; PAGCH and CBCH, which sends one message every 2 s. During idle mode, the mobile station listens to the common downlink channels, and also uses SDCCH (uplink channel) to register a mobile location associated with a particular base station to the network.

GSM Mobility Management

Mobility management is one of the major functions of a GSM or a UMTS network that allows mobile phones to work. The aim of mobility management is to track where the subscribers are, allowing calls, SMS and other mobile phone services to be delivered to them.

Location update procedure :

A GSM or UMTS network, like all cellular networks, is basically a radio network of individual cells, known as base stations. Each base station covers a small geographical area which is part of a uniquely identified location area. By integrating the coverage of each of

these base stations, a cellular network provides a radio coverage over a much wider area. A group of base stations is named a location area, or a routing area.

The location update procedure allows a mobile device to inform the cellular network, whenever it moves from one location area to the next. Mobiles are responsible for detecting location area codes (LAC). When a mobile finds that the location area code is different from its last update, it performs another update by sending to the network, a location update request, together with its previous location, and its Temporary Mobile Subscriber Identity (TMSI).

The mobile also stores the current LAC in the SIM card, concatenating it to a list of recently used LACs. This is done to avoid unnecessary IMSI attachment procedures in case the mobile has beenforced to switch off (by removing the battery, for example) without having a chance to

notify the network with an IMSI detach and then switched on right after it has been turned off. Considering the fact that the mobile is still associated with the Mobile Switching Center/Visitor Location Register (MSC/VLR) of the current location area, there is no need for any kind of IMSIattachment procedures to be done.

TMSI:

The Temporary Mobile Subscriber Identity (TMSI) is the identity that is most commonly sent between the mobile and the network. TMSI is randomly assigned by the VLR to every mobilein the area, the moment it is switched on. The number is local to a location area, and so it has to be updated each time the mobile moves to a new geographical area.

The network can also change the TMSI of the mobile at any time. And it normally does so, in order to avoid the subscriber from being identified, and tracked by eavesdroppers on the radio interface. This makes it difficult to trace which mobile is which, except briefly, when the mobile isjust switched on, or when the data in the mobile becomes invalid for one reason or another. At that point, the global "international mobile subscriber identity" (IMSI) must be sent to the network. The IMSI is sent as rarely as possible, to avoid it being identified and tracked.

Roaming:

Roaming is one of the fundamental mobility management procedures of all cellular networks. Roaming is defined as the ability for a cellular customer to automatically make

and receive voice calls, send and receive data, or access other services, including home data services, when travelling outside the geographical coverage area of the home network, by means of using avisited network. This can be done by using a communication terminal or else just by using the subscriber identity in the visited network. Roaming is technically supported by a mobility management, authentication, authorization and billing procedures.

Location Related Databases

Two databases are used by Location Management to store MS location related data.

Visitor LocationRegister(VLR) Home
Location Register(HLR)

Visitor Location Register

A VLR contains a data record for each of the MS that are currently operating in its area. Each record contains a set of subscriber identity codes, related subscription information, and a Location Area Identity (LAI) code. This information is used by the MSC when handling calls to or from an MS in the area. When an MS moves from one area to another, the responsibility for its supervision passes from one VLR to another. A new data record is created by the VLR thathas adopted the MS, and the old record is deleted. Provided that aninter-working agreement exists between the network operators

concerned, data transaction can cross both network and national boundaries.

Home Location Register

The HLR contains information relevant to mobile subscribers who are fee-paying customers ofthe organization that operates the PLMN.

Subscription Information

The subscription information includes the IMSI and directory number allocated to the subscriber, the type of services provided and any related restrictions.

Location Information

The location information includes the address of the VLR in the area where the subscribers MSis currently located and the address of the associated MSC.

The location information enables incoming calls to be routed to the MS. The absence of this

information indicates that the MS is inactive and cannot be reached.

When an MS moves from one VLR area to another, the location information in the HLR is updated with the new entry for the MS, using subscription data copied from the HLR. Providedthat an inter- working agreement exists between the network operators, concerned datatransactions can move across both network and national boundaries.

Types of Identification Numbers

During the performance of the location update procedure and the processing of a mobile call different types of numbers are used

Mobile Station ISDN Number(MSISDN)Mobile Subscriber

Roaming Number(MSRN)

❑ International Mobile Subscriber

Identity(IMSI) Mobile

❑ Temporary

Subscriber Identity(TMSI) Local MobileStation Identity(LMSI).

GSM Handover

One of the key elements of a mobile phone or cellular telecommunications system, is that thesystem is split into many small cells to provide good frequency re-use and coverage. However

as the mobile moves out of one cell to another it must be possible to retain the connection. The process by which this occurs is known as handover or handoff. The term handover is more widely used within Europe, whereas handoff tends to be use more in North America. Either way, handover and handoff are the same process.

Requirements for GSM handover

The process of handover or handoff within any cellular system is of great importance. It isa critical process and if performed incorrectly handover can result in the loss of the call. Dropped calls are particularly annoying to users and if the number of dropped calls rises, customer dissatisfaction increases and they are likely to change to another network. Accordingly GSM handover was an area to which particular attention was paid when developing the standard.

Types of GSM handover

Within the GSM system there are four types of handover that can be performed for GSM onlysystems:

Intra-BTS handover: **This form of GSM handover occurs if it is required to change the frequency or slot being used by a mobile because of interference, or other reasons. In this form of GSM handover, the mobile remains attached to the same base station transceiver,but changes the channel or slot.**

Inter-BTS Intra BSC handover: **This for of GSM handover or GSM handoff occurs whenthe mobile moves out of the coverage area of one BTS but into another controlled by thesame BSC. In this instance the BSC is able to perform the handover and it assigns a newchannel and slot to the mobile, before releasing the old BTS from communicating with the mobile.**

Inter-BSC handover: **When the mobile moves out of the range of cells controlled by one BSC, a more involved form of handover has to be performed, handing over not only fromone BTS to another but one BSC to another. For this the handover is controlled by the MSC.**

Inter-MSC handover: **This form of handover occurs when changing between networks. The two MSCs involved negotiate to control the handover.**

GSM handover process

Although there are several forms of GSM handover as detailed above, as far as the mobileis concerned, they are effectively seen as very similar. There are a number of stages involved in undertaking a GSM handover from one cell or base station to another.

In GSM which uses TDMA techniques the transmitter only transmits for one slot in eight, and similarly the receiver only receives for one slot in eight. As a result the RF section of the mobilecould be idle for 6 slots out of the total eight. This is not the case because during the slots in which it is not communicating with the BTS, it scans the other radio channels looking for beacon frequencies that may be stronger or more suitable. In addition to this, when the mobile communicates with a particular BTS, one of the responses it makes is to send out a list of the radiochannels of the beacon frequencies of neighboring BTSs via the Broadcast Channel (BCCH).

The mobile scans these and reports back the quality of the link to the BTS. In this way the mobileassists in the handover decision and as a result this form of GSM handover is known as Mobile Assisted Hand Over (MAHO).

The network knows the quality of the link between the mobile and the BTS as well as the strength of local BTSs as reported back by the mobile. It also knows the availability of channels in the nearby cells. As a result it has all the information it needs to be able to make a decision about whether it needs to hand the mobile over from one BTS to another.

If the network decides that it is necessary for the mobile to hand over, it assigns a new channel and time slot to the mobile. It informs the BTS and the mobile of the change. The mobile then retunes during the period it is not transmitting or receiving, i.e. in an idle period.

A key element of the GSM handover is timing and synchronization. There are a number of possible scenarios that may occur dependent upon the level of synchronization.

GSM User Services:

GSM offers three basic types of services:

Telephony services or teleservices Data services or bearer services Supplementary services

Teleservices

The abilities of a Bearer Service are used by a Tele-service to transport data. These services are further transited in the following ways:

Voice Calls

The most basic Teleservice supported by GSM is telephony. This includes full-rate speech at 13 kbps and emergency calls, where the nearest emergency-service provider is notified by dialing three digits.

Videotext and Facsmile

Another group of teleservices includes Videotext access, Teletex transmission, Facsmile alternate speech and Facsmile Group 3, Automatic Facsmile Group, 3 etc.

Short Text Messages

Short Messaging Service (SMS) service is a text messaging service that allows sending and receiving text messages on your GSM mobile phone. In addition to simple text messages,

othertext data including news, sports, financial, language, and location-based data can also be transmitted.

Bearer Services

Data services or Bearer Services are used through a GSM phone. to receive and send data is the essential building block leading to widespread mobile Internet access and mobile data transfer. GSM currently has a data transfer rate of 9.6k. New developments that will push up data transfer rates for GSM users are HSCSD (high speed circuit switched data) and GPRS (generalpacket radio service) are now available.

Supplementary Services

Supplementary services are additional services that are provided in addition to teleservices andbearer services. These services include caller identification, call forwarding, call waiting, multi- party conversations, and barring of outgoing (international) calls, among others. A brief description of supplementary services is given here:

Conferencing : It allows a mobile subscriber to establish a multiparty conversation, i.e., a simultaneous conversation between three or more subscribers to setup a conference call. This service is only applicable to normal telephony.

Call□Waiting : This service notifies a mobile subscriber of an incoming call during a conversation. The subscriber can answer, reject, or ignore the incoming call.

Call□Hold : This service allows a subscriber to put an incoming call on hold and resume after a while. The call hold service is applicable to normal telephony.

Call□Forwarding : Call Forwarding is used to divert calls from the original recipient to another number. It is normally set up by the subscriber himself. It can be used by the subscriber to divert calls from the Mobile Station when the subscriber is not available, and so to ensure that calls are not lost.

Call□Barring : Call Barring is useful to restrict certain types of outgoing calls such as ISDor stop incoming calls from undesired numbers. Call barring is a flexible service that enables the subscriber to conditionally bar calls.

Number Identification : There are following supplementary services related to number identification:

o **Calling Line Identification Presentation : This service displays the telephone number of the calling party on your screen.**

o Calling Line Identification Restriction : A person not wishing their number to bepresented to others subscribes to this service.

o Connected Line Identification Presentation : This service is provided to give the calling party the telephone number of the person to whom they are connected. This service is useful in situations such as forwarding's where the number connected is not the number dialled.

o Connected Line Identification Restriction : There are times when the person called does not wish to have their number presented and so they would subscribe to this person. Normally, this overrides the presentation service.

o Malicious Call Identification : The malicious call identification service was provided to combat the spread of obscene or annoying calls. The victim should subscribe to this service, and then they could cause known malicious calls to be identified in the GSM network, using a simple command.

Advice of Charge (AoC) : This service was designed to give the subscriber an indication of the cost of the services as they are used. Furthermore, those service providers who wish to offer rental services to subscribers without their own SIM can also utilize this service in a slightly different form. AoC for data calls is provided on the basis of time measurements.

Closed User Groups (CUGs) : This service is meant for groups of subscribers who wish to call only each other and no one else.

Unstructured supplementary services data (USSD) : This allows operator-defined individual services.

GSM International mobile Roaming:

International mobile roaming is a service that allows mobile users to continue to use their mobile phone or other mobile device to make and receive voice calls and text messages, browse

the internet, and send and receive emails, while visiting another country. Roaming extends thecoverage of the home operator's retail voice and SMS services, allowing the mobile user to continue using their home operator phone number and data services within another country. The seamless extensionof coverage is enabled by a wholesale roaming agreement between a mobile user's home operatorand the visited mobile operator network. The roaming agreement addresses the technical and commercial components required to

enable the service.

The most common international roaming services are:

Voice: Making and receiving calls to or from home country, visited country or a third country, whileabroad

SMS: Sending and receiving text messages to or from home country, visited country or a third country,while abroad

Email: Reading and replying to emails while abroad

Mobile broadband: Using mobile devices or dongles to access the internet, including downloadingimages, MP3s, films and software, while abroad

Applications: Using mobile applications while abroad that require mobile data, such as location-based services and language translators. International mobile roaming is one of a wider range of communications services offered to mobile users while travelling abroad, which also include hotelservices, Wi-Fi, national "travel" SIMs, and visited operator SIMs.

mobile roaming working principle

When a mobile user is abroad and turns their mobile device on, the mobile device attempts to communicate with a visited mobile network. The visited network picks up the connection from the user's mobile, recognizes whether Figure 3.7 the shows commercial and technical details for international mobile roaming. The diagram focuses on the international roaming wholesale and retail arrangements, for simplicity. The mobile user (Mobile User A) has an international roaming service with their home operator (Home Operator) and is automatically connected to a visited network (Visited Operator A) while roaming. Mobile User A is automatically granted access to Visited Operator A's network when arriving in the visited country by an exchange of a data between Home Operator and Visited Operator A, where Visited Operator A confirms Mobile User A is a roaming customer with Home Operator. As such, the wholesale roaming agreement between Visited Operator A and Home Operator specifies how this data is to be provided to the visited operator. Home Operator usually has wholesale roaming agreements with more than one operator in the same visited country, which in this case is Visited Operator A and a second network, Visited Operator B. As a result, Mobile User A can call home using either visited operator networks, bothof which use international transit services to carry the call back to Mobile User A's home country. Mobile User A pays a retail price to Home Operator for the roaming service and

does not pay Visited Operator A. Provided Mobile User B is not also roaming; they will not incur any extra charges to receive a call from, or to make calls to Mobile User A. Visited Operator A sends transferred account procedure (TAP) files to a clearing house which forwards them to the Home Operator. TAP files are used for billing of calls while roaming. Home Operator can then pay Visited Operator A the wholesale charges as per call volumes in the TAP file and rates in the wholesale roaming agreement. It is registered with its system, and attemptsto identify the user's home network. If there is a roaming agreement between the home network and one of the mobile networks in the visited country, the call is routed by the visited network towards an international transit network (Figure 2.6 and 2.7). The international transit network carrier is responsible for the call delivery to the destination network. Once this is done, the destination network will connect the call.

The visited network also requests service information from the home network about the user, such as whether the phone being used is lost or stolen, and whether the mobile device is authorized for international use. If the phone is authorized for use, the visited network creates a temporary subscriber record for the device and the home network updates its subscriber record on where the device is located so if a call is made to the phone it can be appropriately routed.

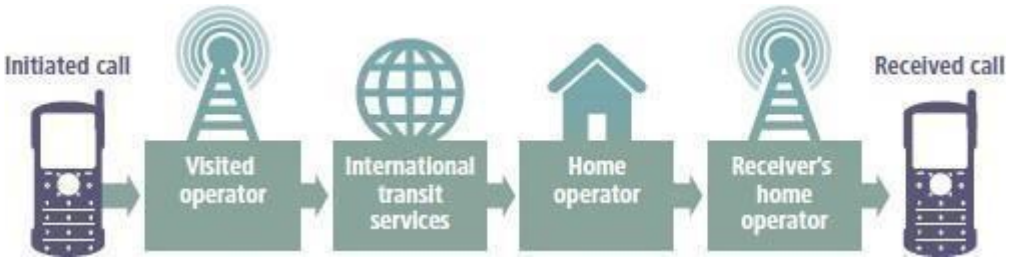


Figure 2.6 overview of international roaming technology and operations

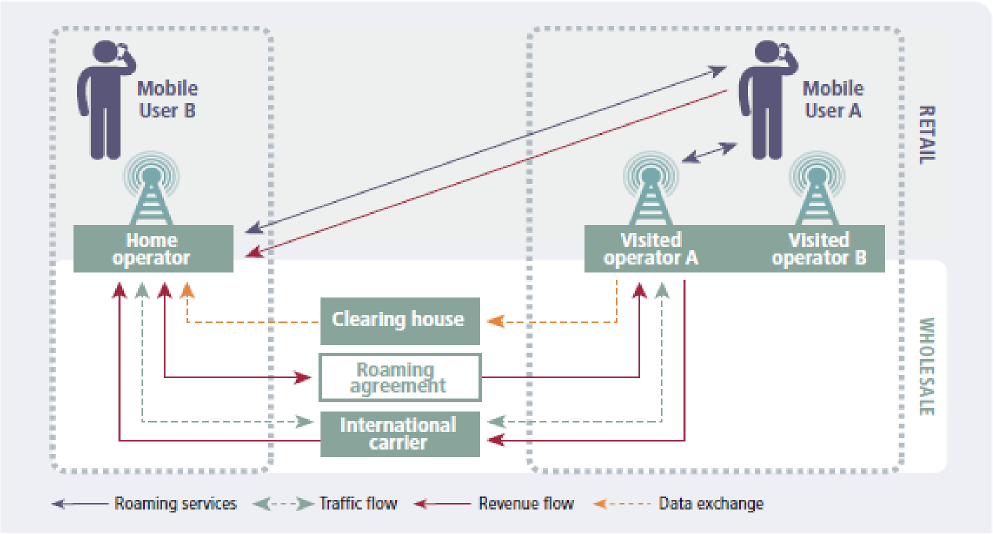


Figure 2.7 commercial link required for international mobile roaming

GSM Security:

GSM is the most secured cellular telecommunications system available today. GSM has its security methods standardized. GSM maintains end-to-end security by retaining the confidentiality of calls and anonymity of the GSM subscriber.

Temporary identification numbers are assigned to the subscriber's number to maintain the privacy of the user. The privacy of the communication is maintained byapplying encryption algorithms and frequency hopping that can be enabled using digital systems and signalling.

This chapter gives an outline of the security measures implemented for GSM subscribers.

Mobile StationAuthentication

The GSM network authenticates the identity of the subscriber through the use of a challenge-response mechanism. A 128-bit Random Number (RAND) is sent to the MS. The MS computes the 32-bit Signed Response (SRES) based on the encryption of the RAND with the authentication algorithm (A3) using the individual subscriber authentication key (Ki). Upon receiving the SRES from the subscriber, the GSM network repeats the calculation to verify the identity of the subscriber.

The individual subscriber authentication key (Ki) is never transmitted over the radio channel, as it is present in the subscriber's SIM, as well as the AUC, HLR, and VLR

databases. If the received SRES agrees with the calculated value, the MS has been

successfully authenticated and may continue. If the values do not match, the connection is terminated and an authentication failure is indicated to the MS.

The calculation of the signed response is processed within the SIM. It provides enhanced security, as confidential subscriber information such as the IMSI or the individual subscriber authentication key (Ki) is never released from the SIM duringthe authentication process.

SignallingandDataConfidentiality

The SIM contains the ciphering key generating algorithm (A8) that is used to producethe 64-bit ciphering key (Kc). This key is computed by applying the same random number (RAND) used in the authentication process to ciphering key generating algorithm (A8) with the individual subscriber authentication key (Ki).

GSM provides an additional level of security by having a way to change the cipheringkey, making the system more resistant to eavesdropping. The ciphering key may be changed at regular intervals as required. As in case of the authentication process, thecomputation of the ciphering key (Kc) takes place internally within the SIM. Therefore, sensitive information such as the individual subscriber authentication key(Ki) is never revealed by the SIM.

Encrypted voice and data communications between the MS and the network is accomplished by using the ciphering algorithm A5. Encrypted communication is initiated by a ciphering mode request command from the GSM network. Upon receipt of this command, the mobile station begins encryption and decryption of datausing the ciphering algorithm (A5) and the ciphering key (Kc).

Subscriber IdentityConfidentiality

To ensure subscriber identity confidentiality, the Temporary Mobile Subscriber Identity (TMSI) is used. Once the authentication and encryption procedures are done, the TMSI is sent to the mobile station. After the receipt, the mobile station responds. The TMSI is valid in the location area in which it was issued. For communications outside the location area, the Location Area Identification (LAI) is necessary in addition to the TMSI.

GSM Billing:

GSM service providers are doing billing based on the services they are providing to their customers. All the parameters are simple enough to charge a customer for the provided services.This chapter provides an overview of the frequently used billing techniques

and parametersapplied to charge a GSM subscriber.

Telephony Service

These services can be charged on per call basis. The call initiator has to pay the charges, and the incoming calls are nowadays free. A customer can be charged based on different parameters such as:

International call or long distance call. Local call.

Call made during peak hours. Call made during night time. Discounted call during weekends. Call per minute or per second.

Many more other criteria can be designed by a service provider to charge their customers.

Most of the service providers charge their customer's SMS services based on the number of text messages sent. There are other prime SMS services available where service providers charge more than normal SMS charge. These services are being availed in collaboration of Television Networks or Radio Networks to demand SMS from the audiences. Most of the time, the charges are paid by the SMS sender but for some services like stocks and share prices, mobile banking facilities, and leisure booking services, etc. the recipient of the SMS has to payfor the service.

Using GPRS service, you can browse, play games on the Internet, and download movies.So a service provider will charge you based on the data uploaded as well as data downloaded on your mobile phone. These charges will be based on per Kilo Byte data downloaded/uploaded

Additional parameter could be a QoS provided to you. If you want to watch a movie, then a low QoS may work because some data loss may be acceptable, but if you are downloading a zip file, then a single byte loss will corrupt your complete downloaded file. Another parameter could be peak and off peak time to download a data file or to browse the Internet.

Supplementary Services

Most of the supplementary services are being provided based on monthly rental or absolutely free. For example, call waiting, call forwarding, calling number identification, andcall on hold are available at zero cost.

Call barring is a service, which service providers use just to recover their dues, etc., otherwise this service is not being used by any subscriber.

Call conferencing service is a form of simple telephone call where the customers are charged for multiple calls made at a time. No service provider charges extra charge for this service.

Closed User Group (CUG) is very popular and is mainly being used to give special discounts to the users if they are making calls to a particular defined group of subscribers.

General Packet Radio System (GPRS):

General Packet Radio System is also known as GPRS is a third-generation step toward internet access. GPRS is also known as GSM-IP that is a Global-System Mobile Communications Internet Protocol as it keeps the users of this system online, allows to make voice calls, and access internet on-the-go. Even Time-Division Multiple Access (TDMA) usersbenefit from this system as it provides packet radio access.

GPRS also permits the network operators to execute an Internet Protocol (IP) based core architecture for integrated voice and data applications that will continue to be used and expanded for 3G services.

GPRS supersedes the wired connections, as this system has simplified access to the packet data networks like the internet. The packet radio principle is employed by GPRS to transport user data packets in a structure way between GSM mobile stations and external packet data networks. These packets can be directly routed to the packet switched networks from the GPRS mobile stations.

Key Features

Following three key features describe wireless packet data:

- **The always online feature - Removes the dial-up process, making applications only one click away.**
- **An upgrade to existing systems - Operators do not have to replace their equipment;rather, GPRS is added on top of the existing infrastructure.**
- **An integral part of future 3G systems - GPRS is the packet data core network for3G systems EDGE and WCDMA.**

Goals of GPRS

GPRS is the first step toward an end-to-end wireless infrastructure and has the following goals:

- **Open architecture**
- **Consistent IP services**
- **Same infrastructure for different air interfaces**
- **Integrated telephony and Internet infrastructure**
- **Leverage industry investment in IP**
- **Service innovation independent of infrastructure**

GPRS – Architecture:

GPRS architecture works on the same procedure like GSM network, but, has additional entities that allow packet data transmission. This data network overlaps a second-generation GSM network providing packet data transport at the rates from 9.6 to 171 kbps. Along with the packet data transport the GSM network accommodates multiple users to share the same air interface resources concurrently

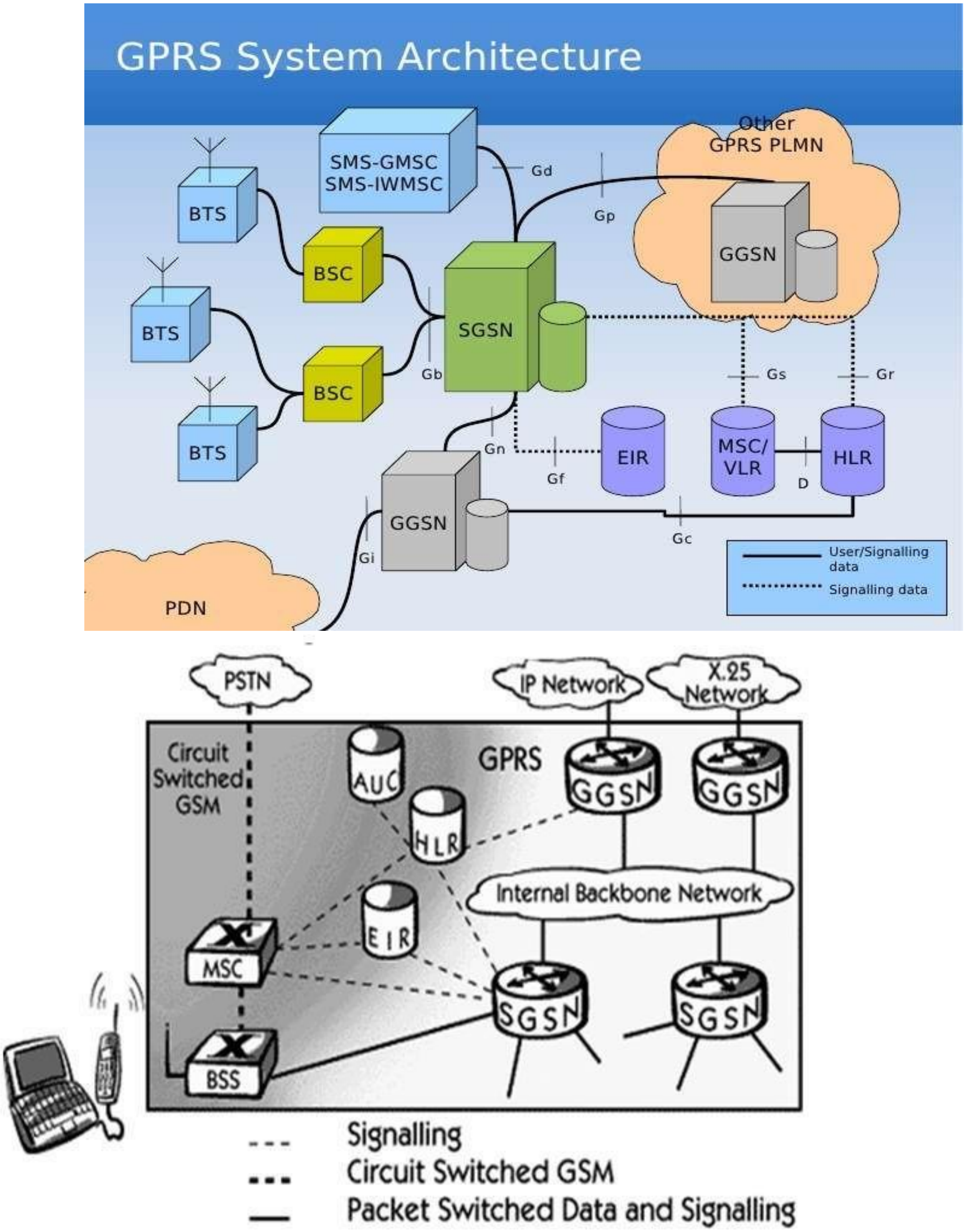


Figure 2.8 GPRS Architecture Block Diagram

GPRS Mobile Stations:

New Mobile Stations (MS) are required to use GPRS services because existing GSM phones

do not handle the enhanced air interface or packet dataas shown in Figure 2.8. A variety of MS can exist, including a high-speed version of current phones to support high-speed data access, a new PDA device with an embedded GSM phone, and PC cards for laptop computers. These mobile stations are backward compatible for making voice calls using GSM.

GPRS Base Station Subsystem:

Each BSC requires the installation of one or more Packet Control Units (PCUs) and a software upgrade. The PCU provides a physical and logical data interface to the Base Station Subsystem (BSS) for packet data traffic. The BTS can also require a software upgrade but typically does not require hardware enhancements.

When either voice or data traffic is originated at the subscriber mobile, it is transportedover the air interface to the BTS, and from the BTS to the BSC in the same way as a standard GSM call. However, at the output of the BSC, the traffic is separated; voice is sent to the MobileSwitching Center (MSC) per standard GSM, and data is sent to a new device called the SGSNvia the PCU over a Frame Relay interface.

GPRS Support Nodes:

Following two new components, called Gateway GPRS Support Nodes (GSNs)and,

Serving GPRS Support Node (SGSN) are added:

Gateway GPRS Support Node (GGSN)

The Gateway GPRS Support Node acts as an interface and a router to external networks. It contains routing information for GPRS mobiles, which is used to tunnel packets through the IP based internal backbone to the correct Serving GPRS Support Node. The GGSN also collects charging information connected to the use of the external data networks and can act as a packet filter for incoming traffic.

Serving GPRS Support Node (SGSN)

The Serving GPRS Support Node is responsible for authentication of GPRS mobiles, registration of mobiles in the network, mobility management, and collecting information on charging for the use of the air interface.

Internal Backbone:

The internal backbone is an IP based network used to carry packets between different GSNs. Tunnelling is used between SGSNs and GGSNs, so the internal backbone does not

needany information about domains outside the GPRS network. Signalling from a GSN to a MSC,HLR or EIR is done using SS7.

Routing Area:

GPRS introduces the concept of a Routing Area. This concept is similar to Location Area in GSM, except that it generally contains fewer cells. Because routing areas are smaller than location areas, less radio resources are used while broadcasting a page message.

GPRS Mobility Management:

The management of GPRS mobility in the network ensures the continuity of packet services when a given subscriber moves from one GPRS LA to another. This implies that the network must know the identifier of the GPRS LA indicating where the MS is located.

The GMM functions enable the network infrastructure to keep track of subscribers' locations within the PLMN or within another PLMN. The SGSN, which is the serving node of an MS, handles the mobility context management related to it. This context contains information such as the IMSI, the P_TMSI, the RAI, and the CI. This mobility context management is also stored at the MS side, in the SIM card. All GPRS mobility procedures require a TBF connection at the RLC/MAC layer between the MS and the PCU.

GPRS Procedure:

GPRS Attach Procedure:

When an MS needs to signal its presence to the network in order to access to GPRS services, it performs an IMSI attach procedure for GPRS services. During this procedure a MM context is created between the MS and the SGSN.

There are two types of GPRS attach procedures:

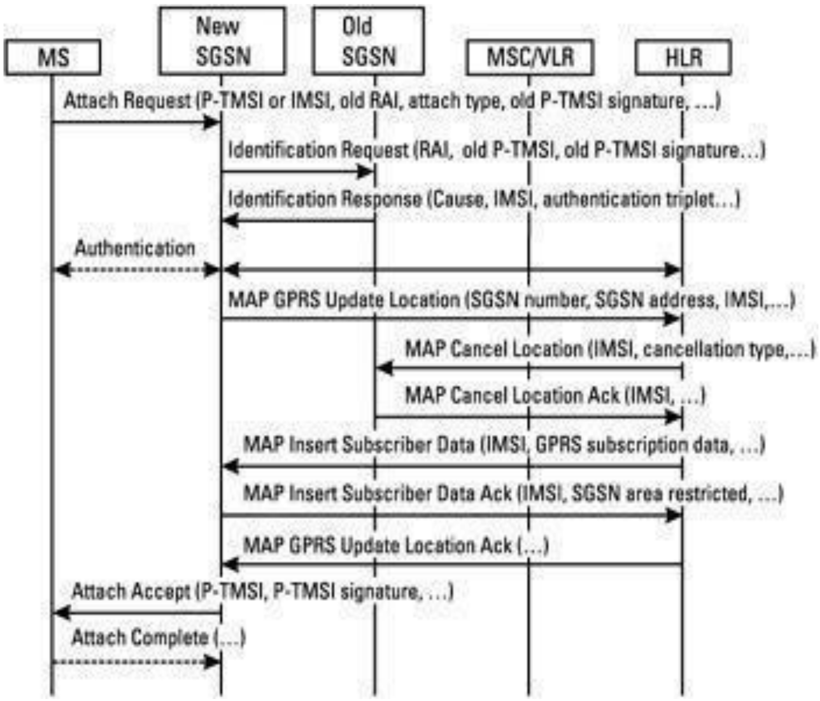
9. *Normal GPRS attach.* This procedure is used by the MS to be IMSI attached for GPRSservices only.

10. *Combined attach procedure.* This procedure is used by a class A or class B MS to be IMSIattached for GPRS and non-GPRS services in a cell that supports GPRS in network operation mode I.

Note that by default, the IMSI-attach procedure is referred to as the *attach procedure for circuit- switched services.* The IMSI-attach procedure for GPRS services is also called the *GPRS-attach procedure.*

Normal GPRS Attach

Figure 3.9 describes a GPRS-attach procedure. In this scenario, the MS signals itself to the network by sending it its old P-TMSI identifier associated with the old RAI identifier. When the SGSN receives this information, it analyzes the RAI identifier in order to determine the associated SGSN. If there is an SGSN change, the new SGSN must contact the old SGSN fromits RAI identifier in order to retrieve the MS identity. Authentication functions may be performed; they are mandatory if no MM context information related to the MS, such as IMSI,P-TMSI, CI, and RA exists anywhere in the network. Then the new SGSN informs the HLR of SGSN change, and location information in the HLR database is updated via the MAP protocol on SS7 signaling. If the HLR receives an indication from an SGSN different from the one stored in its table for a GPRS subscriber, it requests the old SGSN to remove GPRS data related to this subscriber, and then transmits this data to the new SGSN.


MS
New SGSN
Old SGSN
MSC/VLR
HLR
Attach Request (P-TMSI or IMSI, old RAI, attach type, old P-TMSI signature, ...)
Identification Request (RAI, old P-TMSI, old P-TMSI signature...)
Identification Response (Cause, IMSI, authentication triplet...)
Authentication
MAP GPRS Update Location (SGSN number, SGSN address, IMSI,...)
MAP Cancel Location (IMSI, cancellation type,...)
MAP Cancel Location Ack (IMSI, ...)
MAP Insert Subscriber Data (IMSI, GPRS subscription data, ...)
MAP Insert Subscriber Data Ack (IMSI, SGSN area restricted, ...)
MAP GPRS Update Location Ack (...)
Attach Accept (P-TMSI, P-TMSI signature, ...)
Attach Complete (...)

GPRS-attach procedure

GPRS DetachProcess:

When an MS does not need to access GPRS services anymore, an IMSI-detach procedure is

initiated, either by the MS or by the SGSN. During this procedure, the MM context between the MS and the SGSN is removed.

There are two types of GPRS-detach procedures:

11. ***Normal GPRS detach.* This procedure is used to IMSI detach only for GPRS services.**

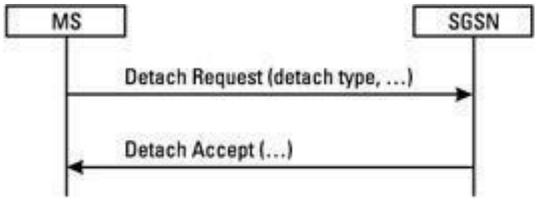
12. ***Combined detach procedure.* This procedure is used to IMSI detach a class A or B MS for GPRS or non-GPRS services in a cell that supports GPRS in network operation mode**

This procedure is initiated either by the MS or by the network MS-Initiated Detach Procedure

MS-Initiated Normal *GPRS Detach* When a GPRS MS wishes to be IMSI detached for GPRS services, it initiates a GPRS-detach procedure to the SGSN. The procedure is ended

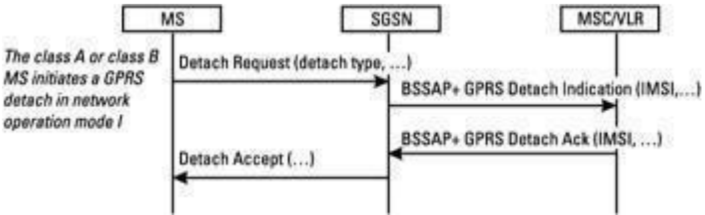
upon the receipt of the DETACH *MS-Initiated Normal GPRS Detach* When a GPRS MS wishesto be IMSI detached for GPRS services, it initiates a GPRS-detach procedure to the SGSN. The

procedure is ended upon the receipt of the DETACH ACCEPT message by the MS



Normal GPRS detach initiated by MS.

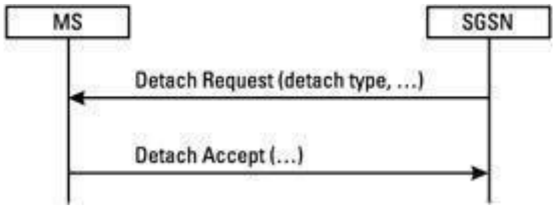
MS-Initiated Combined GPRS Detach :When an MS both IMSI and GPRS attached wishes to perform a GPRS detach in a cell that supports GPRS in network operation mode I, it initiates a combined detach procedure to the SGSN. The latter sends an explicit request to the MSC/VLR to deactivate the association between SGSN and MSC/VLR in order that circuit- switched incoming calls are no longer routed to SGSN. Figure 3.11 illustrates this scenario. Thesame scenario is used for an MS both IMSI and GPRS attached wishing to be IMSI detached or both IMSI and GPRS detached in network operation mode I.


MS
SGSN
MSC/VLR
The class A or class B MS initiates a GPRS detach in network operation mode I
Detach Request (detach type, ...)
BSSAP+ GPRS Detach Indication (IMSI,...)
BSSAP+ GPRS Detach Ack (IMSI, ...)
Detach Accept (...)

Combined GPRS detach initiated by an MS in network operation mode I.

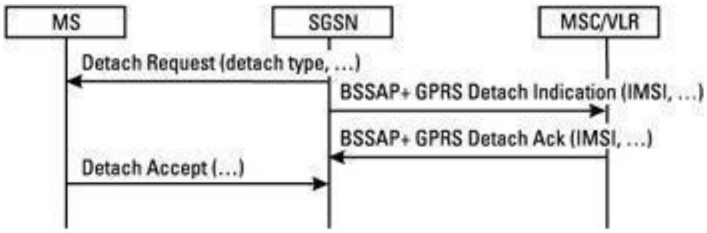
Network-Initiated Detach Procedure

Network-Initiated Normal GPRS Detach **When an SGSN wishes to IMSI detach a given MS forGPRS services, it initiates a GPRS-detach procedure. The procedure is ended upon the receiptof DETACH ACCEPT message by the SGSN, as illustrated in Figure . The network may request the MS to perform a reattach in the case of a network failure condition.**



Normal GPRS detach initiated by an SGSN.

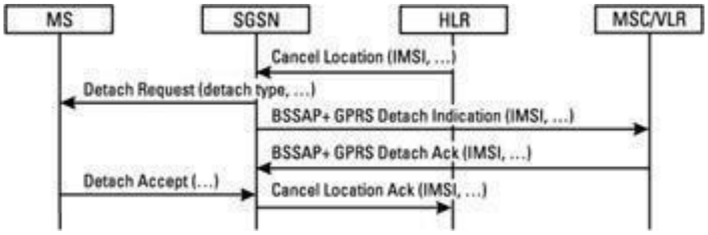
Network-Initiated Combined GPRS Detach When an SGSN wishes to IMSI detach a class A or B MS for GPRS or non-GPRS services, it notifies the relevant MS of a GPRS detach. It alsosends an explicit request to MSC/VLR to deactivate the association between SGSN and MSC/VLR. Circuit-switched incoming calls are no longer routed to SGSN. Figure 3.13 illustrates this scenario.


MS
SGSN
MSC/VLR
Detach Request (detach type, ...)
BSSAP+ GPRS Detach Indication (IMSI, ...)
BSSAP+ GPRS Detach Ack (IMSI, ...)
Detach Accept (...)

GPRS detach initiated by SGSN in network operation mode I.

An HLR may initiate a GPRS detach for operator purposes in order to remove the subscriber's MM and PDP contexts at the SGSN. The HLR sends a CANCEL LOCATION message in order to delete the subscriber's MM and PDP contexts from the SGSN. This

latter then notifies the relevant MS of a GPRS detach. If the MS is both IMSI and GPRS attached, the SGSN sends an explicit request to the MSC/VLR to deactivate the association between theSGSN and the MSC/VLR. Figure illustrates this scenario.


MS
SGSN
HLR
MSC/VLR
Cancel Location (IMSI, ...)
Detach Request (detach type, ...)
BSSAP+ GPRS Detach Indication (IMSI, ...)
BSSAP+ GPRS Detach Ack (IMSI, ...)
Detach Accept (...)
Cancel Location Ack (IMSI, ...)

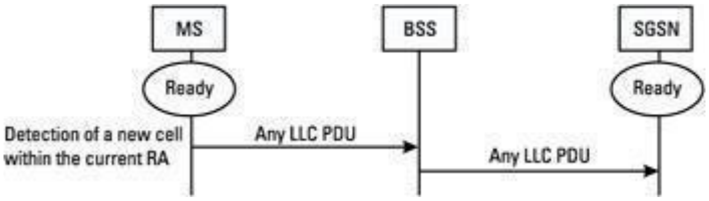
Combined GPRS detach initiated by HLR.

Location Procedures

A location procedure is always initiated by the MS. Under normal circumstances, a location change occurs when the MS decides to camp on a new cell for better radio conditions. If an MSin GMM READY state camps in a new cell within its current RA, it needs to perform a cell update procedure in order to receive directly downlink PDUs from the network without being paged. If the MS camps in a new cell belonging to a new RA, it needs to perform an RA updateprocedure in order to update MM context information between the MS and the SGSN.

Cell Update

When a GPRS MS in GMM READY state detects a new cell within its current RA, it performs a cell update procedure by sending any LLC frame containing its identity. Figure 3.15illustrates the cell update notification.



Cell update.

RA Update Procedure

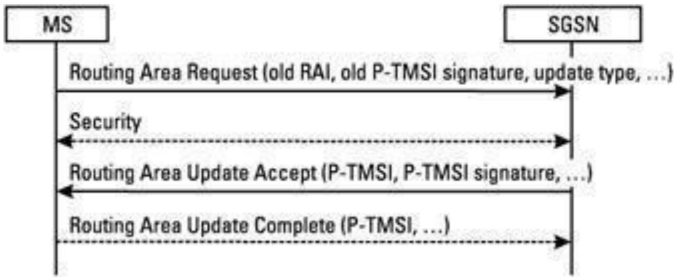
An RA update procedure is performed when a GPRS MS has detected a new RA. Thisprocedure is always initiated by the MS. There are four types of RA update procedures:

1. *Normal RA update*, performed by a class C MS or by a class A or B MS in a cell thatsupports GPRS in network operation mode II or III upon detection of a new RA;
2. *Periodic RA*, performed by any GPRS MS upon expiry of a timer;
3. *Combined RA and LA update*, performed by a class A or B MS in a cell that supportsGPRS in network operation mode I upon detection of a new LA;
4. *Combined RA and IMSI attach*, performed by a class A or B MS in a cell that supports GPRS in network operation mode 1 in order to be IMSI attached for non-GPRS serviceswhen the MS is already IMSI attached for GPRS services.

Normal RA Update

Intra-SGSN HA Update During an RA update procedure, the MS signals itself to the SGSN by sending its old P-TMSI signature associated with the RAI identifier from its old RA.The SGSN has the necessary information about the MS if the SGSN also handles the old RA.

In the case of an intra-SGSN change, the SGSN validates the presence of the MS in thenew RA by returning to it a ROUTING AREA UPDATE ACCEPT message. If the SGSN allocates a new P-TMSI identifier, it is acknowledged by the MS. This procedure is called intra-SGSN RA update since the SGSN does not need to contact an old SGSN, GGSN, and HLR. Figure 3.16 illustrates an intra-SGSN RA update procedure.


MS
SGSN
Routing Area Request (old RAI, old P-TMSI signature, update type, …)
Security
Routing Area Update Accept (P-TMSI, P-TMSI signature, …)
Routing Area Update Complete (P-TMSI, …)

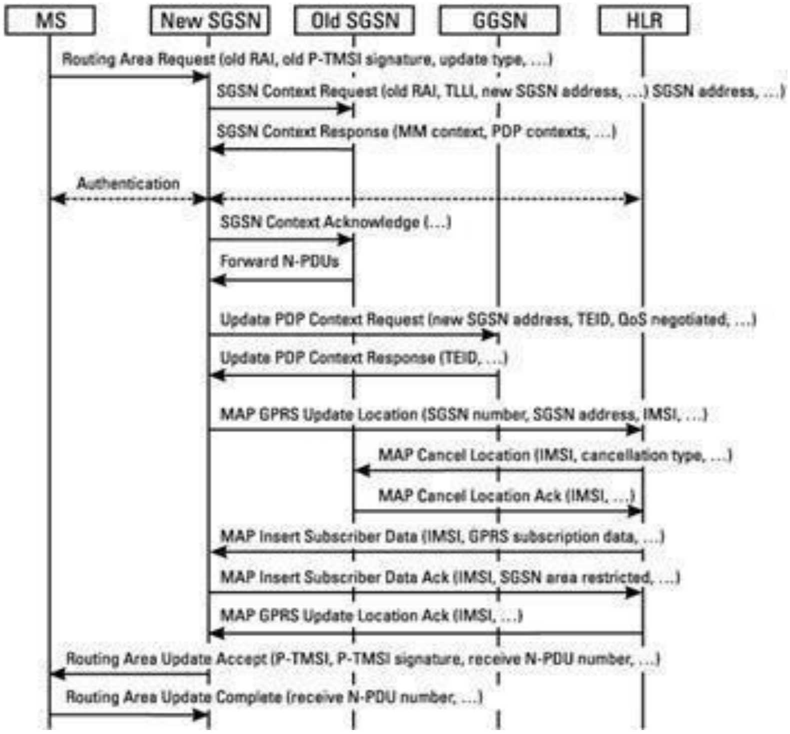
Intra-SGSN RA update.

Note that a periodic RA update is always an intra-SGSN RA update procedure.

Inter-SGSN RA Update When the SGSN detects that the old RA sent by the MS is handled by another SGSN, the SGSN has no information about this MS. In this case, the SGSNneeds to contact the old SGSN, the GGSN, and the HLR in order to retrieve information and update the routing information. This procedure is called an inter-SGSN RA update procedure. Thus the new SGSN is able to contact the old SGSN from the RAI identifier in order to retrieve MM and PDP context information related to the MS identified in the old SGSN by its old P- TMSI. If the old signature does not match the one saved in the old SGSN, the new SGSN performs an MS authentication procedure. If the old SGSN has saved in its buffer some packets addressed to the MS, it forwards the packets toward the new SGSN.

When the new SGSN has retrieved MM and PDP context information, it updates the data related to the new SGSN in the GGSN. The new SGSN then updates location information

in the HLR database via the MAP protocol using the SS7 network. If the HLR receives an indicationfrom an SGSN different from the one saved in its table for a GPRS subscriber, it requests the old SGSN to remove GPRS data related to this subscriber. It then transmits this data to the new SGSN. As shown in Figure. when the new SGSN receives an RA update confirmationin the HLR database, it transmits the RA update confirmation to the MS with its new P-TMSI identifier and the receive N-PDU number. This message contains the acknowledgment of N- PDUs successfully transferred by the MS before the start of the update procedure. The RA update procedure ends as soon as the MS acknowledges its new P-TMSI identifier.


MS
New SGSN
Old SGSN
GGSN
HLR
Routing Area Request (old RAI, old P-TMSI signature, update type, ...)
SGSN Context Request (old RAI, TLLI, new SGSN address, ...) SGSN address, ...)
SGSN Context Response (MM context, PDP contexts, ...)
Authentication
SGSN Context Acknowledge (...)
Forward N-PDUs
Update PDP Context Request (new SGSN address, TEID, QoS negotiated, ...)
Update PDP Context Response (TEID, ...)
MAP GPRS Update Location (SGSN number, SGSN address, IMSI, ...)
MAP Cancel Location (IMSI, cancellation type, ...)
MAP Cancel Location Ack (IMSI, ...)
MAP Insert Subscriber Data (IMSI, GPRS subscription data, ...)
MAP Insert Subscriber Data Ack (IMSI, SGSN area restricted, ...)
MAP GPRS Update Location Ack (IMSI, ...)
Routing Area Update Accept (P-TMSI, P-TMSI signature, receive N-PDU number, ...)
Routing Area Update Complete (receive N-PDU number, ...)

Inter-SGSN RA update.

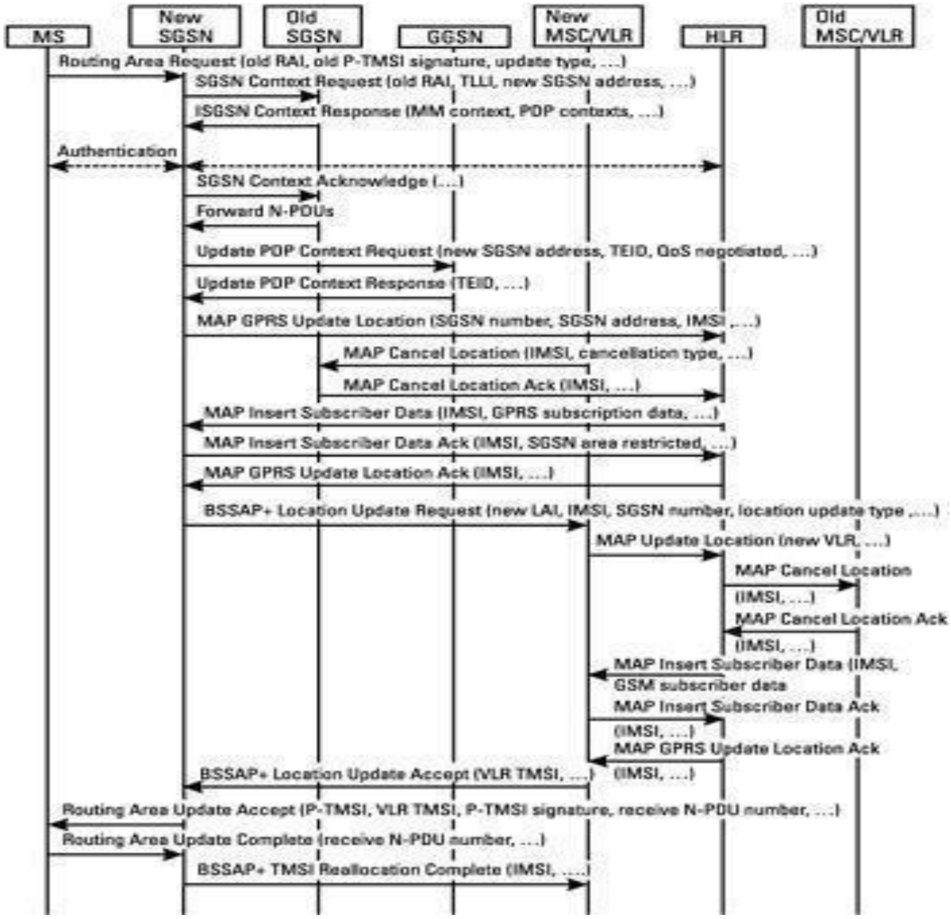
Combined RA and LA Update:

During a combined RA and LA update procedure in a cell that supports GPRS in network operation mode I, the new SGSN (in case of SGSN change) retrieves MM and PDP context information related to the MS from the old SGSN. The new SGSN sends its address to the GGSN, updates routing information in the HLR via the MAP protocol, and retrieves data related to the GPRS subscriber from the HLR. The new SGSN transmits an LA update requestvia the Gs interface.

If the LA change involves a new MSC/VLR entity, the new MSC/VLR updates the location information in the HLR via the MAP protocol. When the HLR receives a notificationfrom an MSC/VLR different from the one saved in its table, it requests the old MSC/VLR to remove data related to the GPRS subscriber and then transmits this data to the new MSC/VLR data. When the new SGSN receives the LA update confirmation from the new MSC/VLR withthe allocation of a new TMSI identifier value, it transmits the confirmation of the combined RA and LA update message toward the MS.

The new SGSN allocates a new P-TMSI identifier for packet services and also returns the receive N-PDU number, containing the acknowledgment of N- PDUs successfully transferred by the MS before the start of the combined procedure. The combined RA and LA update procedure ends as soon as the MS acknowledges its new TMSI and P-TMSI identifiers. Figure 3.18 illustrates the combined RA and LA update procedure. Note that the combined RA and IMSI attach scenario generates the same message exchange between the MS, SGSN, GGSN,

MSC/VLR, and HLR entities as the combined RA and LA update scenario.


MS
New SGSN
Old SGSN
GGSN
New MSC/VLR
HLR
Old MSC/VLR
Routing Area Request (old RAI, old P-TMSI signature, update type, ...)
SGSN Context Request (old RAI, TLLI, new SGSN address, ...)
ISGSN Context Response (MM context, PDP contexts, ...)
Authentication
SGSN Context Acknowledge (....)
Forward N-PDUs
Update PDP Context Request (new SGSN address, TEID, QoS negotiated, ...)
Update PDP Context Response (TEID, ...)
MAP GPRS Update Location (SGSN number, SGSN address, IMSI ,....)
MAP Cancel Location (IMSI, cancellation type, ...)
MAP Cancel Location Ack (IMSI, ...)
MAP Insert Subscriber Data (IMSI, GPRS subscription data, ...)
MAP Insert Subscriber Data Ack (IMSI, SGSN area restricted, ...)
MAP GPRS Update Location Ack (IMSI, ...)
BSSAP+ Location Update Request (new LAI, IMSI, SGSN number, location update type ,....)
MAP Update Location (new VLR, ...)
MAP Cancel Location
(IMSI, ...)
MAP Cancel Location Ack
(IMSI, ...)
MAP Insert Subscriber Data (IMSI,
GSM subscriber data
MAP Insert Subscriber Data Ack
(IMSI, ...)
MAP GPRS Update Location Ack
(IMSI, ...)
BSSAP+ Location Update Accept (VLR TMSI, ...)
Routing Area Update Accept (P-TMSI, VLR TMSI, P-TMSI signature, receive N-PDU number, ...)
Routing Area Update Complete (receive N-PDU number, ...)
BSSAP+ TMSI Reallocation Complete (IMSI, ...)

Combined RA and LA update procedure.

.

PDP Context Procedure:

PDP stands for Packet Data Protocol as shown in fig. The PDP addresses are network layer addresses (Open Standards Interconnect [OSI] model Layer 3). GPRS systems support both X2.5 and IP network layer protocols. Therefore, PDP addresses can be X.25, IP, or both. Each PDP address is anchored at a Gateway GPRS Support Node (GGSN), as shown in figure2.9 below. All packet data traffic sent from the public packet data network for the PDP address goes through the gateway (GGSN).

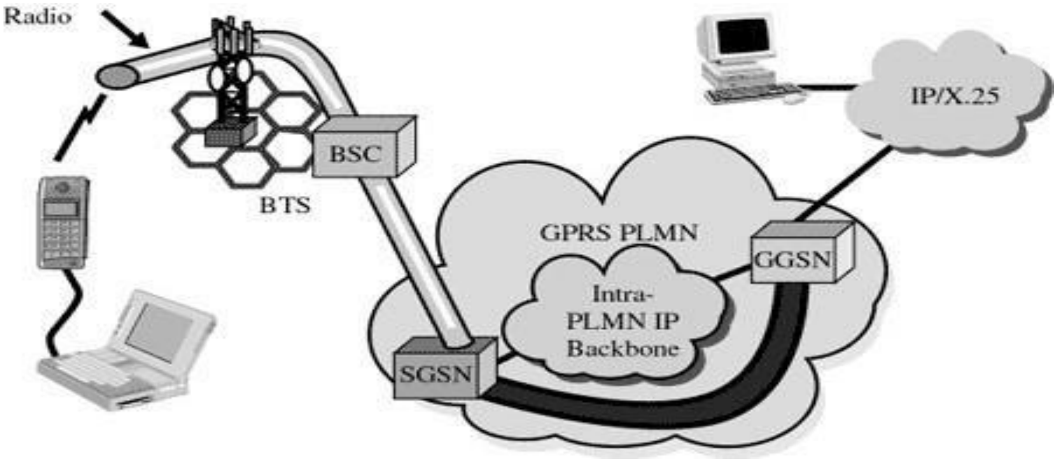


Figure 2.9 Packet Data Protocol

The public packet data network is only concerned that the address belongs to a specific GGSN. The GGSN hides the mobility of the station from the rest of the packet data network and from computers connected to the public packet data network. Statically assigned PDP addresses are usually anchored at a GGSN in thesubscriber's home network. Conversely, dynamically assigned PDP addresses can be anchored either in the subscriber's home network or the network that the user is visiting. When a MS is already attached to a SGSN and it is about to transfer data, it must activate a PDP address. Activating a PDP address establishes an association between the current SGSN of mobile device and the GGSN that anchorsthe PDP address.

The record kept by the SGSN and the GGSN regarding this association is called the PDP context. It is important to understand the difference between a MS attaching to a SGSN and a MS activating a PDP address. A single MS attaches to only one SGSN, however, it may have multiple PDP addresses that are all active at the sametime. Each of the addresses may be anchored to a different GGSN. If packets arrivefrom the public packet data network at a GGSN for a specific PDP address and the GGSN does not have an active PDP context corresponding to that address, it may simply discard the packets. Conversely, the GGSN may attempt to activate a PDP context with a MS if the address is statically assigned to a particular mobile device.

GPRS Billing:

As packet data is introduced into mobile systems, the question of how to bill for the services arises. Always online and paying by the minute does not sound all that appealing. Here, we

describe the possibilities but it totally depends on different service providers, how they want to charge their customers.

The SGSN and GGSN register all possible aspects of a GPRS user's behavior andgenerate billing information accordingly. This information is gathered in so-called Charging Data Records (CDR) and is delivered to a billing gateway.

The GPRS service charging can be based on the following parameters:

- **Volume - The amount of bytes transferred, i.e., downloaded and uploaded.**
- **Duration - The duration of a PDP context session.**
- **Time - Date, time of day, and day of the week (enabling lower tariffs at offpeak hours).**
- **Final destination - A subscriber could be charged for access to thespecific network, such as through a proxy server.**
- **Location - The current location of the subscriber.**
- **Quality of Service - Pay more for higher network priority.**
- **SMS - The SGSN will produce specific CDRs for SMS.**
- **Served IMSI/subscriber - Different subscriber classes (differenttariffs for frequent users, businesses, or private users).**
- **Reverse charging - The receiving subscriber is not charged for thereceived data; instead, the sending party is charged.**
- **Free of charge - Specified data to be free of charge.**
- **Flat rate - A fixed monthly fee.**
- **Bearer service - Charging based on different bearer services (for an operator who has several networks, such as GSM900 and GSM1800, and who wants to promote usage of one of the networks). Or, perhapsthe bearer service would be good for areas where it would be cheaperfor the operator to offer services from a wireless LAN rather than from the GSM network.**

SMS

- **Definition: Short message service (SMS) is a globally accepted wireless service that enables the transmission of alphanumeric messages between mobile**

subscribers and external systems such as electronic mail, paging, and voice-mail systems.

- **SMS appeared on the wireless scene in 1991 in Europe. The European standard for digital wireless, now known as the Global System for Mobile Communications (GSM), included short messaging services from the outset.**

○ **In North America, SMS was made available initially on digital wireless networks built by early pioneers such as BellSouth Mobility, PrimeCo, and Nextel, among others. These digital wireless networks are based on GSM, code division multiple access (CDMA), and time division multiple access (TDMA) standards**

WORKING OF SMS

- **Messages in Short Message Service (SMS) must be no longer than 160 alpha-numeric characters and contain no images or graphics.**
- **Once a message is sent, it is received by a Short Message Service Center (SMSC), which must then get it to the appropriate mobile device.**
- **To do this, the SMSC sends a SMS Request to the home location register (HLR) to find the roaming customer. Once the HLR receives the request, it will respond to the SMSC with the subscriber's status: 1) inactive or active 2) where subscriber is roaming.**
- **If the response is "inactive", then the SMSC will hold onto the message for a period of time. When the subscriber accesses his device, the HLR sends a SMS Notification to the SMSC, and the SMSC will attempt delivery.**
- **The SMSC transfers the message in a Short Message Delivery Point to Point format to the serving system. The system pages the device, and if it responds, the message gets delivered.**
- **The SMSC receives verification that the message was received by the end user,**

○ **then categorizes the message as "sent" and will not attempt to send again.**

- **The number of mobile-phone users expects to reach 500 million worldwide by**

2003, and with the help of SMS, 75 percent of all cellular phones will be Internet- enabled.

○ **BENEFITS OF SMS**

- **At a minimum, SMS benefits include the following:**
- **Delivery of notifications and alerts**
- **Guaranteed message delivery**
- **Reliable, low-cost communication mechanism for concise information Ability to screen messages and return calls in a selective way Increased subscriber productivity**
- **More sophisticated functionality provides the following enhanced subscriber benefits:**
- **Delivery of messages to multiple subscribers at a time**
- **Ability to receive diverse information**
- **E-mail generation**
- **Creation of user groups**
- **Integration with other data and Internet-based applications**
- **The benefits of SMS to the service provider are as follows:**
- **Ability to increment average revenue per user (due to increased number of calls on wireless and wireline networks by leveraging the notification capabilities of SMS)**
- **An alternative to alphanumeric paging services, which may replace or complement an existing paging offer**
- **Ability to enable wireless data access for corporate users**
- **New revenue streams resulting from addition of value-added services such as e-mail, voice mail, fax, and Web-based application integration, reminder service, stock and currency quotes, and airline schedules**
- **Provision of key administrative services such as advice of charge, over- the-**

air downloading, and over-the-air service provisioning

- **Protection of important network resources (such as voice channels), due to SMS' sparing use of the control and traffic channels**

- **Notification mechanisms for newer services such as those utilizing wireless application protocol (WAP)**

SMS ARCHITECTURE

GSM SMS

- **Can contain up to 140 octets, or 160 char.**
- **To allow messages longer than 160 char.**
  - **SMS concatenation**
  - **SMS compression**
- **SDCCH signaling channel**
- **Two type of GSM SMS**
  - **Cell broadcast service**
  - **Point-to-point service**

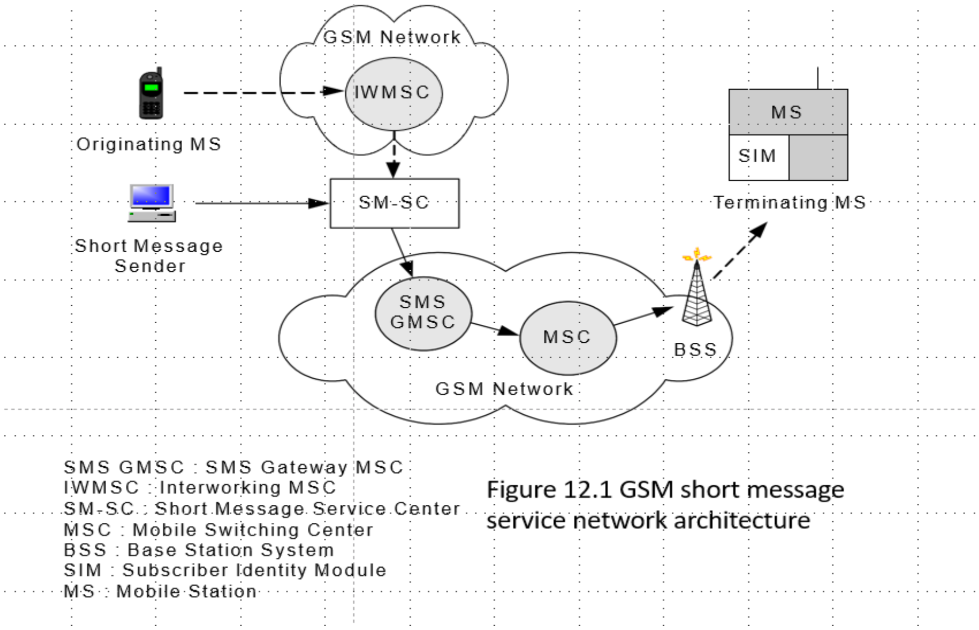
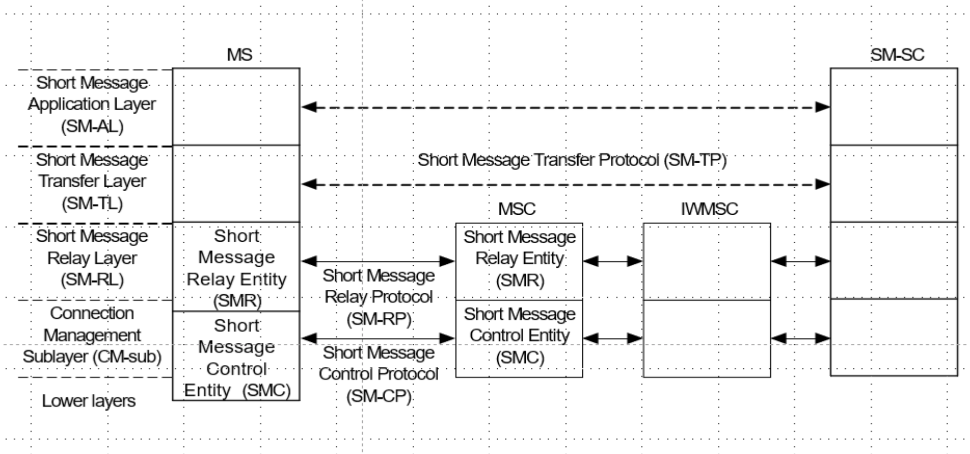

GSM Network
IWMSC
Originating MS
SM-SC
Short Message Sender
MS
SIM
Terminating MS
SMS GMSC
MSC
BSS
GSM Network
SMS GMSC : SMS Gateway MSC
IWMSC : Interworking MSC
SM-SC : Short Message Service Center
MSC : Mobile Switching Center
BSS : Base Station System
SIM : Subscriber Identity Module
MS : Mobile Station

Figure 12.1 GSM short message service network architecture

Figure 2.10 SMS

The Short Message Service (SMS) as shown in Figure 2.10 allows the exchange of short messages between a mobile station and the wireless system, and between the wireless system and an external device capable of transmitting and optionally receiving short messages. The external device may be a voice telephone, a data terminal or a short message entry system. The Short Message Service consists of message entry features, administration features, and message transmission capabilities. These features are distributed between a wireless system and the SMS message center (MC) that together make up the SMS system. The message center may be either separate from or physically integrated into the wireless system. Short message entry features are provided through interfaces to the message center and the mobile station. Senders use these interfaces to enter short messages, intended destination addresses, and various delivery options. The protocols associated with SMS have evolved since the first commercial text message was sent in 1992. Today the 3rd Generation Partnership Project (3GPP) maintains the SMS standard. In addition to officially recognizing SMS as a communication protocol, they also recognize five main short message service center (SMSC, SC or SMS-C) access protocols, though only four are primarily used. These mainstream protocols, which include SMPP, CIMD, UCP/EMI, and OIS, are proprietary binary access protocols associated with SMS that communicate over TCP/IP or X.25. The technical realization specification as outlined by the 3GPP details in great length the service elements, service and message center functionality, routing, architecture, and protocols used within the SMS standard for GSM systems. The 3GPP also produces other specification documents for things like requirements, security, data, and program management, all relating to SMS. It is important to note that this main specification document focuses on the communication between mobile stations (MS or mobile user) and SCs. SMS communication can really extend beyond just the SC to entities like the aggregator or broker (and with other protocols like CDMA).In principle any number of relay points could be included, each containing an SMS protocol stack similar to that shown for the base station. For example, during a call that has undergone an intersystem handoff, SMS messages arriving at the mobile station's anchor base station must be forwarded to the current serving base station for delivery. The SMS bearer service is the portion of the SMS system responsible for delivery of messages between the message center and mobile user

equipment. The bearer service is provided by the SMS Transport Layer and the SMS Relay Layer. The SMS Transport Layer is the highest layer of the bearer service protocol. The Transport Layer manages the end-to-end delivery of messages. In an entity serving as a relay point, the Transport Layer is responsible for receiving SMS Transport Layer messages from an underlying SMS Relay Layer, interpreting the destination address and other routing information, and forwarding the message via an underlying SMS Relay Layer. In entities serving as end points, the Transport Layer provides the interface between the SMS Bearer Service and the SMS Teleservice. The SMS Relay Layer provides the interface between the Transport Layer and the Link Layer used for message transmission.


MS
SM-SC
Short Message Application Layer (SM-AL)
Short Message Transfer Protocol (SM-TP)
Short Message Transfer Layer (SM-TL)
MSC
IWMSC
Short Message Relay Layer (SM-RL)
Short Message Relay Entity (SMR)
Short Message Relay Protocol (SM-RP)
Short Message Relay Entity (SMR)
Connection Management Sublayer (CM-sub)
Short Message Control Entity (SMC)
Short Message Control Protocol (SM-CP)
Short Message Control Entity (SMC)
Lower layers

SMS MS-MSC protocol hierarchy (mobile origination)

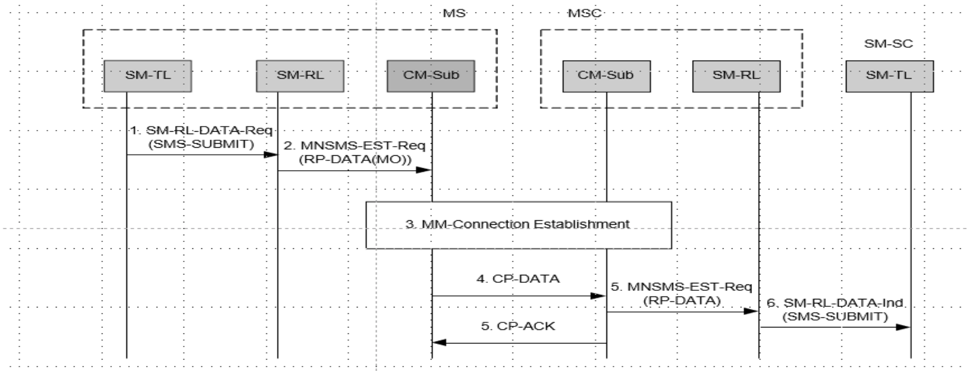
- **Short Message Transfer Layer**
- **Provides services to transfer SM-AL short msg.**
- **Generate a reference number SMI (short message identifier)**
    - **SM-AL SMI is not carried between the MS and SM-SC**
- **Four types of transfer protocol data units (TPDUs)**
    - **SMS-SUBMIT**
    - **SMS-DELIVER**
    - **SMS-STATUS-REPORT**
    - **SMS-COMMAND**
- **Short Message Relay Layer**
- **Provides services to transfer TPDUs and delivery reports for SM-TL**
- **Generate SM-RL SMI for every short message**
- **SM-RL SMI is mapped to and from SM-TL SMI**

- **SM-RL SMI at the MS is not carried at the peer entity in the SM-SC**
- **SM-RP consists of the following RPDU types:**
- **RP-DATA**
- **RP-SM-MEMORY-AVAILABLE**
- **RP-ACK**
- **RP-ERROR**

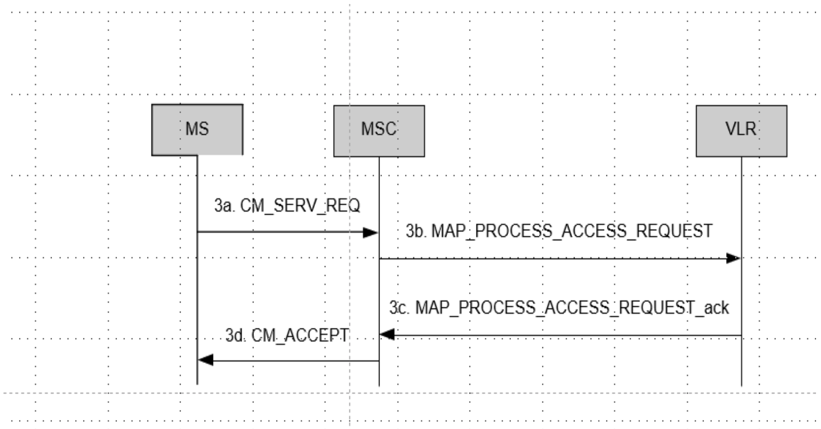
- **Connection Management Sublayer**
- **Provides services to support the SM-RL**
- **MS has two SMC entities**
- **MS-originated (MO) short message service**
- **MS-terminated (MT) short message service**
- **SM-CP consists of following protocol elements**
- **CP-DATA**
- **CP-ACK**
- **CP-ERROR**
- **MNSMS-ESTablish**
- **To establish an MM-connection and transfer RPDU on that establish**
- **MNSMS-DATA**
- **Transfer an RPDU on MM-connection**
- **MNSMS-RELease**
- **MNSMS-ABORT**
- **MNSMS-ERROR**

Mobile-Originated Messaging

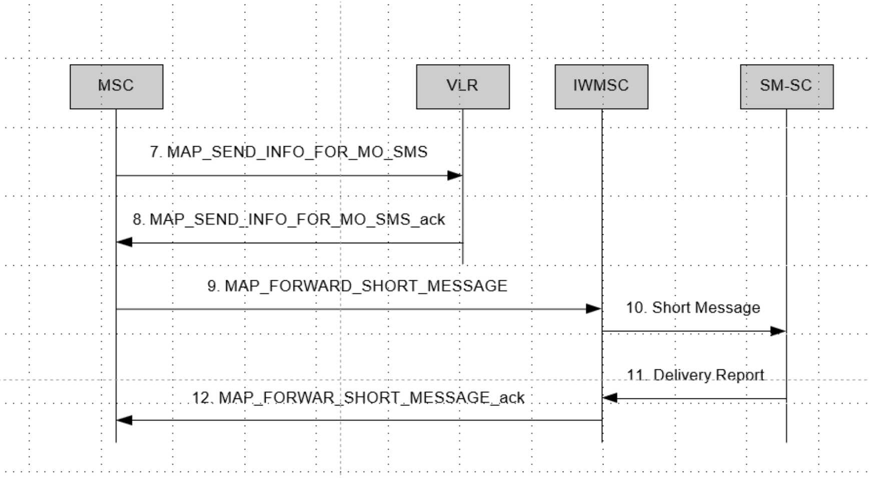
- The logical message path is :
    - MS -> originating MSC -> IWMSC -> SM-SC



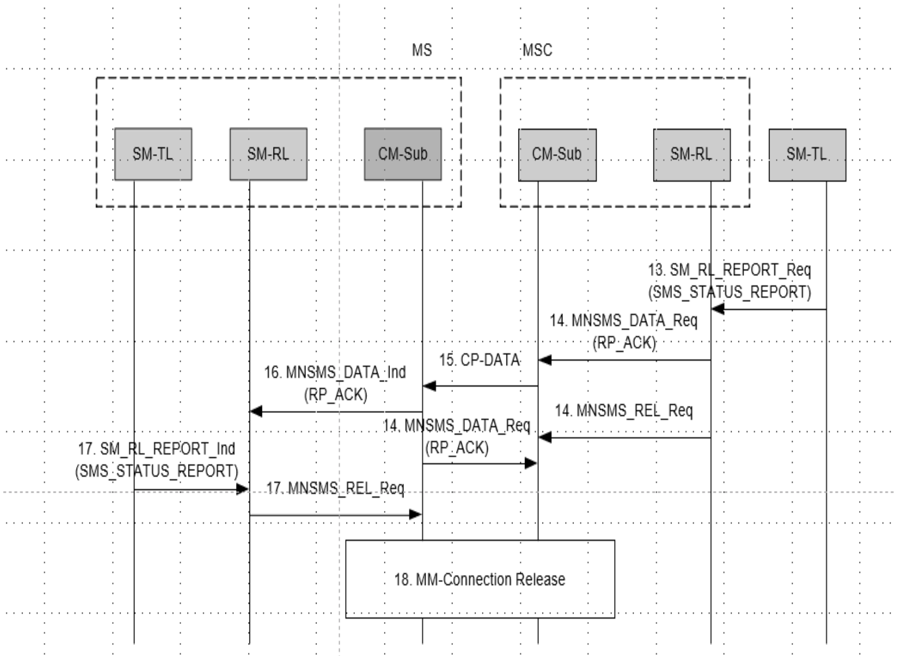
Mobile-originated short messaging (part 1)


MS
MSC
VLR
3a. CM_SERV_REQ
3b. MAP_PROCESS_ACCESS_REQUEST
3c. MAP_PROCESS_ACCESS_REQUEST_ack
3d. CM_ACCEPT

MM-connection establish for mobile-originated short messaging


MSC
VLR
IWMSC
SM-SC
7. MAP_SEND_INFO_FOR_MO_SMS
8. MAP_SEND_INFO_FOR_MO_SMS_ack
9. MAP_FORWARD_SHORT_MESSAGE
10. Short Message
11. Delivery Report
12. MAP_FORWAR_SHORT_MESSAGE_ack

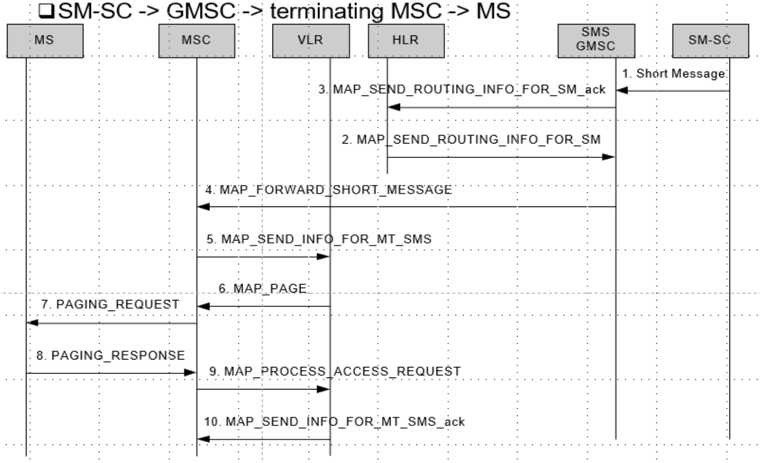
Mobile-originated short messaging (part 2)



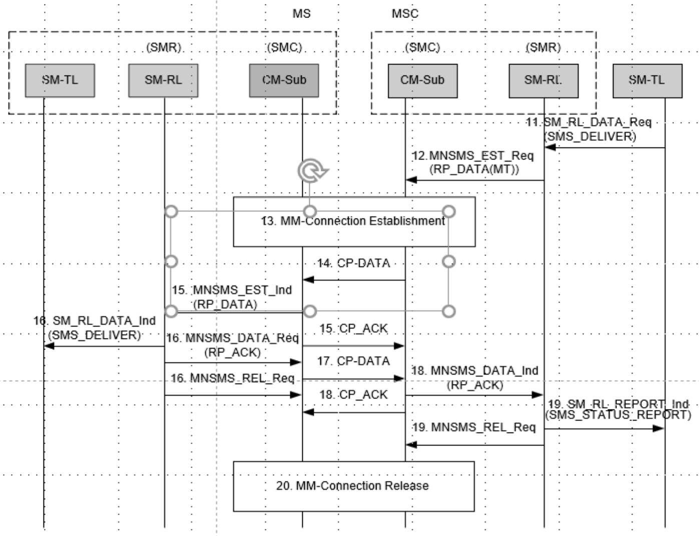
Mobile-originated short messaging (part 3)

MOBILE TERMINATED MESSAGING

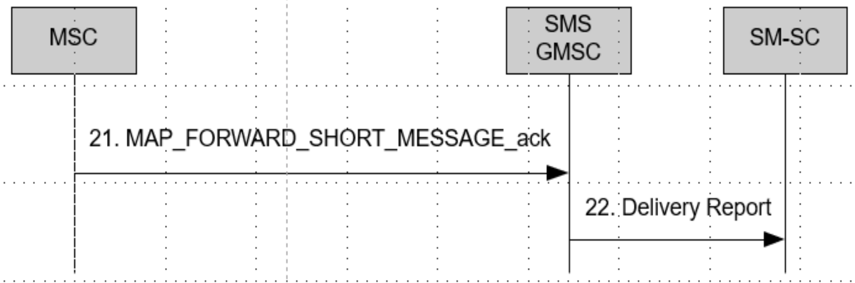
- ❑The logical massage path is :
  - ❑SM-SC -> GMSC -> terminating MSC -> MS


MS
MSC
VLR
HLR
SMS GMSC
SM-SC
1. Short Message
3. MAP_SEND_ROUTING_INFO_FOR_SM_ack
2. MAP_SEND_ROUTING_INFO_FOR_SM
4. MAP_FORWARD_SHORT_MESSAGE
5. MAP_SEND_INFO_FOR_MT_SMS
6. MAP_PAGE
7. PAGING_REQUEST
8. PAGING_RESPONSE
9. MAP_PROCESS_ACCESS_REQUEST
10. MAP_SEND_INFO_FOR_MT_SMS_ack

Mobile-terminated short messaging (part 1)


MS
MSC
(SMR)
(SMC)
(SMC)
(SMR)
SM-TL
SM-RL
CM-Sub
CM-Sub
SM-RL
SM-TL
11. SM_RL_DATA_Req (SMS_DELIVER)
12. MNSMS_EST_Req (RP_DATA(MT))
13. MM-Connection Establishment
14. CP-DATA
15. MNSMS_EST_Ind (RP_DATA)
16. SM_RL_DATA_Ind (SMS_DELIVER)
15. CP_ACK
16. MNSMS_DATA_Req (RP_ACK)
17. CP-DATA
16. MNSMS_REL_Req
18. MNSMS_DATA_Ind (RP_ACK)
18. CP_ACK
19. SM_RL_REPORT_Ind (SMS_STATUS_REPORT)
19. MNSMS_REL_Req
20. MM-Connection Release

Mobile-terminated short messaging (part2)



Mobile-terminated short messaging (part 3)

Question bank

PART A

1 Evolution of GSM.

2 List the GSM channels

3 Define location tracking

4 Explain call setup in GSM

5 How location update is done by GSM

6 Compare GSM and GPRS

7 Sketch the GPRS architecture

8 List the types of handover in GSM

9 What are the various services of GSM

10 Define SMS

11 What is GPRS

12 Define HLR and VLR

13 IMEI helps to find the mobile, Justify.

14 List the benefits of SMS

15 Distinguish SGSN and GGSN

PART B

1 Discuss in detail about GSM architecture

2 Compare and contrast GSM and GPRS

3 Explain the GPRS architecture

4 Discuss the handoff in GSM.

5 Explain the GSM channels

6 Discuss the SMS architecture in details

TEXT / REFERENCE BOOKS

1. Andreas F. Molisch, “Wireless Communications”, 2n d Edition, John Wiley & Sons Ltd, 2011.

2. William C.Y. Lee., "Wireless & Cellular Telecommunications", 3rd edition, McGraw Hill.2006.

3. Yibing Lin, "Wireless & mobile Network architecture", Wiley 2002.

4. Tao Jiang, Lingyang Song and Van Zhang, “Orthogonal Frequency Division Multiple Access Fundamentals and Applications” Taylor and Francis Group, 2010.

5. Yong Soo Cho, Jaekwon Kim, Won Young Yang and Chung G. Kang, “MIMO-OFDM Wireless Communications with MATLAB”, John Wiley & Sons (Asia) Pvt. Ltd, 2010.

SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE
www.sathyabama.ac.in

SCHOOL OF ELECTRICAL AND ELECTRONICS

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

UNIT – III – Wireless Communication –SEC1404

UNIT 3- WAP AND CABLE REPLACEMENT DEVICES

Wireless Application Protocol (WAP) - WAP model - WAP Gateway - WAP Protocols-Wireless Datagram protocol (WDP) - Wireless Transport layer security (WTLS)-Wireless Transaction protocol (WTP) - Wireless Session protocol (WSP) - Wireless Application Environment (WAE) - Wireless bearers for WAP. Functional Architecture, Protocol and technical details of - Bluetooth - Zigbee - Ultra Wide Band (UWB)-IrDA (Infra red Data Association) - Radio Frequency Identification (RFID).

WIRELESS APPLICATION PROTOCOL

WAP - Introduction

WAP is the de facto worldwide standard for providing Internet communications and advanced telephony services on digital mobile phones, pagers, personal digital assistants, and other wireless terminals − *WAP Forum.*

WAP stands for Wireless Application Protocol. The dictionary definition

of these terms are as follows −

- **Wireless − Lacking or not requiring a wire or wires pertaining to radio transmission.**
- **Application − A computer program or piece of computer software that is designed to do a specific task.**
- **Protocol − A set of technical rules about how information should be transmitted and received using computers.**

WAP is the set of rules governing the transmission and reception of data by computer applications on or via wireless devices like mobile phones. WAP allows wireless devices to view specifically designed pages from the Internet using only plain text and very simple black-and-white pictures.

WAP is a standardized technology for cross-platform, distributed computing very similar to the Internet's combination of Hypertext Markup Language (HTML) and Hypertext Transfer Protocol (HTTP), except that it is optimized for:

- **low-display capability**
- **low-memory**
- **low-bandwidth devices, such as personal digital assistants (PDAs), wireless phones, and pagers.**

WAP is designed to scale across a broad range of wireless networks like GSM, IS-95, IS-136, and PDC.

Who is behind WAP?

The Wireless Application Protocol (WAP) is a result of joint efforts taken by companies teaming up in an industry group called WAP Forum (www.wapforum.org).

On June 26, 1997, Ericsson, Motorola, Nokia, and Unwired Planet took the initiative to start a rapid creation of a standard for making advanced services within the wireless domain a reality. In December 1997, WAP Forum was formally created and after the release of the WAP 1.0 specifications in April 1998, WAP Forum membership was opened to all.

The WAP Forum now has over 500 members and represents over 95 percent of the global handset market. Companies such as Nokia, Motorola and Ericsson are all members of the forum.

The objective of the forum is to create a license-free standard that brings information and telephony services to wireless devices.

Why is WAP Important?

Until the first WAP devices emerged, the Internet was a Internet and a mobile phone was a mobile phone. You could surf the Net, do serious research, or be entertained on the Internet using your computer, but this was limited to your computer.

Now with the appearance of WAP, the scene is that we have the massive information, communication, and data resources of the Internet becoming more easily available to anyone with a mobile phone or communications device.

WAP being open and secure, is well suited for many different applications including, but not limited to stock market information, weather forecasts, enterprise data, and games.

Despite the common misconception, developing WAP applications requires only a few modifications to existing web applications. The current set of web application development tools will easily support WAP development, and in the future more development tools will be announced.

WAP Microbrowser

To browse a standard internet site you need a web browser. Similar way to browse a WAP enables website, you would need a micro browser. A Micro Browser is a small piece of software that makes minimal demands on hardware, memory and CPU. It can display information written in a restricted mark-up language called WML. Although, tiny in memory footprint it supports many features and is even scriptable.

Today, all the WAP enabled mobile phones or PDAs are equipped with these micro browsers so that you can take full advantage of WAP technology.

A programming model similar to the Internet's

Though WAP is a new technology, but it reuse the concepts found on the Internet. This reuse enables a quick introduction of WAP-based services, since both service developers and manufacturers are familiar with these concepts today.

Wireless Markup Language (WML)

You must be using HTML language to develop your web-based application. Same way, WML is a markup language used for authoring WAP services, fulfilling the same purpose as HTML does on the Web. In contrast to HTML, WML is designed to fit small handheld devices.

WMLScript

Once again, you must be using Java Script or VB script to enhance the functionality of your web applications. Same way, WMLScript can be used to enhance the functionality of a service, just as Java script can be utilized in HTML. It makes it possible to add procedural logic and computational functions to WAPbased services.

Wireless Telephony Application Interface (WTAI)

The WTAI is an application framework for telephony services. WTAI user agents are able to make calls and edit the phone book by calling special WMLScript functions or by accessing special URLs. If one writes WML decks containing names of people and their phone numbers, you may add them to your phone book or call them right away just by clicking the appropriate hyperlink on the screen.

Optimized protocol stack

The protocols used in WAP are based on well-known Internet protocols, such as HTTP and Transmission Control Protocol (TCP), but they have been optimized to address the constraints of a wireless environment, such as low bandwidth and high latency.

The Internet Model

The Internet model makes it possible for a client to reach services on a large number of origin servers, each addressed by a unique Uniform Resource Locator (URL).

The content stored on the servers is of various formats, but HTML is the predominant. HTML provides the content developer with a means to describe the appearance of a service in a flat document structure. If more advanced features like procedural logic are needed, then scripting languages such as JavaScript or VB Script may be utilised.

The figure below 3.1 shows how a WWW client request a resource stored on a web server. On the Internet standard communication protocols, like HTTP and Transmission Control Protocol/Internet Protocol (TCP/IP) are used.

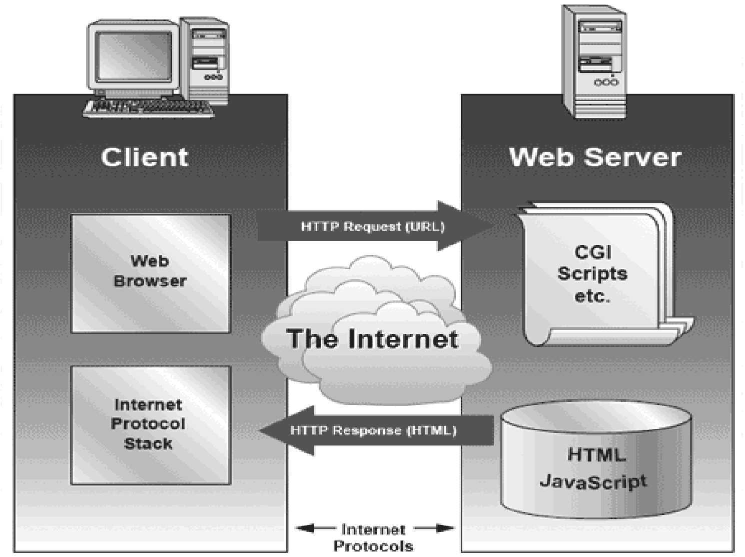


Fig.3.1 client request a resource stored on a web server

The content available at the web server may be static or dynamic. Static content is produced once and not changed or updated very often; for example, a company presentation. Dynamic content is needed when the information provided by the service changes more often; for example, timetables, news, stock quotes, and account information. Technologies such as Active Server Pages (ASP), Common Gateway Interface (CGI), and Servlets allow content to be generated dynamically.

The WAP Model

The figure 3.2 below shows the WAP programming model. Note, the similarities with the Internet model. Without the WAP Gateway/Proxy, the two models would have been practically identical.

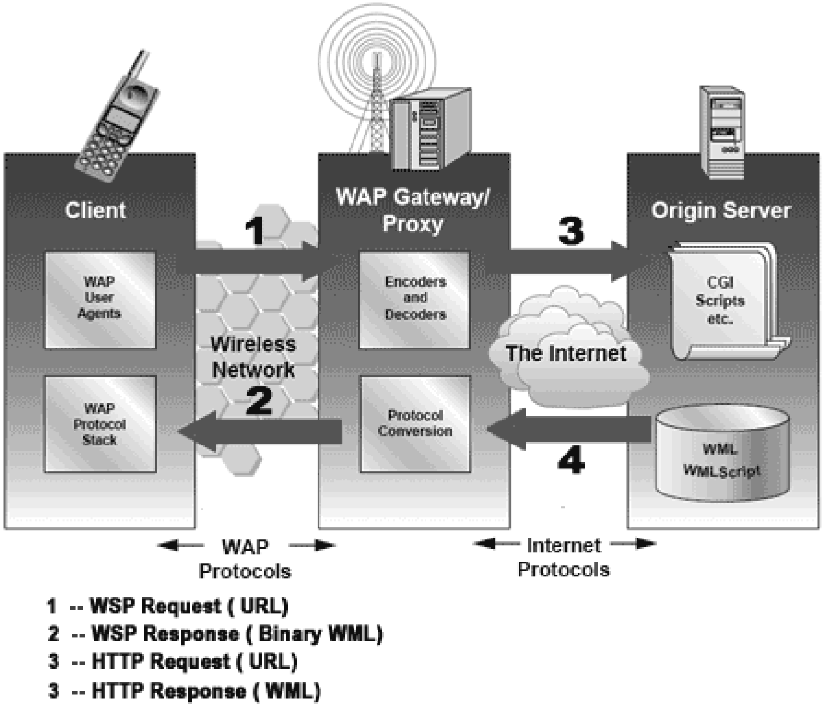


Figure 3.2 WAP programming model

WAP Gateway/Proxy is the entity that connects the wireless domain with the Internet. You should make a note that the request that is sent from the wireless client to the WAP Gateway/Proxy uses the Wireless Session Protocol (WSP). In its essence, WSP is a binary version of HTTP.

A markup language − the Wireless Markup Language (WML) has been adapted to develop optimized WAP applications. In order to save valuable bandwidth in the wireless network, WML can be encoded into a compact binary format. Encoding WML is one of the tasks performed by the WAP Gateway/Proxy.

How WAP Model Works as shown in figure 3.3

When it comes to actual use, WAP works as follows −

- **The user selects an option on their mobile device that has a URL with Wireless Markup language (WML) content assigned to it.**
- **The phone sends the URL request via the phone network to a WAP gateway using the binary encoded WAP protocol.**
- **The gateway translates this WAP request into a conventional HTTP request for the specified URL and sends it on to the Internet.**
- **The appropriate Web server picks up the HTTP request.**

- **The server processes the request just as it would any other request. If the URL refers to a static WML file, the server delivers it. If a CGI script is requested, it is processed and the content returned as usual.**

- **The Web server adds the HTTP header to the WML content and returns it to the gateway.**
- **The WAP gateway compiles the WML into binary form.**
- **The gateway then sends the WML response back to the phone.**
- **The phone receives the WML via the WAP protocol.**
- **The micro-browser processes the WML and displays the content on the screen.**

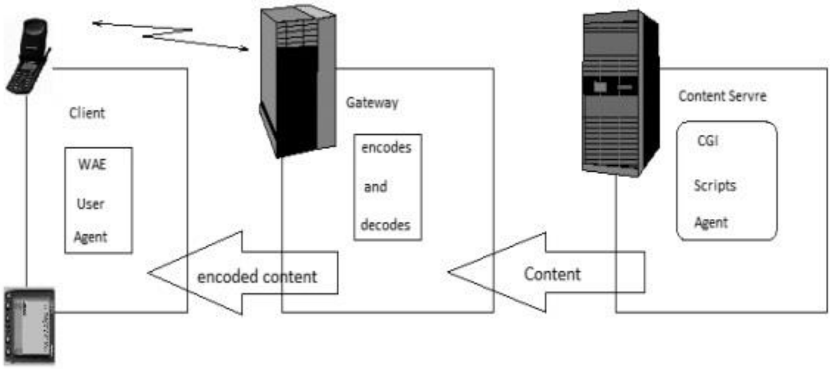


Figure 3.3 WAP Model

Layers of WAP Protocol

Application Layer

Wireless Application Environment (WAE). This layer is of most interest to content developers because it contains among other things, device specifications, and the content development programming languages, WML, and WMLScript.

Session Layer

Wireless Session Protocol (WSP). Unlike HTTP, WSP has been designed by the WAP Forum to provide fast connection suspension and reconnection.

Transaction Layer

Wireless Transaction Protocol (WTP). The WTP runs on top of a datagram service, such as User Datagram Protocol (UDP) and is part of the standard suite of TCP/IP protocols used to provide a simplified protocol suitable for low bandwidth wireless stations.

Security Layer

Wireless Transport Layer Security (WTLS). WTLS incorporates security features that are based upon the established Transport Layer Security (TLS) protocol standard. It includes data integrity checks, privacy, service denial, and authentication services.

Transport Layer

Wireless Datagram Protocol (WDP). The WDP allows WAP to be bearer-independent by adapting the transport layer of the underlying bearer. The WDP presents a consistent data format to the higher layers of the WAP protocol stack, thereby offering the advantage of bearer independence to application developers.

Each of these layers provides a well-defined interface to the layer above it. This means that the internal workings of any layer are transparent or invisible to the layers above it. The layered architecture allows other applications and services to utilise the features provided by the WAP-stack as well. This makes it possible to use the WAP-stack for services and applications that currently are not specified by WAP.

The WAP protocol architecture is shown below alongside a typical Internet Protocol stack.

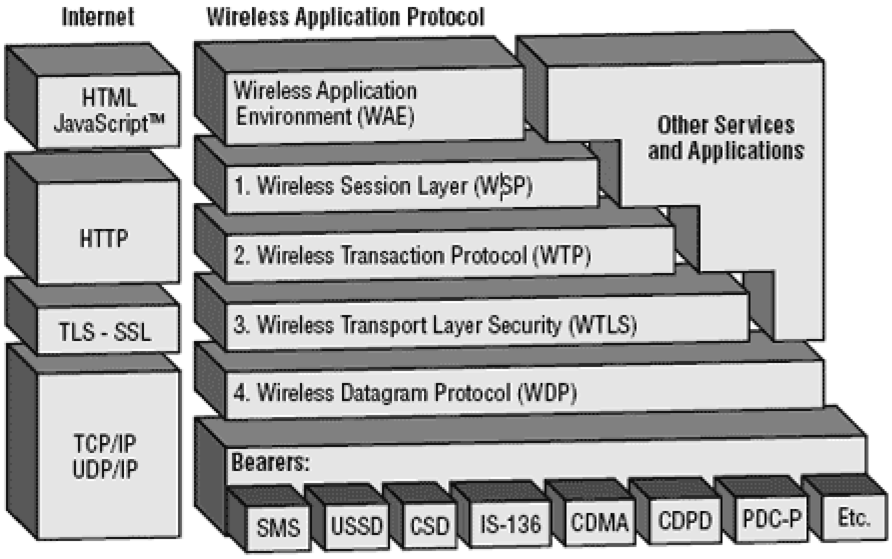

Internet
Wireless Application Protocol
HTML
JavaScript™
HTTP
TLS - SSL
TCP/IP
UDP/IP
Wireless Application Environment (WAE)
1. Wireless Session Layer (WSP)
2. Wireless Transaction Protocol (WTP)
3. Wireless Transport Layer Security (WTLS)
4. Wireless Datagram Protocol (WDP)
Other Services and Applications
Bearers:
SMS
USSD
CSD
IS-136
CDMA
CDPD
PDC-P
Etc.

Figure 3.4 WAP protocol stack

Note that the mobile network bearers in the lower part of the figure 3.4above are not part of the WAP protocol stack.

Wireless Application Environment (WAE), the uppermost layer in the WAP stack, provides an environment that enables a wide range of applications to be used on the wireless devices. We have earlier discussed about the WAP WAE programming model. In this chapter, we will focus on the various components of WAE.

Components of WAE

Addressing Model

A syntax suitable for naming resources stored on servers. WAP use the same addressing model as the one used on the Internet that is Uniform Resource Locators (URL).

Wireless Markup Language (WML)

A lightweight markup language designed to meet the constraints of a wireless environment with low bandwidth and small handheld devices. The Wireless Markup Language is WAP's analogy to HTML used on the WWW. WML is based on the Extensible Markup Language (XML).

WMLScript

A lightweight scripting language. WMLScript is based on ECMAScript, the same scripting language that JavaScript is based on. It can be used for enhancing services written in WML in the way that it to some extent adds intelligence to the services; for example, procedural logic, loops, conditional expressions, and computational functions.

Wireless Telephony Application (WTA, WTAI)

A framework and programming interface for telephony services. The Wireless Telephony Application (WTA) environment provides a means to create telephony services using WAP.

Hardware and Software Requirement

At minimum developing WAP applications requires a web server and a WAP simulator. Using simulator software while developing a WAP application is convenient as all the required software can be installed on the development PC.

Although, software simulators are good in their own right, no WAP application should go into production without testing it with actual hardware. The following list gives a quick overview of the necessary hardware and software to test and develop WAP applications −

- **A web server with connection to the Internet**
- **A WML to develop WAP application**
- **A WAP simulator to test WAP application**
- **A WAP gateway**
- **A WAP phone for final testing.**

Microsoft IIS or Apache on Windows or Linux can be used as the web server and Nokia WAP Toolkit version 2.0 as the WinWAP simulator.

Please have look at WAP - Useful Resources to find out all the above components.

Configure Web Server for WAP

In the WAP architecture, the web server communicates with the WAP gateway, accepting HTTP requests and returning WML code to the gateway. The HTTP protocol mandates

that each reply must include something called a Multi-Purpose Internet Mail Extensions (MIME) type.

In normal web applications, this MIME type is set to text/html, designating normal HTML code. Images on the other hand could be specified as image/gif or image/jpeg for instance. With this content type specification, the web browser knows the data type that the web server returns.

In WAP applications a new set of MIME types must be used, as shown in the following table −

File type	MIME type
WML (.wml)	text/vnd.wap.wml
WMLScript (.wmls)	text/vmd.wap.wmlscript
WBMP (.wbmp)	image/vnd.wap.wbmp

In dynamic applications, the MIME type must be set on the fly, whereas in static WAP applications, the web server must be configured appropriately.

For more information about configuring MIME types for your web server, please consult your web server documentation.

The topmost layer in the WAP architecture is made up of WAE (Wireless Application Environment), which consists of WML and WML scripting language.

WML scripting language is used to design applications that are sent over wireless devices such as mobile phones. This language takes care of the small screen and the low bandwidth of transmission. WML is an application of XML, which is defined in a document-type definition.

WML pages are called decks. They are constructed as a set of cards, related to each other with links. When a WML page is accessed from a mobile phone, all the cards in the page are downloaded from the WAP server to mobile phone showing the content.

WML commands and syntaxes are used to show content and to navigate between the cards. Developers can use these commands to declare variables, format text, and show images on the mobile phone.

BLUETOOTH ARCHITECTURE

Bluetooth is a network technology that connects mobile devices wirelessly over a short range to form a personal area network (PAN). They use short-wavelength, ultra-high frequency (UHF) radio waves within the range 2.400 to 2.485 GHz, instead of RS-232 data cables of wired PANs.

There are two types of Bluetooth networks −

- Piconets
- Scatternets

Piconets

Piconets are small Bluetooth networks, formed by at most 8 stations, one of which is the master node and the rest slave nodes (maximum of 7 slaves). Master node is the primary station that manages the small network. The slave stations are secondary stations that are synchronized with the primary station.

Communication can take place between a master node and a slave node in either one-to-one or one-to-many manner. However, no direct communication takes place between slaves. Each station, whether master or slave, is associated with a 48-bit fixed device address.

Besides the seven active slaves, there can be up to 255 numbers of parked nodes. These are in a low power state for energy conservation. The only work that they can do is respond to a beacon frame for activation from the master node as shown in figure 3.5

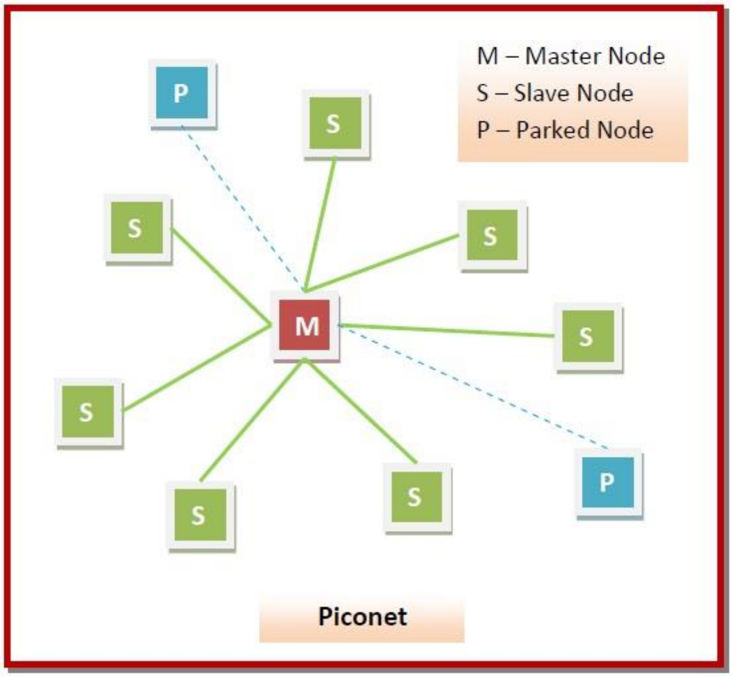


Figure3.5 Piconet

Scatternodes

A scatternet is an interconnected collection of two or more piconets. They are formed when a node in a piconet, whether a master or a slave, acts as a slave in another piconet. This node is called the bridge between the two piconets, which connects the individual piconets to form the scatternet as shown in figure 3.6

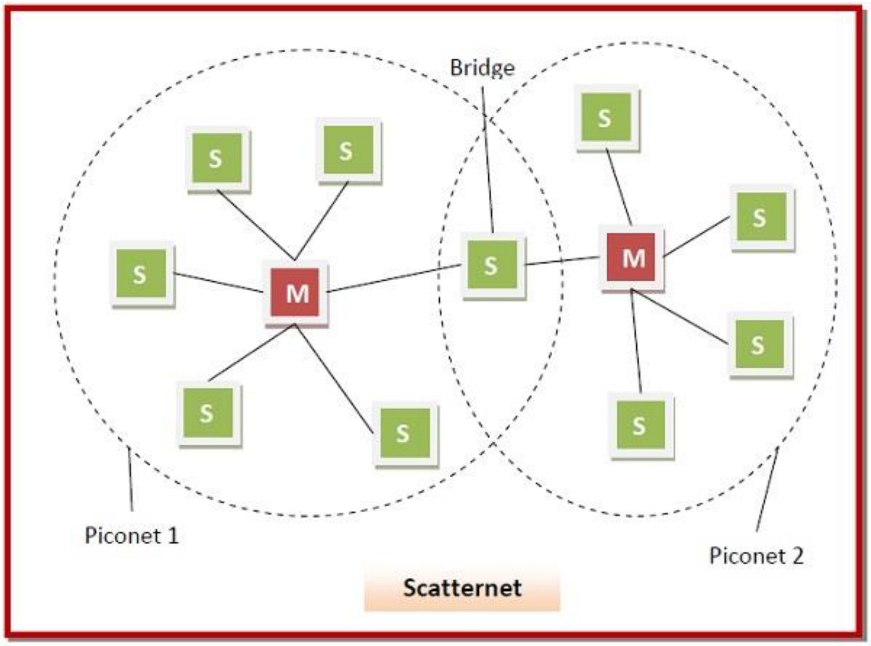


Figure 3.6 Scatternet

Bluetooth network technology connects mobile devices wirelessly over a short-range to form a personal area network (PAN). The Bluetooth architecture has its own independent model with a stack of protocols, instead of following the standard OSI model or TCP/IP model.

The protocols in the Bluetooth standard can be loosely grouped into the physical layer, data link layer, middleware layer, and application layer as shown in the following diagram in figure 3.7

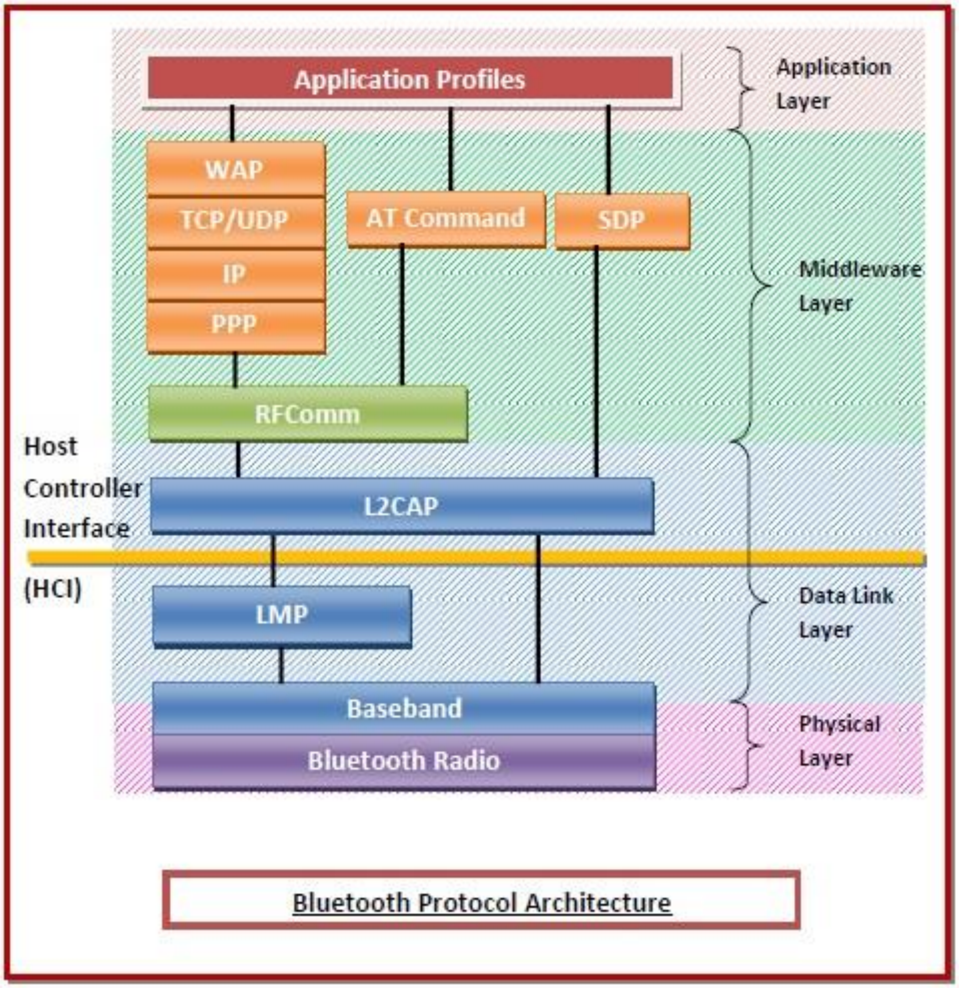


Figure 3.7 Bluetooth Protocol Architecture

Protocols in the Bluetooth Protocol Architecture

- **Physical Layer − This includes Bluetooth radio and Baseband (also in the data link layer.**

○ **Radio − This is a physical layer equivalent protocol that lays down the physical structure and specifications for transmission of radio waves. It defines air interface, frequency bands, frequency hopping specifications, and modulation techniques.**

○ **Baseband − This protocol takes the services of radio protocol. It defines the addressing scheme, packet frame format, timing, and power control algorithms.**

- **Data Link Layer − This includes Baseband, Link Manager Protocol (LMP), and Logical Link Control and Adaptation Protocol (L2CAP).**

○ **Link Manager Protocol (LMP) − LMP establishes logical links between Bluetooth devices and maintains the links for enabling communications. The other main functions of LMP are device authentication, message encryption, and negotiation of packet sizes.**

- **Logical Link Control and Adaptation Protocol (L2CAP) − L2CAP provides adaption between upper layer frame and baseband layer frame format. L2CAP provides support for both connection-oriented as well as connectionless services.**

- **Middleware Layer − This includes Radio Frequency Communications (RFComm) protocol, adopted protocols, SDP, and AT commands.**

  - **RFComm − It is short for Radio Frontend Component. It provides a serial interface with WAP.**

  - **Adopted Protocols − These are the protocols that are adopted from standard models. The commonly adopted protocols used in Bluetooth are Point-to-Point Protocol (PPP), Internet Protocol (IP), User Datagram Protocol (UDP), Transmission Control Protocol (TCP), and Wireless Application Protocol (WAP).**

  - **Service Discovery Protocol (SDP)− SDP takes care of service-related queries like device information so as to establish a connection between contending Bluetooth devices.**

  - **AT Commands − ATtention command set.**

- **Applications Layer − This includes the application profiles that allow the user to interact with the Bluetooth applications.**

Bluetooth network technology connects mobile devices wirelessly over a short-range to form a personal area network (PAN). The Bluetooth architecture has its own independent model with a stack of protocols, instead of following the standard OSI model or TCP/IP model. Another unique feature is that it is not mandatory for all the devices in the Bluetooth system to use all the protocols in the stack. This is because Bluetooth is designed to be used by myriad applications and the application designates which part of the protocol stack is to be used.

Protocols in the Bluetooth Protocol Stack

- **Core protocols − This includes Bluetooth radio, Baseband, Link Manager Protocol (LMP), Logical Link Control and Adaptation Protocol (L2CAP), and Service Discovery Protocol (SDP).**

- **Cable Replacement Protocol − This includes Radio Frequency Communications (RFComm) protocol. It is short for Radio Frontend Component. It provides a serial interface with WAP.**

- **Adopted Protocols − These are the protocols that are adopted from standard models. The commonly adopted protocols used in Bluetooth are Point-to-Point Protocol (PPP), Internet Protocol (IP), User Datagram Protocol (UDP), Transmission Control Protocol (TCP), and Wireless Application Protocol (WAP).**

- **AT Commands − ATtention command set.**

The following diagram as shown in figure 3.8 shows the Bluetooth protocol stack −

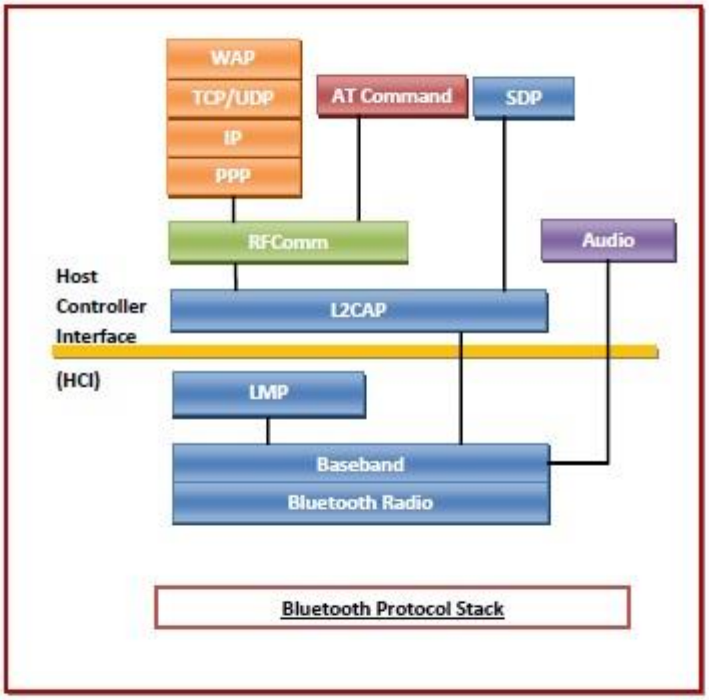


Figure 3.8 Bluetooth protocol stack

Functions of the Core Protocols

- **Radio − This is a physical layer equivalent protocol that lays down the physical structure and specifications for transmission of radio waves. It defines air interface, frequency bands, frequency hopping specifications and modulation techniques.**
- **Baseband − This protocol takes the services of radio protocol. It defines the addressing scheme, packet frame format, timing, and power control algorithms.**
- **Link Manager Protocol (LMP) − LMP establishes logical links between Bluetooth devices and maintains the links for enabling communications. The other main functions of LMP are device authentication, message encryption, and negotiation of packet sizes.**
- **Logical Link Control and Adaptation Protocol (L2CAP) − L2CAP provides adaption between upper layer frame and baseband layer frame format. L2CAP provides support for both connection-oriented as well as connectionless services.**
- **Service Discovery Protocol (SDP)− SDP takes care of service-related queries like device information so as to establish a connection between contending Bluetooth devices.**

ZIGBEE

Introduction

This zigbee tutorial describes everything you would like to know about Zigbee protocol stack. Now-a-days zigbee is becoming very popular for low data rate wireless applications.

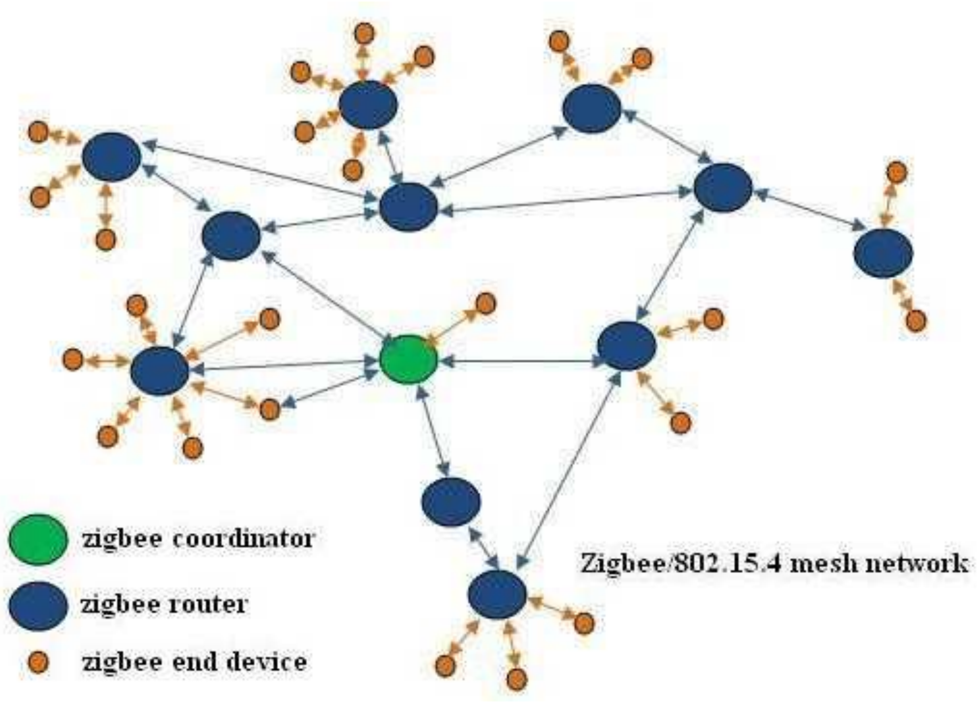
Zigbee devices are used in smart energy, medical and in home automation. In smart energy applications zigbee products are used to monitor and control use of energy and water, which helps consumers save energy and water and save money too.

In medical field it is used to connect unlimited number of health monitoring devices and many more.

In home automation it controls domestic lighting, such as switches, dimmers, occupancy sensors and load controllers.

It has two bands of operation 868/915MHz and 2450MHz. 868/915 band provides about 20-40Kb/s and 2450MHz band provides about 250 kb/s data rates. In addition to this uses zigbee end devices can go to sleep mode which saves battery consumption and it also takes care of security of the information owing to security layer.

Zigbee Network Overview:



As mentioned in the network diagram, Figure 3.9 zigbee network is comprised of coordinator(C), router(R) and end devices (E). Zigbee supports mesh-routing. For detailed information on routing protocol employed in zigbee, one may refer Ad-hoc on-demand Distance Vector Routing protocol (AODV protocol), RFC 3561

Coordinator:
– Always first coordinator need to be installed for establishing zigbee network service, it starts a new PAN (Personal Area Network), once started other zigbee components viz. router(R) and End devices(E) can join the network(PAN). – It is responsible for selecting the channel and PAN ID. – It can assist in routing the data through the mesh network and allows join request from R and E. – It is mains powered (AC) and support child devices. – It will not go to sleep mode.

Router:
– First router needs to join the network then it can allow other R & E to join the PAN. – It is mains powered (AC) and support child devices. – It will not go to sleep mode.

End Devices:
– It cannot allow other devices to join the PAN nor can it assist in routing the data through the network. – It is battery powered and do not support any child devices. – This may sleep hence battery consumption can be minimized to great extent. There are two topologies, star and mesh, as mentioned Zigbee supports mesh routing. PAN ID is used to communicate between zigbee devices, it is 16 bit number. Coordinator will have PAN ID set to zero always and all other devices will receive a 16 bit address when they join PAN. There are two main steps in completing Zigbee Network Installation. Forming the network by Coordinator and joining the network by Routers and End devices.

Forming the Zigbee Network

• Coordinator searches for suitable RF channel which is usable and not interfering with Wireless LAN frequencies in use. This is because WLAN also operates in the same 2.4GHz bands.This is done on all the 16 channels. It is also referred as energy scan.

• Coordinator starts the network by assigning a PAN ID to the network. Assignment is done in two ways. Manual (pre configured) and dynamic (obtained by checking other PAN IDs of networks already in the operation nearby so that PAN ID does not conflict with other networks). Here Coordinator also assigns network address to itself i.e. 0x0000.

• Now coordinator completes its configuration and is ready to accept network joining request queries from routers and end devices who wish to join the PAN.

In addition to above, Coordinator(C) sends broadcast beacon request frame on remaining quiet channel. This is also referred as beacon scan or PAN scan. By this Coordinator receives PAN ID of routers(R) and end devices(E) present nearby. It also comes to know whether R/E allow join or not.

Now R/E can join by sending association request to C. C will respond with association response.

Joining the Zigbee Network

• Let us examine how a router or end device joins zigbee network as part of zigbee tutorial. There are two ways to join a zigbee network viz. MAC association and network re-join.

• First one is implemented by device underlying MAC layer and second one is implemented by network layer, despite the name may also be used to join a network for the first time.

• MAC association can be performed between C and R/E or R and E or R and other R.

• Let us assume that Coordinator(C) has already established the PAN network. Hence next step for R or E is to find out whether C is allowing joining or not. So they do PAN scan or send beacon request frame.

• After they come to know that they can join the network, they will send association request frame and will join the network as soon as they receive the association response.

• As mentioned above whether or not C or R allow a new device to join depends on two main factors:
-Permit joining attribute
-Number of end device children it already has.
One of the applications of zigbee in home is that switch, speakers and lamp is controlled using zigbee technology.

Zigbee protocol

zigbee IP consists of various protocol layers viz. physical layer(PHY), mac layer, network layer and application layer. IEEE 802.15.4 standard defined zigbee PHY and MAC specifications. Zigbee alliance specifies network and application layers.

Zigbee Protocol stack

The following figure 3.10 depicts zigbee protocol stack,which consists of four layers viz. PHY,MAC,network & security and application layer. The first two are covered in IEEE 802.15.4 WPAN standard and the later two are covered in documents published by zigbee

alliance.

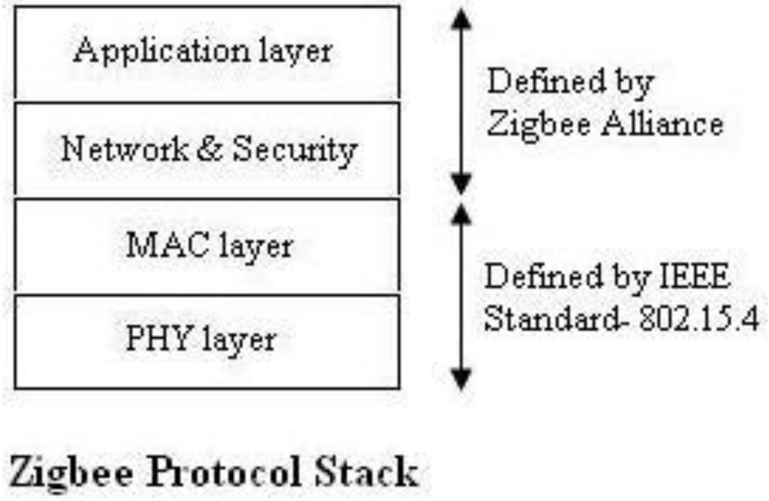


Figure 3.10 Zigbee Protocol stack

Application Layer:

On Basics of OSI and TCPIP to understand application layer in general. There are two profiles at this layer. 1. Manufacturer specific application profile- Operate as closed systems and also ensured that they can coexist with other zigbee systems. 2. Public application profile- for this to work interoperability between various zigbee devices is a must. A single zigbee node supports up to 240 application objects called end points. An end point specifies specific application, for example, 0 dedicated to ZDO (Zigbee device object), provides control and management commands. 6 used for control of light. 8 used for manage heating and air conditioning.

Network Layer:

Ad-hoc on-demand Distance Vector Routing protocol (AODV) is used at network layer.

Security Layer:

If security is enabled C will start up using a 128 bit AES encryption key. Devices having same security key can communicate on PAN. How to obtain this key? 1. Pre-installation 2. Key is received over the air during joining.

MAC Layer

Each MAC frame consists of three fields MAC header, MAC payload and MFR (FCS).

Each MAC frame will contain Frame control field (16 bit), which carry frame type, addressing fields and other control flags.

This MAC control field contain frame type field, which is the main differentiating factor in identifying one MAC frame with the other. It is 3 bit in length.

The MAC frames are divided into following four major categories, which is used by zigbee devices to establish connection to the PAN by exchanging system information.
1. Beacon
2. Data
3. Acknowledgement
4. MAC command

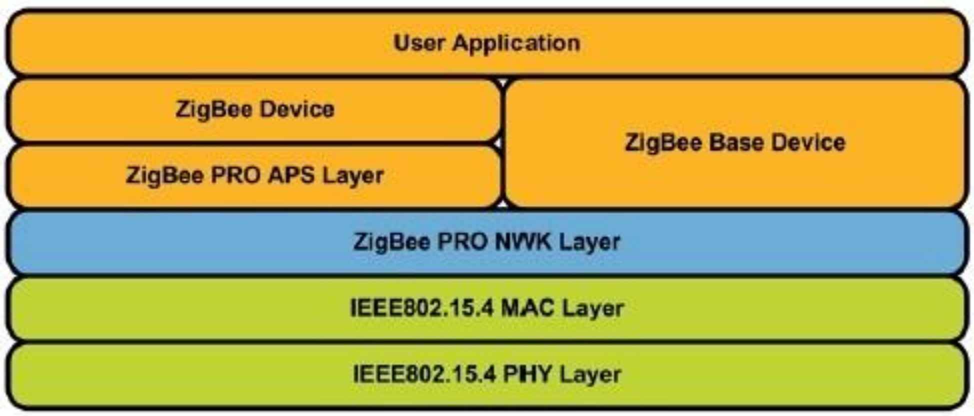
Zigbee 3.0:

The standard zigbee 3.0 is variation to previous zigbee standards. The zigbee 3.0 specification enables interoperability among different application profiles. Due to this, zigbee 3.0 allows devices from different application areas to communicate and form single homogeneous network. For example, device#1 from zigbee light profile can coexist with device#2 from health care profile with same zigbee network.

Moreover zigbee 3.0 compliant devices support connectivity with IP networks such as LAN and WAN. Hence these devices can form IoT network. Hence products from different manufacturers can communicate together as single networking devices. Zigbee 3.0 is based on IEEE 802.15.4 standard specifications and support 2.4 GHz global frequency band. It uses zigbee PRO version.

Following are the features of zigbee 3.0 :
• Low Power: Zigbee 3.0 compliant devices support low power and low data rate. IoT devices require long life battery. Hence this standard is widely used in IoT (Internet of Things) network.
• Reliable and Robust: The zigbee 3.0 supports mesh topology and hence such network will avoid single point of failure and hence ensure reliable delivery of packets.
• Scalable: The devices can be added any time in zigbee 3.0 network.
• Secure: It supports AES-128 encryption type and hence it is secured network.
• Global Standard: The frequency band 2.4 GHz is used widely across the globe which is used in zigbee 3.0 based devices. Hence it is a global standard.
From the above points one can easily derive difference between zigbee 3.0 and other versions of zigbee standard.

Zigbee 3.0 Protocol Stack

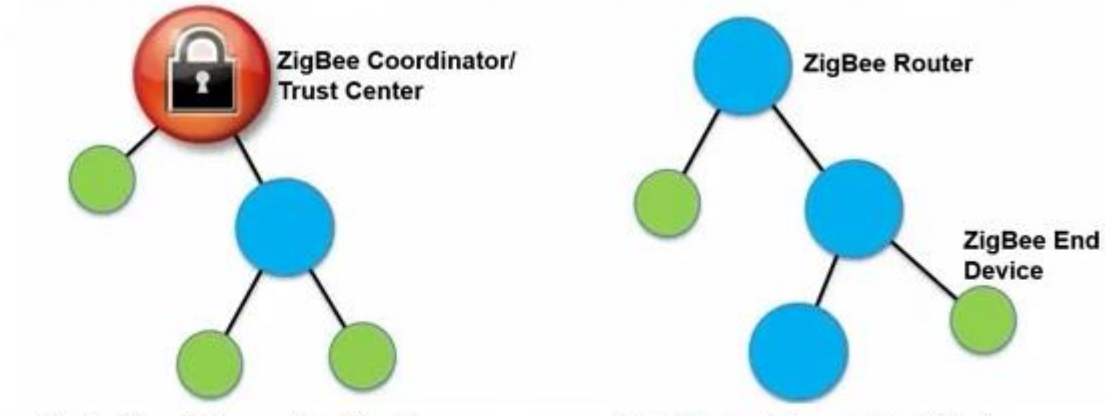


Zigbee 3.0 Protocol Stack

Figure 3.11 Zigbee 3.0 Protocol Stack

The figure-3.11 depicts zigbee 3.0 protocol stack. As shown it consists of PHY, MAC, network and application layers. The changes have been incorporated into application layer in zigbee 3.0 compare to previous zigbee versions. Network layer is sandwitched between upper layer i.e. application layer and PHY/MAC as defined in IEEE 802.15.4 standard.

The zigbee 3.0 protocol stack incorporates zigbee base device layer which provides consistant behaviour for commissioning new nodes in the network.



Centralized Security Mode

Distributed Security Mode

The security layer is also enhanced and here there are two security modes supported. Centralized: This mode is managed by central co-ordinator. This co-ordinator forms the network as well as takes care of key assignment to the new joining nodes. Distributed: This mode does not have any central co-ordinator. The zigbee router itself manages network establishment and key assignment to peer router in the network. The figure-3 depicts zigbee network security modes.

• Zigbee 3.0 support large number of nodes about 250.
• It also supports dynamic nature of the network.
• It supports rejoining of orphaned nodes with the new parent node in the event of loss of parent.
• Zigbee 3.0 provides backward compatibility with other zigbee application profiles such as zigbee light link 1.0 profile, zigbee home automation 1.2 profile etc.

ULTRA-WIDEBAND TECHNOLOGY

Although wireless UWB is a promising technology in theory, there are several practical reasons which make it less popular than BLE for IoT.

Ultra-wideband (WB) is a wireless technology that can be used for data transmission and positioning. Unlike other common wireless technologies like BLE or Wifi, UWB transmits low amounts of power spread over a wide range of frequencies.

You might be familiar with newer Wifi routers transmitting via the less crowded 5GHz band. What that actually means is that the FCC has allowed Wifi networks to operate in a newly allocated set of frequencies between 5.17 to 5.835GHz. Of course, your wifi router uses just one of the many channels which subdivide the 5GHz band.

By comparison, the allowable FCC frequency range for UWB is 3.1-10.6GHz. Officially, the FCC and ITU-R define UWB to be wireless signal transmission with a bandwidth which exceeds 500MHz or 20% of the center (arithmetic mean) frequency.

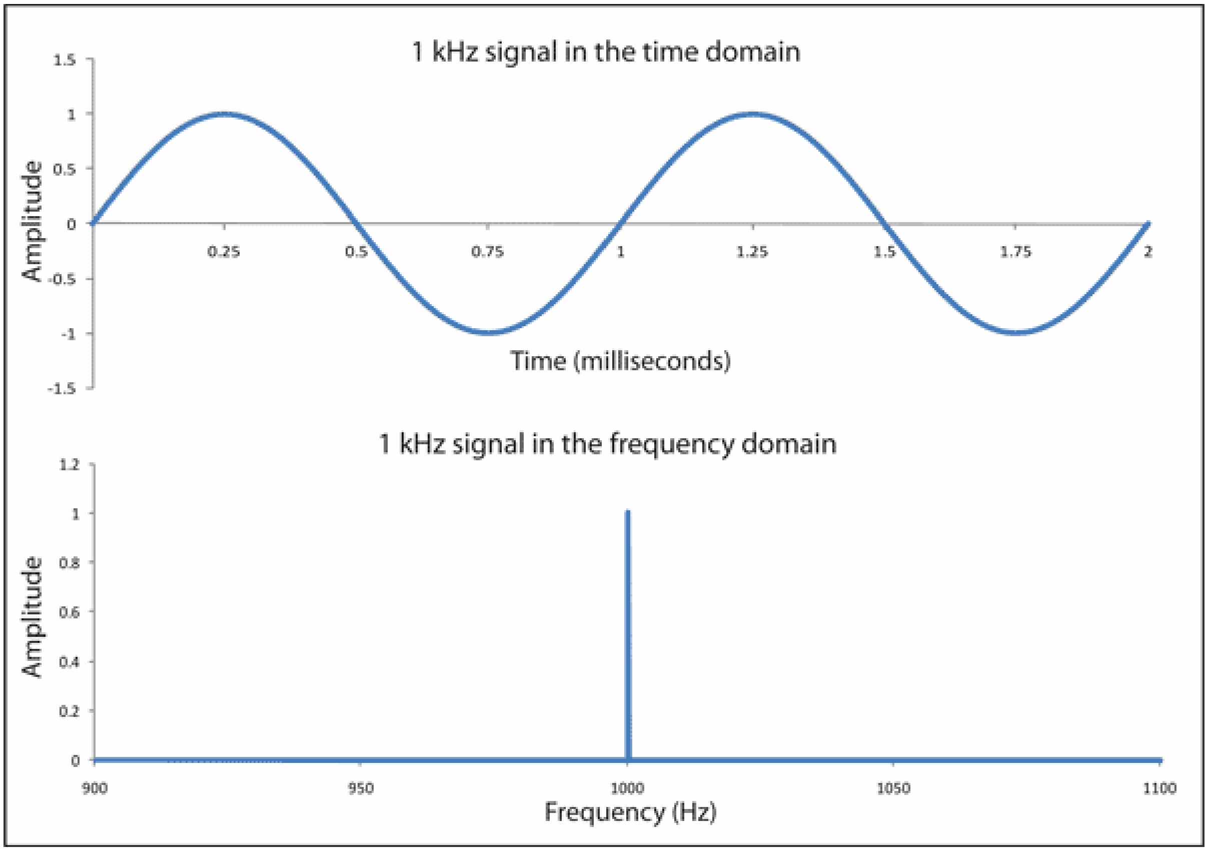
UWB competes directly with BLE for low energy and close-range wireless communications. However, because of the science behind wideband vs narrowband technologies, UWB promises way more accurate positions and higher data speeds over BLE. So, how does this science work and why hasn’t UWB replaced BLE?

How UWB works

To understand the benefits of UWB, we must first take a step back to understand the basics of signal processing.

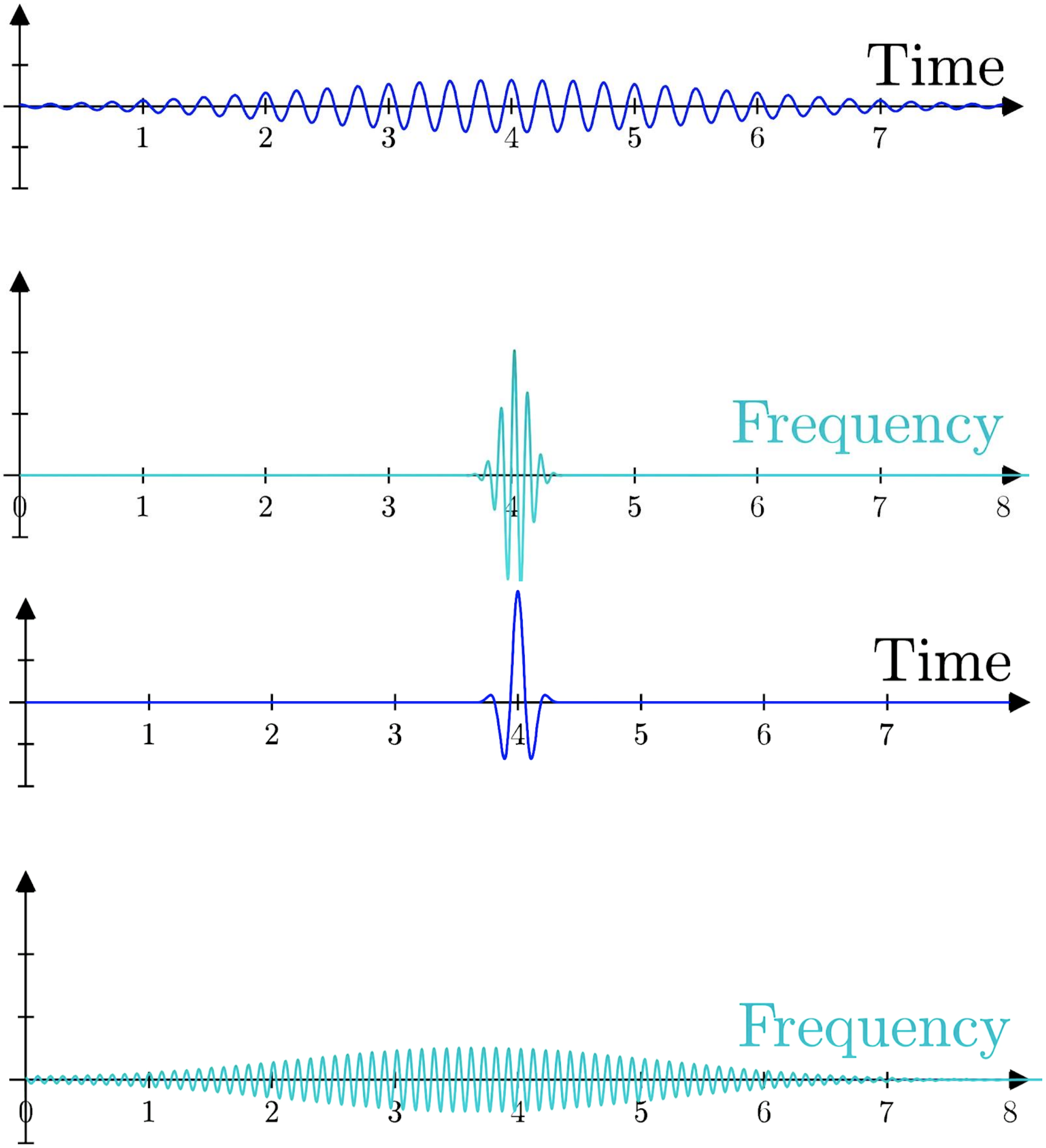
When you see that trippy sound wave visualization in your media player of choice, you are looking at its representation of amplitude (or volume) over time--or in the time domain.

In the real world, sound (and electromagnetic) waves are usually composites of many waves, each of a different frequency, like notes in a chord. When engineers talk about transforming this wave to the frequency domain, they mean graphing out the distribution of frequencies which make up a wave. For example, a chord of two pure musical tones, A and C, would look like a spike at the A frequency and a spike at the C frequency. The mathematical procedure that translates a wave between these two domains is called the Fourier Transform.



So now that we have some familiarity with time and frequency domains, I'm going to introduce the tradeoffs between time duration and frequency ranges.

If someone were to sing a few notes of a song, you might be able to narrow down the list of possible songs they were singing, but your confidence would still be low. The longer they sing, the more confident you would be in determining which song they are singing. If they were to only sing one note, the list of possible songs is much larger.



The time and frequency domains work the same way. If we sampled a wave over a short duration of time, we would not be very confident of which frequencies composed that wave, so our distribution of frequencies would be very wide. The Fourier transform function is invertible--that is reversible--so if we went backwards, the logic still holds true. Therefore,

if we have a large range of frequencies (like an ultra-wideband), we could send this waveform in a very sharp spike in time.

Indoor Positioning

So, why is it useful to be able to send sharp pulses of waves? Well, let's go back to one of the main purposes of UWB: to accurately triangulate positions through precise distance measurements.

One of the first examples of distance determination through waves is radar. In fact, dolphins and bats have been using this long before the invention of radar. If you have any familiarity with animal echolocation, you know it sounds like repeated intervals of chirps or clicks. If your signals are sharp and short you can more accurately measure the time of flight between the original signal and its echo off an object and therefore more accurately deduce its distance from you.

This is how UWB technology is able to determine an object's position within a few centimeters. By contrast, Bluetooth uses signal strength as a proxy for distance which is only accurate to a few meters.

High Data Transmission

$$\underbrace{C}_{\text{Channel capacity in bits/s}} = \overset{\text{bandwidth of the channel}}{B} \log_2 (1+\underbrace{S/N}_{\text{signal-to-noise ratio}})$$

Claude Shannon, the grandfather of Information Technology, developed a groundbreaking theorem which states the maximum data rate capacity of a communication channel. This maximum increases linearly with bandwidth and logarithmically to the signal to noise ratio.

Simply put, widening the frequency range increases the maximum data rate faster than increasing the signal to noise ratio. This allows UWB systems to achieve high data rates by nature of the technology rather than using complicated algorithms to increase signal to noise ratio. In the next few paragraphs I'll describe an analogy to help you understand the Shannon capacity theorem intuitively.

INFRARED DATA ASSOCIATION (IRDA)

Infrared Data Association, or IrDA in short, is a group of device manufacturers that developed a standard for transmitting data via infrared (IR) light waves. It provides specifications for the complete set of protocols for wireless IR communication. The main reason for using IrDA had been wireless data transfer over the "last one meter" using point-and-shoot principles. It is famous for secure data transfer, line-of-sight and very low bit error rate that makes it very efficient .

IR communication is an inexpensive and widely adopted short-range (1-3m) wireless technology. It is widely used in consumer electronics, automobiles, computers, medical devices, household appliances, commercial services, etc.

IrDA-enabled devices can communicate and are bi-directional. IrDA is inexpensive, secure and fast (supporting speeds of up to 100Mbps and even more). IrDA-enabled devices can communicate and are bi-directional. IrDA is inexpensive, secure and fast (supporting speeds of up to 100Mbps and even more).

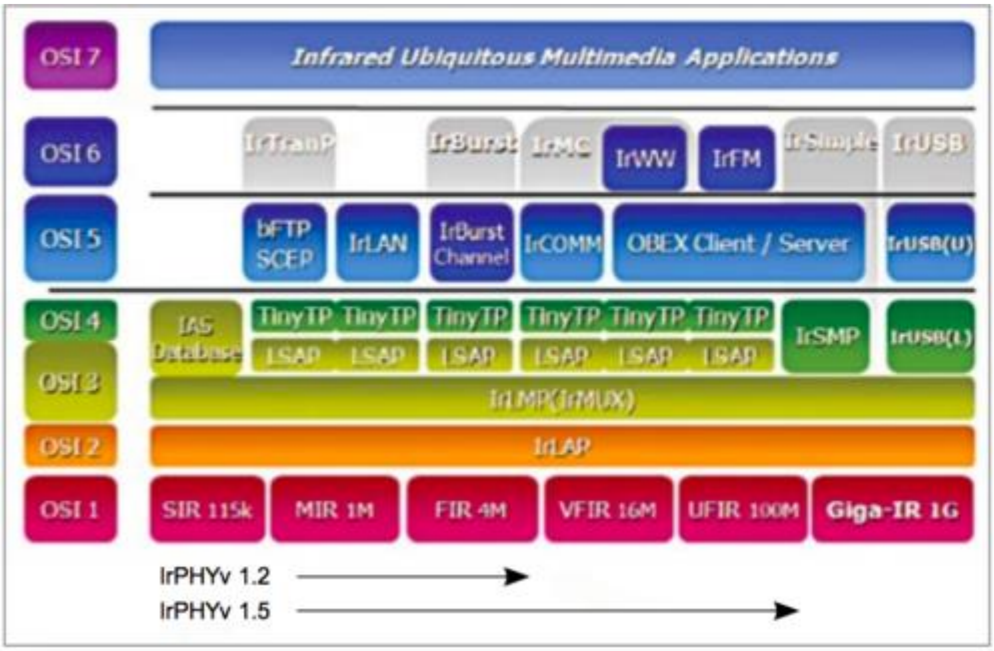


Figure 3.12 Infrared Data Association (IrDA)-protocol-stacks

The Open Systems Interconnection (OSI) model of IrDA protocol stack is shown in Figure 3.12 Some of the specifications based on the OSI model are given below:

Infrared physical layer (IrPHY)

This specification is intended to facilitate point-to-point communication between electronic devices. It specifies the optical media interfaces for Serial Infrared (SIR) data transmission and is part of the first layer of the OSI model.

Infrared link access protocol (IrLAP)

This specification is part of the second layer of IrDA specifications. It lies on top of the IrPHY layer and below the IrLMP layer. It represents the data link layer.

Infrared link management protocol (IrLMP)

It is the third layer of IrDA specifications. It defines link management multiplexer and link management information access service.

Transport protocol (TinyTP)

This optional protocol specified in the fourth layer lies on top of the IrLMP layer.

Infrared communication protocol (IrCOMM)

The IrCOMM protocol specified in the fifth layer lets the infrared device act like either a serial or parallel port.

Infrared Financial Messaging (IrFM)

This protocol specified in the sixth layer is a wireless payment standard developed by the Infrared Data Association.

RADIO FREQUENCY IDENTIFICATION

Radio Frequency Identification (RFID) is the application of radio waves to read and capture information stored on tags affixed to objects. RFID readers are installed at tracking points and can read information from tags when they come into range, which can be of several feet radius. A tag need not be within direct line-of-sight of the reader to be tracked. RFID is used to check identities and track inventory, assets and people. RFID tags can be attached to a variety of objects like cash, clothing, baggage, parcels, and even implanted in animals and people.

Working Principle

There are two parts in a RFID system−

- **a tag or label**
- **a reader**

RFID tags are affixed on the object and have a transmitter and a receiver embedded on it. It contains the serial number that uniquely identifies a specific object. The tags have two parts−

- **a microchip to store and process information, and**
- **an antenna to receive and transmit a signal.**

The RFID reader (also called interrogator) captures the information encoded on the tag using an antenna. It is a two-way radio transmitter-receiver that emits a signal for the tag. The tag responds by sending the information embedded in its memory. The reader captures the results and transmits to the RFID computer program, which then performs the necessary processing.

Types of RFID tags

RFID tags are categorized into three types according to power−

- **Passive tags− They use the radio wave energy of the reader to transmit its ID to the reader.**
- **Active tags− They are equipped with an on-board battery and transmit their ID periodically.**
- **Battery – assisted Passive− They have a small battery on-board and are activated only within the range of an RFID reader.**

According to readability, RFID tags are as follows−

- **Read-only tags− They have a factory-assigned ID which serves as a key into a database.**

- **Read/write tags− In these tags, object-specific data can be written and retrieved by the system user.**

- **Field programmable tags− These are written once by the system, thereby they can be read multiple times.**

- **Blank tags− They may be electronically written by the user.**

Types of RFID readers

RFID readers are categorized into two types according to power−p>

- **Passive readers− They can only receive signals from active tags.**

- **Active readers− They can transmits interrogator signals to both passive, active as well as battery-assisted tags and also receives replies from them.**

According to position, RFID readers are of two types−

- **Fixed readers− They are used to create a highly defined and tightly controlled interrogation area. Tags are read when they enter this area. Active readers are deployed here.**

- **Mobile readers− They are used for creating handheld tag reading devices. They may be also installed in moving vehicles.**

EPC or Electronic Product Code is a universal identifier that are encoded on RFID (Radio Frequency Identification) tags to check identities of objects like inventory, assets and people, and track them. The second generation of this technology, as laid down by EPCglobal Tag Data Standard, is called EPC Gen 2.

The architecture of EPC Gen 2, RFID network has two main components −

- **Tags or labels − They are affixed on objects so that they can be identified or tracked.**
- **Readers or interrogators − They are the intelligent part of the system that tracks the tags.**

The architecture is shown as Figure 3.13below −

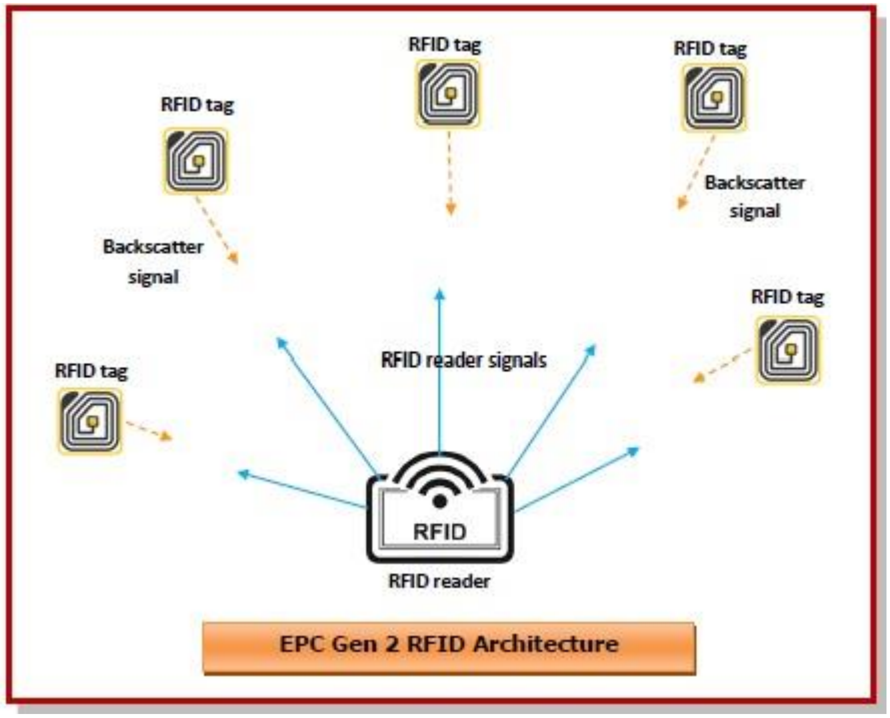


Figure 3.13 RFID Architecture

RFID tags may be like stickers that are affixed on the objects, like a bag, pair of jeans etc.; or they may be integrated into the object like a driving license. The RFID integrated circuit has a transmitter and a receiver embedded on it. It contains the serial number that uniquely identifies a specific object. The tags have two parts, a microchip to store and process information about the object, and an antenna to receive and transmit signals with the reader.

The RFID reader captures the information encoded on the tag using an antenna. It is a two-way radio transmitter-receiver that emits a signal for the tag. The tag responds by sending the information embedded in its memory. The reader captures the results and transmits to the RFID computer program, which then performs the necessary processing.

PART-A

1.Define WML
2. Sketch the WAP programming model.
3.Distinguish Piconet and Scatternet.
4.Define Bluetooth.
5.What are the components comprised in zigbee network?
6.List the major categories of MAC frames used by Zigbee devices.
7.Define Irda and it applications.
8.What is the working principle of RFID?
9.What are the type os RFID readers according to the position.
10.Define UWB.

PART-B

1.Explain WAP architecture.

2.Discuss about the Bluetooth Architecture.

3.Explain the Zigbee model for any application.

4.Write short notes on UWB.

5.Explain in detail about Irda and RFID.

TEXT BOOK / REFERENCE BOOKS

1. Andreas F. Molisch, "Wireless Communications", 2nd Edition, John Wiley & Sons Ltd, 2011.

2. William C.Y. Lee., "Wireless & Cellular Telecommunications", 3rd edition, McGraw Hill.2006.

3. Yibing Lin, "Wireless & mobile Network architecture", Wiley 2002.

4. Tao Jiang, Lingyang Song and Van Zhang, "Orthogonal Frequency Division Multiple Access Fundamentals and Applications" Taylor and Francis Group, 2010.

5. Yong Soo Cho, Jaekwon Kim, Won Young Yang and Chung G. Kang, "MIMO-OFDM Wireless Communications with MATLAB", John Wiley & Sons (Asia) Pvt. Ltd, 2010.

SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE
www.sathyabama.ac.in

SCHOOL OF ELECTRICAL AND ELECTRONICS

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

UNIT – IV- WIRELESS COMMUNICATIONS – SEC1404

IV 3G SYSTEMS

UNIT 4 3G SYSTEMS.

3G Networks - Features and Performance of 3G networks -Frequency allocation for IMT (International Telecommunications Union) 2000 - IMT 2000 family - Architecture of Universal Mobile Telecommunications System (UMTS) network - MAC layer-RLC layer-RRC layer - 3GPP release 99 network architecture. Network architecture of Enhanced Data rates for Global Evaluation (EDGE).CDMA 2000 - Physical channels - Radio Interface parameters of CDMA 2000 FDD- Transmission characteristics of CDMA 2000 TDD

4.1 3G NETWORKS

- ITU (International Telecommunications Union) has called the future cellular networks 3G networks or IMT-2000; the previous term was Future Public Land Mobile Telephone System (FPLMTS). The performance for IMT-2000 air interference can be summarized as

- Wideband CDMA systems
- Spectrum bandwidth 5 MHz
- Full coverage and mobility for a data rate of 144 kbps to 384 kbps
- Limited coverage and mobility or no mobility for 2 Mbps
- High spectrum efficiency compared to 2G system
- High flexibility to introduce new and multimedia services

3G features

- Provision of multirate services
- Packet data
- A user-dedicated pilot for a coherent uplink
- An additional DL pilot channel for beam forming
- Intercarrier handover
- Fast power control
- Multiuser detection

IMT-2000 has published a minimum performance requirement of a 3G wireless system, which is for both circuit-switched (CS) and packet-switched (PS) data:

- Data rate of 144 kbps in the vehicular environment
- Data rate of 384 kbps in the pedestrian environment
- Data rate of 2 Mbps in the fixed indoor and pico cell environment

4.2 IMT-2000

- In total, 17 proposals for different IMT-2000 standards were submitted by regional SDOs to ITU in 1998. 11 proposals for terrestrial systems and 6 for mobile satellite systems (MSSs).
- All 3G standards have been developed by regional standard developing organizations (SDOs).
- Evaluation of the proposals was completed in 1998, and negotiations to build a consensus among different views were completed in mid 1999. All 17 proposals have been accepted by ITU as IMT-2000 standards. The specification for the Radio Transmission Technology (RTT) was released at the end of 1999.

- The (IMT-2000), consists of 3 operating modes based on Code Division Multiple Access (CDMA) technology.
- 3G CDMA modes are most commonly known as:
- CDMA2000,
- WCDMA (called UMTS) and
- TD-SCDMA (Time Division-Synchronous Code Division Multiple Access)

- IMT-2000 has published a minimum performance requirement of a 3G wireless system, which is for both circuit-switched (CS) and packet-switched (PS) data:
- Data rate of 144 kbps in the vehicular environment
- Data rate of 384 kbps in the pedestrian environment
- Data rate of 2 Mbps in the fixed indoor and pico cell environment

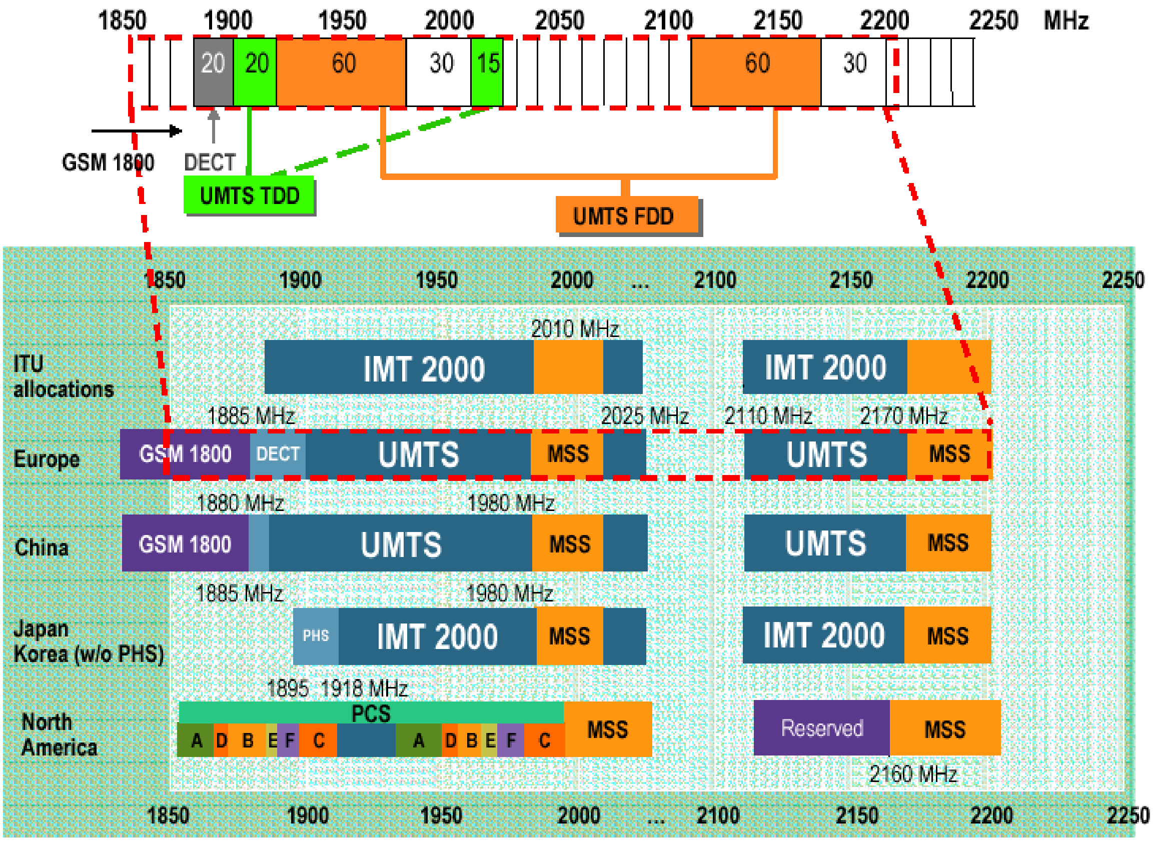


Fig 4.1 Frequency allocation in IMT 2000

4.3 3G UMTS Network Architecture

With the change from 2G to 3G, the emphasis for the systems changed from a focus on mobile voice communications to mobile data and general connectivity.The foundations for the UMTS network had been set in place when GSM was launched. This provided the basic access elements as well as circuit switched voice. The additional of packet data with GPRS required additional network entities to be added. It was the combination of these two network elements that provided the basis for the 3G UMTS network architecture.

The radio access network changed considerably as a completely new radio interface was used based around the use of CDMA. Also the handset name was changed to user equipment indicating a change in its use from just a voice phone to a data set which could have been a phone, PDA or laptop, with many laptops requiring a 3G dongle to plug into a USB port.

4.3.1 3G UMTS network constituents

The UMTS network architecture can be divided into three main elements:

User Equipment (UE): The User Equipment or UE is the name given to what was previous termed the mobile, or cellphone. The new name was chosen because the considerably greater functionality that the UE could have. It could also be anything between a mobile phone used for talking to a data terminal attached to a computer with no voice capability.

Radio Network Subsystem (RNS): The RNS also known as the UMTS Radio Access Network, UTRAN, is the equivalent of the previous Base Station Subsystem or BSS in GSM. It provides and manages the air interface for the overall network.

Core Network: The core network provides all the central processing and management for the system. It is the equivalent of the GSM Network Switching Subsystem or NSS.

The core network is then the overall entity that interfaces to external networks including the public phone network and other cellular telecommunications networks.

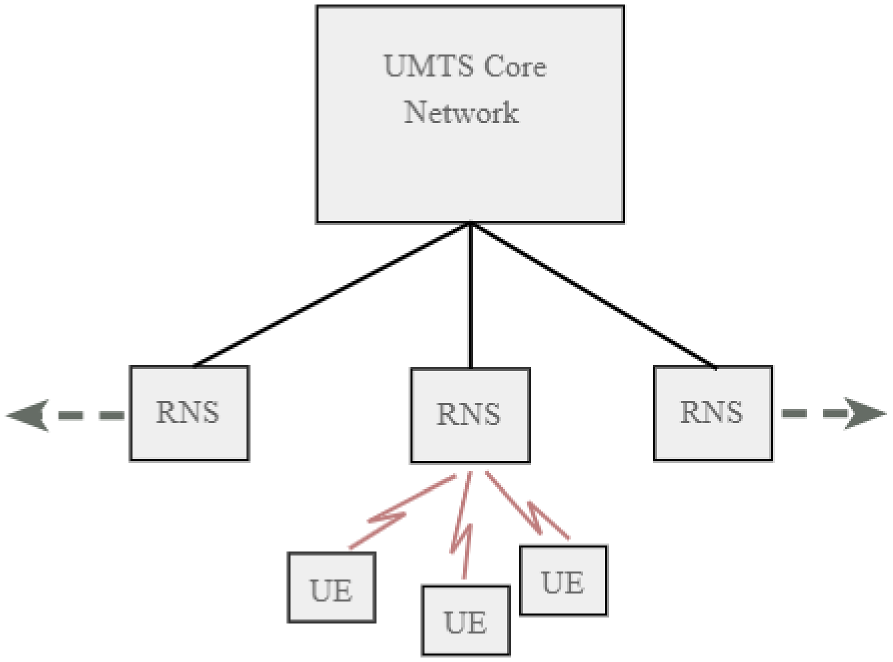


Fig 4.2 The Main UMTS network blocks

The USER Equipment

The USER Equipment or UE is a major element of the overall 3G UMTS network architecture. It forms the final interface with the user. In view of the far greater number of applications and facilities that it can perform, the decision was made to call it a user equipment rather than a mobile. However it is essentially the handset (in the broadest terminology), although having access to much higher speed data communications, it can be much more versatile, containing many more applications. It consists of a variety of different elements including RF circuitry, processing, antenna, battery, etc.

There are a number of elements within the UE that can be described separately:

RF circuitry: The RF areas handle all elements of the signal, both for the receiver and for the transmitter. One of the major challenges for the RF power amplifier was to reduce the power consumption. The form of modulation used for W-CDMA requires the use of a linear amplifier. These inherently take more current than non linear amplifiers which can be used for the form of modulation used on GSM. Accordingly to maintain battery life, measures were introduced into many of the designs to ensure the optimum efficiency.

Baseband processing: The base-band signal processing consists mainly of digital circuitry. This is considerably more complicated than that used in phones for previous generations. Again this has been optimised to reduce the current consumption as far as possible.

Battery: While current consumption has been minimised as far as possible within the circuitry of the phone, there has been an increase in current drain on the battery. With users expecting the same lifetime between charging batteries as experienced on the previous generation phones, this has necessitated the use of new and improved battery technology. Now Lithium Ion (Li-ion) batteries are used. These phones to remain small and relatively light while still retaining or even improving the overall life between charges.

Universal Subscriber Identity Module, USIM: The UE also contains a SIM card, although in the case of UMTS it is termed a USIM (Universal Subscriber Identity Module). This is a more advanced version of the SIM card used in GSM and other systems, but embodies the same types of information. It contains the International Mobile Subscriber Identity number (IMSI) as well as the Mobile Station International ISDN Number (MSISDN). Other information that the USIM holds includes the preferred language to enable the correct language information to be displayed, especially when roaming, and a list of preferred and prohibited Public Land Mobile Networks (PLMN).

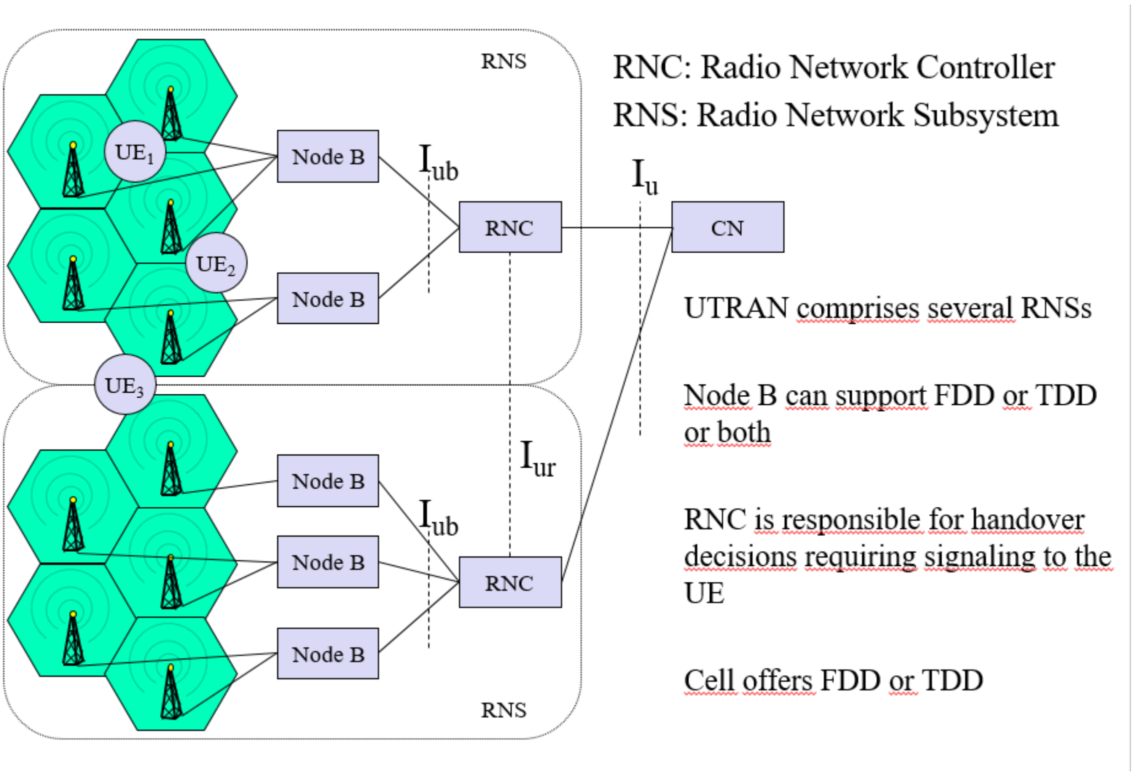
The USIM also contains a short message storage area that allows messages to stay with the user even when the phone is changed. Similarly "phone book" numbers and call information of the numbers of incoming and outgoing calls are stored.

The UE can take a variety of forms, although the most common format is still a version of a "mobile phone" although having many data capabilities. Other broadband dongles are also being widely used.

4.3.2 3G UMTS Radio Network Subsystem

This is the section of the 3G UMTS / WCDMA network that interfaces to both the UE and the core network. The overall radio access network, i.e. collectively all the Radio Network Subsystem is known as the UTRAN UMTS Radio Access Network.

The radio network subsystem is also known as the UMTS Radio Access Network or UTRAN.



RNC: Radio Network Controller

RNS: Radio Network Subsystem

UTRAN comprises several RNSs

Node B can support FDD or TDD or both

RNC is responsible for handover decisions requiring signaling to the UE

Cell offers FDD or TDD

Fig 4.3 3G UMTS Core Network

The 3G UMTS core network architecture is a migration of that used for GSM with further elements overlaid to enable the additional functionality demanded by UMTS.

In view of the different ways in which data may be carried, the UMTS core network may be split into two different areas:

Circuit switched elements: These elements are primarily based on the GSM network entities and carry data in a circuit switched manner, i.e. a permanent channel for the duration of the call.

Packet switched elements: These network entities are designed to carry packet data. This enables much higher network usage as the capacity can be shared and data is carried as packets which are routed according to their destination.

Some network elements, particularly those that are associated with registration are shared by both domains and operate in the same way that they did with GSM.

The Core Network (CN) and the Interface I_u, are separated into two logical domains:

❑Circuit Switched Domain (CSD)

- Circuit switched service incl. signaling
- Resource reservation at connection setup
- GSM components (MSC, GMSC, VLR)
- I_uCS

❑Packet Switched Domain (PSD)

- GPRS components (SGSN, GGSN)
- I_uPS

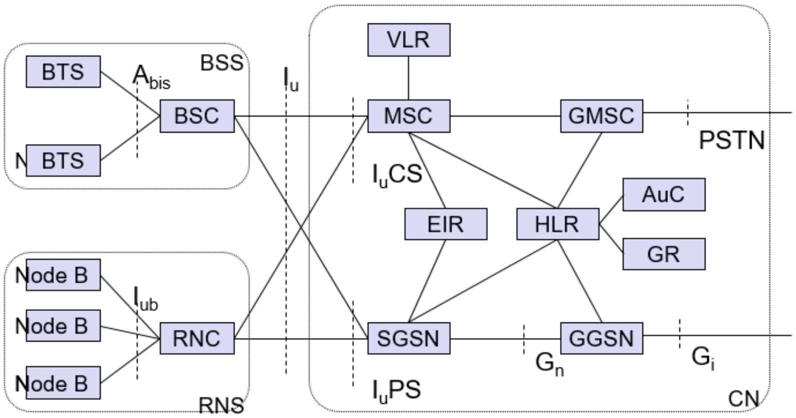


Fig 4.4 The core network and the Interfaces

UMTS Network Architecture Overview

Circuit switched elements

The circuit switched elements of the UMTS core network architecture include the following network entities:

Mobile switching centre (MSC): This is essentially the same as that within GSM, and it manages the circuit switched calls under way.

Gateway MSC (GMSC): This is effectively the interface to the external networks.

Packet switched elements

The packet switched elements of the 3G UMTS core network architecture include the following network entities:

Serving GPRS Support Node (SGSN): As the name implies, this entity was first developed when GPRS was introduced, and its use has been carried over into the UMTS network architecture. The SGSN provides a number of functions within the UMTS network architecture.

Mobility management When a UE attaches to the Packet Switched domain of the UMTS Core Network, the SGSN generates MM information based on the mobile's current location.

Session management: The SGSN manages the data sessions providing the required quality of service and also managing what are termed the PDP (Packet data Protocol) contexts, i.e. the pipes over which the data is sent.

Interaction with other areas of the network: The SGSN is able to manage its elements within the network only by communicating with other areas of the network, e.g. MSC and other circuit switched areas.

Billing: The SGSN is also responsible billing. It achieves this by monitoring the flow of user data across the GPRS network. CDRs (Call Detail Records) are generated by the SGSN before being transferred to the charging entities (Charging Gateway Function, CGF).

Gateway GPRS Support Node (GGSN): Like the SGSN, this entity was also first introduced into the GPRS network. The Gateway GPRS Support Node (GGSN) is the central element within the UMTS packet switched network. It handles inter-working between the UMTS packet switched network and external packet switched networks, and can be considered as a very sophisticated router. In operation, when the GGSN receives data addressed to a specific user, it checks if the user is active and then forwards the data to the SGSN serving the particular UE.

Shared elements

The shared elements of the 3G UMTS core network architecture include the following network entities:

Home location register (HLR): This database contains all the administrative information about each subscriber along with their last known location. In this way, the UMTS network is able to route calls to the relevant RNC / Node B. When a user switches on their UE, it registers with the network and from this it is possible to determine which Node B it communicates with so that incoming calls can be routed appropriately. Even when the UE is not active (but switched on) it re-registers periodically to ensure that the network (HLR) is aware of its latest position with their current or last known location on the network.

Equipment identity register (EIR): The EIR is the entity that decides whether a given UE equipment may be allowed onto the network. Each UE equipment has a number known as the International Mobile Equipment Identity. This number, as mentioned above, is installed in the equipment and is checked by the network during registration.

Authentication centre (AuC) : The AuC is a protected database that contains the secret key also contained in the user's USIM card.

4.3.3 UMTS radio access network, UTRAN

The UMTS Radio Access Network, UTRAN, or Radio Network Subsystem, RNS comprises two main components:

Radio Network Controller, RNC: This element of the UTRAN / radio network subsystem controls the Node Bs that are connected to it, i.e. the radio resources in its domain.. The RNC undertakes the radio resource management and some of the mobility management functions, although not all. It is also the point at which the data encryption / decryption is performed to protect the user data from eavesdropping.

- Node B: Node B is the term used within UMTS to denote the base station transceiver. This part of the UTRAN contains the transmitter and receiver to communicate with the UEs within the cell. It participates with the RNC in the resource management. NodeB is the 3GPP term for base station, and often the terms are used interchangeably.

In order to facilitate effective handover between Node Bs under the control of different RNCs, the RNC not only communicates with the Core Network, but also with neighbouring RNCs.

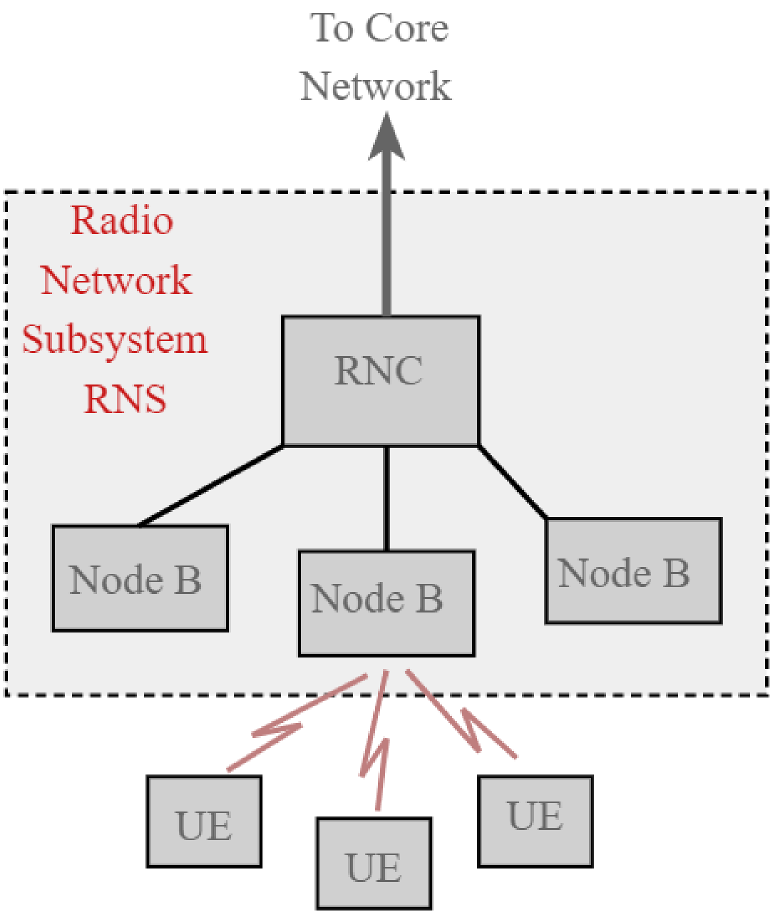


Fig 4.5 Architecture of the UMTS radio network subsystem, RNS

4.3.4 UTRAN / RNS interfaces

The UMTS standards are structured in a way that the internal functionality of the different network elements is not defined. Instead, the interfaces between the network elements is defined and in this way, so too is the element functionality.

There are several interfaces that are defined for the UTRAN elements:

- Iu : The Iu interface connects the UTRAN to the core network.
- Iub : The Iub connects the NodeB and the RNC within the UTRAN. Although when it was launched, a standardisation of the interface between the controller and base station in the UTRAN was revolutionary, the aim was to stimulate competition between suppliers, allowing opportunities like some manufacturers who might concentrate just on base stations rather than the controller and other network entities.
- Iur : The Iur interface allows communication between different RNCs within the UTRAN. The open Iur interface enables capabilities like soft handover to occur as well as helping to stimulate competition between equipment manufacturers.

Having standardised interfaces within various areas of the network including the UTRAN allows network operators to select different network entities from different suppliers.

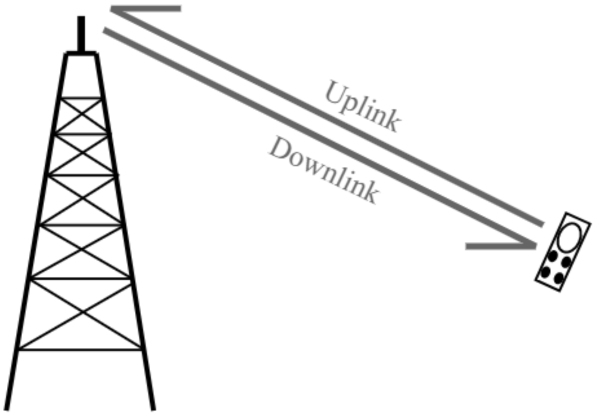
4.3.5 UTRA uplink & downlink

When looking at the radio air interface and its associated properties, it is necessary to define the directions in which the transmissions are occurring. Being a full duplex system, i.e.

transmitting simultaneously in both directions, it is necessary to be able to define which direction is which.

- Downlink; This may also sometimes be known as the forward link, and it is the link from the Node B or base station to the User Equipment (UE).
- Uplink; This may also sometimes be known as the reverse link, and it is the link from the User Equipment (UE) to the Node B or base station.

The terms Uplink and Downlink are the terms that are used with UMTS, and especially within Europe. The terms forward link and reverse link are more commonly used with the CDMA2000 technologies and also within North America.



Uplink and downlink directions

Fig 4.6 Uplink and downlink

4.3.6 Frequency division and time division duplex

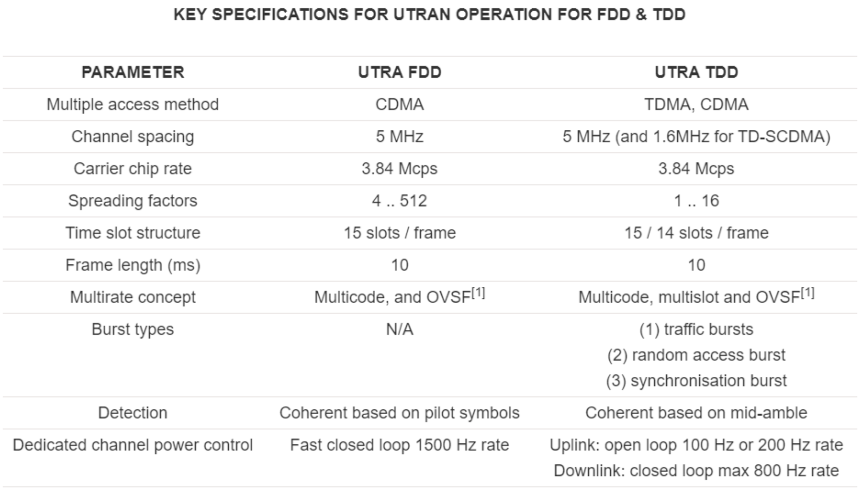
In view of the fact that transmissions have to be made in both directions, i.e. in both uplink and downlink. It is necessary to organise the way these transmissions are made. Two techniques are used to ensure concurrent or near concurrent transmissions in both directions: frequency division duplex and time division duplex.

- UTRA-FDD: The frequency division duplex version of UTRA uses a scheme whereby transmissions in the uplink and downlink occur on different frequencies. Although this requires double the bandwidth to accommodate the two transmissions, and filters to prevent the transmitted signal from interfering with the receiver. Even though there is a defined split between uplink and downlink, effective filters are required.
- UTRA-TDD: The time division version of the UTRA uses uplink and downlink transmissions that use the same frequency but are timed to occur at different intervals.

Both UTRA-FDD and UTRA-TDD have their own advantages and disadvantages and therefore tend to be used in different areas.

While the UTRA-FDD and UTRA-TDD both belong to 3G UMTS and are contained within the 3GPP standards, they may have some slightly different parameters for their transmissions.

Table 4.1 Specifications for UTRAN



KEY SPECIFICATIONS FOR UTRAN OPERATION FOR FDD & TDD

PARAMETER	UTRA FDD	UTRA TDD
Multiple access method	CDMA	TDMA, CDMA
Channel spacing	5 MHz	5 MHz (and 1.6MHz for TD-SCDMA)
Carrier chip rate	3.84 Mcps	3.84 Mcps
Spreading factors	4 .. 512	1 .. 16
Time slot structure	15 slots / frame	15 / 14 slots / frame
Frame length (ms)	10	10
Multirate concept	Multicode, and OVSF[1]	Multicode, multislot and OVSF[1]
Burst types	N/A	(1) traffic bursts (2) random access burst (3) synchronisation burst
Detection	Coherent based on pilot symbols	Coherent based on mid-amble
Dedicated channel power control	Fast closed loop 1500 Hz rate	Uplink: open loop 100 Hz or 200 Hz rate Downlink: closed loop max 800 Hz rate

.

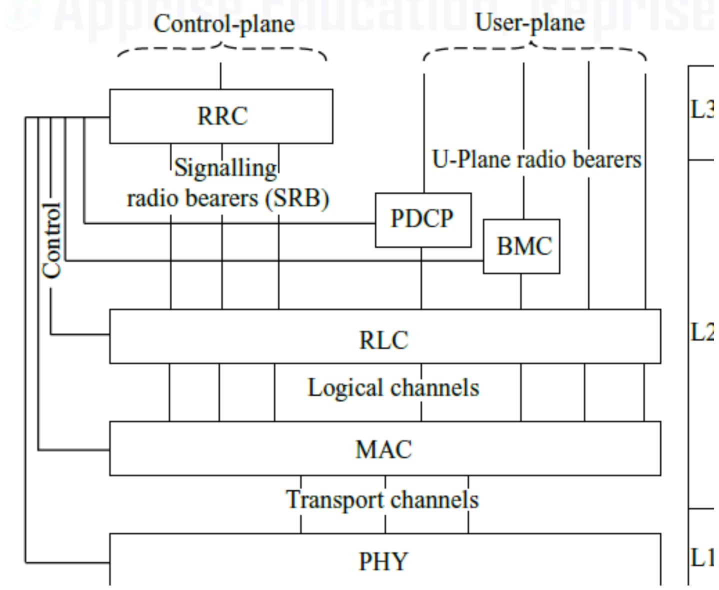


Fig 4.7 UTRA-FDD Radio Interface protocol architecture.

The physical layer offers services to the MAClayer via transport channels.

In the physical layer, the design is to how and with what characters the data is transferred. The logical channels are characterized by what type of data is transmitted. MAC layer offers services to the RLC layer by means of logical channels. RLC layer offers service to higher layers. On the control plane, the RRC layer for signaling transport takes the RLC services. On the user plan, the RLC services are taken either by the service (specific protocol layers PDCP or BMC) or by other high-layer u-plane functions (e.g., speech coder) shown in the WCDMA radio interface protocol architecture in Fig. 4.7.

The two protocols:

1. The PDCP (Packet Data Convergence Protocol) is used for packet switches service, and its main function is the harder compression.

2. The BMC (Broadcast Multicast Control Protocol) is used to convey the radio interface messages originating from cell broadcast center.

The service offered by both protocols is called Radio Bearer.
The RRC layer offers services to higher layers through access points. The entire higher layer signaling such as mobility management, call control, session management, and so forth is placed into RRC messages for transmission over the radio interface. The control interfaces between the RRC and all the lower layer protocols are used to command the lower layers to perform certain types of measurements and to report measurement results and errors to the RRC. There are three types of channels transmitting information between layers; physical channels, transport channels, and logical channels. Those types of channels **perform their unique operations.**

4.3.7 MAC Layer

Logical Channels. As mentioned earlier, the transport channels convey information passed from the MAC layer to the PHY layer. However, the information can originate higher in the protocol stack and is conveyed from RLC layer to the MAC layer through the logical channels. Therefore, the logical channels are mapped to transport channels, which in turn are mapped to physical channels.
The data transfer services of the MAC layer are provided on logical channels. There are different kinds of data transfer services offered by MAC. Logical channels can be classified into two groups: control channels and traffic channels. The MAC layer architecture is shown in Fig. 4.8. MAC-b handles the broadcast channel (BCH). MACc/sh handles the common channels and shared channels. MAC-d handles dedicated channels.

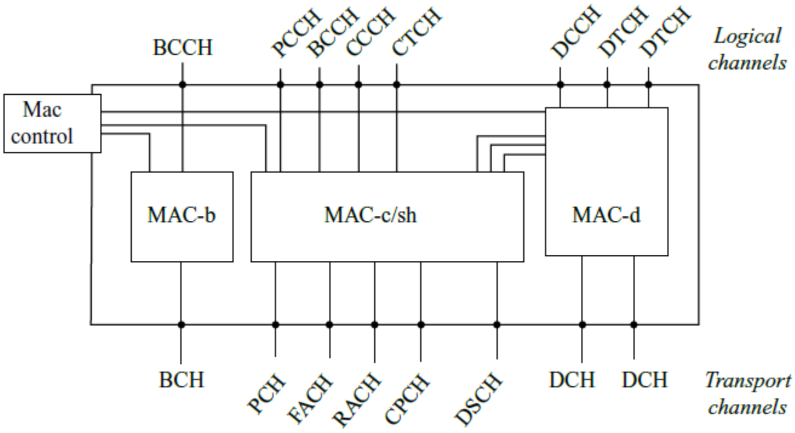


Fig 4.8 MAC Layer architecture

The control channels are

BCCH (Broadcast Control Channel [DL]): Transmits system information.
PCCH (Paging Control Channel [DL]): Pages an MS across one or more cells.
DCCH (Dedicated Control Channel [DL and UL]): A bidirectional point-to-point between an MS and the RNC for sending control information.
CCCH (Common Control Channel [DL and UL])
1. Used for the uplink by MS that wants to access the network but do not already have any connection with the network.
2. Used for the downlink to respond to such access attempts.
B. The traffic channels are
DTCH (Dedicated Traffic Channel [UL and DL]): A bidirectional point-to-point channel, dedicated to one MS, for the transfer of user information.
CTCH (Common Traffic Channel [DL]): A point-to-multipoint downlink channel for transfer of user information for all or a group of specified MS.
C. Mapping between logical channels and transport channels is shown in Fig. 4.9. On the uplink side, three logical channels are mapped to three transport channels. On the downlink side, five logical channels are mapped to five transport channels. The mapping is based on the operation of the MAC layer and shows the MAC functions when data is processed through the layer.

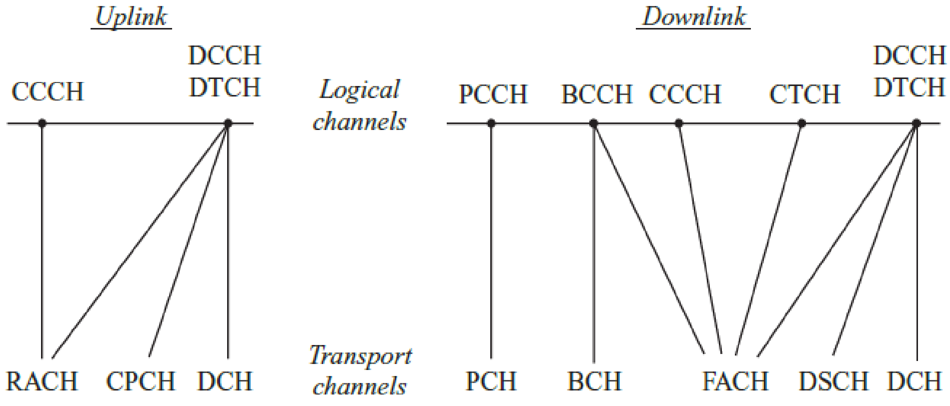


Fig 4.9 Mapping between logical channels and transport channels, uplink and downlink directions.

4.3.7.1 MAC Functions.

MAC layer is a layer between PHY layer and RLC layer, therefore, the information conveys to PHY layer through transport channels and conveys to RLC layer through logical channels. The functions of MAC layer are
1. Handling the data flows in one MS and between MSs with priority and dynamic scheduling.
2. Identifying MSs in the MAC header on common transport channels.
3. Handling service multiplexing and de-multiplexing of higher layer PDUs for common transport channels and dedicated transport channels.
4. Monitoring traffic volume in RLC transmission buffer. Also provides traffic status to

RRC.
5. Switching between common and dedicated transport channels based on a switching decision from RRC.
6. Ciphering is performed if a radio bearer is using transparent RLC mode.
7. Use different access service classes (ASC) to provide different priorities ofRACHusage.

4.3.8 RLC Layer

A. RLC layer architecture

The RLC layer architecture is showing Fig. 4.10. The three RLC entity types, transparent mode (Tr), acknowledged mode (AM), and unacknowledged mode (UM), are associated with its service access point (SAP). The transparent and unacknowledged modes of RLC are used as unidirectional; each one has transmitting and receiving entities. The acknowledged mode is bidirectional.

1. ***Transparent mode:*** No protocol overhead is added to higher layer area, thus the transmission can be of the streaming type in which higher layer data is not segmented.
2. ***Unacknowledged mode:*** No retransmission protocol is in use and data delivery is no guarantee of arrival. It is used for cell broadcast service and voice over IP (VoIP).
3. ***Acknowledged modes:*** An automatic repeat request (ARQ) scheme is used for error correction. The quality versus delay performance of RLC can be controlled by RRC. The acknowledged mode is the normal RLC mode for packet type services, such as Internet browsing and e-mail downloading.

B.RLC Functions

The RLC functions are most related to the quality of link connections.

1. Segmentation and reassembly of variable-length higher layer PDUs into or from smaller RLC payload units (PUs).
2. Concatenation and Padding: in case the contents of an RLCSDUdo not fill an integral number of RLC PUs. When concatenation is not applicable, the remaining data is filled with padding bits.
3. Transfer of user data is controlled by QoS setting. The error correction by retransmission is in the acknowledged data transfer mode.
4. Delivery of higher layer PDUs in sequence by RLC using the acknowledged data transfer service and has duplication detection.
5. Detects and recovers from errors in the operation of the RLC protocol.
6. Using the same ciphering algorithm as MAC layer ciphering.
7. Suspensions and resumptions are local operations at RLC but commanded by RRC via the control interface.

4.3.9 RRC Layer

A. Architecture

RRC layer handles the main part of control signaling between MS and RAN. RRC messages carry all parameters required to set up, modify, and release MAC layer and

PHY layer protocol entities. The RRC layer architecture is shown in Fig. 6.19. There are four functional entities:

1. ***DCFE (Dedicated Control Functional Entity):*** Handles all functions and signaling specific to one MS. DCFE can utilize services from all SRB (see Fig. 6.14).
2. ***PNFE (Paging and Notification control Function Entity):*** Handles paging of idle mode in MS.
3. ***BCFE (Broadcast Control Function Entity):*** Handles the system information broadcasting.
4. ***RFE (Routing Function Entity):*** The routing of higher layer messages to different MM/CM entities on MS side or different core network domain on the RAN side.

B. RRC Functions

1. Broadcast of system information, paging, and initial call selection and reselection in idle mode.
2. Establishment, maintenance, and release of an RRC connection between MS and RAN in connected mode.
3. Control of Radio Bearers, transport channels, physical channels, and security functions.
4. Connection of mobility functions, MS positioning function, reception of MS measurement reporting, and support for DL open loop power control and outer loop power control in MS.
5. Cell broadcast service related functions.

4.4 Overview of 3GPP Release 99 Network

General Description.

In 3GPP terminology, Mobile Equipment (ME) is the radio terminal used for radio communication. The User Equipment (UE) contains ME and the UMTS Subscriber Identity Module (USIM). USIM is a chip that contains some subscription-related information, plus security keys. UE is also called Mobile Station (MS).

The network architecture for 3GPP Release 99 is shown in Fig. 4.10. The interface between the UE and the Node B is called Uu. Node B is named for BTS in 3GPP specification. The interface between Node B and RNC is called Iub. RNC is analogous to a BSC in GSM.

Combining an RNC and many Node Bs is called Radio Network Subsystem (RNS).

An interface between the RNCs is called Iur.

The primary purpose of this interface Iur is to support inter-RNC mobility and soft handover between Node Bs and different RNCs.An interface between RNC and the core network is called Iu. Iu interface has two different components. The interface between RNC and a single MSC/VLR is called Iu-CS. CS stands for Circuit Switched. The interface betweenRNCand SGSN (Serving GPRS Support Node) is called Iu-ps. PS stands for Packet switched.

In all the interfaces in the UTRAN of 3GPP Release 99 are based on Asynchronous Transfer Mode (ATM). ATM was chosen because it can support a valuable bit rate for packet-switched services and a constant bit rate for circuit-switched services. In Fig. 4.10 is the possibility for an existing core network such as GPRS to be upgraded to support UTRAN. A MSC could connect to both a GSM
BSC and a UTRAN RNC.

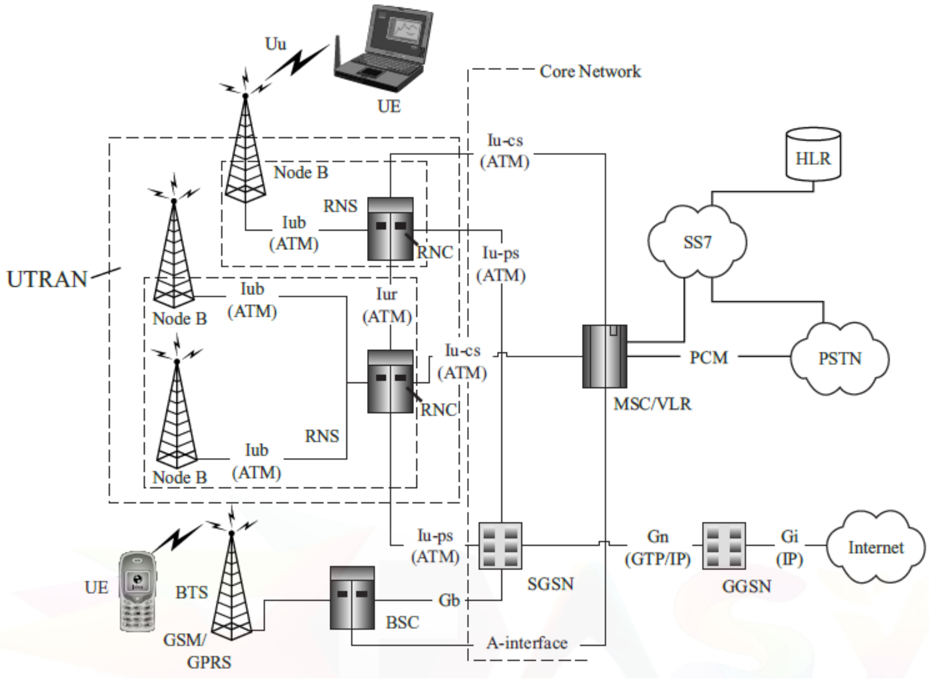


Fig 4.10 3GPP Release 1999 network architecture.

The radio access network (RAN) of WCDMA is known as UTRAN (UMTS Terrestrial Radio Access Network). A UTRAN consists of several RNSs illustrated in the ultimate

UTRAN architecture diagram shown in Fig. 4.11.

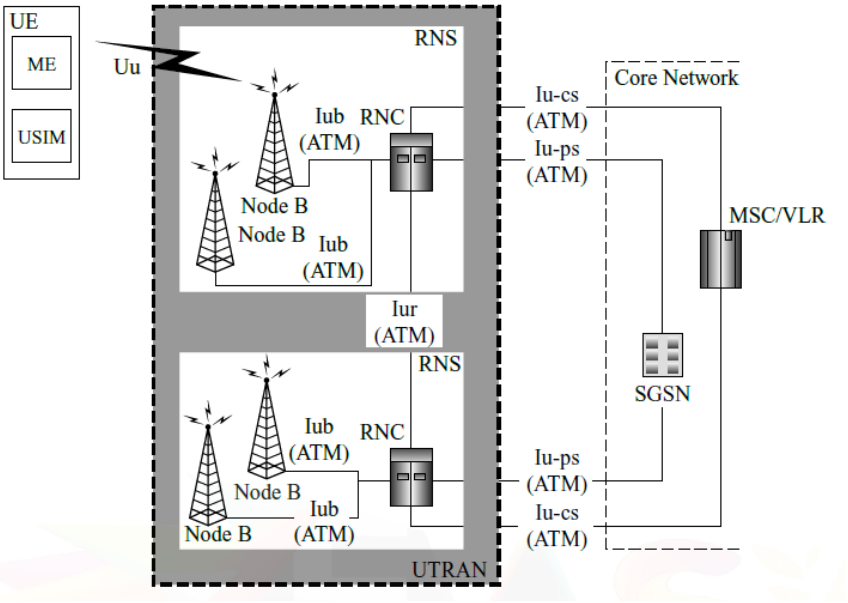


Fig 4.11 UTARN Architecture

Role of the RNC

A. The RNC controlling one or several Node Bs through Iub interfaces is called controlling RNC (CRNC) of the Node B. CRNC is responsible for the load and congestion control of its own cells, also for the allocation for new radio links to be established in those cells.

B. RNC as two logical roles with respect to the ME and UTRAN connections as shown in Fig. 4.12

1. Serving RNC (SRNC): One UE connected to UTRAN through only one SRNC. Basic Radio Resource Management (RRM) operations are executed in SRNC, such as the handover decision, and outer loop power control.

2. Drift RNC (DRNC): Can be any RNC other than the SRNC. It controls cells used by the mobile. One UE may have zero, one, or more DRNCs.

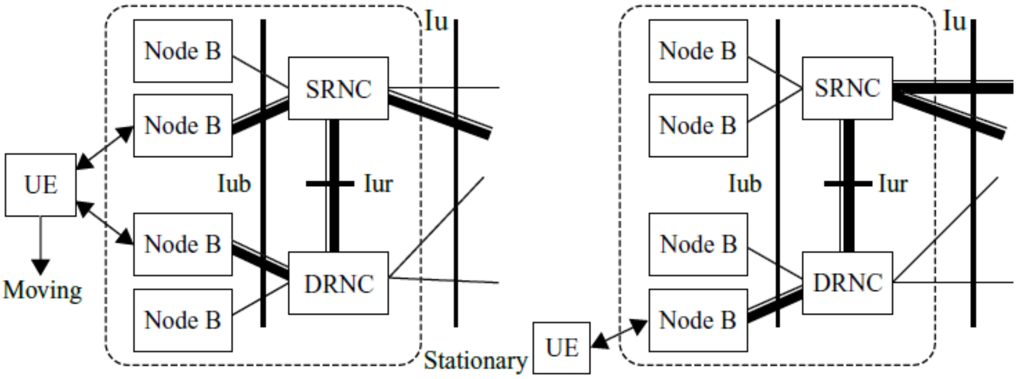


Fig 4.12Logical role of the RNC for one UE UTRAN connection. The left-hand scenario shows one UE in inter-RNC soft handover (combining is performed in the SRNC). The right-hand scenario represents one UE using resources from one Node B only, controlled by the DRNC.

A Generic Model for UTRAN Interfaces.19 All the interfaces, such as Iu-CS, Iu-PS, Iur, and Iub interfaces, have two main components; the radio network layer and the transport network layer, as shown in Fig. 4.13 . The radio network layer represents the application information (user data or control information) to be carried. The transport network layer represents the transport technology (ATM transport or others). The transport network layer could be different, but the radio network layer should be kept as no difference.

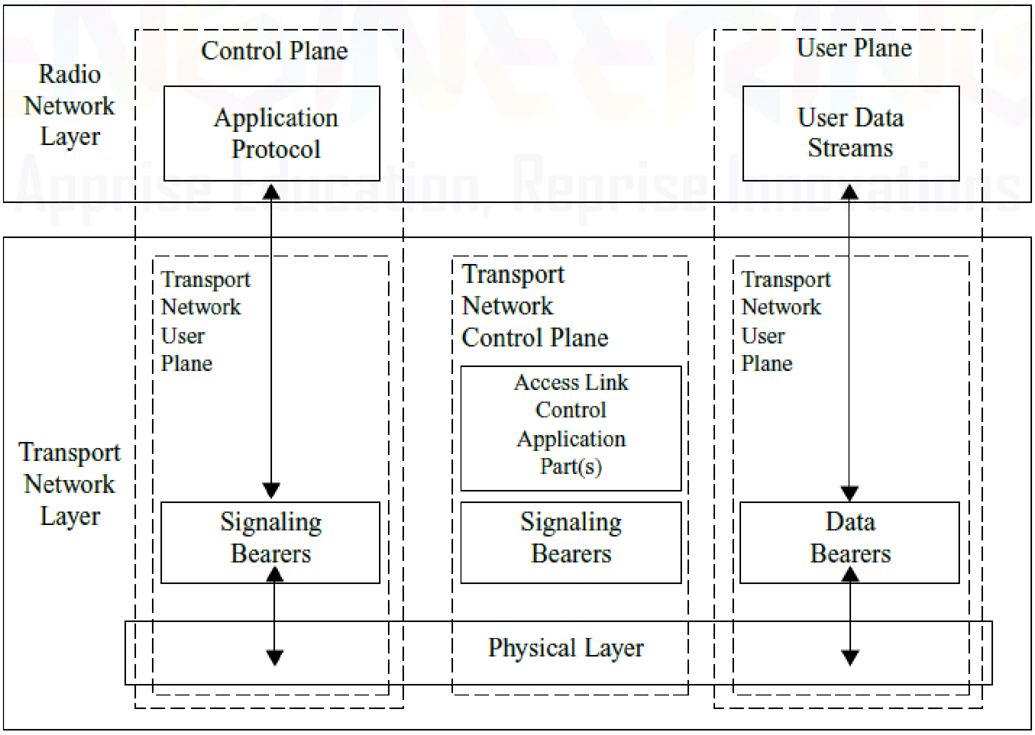
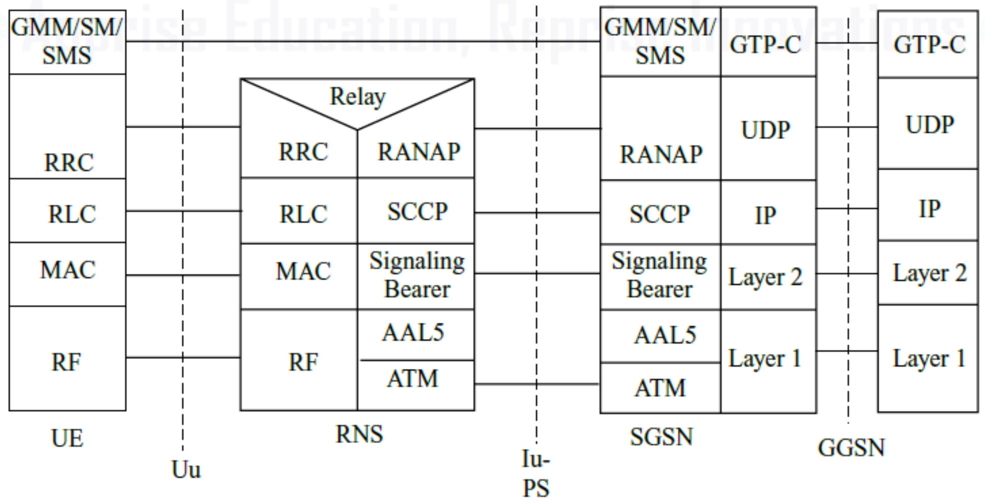


Fig 4.13 Generic model for UTRAN terrestrial interfaces.

in the vertical domain, there are three planes: the control plane,
the user plane, and the transport network user plane.
1. The control plane is used by control signaling, including the application protocol for establishing the bearers, which is transport user data, but the user data itself is carried on the user plane. The signaling bearers that carry the application signaling are analogous to the SS7 signaling links that are used between BSC and MSC in GSM.
2. The user plane is carrying the actual user data. The data packets are sent or received by the UE as part of a data session.
3. The transport network control plane contains functionality that is specific to the transport technology being used. It is not visible to the radio network layer. It involves the use of an Access Link Control Application Part (ALCAP). It is a generic term that describes a protocol or a set of protocols used to set up a transport bearer.

UMTS Packet Data Sessions. The packet data services used in Release 99 architecture as shown in Fig. 4.10 is largely the same mechanisms as used for GPRS data.
The Gb interface of GPRS is replaced by the Iu-PS interface, which uses RAN Application Part (RANAP) as the application protocol. The IP over ATM is used between the SGSN and RNC. Thus an IP network is set up from GGSN to SGSN to RNC. The GTP-C (GPRS – Tunneling Protocol in Control plane) starts at GGSN and terminates at the SGSN shown in Fig. 4.14. It is because the application protocol between RNC and SGSN is RANAP rather than GTP. The GTP-U tunnel in the user plane can be relayed from the GGSN through the SGSN to the RNC.

From an interface perspective, UMTS provides greater flexibility than GPRS in terms of allocation of resources for packet data traffic. The UMTS can offer a greater range of data speeds and also provides a selection of different channel types of air interface for packet data. In the uplink, theRACH, CPCH, andDCHare available, and in the downlink, the DCH, FACH, and DSCH are available. RNC controls the choice of channels to be used depending on the characteristics of session required by the user, such as high-volume streaming versus low-volume bursting traffic.



UMTS GPRS Control Plane UE to SGSN to GGSN

Fig 4.14 UMTS GPRS control plane protocol stacks.

4.5 *cdma2000 PHYSICAL LAYER*

Cdma2000 is an evaluation of cdmaOne, which extrapolates the air interface specification of IS-95 to meet the requirement for IMT-2000 as one among the third generation of cellular systems. cdma2000 supports backward compatibility with IS-95.
The physical layer is responsible for:
1. Transmitting and receiving bits over the physical medium, which is the air. The bits have to convert into waveforms by modulation.
2. Carrying out coding functions to perform error control functions at the bit and frame levels.

Cdma2000 accepts both signal carrier and multiple carrier implementations. It also has proposed two kinds of multiplexing: FDD and TDD. The physical layer channels for both FDD and TDD are the same. However, FDD is first to implement. Physical channels are distinguished in two groups: dedicated and common channels.

Physical Channels

Physical channels are distinguished in two groups: dedicated and common channel.

A. Dedicated Physical Channel (DPHCH)

1. Forward Dedicated Physical Channel (F-DPHCH): There are four dedicated channels.

- Fundamental channel (F-FCH): Provides for transportation of dedicated data.
- Supplemental Channel (F-SCH): Allocated dynamically to supply a required data rate.
- Dedicated Control Channel (F-DCCH): Used to transport mobile-specific control information.
- Dedicated Auxiliary Pilot Channel (F-DAPICH): Used with antenna beam-forming and beam-steering to increase coverage or data rate of a desired user. This channel is optional.

2. Reversed Dedicated Physical Channel (R-DPHCH): There are three dedicated channels.

- Fundamental Channel (R-FCH): Same function as F-FCH.
- Supplemental Channel (R-SCH): Same function as F-SCH channel.
- Dedicated Control Channel (R-DCCH)

B. Common Physical Channel (CPHCH)

1. Forward Common Physical Channel (F-CPHCH)

- Pilot Channel (F-PICH): Carries the Pilot symbol and provides capabilities for channel estimation and coherent detection and soft handoff.
- Common Auxiliary Pilot Channel (F-CAPICH): Provides a fine-tuning on coherent detection and soft handoff.
- Sync Channel (F-SYNC): Provides the mobile station with system information and synchronization.
- Common Assignment Channel (F-CACH): Support the reservation access mode on the R-EACH (Enhanced Access Channel). The message that assigns the R-CCCH is transmitted on the F-CACH.

- Paging Channel (F-PCH): It can enable paging functions, also provides a means for short burst data communications. Each mobile is assigned an 80-ms slot and decodes periodically to receive page messages. Two channels F-BCCH and F-CCCH can substitute it.
- Broadcast Control Channel (F-BCCH): Serves to broadcast system–specific and cell-specific overhead information.
- Common Control Channel (F-CCCH): It provides a means for paging functions and support different data rates for short burst data communications.

The F-BCCH and F-CCCH do not have to operate at the same data rates and the same power level.

- Quick Paging Channel (F-QPCH): The idea of having F-QPCH is to decrease the time and mobile station needs to monitor the F-PCH or F-CCCH. The period at which the mobile station must decide F-PCH or F-CCCH as short as 1.28 ms.
- Common Power-Control Channel (F-CPCCH): Serves two purposes:

a. To allowpower control of the R-CCH and R-PICHworks during the reservation access.

b. To control the R-PICH when the mobile station is in the traffic state.

- Packet Data Control (F-PDCH): A shared packet data channel that supports highspeed operation traffic. Access to this channel is handled through MAC layer scheduling.

2. Reverse Common Physical Channel

- Access Channel (R-ACH): Used for mobile stations communications messages to the base station for backward compatibility reasons.
- Common Control Channel (R-CCCH): To transport control information.
- Enhanced Access Channel (R-EACH): An enhanced access product relative to that of the R-ACH.
- Dedicated Control Channel (R-DCCH): Same function as F-DCCH.
- Pilot Channel (R-PICH): Provides the signal for coherent detection.
- Channel Quality Indicator Channel (R-CQICH): A support channel for adoptive coding and modulation over the F-PDCH.
- Acknowledgment Channel (R-ACKCH): Check whether the CRC of the decoded packet has passed or failed.

Radio Interface Parameters of cdma2000 FDD

The radio interface parameters of cdma2000 are similar to IS-95.

A. Channel Structure

After the physical channel generates a frame, then the physical layer performs the same functions as does in IS-95.

_ Adding the CRC bits for detecting frame errors

_ Coding the FEC bits

_ Interleaving for combating the long term fading

The final data stream as input {di} goes through single carrier forward link radio access shown in Fig. 6.32.

B. Chip Rates: cdma2000 supports a range of chip rates; all can be expressed by: N ×1.2288 Mcps, N = 1, 3, 6, 9, 12. When N > 1, there are two ways by which cdma2000 can spread the signal. The first one, Multicarrier, basically de-multiplexes the message signal into N information signals and spreads each of those on a different carrier, at a chip rate of 1.2288 Mcps. The second one, Direct Spread, simply spreads the message signal directly with a chip rate of N × 1.2288 Mcps. In the Multicarrier mode, each carrier has an IS-95 signal format.

The two methods are illustrated next.

C. Modulation and Spreading

1. For Single Carrier

a. Forward Link

Figure 6.32 illustrates the modulation and spreading process for forward-link, single carrier of cdma2000. The input consists of a single channel that is already coded, punctured, and interleaved according to the cdma2000 specifications. Each channel has different possible configurations, but the modulation and spreading process is the same for all channels.

First, a long PN code scrambles the channel. The rate of the scrambling code depends on the code rate of the input. Only the PCH, DCCH, FCH, and SCH are scrambled.

Then the MUX maps the codes to polar form, transfers the serial data to parallel, and also provides the possibility of puncturing the data stream, to insert a bit of power control (indicated by the Bit Sel. Box).

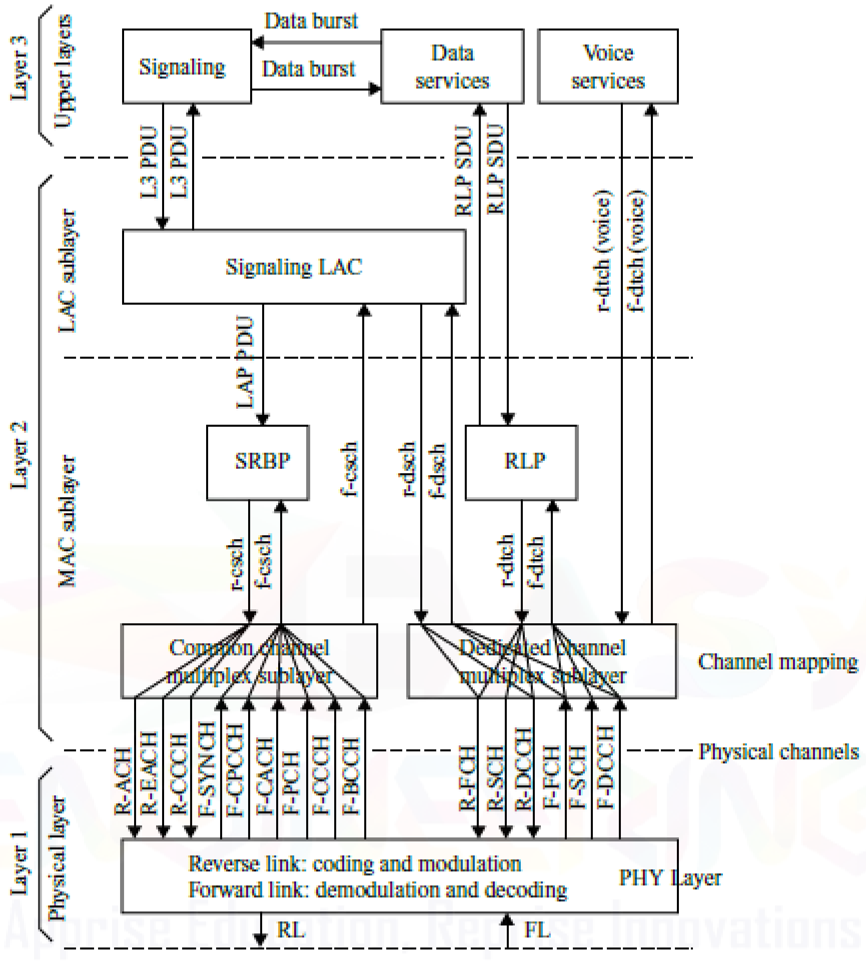
cdma2000 NETWORK

In cdma2000, four different protocol layers are specified:
1. Physical (Layer 1)
2. MAC sublayer (Layer 2) for controlling higher layers' access to the physical medium.
3. Link access control (LAC) sublayer (Layer 2) for responding to the reliability of signaling.
4. Upper layer (Layer 3) for an overall control of the cdma2000 system.

MAC Sublayer

A. Four Entities

In the MAC sublayer, there are four different entities: Radio Link Protocol (RLP),Signaling Radio Burst Protocol (SRBP), Common Channel Multiplex Sublayer, and Dedicated Channel Multiplex Sublayer



Dedicated Channel Multiplex Sublayer.

_ The Signaling Radio Burst Protocol (SRBP) handles common-channel signaling using radio burst techniques. The SRBP is performing in the Common Channel Multiplex Sublayer.

_ The Common Channel Multiplex Sublayer performs the mapping between the logical common channels (i.e., those channels are shared among multiple users) and the physical common channels.
_ Dedicated channel multiplex sublayer performs the mapping between the logical dedicated channels (i.e., those channels are dedicated to specific users) and the physical dedicated channels.
The primary function of theMACsublayer is to multiplex logical channels onto different physical channels before sending and to de-multiplex physical channels into different logical channel after receiving. The two multiplex sublayers of the MAC as mentioned above handle these two functions.
The dedicated channels can be used for both signaling and user data; common channels are only used for signaling. The same arrangement of channels appears inWCDMA. However, the transport channels used in WCDMA for exchanging information between physical layer and logical channels replay MAC layer directly as a means to exchange information between Layer 1 and Layer 2.

Primitives
The messages sending and receiving between layers/sublayers are primitives, a form of these communication messages. Two widely used types of primitives are _ Request primitives: A service requester (MS) uses request primitives to request a service or a resource.
_ Indication primitives: A service provider uses indication primitives to indicate an event requested by service requester has occurred.
C. Logical Channels
The multiplex sublayers, both common channels and dedicated channels, are responsible for the mapping between logical channels and physical channels. The mapping between logical channels and physical channels on the forward link. and on the reverse link. The forward-dedicated traffic channel (F-DTCH) Logical Channel Data (common or dedicated) should be reliably delivered from end to end. In executing reliable delivery, the MAC sublayer assembles data received from higher layers and passes the assembled data to the physical layer for transmission.
The MAC sublayer also receives data from the physical layer, disassembles the data, and passes the disassembled data to higher layers. The mapping connections between logical channels and physical channels .
D. SDU (Service Data Unit)
On the transmit site, the MAC sublayer assembles data blocks received from a higher layer into an SDU and delivers the SDU to the physical layer for transmission. The MAC sublayer receives an SDU, disassembles the SDU into data blocks, and delivers them to higher layers. Adding one or more data blocks with a header can assemble another SDU. All SDUs can be sent either by common channels or dedicated channels.
E. Multiplex Sublayer’s Interaction
Multiplex sublayer can interact not only with physical layer (Layer 1) below, but can interact with four entities above it, RLP and Voice service on the dedicated channel side,LAC (Link Access protocol), and SRBP on the common channel side.

RLP Layer
RLP controls the process of user packet data that travels on dedicated user channels. The RLP is a Layer 2 protocol that responds for the delivery and receipt of user packet data. An important function of Layer 2 entity is to control packet errors introduced by the physical layer. There are several techniques to control packet errors.

1. Positive acknowledgment (ACK): Acknowledgment of receiving successfully.
2. Negative acknowledgment (NAK): Acknowledgment of receiving unsuccessfully.
3. Retransmission: Retransmit when neither an acknowledgment nor a NAK is received.

Other data link control protocols in Layer 2 are
1. Logical Link Control (LLC): for operating over a LAN using IEEE 802 standards.
2. Link Access Protocol: balanced for connecting a device to a packet switched network using the X.25 standard.
Three Classes of Frames in RLP
1. Control frames: carrying control information that have the highest priority.
2. Retransmitted data frames: retransmit the old data frames.
3. New data frame: transmit with the lowest priority.

PART –A

1. Signify IMT-2000
2. Discuss the importance of UTRA-FDD
3. Distinguish FDD and TDD in UTRA
4. List the components of UMTS.
5. Compare downlink and uplink functions
6. Mention some of the RRC functions
7. Distinguish the two logic domains in core network.
8. Discuss the MAC layer control channels
9. Infer any two interfaces in UTRAN.
10. Mention the shared elements in 3G cre network.

PART B

1. Discuss in detail about the UMTS architecture and its functions.
2. Ellobarate the RLC ,RRC functions
3. Explain about cdma 2000 and it architecture
4. Ellaborate in detail the 3GPP 99 functions with its architecture
5. Explain the core network in UTRA

TEXT BOOK / REFERENCE BOOKS

1. Andreas F. Molisch, “Wireless Communications”, 2nd Edition, John Wiley & Sons Ltd, 2011.
2. William C.Y. Lee., "Wireless & Cellular Telecommunications", 3rd edition, McGraw Hill.2006.
3. Yibing Lin, "Wireless & mobile Network architecture", Wiley 2002.
4. Tao Jiang, Lingyang Song and Van Zhang, “Orthogonal Frequency Division Multiple Access Fundamentals and
Applications” Taylor and Francis Group, 2010.
5. Yong Soo Cho, Jaekwon Kim, Won Young Yang and Chung G. Kang, “MIMO-OFDM Wireless Communications with
MATLAB”, John Wiley & Sons (Asia) Pvt. Ltd, 2010.

SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE
www.sathyabama.ac.in

SCHOOL OF ELECTRICAL AND ELECTRONICS

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

UNIT – V- WIRELESS COMMUNICATIONS – SEC1404

UNIT 5 B3G SYSTEMS

Features, operation and applications of Wi-Fi, WiMax, OFDM, OFDMA, OFDM-IDMA, MIMO, Cognitive Radio, LTE

WI-FI

WiFi stands for Wireless Fidelity. WiFiIt is based on the IEEE 802.11 family of standards and is primarily a local area networking (LAN) technology designed to provide in-building broadband coverage.

Current WiFi systems support a peak physical-layer data rate of 54 Mbps and typically provide indoor coverage over a distance of 100 feet.

WiFi has become the *de facto* standard for *last mile* broadband connectivity in homes, offices, and public hotspot locations. Systems can typically provide a coverage range of only about 1,000 feet from the access point.

WiFi offers remarkably higher peak data rates than do 3G systems, primarily since it operates over a larger 20 MHz bandwidth, but WiFiWiFi systems are not designed to support high-speed mobility.

One significant advantage of WiFi over WiMAX and 3G is its wide availability of terminal devices. A vast majority of laptops shipped today have a built-in WiFi interface. WiFi interfaces are now also being built into a variety of devices, including personal data assistants (PDAs), cordless phones, cellular phones, cameras, and media players.

WiFi is Half Duplex

All WiFi networks are contention-based TDD systems, where the access point and the mobile stations all vie for use of the same channel. Because of the shared media operation, all WiFi networks are half duplex.

There are equipment vendors who market WiFi mesh configurations, but those implementations incorporate technologies that are not defined in the standards.

Channel Bandwidth

The WiFi standards define a fixed channel bandwidth of 25 MHz for 802.11b and 20 MHz for either 802.11a or g networks.

Radio Signals

Radio Signals are the keys, which make WiFi networking possible. These radio signals transmitted from WiFi antennas are picked up by WiFi receivers, such as computers and cell phones that are equipped with WiFi cards. Whenever, a computer receives any of the signals within the range of a WiFi network, which is usually 300 — 500 feet for antennas, the WiFi card reads the signals and thus creates an internet connection between the user and the network without the use of a cord.

Access points, consisting of antennas and routers, are the main source that transmit and receive radio waves. Antennas work stronger and have a longer radio transmission with a radius of 300-500 feet, which are used in public areas while the weaker yet effective router is more suitable for homes with a radio transmission of 100-150 feet.

WiFi Cards

You can think of WiFi cards as being invisible cords that connect your computer to the antenna for a direct connection to the internet.

WiFi cards can be external or internal. If a WiFi card is not installed in your computer, then you may purchase a USB antenna attachment and have it externally connect to your USB port, or have an antenna-equipped expansion card installed directly to the computer (as shown in the figure given above). For laptops, this card will be a PCMCIA card which you insert to the PCMCIA slot on the laptop.

WiFi Hotspots

A WiFi hotspot is created by installing an access point to an internet connection. The access point transmits a wireless signal over a short distance. It typically covers around 300 feet. When a WiFi enabled device such as a Pocket PC encounters a hotspot, the device can then connect to that network wirelessly.

Most hotspots are located in places that are readily accessible to the public such as airports, coffee shops, hotels, book stores, and campus environments. 802.11b is the most common specification for hotspots worldwide. The 802.11g standard is backwards compatible with .11b but .11a uses a different frequency range and requires separate hardware such as an a, a/g, or a/b/g adapter. The largest public WiFi networks are provided by private internet service providers (ISPs); they charge a fee to the users who want to access the internet.

Hotspots are increasingly developing around the world. In fact, T-Mobile USA controls more than 4,100 hotspots located in public locations such as Starbucks, Borders, Kinko's, and the airline clubs of Delta, United, and US Airways. Even select McDonald's restaurants now feature WiFi hotspot access.

Any notebook computer with integrated wireless, a wireless adapter attached to the motherboard by the manufacturer, or a wireless adapter such as a PCMCIA card can access a wireless network. Furthermore, all Pocket PCs or Palm units with Compact Flash, SD I/O support, or built-in WiFi, can access hotspots.

Some Hotspots require WEP key to connect, which is considered as private and secure. As for open connections, anyone with a WiFi card can have access to that hotspot. So in order to have internet access under WEP, the user must input the WEP key code

Wi-Fi - IEEE Standards

The 802.11 standard is defined through several specifications of WLANs. It defines an over-the-air interface between a wireless client and a base station or between two wireless clients.

There are several specifications in the 802.11 family −

- **802.11 − This pertains to wireless LANs and provides 1 - or 2-Mbps transmission in the 2.4-GHz band using either frequency-hopping spread spectrum (FHSS) or direct-sequence spread spectrum (DSSS).**

- 802.11a − This is an extension to 802.11 that pertains to wireless LANs and goes as fast as 54 Mbps in the 5-GHz band. 802.11a employs the orthogonal frequency division multiplexing (OFDM) encoding scheme as opposed to either FHSS or DSSS.

- 802.11b − The 802.11 high rate WiFi is an extension to 802.11 that pertains to wireless LANs and yields a connection as fast as 11 Mbps transmission (with a fallback to 5.5, 2, and 1 Mbps depending on strength of signal) in the 2.4-GHz band. The 802.11b specification uses only DSSS. Note that 802.11b was actually an amendment to the original 802.11 standard added in 1999 to permit wireless functionality to be analogous to hard-wired Ethernet connections.

- 802.11g − This pertains to wireless LANs and provides 20+ Mbps in the 2.4-GHz band.

Here is the technical comparison between the three major WiFi standards.

Feature	WiFi (802.11b)	WiFi (802.11a/g)
PrimaryApplication	Wireless LAN	Wireless LAN
Frequency Band	2.4 GHz ISM	2.4 GHz ISM (g) 5 GHz U-NII (a)
Channel Bandwidth	25 MHz	20 MHz
Half/Full Duplex	Half	Half
Radio Technology	Direct Sequence Spread Spectrum	OFDM (64-channels)
Bandwidth	<=0.44 bps/Hz	≤=2.7 bps/Hz
Efficiency		
Modulation	QPSK	BPSK, QPSK, 16-, 64-QAM
FEC	None	Convolutional Code
Encryption	Optional- RC4m (AES in 802.11i)	Optional- RC4(AES in 802.11i)
Mobility	In development	In development
Mesh	Vendor Proprietary	Vendor Proprietary
Access Protocol	CSMA/CA	CSMA/CA

Wi-Fi - Access Protocols

IEEE 802.11 wireless LANs use a media access control protocol called Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). While the name is similar to Ethernet's Carrier Sense Multiple Access with Collision Detection (CSMA/CD), the operating concept is totally different.

WiFi systems are the half duplex shared media configurations, where all stations transmit and receive on the same radio channel. The fundamental problem of a radio system is that a station cannot *hear* while it is sending, and hence it is impossible to detect a collision. Because of this, the developers of the 802.11 specifications came up with a collision avoidance mechanism called the Distributed Control Function (DCF).

According to DCF, a WiFi station will transmit only when the channel is clear. All transmissions are acknowledged, so if a station does not receive an acknowledgement, it assumes a collision occurred and retries after a random waiting interval.

The incidence of collisions will increase as the traffic increases or in situations where mobile stations cannot hear each other.

WIMAX

WiMAX is one of the hottest broadband wireless technologies around today. WiMAX systems are expected to deliver broadband access services to residential and enterprise customers in an economical way.

Loosely, WiMax is a standardized wireless version of Ethernet intended primarily as an alternative to wire technologies (such as Cable Modems, DSL and T1/E1 links) to provide broadband access to customer premises.

More strictly, WiMAX is an industry trade organization formed by leading communications, component, and equipment companies to promote and certify compatibility and interoperability of broadband wireless access equipment that conforms to the IEEE 802.16 and ETSI HIPERMAN standards.

WiMAX would operate similar to WiFi, but at higher speeds over greater distances and for a greater number of users. WiMAX has the ability to provide service even in areas that are difficult for wired infrastructure to reach and the ability to overcome the physical limitations of traditional wired infrastructure.

WiMAX was formed in April 2001, in anticipation of the publication of the original 10-66 GHz IEEE 802.16 specifications. WiMAX is to 802.16 as the WiFi Alliance is to 802.11.

WiMAX is

- **Acronym for Worldwide Interoperability for Microwave Access.**
- **Based on Wireless MAN technology.**
- **A wireless technology optimized for the delivery of IP centric services over a wide area.**

- **A scalable wireless platform for constructing alternative and complementary broadband networks.**

- **A certification that denotes interoperability of equipment built to the IEEE 802.16 or compatible standard. The IEEE 802.16 Working Group develops standards that address two types of usage models −**

    - **A fixed usage model (IEEE 802.16-2004).**
    - **A portable usage model (IEEE 802.16e).**

What is 802.16a ?

WiMAX is such an easy term that people tend to use it for the 802.16 standards and technology themselves, although strictly it applies only to systems that meet specific conformance criteria laid down by the WiMAX Forum.

The 802.16a standard for 2-11 GHz is a wireless metropolitan area network (MAN) technology that will provide broadband wireless connectivity to Fixed, Portable and Nomadic devices.

It can be used to connect 802.11 hot spots to the Internet, provide campus connectivity, and provide a wireless alternative to cable and DSL for last mile broadband access.

WiMax Speed and Range

WiMAX is expected to offer initially up to about 40 Mbps capacity per wireless channel for both fixed and portable applications, depending on the particular technical configuration chosen, enough to support hundreds of businesses with T-1 speed connectivity and thousands of residences with DSL speed connectivity. WiMAX can support voice and video as well as Internet data.

WiMax developed to provide wireless broadband access to buildings, either in competition to existing wired networks or alone in currently unserved rural or thinly populated areas. It can also be used to connect WLAN hotspots to the Internet. WiMAX is also intended to provide broadband connectivity to mobile devices. It would not be as fast as in these fixed applications, but expectations are for about 15 Mbps capacity in a 3 km cell coverage area.

With WiMAX, users could really cut free from today's Internet access arrangements and be able to go online at broadband speeds, almost wherever they like from within a MetroZone.

WiMAX could potentially be deployed in a variety of spectrum bands: 2.3GHz, 2.5GHz, 3.5GHz, and 5.8GHz

Why WiMax ?

- **WiMAX can satisfy a variety of access needs. Potential applications include extending broadband capabilities to bring them closer to subscribers, filling gaps in cable, DSL and T1 services, WiFi, and cellular backhaul, providing last-100 meter access from fibre to the curb and giving service providers another cost-effective option for supporting broadband services.**

- **WiMAX can support very high bandwidth solutions where large spectrum deployments (i.e. >10 MHz) are desired using existing infrastructure keeping costs down while delivering the bandwidth needed to support a full range of high-value multimedia services.**

- **WiMAX can help service providers meet many of the challenges they face due to increasing customer demands without discarding their existing infrastructure investments because it has the ability to seamlessly interoperate across various network types.**

- **WiMAX can provide wide area coverage and quality of service capabilities for applications ranging from real-time delay-sensitive voice-over-IP (VoIP) to real-time streaming video and non-real-time downloads, ensuring that subscribers obtain the performance they expect for all types of communications.**

- **WiMAX, which is an IP-based wireless broadband technology, can be integrated into both wide-area third-generation (3G) mobile and wireless and wireline networks allowing it to become part of a seamless anytime, anywhere broadband access solution.**

Ultimately, WiMAX is intended to serve as the next step in the evolution of 3G mobile phones, via a potential combination of WiMAX and CDMA standards called 4G.

WiMAX Goals

A standard by itself is not enough to enable mass adoption. WiMAX has stepped forward to help solve barriers to adoption, such as interoperability and cost of deployment. WiMAX will help ignite the wireless MAN industry by defining and conducting interoperability testing and labeling vendor systems with a "WiMAX Certified™" label once testing has been completed successfully.

WiMAX & Wi-Fi Comparison

WiMAX is similar to the wireless standard known as Wi-Fi, but on a much larger scale and at faster speeds. A nomadic version would keep WiMAX-enabled devices connected over large areas, much like today's cell phones. We can compare it with Wi-Fi based on the following factors.

IEEE Standards

Wi-Fi is based on IEEE 802.11 standard whereas WiMAX is based on IEEE 802.16. However, both are IEEE standards.

Range

Wi-Fi typically provides local network access for a few hundred feet with the speed of up to 54 Mbps, a single WiMAX antenna is expected to have a range of up to 40 miles with the speed of 70 Mbps or more. As such, WiMAX can bring the underlying Internet connection needed to service local Wi-Fi networks.

Scalability

Wi-Fi is intended for LAN applications, users scale from one to tens with one subscriber for each CPE device. Fixed channel sizes (20MHz).

WiMAX is designed to efficiently support from one to hundreds of Consumer premises equipments (CPE)s, with unlimited subscribers behind each CPE. Flexible channel sizes from 1.5MHz to 20MHz.

Bit rate

Wi-Fi works at 2.7 bps/Hz and can peak up to 54 Mbps in 20 MHz channel.

WiMAX works at 5 bps/Hz and can peak up to 100 Mbps in a 20 MHz channel.

Quality of Service

Wi-Fi does not guarantee any QoS but WiMax will provide your several level of QoS.

As such, WiMAX can bring the underlying Internet connection needed to service local Wi-Fi networks. Wi-Fi does not provide ubiquitous broadband while WiMAX does.

Comparison Table

Freature	WiMax (802.16a)	Wi-Fi (802.11b)	Wi-Fi (802.11a/g)
Primary Application	Broadband Wireless Access	Wireless LAN	Wireless LAN
Frequency Band	Licensed/Unlicensed 2 G to 11 GHz	2.4 GHz ISM	2.4 GHz ISM (g) 5 GHz U-NII (a)
Channel Bandwidth	Adjustable 1.25 M to 20 MHz	25 MHz	20 MHz
Half/Full Duplex	Full	Half	Half
Radio Technology	OFDM (256-channels)	Direct Sequence Spread Spectrum	OFDM (64-channels)
Bandwidth Efficiency	<=5 bps/Hz	<=0.44 bps/Hz	<=2.7 bps/Hz
Modulation	BPSK, QPSK, 16-, 64-, 256-QAM	QPSK	BPSK, QPSK, 16-, 64-QAM
FEC	Convolutional Code Reed-Solomon	None	Convolutional Code
Encryption	Mandatory- 3DES	Optional-	Optional-

	Optional- AES	RC4 (AES in 802.11i)	RC4 (AES in 802.11i)
Mobility	Mobile WiMax (802.16e)	In development	In development
Mesh	Yes	Vendor Proprietary	Vendor Proprietary
Access Protocol	Request/Grant	CSMA/CA	CSMA/CA

WiMAX - Salient Features

WiMAX is a wireless broadband solution that offers a rich set of features with a lot of flexibility in terms of deployment options and potential service offerings. Some of the more salient features that deserve highlighting are as follows −

Two Type of Services

WiMAX can provide two forms of wireless service −

- **Non-line-of-sight − service is a WiFi sort of service. Here a small antenna on your computer connects to the WiMAX tower. In this mode, WiMAX uses a lower frequency range -- 2 GHz to 11 GHz (similar to WiFi).**

- **Line-of-sight − service, where a fixed dish antenna points straight at the WiMAX tower from a rooftop or pole. The line-of-sight connection is stronger and more stable, so it's able to send a lot of data with fewer errors. Line-of-sight transmissions use higher frequencies, with ranges reaching a possible 66 GHz.**

OFDM-based Physical Layer

The WiMAX physical layer (PHY) is based on orthogonal frequency division multiplexing, a scheme that offers good resistance to multipath, and allows WiMAX to operate in NLOS conditions.

Very High Peak Data Rates

WiMAX is capable of supporting very high peak data rates. In fact, the peak PHY data rate can be as high as 74Mbps when operating using a 20MHz wide spectrum.

More typically, using a 10MHz spectrum operating using TDD scheme with a 3:1 downlink-to-uplink ratio, the peak PHY data rate is about 25Mbps and 6.7Mbps for the downlink and the uplink, respectively.

Scalable Bandwidth and Data Rate Support

WiMAX has a scalable physical-layer architecture that allows for the data rate to scale easily with available channel bandwidth.

For example, a WiMAX system may use 128, 512, or 1,048-bit FFTs (fast fourier transforms) based on whether the channel bandwidth is 1.25MHz, 5MHz, or 10MHz,

respectively. This scaling may be done dynamically to support user roaming across different networks that may have different bandwidth allocations.

Adaptive Modulation and Coding (AMC)

WiMAX supports a number of modulation and forward error correction (FEC) coding schemes and allows the scheme to be changed as per user and per frame basis, based on channel conditions.

AMC is an effective mechanism to maximize throughput in a time-varying channel.

Link-layer Retransmissions

WiMAX supports automatic retransmission requests (ARQ) at the link layer for connections that require enhanced reliability. ARQ-enabled connections require each transmitted packet to be acknowledged by the receiver; unacknowledged packets are assumed to be lost and are retransmitted.

Support for TDD and FDD

IEEE 802.16-2004 and IEEE 802.16e-2005 supports both time division duplexing and frequency division duplexing, as well as a half-duplex FDD, which allows for a low-cost system implementation.

WiMAX Uses OFDM

Mobile WiMAX uses Orthogonal frequency division multiple access (OFDM) as a multiple-access technique, whereby different users can be allocated different subsets of the OFDM tones.

Flexible and Dynamic per User Resource Allocation

Both uplink and downlink resource allocation are controlled by a scheduler in the base station. Capacity is shared among multiple users on a demand basis, using a burst TDM scheme.

Support for Advanced Antenna Techniques

The WiMAX solution has a number of hooks built into the physical-layer design, which allows for the use of multiple-antenna techniques, such as beamforming, space-time coding, and spatial multiplexing.

Quality-of-service Support

The WiMAX MAC layer has a connection-oriented architecture that is designed to support a variety of applications, including voice and multimedia services.

WiMAX system offers support for constant bit rate, variable bit rate, real-time, and non-real-time traffic flows, in addition to best-effort data traffic.

WiMAX MAC is designed to support a large number of users, with multiple connections per terminal, each with its own QoS requirement.

Robust Security

WiMAX supports strong encryption, using Advanced Encryption Standard (AES), and has a robust privacy and key-management protocol.

The system also offers a very flexible authentication architecture based on Extensible Authentication Protocol (EAP), which allows for a variety of user credentials, including username/password, digital certificates, and smart cards.

Support for Mobility

The mobile WiMAX variant of the system has mechanisms to support secure seamless handovers for delay-tolerant full-mobility applications, such as VoIP.

IP-based Architecture

The WiMAX Forum has defined a reference network architecture that is based on an all-IP platform. All end-to-end services are delivered over an IP architecture relying on IP-based protocols for end-to-end transport, QoS, session management, security, and mobility.

WiMAX - Building Blocks

A WiMAX system consists of two major parts −

- **A WiMAX base station.**
- **A WiMAX receiver.**

WiMAX Base Station

A WiMAX base station consists of indoor electronics and a WiMAX tower similar in concept to a cell-phone tower. A WiMAX base station can provide coverage to a very large area up to a radius of 6 miles. Any wireless device within the coverage area would be able to access the Internet.

The WiMAX base stations would use the MAC layer defined in the standard, a common interface that makes the networks interoperable and would allocate uplink and downlink bandwidth to subscribers according to their needs, on an essentially real-time basis.

Each base station provides wireless coverage over an area called a cell. Theoretically, the maximum radius of a cell is 50 km or 30 miles however, practical considerations limit it to about 10 km or 6 miles.

WiMAX Receiver

A WiMAX receiver may have a separate antenna or could be a stand-alone box or a PCMCIA card sitting in your laptop or computer or any other device. This is also referred as customer premise equipment (CPE).

WiMAX base station is similar to accessing a wireless access point in a WiFi network, but the coverage is greater.

Backhaul

A WiMAX tower station can connect directly to the Internet using a high-bandwidth, wired connection (for example, a T3 line). It can also connect to another WiMAX tower using a line-of-sight microwave link.

Backhaul refers both to the connection from the access point back to the base station and to the connection from the base station to the core network.

It is possible to connect several base stations to one another using high-speed backhaul microwave links. This would also allow for roaming by a WiMAX subscriber from one base station coverage area to another, similar to the roaming enabled by cell phones.

WiMAX - Reference Network Model

The IEEE 802.16e-2005 standard provides the air interface for WiMAX, but does not define the full end-to-end WiMAX network. The WiMAX Forum's Network Working Group (NWG) is responsible for developing the end-to-end network requirements, architecture, and protocols for WiMAX, using IEEE 802.16e-2005 as the air interface.

The WiMAX NWG has developed a network reference model to serve as an architecture framework for WiMAX deployments and to ensure interoperability among various WiMAX equipment and operators.

The network reference model envisions a unified network architecture for supporting fixed, nomadic, and mobile deployments and is based on an IP service model. Below is simplified illustration of an IP-based WiMAX network architecture. The overall network may be logically divided into three parts −

- **Mobile Stations (MS) used by the end user to access the network.**
- **The access service network (ASN), which comprises one or more base stations and one or more ASN gateways that form the radio access network at the edge.**
- **Connectivity service network (CSN), which provides IP connectivity and all the IP core network functions.**

The network reference model developed in figure 5.1 by the WiMAX Forum NWG defines a number of functional entities and interfaces between those entities. The following figure shows some of the more important functional entities.

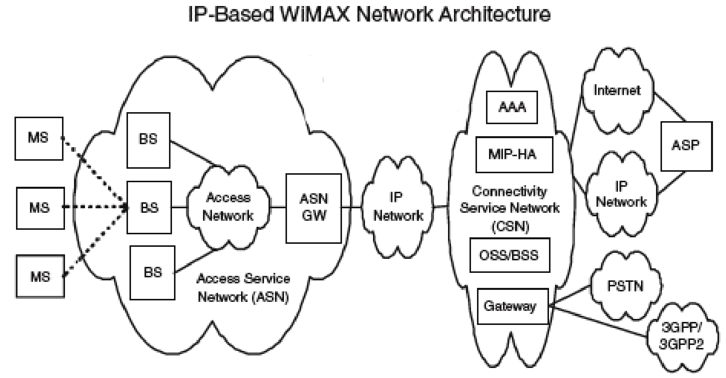


Figure 5,1 WiMAX

- **Base station (BS) − The BS is responsible for providing the air interface to the MS. Additional functions that may be part of the BS are micro mobility management functions, such as handoff triggering and tunnel establishment, radio resource management, QoS policy enforcement, traffic classification, DHCP (Dynamic Host Control Protocol) proxy, key management, session management, and multicast group management.**
- **Access service network gateway (ASN-GW) − The ASN gateway typically acts as a layer 2 traffic aggregation point within an ASN. Additional functions that may be part of the ASN gateway include intra-ASN location management and paging, radio resource management, and admission control, caching of subscriber profiles, and encryption**

keys, AAA client functionality, establishment, and management of mobility tunnel with base stations, QoS and policy enforcement, foreign agent functionality for mobile IP, and routing to the selected CSN.

- **Connectivity service network (CSN) − The CSN provides connectivity to the Internet, ASP, other public networks, and corporate networks. The CSN is owned by the NSP and includes AAA servers that support authentication for the devices, users, and specific services. The CSN also provides per user policy management of QoS and security. The CSN is also responsible for IP address management, support for roaming between different NSPs, location management between ASNs, and mobility and roaming between ASNs.**

The WiMAX architecture framework allows for the flexible decomposition and/or combination of functional entities when building the physical entities. For example, the ASN may be decomposed into base station transceivers (BST), base station controllers (BSC), and an ASNGW analogous to the GSM model of BTS, BSC, and Serving GPRS Support Node (SGSN).

WiMAX - Technology

WiMAX is a technology based on the IEEE 802.16 specifications to enable the delivery of last-mile wireless broadband access as an alternative to cable and DSL. The design of WiMAX network is based on the following major principles −

- **Spectrum − able to be deployed in both licensed and unlicensed spectra.**
- **Topology − supports different Radio Access Network (RAN) topologies.**
- **Interworking − independent RAN architecture to enable seamless integration and interworking with WiFi, 3GPP and 3GPP2 networks and existing IP operator core network.**
- **IP connectivity − supports a mix of IPv4 and IPv6 network interconnects in clients and application servers.**
- **Mobility management − possibility to extend the fixed access to mobility and broadband multimedia services delivery.**

WiMAX has defined two MAC system profiles the basic ATM and the basic IP. They have also defined two primary PHY system profiles, the 25 MHz-wide channel for use in (US deployments) the 10.66 GHz range, and the 28 MHz wide channel for use in (European deployments) the 10.66 GHz range.

WiMAX Physical and MAC Layers are explained in separate chapters of this tutorial.

The WiMAX technical working group is defining MAC and PHY system profiles for IEEE 802.16a and HiperMan standards. The MAC profile includes an IP-based version for both wireless MAN (licensed) and wireless HUMAN (licence-exempt).

IEEE Standard 802.16 was designed to evolve as a set of air interfaces standards for WMAN based on a common MAC protocol, but with physical layer specifications dependent on the spectrum of use and the associated regulations.

The WiMAX framework is based on several core principles −

- **Support for different RAN topologies.**

- **Well-defined interfaces to enable 802.16 RAN architecture independence while enabling seamless integration and interworking with WiFi, 3GPP3 and 3GPP2 networks.**

- **Leverage and open, IETF-defined IP technologies to build scalable all-IP 802.16 access networks using common off the shelf (COTS) equipment.**

- **Support for IPv4 and IPv6 clients and application servers, recommending use of IPv6 in the infrastructure.**

- **Functional extensibility to support future migration to full mobility and delivery of rich broadband multimedia.**

WiMAX - Physical Layer

The WiMAX physical layer is based on orthogonal frequency division multiplexing. OFDM is the transmission scheme of choice to enable high-speed data, video, and multimedia communications and is used by a variety of commercial broadband systems, including DSL, Wi-Fi, Digital Video Broadcast-Handheld (DVB-H), and MediaFLO, besides WiMAX.

OFDM is an elegant and efficient scheme for high data rate transmission in a non-line-of-sight or multipath radio environment.

Adaptive Modulation and Coding in WiMAX

WiMAX supports a variety of modulation and coding schemes and allows for the scheme to change on a burst-by-burst basis per link, depending on channel conditions. Using the channel quality feedback indicator, the mobile can provide the base station with feedback on the downlink channel quality. For the uplink, the base station can estimate the channel quality, based on the received signal quality.

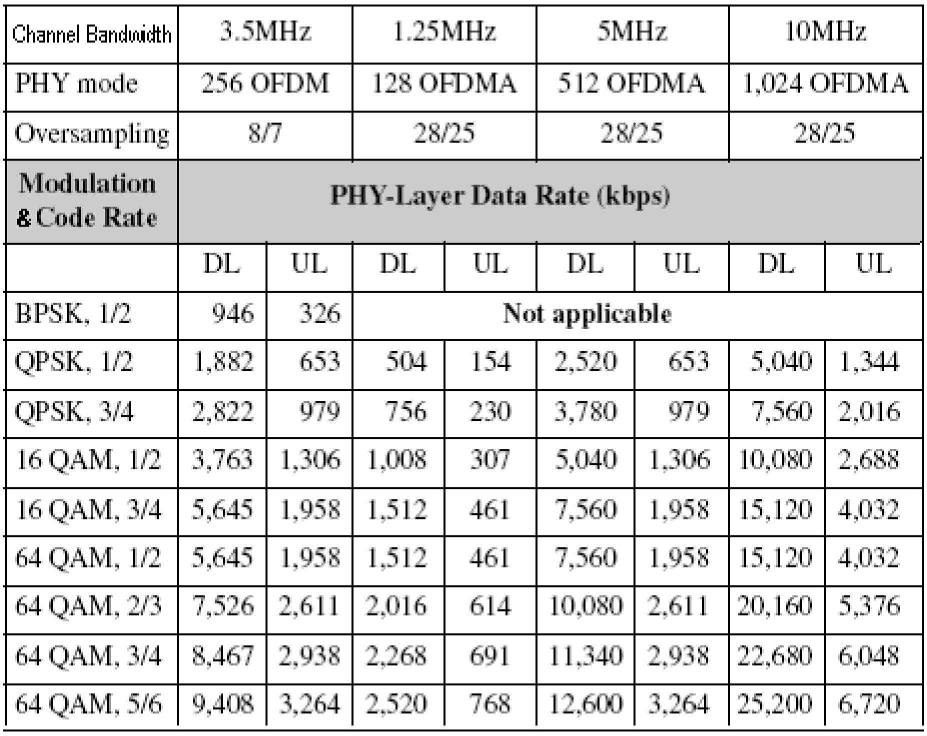
The following table provides a list of the various modulation and coding schemes supported by WiMAX −

	Downlink	**Uplink**
Modulation	**BPSK, QPSK, 16 QAM, 64 QAM; BPSK optional for OFDMA-PHY**	**BPSK, QPSK, 16 QAM; 64 QAM optional**
Coding	**Mandatory: convolutional codes at rate 1/2, 2/3, 3/4, 5/6** **Optional: convolutional turbo codes at rate 1/2, 2/3, 3/4, 5/6; repetition codes at rate 1/2, 1/3, 1/6, LDPC, RS-Codes for OFDM-PHY**	**Mandatory: convolutional codes at rate 1/2, 2/3, 3/4, 5/6** **Optional: convolutional turbo codes at rate 1/2, 2/3, 3/4, 5/6; repetition codes at rate 1/2, 1/3, 1/6, LDPC**

PHY-Layer Data Rates

Because the physical layer of WiMAX is quite flexible, data rate performance varies based on the operating parameters. Parameters that have a significant impact on the physical-layer data rate are channel bandwidth and the modulation and coding scheme used. Other parameters, such as number of sub-channels, OFDM guard time, and oversampling rate, also have an impact.

Following is the PHY-layer data rate at various channel bandwidths, as well as modulation and coding schemes.



Channel Bandwidth	3.5MHz		1.25MHz		5MHz		10MHz	
PHY mode	256 OFDM		128 OFDMA		512 OFDMA		1,024 OFDMA	
Oversampling	8/7		28/25		28/25		28/25	
Modulation & Code Rate	**PHY-Layer Data Rate (kbps)**							
	DL	UL	DL	UL	DL	UL	DL	UL
BPSK, 1/2	946	326	**Not applicable**					
QPSK, 1/2	1,882	653	504	154	2,520	653	5,040	1,344
QPSK, 3/4	2,822	979	756	230	3,780	979	7,560	2,016
16 QAM, 1/2	3,763	1,306	1,008	307	5,040	1,306	10,080	2,688
16 QAM, 3/4	5,645	1,958	1,512	461	7,560	1,958	15,120	4,032
64 QAM, 1/2	5,645	1,958	1,512	461	7,560	1,958	15,120	4,032
64 QAM, 2/3	7,526	2,611	2,016	614	10,080	2,611	20,160	5,376
64 QAM, 3/4	8,467	2,938	2,268	691	11,340	2,938	22,680	6,048
64 QAM, 5/6	9,408	3,264	2,520	768	12,600	3,264	25,200	6,720

WiMAX - OFDM Basics

OFDM belongs to a family of transmission schemes called multicarrier modulation, which is based on the idea of dividing a given high-bit-rate data stream into several parallel lower bit-rate streams and modulating each stream on separate carriers, often called subcarriers or tones.

Multicarrier modulation schemes eliminate or minimize inter-symbol interference (ISI) by making the symbol time large enough so that the channel-induced delays are an insignificant (typically, < 10 percent) fraction of the symbol duration.

Therefore, in high-data-rate systems in which the symbol duration is small, being inversely proportional to the data rate splitting the data stream into many parallel streams increases the symbol duration of each stream such that the delay spread is only a small fraction of the symbol duration.

OFDM is a spectrally efficient version of multicarrier modulation, where the subcarriers are selected such that they are all orthogonal to one another over the symbol duration, thereby avoiding the need to have non-overlapping subcarrier channels to eliminate inter-carrier interference.

In order to completely eliminate ISI, guard intervals are used between OFDM symbols. By making the guard interval larger than the expected multipath delay spread, ISI can

be completely eliminated. Adding a guard interval, however, implies power wastage and a decrease in bandwidth efficiency.

WiMAX - MAC Layer

The IEEE 802.16 MAC was designed for point-to-multipoint broadband wireless access applications. The primary task of the WiMAX MAC layer is to provide an interface between the higher transport layers and the physical layer.

The MAC layer takes packets from the upper layer, these packets are called MAC service data units (MSDUs) and organizes them into MAC protocol data units (MPDUs) for transmission over the air. For received transmissions, the MAC layer does the reverse.

The IEEE 802.16-2004 and IEEE 802.16e-2005 MAC design includes a convergence sublayer that can interface with a variety of higher-layer protocols, such as ATM TDM Voice, Ethernet, IP, and any unknown future protocol.

The 802.16 MAC is designed for point-to-multipoint (PMP) applications and is based on collision sense multiple access with collision avoidance (CSMA/CA).

The MAC incorporates several features suitable for a broad range of applications at different mobility rates, such as the following −

- **Privacy key management (PKM) for MAC layer security. PKM version 2 incorporates support for extensible authentication protocol (EAP).**
- **Broadcast and multicast support.**
- **Manageability primitives.**
- **High-speed handover and mobility management primitives.**
- **Three power management levels, normal operation, sleep, and idle.**
- **Header suppression, packing and fragmentation for an efficient use of spectrum.**
- **Five service classes, unsolicited grant service (UGS), real-time polling service (rtPS), non-real-time polling service (nrtPS), best effort (BE), and Extended real-time variable rate (ERT-VR) service.**

These features combined with the inherent benefits of scalable OFDMA make 802.16 suitable for high-speed data and bursty or isochronous IP multimedia applications.

Support for QoS is a fundamental part of the WiMAX MAC-layer design. WiMAX borrows some of the basic ideas behind its QoS design from the DOCSIS cable modem standard.

Strong QoS control is achieved by using a connection-oriented MAC architecture, where all downlink and uplink connections are controlled by the serving BS.

WiMAX also defines a concept of a service flow. A service flow is a unidirectional flow of packets with a particular set of QoS parameters and is identified by a *service flow identifier* (SFID).

WiMAX - Mobility Support

WiMAX envisions four mobility-related usage scenarios −

- Nomadic − The user is allowed to take a fixed subscriber station and reconnect from a different point of attachment.

- Portable − Nomadic access is provided to a portable device, such as a PC card, with expectation of a best-effort handover.

- Simple mobility − The subscriber may move at speeds up to 60 kmph with brief interruptions (less than 1 sec) during handoff.

- Full mobility − Up to 120 kmph mobility and seamless handoff (less than 50 ms latency and < 1% packet loss) is supported.

It is likely that WiMAX networks will initially be deployed for fixed and nomadic applications and then evolve to support portability to full mobility over time.

The IEEE 802.16e-2005 standard defines a framework for supporting mobility management. In particular, the standard defines signaling mechanisms for tracking subscriber stations as they move from the coverage range of one base station to another when active or as they move from one paging group to another when idle.

The standard also has protocols to enable a seamless handover of ongoing connections from one base station to another.

The standard also has protocols to enable a seamless handover of ongoing connections from one base station to another. The WiMAX Forum has used the framework defined in IEEE 802.16e-2005, to further develop mobility management within an end-to-end network architecture framework. The architecture also supports IP-layer mobility using mobile IP.

WiMAX - Security Functions

WiMAX systems were designed at the outset with robust security in mind. The standard includes state-of-the-art methods for ensuring user data privacy and preventing unauthorized access with additional protocol optimization for mobility.

Security is handled by a privacy sublayer within the WiMAX MAC. The key aspects of WiMAX security are as follow −

Support for Privacy

User data is encrypted using cryptographic schemes of proven robustness to provide privacy. Both AES (Advanced Encryption Standard) and 3DES (Triple Data Encryption Standard) are supported.

The 128-bit or 256-bit key used for deriving the cipher is generated during the authentication phase and is periodically refreshed for additional protection.

Device/user Authentication

WiMAX provides a flexible means for authenticating subscriber stations and users to prevent unauthorized use. The authentication framework is based on the Internet Engineering Task Force (IETF) EAP, which supports a variety of credentials, such as username/password, digital certificates, and smart cards.

WiMAX terminal devices come with built-in X.509 digital certificates that contain their public key and MAC address. WiMAX operators can use the certificates for device authentication and use a username/password or smart card authentication on top of it for user authentication.

Flexible Key-management Protocol

The Privacy and Key Management Protocol Version 2 (PKMv2) is used for securely transferring keying material from the base station to the mobile station, periodically re-authorizing and refreshing the keys.

Protection of Control Messages

The integrity of over-the-air control messages is protected by using message digest schemes, such as AES-based CMAC or MD5-based HMAC.

Support for Fast Handover

To support fast handovers, WiMAX allows the MS to use pre-authentication with a particular target BS to facilitate accelerated re-entry.

A three-way handshake scheme is supported to optimize the re-authentication mechanisms for supporting fast handovers, while simultaneously preventing any man-in-the-middle attacks.

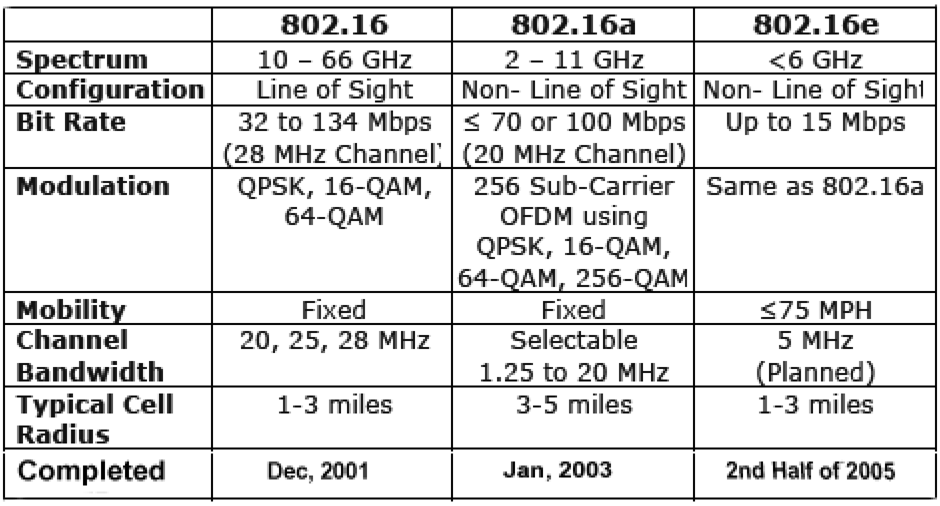
WiMAX - IEEE Standards

The IEEE 802.16, the *Air Interface for Fixed Broadband Wireless Access Systems*, also known as the IEEE WirelessMAN air interface, is an emerging suite of standards for fixed, portable and mobile BWA in MAN.

These standards are issued by IEEE 802.16 work group that originally covered the wireless local loop (WLL) technologies in the 10.66 GHz radio spectrum, which were later extended through amendment projects to include both licensed and unlicensed spectra from 2 to 11 GHz.

The WiMAX umbrella currently includes 802.16-2004 and 802.16e. 802.16-2004 utilizes OFDM to serve multiple users in a time division fashion in a sort of a round-robin technique, but done extremely quickly so that users have the perception that they are always transmitting/receiving. 802.16e utilizes OFDMA and can serve multiple users simultaneously by allocating sets of *tones* to each user.

Following is the chart of various IEEE 802.16 Standards related to WiMAX.



	802.16	802.16a	802.16e
Spectrum	10 – 66 GHz	2 – 11 GHz	<6 GHz
Configuration	Line of Sight	Non- Line of Sight	Non- Line of Sight
Bit Rate	32 to 134 Mbps (28 MHz Channel)	≤ 70 or 100 Mbps (20 MHz Channel)	Up to 15 Mbps
Modulation	QPSK, 16-QAM, 64-QAM	256 Sub-Carrier OFDM using QPSK, 16-QAM, 64-QAM, 256-QAM	Same as 802.16a
Mobility	Fixed	Fixed	≤75 MPH
Channel Bandwidth	20, 25, 28 MHz	Selectable 1.25 to 20 MHz	5 MHz (Planned)
Typical Cell Radius	1-3 miles	3-5 miles	1-3 miles
Completed	Dec, 2001	Jan, 2003	2nd Half of 2005

NOTE − The IEEE 802.16 standards for BWA provide the possibility for interoperability between equipment from different vendors, which is in contrast to the

previous BWA industry, where proprietary products with high prices are dominant in the market.

WiMAX - WiMAXForum™

A nonprofit organization called WiMAX Forum™ was formed in 2001, with the aim of harmonizing standards, testing and certifying interoperability between equipment from different manufacturers.

WiMAX Forum™ was formed by equipment and component suppliers to support the IEEE 802.16 BWA system by helping to ensure the compatibility and interoperability of BWA equipment, which will lead to lower cost through chip-level implementation.

WiMAX Forum™ is doing what WiFi Alliance has done for wireless LAN and IEEE 802.11. WiMAX Forum Certified™ products adhere to the IEEE 802.16 standard and offer higher bandwidth, lower costs, and broader service capabilities than most of the available proprietary solutions.

The WiMAX Forum™ is working on setting up a baseline protocol that allows equipment and devices from multiple vendors to interoperate and also provides a choice of equipment and devices from different suppliers.

Members of WiMAXForum

The WiMAX Forum™ has more than 400 members from equipment manufacturers, semiconductor suppliers, and services providers, and membership was recently opened for content providers. Some of the noted members are Alcatel, AT&T, Fujitsu, Intel, Nortel, Motorola, SBC, and Siemens

ORTHOGONAL FREQUENCY DIVISION MULTIPLEXING (OFDM)

In data communications and networking, orthogonal frequency-division multiplexing (OFDM) is a method of digital data modulation, whereby a single stream of data is divided into several separate sub-streams for transmission via multiple channels.

OFDM uses the principle of frequency division multiplexing (FDM), where the available bandwidth is divided into a set of sub-streams having separate frequency bands. OFDM was introduced in 1966 by Chang at Bell Labs and was improved by Weinstein and Ebert in 1971.

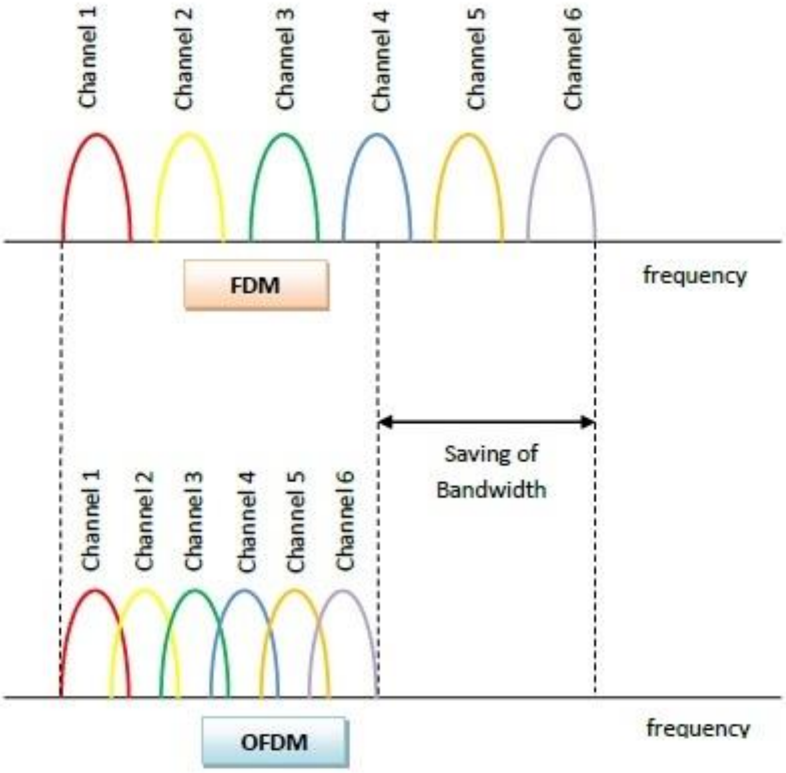
Working Principle of OFDM

OFDM is a specialised FDM having the constraint that the sub-streams in which the main signal is divided, are orthogonal to each other. Orthogonal signals are signals that are perpendicular to each other. A main property of orthogonal signals is that they do not interfere with each other.

When any signal is modulated by the sender, its sidebands spread out either side. A receiver can successfully demodulate the data only if it receives the whole signal. In case of FDM, guard bands are inserted so that interference between the signals, resulting in cross-talks, does not occur. However, since orthogonal signals are used in OFDM, no interference occurs between the signals even if their sidebands overlap. So, guard bands can be removed, thus saving bandwidth. The criteria that needs to be maintained is that the carrier spacing should be equal to the reciprocal of the symbol period.

In order that OFDM works, there should be very accurate synchronization between the communicating nodes. If frequency deviation occurs in the sub-streams, they will not be orthogonal any more, due to which interference between the signals will occur.

The following diagram plots FDM versus OFDM, to depict the saving in bandwidth obtained by OFDM −



Usages

OFDM is used in the following area −

- **Wi-Fi**
- **DSL internet access**
- **4G wireless communications**
- **digital television**
- **radio broadcast services**

Frame Structure for OFDMA with Time Division Duplexing

ORTHOGONAL FREQUENCY DIVISION MULTIPLE ACCESS

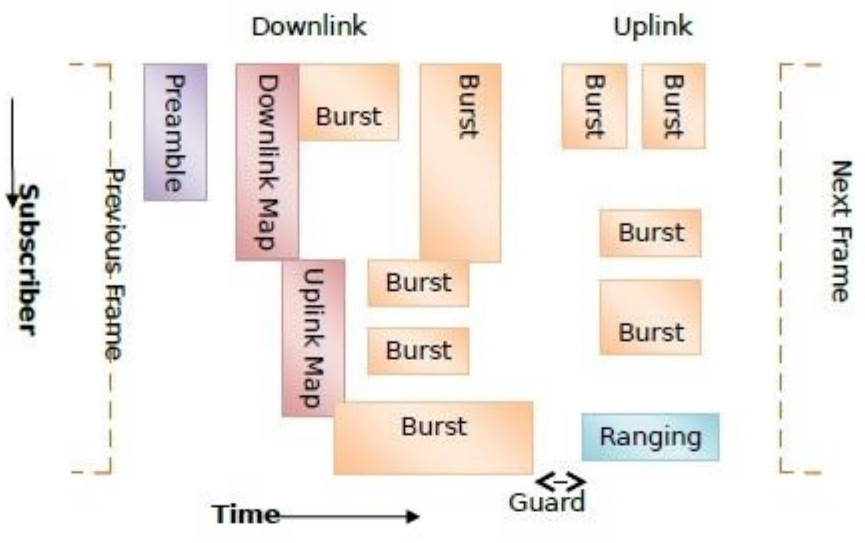
Orthogonal frequency division multiple access (OFDMA) is a multi-user version of digital data modulation scheme OFDM (orthogonal frequency division multiplexing). In OFDM, a single stream of data is divided into several separate sub-streams for transmission via multiple channels. OFDM uses the principle of frequency division multiplexing (FDM), where the available bandwidth is divided into a set of sub-streams having separate frequency bands.

In OFDMA, multiple access is achieved by assignment of different subsets of subcarriers to individual stations. This permits transmission to go on simultaneously at lower data rate from several stations.

The stations assigned to a given subcarrier alternate between sending and receiving using time division duplexing (TDD). In TDD, the uplink of a station is separated from the downlink by allocating different time slots in the same frequency band of a subcarrier. This allows asymmetric flow of data for upstream and downstream. Each station is allotted separate time slots for uplink and downlink transmission.

Frame Structure of OFDMA with TDD

The following diagram shows the frame structure that needs to be used for orthogonal frequency division multiple access with time division duplexing −



Frame Structure of OFDMA with TDD

The particulars of the frame that is sent with respect to time is as follows −

- **Each frame starts with a preamble. The function of the preamble is to synchronize all the stations that are contending for the wireless channel.**
- **The preamble is followed by two maps for downlink and uplink bursts. They hold information about how the downlink bursts and the uplink bursts are assigned over the frame in the subcarrier.**
- **The above maps are controlled by the base station. This adds flexibility to the system, as the base station can allot different amount of bandwidth to the stations for each frame as per the requirements of the stations.**
- **After the maps are transmitted, the base station sends bursts of downlink data streams to the concerned stations according to the timings laid down in the downlink map.**
- **Downlink traffic ends with a guard band that allows the stations to switch from receiving to transmitting mode.**
- **The stations then send their data in bursts of uplink data streams to the base station.**

- **Among the uplink bursts, one is reserved for ranging. In the ranging process, new stations can send their upstream data. The stations request for bandwidth to connect to the base station and adjust their burst time according to the ranging slot.**
- **After the whole frame has been sent, an inter-frame spacing is kept and then the base station initiates transmission of the next frame.**

MIMO WIRELESS TECHNOLOGY

MIMO: Multiple Input Multiple Output technology uses multiple antennas to make use of reflected signals to provide gains in channel robustness and throughput.

Multiple-input multiple-output, or MIMO, is a radio communications technology or RF technology that is being mentioned and used in many new technologies these days.

Wi-Fi, LTE; Long Term Evolution, and many other radio, wireless and RF technologies are using the new MIMO wireless technology to provide increased link capacity and spectral efficiency combined with improved link reliability using what were previously seen as interference paths.

Even now many there are many MIMO wireless routers on the market, and as this RF technology is becoming more widespread, more MIMO routers and other items of wireless MIMO equipment will be seen.

Typical modern WiFi router using MIMO technology with multiple antennas

As the technology is complex many engineers are asking what is MIMO and how does it work.

MIMO development and history

MIMO technology has been developed over many years. Not only did the basic MIMO concepts need to be formulated, but in addition to this, new technologies needed to be developed to enable MIMO to be fully implemented. New levels of processing were needed to allow some of the features of spatial multiplexing as well as to utilise some of the gains of spatial diversity.

Up until the 1990s, spatial diversity was often limited to systems that switched between two antennas or combined the signals to provide the best signal. Also various forms of beam switching were implemented, but in view of the levels of processing involved and the degrees of processing available, the systems were generally relatively limited.

However with the additional levels of processing power that started to become available, it was possible to utilise both spatial diversity and full spatial multiplexing.

The initial work on MIMO systems focussed on basic spatial diversity - here the MIMO system was used to limit the degradation caused by multipath propagation. However

this was only the first step as system then started to utilise the multipath propagation to advantage, turning the additional signal paths into what might effectively be considered as additional channels to carry additional data.

Two researchers: Arogyaswami Paulraj and Thomas Kailath were first to propose the use of spatial multiplexing using MIMO in 1993 and in the following year their US patent was granted.

However it fell to Bell Labs to be the first to demonstrate a laboratory prototype of spatial multiplexing in 1998.

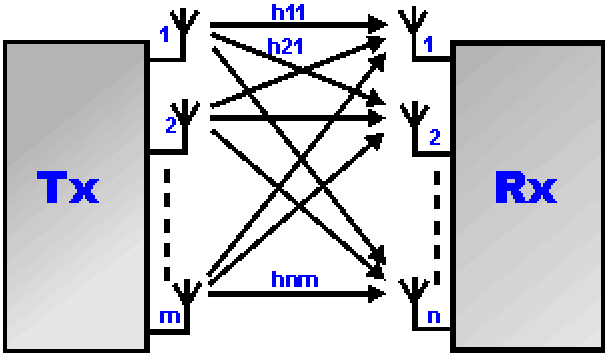
MIMO -Multiple Input Multiple Output basics

A channel may be affected by fading and this will impact the signal to noise ratio. In turn this will impact the error rate, assuming digital data is being transmitted. The principle of diversity is to provide the receiver with multiple versions of the same signal. If these can be made to be affected in different ways by the signal path, the probability that they will all be affected at the same time is considerably reduced. Accordingly, diversity helps to stabilise a link and improves performance, reducing error rate.

Several different diversity modes are available and provide a number of advantages:

- ***Time diversity:*** **Using time diversity, a message may be transmitted at different times, e.g. using different timeslots and channel coding.**
- ***Frequency diversity:*** **This form of diversity uses different frequencies. It may be in the form of using different channels, or technologies such as spread spectrum / OFDM.**
- ***Space diversity :*** **Space diversity used in the broadest sense of the definition is used as the basis for MIMO. It uses antennas located in different positions to take advantage of the different radio paths that exist in a typical terrestrial environment.**

MIMO is effectively a radio antenna technology as it uses multiple antennas at the transmitter and receiver to enable a variety of signal paths to carry the data, choosing separate paths for each antenna to enable multiple signal paths to be used.



General Outline of MIMO system

One of the core ideas behind MIMO wireless systems space-time signal processing in which time (the natural dimension of digital communication data) is complemented with the spatial dimension inherent in the use of multiple spatially distributed antennas, i.e. the use of multiple antennas located at different points. Accordingly MIMO wireless systems can be viewed as a logical extension to the smart antennas that have been used for many years to improve wireless.

It is found between a transmitter and a receiver, the signal can take many paths. Additionally by moving the antennas even a small distance the paths used will change. The variety of paths available occurs as a result of the number of objects that appear to

the side or even in the direct path between the transmitter and receiver. Previously these multiple paths only served to introduce interference. By using MIMO, these additional paths can be used to advantage. They can be used to provide additional robustness to the radio link by improving the signal to noise ratio, or by increasing the link data capacity.

The two main formats for MIMO are given below:

- ***Spatial diversity:*** **Spatial diversity used in this narrower sense often refers to transmit and receive diversity. These two methodologies are used to provide improvements in the signal to noise ratio and they are characterised by improving the reliability of the system with respect to the various forms of fading.**
- ***Spatial multiplexing :*** **This form of MIMO is used to provide additional data capacity by utilising the different paths to carry additional traffic, i.e. increasing the data throughphut capability.**

As a result of the use multiple antennas, MIMO wireless technology is able to considerably increase the capacity of a given channel while still obeying Shannon's law. By increasing the number of receive and transmit antennas it is possible to linearly increase the throughput of the channel with every pair of antennas added to the system. This makes MIMO wireless technology one of the most important wireless techniques to be employed in recent years. As spectral bandwidth is becoming an ever more valuable commodity for radio communications systems, techniques are needed to use the available bandwidth more effectively. MIMO wireless technology is one of these techniques.

There is a number of different MIMO configurations or formats that can be used. These are termed SISO, SIMO, MISO and MIMO. These different MIMO formats offer different advantages and disadvantages - these can be balanced to provide the optimum solution for any given application.

The different MIMO formats - SISO, SIMO, MISO and MIMO require different numbers of antennas as well as having different levels of complexity. Also dependent upon the format, processing may be needed at one end of the link or the other - this can have an impact on any decisions made.

SISO, SIMO, MISO, MIMO terminology

The different forms of antenna technology refer to single or multiple inputs and outputs. These are related to the radio link. In this way the input is the transmitter as it transmits into the link or signal path, and the output is the receiver. It is at the output of the wireless link.

therefore the different forms of single / multiple antenna links are defined as below:

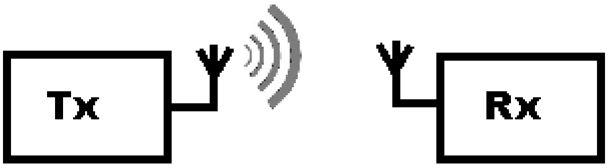
- **SISO - Single Input Single Output**
- **SIMO - Single Input Multiple output**
- **MISO - Multiple Input Single Output**
- **MIMO - Multiple Input multiple Output**

The term MU-MIMO is also used for a multiple user version of MIMO as described below.

MIMO - SISO

The simplest form of radio link can be defined in MIMO terms as SISO - Single Input Single Output. This is effectively a standard radio channel - this transmitter operates

with one antenna as does the receiver. There is no diversity and no additional processing required.

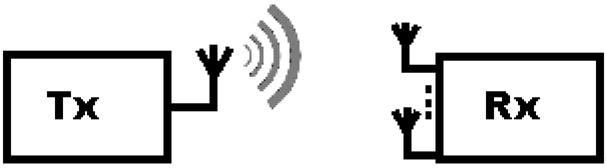


SISO - Single Input Single Output

The advantage of a SIS system is its simplicity. SISO requires no processing in terms of the various forms of diversity that may be used. However the SISO channel is limited in its performance. Interference and fading will impact the system more than a MIMO system using some form of diversity, and the channel bandwidth is limited by Shannon's law - the throughput being dependent upon the channel bandwidth and the signal to noise ratio.

MIMO - SIMO

The SIMO or Single Input Multiple Output version of MIMO occurs where the transmitter has a single antenna and the receiver has multiple antennas. This is also known as receive diversity. It is often used to enable a receiver system that receives signals from a number of independent sources to combat the effects of fading. It has been used for many years with short wave listening / receiving stations to combat the effects of ionospheric fading and interference.



SIMO - Single Input Multiple Output

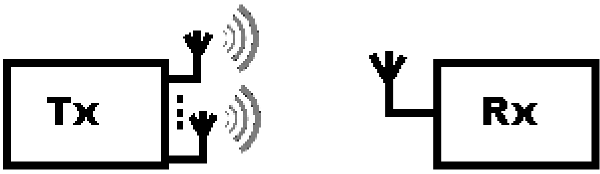
SIMO has the advantage that it is relatively easy to implement although it does have some disadvantages in that the processing is required in the receiver. The use of SIMO may be quite acceptable in many applications, but where the receiver is located in a mobile device such as a cellphone handset, the levels of processing may be limited by size, cost and battery drain.

There are two forms of SIMO that can be used:

- *Switched diversity SIMO:* This form of SIMO looks for the strongest signal and switches to that antenna.
- *Maximum ratio combining SIMO:* This form of SIMO takes both signals and sums them to give the a combination. In this way, the signals from both antennas contribute to the overall signal.

MIMO - MISO

MISO is also termed transmit diversity. In this case, the same data is transmitted redundantly from the two transmitter antennas. The receiver is then able to receive the optimum signal which it can then use to receive extract the required data.

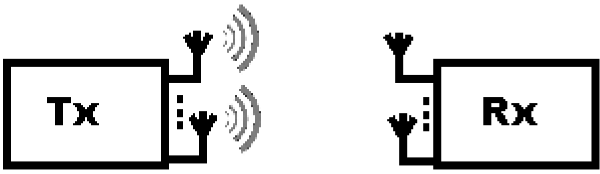


MISO - Multiple Input Single Output

The advantage of using MISO is that the multiple antennas and the redundancy coding / processing is moved from the receiver to the transmitter. In instances such as cellphone UEs, this can be a significant advantage in terms of space for the antennas and reducing the level of processing required in the receiver for the redundancy coding. This has a positive impact on size, cost and battery life as the lower level of processing requires less battery consumption.

MIMO

Where there are more than one antenna at either end of the radio link, this is termed MIMO - Multiple Input Multiple Output. MIMO can be used to provide improvements in both channel robustness as well as channel throughput.



MIMO - Multiple Input Multiple Output

In order to be able to benefit from MIMO fully it is necessary to be able to utilise coding on the channels to separate the data from the different paths. This requires processing, but provides additional channel robustness / data throughput capacity.

There are many formats of MIMO that can be used from SISO, through SIMO and MISO to the full MIMO systems. These are all able to provide significant improvements of performance, but generally at the cost of additional processing and the number of antennas used. Balances of performance against costs, size, processing available and the resulting battery life need to be made when choosing the correct optio

Shannon's Law and MIMO spatial multiplexing

As with many areas of science, there a theoretical boundaries, beyond which it is not possible to proceed. This is true for the amount of data that can be passed along a specific channel in the presence of noise. The law that governs this is called Shannon's Law, named after the man who formulated it. This is particularly important because MIMO wireless technology provides a method not of breaking the law, but increasing data rates beyond those possible on a single channel without its use.

Shannon's law defines the maximum rate at which error free data can be transmitted over a given bandwidth in the presence of noise. It is usually expressed in the form:

$C = W \log_2(1 + S/N)$

Where C is the channel capacity in bits per second, W is the bandwidth in Hertz, and S/N is the SNR (Signal to Noise Ratio).

From this it can be seen that there is an ultimate limit on the capacity of a channel with a given bandwidth. However before this point is reached, the capacity is also limited by the signal to noise ratio of the received signal.

In view of these limits many decisions need to be made about the way in which a transmission is made. The modulation scheme can play a major part in this. The channel capacity can be increased by using higher order modulation schemes, but these require a better signal to noise ratio than the lower order modulation schemes. Thus a balance

exists between the data rate and the allowable error rate, signal to noise ratio and power that can be transmitted.

While some improvements can be made in terms of optimising the modulation scheme and improving the signal to noise ratio, these improvements are not always easy or cheap and they are invariably a compromise, balancing the various factors involved. It is therefore necessary to look at other ways of improving the data throughput for individual channels. MIMO is one way in which wireless communications can be improved and as a result it is receiving a considerable degree of interest.

MIMO spatial multiplexing

To take advantage of the additional throughput capability, MIMO utilises several sets of antennas. In many MIMO systems, just two are used, but there is no reason why further antennas cannot be employed and this increases the throughput. In any case for MIMO spatial multiplexing the number of receive antennas must be equal to or greater than the number of transmit antennas.

To take advantage of the additional throughput offered, MIMO wireless systems utilise a matrix mathematical approach. Data streams t1, t2, . . . tn can be transmitted from antennas 1, 2, . . . n. Then there are a variety of paths that can be used with each path having different channel properties. To enable the receiver to be able to differentiate between the different data streams it is necessary to use. These can be represented by the properties h12, travelling from transmit antenna one to receive antenna 2 and so forth. In this way for a three transmit, three receive antenna system a matrix can be set up:

r1 = h11 t1 + h21 t2 + h31 t3
r2 = h12 t1 + h22 t2 + h32 t3
r3 = h13 t1 + h23 t2 + h33 t3
Where r1 = signal received at antenna 1, r2 is the signal received at antenna 2 and so forth.

In matrix format this can be represented as:

[R] = [H] x [T]
To recover the transmitted data-stream at the receiver it is necessary to perform a considerable amount of signal processing. First the MIMO system decoder must estimate the individual channel transfer characteristic hij to determine the channel transfer matrix. Once all of this has been estimated, then the matrix [H] has been produced and the transmitted data streams can be reconstructed by multiplying the received vector with the inverse of the transfer matrix.

$[T] = [H]^{-1} \times [R]$
This process can be likened to the solving of a set of N linear simultaneous equations to reveal the values of N variables.

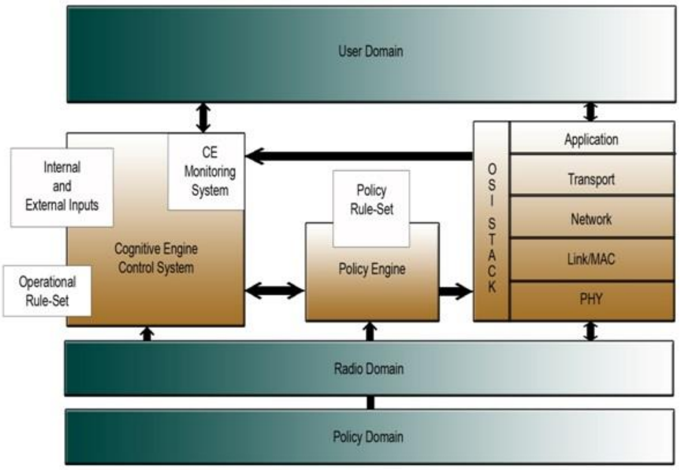
In reality the situation is a little more difficult than this as propagation is never quite this straightforward, and in addition to this each variable consists of an ongoing data stream, this nevertheless demonstrates the basic principle behind MIMO wireless systems.

COGNITIVE RADIO CONCEPT ARCHITECTURE

There are two major subsystems in a cognitive radio; a cognitive unit that makes decisions based on various inputs and a flexible SDR unit whose operating software

provides a range of possible operating modes. A separate spectrum sensing subsystem is also often included in the architectural a cognitive radio to measure the signal environment to determine the presence of other services or users. It is important to note that these subsystems do not necessarily define a single piece of equipment, but may instead incorporate components that are spread across an entire network. As a result, cognitive radio is often referred to as a cognitive radio system or a cognitive network.

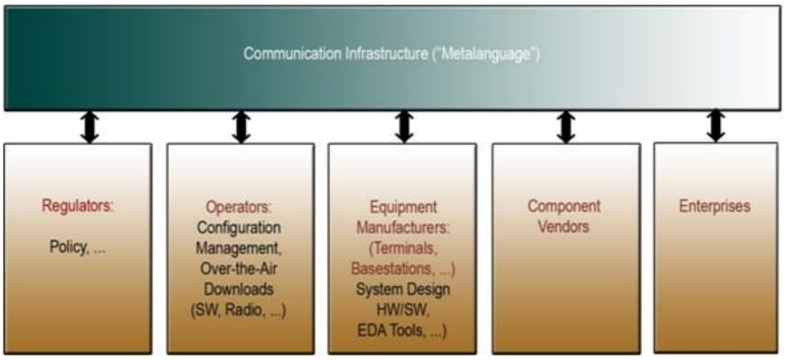
The cognitive unit is further separated into two parts as shown in the block diagram below. The first labeled the "cognitive engine" tries to find a solution or optimize a performance goal based on inputs received defining the radio's current internal state and operating environment. The second engine is the "policy engine" and is used to ensure that the solution provided by the "cognitive engine" is in compliance with regulatory rules and other policies external to the radio.



Cognitive Radio Concept Architecture

Enabling Architectures Supporting Cognitive Radio and Dynamic Spectrum Access
Support for cognitive radio and dynamic spectrum access requires a number of enabling technologies that are under development by the members of the Wireless Innovation Forum:

- **Information Process Architecture: Understanding the current state of complex information systems and their associated communications subsystems to determine how to enhance them from a process perspective, and analyze them for opportunities to interact with other systems is a key problem. An information process architecture solves this problem by providing a top-down model and a series of tools for depicting the structure of complex systems to aid in defining, designing and selecting relevant cognitive radio processes and to facilitate an improved understanding of the structure and relationships between systems that span user domains.**
- **Modeling Language: Flexible and efficient communication protocols are required between advanced radio systems and subsystems to support next generation features such as vertical and horizontal mobility, spectrum awareness, dynamic spectrum adaption, waveform optimization, feature exchanges, and advanced applications. A modeling language built on detailed use cases, and defining the signalling plan, requirements and technical analysis of the information exchanges provides the basis for developing specifications and standards supporting these capabilities.**


Communication Infrastructure ("Metalanguage")
Regulators: Policy, ...
Operators: Configuration Management, Over-the-Air Downloads (SW, Radio, ...)
Equipment Manufacturers: (Terminals, Basestations, ...) System Design HW/SW, EDA Tools, ...)
Component Vendors
Enterprises

A modeling language, or meta-language, expressed in a formal declarative language that is machine readable defines the communications infrastructure of the cognitive radio [source]

- **Radio Environment Map: Operation of a cognitive engine requires data and meta-data defining the spectral environment that a terminal is operating in at a given moment in time. Referred to as the radio environment map, this data can include information on spectrum economic transactions, dropouts, handovers, available networks, and services. Data contained within the map is derived, in part, by capturing and synthesizing measurements from many radios, and may be stored in a database that can be accessed remotely by the cognitive engine. Requirements for a database structure enabling this access including standardized database structures, data formats and functionality must be defined to support the flexibility necessary to accommodate current and future cognitive radio spectrum applications, such as mobility, spectrum economic transactions, dropouts, handovers, available networks, and services.**
- **Test and Measurement: Cognitive radios pose unique test challenges in quantifying the performance of critical functions such as spectrum sensing, interference avoidance, database performance, and adherence to policy. Test methodologies supporting these challenges must be developed must consider a range of hardware platforms, protocols, algorithms, use cases, and spectrum stakeholder requirements. Test equipment functionality and performance, test interfaces and test modes must also be taken into account.**

LTE

Introduction:

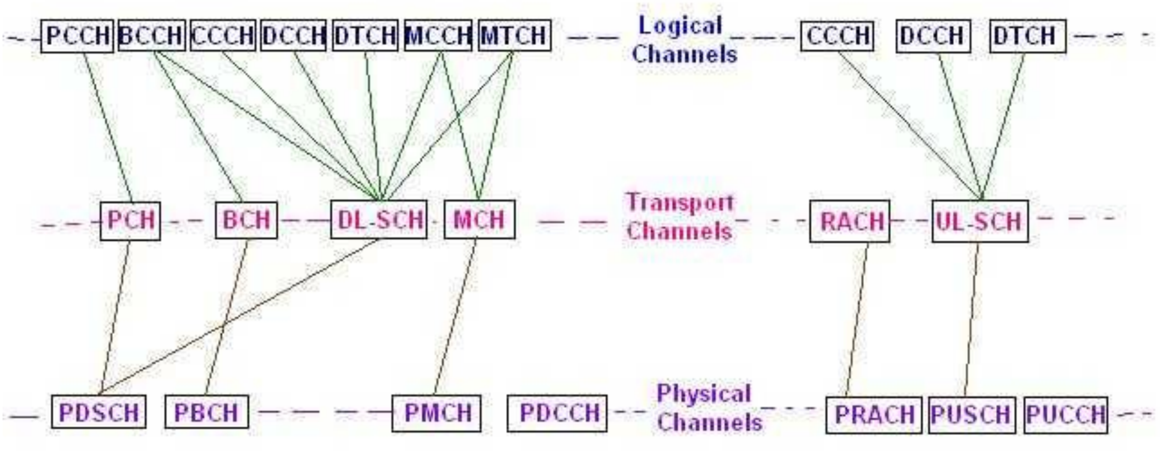
LTE standard has been published by 3GPP as an extension of UMTS(based on 3GPP standard) and 1xEV-DO(base on 3GPP2 standard) technologies. LTE is mainly designed for high speed data applications both in the uplink and downlink. LTE network offers about 300Mbps data rate in the downlink and about 75 Mbps in the uplink. There is possibility of supporting voice over LTE(VoLTE) in the future. There are various methods under progress to support VoLTE some of them includes VOIP, legacy fallback to previous existing wireless networks.

LTE Air interface

The Air interface between LTE network and UE supports high data rate owing to OFDM and Multiple antenna techniques employed. OFDMA is used from network to UE air interface and SC-FDMA is used from UE to network air interface. Refer

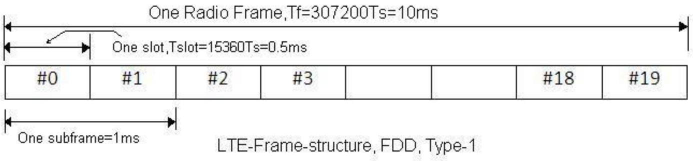
following links to know OFDMA basics. OFDMA Types OFDM versus OFDMA OFDMA Physical layer

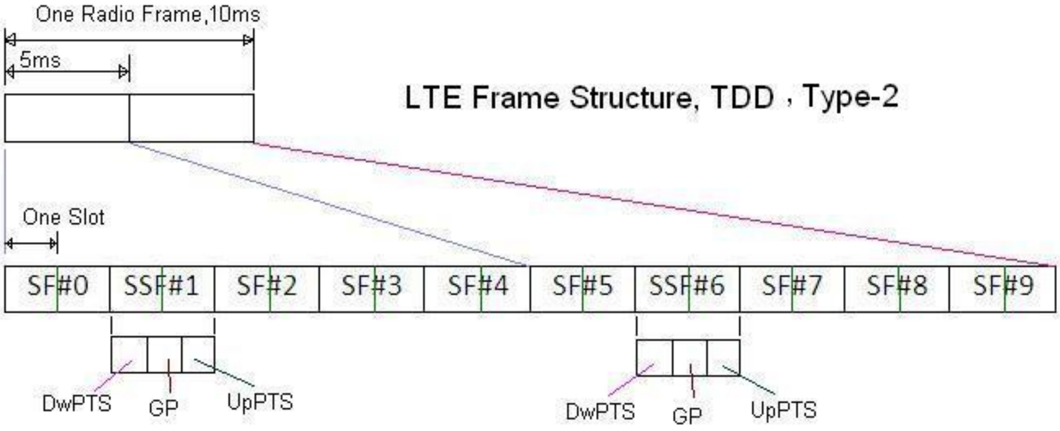
LTE Channels



The channels in LTE system are mainly categorized into logical, transport and physical channels based on their functions. The downlink channels are PBCH, PDSCH, PDCCH, PMCH, PCH etc. The uplink channels are PRACH, PUSCH and PUCCH.

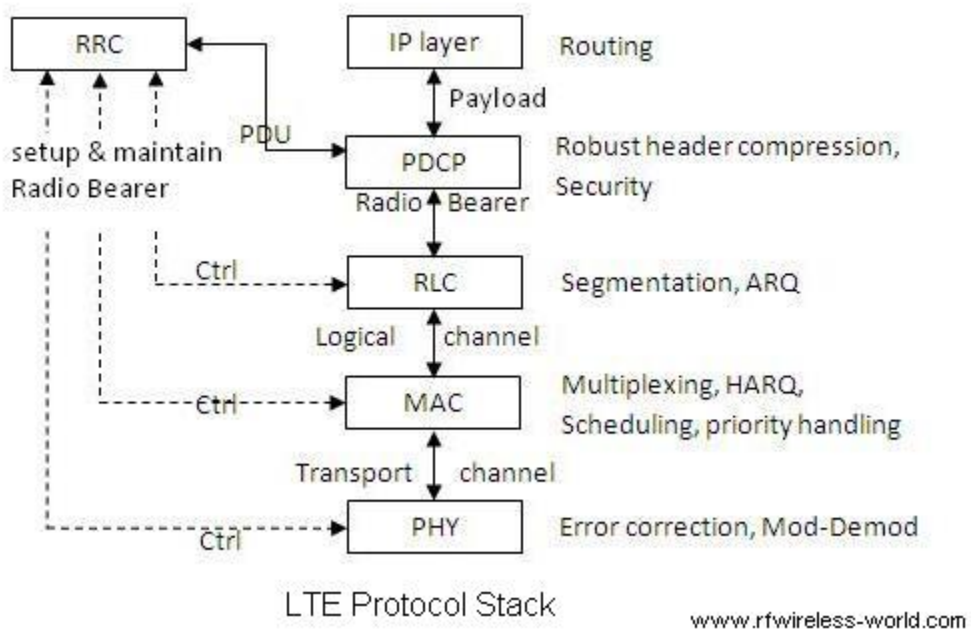
LTE Frame structure


One Radio Frame,Tf=307200Ts=10ms
One slot,Tslot=15360Ts=0.5ms
#0
#1
#2
#3
#18
#19
One subframe=1ms
LTE-Frame-structure, FDD, Type-1



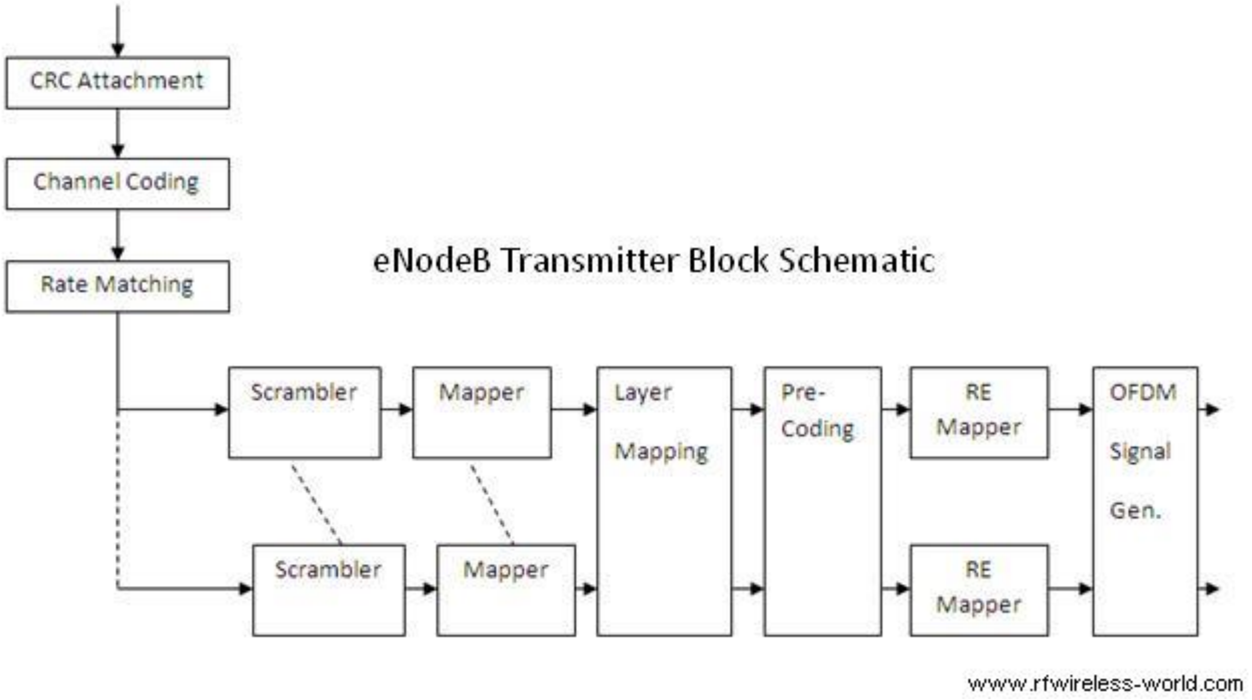
LTE frame is 10 ms in duration and consists of 10 subframes. Each subframe consists of two slots. The frame structure is different for FDD and TDD topologies. Refer LTE Frame >>.

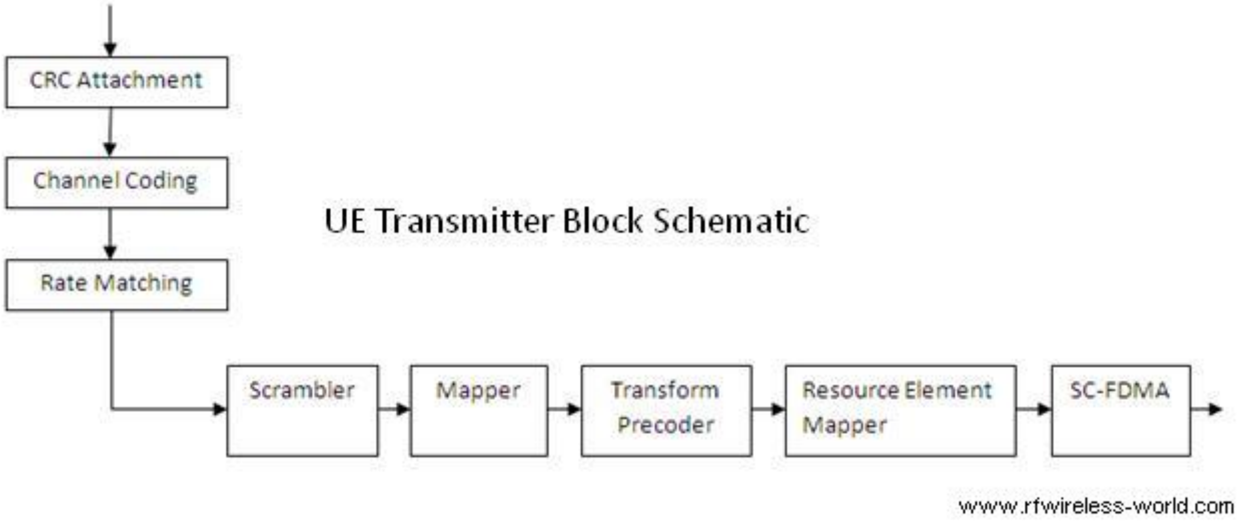
LTE Protocol Stack



The stack consists of different layers viz. Physical, MAC, RLC, PDCP and RRC as shown in the figure. Refer LTE stack >>.

LTE Physical layer

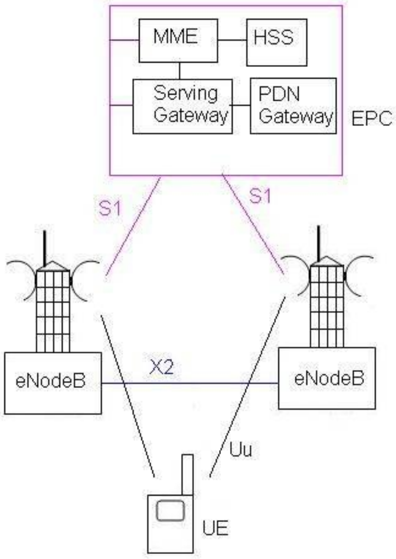




The figure depicts LTE eNodeB physical layer and LTE UE physical layer transmitter modules.

Refer LTE Physical Layer >> for more information.

LTE System Architecture Evolution



As shown in the figure LTE SAE(System Architecture Evolution) consists UE,eNodeB and EPC(evolved packet core). Various interfaces are designed between these entities which include Uu between UE and eNodeB, X2 between two eNodeB, S1 between EPC and eNodeB. eNodeB has functionalities of both RNC and NodeB as per previous UMTS architecture.LTE is completely IP based network.

The basic architecture contains the following network elements.
1. LTE EUTRAN (Evolved Universal Terrestrial Radio)
2. LTE Evolved Packet Core.

LTE EUTRAN

It is a radio access network standard meant to be a replacement of the UMTS, HSDPA and HSUPA . Unlike HSPA, LTE's E-UTRA is an entirely new air interface system. It provides higher data rates, lower latency and is optimized for packet data. EUTRAN (Evolved Universal Terrestrial Radio) consists of eNB (Base station). EUTRAN is responsible for complete radio management in LTE. When UE powered is on, eNB is responsible for Radio Resource Management, i.e. it shall do the radio bearer control, radio admission control, allocation of uplink and downlink to UE etc. When a packet from UE arrives to eNB, eNB shall compress the IP header and encrypt the data stream. It is also responsible for adding a GTP-U header to the payload and sending it to the SGW. Before the data is actually transmitted the control plane has to be established. eNB is responsible for choosing a MME using MME selection function. The QoS is taken care by eNB as the eNB is only entity on radio. Other functionalities include scheduling and transmission of paging messages, broadcast messages, and bearer level rate enforcements also done by eNB.

LTE Evolved Packet Core (EPC)

The LTE EPC consists of MME, SGW, PGW, HSS and PCRF.

PART-A

1.Define Wifi and its advantages.
2,Define Wifi hotspot.
3.List the several specifications in 802.11 family.
4.What are the two types of usage models in IEEE802.16 working groups?
5.Compare Wimax and Wifi.
6.State the working principle of OFDM.
7.Define OFDMA.
8.What are the different diversity modes available in MIMO?
9.Define SISO and MISO.
10.Define Cognitive radio network.

PART-B

1.Discuss about Wifi technology.

2.Compare the WIMAX and WIFI technology.

3.Explain about OFDM and OFDMA.

4.Discuss about MIMO technology.

5. Explain about the Cognitive radio network.

6.Discuss in detail about LTE.

TEXT BOOK / REFERENCE BOOKS

1. Andreas F. Molisch, “Wireless Communications”, 2nd Edition, John Wiley & Sons Ltd, 2011.

2. William C.Y. Lee., "Wireless & Cellular Telecommunications", 3rd edition, McGraw Hill.2006.

3. Yibing Lin, "Wireless & mobile Network architecture", Wiley 2002.

4. Tao Jiang, Lingyang Song and Van Zhang, “Orthogonal Frequency Division Multiple Access Fundamentals and Applications” Taylor and Francis Group, 2010.

5. Yong Soo Cho, Jaekwon Kim, Won Young Yang and Chung G. Kang, “MIMO-OFDM Wireless Communications with MATLAB”, John Wiley & Sons (Asia) Pvt. Ltd, 2010.