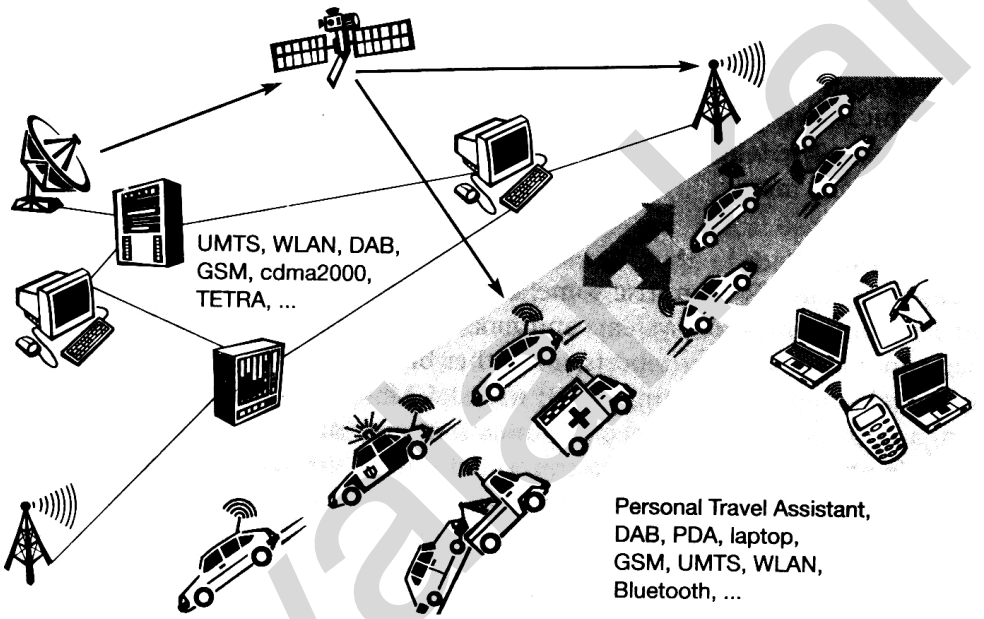
APPLICATIONS

1. Vehicles

Cars driving in the same area build ad–hoc network for the fast exchange of information. In emergency situation or to help each other keep a safe distance. In the future, cars will also inform other cars about accidents via the ad–hoc network, to help them slow down in the time even before a driver can recognize an accident



A typical application of mobile communications : road traffic.

Networks with a fixed infrastructure like cellular phones (GSM, UMT) will be interconnected with trunked radio systems (TETRA) and wireless. LAN, (WLAN). Satellite links can also be used. The networks between cars and inside each car will more likely work in an ad–hock fashion. Wireless pico networks inside a car can comprise personal digital assistants (PDA), laptops, or mobile phones, e.g. connected with each other using the Bluetooth technology.

2. Emergencies

Wireless networks are the only means of communication in the case of natural disasters such as hurricanes or earthquake. In the worst cases, only decentralized, wireless ad–hoc network survive.

3. Business

A traveling salesman today needs instant access to the company's database to ensure that files on his or her laptop reflect the current situation, to enable the company to keep track of all activities of their traveling employees, to keep databases consistent etc. With wireless access, the laptop can be turned into a true mobile

office, but efficient and powerful synchronization mechanism are needed to ensure data consistency.

4. Replacement of wired networks

Wireless networks can also be used to replace wired networks, e.g. remote sensors, for tradeshows, or in historic building. Due to economic reasons, it is often impossible to wire remote sensors for weather forecasts, earthquake detection, or to provide environmental information. Wireless connections, e.g. via satellite can help in this situation.

5. Infotainment and more

Static information might be loaded via CD–ROM, DVD, or even at home via the internet. But wireless networks can provide up–to–date information at any appropriate location. Another field of wireless network application lies in entertainment and games to enable, e.g. ad–hoc gaming network as soon as people meet to play together.

6. Location dependent Services :

(a) Follow on services
(b) Location aware services
(c) Privacy
(d) Information services
(e) Support services

7. Mobile and Wireless devices :

(a) Sensor
(b) Embedded Controllers
(c) Pager
(d) Mobile Phones
(e) Personal digital Assistant
(f) Pocket computer
(g) Notebook / laptop.

A SHORT HISTORY OF WIRELESS COMMUNICATION

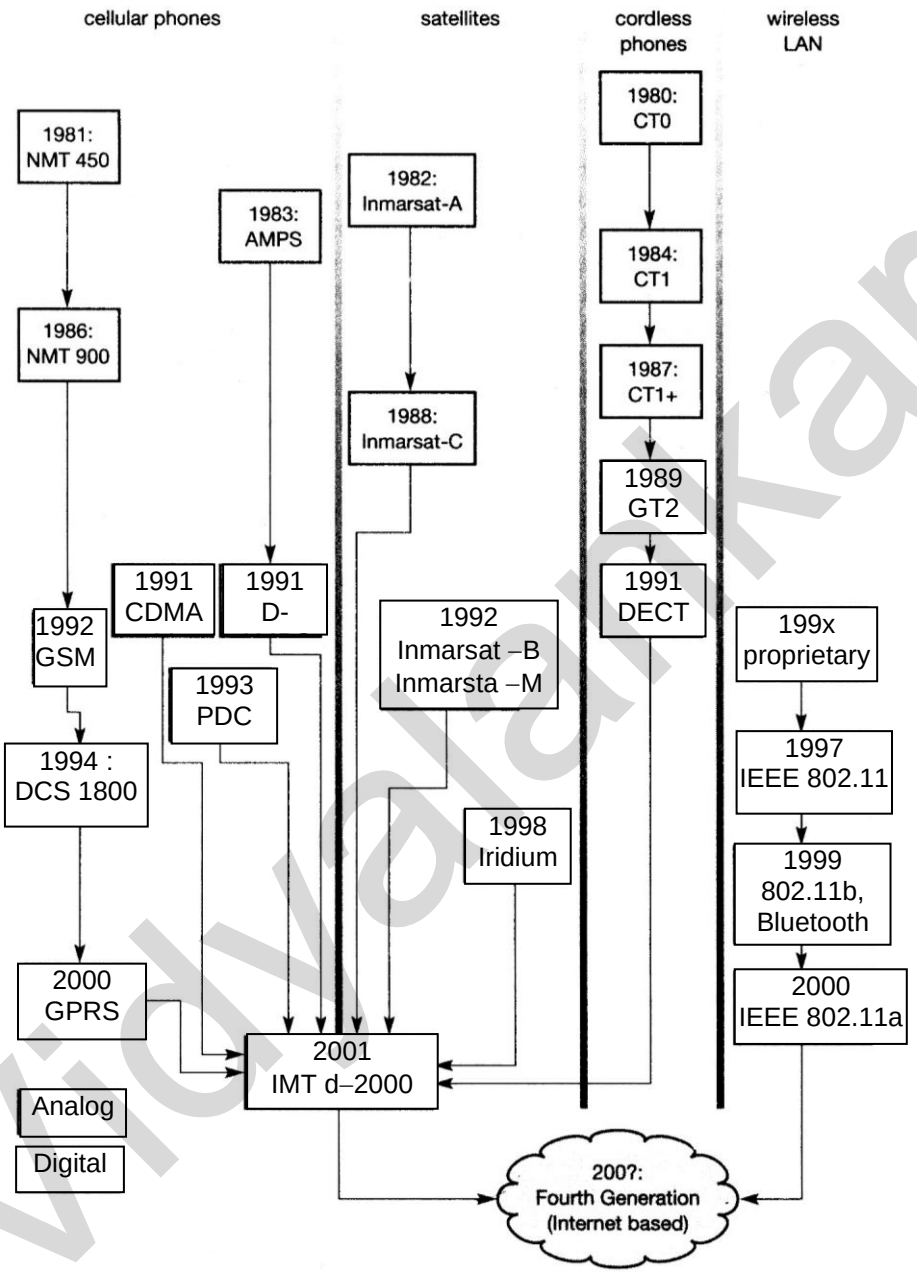
Wired communication started with the first commercial telegraph line between Washington and Baltimore in 1843, and Alexander Graham Bell's invention and marketing of the telephone in 1876. All optical transmission system suffer from the high frequency of the carrier light. At that time it was not possible to focus light as efficiently as can be done today by means of a laser, wireless communication did not really take off until the discovery of electromagnetic waves and the development of the equipment to modulate them.

It all started with Michael Faraday, demonstrating electromagnetic induction in 1831 and James C Maxwell (1831 – 79) laying the theoretical foundations for electromagnetic fields with his famous equations. Heinrich Hertz (1857 – 94) was the first to demonstrate character of electrical transmission through space (1886), thus proving Maxwell's equation, "Unit Hz" reminds this history. Guglielmo Macroni (1874–1937) gave the first demonstration of wireless telegraphy in 1895 using long wave transmission power

(7200 kw). The first radio broadcast took place in 1906 when Reginald, A Fessenden (1866 – 1932) transmitted voice and music for Christmas. In 1915 first wireless voice transmission was set up between New York and San Francisco. The invention of the electronic vacuum tube in 1906 by Lee Deforest (1873–1961) and Robert Von Liben (1878– 1913) helped to reduce the size of sender and receiver. The first car radio was commercially available in 1927. John. L Baird (1888– 1946) transmitted TV across the Atlantic and demonstrated color TV, the station WYG (Schenectady, NY) started regular TV broadcacsts and the first TV news. The first teleteaching started in 1932 from the CBS station W2XAB.

One big step forward in this respect was the invention of frequency modulation. In 1933 by Edwin H Armstrong. After the second world was many national and international projects in the area of wireless communication were triggered off. In 1983 the US system, advanced mobile phone system (AMPS) started. (EIA, 1989). The early 1990s marked the beginning of fully digital systems. In 1991, ETSI adopted the standard digital European cordless telephone(DECT) for digital cordless telephones. Today DECT has been renamed digital enhanced cordless telecommunication for marketing reasons and to reflect the capabilities of DECT to transport multimedia data streams. GSM was standardized in a document of more than 5,000 pages in 1991. This first version of GSM, now called, global system for mobile communication, works at 900MHz and uses 124 full duplex channels. Many proprietary wireless local area network systems already existed when ETSI standardized the high performance radio local area network (HIPERLAN) in 1996. 1998 marked the beginning of mobile communication using satellites with the Iridium system (Iridium, 2002). In 1998 the Europeans agreed on the universal mobile telecommunication systems (UMTS) as the European proposal for the International Telecommunication Union (ITU) IMT – 2000 (International Mobile Telecommunication). 1999 saw several more powerful WLAN standards. IEEE published. 802.11b offering 11Mbit/s at 2.4GHz. The same spectrum is used by Bluetooth, a short range technology to set–up wireless personal area networks with gross data rates less then 1Mbit/s.

The wireless application protocol (WAP) started at the same time as i–mode in Japan. The year 2000, came with higher data rates and packet – oriented transmission for GSM. Third generation of mobile communication gross data rates of 54 Mbit/s. In 2002 new WLAN developments followed. Examples are 802.11g offering upto 54 Mbit/s at 2.4GHz and many new Bluetooth applications. No one knows exactly what the next generation of mobile and wireless system will look like, but there are strong indicators that it will be widely Internet based the system will use Internet protocols and Internet applications.



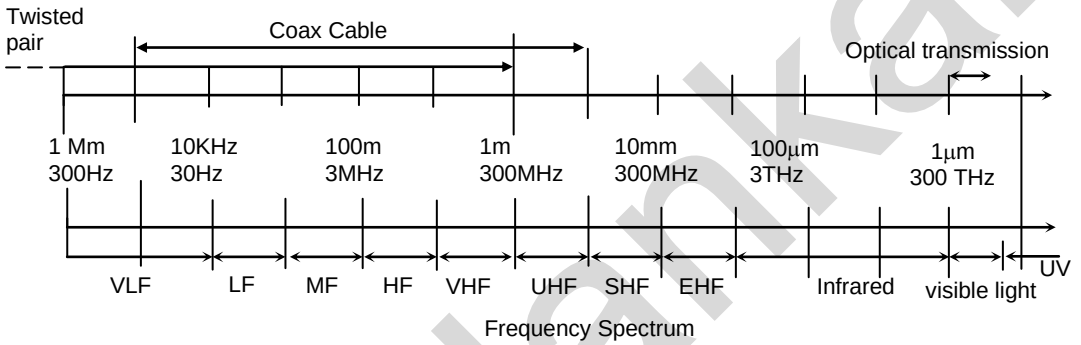
Overview of some wireless communication systems

FREQUENCY FOR RADIO TRANSMISSION

Radio transmissions can take place using many different frequency bands. Radio transmission starts at several KHz, the very low frequency (VLF) range. These are very long waves. Waves in the low frequency (LF) range are used by submarines, because they can penetrate water and can follow the earth's surface. Some radio stations still use

these frequencies, e.g. between 148.5KHz and 283.5KHz in Germany. The medium frequency (MF) and high frequency (HF) ranges are typical for transmission of hundreds of ratio stations, either as amplitude modulation (AM) between 520 KHz. and 1605.5 KHz as short wave (SW) between 5.9MHz and 26.1 MHz or as frequency modulation (FM) between 87.5MHz and 108MHz. The frequencies limiting these ranges are typically fixed by national regulation and vary from country to country short waves are typically used for (amateur) radio transmission around the world, enabled by reflection at the ionosphere (layer in space). Transmit power is upto 500kw which is quite high compared to the 1w of a mobile phone. All radio frequencies are regulated to avoid interference e.g. the German regulation covers 9KHz – 275GHz.

The figure shows frequencies starting at 300Hz and going up to over 300THz.



Frequency Spectrum

Above figure gives a rough overview of the frequency spectrum that can be used for data transmission. Directly coupled to the frequency is the wavelength λ via the equation :

$\lambda = C / f$, where $c \cong 3.10^8$m/s and f the frequency.

SIGNALS

Signals are functions of time and location. The most interesting and typical types of signals for radio transmission are periodic signals, especially sine waves as carriers. General function for sine wave is

$g(t) = A_t \sin(2\pi f_t t + \phi_t t)$

where A : Amplitude
f : frequency
ϕ : phase shift

Finally, the phase shift determines the shift of the signal relative to the same signal without a shift ϕ. An example for shifting a function is shown in figure given below.

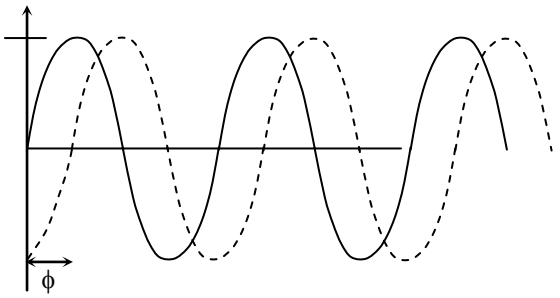


Fig.: Time domain representation of a signal

Sine waves are of special interest, as it is possible to construct every periodic signal "g" by using sine and cosine functions according to fundamental equation of fourier :

$$g(t) = \frac{1}{2}c + \sum_{n=1}^{\infty} a_n \sin(2\pi nft) + \sum_{n=1}^{\infty} b_n \cos(2\pi nft)$$

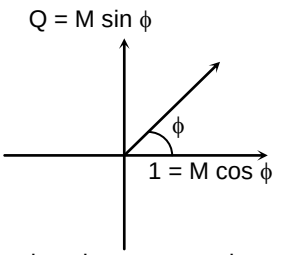
In this equation the parameter c determines the Direct current (DC) component of the signal, the coefficients a_n and b_n are the amplitudes of the n^{th} sine and cosine function. The frequencies of these functions (the so–called harmonics) increase with a growing parameter n and are a multiple of the fundamental frequency f. A typical way to represent signals is the time domain. Here the amplitude A of a signal is shown versus time.

If a signal consists of many different frequencies the representation in time domain is problematic, in such case a better representation of a signal is the frequency domain. Here the amplitude of a certain frequency part of the signal is shown versus the frequency.

Frequency domain presentation of a signal

A third way to represent signal is the phase domain shown in figure given below.

This representation also called phase state or signal constellation diagram, shows the amplitude M of a signal and its phase ϕ in polar co-ordinates. (The length of the vector represents the amplitude, the angle the phase shift). The x–axis represents a phase of 0 and is also called in phase (I). A phase shift of 90° or $\pi/2$ would be a point on the y–axis, called Quadrature (Q).



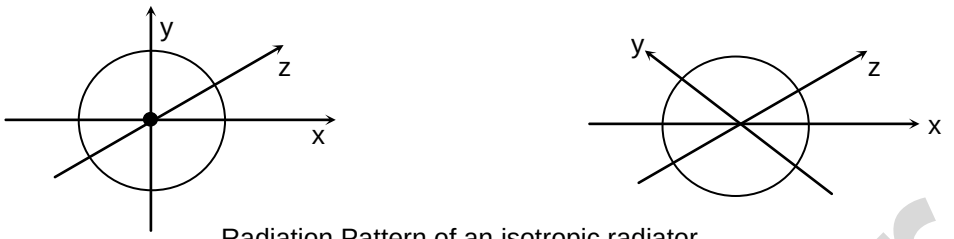
Phase domain representation of a signal

ANTENNAS

Antennas couple electromagnetic energy to and from space to and from a wire or coaxial cable (or any other appropriate conductor).

A theoretical reference antenna is the isotropic radiator, a point in space radiating equal power in all directions i.e. all points with equal power are located on a sphere with the antenna as its centre.

The radiation pattern is symmetric in all directions.

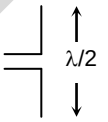


Radiation Pattern of an isotropic radiator

Real antennas all exhibit directive effects (intensity of radiation is not the same in all directions from the antenna. Simplest real antenna is a thin, center–fed, dipole, called, Hertzian dipole as shown in figure given below. The dipole consists of two collinear conductors of equal length, separated by a small feeding gap.

λ = wavelength

A $\lambda/2$ dipole has a uniform or omni-directional radiation pattern in one plane and a figure eight pattern in the other two planes as shown in figure.



Directional antennas with certain fixed preferential transmission and reception directions can be used in case of failure of omni directional radiation pattern.

Several directed antennas can be combined on a single pole to construct a sectorised antenna.

Multi element antenna arrays, allow different diversity schemes. (Two or more antennas combined to improve reception by counteracting negative effects of multipath propagation.

Switched diversity or selection diversity is the example of above scheme in which receiver always uses the antenna element with the largest output. Diversity computing combining constitutes a combination of the power of all signals to produce gain. A more advanced solution is provided by smart antennas which combine multiple antenna elements with signal processing to optimize the radiation / reception pattern in response to the signal environment.

SIGNAL PROPAGATION

In wireless networks, the signal has no wire to determine the direction of propagation, where as signals in wired networks only travel along the wire. (for e.g. coax cable, fiber etc)

For wireless transmission predictable behavior is only valid in vacuum (i.e. without matter between the sender and the receiver. Situations would be as follows :

1. Transmission range : Within certain radius of sender transmission is possible.
2. Detection range : Within a second radius, detection of transmission is possible.
3. Interference range : Within a third even larger radius, the sender may interfere with other transmission by adding to the background noise.

- **Path Loss of Radio Signals**

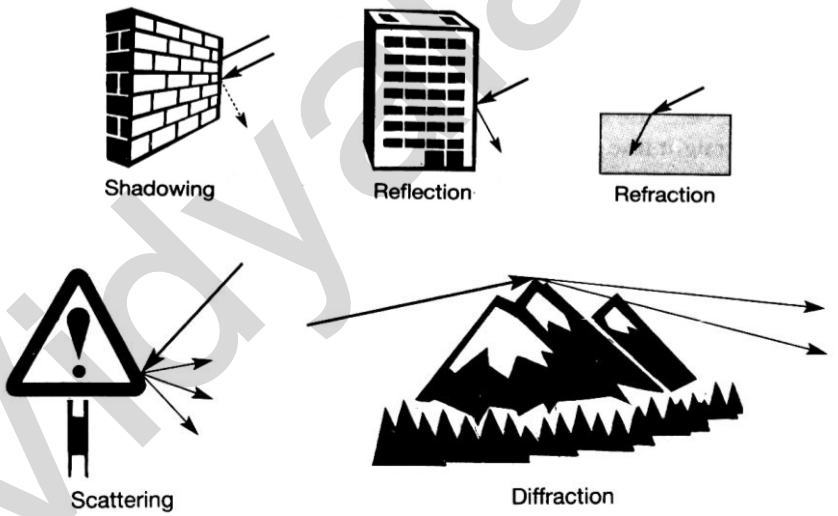
Most radio transmission takes place through the atmosphere –signal, travel through air, rain snow, fog dust particles, smog, etc. while the path loss or attenuation does not cause too much trouble for short distances e.g. for LANs. Even mobile phone systems are influence by weather condition as heavy rain. Rain can absorb much of radiated energy of the antenna. Radio waves can exhibit three fundamental propagation behaviors depending on their frequency.

1. Ground wave (<2MHz) : Such low frequencies follow earth's surface can propagate long distances.
   Usage : Submarine communication or AM radio.
2. Sky wave (2–30 MHz) : Many international broadcasts and amateur radio use these short waves that are reflected in ionosphere.
3. Line of sight (>30MHz) : This enables direct communication with satellites or microwave links on the ground.

- **Additional Signal Propagation Effects**

An extreme form of attenuation is blocking or shadowing of radio signals due to large obstacles (Refer figure). The higher the frequency of a signal, the more it behaves like light.

Another effect is reflection of signals as shown in the middle in the figure. If an object is large compared to the wavelength of signal or the surface of the earth, the signal is reflected.

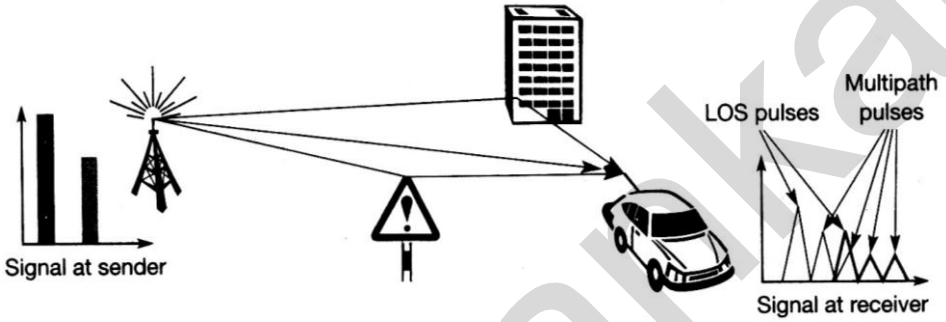


The more often the signal is reflected, the weaker it becomes. The right most figure shows refraction. If the size of an obstacle is in the order of wavelength or less then waves can be scattered. Many objects in the environment can cause these scattering effects. One more effect is diffraction of waves. In this, radio waves will be deflected at an edge and propagate in different direction.

- **Multi–path Propagation**

The propagation effects lead to one of the most severe radio channel impairments, called multipath propagation. Due to the finite speed of light, signals traveling along different paths with different lengths arrive at the receiver at different times. This effect is called delay spread, which means the original signal is spread due to different delays of parts of the signal. This delay spread is effect radio transmission, because no wire guides the waves along a single path as in case of wired networks. Effects of this delay spread on the signal representing data :

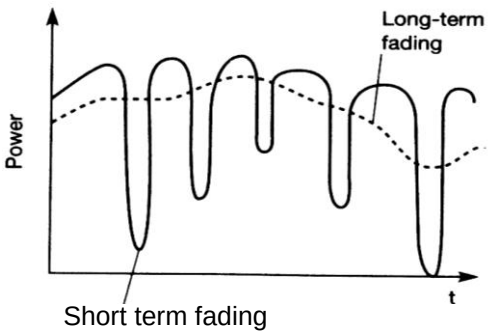
The first effect is that a short impulse will be smeared out into a broader impulse, or rather into several weaker impulses at the sender will result in three smaller impulses at the receiver.



Multi-path propagation and intersymbol interference

Now consider the second impulse as shown in above figure. On sender side, both impulses interfere are separated. Consider that each impulse should represent a symbol and that one or several symbols could represent a bit. The energy intended for one symbol now spills over to the adjacent symbol, this effect is called inter symbol interference (ISI). The higher the symbol rate to be transmitted, the worst the effects of ISI will be, because the original symbols are moved closer to each other.

The sender may first transmit a training sequence known by the receiver. The receiver then compares the received signal to the original training sequence and programs an equalizer that compensates for the distortion. While ISI and delay spread, already occur in the case of fixed radio transmitters and receivers, the situation is even worse if receivers or senders or both move. Then the channel characteristics change over time, and the paths a signal can travel along vary. This effect is well known (and audible) with analog radios while driving. The power of the received signal changes considerably over time. These quick changes in the received power are so called short term fading.



Short term & long term fading

The receiver has to try to constantly adapt to the varying channel characteristics. Long term fading of a received signal is caused by varying channel characteristics. For example varying distance to the sender or more remote obstacles. Generally, senders can compensate for long term fading by increasing / decreasing sending power so that received signal always stays within certain limit.

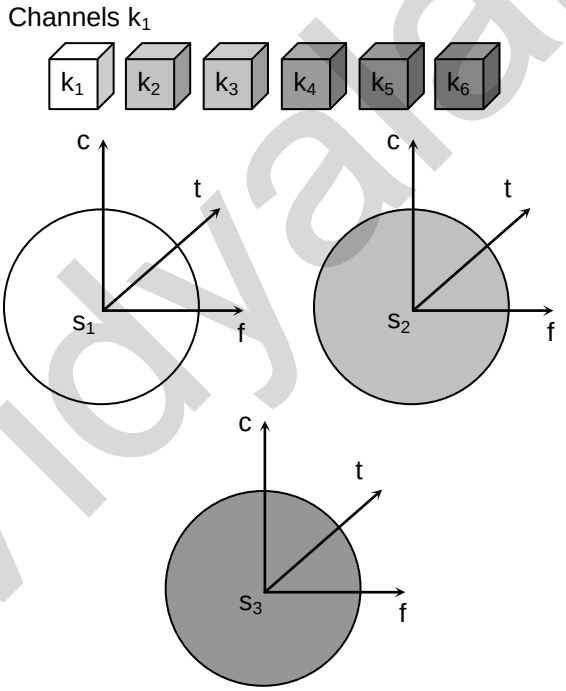
MULTIPLEXING

Multiplexing means how several users can share a medium with minimum or no interference. For wireless communication, multiplexing can be carried out in four dimension.
(i) space (ii) frequency (iii) time (iv) code.

(i) Space Division Multiplexing

Take an example in which there are six channels : ki and introduces a three dimensional co-ordinate system. This system shows the dimensions of code c, time t and frequency f. For this type of multiplexing, space division multiplexing is shown.

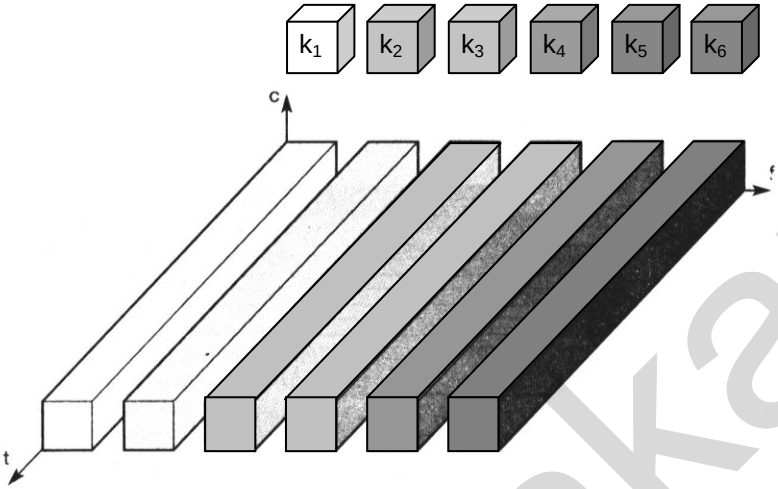
The channels k_1 to k_3 can be mapped onto three 'spaces'. s_1 to s_3 , which clearly separate the channels and prevent the interference ranges from overlapping. The space between eh interference ranges is sometimes called as guard space. Such a guard space is needed in all four multiplexing schemes represented. For remaining (k_4 to k_6) three additional spaces would be needed.



Space Division Multiplexing

In wireless transmission, SDM implies a separate sender for each communication channel with a wide enough distance between senders. This SDM is used at FM radio stations, where the transmission range is limited to a certain region. Many radio stations around the world can use the same frequency without interference.

(ii) Frequency Division Multiplexing



Frequency division multiplexing

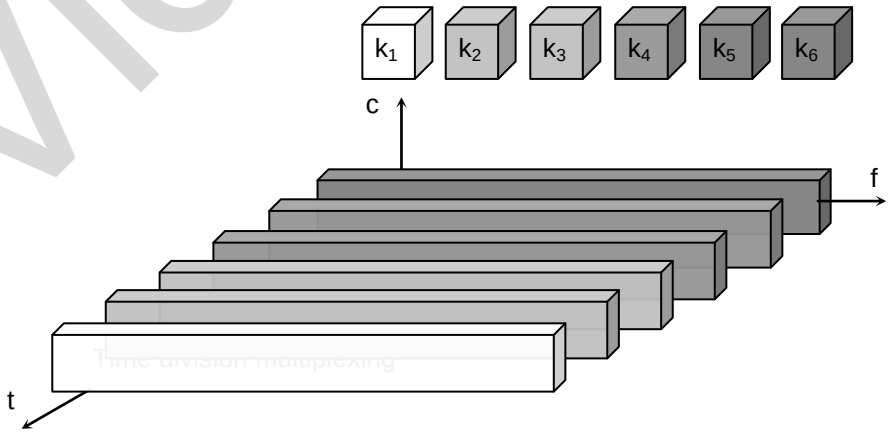
Frequency division multiplexing describes schemes to subdivide the frequency dimension into several non-overlapping frequency bands as shown in figure. Each channel is now allotted its own frequency band. Senders using a certain frequency band can use this band but guard spaces are always needed to avoid frequency band overlapping (adjacent channel interference). This is very simple scheme in which receiver only has to tune into the specific sender.

- **Disadvantages :**

1) Waste of frequency resources because separate frequency for each one is assigned.
2) Inflexibility and limitations to the number of senders.

(iii) Time Division Multiplexing

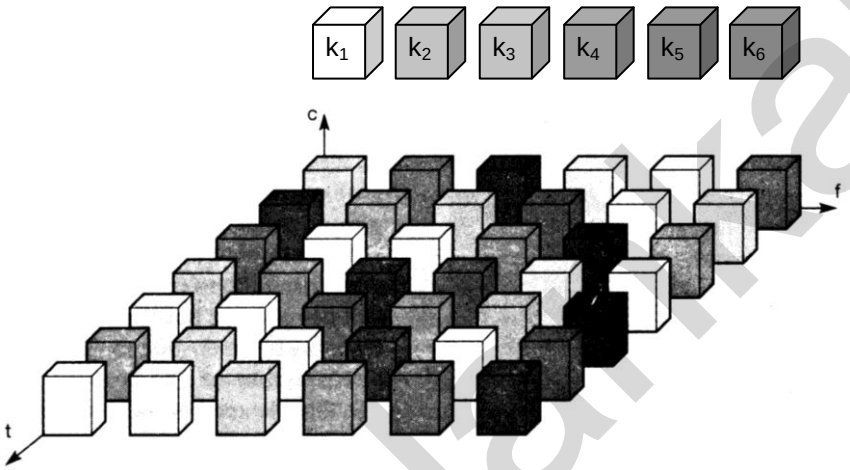
Time division multiplexing is a flexible scheme for mobile communication. In this a channel is given a whole bandwidth for a certain amount of time, means all senders use the same frequency but at different points in time. Guard spaces representing time gaps have to separate the different periods when the senders use the medium.



Time division multiplexing

To avoid interference, precise synchronisation between different senders is necessary. This is a drawback as all senders need precise clocks or alternatively a way has to be found to distribute a synchronization signal to all senders.

Frequency and time division multiplexing can be combined, i.e. a channel k_1 can use a certain frequency band for a certain amount of time as shown in figure below. Guard spaces are needed in both time and frequency dimension. This scheme provides some protection against tapping, as in this case sequence of frequencies a sender uses has to be known to listen into the channel.



Frequency and time division multiplexing combined.

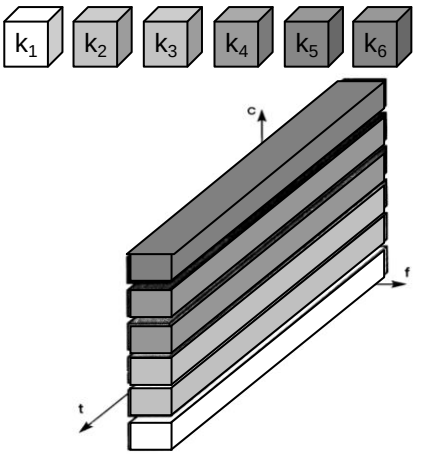
The mobile phone standard GSM uses this combination of frequency and time division multiplexing for transmission between a mobile phone and a so–called base station.

- **Disadvantage :**

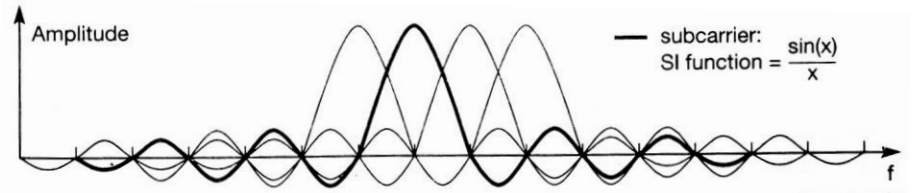
1) Two senders will interfere as soon as they select the same frequency at the same time.

(iv) Code Division and Multiplexing

Code division and multiplexing is used in may applications like military, civil due to inherent security features. In this scheme all channels k_i use the same frequency at the same time for transmission. Separation is now achieved by assigning each channel, it own 'code', guard spaces are realized, by using codes with the necessary 'distance' in code space e.g. orthogonal codes. Typical example of CDM is a party with many participants form different countries around the world who establish communication channels. i.e. they talk to each other, using the same frequency range at same time.



Code division multiplexing

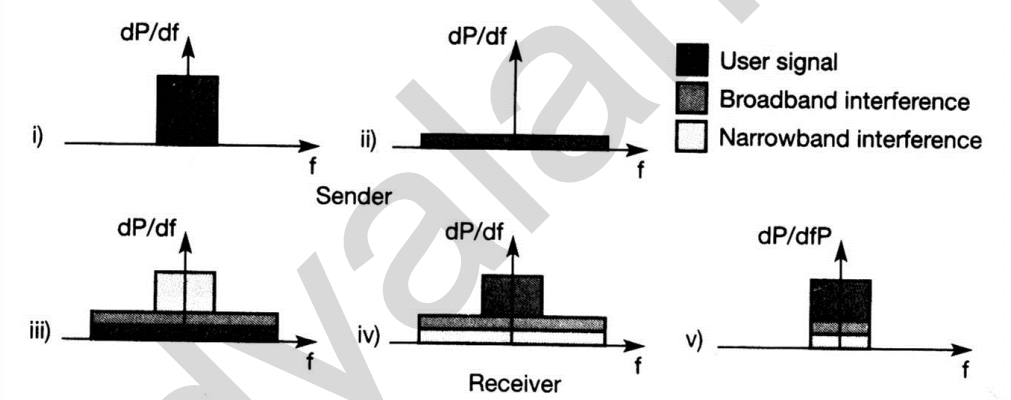


Superposition of orthogonal frequencies

- **Benefit of MCM**
  Using the above scheme, frequency selective fading influences some subcarriers and not the whole signal.
  MCM transmits symbols with guard spaces which helps the receiver to handle multipath propagation. OFDM is method of implementing MCM using orthogonal carriers.

SPREAD SPECTRUM (SPREADING BANDWIDTH NEEDED TO TRANSMIT DATA)

Spread spectrum is resistance to narrowband interference.
To understand working of spread spectrum Let's see a diagram.

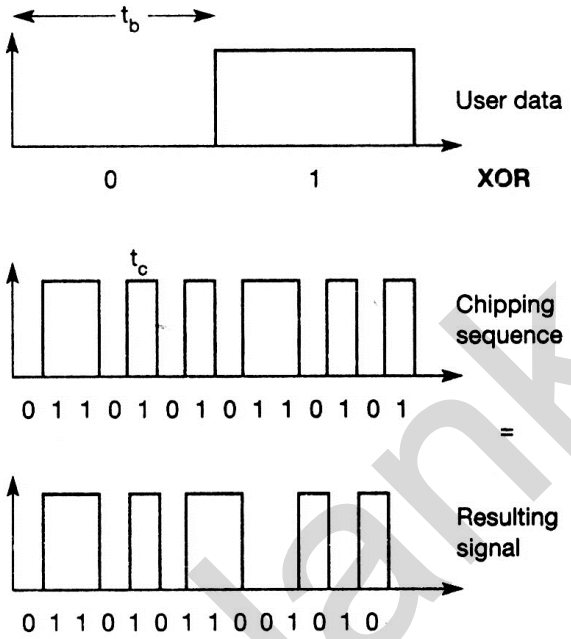


Super spectrum : Spreading and despreading

(i) Idealized narrow band signal from sender of user data.
(ii) Sender is spreading the signal. Converts narrowband signal into broadband signal, spread over larger frequency range.
(iii) &(iv) Sum of user signal and interference is received.
Receiver converts spread user signal into a narrowband signal again.
(iv) Receiver applies a bandpass filter to cut off frequencies. Left and right of narrowband signal.

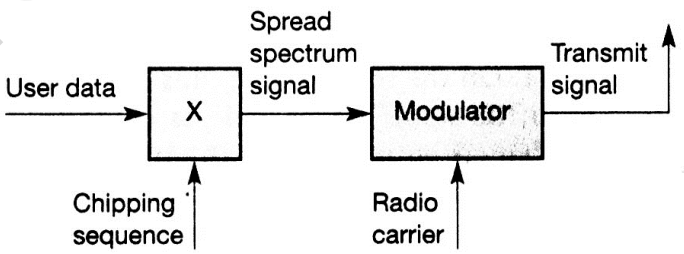
Disadvantage of spread spectrum is that the increased complexity of receivers that have to despread a signal. Second, the large frequency band is needed due to the spreading of signal

- **Direct Sequence spread spectrum (DSSS) :**
  Consider the following figure to understand DSSS Chipping sequence is referred to "digital modulation".



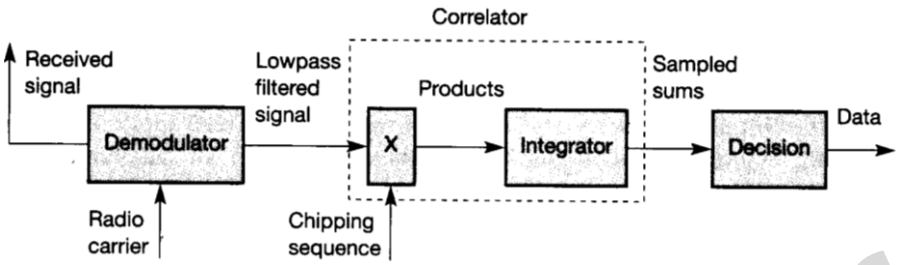
Spreading with DSSS

1. The user data (bit stream) is taken by DSSS and an XOR is performed with chipping sequence.
2. The result is either the sequence 0110101 or its complement 1001010.
3. Chipping sequence generated properly, appearing in random noise is called " pseudo–noise" sequence.
4. Spreading factor $s = t_b / t_c$ determines the bandwidth of resulting signal
   where t_b = duration of bit, t_c = duration of chips (pulses)
5. Original signal needs a bandwidth w, the resulting signal needs s. w. after spreading.



DSSS transmitter

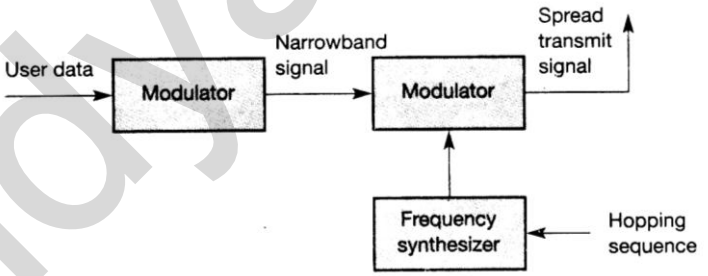
1. First step is the spreading of user data with the chipping sequence.
2. Spread signal is modulated with a radio carrier and then the signal is transmitted as radio carrier shift the signal to the carrier frequency.



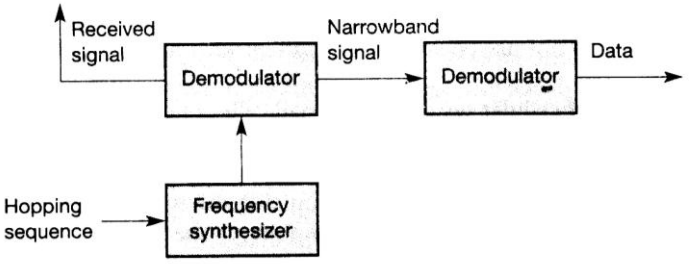
DSSS receiver

3. First step in receiver involves demodulating the received signal
4. Second step is the receiver has to know the original chipping sequence as that of transmitter.
5. Receiver calculates products of chip and signal using XOR calculating the products of chips and signal and adding products in integrator is called co–relation, the device co-relater.
6. In each bit period a decision unit samples the sums generated by integrator and decides if this sum represents a binary 1 and 0.
7. If transmitter and receiver are perfectly by noise or multi–path propagation.

- **Frequency Hopping Spread Spectrum**
  (Total available bandwidth is split into many channels of smaller bandwidth plus guard spaces between the channels)
  The pattern of channel usage is called the chopping sequence, the time spend on a channel with a 'certain frequency is called the dwell time.
  Slow hopping : The transmitter uses one frequency for several bit periods.
  Fast hopping : The transmitter changes the frequency several times during the transmission of single bit.



FHSS transmitter



FHSS receiver

1. The first step in an FHSS transmitter is the modulation of user data according to one of the digital to analog modulation schemes.
2. This results in a narrowband signal, if FSK is used with a frequency f_0 for a binary 0 and f_1 for a binary 1.
3. The next, hopping sequence is fed into a frequency synthesizer generating the carrier frequencies f_i.
4. A second modulation uses the modulated narrow band signal and the carrier frequency to generate a new spread signal with frequency of f_i to f_0 for a 0 and $f_i + f_1$ for a 1 respectively.
5. The receiver of an FHSS system has to know the hopping sequence and must stay synchronized. It then performs the inverse operations of the modulation to reconstruct user data.

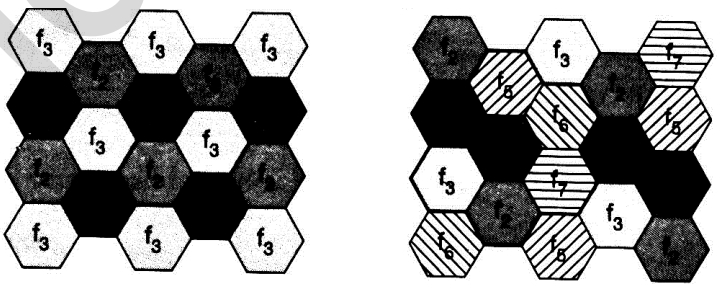
CELLULAR SYSTEMS

Cellular systems implement SDM (Space Division Multiplexing). Each transmitter, typically called a base station, covers a certain area called cell.

- **Advantages :**
  i) *Higher capacity* : SDM is implemented it allows frequency reuse.
  ii) *Less transmission power* : A receiver far away from a base station would need much more transmit power than the current few watts.
  iii) *Local interference only* : Having long distances between sender and receiver results in even more interference problems.

- **Disadvantages :**
  i) *Infrastructure needed* : Cellular systems need a complex infrastructure to connect all base stations.
  ii) *Handover needed* : The mobile station has to perform a handover when changing from one cell to another.
  iii) *Frequency planning* : To avoid interference between transmitters. Using the same frequencies, frequencies have to be distributed carefully.
  The basic goal of cellular system is never to use same frequency at the same time within the interference range.

- **Architecture of Cellular System**



Cellular system with three and seven cell clusters

– Cells are combined in clusters : on the left side three cells from a cluster, on the right side seven cells from a cluster.

- Hexagonal pattern is chose as a simple way of illustrating model
- The transmission power of a sender has to be limited to avoid interference with the next cell using same frequencies.
- To reduce interference, sectorized antennas can be used.
- Cells with more traffic are dynamically allotted more frequencies. This scheme is known as borrowing channel allocation (BCA)
- Fixed assignment of frequencies i.e. fixed channel allocation (FCA) is not always efficient
- CDM cells are commonly said to 'breathe'. The higher the noise, the higher the path loss & higher transmission errors

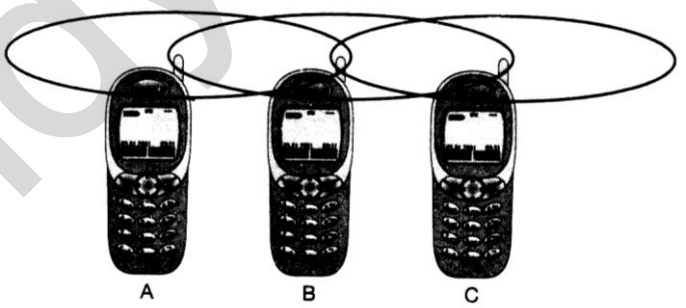
MOTIVATION FOR A SPECIALIZED MAC

- CSMA / CD does not work same in wireless transmission. It means that situation is different in wireless network since CSMA / CD cannot be successful here.
- In wireless network, the strength of a signal decrease proportionately to the square of the distance to the sender.
- Obstacles attenuate the signal further.
- The sender applies carrier sense and detect the medium. The sender starts sending but a collision happens at the receiver due to a second sender.

Here comes the problem of hidden terminals. Same happens with collision detection, like, the sender detects no collision and assumes that data has been transmitted without errors, but collision might actually have destroyed the data at receiver.

This is why specialized MAC are needed to be studied.
Some more situations due to which specialized MAC are needed.
→ Hidden and exposed terminals
→ Near and far terminals.

- **Hidden and Exposed Terminals :**



Hidden and exposed terminals

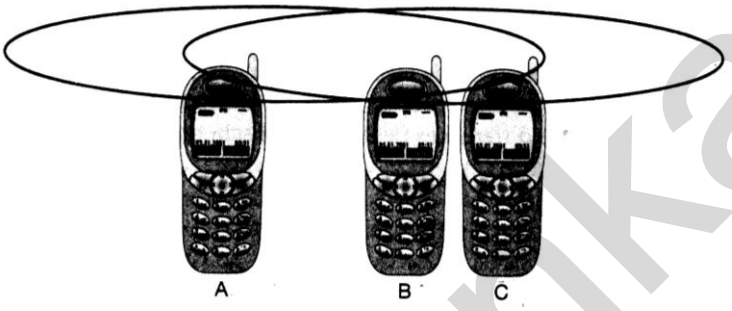
Hidden terminal
A, B, C Mobile Phones : Transmission range of A reaches B, not to C; C reaches B, but not A; B reaches A and C.

A sends to B, C does not receive, C want to send something to B and senses the medium. Medium appears to be free, the carrier sense fails. C also starts, sending causing a

collision at B. But A cannot detect this collision and continues with its transmission. In such situation "A" is hidden for C and vice versa.

Exposed terminal : B sends something to A and C wants to transmit data to other mobile phone outside the interference range of A and B. C senses carrier and detects that carrier is busy. So see postpones its transmission and detects medium till it become idle. So in this case C has to wait unnecessary. Here C is exposed to B.

- **Near and Far terminals**



Near and Far terminals

In above figure A and B are both sending data with the same transmission power. Signal strength decreases proportionally to the square of distance, B's signal drowns out A's signal. C cannot receive A's transmission.

Now, C as being an arbitrator for sending rights. In such case, terminal B would already drown out terminal A on the physical layer. C in turn can hear only B
This near / far effect is a severe problem of wireless networks using SDM.

SDMA

- Allocates separate space for users in network.
- MAC algorithm decides base stations. Considering FDM, TDM, SDM.
- SDMA algorithm basis is formed by cells and sectorized antenna. Constituting infrastructure of implementing SDMA.
- SDMA always used in combination.

FDMA

Allocates frequencies to transmission channels according to the FDM.
Sender and receiver have to agree upon hopping pattern, which are fixed at least for a longer period. To jump arbitrarily in frequency space is one of main difference between FDM schemes and TDM schemes. Two patterns typically establish a duplex channel. Two directions, mobile stations to base station and vice versa are separated using different frequencies. This scheme is called frequency division duplex (FDD). From mobile station to base station or from ground control to satellite is called uplink. From base station to mobile station or from satellite to ground control is called downlink.

TDMA

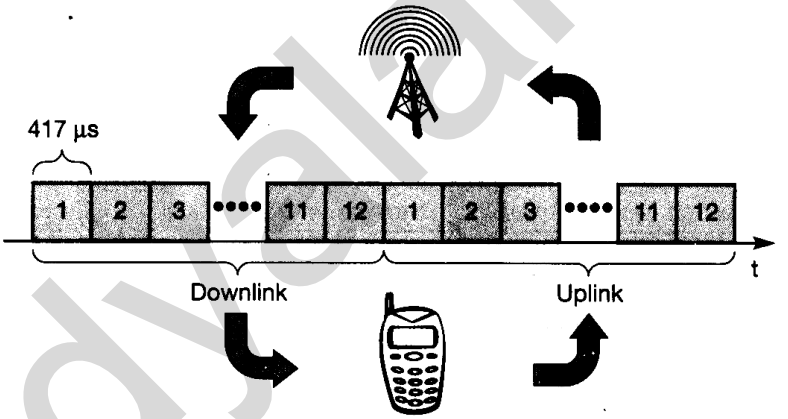
Offers much more flexible scheme. Allocates certain time slots for communication for eg. Controlling TDM. Synchronozation between sender and receiver has to be achieved in

time domain. Dynamic allocation schemes require an identification for each transmission as this is the case for typical wired MAC schemes. This enables a receiver in a broadcast medium to recognize if it really is the intended receiver of a message.

- **Fixed TDM**
  Simplest algorithm for using TDM is allocating time slots for channels in a fixed pattern. This results in a fixed bandwidth which is typical solution for wireless phone systems. Fixed access patterns fit perfectly well for connections with a fixed bandwidth. Assigning different slots for uplink and downlink using the same frequency is called time division duplex (TDD) figure.

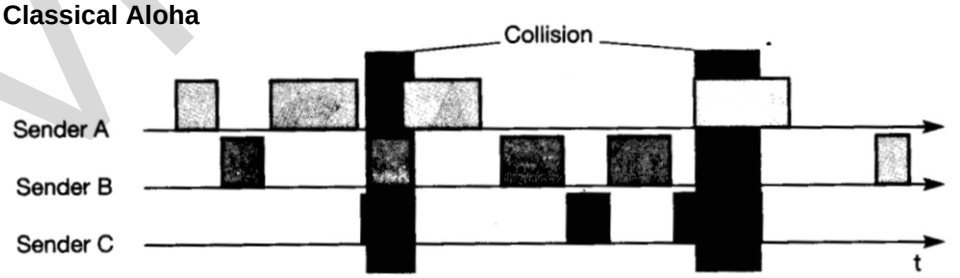
  The base station uses one out of 12 slots for downlink, whereas the mobile station uses one out of 12 different slots for the uplink. Uplink and downlink are separated by time. Upto 12 different mobile stations can use the same frequency without interference using this sceheme.

  In below figure, the standard case is shown in which DECT cordless phone system, the pattern is repeated every 10ms. i.e. each slot has a duration of 417μs. This repetition guarantees access to the medium every 10 ms, independent of any other connections.



Time division multiplexing for multiple access and duplex

- **Classical Aloha**



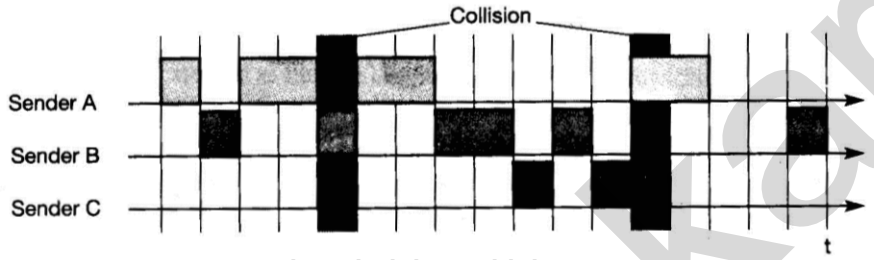
Classical Aloha multiple access

Aloha neither co-ordinates medium access nor does it resolve contention on the MAC layer as shown in figure. This is a random access scheme, without a central arbiter

controlling access, without coordination among the stations. If 2 or more stations access the medium at same time a collision occurs and transmitted data is destroyed. This problem is left to higher layers.

As classical assumption that data packet arrival follows a poisson distribution, maximum throughput is achieved for an 18% load.

- **Slotted Aloha**



Slotted Aloha multiple access

Slotted Aloha is the first refinement of classical aloha scheme. That was, done by introducing time synchronized, transmission can only start at the beginning of timeslot as shown in figure.
The throughput raises from 18% to 36% (slotting dubles throughput).

- **Carrier sense multiple access (CSMA)**

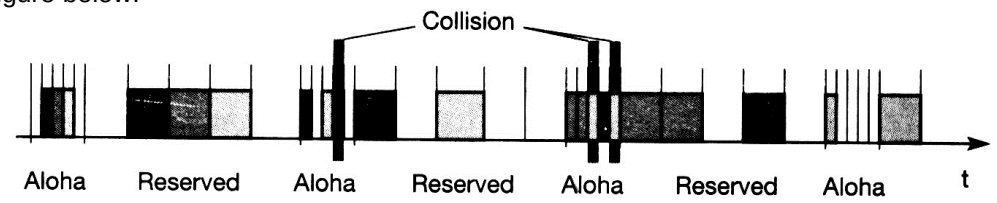
This is sensing the carrier before accessing the medium.
Some versions of CSMA :

1. Non–persistant CSMA : Stations sense the carrier and start sending immediately if the medium is idle
2. P– persistent CSMA : System nodes also sense the medium but only transmit with a probability of p, with the station deferring to the next shot with the probability 1p.
3. In 1– persistent CSMA system all stations wishing to transmit access the medium at the same time as soon as it becomes idle.

CSMA with collision avoidance (CSMA/CA) is one of the access. Schemes used in wireless LANs follows the standard IEEE 802.11
EYNMPA (Elimination yield, non preemptive multiple access) used in HIPERLAN1 specification.

- **Demand assigned multiple access (DAMA)**

DAMA is called reservation Aloha, scheme typical for satellite systems as shown in figure below.

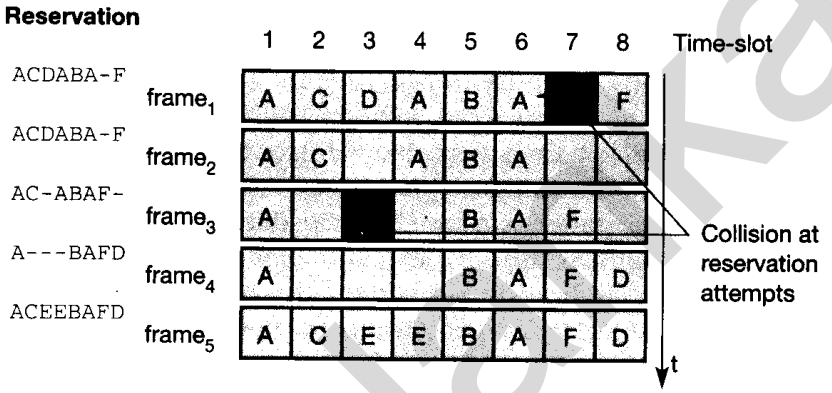


Demand assignment multiple access with explicit reservation

Different stations on earth try to reserve access time for satellite transmission. Collisions during the reservation phase do not destroy data transmission – but only the short requests. For data transmission. If successful , a time slot in the future is reserved and no other station is allowed to transmit during this slot. Therefore, the satellite collects all successful requests and sends back a reservation list indicating access right for future slots. DAMA is an explicit reservation scheme where each transmission slot has to be reserved explicitly.

- **PRMA packet reservation multiple access**

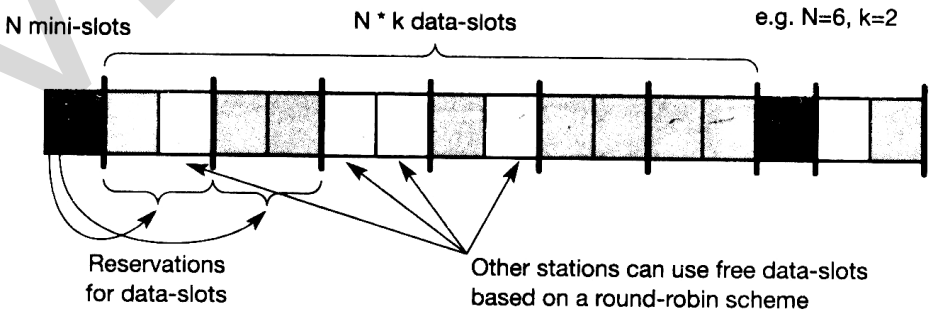
PRMA is an example of implicit reservation scheme. A certain number of slots form a frame. This frame is repeated in time.



Demand assignment multiple access with implicit reservation

In above example, the base station broadcasts the reservation status 'ACDABA –F' to all stations, from A to F, slots one to six and eight are occupied, but slot seven is free in following transmission. One station wants to access this slot. So collision occurs. The base station returns the reservation status 'ACDABA–F', indicating that reservation of slot seven failed. For this slot again compelling is started, plus station D has stopped sending in slot three and station F in slot eight. This is observed by base station after the second frame. Now in third frame, slot three and eight are indicated idle by base station.

PRMA constitutes another combination of fixed and random. TDM schemes with reservation compared to previous scheme.



Reservation TDMA access scheme

RESERVATION TDMA. ACCESS SCHEME

Reservation TDM

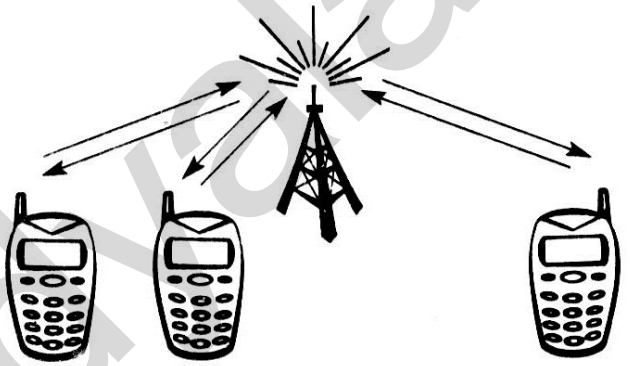
In fixed TDM scheme N mini–slots followed by N. K data slots form a frame that is repeated. Each station is allocated its own mini–slot and can use it to reserve upto K data slots. This ensures each station a certain bandwidth and fixed delay.

- **Multiple access with collision avoidance (MACA) :** With MACA, A does not start its transmission at once but sends a request to send. MACA solves the problem of hidden terminal.

- **Polling :** Polling is a centralized scheme with one master and several slave stations. The master can poll the slaves according to many schemes round robin, randomly. A master can establish list of connections wishing to transmit.

- **Inhibit sense multiple–access :** This is used for packet data transmission service. (CDPD) in AMPS mobile phones. It is also referred as digital sense multiple access. Base station signals busy medium via a busy tone according to which next transmission is followed.

- **Spread Aloha multiple access :** Combining the spreading of CDMA and the medium access of Aloha is called as spread Aloha multiple access. SAMA is also combination of CDMA and TDMA.

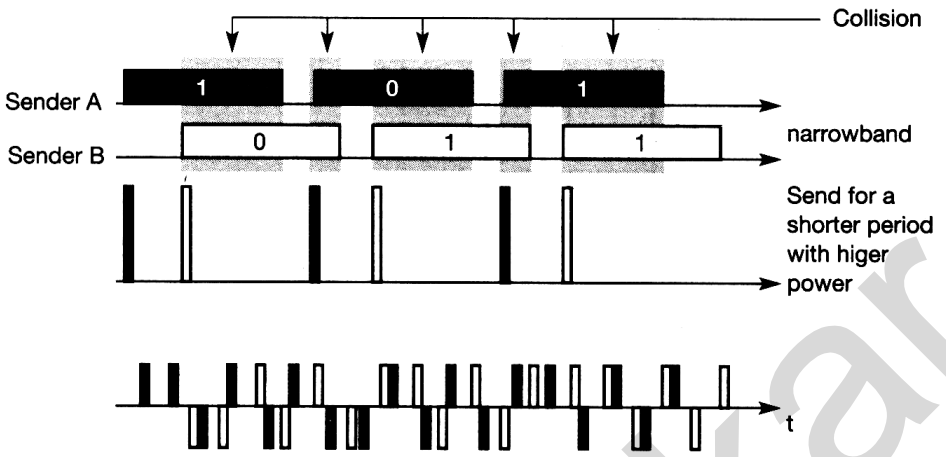


Inhibit sense multiple access using a busy tone

Working of SAMA

Each sender uses the same spreading code. The standard case for Aloha access is shown in the upper part of figure. Sender A and sender B access the medium at the same time in their narrowband spectrum, so that all three bits shown in figure cause a collision.

Separation on the two signals is still possible if one receiver is synchronized to sender A and another one to sender B.



Spread Aloha multiple access

The probability of a "Collision" is quite low if the number of simultaneous transmitter stays below 0.1 – 0.25. Main problem is using this approach is finding good chipping sequence. The code is not orthogonal to itself. It should have good co-relation at same time.

But this approach benefits from advantages of spread spectrum techniques. Like robustness against narrowband interference and simple co-existence with other systems in the same frequency band.

❑ ❑ ❑ ❑ ❑

PCS Architecture

PCS technologies have grown rapidly in the telecommunications industry. Two of the most popular are:

- Cellular telephony
- Cordless and low-tier PCS telephony

These technologies have similar architectures as shown in figure 1. This basic architecture consists of two parts:

Radio Network

PCS users carry 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. Throughout this book, we will use these terms interchangeably, depending on the context. For example, the term subscriber unit is used when we describe wireless local loop; the term portable is used when we describe the low-tier systems such as PACS; and the term mobile station is used when we describe the GSM system.

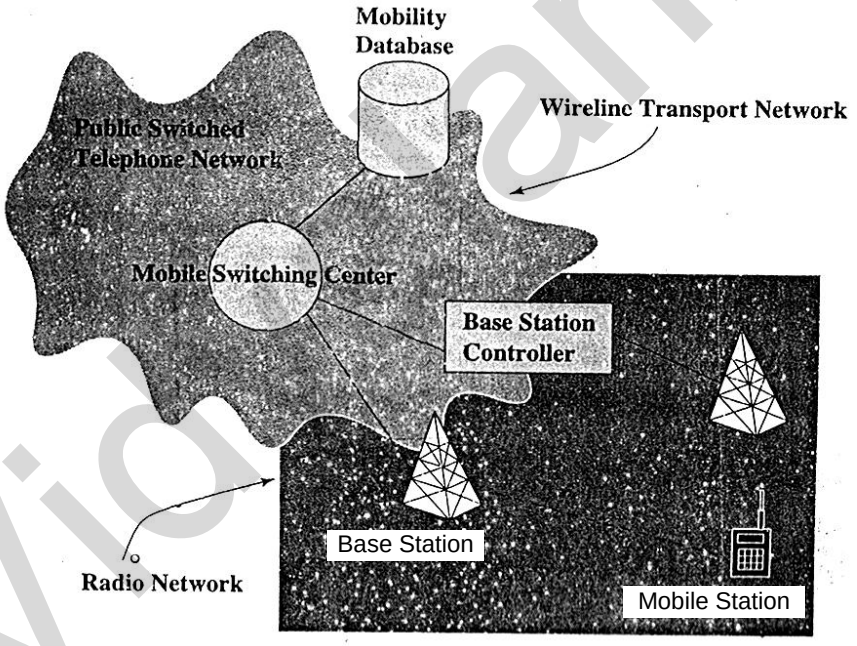


Fig. 1 : The basic PCS network architecture

Modern MS technology allows the air interface to be updated (eg., from DECT to GSM) over the air remotely. The MS can also be remotely monitored by the system maintenance and diagnostic capabilities. Different types of MSs have various power ranges and radio coverages. For example, hand-held MSs have a lower output power (where the maximum output power can be as low as 0.8 watts for GSM 900) and shorter range compared with vehicle-installed MSs with roof-mounted antennas (where the maximum output power can be as high as 8 watts in GSM900).

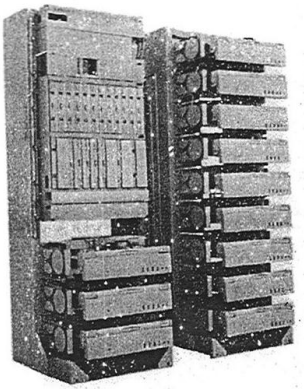


Fig. 2: CDMA base transceiver station (by courtesy of Nortel)

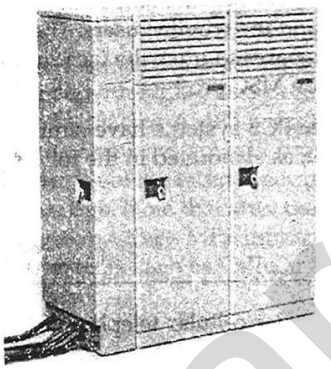


Fig. 3: CDMA base station controller (by courtesy of Nortel)

The radio coverage of a base station, or a sector in the base station, is called a cell. For systems such as GSM, cdmaOne, and PACS, the base station system is partitioned into a controller (base station controller in GSM and radio port control unit in PACS) and radio transrnitters/receivers (base transceiver stations in GSM and radio ports in PACS). The base stations usually reach the wireline transport network (core or backbone network) via land links or dedicated microwave links. Figures 2 and 3 show base transceiver station and base station controller products.

Wireline Transport Network

The mobile switching center (MSC) connected to the base station is a special switch tailored to mobile applications. For example, the Lucent 5ESS MSC 2000 is an MSC modified from Lucent Technologie' 5ESS switching system. The Siemens' D900/1800/1900 GSM switch platform is based on its EWSD (Digital Electronic Switching System) platform. The Ericsson MSC is based on its AXE switching platform. The MSC is connected to the PSTN to provide services between the PCS users and the wireline users. The MSC also communicates with mobility databases to track the locations of mobile stations. Figure 4 illustrates an MSC product.

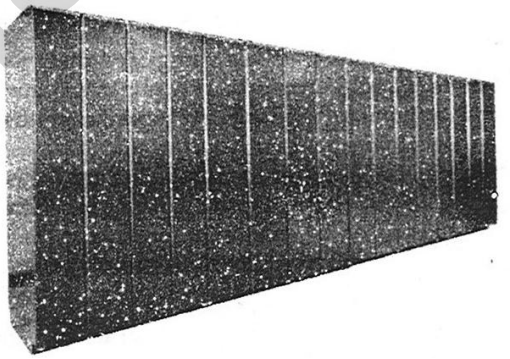


Fig. 4 : Mobile switching center (CDMA MTX MSC by courtesy of Nortel)

Although cellular and cordless/low-tier PCS systems have similar are architectures their design guidelines differ, as elaborated in the following two sections.

CELLULAR TELEPHONY

This section gives an overview of four popular cellular telephony networks: AMPS, GSM, DAMPS (IS-136), and CDMA (IS-95).

Advanced Mobile Phone Service (AMPS)

AMPS was the first cellular system. Developed during the 1970s in the Bell Laboratories, this first-generation analog cellular system has been considered a revolutionary accomplishment. The AMPS specification was generated from a laborious process of research, system design, and switching design over a period of 10 years. From 1974 to 1978, a large-scale AMPS trial was conducted in Chicago. Commercial AMPS service has been available since 1983. Based on frequency division multiple access (FDMA) technology for radio communications, AMPS was designed as a high-capacity system based on a frequency reuse scheme. Voice channels are assigned to radio frequencies using FDMA. A total of 50 MHz in the 824-849 MHz and 869-894 MHz bands is allocated for AMPS. This spectrum is divided into 832 full-duplex channels using 1664 discrete frequencies, that is, 832 downlinks and 832 uplinks. Downlinks are the transmission paths from base stations to handsets, and uplinks are the transmission paths from handsets to the base stations.

In the frequency reuse scheme, cells are grouped into clusters. Cells within a cluster may interfere with each other, and thus must use different frequencies. Frequencies may be reused by cells in different clusters. In AMPS, the typical frequency reuse plan employs either a 12-group frequency cluster using omnidirectional antennas or a 7-group cluster using three sectors per base station. Thus, there are about 50 channels per cell. Motorola uses a 4-cell; 6-sector design, in its AMPS system. AMPS follows the EIA/TIA IS-41 standard for roaming management.

Compared with the digital alternatives in the United States, AMPS service offers more complete geographical coverage at a cheaper service charge partly due to the low cost of mass production of handsets. However, digital networks are replacing AMPS because the digital technology can cope with higher user densities, and offer lower costs. In 2000, Taiwan started replacing AMPS with the IS-95 CDMA system. After the replacement, the new system will provide the same service at less than half the bandwidth of the radio spectrum; the extra bandwidth will be released for other usage. Note that after the AMPS voice service is replaced by the digital systems, the AMPS infrastructure can be utilized to support mobile data systems such as Cellular Digital Packet Data (CDPD).

Global System for Mobile Communications (GSM)

GSM is a digital cellular system developed by Groupe Special Mobile of Conference Europeenne des Posies et Telecommunications (CEPT) and its successor European Telecommunications Standard Institute (ETSI). An important goal of the GSM development process was to offer compatibility of cellular services among European countries. GSM is a revolutionary technology that combines both time division multiple access (TDMA) and FDMA. With TDMA, the radio hardware in the base station can be shared among multiple users. In GSM, a frequency carrier is divided into eight time slots where the speech coding rate is 13 Kbps. In a GSM base station, every pair of radio transceiver-receiver supports eight voice channels, whereas an AMPS base station needs one such pair for every voice channel. The GSM MSs control their RF output power to maintain interference at low levels. The GSM air interface has been evolved into Enhanced Data Rate for GSM Evolution (EDGE) with variable data rate and link adaptation. EDGE utilizes highly spectrum-efficient modulation for bit rates higher than existing GSM technology. EDGE requires upgrade of existing base transceiver station, which supports high-speed data transmission in smaller cells and at short ranges within cells. EDGE does not support ubiquitous coverage; that is, it supports island coverage in indoor, pico, and micro cells.

EIA/TIA IS-136 Digital Cellular System

Also referred to as digital AMPS (DAMPS), American Digital Cellular (ADC), or North American TDMA (NA-TDMA), IS-136, the successor to IS-54, supports a TDMA air interface similar to that of GSM, and is thus considered an evolutionary technology. It took four months to create the IS-54 specification, and no significant trial was conducted. IS-54 was renamed IS-136 when it reached revision C.

Using TDMA, every IS-136 frequency carrier supports three voice channels, where the speech coding rate is 7.95 Kbps. IS-136 systems operate in the same spectrum with the same frequency spacing (30 KHz) used by the existing AMPS systems. Thus, the IS-136 capacity is around three times that of AMPS. An existing AMPS system can be easily upgraded to IS-136 on a circuit-by-circuit basis. In this way, the evolution from AMPS to DAMPS can be made gracefully. IS-136 is also defined for the new PCS spectrum allocation at 1850 to 1990 MHz. Like GSM, features of IS-136 include point-to-point short messaging, broadcast messaging, group addressing, private user groups, hierarchical cell structures, and slotted paging channels to support a “sleep mode” in the handset, to conserve battery power. Like AMPS, IS-136 uses the IS-41 standard for mobility management.

EIA/TIA IS-95 Digital Cellular System

This digital cellular system was developed by Qualcomm, and has been operating in the United States since 1996. IS-95 is based on code division multiple access (CDMA) technology. CDMA allows many users to share a common frequency/time channel for transmission; the user signals are distinguished by spreading them with different codes. In theory, this technology optimizes the utilization of the frequency bandwidth by equalizing signal-to-noise ratio (SNR) among all the users, thereby more equitably sharing the system power resources among them. While AMPS users who are near base stations typically enjoy SNRs in excess of 80 dB, users at the edge of cell coverage areas experience SNRs near the lower limit. With CDMA, users who are near base stations transmit less power, maintaining the same SNR as users at the edge of a cell’s coverage.

By utilizing the minimum necessary amount of power, systemwide co-channel interference is kept at a minimum.
IS-95 MSs may need to maintain links with two or more base station continuously during phone calls, so that, as multipath varies, the base station with the best received signal on a burst-by-burst basis will be selected to communicate with the MS. More details on CDMA technology are given.

The channel bandwidth used by IS-95 is 1.25 MHz. This bandwidth is relatively narrow for a CDMA system, which makes the service migration from analog to digital within an existing network more difficult than at AMPS and D AMPS. In the third-generation wideband CDMA proposal, the bandwidth has been extended to 5 MHz. The speech coding rate for IS-95 is l3 Kbps or 8 Kbps. IS-95’s capacity is estimated to be 10 times that of AMPS.

Like AMPS, IS-95 uses the IS-41 standard for mobility management. One of the third-generation mobile system standards, cdma2000, is evolved from the narrowband IS-95.

CORDLESS TELEPHONY AND LOW-TIER PCS

This section introduces two cordless telephony technologies, CT2 and DECT, and two low-tier PCS technologies PHS and PACS.

Cordless Telephone, Second Generation (CT2)

CT2 was developed in Europe, and has been available since 1989. The first CT2 products conformed to the final version of the CT2 specifications, CAI (Common Air Interface). CT2 is allocated 40 FDMA channels with a 32-Kbps speech coding rate. For a user, both base-to-handset signals and handset-to-base signals are transmitted in the same frequency. This duplexing mode is referred to as time division duplexing (TDD).

The maximum transmit power of a CT2 handset is 10 mW. In the call setup procedure, CT2 moves a call path from one radio channel to another after three seconds of handshake failure. CT2 also supports data transmission rates of up to 2.4 Kbps through the speech codec and up to 4.8 Kbps with an increased error rate. CT2 does not support handoff.

Digital European Cordless Telephone (DECT)

DECT specifications were published in 1992 for definitive adoption as the European cordless standard. The name Digital European Cordless Telephone has been replaced by Digital Enhanced Cordless Telephone to denote global acceptance of DECT. DECT supports high user density with a picocell design. Using TDMA, there are 12 voice channels per frequency carrier. Sleep mode is employed in DECT to conserve the power of handsets. DECT may move a conversation from one time slot to another to avoid interference. This procedure is called time slot transfer. DECT also supports seamless handoff.

Like CT2, DECT uses TDD. Its voice codec uses a 32 Kbps speech coding rate. DECT channel allocation is performed by measuring the field strength; the channel with quality above a prescribed level is autonomously selected. This strategy is referred to as dynamic channel allocation. DECT is typically implemented as a wireless-PBX (private branch exchange) connected to the PSTN. An important feature of DECT is that it can interwork with GSM to allow user-mobility, where the GSM handsets provide DECT connection capabilities.

Personal Handy Phone System (PHS)

PHS is a standard developed by the Research and Development Center for Radio Systems (RCR), a private standardization organization in Japan. PHS is a low-tier digital PCS system that offers telecommunications services for homes, offices, and outdoor environments, using radio access to the public telephone network or other digital networks. PHS uses TDMA, whereby each frequency carrier supports four multiplexed channels. Sleep mode enables PHS to support five hours of talk-time, or 150 hours of standby-time. PHS operates in the 1895-1918. 1 MHz band. This bandwidth is partitioned into 77 channels, each with 300 KHz bandwidth. The band 1906.1-1918.1 MHz (40 channels) is designated for public systems, and the band 1895-1906.1 MHz (37 channels) is used for home/office applications.

Like DECT, PHS supports dynamic channel allocation. PHS utilizes dedicated control channels, that is, a fixed frequency that carries system and signaling information is

initially selected. The PHS speech coding rate is 32 Kbps. Like CT2 and DECT, the duplexing mode used by PHS is TDD. Handoff can be included in PHS as an option. PHS supports Group 3 (G3) fax at 4.2 to 7.8 Kbps and a full-duplex modem with transmission speeds up to 9.6 Kbps.

Personal Access Communications System

PACS is a low-power PCS system developed at Telcordia (formerly Bellcore). PACS is designed for wireless local loop and for personal communications services. TDMA is used in PACS with eight voice channels per frequency carrier. The speech coding rate is 32 Kbps. Both TDD and frequency division dublexing (FDD) are accommodated by the PACS standard. In FDD mode, the PACS uplink and downlink utilize different RF carriers, similar to cellular systems. The highly effective and reliable mobile-controlled handoff (MCHO) completes in less than 20 msec.

Unlicensed Systems

In addition to these standardized cordless radio technologies, unlicensed communications devices for cordless telephony may make use of the industrial, scientific, and medical (ISM) spectrum. A number of commercially available products (wireless PBXs, wireless LANs, cordless telephones) make use of the ISM spectrum to avoid the delays associated with spectrum allocation, licensing, and standardization.

The applicability of the AMPS analog cellular air interface for cordless telephones and office business phones (using the 800 MHz cellular spectrum) has been tested by several cellular service providers. From a customer's perspective, these trials have been an overwhelrning success, indicating desire for interoperability between private and public wireless access. From a service provider perspective, the service is difficult to operate and maintain because of hard-to-control interference from the private systems into the public system. The TIA interim standard IS-94 describes the air interface requirements for this application of AMPS. It also describes the protocol and interface between the cordless base station and the network, to control the base station emissions as necessary to limit interference to the public system, and to register and deregister the location of the handsets to and from the private cordless base station at the service provider's mobility databases for the purpose of routing calls. Authentication of the handset is included in this protocol. The networking protocol described by IS-94A is extensible to digital cellular systems, and it affects interoperability between any public systems using licensed spectrum and any private systems using the unlicensed spectrum.

Third-Generation Wireless Systems

Mobile telecommunication systems have been evolving for three generations. For the mobile systems introduced in Cellular telephony, AMPS is the first-generation system; GSM, IS-136, IS-95, and the lower-tier systems described in Cordless Telephony and Low-Tier PCS are second-generation technologies. These systems have been designed primarily for speech with low-bit-rate data services. They are limited by their vertical architectures. Most system aspects have been specified from services to the bearer services. Consequently, any enhancements or new services affect the network from end to end.

Compared with second-generation systems, third-generation systems offer better system capacity; high-speed, wireless Internet access (up to 2 Mbps), and wireless multimedia

services, which include video, images, and data. Several technologies, such as General Packet Radio Service (GPRS) and EDGE, bridge second-generation systems into third-generation systems. In third-generation systems, new network technologies such as ATM (Asynchronous Transfer Mode) backbone, network management, and service creation are integrated into the existing second-generation core networks. Air interfaces such as Wideband CDMA (W-CDMA) and cdma2000 are major third-generation radio standards.

The increasing number of Internet and multimedia applications is a major factor driving the third-generation wideband wireless technology. Some studies indicate that more than 20 percent of the adult population in the United States are interested in wireless Internet access. By the end of 1999, wireless data services were marketed as modem access for laptop. As the advanced third-generation infrastructure becomes available, and the inexpensive wireless handheld devices (e.g., wireless personal data assistant and wireless smart phones) become popular, subscribers will begin to enjoy instant wireless Internet access. The services include sales force automation, dispatch, instant content access, banking, e-commerce, and so on.

Handoff

Three strategies have been proposed to detect the need for handoff:

- In mobile-controlled handoff (MCHO), the MS continuously monitors the signals of the surrounding BSs and initiates the handoff process when some handoff criteria are met MCHO is used in DECT and PACS.
- In network-controlled handoff (NCHO), the surrounding BSs measure the signal from the MS, and the network initiates the handoff process when some handoff criteria are-met. NCHO is used in CT-2 Plus and AMPS.
- In mobile-assisted handoff (MAHO), the network asks the MS to measure the signal from the surrounding BSs. The network makes the handoff decision based on reports from the MS. MAHO is used in GSM and IS-95 CDMA.

The BSs involved in the handoff may be connected to the same MSC (inter-cell handoff or inter-BS handoff) or two different MSCs (inter-system handoff or inter-MSC handoff.

Inter-BS Handoff

In inter-BS handoff, the new and the old BSs are connected to the same MSC. Assume that the need for handoff is detected by the MS; the following actions are taken:

i) 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 (see Figure 5(a))

ii) 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 (see Figure 5(b)).

iii) After the MS has been transferred to the new BS, it signals the network (see Figure 5(c)), and resumes conversation using the new channel.

iv) Upon receipt of the handoff completion signal, the network removes the bridge from the path and releases resources associated with the old channel. (see Figure 5(d)).

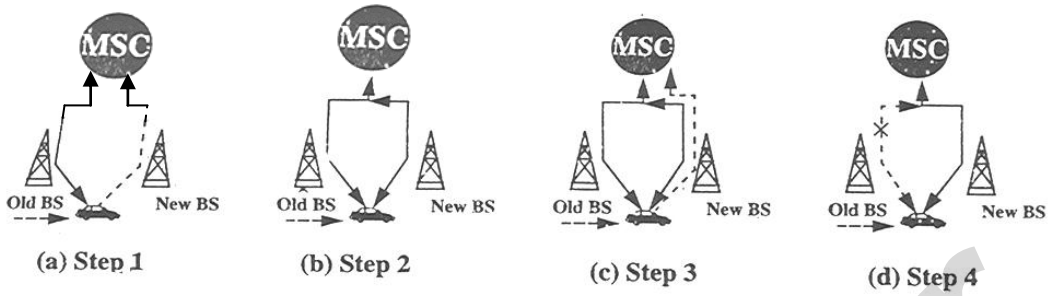


Fig. 5 : Inter-BS link transfer

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 thea 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 unit the call is completed or when the failing link is no longer available. This is referred to as the nonprioritiezed scheme. To reduce forced termination and to promote call competion, three channel assignement schemes have been proposed:

Reserved channel scheme
Similar to the nonprioritized scheme, except that some channels in each BS are reserved for handoff calls.

Queueing priority scheme
Based on the fact that adjacent coverage areas of BSs overlap. Thus, there is a considerable area where a call can be handled by either BS. This area is called the handoff area. If no channel is available in the new BS during handoff, the new BS buffers the handoff request in a waiting queue. The MS continues to use the channel with the old BS until either a channel in the new BS becomes available (and the handoff call is connected) or the MS moves out of the handoff area (and the call is forced to terminate).

Subrating scheme
Creates a new channel for a handoff call by sharing resources with an existing call if no channel is available in the new BS. Subrating means an occupied full-rate channel is temporarily divided into two channels at half the original rate: one to serve the existing call and the other to serve the handoff request. When occupied channels are released, the subrated channels are immediately switched back to full-rate channels.

Studies have indicated that under certain conditions, these handoff schemes can significantly reduce the probability of forced termination as well as the probability of call incompletion (new call blocking plus handoff call forced termination).

Intersystem Handoff

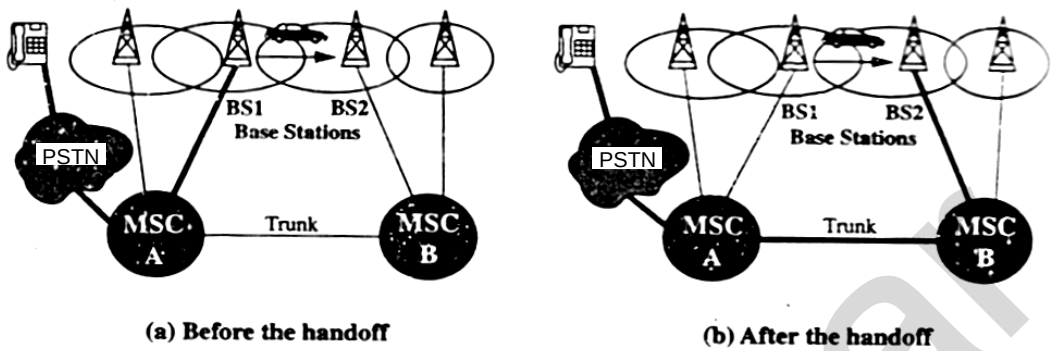


Fig. 6 : Intersystem handoff

In intersystem handoff, the new and old BSs are connected to two different MSCs. In the description that follows, we trace the intersystem. handoff procedure of IS-41, where network-controlled handoff is assumed. Figure 6 illustrates the trunk connection before and after the intersystem handoff. In this figure, a communicating mobile user moves out of the BS served by MSC A and enters the area covered by MSC B. Intersystem handoff requires the following steps:

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

ii) MSC A checks if the MS has made too many handoffs recently (this is to avoid, for example, numerous handoffs between BS1 and BS2 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.

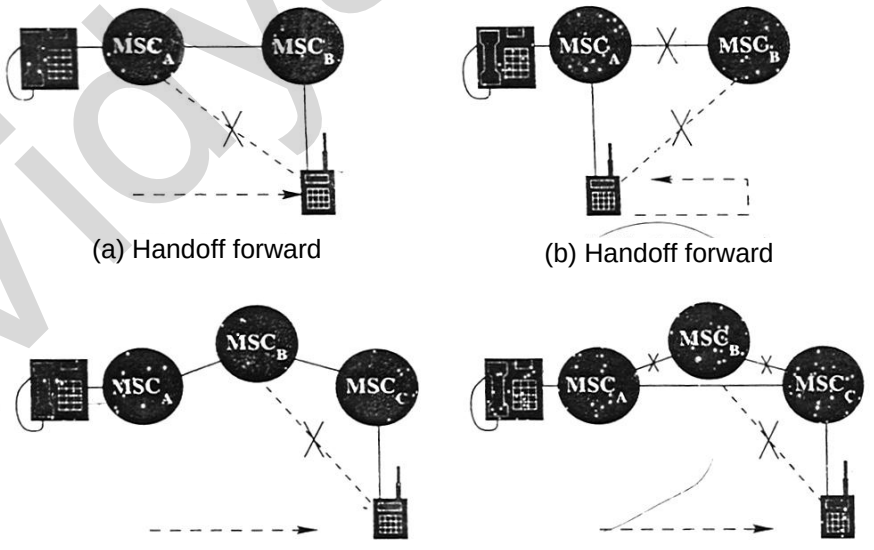
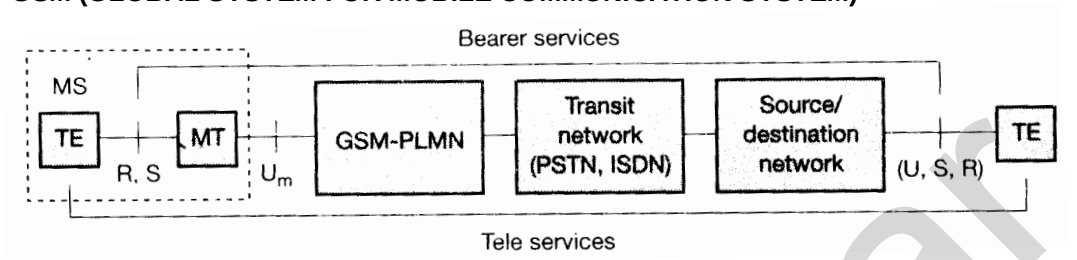


Fig. 7: Handoff forward, handoff backward, and handoff to the third

GSM (GLOBAL SYSTEM FOR MOBILE COMMUNICATION SYSTEM)



Bearer and teleservices reference model

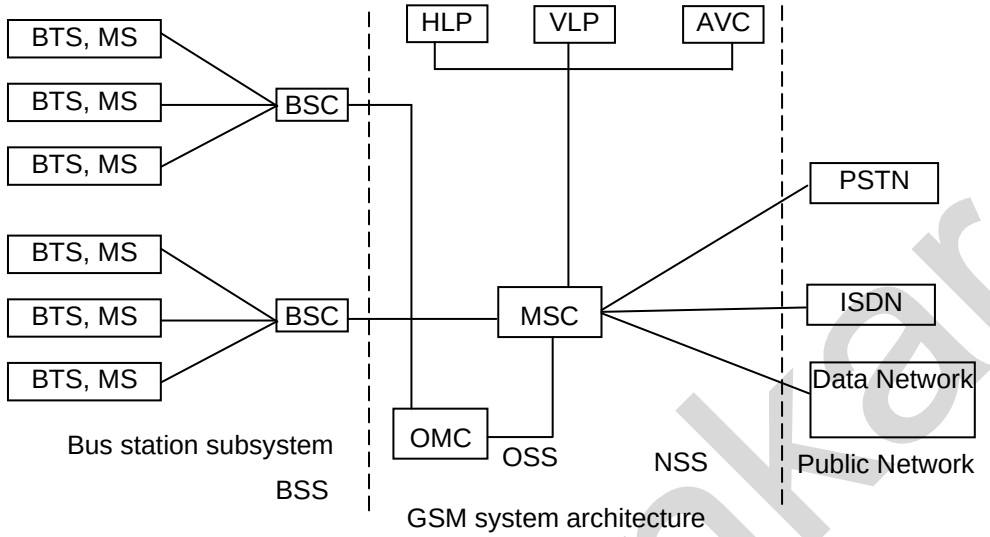
A mobile station MS is connected to the GSM public land mobile network (PLMN) via the U_m interface. This network is connected to transit networks, e.g. Integrated service digital network (ISDN) or transitional public switched telephone network (PSTN). There might be an additional network, the source / destination network before another terminal TE is connected. Within the mobile station MS, the mobile termination (MT) performs all network specific tasks (TDMA, FDMA, etc) and offers an interface for data transmission(s) to terminal TE which can then be network independent.

- **Bearer Services (non voice service) :** Bearer Services permit transparent and non-transparent, synchronous and asynchronous data transmission. Transparent bearer services only use the functions of physical layer (layer 1) to transmit data forward error correction mechanism is to correct transmission errors. Non transparent bearer services use protocols of layer 2 and 3, additional radio link protocol (RLP). RLP comprises HDLC.

- **Teleservices :** GSM Mainly focuses on voice – oriented teleservices, as main service is telephony. It offers bandwidth of 3.1KHz of analog phone system SMS (short message service) is useful service proving SMS length of 160 characters. EMS (enhanced mobile service) offers large message of 760 characters, animated pictures, ring tones etc. MMS (Multimedia message service) offer transmission of large pictures GIF, BMP, Video clips can comes with mobile phones that integrate small cameras. Non voice teleservice is group fax.

- **Supplementary Services :** GSM offer supplementary services like identification, call redirection, or forwarding of ongoing calls. Closer user groups and multi–party communications can be available in standard ISDN.

SYSTEM ARCHITECTURE



GSM system consist of 3 subsystem.

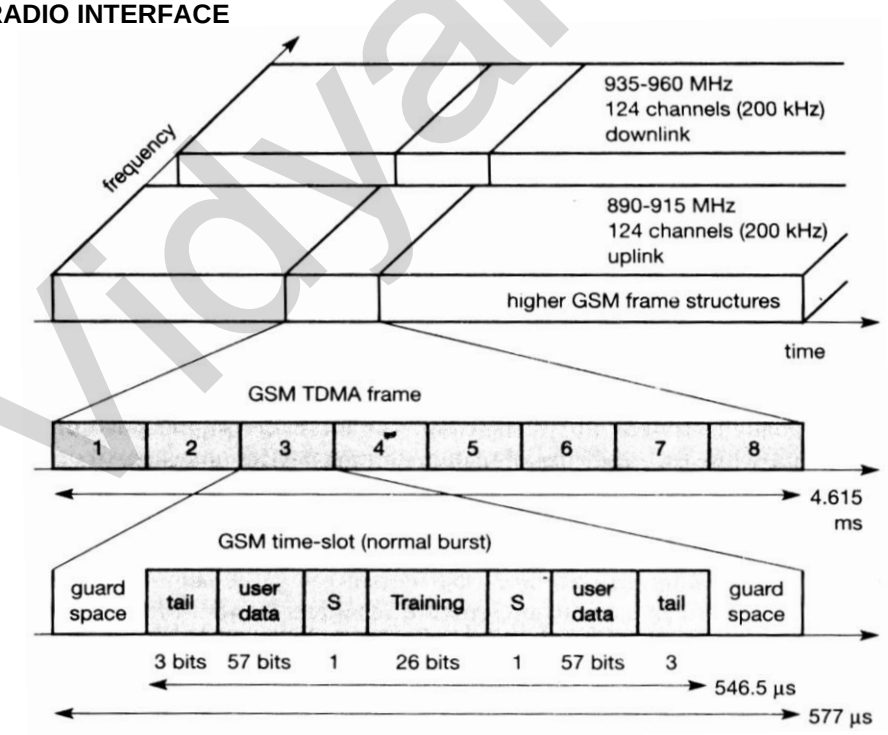
1. Radio sub system (RSS)
2. The network and switching subsystem (NSS)
3. Operation subsystem (OSS)

- **Radio Subsystem (RSS)**
  RSS consist of MS(mobile stations) & BSS (base station subsystem) RSS and NSS is connected via A interface and NSS and OSS via O interface.
- **Base station subsystem (BSS)**
  Each BSS is controlled by base station controller (BSC).
  Performs necessary function to maintain radio connections to MS(coding / decoding of voice)
- **Base transceiver station (BTS)**
  BTS can form a radio cell or sectorized antennas, several cells
  Connected to MS via U_m (ISDN) interface for mobile use and to BSC via Abis interface.
- **Base station controller (BSC)**
  Manages BTSs
- **Mobile Stations (MS)**
  Consists of user independent h/w, s/w and SIM (subscriber identity module) can be identified by international mobile equipment identity (IMEI). SIM can be personalized.
  SIM contains many identifiers, services as personal identity number (PIN), PIN unblocking key (PUK), authentication key K_1, international mobile subscriber identity (IMSI).
  MS stores dynamic information when logged onto GSM system like cipher key, temporary mobile subscriber identity (TMSI), & location area identification (LAI).
- **Network and Switching subsystem**
  NSS forms the heart of GSM system.
- **Mobile services switching center (MSC)**
  → High performance digital ISDN switches.
  → Gateway MSC (GMSC) has additional connections to other fixed network as PSTN and ISDN. Using IWF MSC can connect to public data network (PDN).

- **Home Location Register (HLR)**
  - → Most important database in GSM, stores user relevant information.
  - → All user specific information only exists once for each user in single HLR.
  - → IMSI, LA, MSRN, (mobile subscriber roaming number) etc. stored.
- **Visitor Location register (VLR)**
  - → Related to each MSC, stores dynamic database needed for MS users.
  - → If new MS comes into an LA the VLR is responsible for, and it copies all relevant information for this user from HLR.
  - → Hierarchy of VLR & HLR avoid frequent HLR updates and long distance signaling of user information.

- **Operation Subsystem (OSS)**
  - → Contains network entities as follows :
  - **Operation and Maintenance Center (OMC)**
    - Uses concepts of telecommunication management network (TMN) given by ITU–T and performs functions like traffic monitoring, status report of network entities etc.
  - **Authentication Centre (AVC)**
    - Defined to protect user identity and data transmission
    - Contains algorithms, keys for encryption needed in HLR.
  - **Equipment Identity Register (EIR)**
    - Stores all device identification .
    - Also contain valid IMEIs.

RADIO INTERFACE



GSM TDMA frame, slots and bursts

→ GSM implements SDMA using cells with BTS and assigns an MS to BTS.
→ Media combines FDMA and TDMA. In GSM 900, 124 channels each 200KHz wide are used for FDMA, but GSM uses 374 channels.
→ Each 248 channel is additionally separated in time via a GSM TDMA frame. The frame duration is 4.615ms, this frame is subdivided into 8GSM time slots.
→ Data is transmitted is small portion called bursts. Normal burst used for data transmission inside lime slots.
→ The first and last three bits of a normal burst (tail) are set to 0, to enhance receive performance.
→ Training sequence is used to adapt receiver's parameter.
→ Flag 'S' indicates whether data field contains user on network control data.
→ A more burst for data transmission are :
1) Frequency correction : allows MS to correct local oscillator to avoid interference with neighbour channel.
2) Synchronization burst : synchronizes the MS with BTS in time.
3) Access burst : for initial connection set up between MS and BTS.
4) Dummy burst : used if no data available for slot.

→ To avoid frequency selective fading, GSM specifies an optional slow frequency hopping mechanism.

Logical channels and frame hierarchy

GSM specifies two basic groups of logical channels, i.e. traffic channels and control channels.

Logical channels C_1 that only takes up every fourth slot and another logical channel C_2 that uses every other slot.

Traffic Channels (TCH)

Used by GSM to transmit user data

2 Categories (i) full rate TCH (TCH / F) → data rate 22.8kbits
(ii) half rate TCH (TCH / H) → data rate 11.4kbit/s.

(TCH / FS) used for error correction

Standard codes for voices. → Full rate FR, 13 bit/s
→ half rate HR, 5.6kbit/s.
→ Enhanced full rate EFR provides better quality than FR.

Tandem free operations, (TFO) provide increase in voice quality.

Control Channel (CCH)

→ To control medium access, allocation of traffic channels and mobility management.

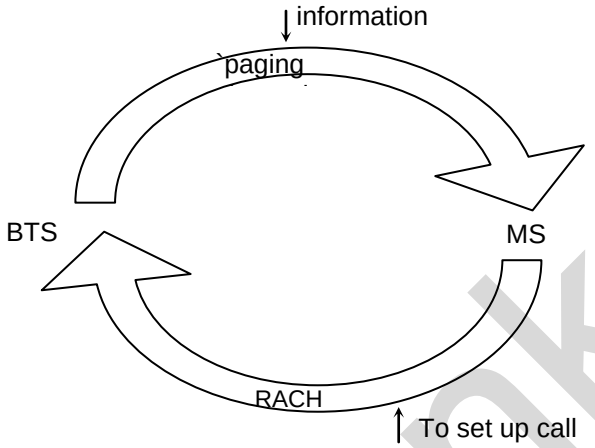
i) Broadcast control channel (BCCH) :

Subchannels i) Frequency correction channel (FCCH).
ii) Synchronization channel (SCH).

Used by BTS to send information about frequency and synchronization respectively to MS

ii) Common control channel (CCCH) :

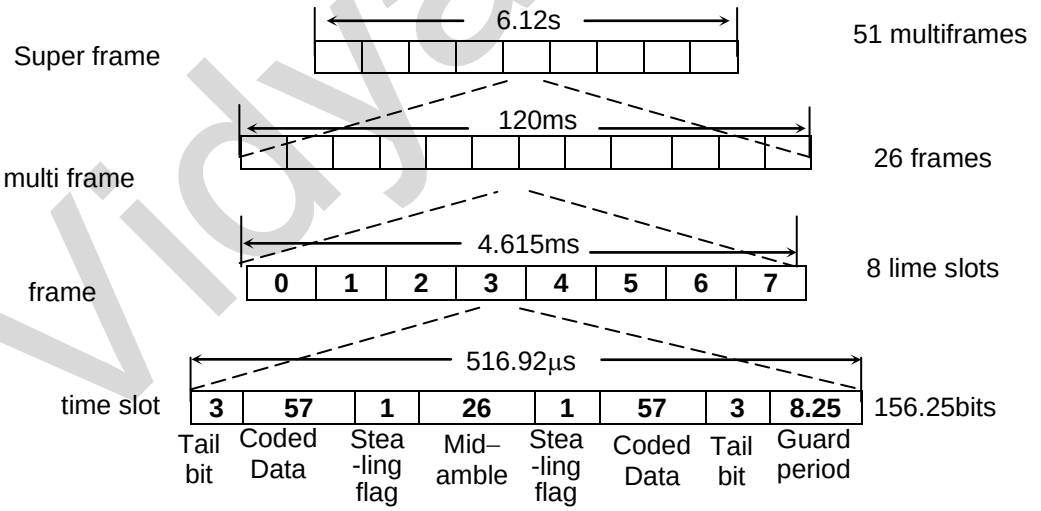
Subchannel i) PCH (Paging Channel)
ii) RACH (random access channel)
iii) AGCH (access grant channel) for signaling purpose to MS)



iii) Dedicated control channel (DCCH)

Sub channel → (SDCCH) Standalone dedicated control channel.
→ (SACCH) Slow associated dedicated control channel
→ (FACCH) fast associated dedicated control channel

GSM Frame Structure

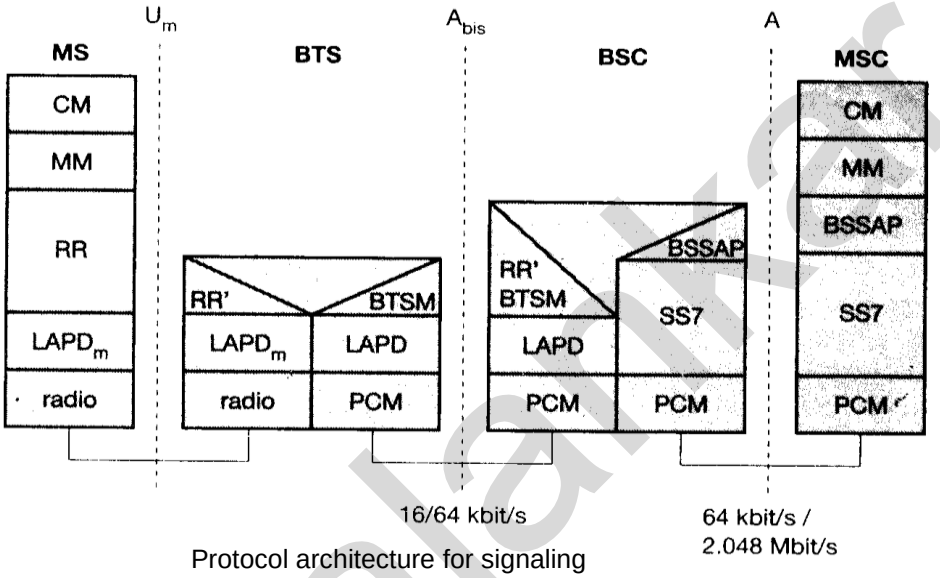


1. As shown in the above figure there are 8 time slots per TDMA frame, and frame period is 4.615ms, contains 8 × 156.25 1250 bits, of rate 270.833 kbps 1250 bits / frame.

2. Each of normal speech frames are grouped into larger structures called multiframes which inturn are grouped into superframes.

3. One multiframe contains 26 TDMA features, and one superframe contains 51 multiframes or 1326 TDMA frames.

PROTOCOLS



Protocol architecture for signaling

Main differentiating interface here is U_m interface (mobile user) because other interfaces occur between entities in a fixed network.

→ Layer 1, handles all radio specific functions.

For e.g.
- Multiplexing of bursts into TDMA frame
- Synchronization with BTS
- Measurement of channel quality on downlink
- Digital modulation and encryption and decryption.

1. All MSs within a cell use the same BTS and thus must be synchronized to this BTS. The BTS generates time structure of frames.
2. An MS close to BTS has very short round trip time (RTT), whereas an MS 35km away already exhibits an RTT of around 0.23 ms.
3. The BTS sends the current RTT to the MS, which then adjusts its access time so that all bursts reach the BTS within their limits. This reduces guard space by 30.5 μs or 5%. Adjusting the access is controlled via the variable timing advance.
4. The main task of physical layer is channel coding and error detection / correction which uses forward error correction FEC scheme.
5. As voice is assumed to be main service in GSM, the physical layer contains special functions as voice activity detection (VAD), which transmits voice data only when

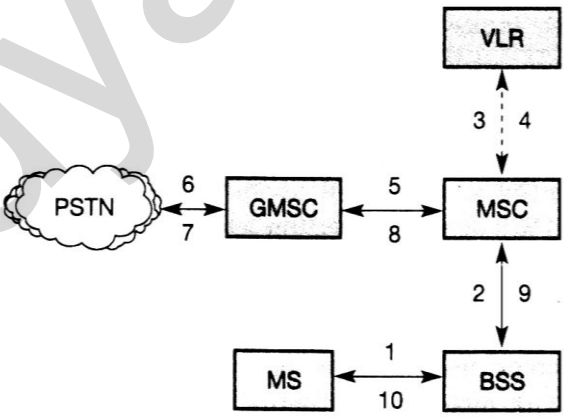
there is voice signal. This mechanism help to decrease interference as channel is silent for 60% of time.

6. All this interleaving of data for a channel to minimize interference due to burst errors and the recurrence pattern of a logical channel generates a delay for transmission.
7. Signaling between entities in GSM network requires higher layers. For this purpose, the LAPDm protocol has been defined at the U_m interface for layer two. It has derived from link access procedure for D–channel.
8. As there is no buffering between layer one and two, LAPDm has to obey the frame structures, recurrence patterns defined for U_m interface.
9. Third layer in GSM network, comprised several sublayers.
   i) RR : – Radio resource management – implemented in BTS.
   ii) BTSM : BTS management – functions of RR′ are supported by BSC via this BTSM.
10. MM – mobility management contains functions for registration, authentication, identification offers reliable connection to next higher layer
11. CM – call management – contains
    - call control
    - short message service (SMS)
    - supplementary services (SS)

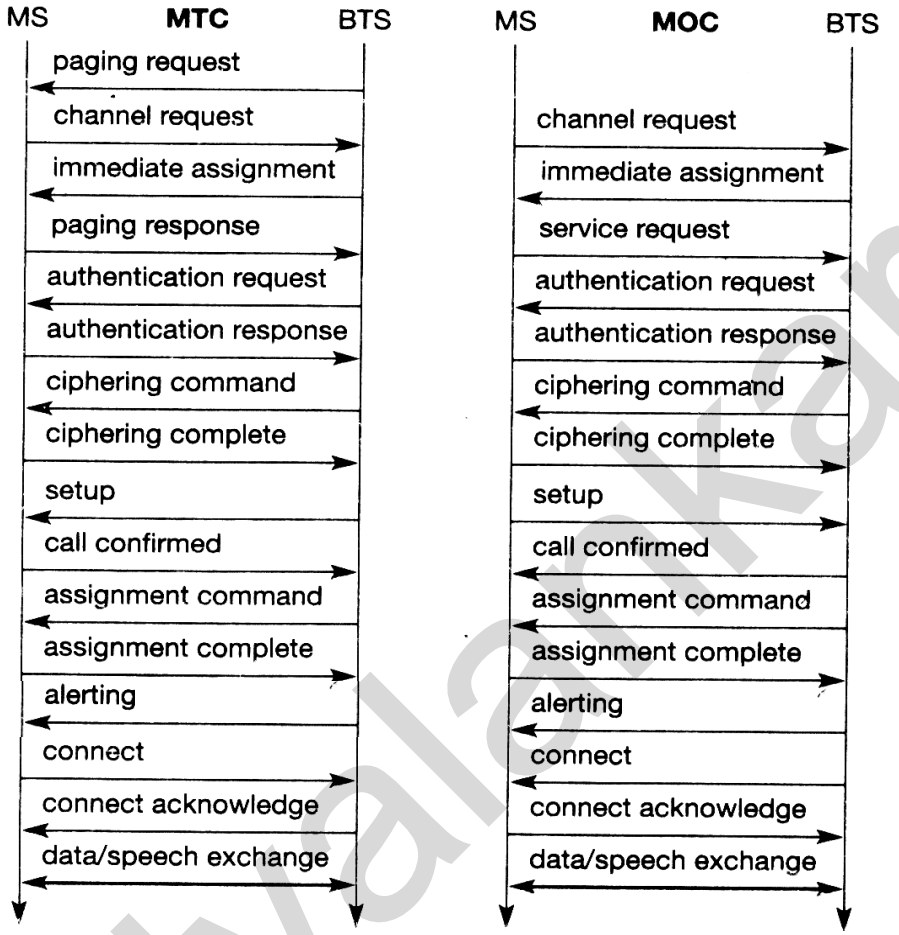
    Provides Dual tone multiple frequency (DTMF) for sending bandtone.
    DTMF transferred as signals and then converted into tones in the fixed network park of GSM.
12. Data transmission at physical layer uses pulse code modulation (PCM) systems.
13. Signaling system No.7 SS7 is used for signaling between an M.SC. and B.SC.

- **Localization and Calling**

MOC – Mobile originated call
MOC performing is much simpler than MTC. (mobile terminated call).



Mobile Originated call (MOC)



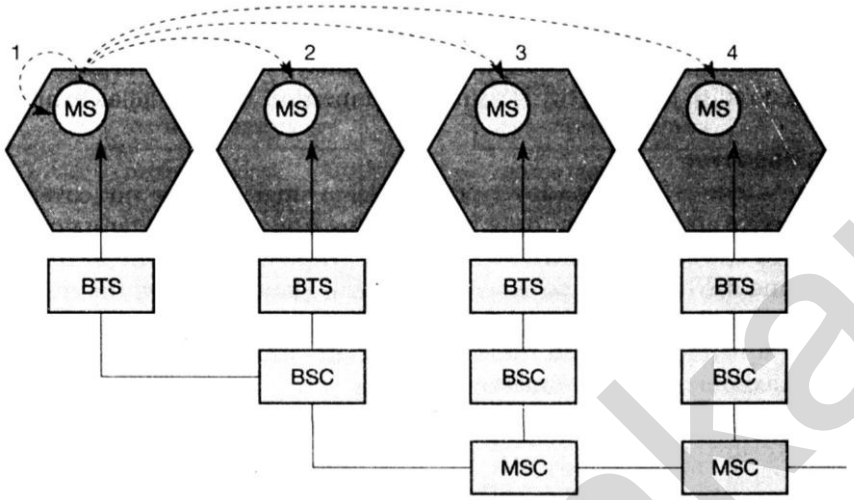
Message flow for MTC and MOC

Some additional messages are exchanged between MS and BTS during connection set up. These messages can be quite often heard in radios or badly shielded loudspeakers as cracking noise before the phone rings. Paging is necessary for an MTC.

First step is the channel access via the random access channel with consecutive channel assignment. It can be traffic channel (TCH) or slower signalizing channel (SDCCH).

Next step is, authentication of MS and switching to encrypted communication. System assigns a TCH. This has advantage of only having to use an SDCCH during first setup step. If setup fails no TCH has been blocked. Still using a TCH from the beginning has speed advantage.

The following steps depend on the use of MTC or MOC.



Types of handover in GSM

Above figure shows 4 possible handover scenarios in GSM

1. Intra cell handover : Within cell, narrow band interference could make transmission at a impossible frequency.

2. Intercell, intra BSC handover : MS moves from one cell to another but stays within the same control of BSC.

3. Inter BSC, intra–MSC handover : GSM perform handovers controlled by different BSC which inturn controlled by MSC.

4. Inter MSC handover : Both MSCs perform together handover .

- **Security**

Security services :

1. Access control and authentication : Uses needs secret PIN to access SIM. Next is subscriber authentication.

2. Confidentiality : User related data is encrypted which is encrypted by MS and BTS.

3. Anonymity : For providing user anonymity, GSM transmits a temporary identifier which is newly assigned by VLR after each location update.

In GSM, three algorithms are specified to provide security services

Algorithm $A_3 \rightarrow$ authentication .
$A_5 \rightarrow$ encryption.
$A_8 \rightarrow$ generation of cipher key.

Here only A_5 was publicly available, whereas A_3 and A_8 were secret.

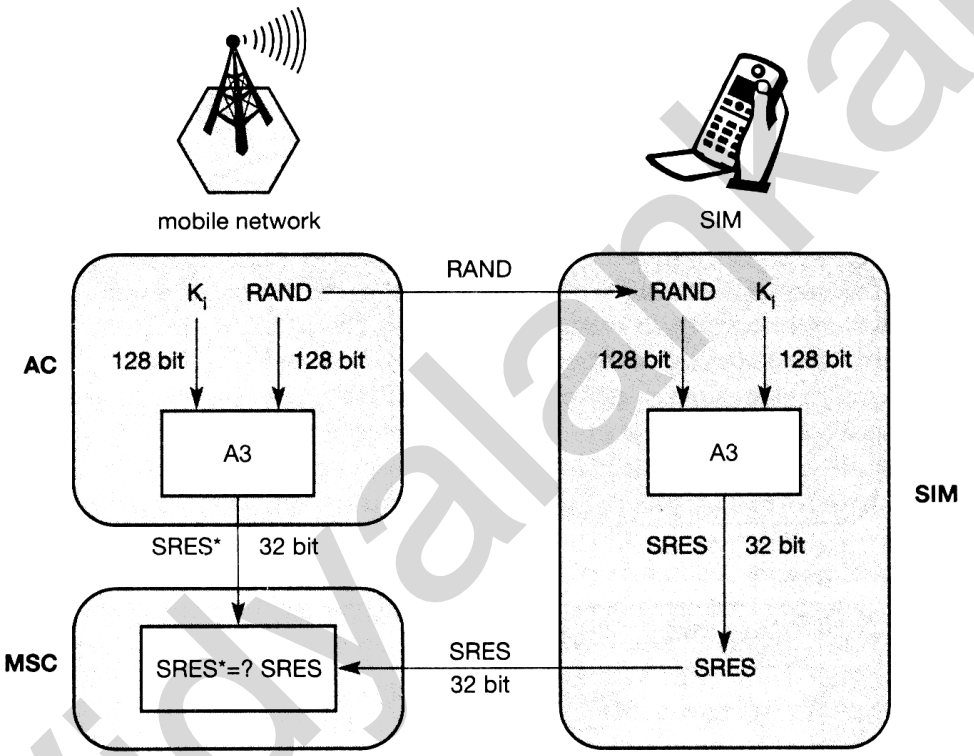
Authentication :

→ Authentication is based on the SIM, which stored the individual authentication key k_i. The user identification IMSI, and the algorithm used for authentication A_3.

→ Authentication uses a challenge response method : Challenge response method.

→ Access control generates random number RAND as challenge and the SIM within the MS answers with SRES as response.

For Authentication Process :



Subscriber Authentication

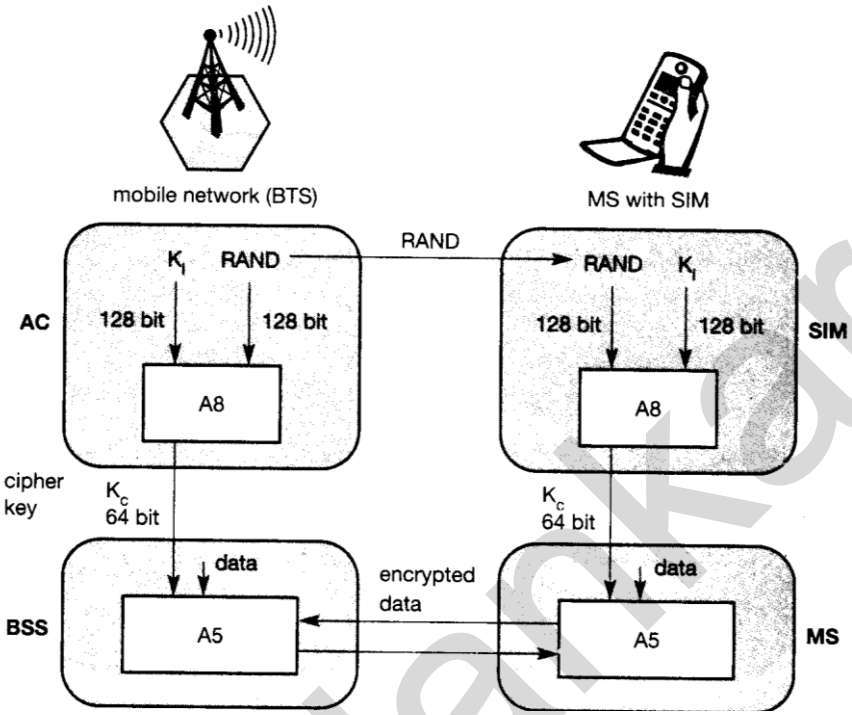
→ The VLR sends the random value RAND to SIM.

→ Both side party perform same operation, with RAND and key K_i is called A_3.

→ MS sends back the SRES given by SIM, VLR compares both values.

→ If both values same, VLR accepts subscriber otherwise rejected.

Encryption :
K_C – Cipher key generated using individual key K_i
RAND – generated by applying the algorithm A_8



Data encryption

MS and BTS can encrypt and decrypt data using the algorithm A_5 and cipher key K_C. K_C should be 64 bit key.

- **New data services :**

To enhance data transmission capabilities of GSM, 2 approaches are possible.

i) HSCSD (Connection oriented)
ii) GPRS (Packet oriented)

i) HSCSD

→ High speed circuit switched data, in which higher data rates are achieved by combining several TCHs.
→ MS requests one or more TCHs from GSM, it allocates several TDMA slots within TDMA frame
→ HSCSD only requires software upgrade in MS and MSC.
→ User connection – oriented mechanism of GSM.
→ For n channels, HSCSD requires n times signaling during handover, connection setup and release. So probability of blocking or service degradation increase during handover.

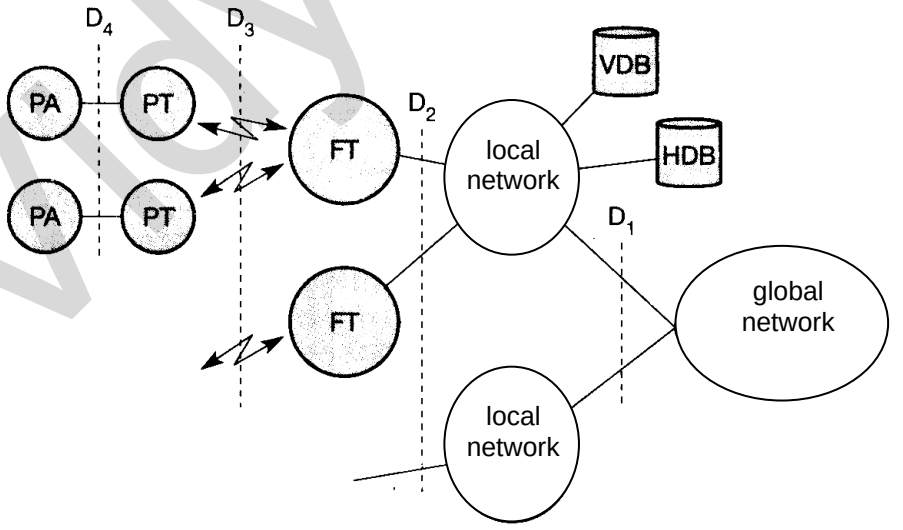
ii) GPRS

→ General packet radio service provides flexible and powerful data transmission.
→ Main benefit for users of GPRS is the 'always on' characteristic – no connection has to be set up prior to data transfer.

→ Unlike HSCSD, GPRS does not only represent a software update to allow for the bundling of channels, it also represents a big step towards UMTS as the main internal infrastructure needed for UMTS.
→ For new GPRS radio channels, the GSM system can allocate between one and eight time slots within a TDMA frame.
→ Time slots are not allocated in a fixed, predetermined manner but on demand
→ All time slots could be shared by the active users; up and downlink are allocated separately.
→ Allocation of the slots is based on current load and operator preferences.
→ In GPRS, real available data rate heavily depend on current load of the cell as GPRS typically only uses idle time slots.
→ GPRS offers a point to point packet transfer service.
→ GPRS has one ability of GPRS to maintain a virtual circuit upon change of the cell within the GSM network.
→ Users of GPRS can specify a QoS profile
→ In GPRS network, delay is incurred by channel access delay, coding for error correction. GPRS architecture introduces 2 network elements.
   i) GPRS support nodes (GSN) – contains, nodes having routing information.
   ii) Serving GPRS support node (SGSN) – supports MS via the Gb interface.
   Mobility management procedures are attached to data by MS whenever it is transmitted.

DECT [Digital Enhanced Cordless Telecommunications]
DECT replaces older analog cordless phone system. Main difference in GSM and DECT is the cell diameter and cell capacity.
GSM → Designed for outdoor use with a cell diameter of upto 70 km.
DECT → Range is limited to about 300m from the base station.

- **System Architecture**



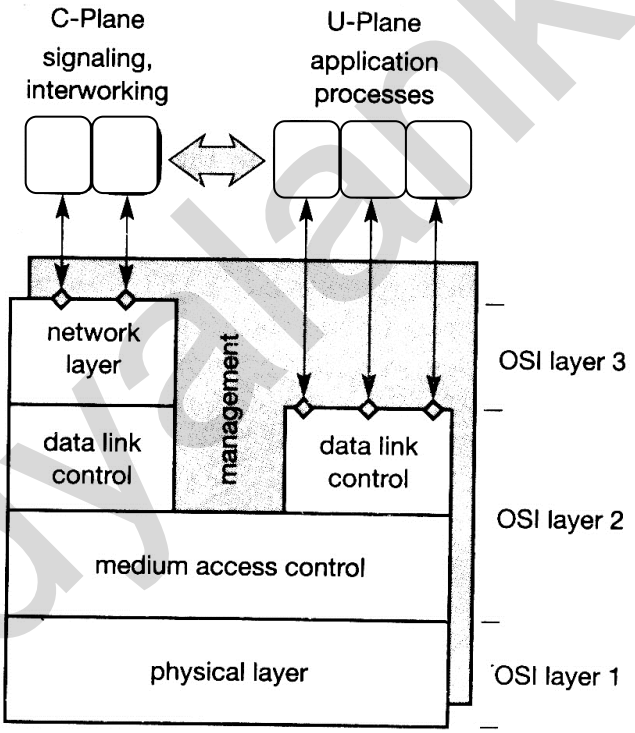
DECT system architecture reference model

A global network connects the local communication structure to the outside world and offers its services via the interface D_1. The services offered by these networks include transportation of data and the translation of addresses and routing of data between the local networks.

Local networks in the DECT context offer local telecommunication services that can include everything from simple switching to intelligent call forwarding address translation etc. As the core of DECT system itself is quiet simple, all typical network functions have to be integrated. In the local or global network where the databases home database (HDB) and visitor data base (VDB) are also located. The DECT core network consist of fixed radio termination (FT) and the portable radio transmission (PT).

- **Protocol Architecture**

Physical layer, medium access control and data link control & network layer are covered by control plane and user plane.



DECT protocol layers

TETRA [Terrestrial Trunked Radio]
TETRA offers two standards :

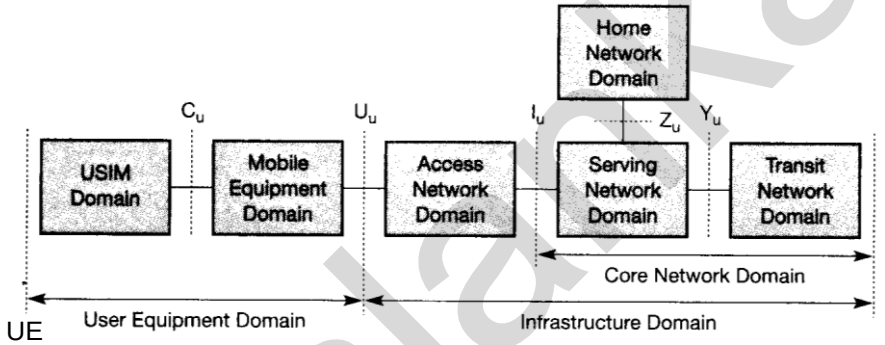
→ Voice + Data (V + D) service – offers circuit switched voice and data transmission
→ Packet data optimized (PDO) – only packet data transmission.

* UTRAN — funs → Cell level mobility
RNS (Radio network subsystem) —fun→ Radio Channel Ciphering, Dephering, handover control

* Radio interfaces → V_u similar to V_m interface in GSM.
$I_u \rightarrow$ similar to A interface in GSM

* CN funs → Intersystem handover, Gateways, Location management

Above architecture subdivided in domain as below



UMTS domains and interfaces

UE → VSIM domain —contains→ SIM, UMTS —funs→ encryption, authentication, data base storage

UE → Mobile Equipment domain —contain→ functions for radio transmission.

Infrastructure → Access network → Serving network domain → functions for UMT services.
Home network domain —funs→ user data lookup
Core network → Transit network domain —funs→ if serving network fails.

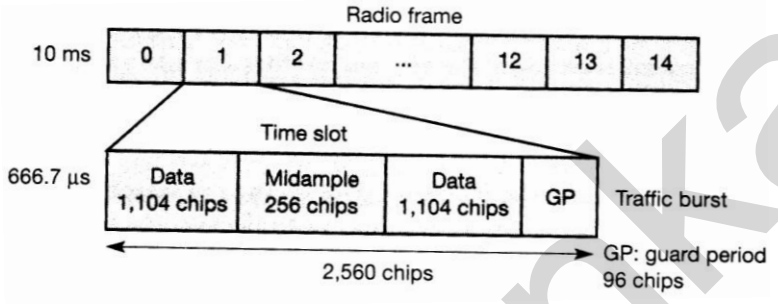
ULTRA – FDD MODE

FDD mode for UTRA uses wideband CDMA with direct sequence spreading. It is also referred as W–CDMA. W–CDMA interface is designed for "always on" packet based wireless services. W–CDMA supports data rates upto 2.048 Mbps / user. It allows, high quality data, multimedia, videoconferencing services to consumers. W–CDMA requires minimum spectrum allocation of 5MHz. W–CDMA provides backward compatibility and interoperability for all GSM. Therefore it requires a complete change of a RF equipment at each base station. A single W–CDMA 5MHz radio channel can carry the lowest 8kbps to highest 2Mbps simultaneously. W–CDMA provides six times increase in spectral efficiency.

W– CDMA requires, expensive new base station equipment, therefore installation will be slow and gradual.

ULTRA TDD : (TD – CDMA)

To meet the different users needs in terms of data rates, the TDD frame can be symmetrical or asymmetrical. This means the frame can obtain same number of uplink and downlink slots or any arbitrary combination. The frame can have only one switching point from uplink to do downlink or several switching points.



UMTS domains and interfaces

The above figure shows a burst of type 2 which comprises two data fields of 1,104 chips each. A midample is used for training and channel estimation. Guard period has been introduced at the end of each slot to loose the light synchronization. TDD licensing is quiet cheap than FDD.

❑ ❑ ❑ ❑ ❑

- **Advantages of WLAN :**

i) *Flexibility* :
Radio waves can penetrate walls, senders and receivers can be placed anywhere.
ii) *Planning* :
Only wireless ad–hoc networks for communication without previous planning.
iii) *Design* :
Only wireless networks allow for design of small, independent devices which can for be put into a pocket.
iv) *Robustness* :
Wireless networks can survive in disasters e.g. earthquakes.
v) *Cost* :
Wireless network will not increase cost whenever new users are added to first user via access point.

- **Disadvantages of WLAN :**

1) *Quality of Service* :
Low quality of service due to limitations in radio transmissions.
2) *Proprietary solutions* :
Proprietary solutions has to be offered by standardized company due to slow standardization process.
3) *Restrictions* :
WLANs are limited to certain – license free frequency bands, which are not same worldwide.
4) *Safety and Security* :
Open radio interfaces makes eavesdropping very easy in WLANs.

7.1 INFRARED VS RADIO TRANSMISSION

Infrared technology is very simple, it uses diffuse light reflected at walls, furniture, whenever LOS (line of sight) exist between sender and receiver.

- **Advantages of red technology :**

1. These are very simple and extremely cheap.
2. Easily available hence nowadays all mobile devices consists it.
3. No license is needed for red technology.
4. Shielding is very simple.
5. Electrical devices do not interface with red transmission.

- **Disadvantages of Infra–red transmissions :**

1. Infra-red transmissions are of low–bandwidth compared to other LAN technologies.
2. Infrared is quite easily shielded is one of its disadvantage.
3. Infrared transmissions can not penetrate walls or other obstacles.
4. For good transmission quality and high data rates a LOS is needed which is not possible.
5. IrDA services which are internally connected to a serial port limiting transfer rates to 115Kbits/s. Even 4Mbit/s is not a particularly high data rate.

- **Radio transmission :**

Advantages :–

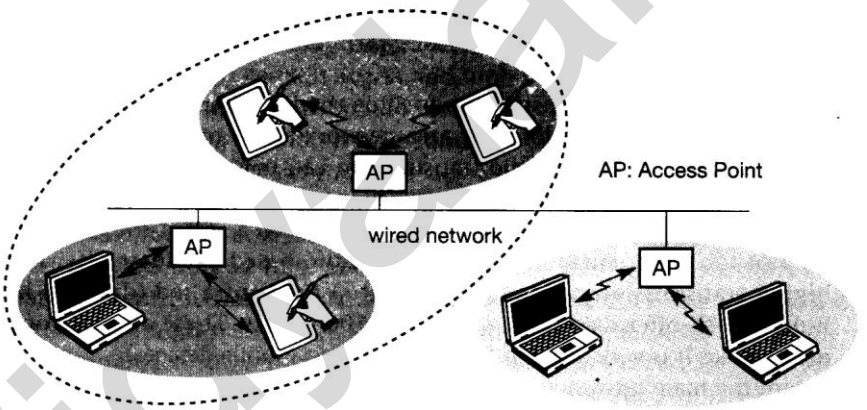
1. With radio transmission long term experiences are possible for wide area networks and mobile cellular phones.
2. Radio transmission can cover larger areas and can penetrate walls, furniture, plants etc.
3. Radio transmission gives additional coverage by reflection mechanism.
4. LOS problem is solved here. Radio transmission does not need a LOS if frequency is not too high.

Disadvantages :

1. In radio transmission, shielding is not simple.
2. Radio transmission can destroy data transmitted via radio by interfering senders electrical devices.
3. Since radio transmission is only permitted in certain frequency bands, very limited ranges of license –free bands are available all over world.

INFRASTRUCTURE AND AD–HOCK NETWORKS

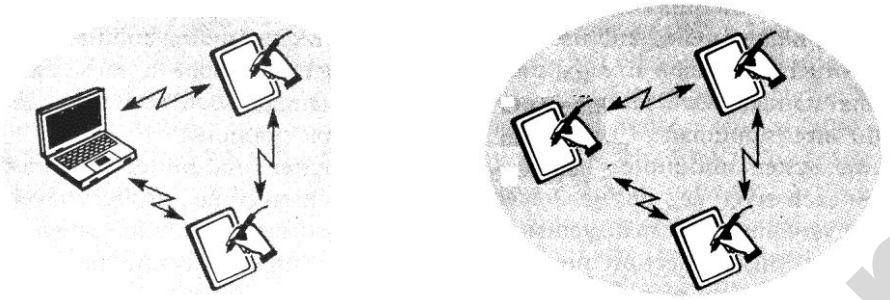
In infrastructure base wireless networks, communication between wireless nodes and the access point takes place. Two wireless nodes directly can not communicate.



Infra-structure based wireless networks

In above figure, three wireless networks can be connected with three access points. Thus access points together with fixed network can connect several networks to form a larger network beyond actual radio coverage. The design of such wireless networks are simple because the access point are the main functional elements, and this network structure is adopted from switched Ethernet or star–based networks in which central element controls the network flow. In this, if only the access points control medium access, no collision are possible. This guarantees the quality of service. For bandwidth of certain nodes.

There are some lackings also in infra–structure based networks. They lose some amount of flexibility. For e.g. disaster case where no infrastructure is left after that mishap. Cellular phone networks are this types of network, as well as satellite based cellular phones have the same. Bluetooth is wireless ad–hock network.



Example of two ad-hock wireless networks

In above figure, example of two ad–hock wireless networks are shown. Since each node can communicate with each other directly. If they are within each other's radio range, no access point is needed. Nodes which are from two networks can not communicate directly if they are not within the same radio range.

Complexity of each node is very high, because each node has to implement medium access mechanism, mechanism to handle hidden or exposed terminal problem, priority mechanism and quality of service. These type of networks exhibits greatest possible flexibility. Unexpected meetings quick replacements of infrastructure, and any such kind of incidences demand for such type of networks. In ad–hock networks, it may have selected nodes with capabilities of forwarding data, to which other node have to be connected first to transmit data, if receiver is out of their range. IEEE 802.11 and Hiper LAN 2 are example of infrastructure based networks which also supports ad–hock networking. Bluetooth's typical wireless ad–hock network.

IEEE 802.11

This standard belongs to the group of 802 × LAN standard like 802.3 Ethernet, 802.5 Token ring.

Primary goal of this standard was the specification of a simple and robust WLAN which offers time-bounded and asynchronous services. This standard specifies physical and medium access layer to the special requirement of wireless LANs, offering same interfaces to higher layer to maintain interoperability. Additional features of WLAN include :

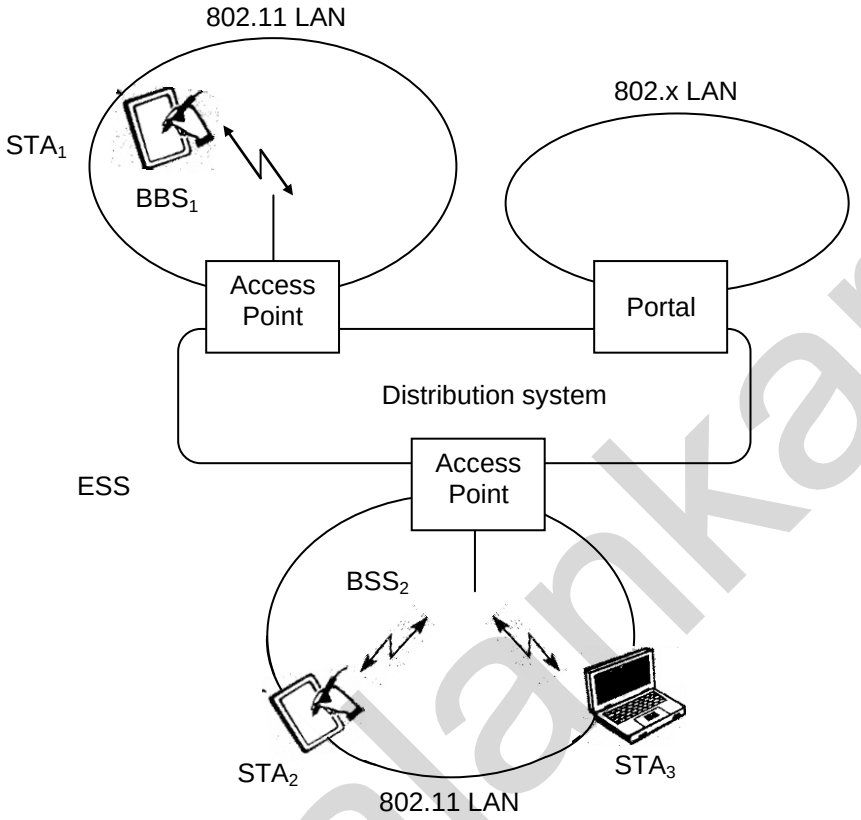
→ support of power management to save battery power
→ handing of hidden nodes and the ability to operate worldwide.

Original standard was 2.4GHz ISM band. Data rate for the standard were 1Mbit/s mandatory and 2bit/s optional.

- **System Architecture**

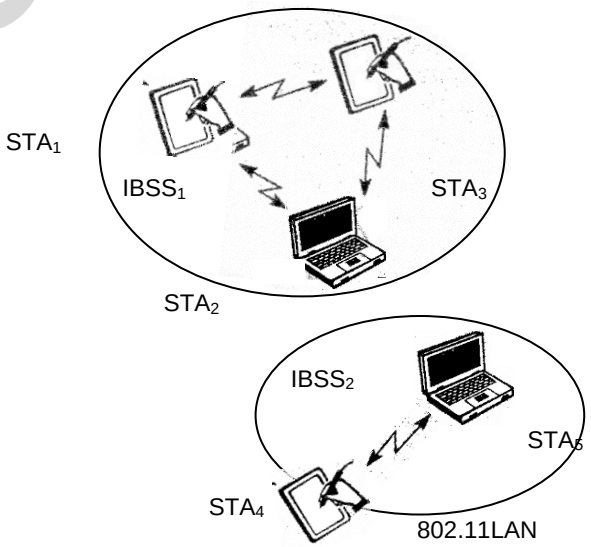
Two different basic system architecture should be studied in this topic which are

→ Infrastructure based
→ Ad–hoc based.



Architecture of an infrastructure based IEE 802.11

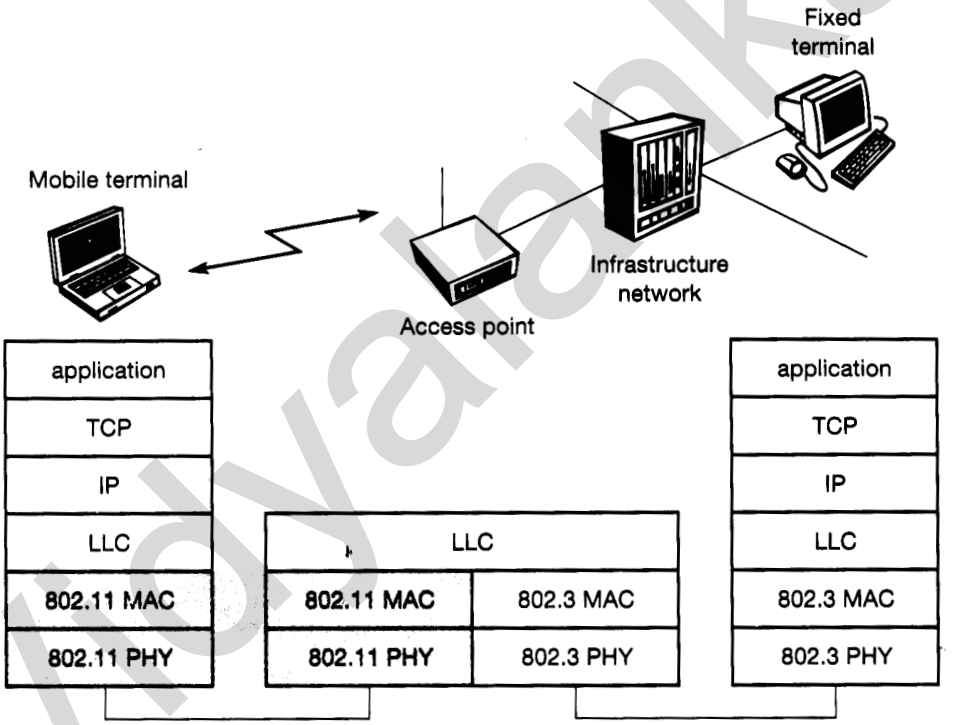
The figure, illustrates the architecture of an infrastructure based IEEE 802.11. In these several nodes, called stations (STA_1) are connected to access points (AP). Stations are terminals with access mechanism to the wireless medium and radio contact to the AP. Basic Service Set(BSS_1) is formed by the stations and the AP which are within same radio range. Two BSSs are connected to each other by distribution system as shown in figure. Thus distribution system forms a network by connecting several BSS via AP and extends wireless network. Now such network is called extended service set (ESS) having its own identifier the ESSID, without which entering in WLAN is impossible. Portal forms the internetworking unit to other LAN.



Distribution system provides services like protocols, bridge IEEE LANs, wireless LANs, data transfer between APs Distribution systems are defined in standards.

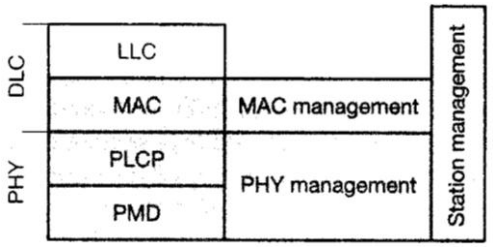
APs provide synchronization within a BSS support roaming, power management and can control medium access to support time–bound services. This was all about an infra-structure based IEEE 802.11. This standard allows the building of Ad–hock networks between stations. This forms one or more independent BSS_s ($IBSS_s$) as shown in figure above.

An IBSS contains a group of stations using the same radio frequency. STA_1 , STA_2 and STA_3 are in $IBSS_1$ and STA_4 and STA_5 in $IBSS_2$. STA_3 can communicate with STA_2 but not with STA_5. By using different carrier frequency, $IBSS_s$ can be formed. No special node is specified by IEEE 802.11 for supporting routing, forwarding of data or exchange of topology information as in infrastructure network, and HIPERLAN or Bluetooth.



IEEE 802.11 protocol architecture and bridging

The figure shows the most common scenario of IEEE 802.11 wireless LAN connection with switched IEE 802.3 Ethernet via bridge. In an application layer sender / receiver should not know the difference except lower bandwidth and higher access time from the wireless LAN, since WLAN behaves like a slow wired LAN. The upper portion of data link control layer, the logical link control covers the differences needed for different media. The IEEE 802.11 standard has the physical layer. (PHY) and medium access (MAC) Just like other 802 $\times$ LANs do.



Detailed IEEE 802–11 protocol architecture and management

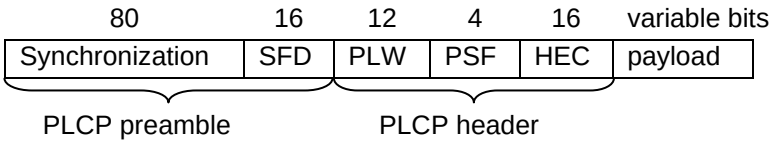
Let's understand the functions of each layer in above figure. Physical layer is divided into
(1) Physical layer convergence protocol (PLCP)
(2) Physical medium dependent (PMD)

- Functions of PLCP → Carrier sense signals called clear channel assessment (CCA).
  → Common PHY service access point (SAP).
- Functions of PMD → Handling modulation.
  → Encoding and decoding of signal.
- Functions of MAC layer → medium access control.
  → fragmentation of user data.
  → encryption.
- Functions of MAC management → supports association and reassociation of a station to an access point.
  → Power management saving battery power.
  → Maintains MAC management information base (MIB).
- PHY management functions → channel tunning and PHY, MIB maintenance.
- Station management function → to interact with both management layer.
  → higher layer functions.

- **Physical layer :**

PHY variants include the provision of clear channel assessment signal (CCA), for controlling MAC mechanism controlling medium access. There are three versions of a PHY layer defined in the standard.
1) Frequency hopping spread spectrum
2) Direct sequence spread spectrum
3) Infra red

1) Frequency Hopping Spread Spectrum (FHSS)
This mechanism allows for the coexistence of multiple networks in the same area by separating different networks using different hopping sequences



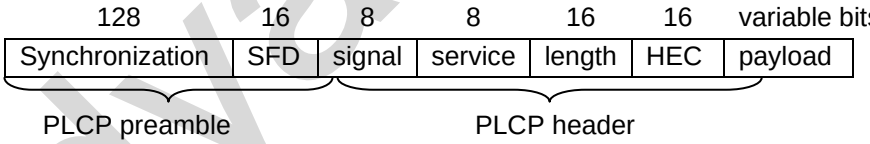
Format of an IEEE 802.11 PHY frame

The above figure shows a frame of the physical layer used with FHSS. The frame consist of two basic parts, the PLCP part header and preamble, and pay load part. The fields of the frame perform following functions.

i) *Synchronization* : PLCP preamble starts with 80bit synchronization, which is 010101 pattern, used for synchronization of potential receivers and signal detection by the CCA.
ii) *Start frame delimiter (SFD)* : this 16 bit pattern indicates the start of the frame and provide frame synchronization
iii) *PLCP PDU length word (PLW)* : First field of PLCP header indicates the length of the payload in bytes including the 32bit CRC at the end of payload.
iv) *PLCP signaling filed (PSF)* : This 4 bit field indicates the data rate of the payload following.
v) *Header error check (HEC)* : The PLCP header is protected by a 16bit checksum with the standard ITU–T generator polynomial $G(x) = x^{16} + x^{12} + x^5 + 1$

2) Direct Sequence Spread Spectrum (DSSS)

DSSS is the alternative spread spectrum method for separation by code and not by frequency. Main characteristics of this method is its robustness against interference and its intensity to multipath propagation



Format of an IEEE 802.11 PHY frame using DSSS

Above figure shows the frame structure using DSSS. The fields in the frame performs following functions.

i) Synchronization : First 128 bits not used in synchronization. This field only consists of scramble 1 bits.
ii) Start frame delimiter : This is 16 bit field used for synchronization of beginning of a frame and consist pattern 1 1 1 1 0 0 1 1 1 0 1 0 0 0 0 0.
iii) Signal : Two values have been defined for this field to indicate data rate at payload.
   (a) $0 \times 0A$ indicates 1Mbit/s
   (b) 0×14 indicates 2 Mbit/s.
iv) Service : Reserved for future use. 0×00 indicates IEEE 802.11 compliant frame
v) Length : 16 bits used to indicate length of payload
vi) Header error check (HEC) : Signal, service and length fields are protected by this

3) Infrared

Infra red transmission used by PHY layer, uses visible light at 850–950 mm. No need of LOS between sender and receiver, but should be working in diffuse light. Such mechanism using network will work in class rooms, buildings etc. No products are available in market that offers infra–red communication based on 802.11

- **Medium Access Sublayer**

Basic services provided by MAC layer are :

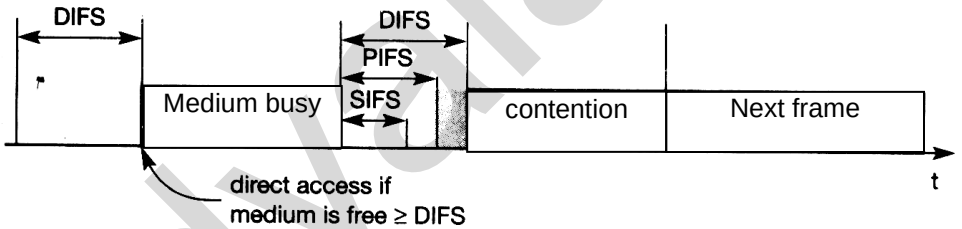
1. Asynchronous data service.
2. Time bound service.

These both services are offered in infrastructure based network with access points co-ordinating medium access. Three basic access mechanism are defined for IEEE 802.11 based on a version of CSMA/CA, one optional method to avoid the hidden terminal problem, and a contention free polling method for time–bound services. The first two methods are summarized as

Distributed co-ordination function (DCF)
and third method is summarized as
Point co-ordination function (PCF)

DCF → offers asynchronous service

PCF → offers both asynchronous and time bound service. Seeking an access point to control medium access and to avoid contention. MAC mechanism are also called distributed foundation wireless medium access control (DFWMAC)



Medium access and inter frame spacing

The above figure shows the three different parameters that define the priorities of medium access. The parameters depend on PHY and defined in relation to slot time. Slot time is 50μs for FHSS and 20μs for DSSS. The medium can be busy or idle. If it is busy, it is due to data frames or other control frames.

The phases in figure are

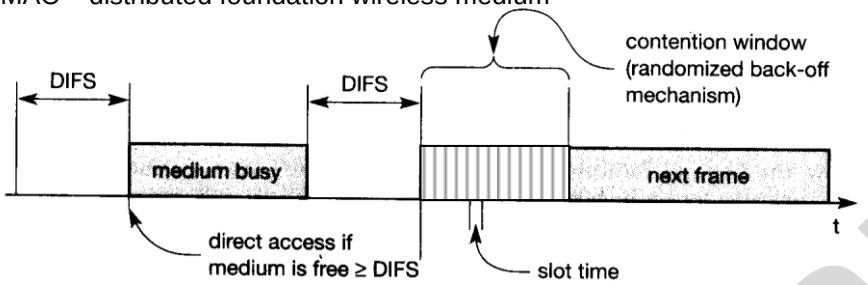
1) Short inter–frame spacing (SIFS)
   Shortest waiting time for medium access is defined for short control message such as acknowledgement of data packets or polling responses.

2) PCF interframe spacing (PIFS)
   AP which is polling other nodes only has to wait PIFS for medium access.
   PIFS = SIFS + One slot time

3) DCF interframe spacing (DIFS)
   This denotes the longest waiting time and has the lowest priority for medium access.
   Medium access control layer mechanisms are also called DFWMAC.

- **Basic DFWMAC using CSMA /CA**

DFWMAC – distributed foundation wireless medium



Contention window and waiting time

The above figure shows the CSMA / CA mechanism. CSMA / CA – carrier sense multiple access and collision avoidance.

If the medium is idle for at least, the duration of the period of DIFS a node can access the medium at once. By this short access delay under light load is allowed. Additional mechanisms are needed if more nodes are accessed.

If the medium is busy, node has to wait for the duration of DIFS, and enters a contention phase later. After this, a random back off time within a contention window is chosen by node and also delays medium access for this random amount of time. When a node senses the channel is busy and has lost its cycle it has to wait for the next chance.

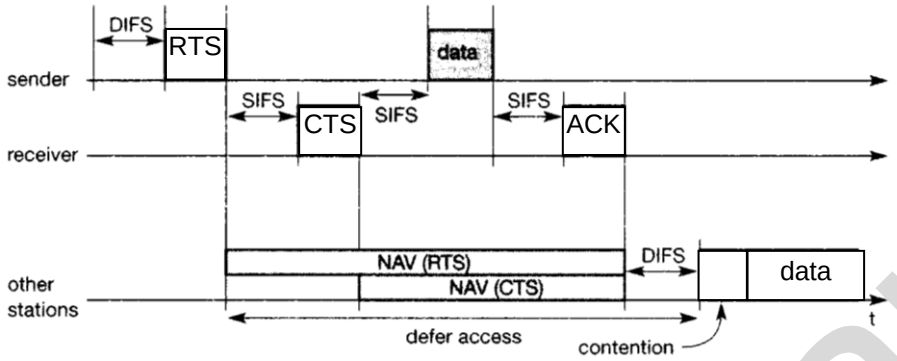
The additional waiting time is measured in multiples of above mentioned slots. This delay helps to avoid collisions – otherwise all stations would try to transmit data after waiting for the medium becoming idle.

To provide justice for waiting IEEE 802.1 adds a backoff timer. Now, again each node selects random waiting time as earlier. But if a station does not get access to the medium in first cycle, it stops backoff timer waits for channel to be idle again for DIFS and starts counter again. When counter expires, node access medium. This shows that deferred stations do not choose a randomized backoff time again but continue to count down.

In such case, stations that have waited longer have the advantage. Over stations that have just entered, in that they only have to wait for the remainder of their backoff timer form the previous cycle(s).

- **DFWMAC – DCF with RTS / CTS extension :**

Hidden terminals problem was discussed in the above problem. This problem occurs if one station can receive two others, but those stations cannot receive each other. If the two stations sense the channel is idle, send a frame and cause a collision at the receiver in the middle. RTS and CTS is solution to this problem which is defined by standard. The use of this mechanism is optional.



IEEE 802.11 hidden node provision for contention free access

In the above figure after waiting for DIFS, the sender can issue a request to send (RTS) control packet. The RTS packet includes the receiver of the data transmission to come and the duration of the whole data transmission. Every node which receives this RTS has to set its net allocation vector (NAV) in accordance with duration field. NAV gives the earliest point where the stations try to access the medium again.

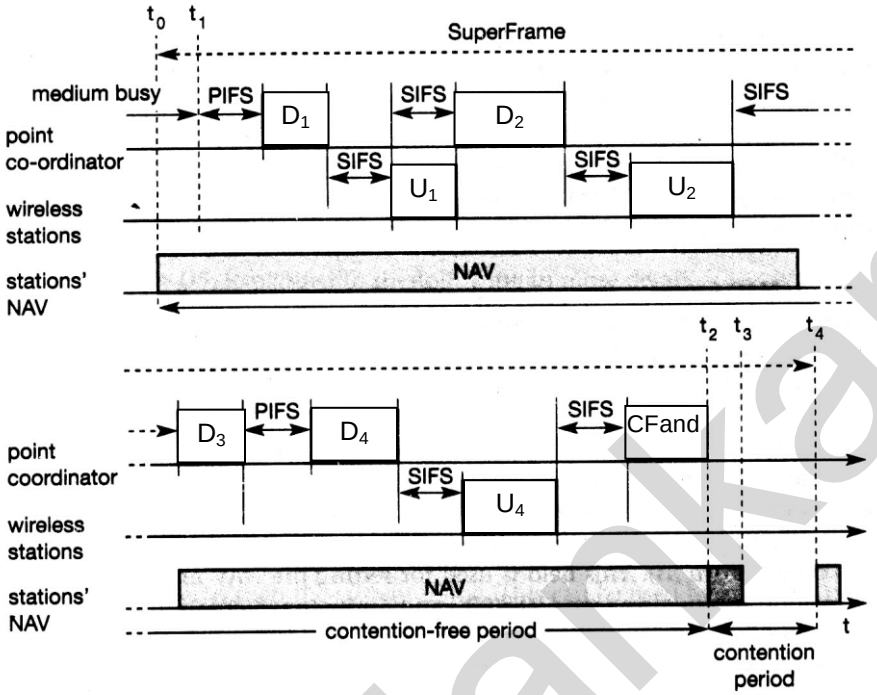
If the receiver of data transmission receives the RTS, it answers with a clear to send (CTS) message after waiting for SIFS. CTS packet contains the duration field again and all stations receiving this packet from the receiver of the intended data transmission have to adjust their NAV. The RTS packets received in later and early set are not necessarily same. All nodes within receiving distance around sender and receiver are informed that they have to wait more time before accessing the medium.

At the end the sender can send the data after SIFS. Receiver waits for SIFs after receiving the data packet and then acknowledges whether the transfer was correct. When the NAV in each node marks the medium as free, the standard cycle can start again. Collisions can only occur at the beginning while the RTS is sent. This happens because two or more stations may stand. Sending at the same time. RTS threshold can determine when to use the additional mechanism and when to disable it.

- **DFWMAC – PCF with Polling :**

Point coordination function (PCF) is specified by standards to provide time bound services. PCF requires an access point to control the medium access and polls the single node. Ad–hock networks do not support this function but provide 'best effort'.

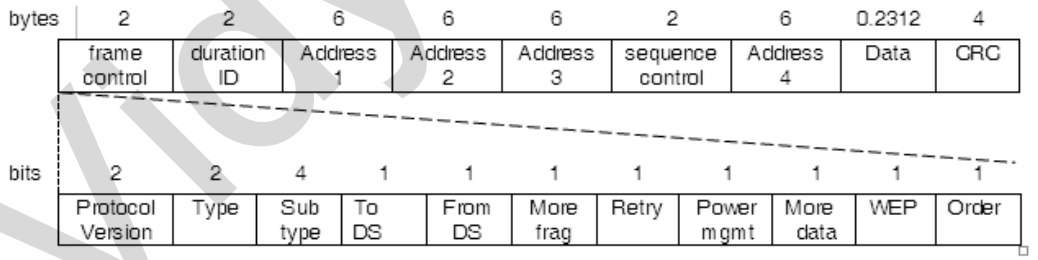
In the below figure, point co–ordinator in the access point splits the access time into super frame. A superframe contains contention free period and a contention period. At time to the contention free period of superframe starts theoretically but another station is still transmitting data. To avoid variations, the best possibility is not to have contention period. As soon as the medium has been idle i.e. t_1, the point co–ordinator has to wait PIFs before accessing the medium. Since PIFs is smaller than DIFs, none of the stations can start sending earlier. This starting and sending point coordination is send to data D_1 downstream. After answering of station, it waits for SIFs again. The point coordinator can poll the second station by sending D_2. This station answers upstream to coordinator with data V_2.



Contention free access using polling mechanism (PCF)

After waiting for PIFs, the co–ordinator resume polling the stations. By using PCF automatically sets the NAV, preventing other station from sending. This method can be reassembled with a static, centrally controlled time division multiple access with time division duplex transmission. One possibility of problem arises here if nodes having nothing to send, still the access point polls them permanently.

MAC FRAMES



IEEE 802.11 MAC packet structure

The fields in the above figure are listed below

1. Frame control ⇒ Contains several sub–fields that are explained after the MAC frame.
2. Duration / ID ⇒ Field used for setting the NAV for the virtual reservation mechanism and also contains value indicating the period for which medium is occupied.
3. Address 1 to 4 ⇒ Contains standard IEEE 802 MAC address.

Address 1 to 4 ⇒ Meaning of each bit depends upon the DS bits in frame control field.

4. Sequence control ⇒ Sequence number is used to filter duplicates.
5. Data ⇒ An arbitrary data is transferred transparently from a sender to receiver.
6. Checksum ⇒ Used to protect the frames

Frame control field components shown in figure are listed below.

1. Protocol Version ⇒ Contains current protocol version and fixed to 0 by now.
   ⇒ Value will be increased if standards are incompatible with current version.
2. Type ⇒ contains function of frame
   ⇒ management (= 00)
   ⇒ control (= 01)
   ⇒ data (=10)
   ⇒ 11 is reserved.

   Each has several subtypes given below.
3. Subtype ⇒ 0000 → for association requests,
   1000 → for beacon
   1011 → this subtype belongs to RTS
   1011 → CTS decoded as 1011
4. To DS / from DS ⇒ below explained
5. More fragments ⇒ This field is 1in management frame when they have another fragment of current MSDU to follow.
6. Retry ⇒ Set to 1 if repetition of transmitted frame.
   ⇒ Receivers can eliminate duplicate copies with help of this bit.
7. Power management ⇒ Can be used by station to access point to indicate that through polling is done more polling is required.
8. Wired Equivalent privacy ⇒ Though 802.11 standard security mechanism is used, many (WEP) weakness found in WEP algorithm, so higher layer security is needed to secure.
9. Order ⇒ If set to 1, frame are processed.

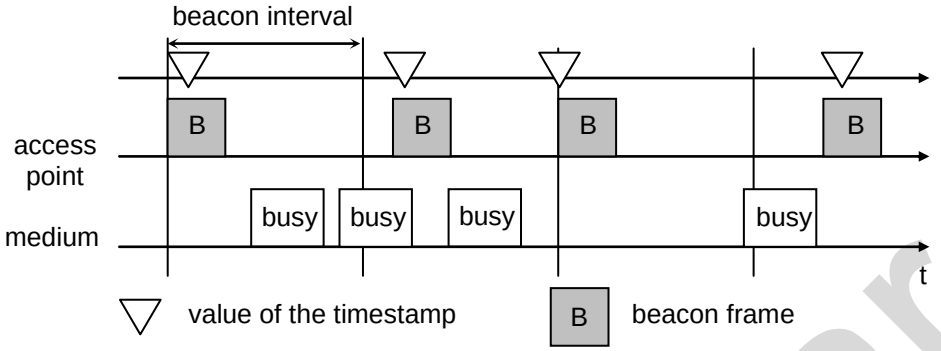
MAC MANAGEMENT

The below functional groups are classified in MAC management.

i) Synchronisation
ii) Power management
iii) Roaming.
iv) Management information base (MIB)

i) Synchronization

Timing synchronization function (TSF) are specified by IEEE 802.11 to synchronise the clocks of all nodes, which are needed for power management. Synchronization of clocks are also needed for coordination of the PCF and for synchronization of the hopping sequence in the FHSS system.



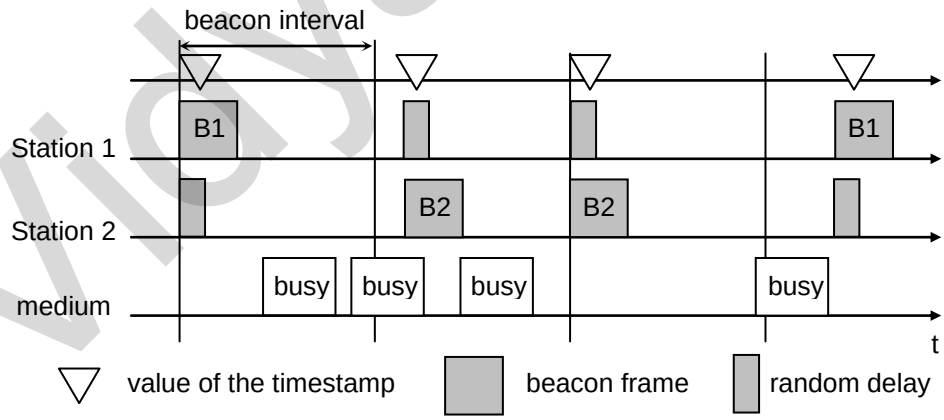
Beacon transmission in a busy 802.11 infrastructure network

In BSS, timing is conveyed by periodic transmission of beacon frame.

A beacon contains a timestamp and other management information used for power management and roaming. The node is not required to hear each beacon to stay synchronized, still time to time internal clocks should be adjusted.

In infrastructure based networks, the access – point performs synchronization by transmitting the periodic beacon signal, at that time other wireless nodes adjust their local timer to the time stamp. This situation is represented in figure showed above. The access point always tries to schedule transmission according to the expected beacon interval (target beacon transmission time). The time reflects the real transmit time, not the scheduled time.

Ad–hock networks don't have an access point for beacon transmission. So the situation is more complicated.

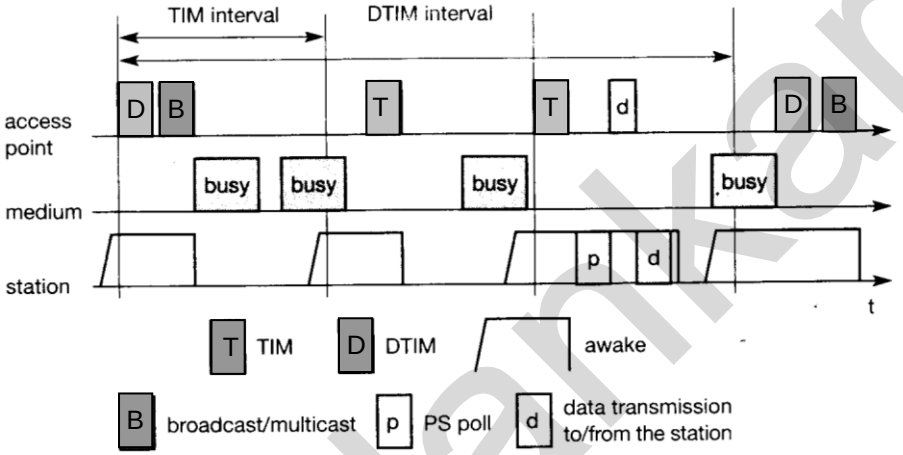


Beacon transmission in a busy 802.11 ad–hoc network

The above figure shows an example where multiple stations try to send their beacon. Standard random back off algorithms are applied to the beacon frames. So only one beacon could get, other stations adjust their internal clocks according to the received

beacon and suppress their beacons for this cycle. The beacon is lost if collision occurs. In such case, the beacon intervals can be shifted slightly because all clocks may vary as may the start of a beacon interval from a node's point of view.

- **Power management :**
  Basic idea of power saving includes two states for a station. Sleep and awake and buffering of data senders waking up at the right moment requires the timing synchronization function (TSF).



Power management in IEEE 802.11 infrastructure networks

Power management in infrastructure–based networks is much simpler compared to ad–hoc networks. A beacon is sent by access point along with a traffic indication map (TIM) is transmitted. TIM contains a list of stations for which unicast data frames are buffered in the access point. The access point transmits a beacon from each beacon interval. This interval is same as TIM interval. The access point maintains a delivery traffic indication map (DIM) interval for sending broadcast / multicast frames, this is multiple of the TIM interval.

In the above figure, all stations wake up prior to an expected TIM or DTIM. Here in first case, the access point has to transmit a broadcast frame and the stations stays awake to receive it. The stations returns to sleeping mode when it receives broadcast frame and again wake up just before the next TIM transmission. Since TIM is delayed due to busy medium, the stations stays awake. At this time access point has nothing to send and the station goes back to sleep.

At next TIM interval, the access point indicates that the station is the destination for a buffered frame. The station answers with a PS poll and stays awake to receive data. The access point acknowledges the receipt and may also send some data, which is acknowledged by access point.
The shorter the TIM interval, the shorter the delay, but the lower the power–saving effect.

In ad–hoc networks, power management is more complicated than in infrastructure networks. There is no access point to buffer data in one location but each station

needs the ability to buffer data if it wants to communicate with a power–saving station. Destination are announced using ad–hoc traffic indication map (ATIMs). The announcement period is called ATIM window.

- **Roaming**

  Moving between access points is called "roaming" "handoff" & handover" terms are related with mobile or cellular phone systems.

  The steps for roaming between access point are :

  1. The station starts scanning for the access point having the current link quality good.
  2. Scanning involves active search for another BSS. Passive scanning means listening or receiving the beacon of another network issued by synchronization function.
     Active scanning means sending a probe on each channel and waiting for a response.
     Beacon and probe contains necessary information to join the new BSS.
  3. Selection of the best access point for roaming based on signal strength and sending an association request to the selected access point AP_2
  4. If Association response answered by AP_2 is successful, the station has roamed to the new access point AP_2 or need to continue scanning.
  5. The distributed system updates its database, containing the current location of wireless stations which is needed to be forwarded between different BSS.

- **Future Development**

  1) 802.11e (MAC enhancements) : Since currently 802.11 standards don't offer quality of service in DCF operation mode, and some QoS guarantees are given only via polling PCF. The MAC layer is needed to be compared with current standards.

  2) 802.11F (Inter access point protocol) : In the current standard implementation of components such as distribution system, and detailed interface definition were not provided. 802.11F standardizes the necessary exchange of information between access points to support distribution system.

  3) 802.11g (Data rates above 20Mbit/s at 2.4GHz) : The 802.11g proposed standard offers packet binary convolutional coding to reach a data rate of 22Mbit/s. By providing this, coverage is better at 2.4 GHz and fewer access points are needed, lowering the overall system cost. Access points in 802.11 can also communicate with 802.11b devices as the current 802.11g products show.

  4) 802.11h (Spectrum managed 802.11a) : This standard comprises the enhanced spectrum managed 802.11a, with which 802.11a products can also be operated in Europe. The mechanism try to balance the load in the 5GHz band. The European requirements for power control and dynamic selection of the transmit frequency was not comprised in earlier standard.

  5) 802.11i (Enhanced security mechanism) : This mechanism provides strong encryption and authentication mechanism.

BLUETOOTH

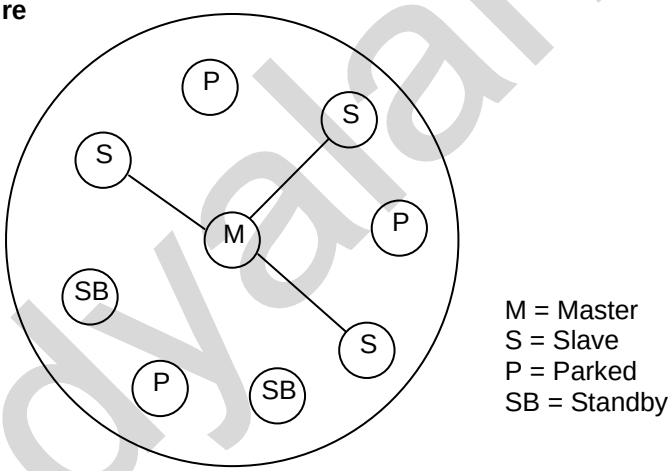
Bluetooth fulfill the following criterias :

1. Market Potential : For a certain technology whether there are applications, devices, vendor, customers are available.
2. Compatibility : Compatible with IEE 802
3. Distinct identity : Low cost, low power or second small form factor not addressed in 802.11 standard.
4. Technical feasibility : Prototypes are studied.
5. Economic feasibility : The developed things are cheaper than other solution and allow for high volume protection.

User Scenarios :

1. Connection of peripheral devices : No wires are needed, batteries replaced by power supply and also supply the peripheral devices with power. So wires blocking is eliminated which used to happen in early transmission.
2. Support of ad–hoc networking : Wireless networks supports interaction by having cheaper Bluetooth chips built in.
3. Bridging of networks : Mobile can be connected to a PDA or laptop by using simple Bluetooth chip built in.

- **Architecture**



Simple Bluetooth piconet

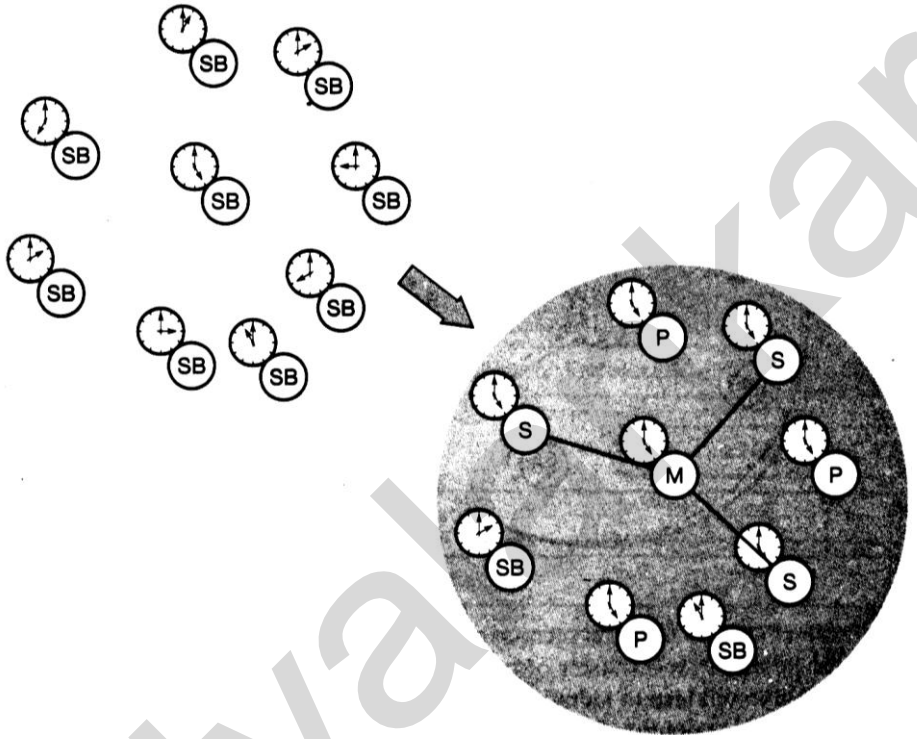
The important term in context of Bluetooth is piconet. A piconet is a collection of Bluetooth devices which are synchronized to the same hopping sequence. The above figure shows a collection of devices which performs different roles. In the devices, one device is called master (M), all other devices connected to master act as slaves(s). Functions of master is to determine hopping pattern in the piconet and the function of slave is to synchronize this pattern. Each piconet has a unique hopping pattern, whenever a device want to participate it has to synchronize this.

Two additional devices shown are :

1. Parked devices
2. Stand–by devices.

Parked devices ⇒ These cannot actively participate in piconet but can be reactivated within some milliseconds.
Stand by ⇒ These do not participate in the piconet

If a parked device wants to communicate and there are already seven active slaves, one slave have to switch to park mode to allow the parked device to switch to active mode.



Foaming a Bluetooth piconet

"Forming a Bluetooth piconet" process has the first step which involves a master sending its clock and device ID. Any device can be master or slave because all devices have same networking capability, like that terminals and base stations don't have any distinction. The two or more devices can form a piconet. The unit establishing the piconet automatically becomes the master and all other devices become slave. After adjusting the internal clock according to the master as a device may participate in the piconet. Active devices are assigned a 3–bit active member address (AMA). Parked devices use an 8bit parked performance of a single piconet is degraded because more collisions may occur. If two or more piconets use same carrier frequency, collision occurs. A device wishing to participate in more than one piconet, has to synchronize to the hopping sequence of the piconet it want to take part in. A slave informs the current master that it will be unavailable for a certain amount of time while leaving one piconet. Roaming devices keeps continuing communicating. A master can also leave its piconet and act as a slave in another piconet. As soon as a master leaves a piconet, all traffic within this piconet is suspended until the master returns.

SECURITY

Main security features offered by Bluetooth are

⇒ Challenge response routine for authentication.

⇒ Stream cipher for encryption

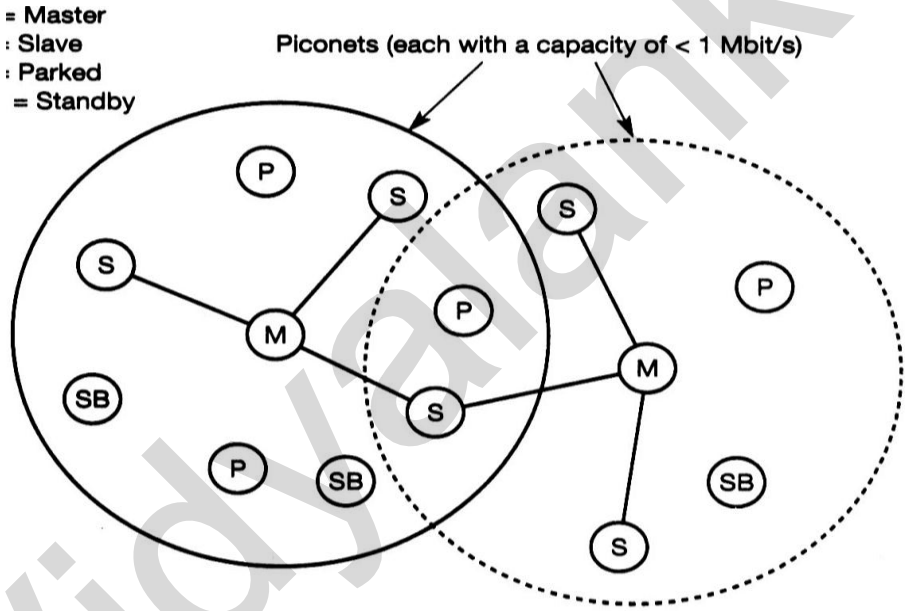
⇒ A session key generation

All the above features have to be implemented in silicon and higher layers should offer stronger encryption if needed.

Member devices (PMA) Devices in stand–by do not need an address.

Scatternet :

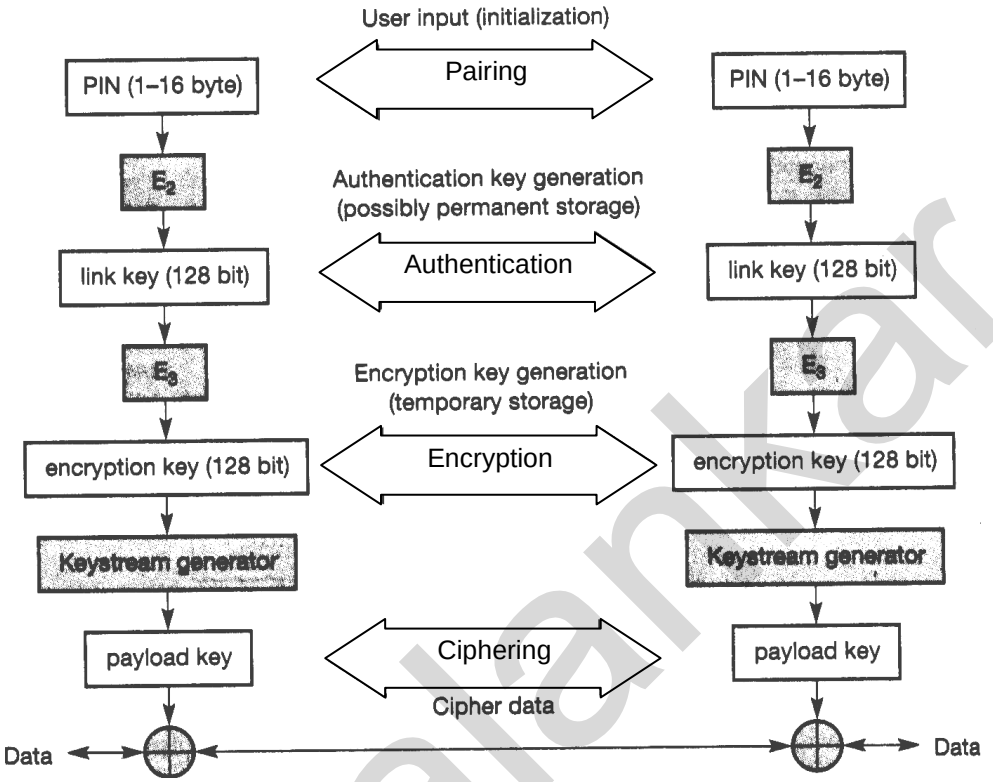
Since more users join the piconet, the throughput per user drops quickly. This led to the idea of formation of groups of piconet called scatternet. Units exchanging data, share the same piconet, so that many piconets with overlapping coverage can exist simultaneously.



Bluetooth Scatternet

In the above figure, scatternet consist of two piconets, in which one device participate in two different piconets. Master of the piconet determines the hopping frequency which is different for both piconets. FH–CDMA is used for separation of piconets. If more piconets are added, the authentication, and random number an encryption key is generated during the encryption stage of security architecture. This key is of 128bits. Payload key is generated based on encryption for ciphering data. The payload key is a stream of pseudo–random bits. The ciphering process is simple XOR of user data and payload key.

LINK MANAGEMENT



Bluetooth security components and protocols

Link management is performed by groups formed by link management protocol based on their functionality. Link management comprises of the functions given below.

1. Authentication, pairing and encryption : Authentication is handled in the baseband, and deals with controlling the exchange of random numbers and signed responses. Paring services are needed to establish initial relation between two devices which has never communicated before which results in a link key. Link management do not directly deal with encryption process but sets encryption mode, key size and random speed.

2. Synchronization : Link management has a major function “precise synchronization” in Bluetooth network. In this security algorithm use parameter below :
   - ⇒ Public identity of a device.
   - ⇒ Secret private user key
   - ⇒ Internally generated random key.

The very first step pairing is necessary if two Bluetooth devices have never met before. A user can enter a secret PIN into two devices to set up trust between then, which is of 16byte length. The device address and random numbers, and several keys are computed based on PIN, those are used as link key for authentication.

Based on the link, key, values generated during functions included are clock offset updating each time a packet is receiver from the master.

- **Capability negotiation :**
  Link management not only support the exchanging but also information about supported features.

- **Quality of Service negotiation :**
  The parameters of controlling the quality of service lie in lower layers. The parameters are poll interval, controlling the latency and transfer capacity. The features are multi–slot packet, encryption, voice encoding, etc.

- **Power Control :**
  A Bluetooth device measures the received signal strength, depending the signal level. The device can direct the sender of the measured signal to increase or decrease its transmit power.

- **Link Supervision :**
  Link management has LMP link manage protocol to control the activity of a link, it may set up new links, or it may declare the failure of a link.

- **State and transmission mode change :**
  Link management also performs the following function
  ⇒ Switching from & to master / slave role
  ⇒ Detach themselves from a connection
  ⇒ Change the operating mode.

❑ ❑ ❑ ❑ ❑

MOBILE IP

Mobile IP does not involve major changes in the basic architecture but corrects some minor problems.

- **Goals, assumptions and requirements :** Routers in the internet look at the destination address of incoming packets. And forward them according to internal look–up tables. To avoid an explosion of routing tables, only prefixes are stored and further optimizations are applied. As long as the receiver can be reached within its physical subnet, it gets the packets as soon as it moves outside the subnet.

- **Quick Solutions :** The domain name system (DNS) needs some time before it updates the internal tables necessary to map a logical name to an IP address, changing the IP address while still having a TCP connection open means breaking connection. Socket Pair (TCP connection) is identified by a tuple. TCP connection can not survive any address change which is a severe problem.

  Another approach to solve this problem is creation of specific routes to the mobile node, whenever it is possible to change routing tables all over the world to create specific routes to a mobile node. No service provider or system administrator allows changes to the routing tables, because routers are brains of internet which holds the whole net together.

- **Requirement :** The requirement for enabling mobile IP, as a standard in the internet is as follows :

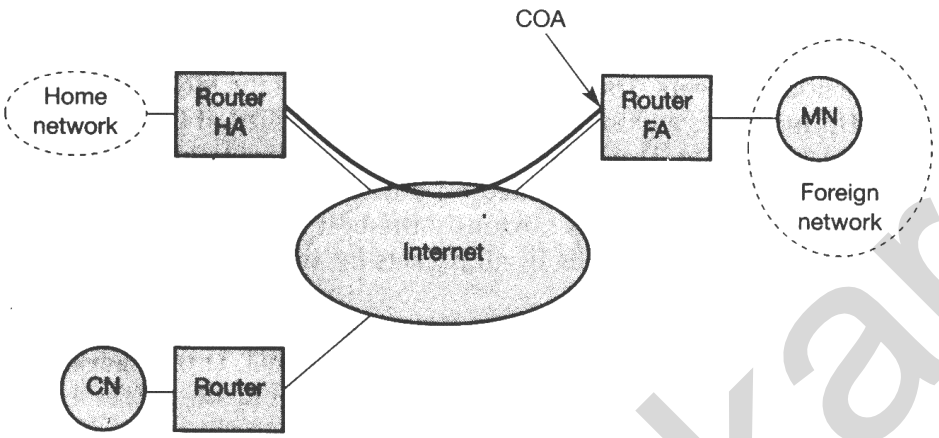
  1) Compatibility : A mobile IP should be integrated into existing operating systems so as to work with them. Mobile IP has to remain compatible with all lower layers used for the standard, non–mobile IP. Mobile IP should remain compatible. Same interferences and mechanisms to access the lower layers as IP does should not require media MAC/LLC protocols.

  2) Transparency : The mobility should remain 'invisible' for many higher layer protocols, without noticing a lower bandwidth any interruption in service. In context, to TCP, the computer must keep its IP address.

  3) Scalability and efficiency : The mobile IP enhancing must not decrease efficiency. Scaling mobile IP over a large number of participants in a whole internet is a crucial factor.

  4) Security : The IP layer can guarantee that the IP address of the receiver is correct. There is no way to prevent fake IP address or other attacks.

ENTITIES AND TERMINOLOGY



Mobile IP example

- Mobile Node (MN)
  - ⇒ An end system or router that can change its point of attachment to the internet using IP.
  - ⇒ Keeps its IP address and continuously communicate with other system, till the link layer connectivity is there.

- Correspondent node (CN)
  - ⇒ CN represent communication partner for MN.
  - ⇒ Can be fixed or mobile node.

- Home network
  - ⇒ Subnet of MN belongs with respect to its IP address.

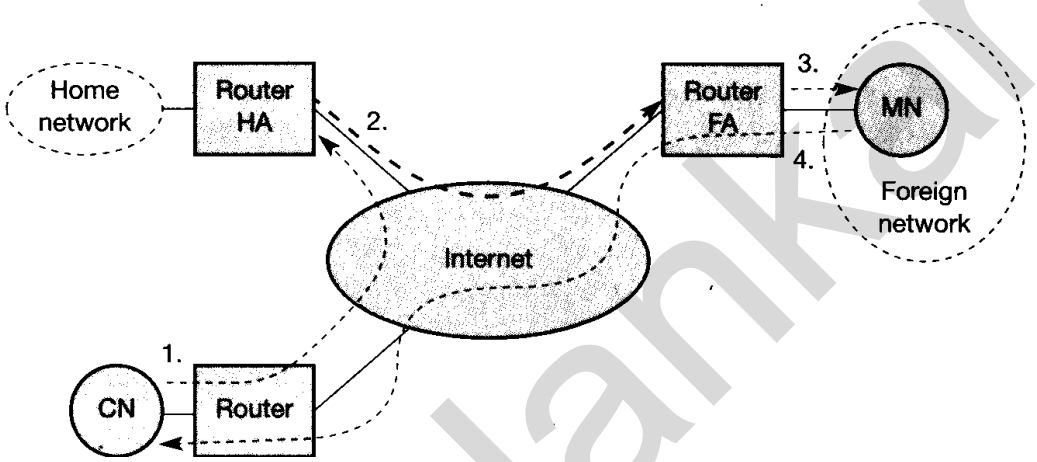
- Foreign network
  - ⇒ Current subnet, the MN visits, not in home network.

- Foreign Agent (FA)
  - ⇒ FA have COA (care of address) which act as tunnel endpoint and forward packet to MN.

- Care–of address (COA)
  - ⇒ It defines current location of MN from IP point of view.
  - ⇒ Foreign Agent COA (FA) →
    COA is an IP address of FA.
  - ⇒ Co–located COA
  - ⇒ COA co–located if MN temporarily acquired, an additional IP address, ads as COA.
  - ⇒ COA is not always considered for scarcity of IPV4 address.

- Home Agent (HA)
  - ⇒ It maintains a location registry.
    Alternative for HA
  - ⇒ HA can be implement in router & responsible for home network.
  - ⇒ HA could also be implemented on an arbitrary node in the subnet.
  - ⇒ Though HA could be implemented an router can act only as a manager for MNS.

IP PACKET DELIVERY



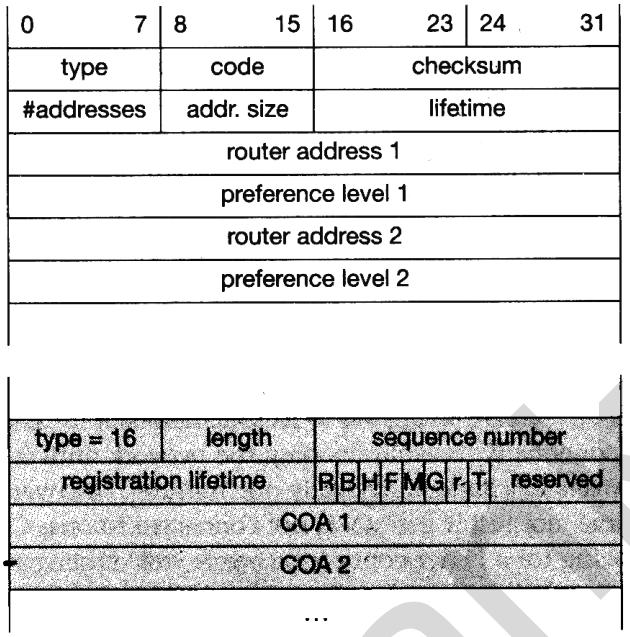
Packet delivery to and from the mobile node

Step 1 : CN do not need to know anything about the MN's current location and sends the packet as usual to the IP address of MN.
Step 2 : HA intersects packet, considering MN is currently not in home network. Packet is forwarded into subnet as usual; but encapsulated and tunneled to the COA. New header is put in front of the old IP header shown the COA as new destination & HA as resource of encapsulated packet.
Step 3 : The foreign agent duplicates, the packet by removing the additional header and forwards the original packet with CN as source and MN as destination to the MN.
Finally, it receivers the packet with same sender and receiver address as it would have done in home network.

- **Agent advertisement and discovery**

To find out foreign agents, MN has to search for it. To enable MN to know that it has moved, mobile IP described & methods.
1) Agent advertisement
2) Agent solicitation

The below figure is the agent advertisement packet according to RFC 1256 with the extension for mobility.



Agent advertisement packet (RFC 1256 + mobility ext)

In the above figure, upper part represents the ICMP packet and the lower part is extension needed for mobility. Internet control message protocol (ICMP) used with mobility extension according to RFC. The fields In ICMP part are as follows. Foreign agents are required to forward packets from mobile node. The number of addresses advertised with this packet is in address.

The fields are as follows:

- Lifetime ⇒ for the length of time this advertisement is valid.
- Preference level ⇒ helps a node to choose the router.
- Extension for mobility ⇒ 1) Type set is 16
  2) Length depends on number of COAs provided.
- Sequence number ⇒ Total number of advertisement from initialization.
- Registration lifetime ⇒ specify the maximum lifetime in seconds.
- R bit ⇒ Registration with this agent required when using a collocated COA at MN.
- B bit ⇒ If agent is too busy to accept new registration.
- H bit and F bit ⇒ If agent offer services as home agent (H) or foreign agent (F).
- M and G bit ⇒ The method of encapsulation for tunnel.
  M → Minimal encapsulation
  G → Generic routing encapsulation
- V bit → for use of header compression
- r bit → set to zero must be ignored.
- T bit → reverse tunneling.

This is one way for MN to discover its location.

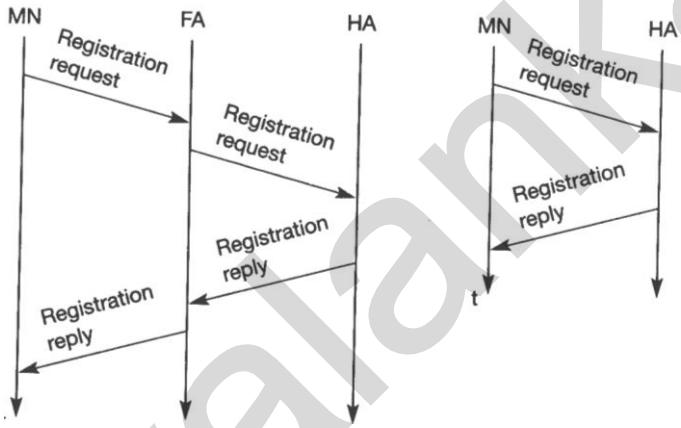
- **Agent Soliciations**

Mobile node must send agent soliciation and it sends 3 soliciation messages whenever it enters in new network. If in case, a node does not receive an answer to its soliciations it must decrease the rate of soliciations to avoid flooding until it reaches a maximum interval between soliciations.

After these steps of advertisement or soliciations the MN can receive a COA either from FA or co–located COA. Registration is the next step for the MN with HA if MN is in a foreign network. MN knows its location and capabilities of agent.

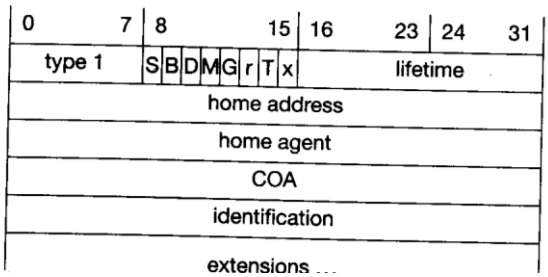
- **Registration**

Main goal of registration is to inform the HA of the current location for correct forwarding of packets. There are two different ways, the registration can be done depending on the location of the COA.



Registration of mobile node via the FA or directly with the HA

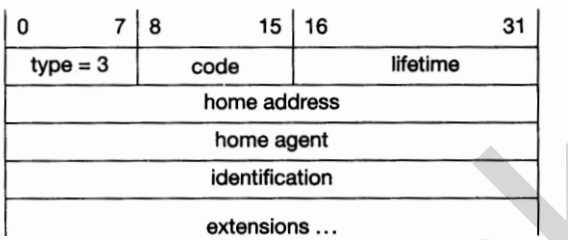
The MN sends its registration request which contains the COA to FA. FA forwards the request to the HA. HA sets up a mobility binding which contains the mobile node's IP and current COA and also lifetime of the registration. The registration process expires automatically as soon as lifetime is deleted. Again mobility binding is set up and HA sends a reply message back to the FA, is forwarded to MN.



Registration request

If the COA is co-located, registration is simpler. MN sends the request directly to HA. If the MN received an agent advertisement from the FA it should register via this FA if R bit is set in the advertisement. Registration request uses UDP packets, because they are low overheads and better performance as compared to TCP in wireless environments. The relevant fields, for mobile IP registration requests follow as UDP data. The fields are defined as below:

Type → Set to 1 for registration request.
S → MN specify if it wants the HA to retain prior mobility binding.
B → indicates that MN also want to receive the broadcast packets.
D → indicates the behaviour of MN in case of if it uses co-locate COA and also takes care of decapsulation at tunnel endpoint.
M & G → Minimal encapsulation & generic routing.
T → reverse tunneling
r & x → set to zero.



Registration reply

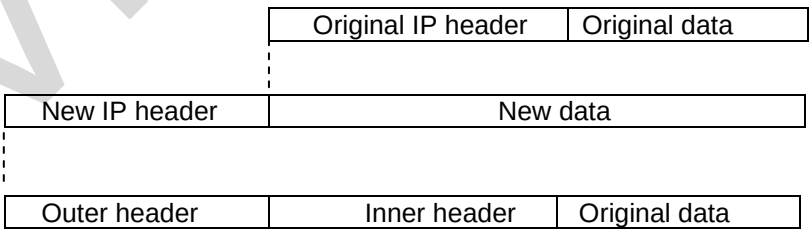
In the above figure :
Lifetime → denotes validity of registration in seconds.
Home address → is fixed IP address of the MN.
Identification → 64 bit, generated by MN to identify request & match registration replies.
Extensions → for the purpose of containing parameters for authentication.

A registration reply is conveyed in UDP packet contains. Type field, set to 3 and code indicates the result of registration request.

Tunneling and Encapsulation
A tunnel creates a virtual pipe for data packets between a tunnel entry and a tunnel endpoint.

- Encapsulation : This is the mechanism of taking a packet consisting of packet header and data and putting it into the data part of a new packet.

- Decapsulation : It is the reverse operation of taking a packet out of the data part of another packet.



IP encapsulation

The both procedures stated above are performed. When a packet is transferred from a higher protocol layer respectively. The above figure show that the HA enters in tunnel and takes the original packet with the MN as destination, puts it into the data part of a

new packet and sets the new IP. Header in such a way that packet is routed to the COA. Now the new header is called the outer header. There is one more an inner header which is identical to original header and can be computed during encapsulation :

IP IN IP ENCAPSULATION

This mechanism is specified in RFC 2003.

Ver	IHL	DS(TOS)	length	
IP identification			flags	Fragment offset
TTL	Ip in IP		IP checksum	
IP address of HA				
Care–of–address of COA				
Ver	IHL	DS(TOS)	length	
IP identification			flags	Fragment offset
TTL	Lay 4 prot		IP checksum	
IP address of CN				
IP address of MN				
RCP/UDP/__ _ _ _ payload				

IP in IP encapsulation

The above figure shows a packet inside the tunnel. The fields follow the standard specification given in RFC 791.

- Ver : This is the version filed 4 for IP version 4.
- IHL : This is the internet header length denotes the length of outer header in 32 bit words.
- DS(TOS) → This is copied from inner header,
- Length – This is covers the complete encapsulated packet.
- IP in IP → This is the type of protocol used in IP payload.
- IP checksum → This is calculated as usual.

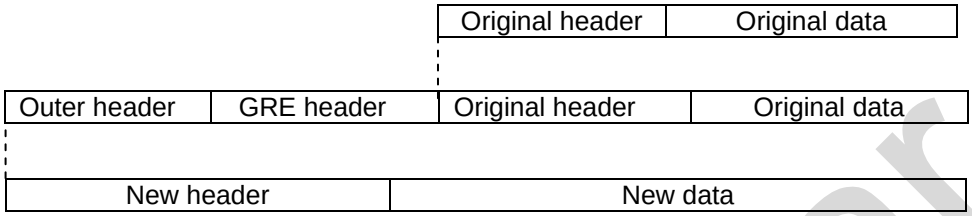
The header remains unchanged during encapsulation thus it shows the original sender CN and the receiver MN of packet. The only change is TTL, which is decremented by 1. By this it means that the whole tunnel is considered a single hop from the original packet's point of view. This feature is very important because it allows the MN to behave as if it attached to the home work..

- **Minimal Encapsulation**
  This is an optional encapsulation method for mobile IP. Here the header contains value 55% of the minimal encapsulation protocol.
  If S bit is set, the original sender address of CN is included. In inner header no field for fragmentation offset is left.

- **Generic Routing Encapsulation**

This mechanism allows the encapsulation of packets of one protocol suit into the payload portion of a packet of another protocol suit. This forms the new data part of the new packet and the header of the second protocol suit is put in front.

The below figure is of Generic routing encapsulation which shows the leftside is of fields of a packet inside the channel between home agent and COA using GRE as an encapsulation scheme specified to RFC 1701. The outer header shown is the standard. IP header with HA as source address and COA as destination address.



Generic routing encapsulation

The GRE headers starts with several flags indicating if certain fields are present or not. The protocol fields for GRE according to RFC 1701 are as follows along with their functionality.

C bit → indicates presentence of checksum field.

R bit → indicates offset and routing fields are present or not.

Offset → represents offset in bytes for first source routing.

Key → This field is used for authentication depending on this bit K bit is set or reset.

S → Sequence number's presence is indicated by this field.

Ver	IHL			DS (TOS)			length	
IP identification							flags	Fragment offset
TTL				GRE			IP checksum	
IP address of HA								
Care – of – address of COA								
C	R	K	S	S	rec	rsv	ver	Protocol
Checksum (optional)							Offset (optional)	
Key (optional)								
Sequence number (optional)								
Routing (optional)								
ver	IHL			DS (TOS)			length	
IP identification							flags	Fragment offset
TTL				Lay 4 prot			IP checksum	
IP address of CN								
IP address of MN								
TCP/UDP_ _ _payload								

Protocol fields for GRE according to RFC 1701

OPTIMIZATION

To optimize the route it is necessary to inform the CN of the current location of MN. The most suitable entry to inform the CN of the location is the HA. The optimized mobile IP protocol needs four additional messages

1) Binding request : Nodes which want to know the current location of an MN can send binary request to HA. If HA is allowed to reveal the location, it sends back a binary update.
2) Binding update : This message contains the fixed IP address of the MN and the COA, which is sent by HA to CN.
3) Binding acknowledgement : When ever a node is requested, it returns this acknowledgement after receiving a binary update massage.
4) Binding warning : If a node decapsulates a packet for an MN, which is not current FA for this MN, this node sends a binding warning. A binding warning contains MN's home address and a target node address.

REVERSE TUNNELING

Reverse tunneling arise with severe problems associated with it.

1) **Firewall :** All data in organization must to and from pass through the firewall. Firewalls are set to filter out malicious addresses from administrator's view. Firewalls are simple protection against misconfigured system. This also implies that an MN can not send a packet to a computer residing in its home network. Afterwards complications arise through the use of private address inside the intranet and translation into global address when communicating with the internet. Network address translation (NAT) is used by many companies to hide internal resources.

2) **Multi–cast :** Multicast group requires MN to participate in it. MN requires reverse tunnels. Nodes in home network participate in a multicast group but MN in foreign network can not transmit multi–cast packets.

3) **TTL :** If MN moves to foreign network, TTL might be too low, for the packets to reach the same nodes as before. Mobile IP is not transparent if a user has to adjust the TTL while moving. Reverse tunneling arise with several security issues. For example : Tunnels starting in the private network of a company and reaching out into the internet could be hijacked and abused for sending packets through firewall.

IPv6

IP version 6.

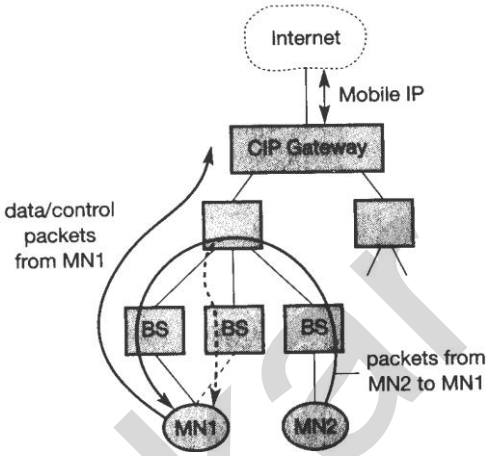
Each IPv6 node masters address autoconfiguration. Autoconfiguration means the mechanism for acquiring a COA that are already built in. Neighbor discovery is a mandatory mechanism for everynode. The combinations of above two mechanisms make enable the mobile node to create or obtain a topologically correct address for the current point of attachment.

Each IPv6 node can send binding updates to another node so the MN can send its current COA directly to the CN and HA. Now the MN sends new COA to the old router. Servicing the MN at the old COA, and the old router encapsulates all incoming packets for the MN and forwards them to new COA.

Altogether mobile IP in IPV6 networks requires very few additional mechanisms of a CN, MN and HA. Here CN should be able to process binding updates. The MN should be able to decapsulate packets to detect when it needs a new COA, and to determine when to send binary updates to the HA and CN. A HA have to be able to encapsulate packets.

- **Cellular IP :** All nodes collect routing information for accessing based on the origin of packets sent by the MNs towards the C1PGW & mobile node moving between adjacent cells will temporarily be able to receive packet via both old and new base stations (BS). If supported by lower protocol layer.

- Advantages :
  i) Manageability : Cellular IP is self configuring. CIPGW facilitate administration of mobility – related functionality.



Basic architecture of cellular IP

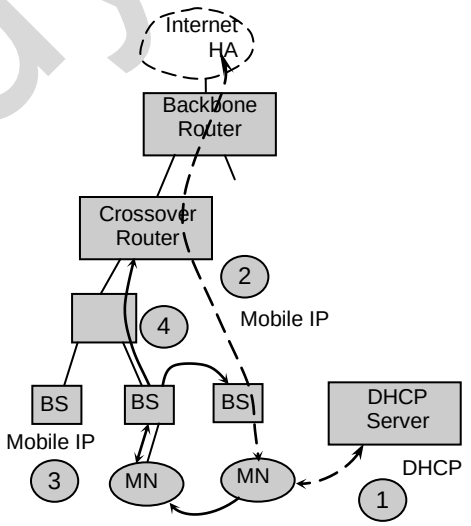
- Disadvantages :
  1) Efficiency : Additional network load is increased by forwarding packets on multiple paths.
  2) Transparency : Changes to MNs are required.
  3) Security : Routing tables are changed based on messages sent by mobile nodes.

HAWAII (Handoff – Aware wireless Access Internet infrastructure)

HAWAII tries to keep micro – mobility support as transparent as possible for home agent and mobe nodes. The core goal of HAWAII are performance and reliability improvements and support for quality of service mechanisms.

Following are the steps in HAWAII domain,

1) A mobile node obtains a co-located COA.
2) Registration of a mobile node with HA.
3) MN sends a registration request to the new base station as to a foreign agent.
4) Base station intercepts the registration request and sends out a handoff update message.



Basic architecture of HAWAII

- Advantages :
  i) Security : Extensions to challenge response has improved security features.

  ii) Transparency : It is the most transparent to mobile nodes.

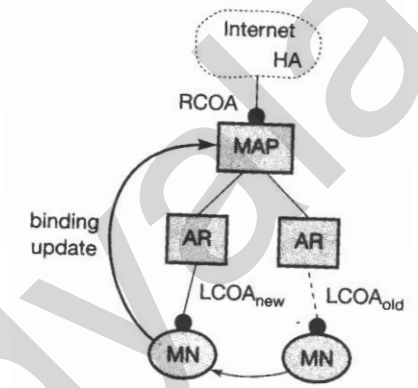
- Disadvantages :
  i) Security : No provisions regarding the setup of IPSEC tunnels.

  ii) Implementations : Private address supports are not possible due to co-located COAs.

Hierarchical mobile IPv6 (HMIPV6)

This provides micro–mobility support by installing a mobility anchor point (MAP), acts as a local HA within this domain for visiting MNs. MAP receives all packets on behalf of the MN, it encapsulates, and forward them directly to the MN's current address (LCOA).

MAP domains boundaries are defined by the access routers (AR). Whenever a MN moves locally it must register its new LCOA with its MAP. The period for which MN stays within the domain of a MAP, the globally visible COA (regional RCOA) does not change. MAP assists with local handovers and maps RCOA to LCOA.



Basic architecture of HMIPVG

- Advantages :
  1) Security : MNs have limited location privacy because LCOA can be hidden.
  2) Efficiency : Same link can be shared by CN while direct routing.

- Disadvantages :
  1) Transparency : Additional infrastructure components are required.
  2) Security : Since routing tables are changed based on messages sent by mobile nodes, hence it requires strong authentication and protection against denial of service attacks.

S_1 chooses the lowest cost path (S_1, N_1, N_2, R_1) due to low interference. Same way S_2 also calculate cost of path. The metrics can be

h $\rightarrow$ number of hops
i $\rightarrow$ interference
r $\rightarrow$ reliability
e $\rightarrow$ error rate.

Cost of path can be determined by
Cost = $\alpha h + \beta i + \gamma r + \delta e + ...$

$(\alpha, \beta, \gamma, \delta; ....\text{are weights choosen})$.

TRADITIONAL TCP

Several mechanisms of transmission control protocol (TCP) are as follows :
(i) Congestion control
(ii) Slow start
(iii) Fast retransmit / fast recovery
(iv) Implications on mobility

(i) Congestion Control : During transmission some times packets to be forwarded are dropped because of the asymmetry link of sender and receiver's output link. The packet which is dropped is a lost of transmission. When the sender comes to know that the receivers has sent acknowledgement of all packets except the dropped packet, he realizes that the packet is missed in transmission, due to congestion. To mitigate congestion, TCP slows down the transmission rate dramatically and all other TCP connections facing the same congestion problem do the same and congestion is resolved. This co–operation of TCP is the main reason of the survival of internet. VDP is not desirable and preferable, since throughput is more in it.

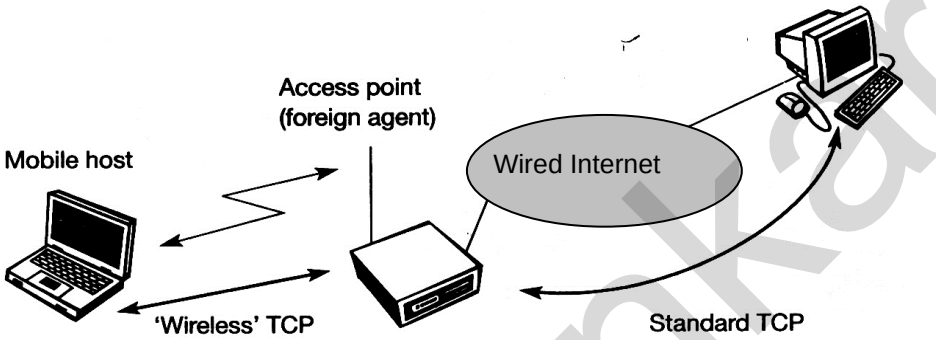
(ii) Slow Start : Slow start is a very next step taken by TCP after detection of congestion. The sender always calculate and send the congestion window for receiver which is one segment size at first. The sender waits for acknowledgement if it arrives, sender increase the congestion window by one. After getting two acknowledgements it sends 2 more congestion window. Each time window takes round trip time (R. T. T), is called exponential growth of congestion window. Linear increment in window size continues till it reach to congestion threshold.

(iii) Fast Retransmit / Fast Recovery : The receiving acknowledgement from a receiver shows that receiver is continuously receiving sent by sender. The gap in packet stream is due to transmission error and not congestion problem. The sender now retransmit the missing packet before timer expires. This is called as fast retransmit. The sender gives receipt of acknowledgement indicating no congestion to slow start. The sender continues with the current congestion window and perform fast recovery from pack loss.

(iv) Implications of mobility : Mobility can cause packet loss. Soft handover from one access point to another is not possible for mobile end system. Error rates on wireless links are orders of magnitude higher compared to fixed fibre or copper links. For example when using mobile IP, there could be some packets in transit to the old

foreign agent while the mobile node moves to the new foreign agent. Old foreign agent may not be able to forward those packets to new foreign agent. TCP mechanism detecting missing acknowledgement via time–out and conducting packet loss due to congestion can not distinguish. This is fundamental design problem in TCP. Still it is hard to completely change TCP to support mobile users.

INDIRECT TCP



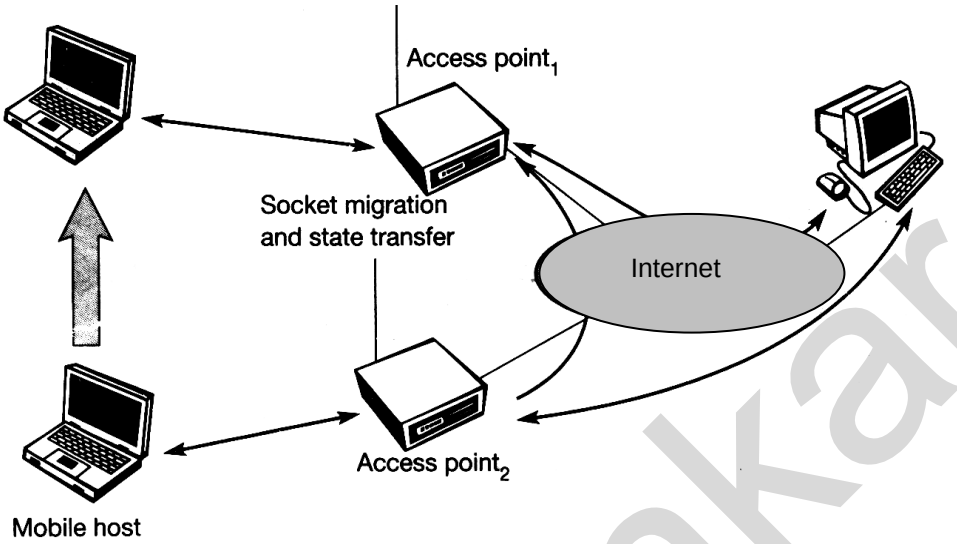
Indirect TCP segments

Two main reasons arise to for the development of indirect TCP (I – TCP)
1. TCP performs poorly with wireless links.
2. TCP within fixed network can not be changed.

In the above figure a mobile host is connected via a wireless link and an access point to wired internet where correspondent host resides which could also use wireless access. A standard TCP is used between the fixed computer and access point. The mobile host, access point terminates the standard TCP connection and act as proxy. A preferable place for segmenting the connection between mobile host and correspondent host is at the foreign agent of mobile IP. This foreign agent controls the mobility of the mobile host and also handover connection to next foreign agent when the mobile host moves ahead. The foreign agent acts as a proxy and relays all data in both directions. Foreign agent acknowledges the packet sent by correspondent host and forwards it to mobile host. Mobile host acknowledges packet as soon as it receives. Foreign agent uses this acknowledgement if in case a packet is lost in transmission. The same procedure is repeated in reverse mobile host sends packet and foreign agent acknowledges it.
After handover, I–TCP performs some actions.

The main function comprised directing the packets using mobile IP.

As shown in example above, the access point acts as a proxy buffering packets for retransmission. After registration, the new foreign agent can inform the old one about its location to enable packet forwarding. There is no need of new connection establishment for mobile host and the correspondent host must not see any changes in connection state.



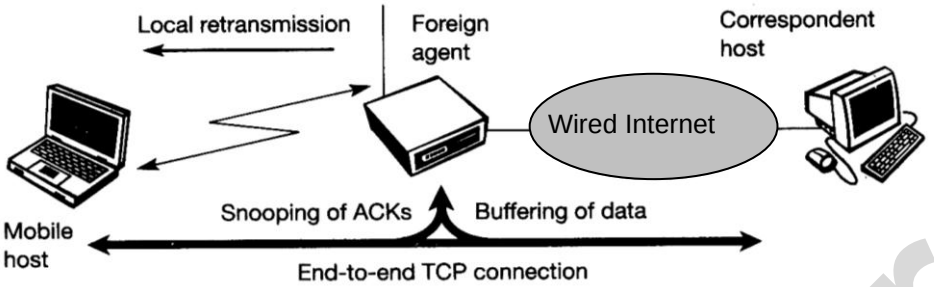
Socket and state migration after handover of a mobile host

- Advantages with I – TCP :
  1. I – TCP does not require any change in TCP protocol.
  2. Transmission errors are eliminated by making strict partitioning in two connections.
  3. Whenever new mechanism is used to improve TCP performance, by optimizing these new mechanism it is made simple because they cover only one hop.
  4. In I-TCP optimized TCP could use precise time–outs to guarantee retransmission more faster.
  5. Different transport layer protocol can be used between mobile host and foreign agent.

- Disadvantages in I – TCP :
  1. Loss of end to end semantics of TCP cause problems if the foreign agent partitioning the TCP connection crashes which may result into crashing application running on correspondent node.
  2. Increased handover latency is problematic since foreign agent not necessarily forwards packets sent by correspondent host to mobile host.
  3. The foreign agent is required to be trusted entity because TCP connection end at this point.

Snooping TCP

The drawback of I–TCP is the segmentation of single TCP connection into two TCP connections. Due to this the original end to end TCP semantic is lost. One improvement for TCP might be enhancement of foreign agent in the Mobile IP.



Snooping TCP as a transparent TCP extension

Foreign agent buffers all packet with destination mobile host and snoops the packet flow in both direction. Buffering packets toward mobile node is to enable the foreign agent to perform a local retransmission in case of packet loss on the wireless link. The foreign agent must not acknowledge data to maintain transparency to the correspondent host. Foreign agent can filter the duplicate acknowledgements to avoid unnecessary traffic on wireless link.

The foreign agent sends a negative acknowledgement to mobile host as soon as it detects the negative acknowledgement. Mobile host retransmit the missing packet and then packets are reordered at correspondent host by TCP. This is the data transfer from mobile host with destination correspondent host.

- Advantages of snooping TCP :
  1. Since end to end TCP semantic is preserved, the crashing timing of foreign agent is not bauthered.
  2. No changes in correspondent host and mobile host are needed.
  3. When mobile host moves to another foreign agent, there is no need of handover state.
  4. If the foreign agent does not use enhancement, the approach automatically falls back to the standard solution, this is the situation. The above situation was the problem in I–TCP which has been overcome here in “Snooping TCP”.

- Disadvantages in Snooping TCP :
  1. Snooping TCP do not isolate the behavior of wireless link. The quality of isolation strongly depends on the quality of wireless link which may be problematic if wireless links exhibits very high delay as compared to wired links.
  2. Negative acknowledgement between the foreign agent and mobile host needs additional mechanisms on mobile host to maintain transparency.
  3. If encryption is applied, snooping and buffering data may be useless.

MOBILE TCP (M–TCP)

M – TCP aims at preventing the sender window from shrinking if bit errors or disconnection occurs. M–TCP tries to improve overall performance, throughput, to lower delay and maintain end to end semantics of TCP and provide more efficient handover. M – TCP splits the TCP connection in two parts.

1. An unmodified TCP used on the standard host – supervisory host (SH) connection.
2. Optimized TCP used on the SH – MH connection.

SH is responsible for exchanging data between both parts similar to the proxy in I–TCP. The M–TCP, assumes a low bit error rate on wireless link. Hence it does not need to perform caching or retransmit via SH. Whenever a packet is lost on wireless link it has to be transmitted by original sender which results in maintaining the TCP end to end semantics. If SH does not receive an acknowledgement, it chokes the sender by assuming that the MH is disconnected and sets the senders window size to 0. This mean the sender go into persistent mode which means that sender won't retransmit data. When SH detects connectivity again, it reopens the window of the sender to the old value. M–TCP needs a bandwidth manager to implement fair sharing over the wireless link changes to the sender's TCP is not required.

- Advantages of M–TCP :
  1. It maintains the TCP end–to–end semantics
  2. In case of MH gets disconnected, it avoids useless retransmissions, slow starts by shrinking the sender's window too.
  3. Lost packets are automatically retransmitted to the new SH.
- Disadvantages :
  1. Packet loss on wireless link due to errors is propagated to the sender because SH does not act as proxy.
  2. M – TCP always assumes low bit error rates, which are not always valid assumption.
  3. Modification to MH protocol software and new network elements are required for bandwidth manager.

FAST RETRANSMIT / FAST RECOVERY

In fast recovery/fast transmit a host can use after receiving duplicate acknowledgements, hence concludes packet loss without congestion.

In this mechanism as soon as the mobile host registers at a new foreign agent using mobile IP, it starts three duplicates. The proposal in this mechanism is to send three duplicates, which forces the corresponding host to go into fast retransmit mode and not to start slow start. The mobile host may also go into slow start after moving to a new foreign agent.

- Advantages of fast retransmit / fast recovery :
  1. It is simple.
  2. Minor changes in the mobile host's software already result in a performance increase and no foreign agent or correspondent host has to be changed.
- Disadvantages :
  1. There is insufficient isolation of packet losses.
  2. Losses due to handover.
  3. Though efficiency is increased due to fast retransmission, retransmission packets have to cross the whole network.

TRANSMISSION / TIME–OUT FREEZING

MAC layer has already noticed connection problems from the TCP point of view. MAC layer informs the TCP layer of an upcoming loss of connection or that the current interruption is not caused by congestion. The TCP stop sending and freezes the current state of its congestion window and further timers. If MAC layer notices the upcoming interruption. Early, both the mobile and correspondent host can be informed. Additional mechanisms are needed to inform correspondent host of the reason for interruption.

MAC layer signals TCP that it can resume operation at the same point form where it is stopped, as it detects connectivity.

- Advantages :
  1. It offers a way to resume TCP connection even after longer interruption.
  2. It is independent of any other TCP mechanism.
- Disadvantages :
  1. Correspondent host are needed to be changed
  2. All mechanisms are dependent on MAC layer capability.
  3. Freezing state of TCP do not help in case of encryption schemes.

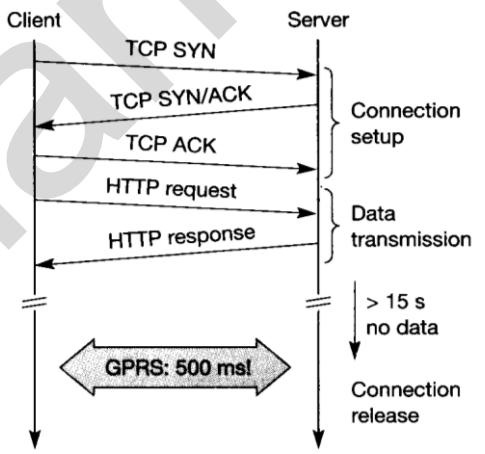
SELECTIVE TRANSMISSION

This is an extension of TCP which is useful. TCP acknowledgements are cumulative. This means they acknowledge in–order receipt of packets upto a certain packet. TCP indirectly request selected retransmission of packets. The receiver acknowledges single packets and sender retransmits the needed packet.

TRANSACTION ORIENTED TCP

Using TCP requires several packets over the wireless link. First TCP uses a three–way handshake to establish the connection. One additional packet is needed for transmission of request and requires three more packets to close the connection via a three–way handshake.

But in an example show above is of one data packet, whereas TCP may need seven packets. The above example shows overhead, introduced by using TCP over GPRs web scenario. In an internet TCP is used for this purpose, before a HTTP request can be transmitted the TCP connection has to be established. T / TCP can combine packets for connection establishment and connection release with user data packets. This reduces the number of packets down.



Example TCP connection setup overhead

- Advantage :
  The reduction in the overhead.

- Disadvantage :
  Requires changes in the mobile host and correspondent hosts.

❑ ❑ ❑ ❑ ❑