

**LECTURE NOTES
ON
MOBILE COMPUTING (5TH SEM,CSE)**

**PREPARED BY
SUNITA MAHAPATRA
SR.LECT. IN DEPT.OF CSE (PKAIET, BGH)**

CONTENTS :

1. Introduction to Wireless networks & Mobile Computing

- Networks
- Wireless Networks
- Mobile Computing
- Mobile Computing Characteristics
- Application of Mobile Computing

2. Introduction to Mobile Development Framework

- C/S architecture
- n- tier architecture
- n- tier architecture and www
- Peer-to Peer architecture
- Mobile agent architecture

3. Wireless Transmission

- Introduction
- Signals
- Period
- Frequency and Bandwidth.
- Antennas
- Signal Propagation
- Multiplexing
- Modulation
- Spread Spectrum
- Cellular System

4. Medium Access Control

- Introduction
- Hidden/ Exposed Terminals
- The basic Access Method
- Near / Far Terminals
- SDMA, FDMA, TDMA, CDMA

5. Wireless LANs

- Wireless LAN and communication
- Infrared
- Radio Frequency
- IR Advantages and Disadvantages
- RF Advantages and Disadvantages
- Wireless Network Architecture Logical

- Types of WLAN
- IEEE 802.11
- MAC layer
- Security
- Synchronization
- Power Management
- Roaming
- Bluetooth Overview

6. Ubiquitous Wireless Communication

- Introduction
- Scenario of Mobile Communication
- Mobile Communication Generations 1G to 3G
- 3rd Generation Mobile Communication Network
- Universal Mobile telecommunication System (UMTS)

7. Mobile IP

- Mobile IP entities
- IP address
- Ipv4
- IPv6
- Mobile IP architecture

8. Wireless Telecomm Networks

- GSM
- System architecture
- Handover
- GPRS
- UMTS
- UTRAN
- IS-95,CDMA-2000

Introduction:

A communication device can exhibit one of the following characteristics:

- * fixed and wired: This configuration describes the typical desktop computer in an office.
- * Mobile and wired: Many of today's laptop fall into this category, where carrying the laptop from one location to the other, reconnecting to the company's network via the telephone network and a modem.
- * fixed and wireless: This mode is used for installing networks e.g. in residential buildings to avoid damage by installing wires.
- * Mobile and wireless: Here no cable restricts the user, who can roam between different wireless networks. Today most successful example of this category is GSM with more than several hundreds of millions of users.

Applications: Although many applications can benefit from wireless networks and mobile communications, particular application environments seem to be predestined for their use.

Vehicles Today's car already comprise some, but tomorrow's car will comprise many wireless communication systems and mobility aware applications. News, news, road conditions, weather reports and other broadcast information are received via digital audio broadcasting.

- For personal communication, a universal mobile telecommunications system (UMTS) phone might be available offering voice and data connectivity.
- For remote areas, satellite communications might be used.

Emergencies: wireless networks are the only means of communication in the case of natural disasters such as hurricanes or earthquakes.

- In the worst cases, only decentralized, wireless ad-hoc networks survive. The breakdown of all cabling not only implies the failure of the standard wired telephone system, but also the crash of all mobile phone systems requiring base stations.

→ An ambulance can also be equipped with high-quality wireless connections to a hospital. vital information about the injured persons can be sent to the hospital from the scene of the accident.

Business: A travelling salesman today needs instant access to the company's database; to ensure that the files on his or her laptop reflect the current situation, to enable the company to keep track of all activities of their travelling employees, to keep databases consistent.

→ with the wireless access, the laptop can be turned into a true mobile office but efficient and powerful synchronization mechanisms are needed to ensure the data consistency.

→ Leaving home requires a handover to another technology e.g. to an enhanced version of GSM, as soon as the WLAN coverage ends.

Replacement of wired networks: In some cases, wireless networks can also be used to replace wired networks, e.g. remote sensors, for telephones, or in office buildings.
→ 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.

Entertainment and more: wireless networks can provide up-to-date information at any appropriate location.
→ we may choose a seat, pay via electronic cash, and send this information to a service provider.
→ Another growing field of wireless network applications lies in entertainment and games to enable, e.g. ad-hoc gaming networks as soon as people meet to play together.

Location dependent Services: In many cases, however, it is important for an application to 'know' something about the location or the user might need location information for further activities.

Follow-on services: The function of forwarding calls to the current user location is well known from the good old telephone system. Whenever you are, just transmit your temporary phone number to your phone and it redirects incoming calls.

Location aware services: Imagine we wanted to print a document sitting in the lobby of a hotel using your laptop. If you drop the document over the printer icon, where would you expect the document to be printed? certainly not by the printer in your office! However without additional information about the capabilities of your environment, this might be the only thing you can do. For instance, there could be a service

in the hotel announcing that a standard laser printer is available in the lobby or a color printer in a hotel meeting room, etc. your computer might then transmit your personal profile to your hotel which then changes you with the printing costs.

Information services: while walking around in a city you could always use your wireless travel guide to pull information from a service.

Mobile and wireless devices: even though many mobile and wireless devices are available, there will be many more in the future. There is no precise classification of such devices by size, shape, weight or computing power. Currently, laptops are considered the upper end of the mobile device range. However, there is no sharp line between the categories and companies tend to invent more and more new categories.

* beeper: A very simple wireless device is represented by a sensor transmitting state information.

Embedded controllers: many appliances already contain a simple or sometimes more complex controllers. keyboards, mice, headsets, washing machines, coffee machines, hair dryers are just some examples.

Pager: As a very simple receiver, a pager can only display short text messages, has a tiny display, and cannot send any messages. However, nowadays mobile phones have replaced the use of pagers.

Mobile phones: Today mobile phones migrate more and more toward PDAs. Mobile phones with full color graphic displays, touch screen and internet browsers are easily available.

personal digital assistant: PDAs typically accompany a user and offer simple versions of office software (calender, note-pad, mail). web browsers and many other software packages are available for these devices.

pocket computer: The next step toward full computers are pocket computers offering tiny keyboards, color displays and simple versions of programs found on desktop computers.

Notebook / laptop: Finally, laptops offer more or less the same performance as standard desktop computers, they use the same b/w the only difference being size, weight and the ability to run on a battery. If operated mainly via a resistive display (touch sensitive or electromagnetic), the devices are also known as notepads or tablet pc's.

Chapter 2 Wired transmission

Frequencies for radio transmission

→ Radio transmission can take place using many different frequency bands. Each frequency band exhibits certain advantages and disadvantages.

$$\lambda = c/f \text{ where } \lambda = \text{'wave length'}$$

$$c = 3 \cdot 10^8 \text{ m/s speed of light}$$

in vacuum

$$f = \text{frequency}.$$

→ For traditional wired networks frequency upto several hundred KHz are used for distances upto some km with twisted pair copper wires, while frequencies of several MHz are used with coaxial cable. Fibre optics are used for frequency ranges of several hundred THz but here one typically refers to the wavelength which is e.g. 1500 nm, 1350 nm etc. (infra red).

→ Radio transmission starts at several KHz, the very low frequency (VLF) range. These are very long waves and waves in low frequency are used by submarines, some radio stations also use this frequency.

→ The medium frequency (MF) and high frequency (HF) ranges are typically used for transmission of hundreds of radio stations. (520 KHz and 1605.5 KHz)

→ As we move to very high frequency (VHF) 174 - 230 MHz and ultra high frequency (UHF) 470 - 790 MHz that is used in TV stations.

→ Super high frequencies (SHF) are typically used for directed microwave links and fixed satellite services. (11 - 19 GHz)

→ Extremely high frequency (EHF) range which is closer to infra red and these are used for directed links. For example to connect different building via laser link. The most wide spread infrared technology, infrared data association (IrDA), uses wavelength of approximately 850 - 900 nm to connect laptops, PDAs.

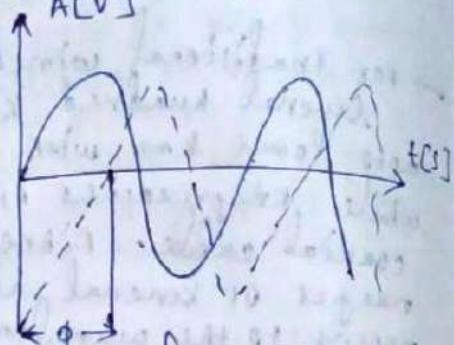
signals: Signals are the physical representation of data. users of a communication system can only exchange data through the transmission of signals.

→ Layer 1 of the ISO/OSI basic reference model is responsible for the conversion of data; i.e. bits into signals and vice-versa. Signals are the function of time and location.

- The most interesting types of signals for radio transmission are periodic signals, especially sine waves as carriers. The general function of a sine wave is:

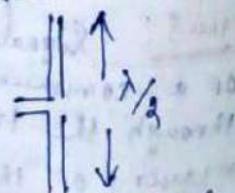
$$g(t) = A \sin(2\pi f_1 t + \Phi)$$

- Signals parameters are the amplitude A , frequency f and the phase shift Φ . The amplitude as a factor of the function g may also change over time. The frequency f expresses the periodicity of the signal with the period $T = 1/f$ it can also be changed with time Δt .



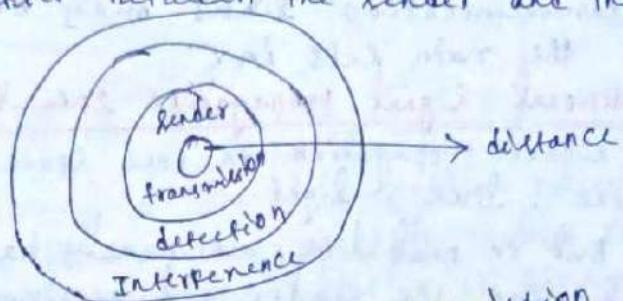
Antennas: wireless communication mode involves "getting rid" of wires and transmitting signals through space without guidance. We do not need any medium for the transmission of electromagnetic waves.

- Somehow, we have to couple the energy from the transmitter to the outside world and in reverse, from the outside world to the receiver. This is what exactly the antennas do.
- 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 at its center.
- The radiation pattern is symmetric in all directions. However such an antenna does not exist in reality. Real antennas all exhibit directive effects i.e. the intensity of radiation is not the same in all directions from the antenna.
- The simplest real antenna is thin, centre-fed dipole, also called hertzian dipole. The dipole consists of two collinear conductors of equal length, separated by a small feeding gap.
- The $\lambda/2$ dipole antenna is also called marconi antenna, it has a uniform or omni-directional radiation pattern. This type of antenna can only overcome environmental challenges by boosting the power level of the signal. Challenges could be mountains, valleys etc.



Signal Propagation :

- Like wired networks, wireless communication networks also have senders and receivers of signals. In wireless networks, the signal has no wire to determine the direction of propagation, whereas the signals in a wired network travels along the wire (which can be twisted pair copper wires, coaxial, fibre optic etc.).
- For wireless transmission, the signal propagation ~~behaves~~ predictable behaviour is only valid in a vacuum, i.e. without matter between the sender and the receiver.



(Ranges for transmission, detection and interference of signals)

- Transmission range: within a certain radius of the sender transmission is possible i.e. a receiver receives the signals with an error rate low enough to be able to communicate and can also act as a sender.
- detection range: within a second radius, detection of transmission is possible i.e. the transmission power is large enough to differ from background noise. However, the error rate is too high to establish communication.
- Interference range: within a third even larger radius the sender may interfere with other transmission by adding to the background noise. A receiver can't detect the signal but the signals may disturb other signals.

Path loss of radio signals: in free space radio signals propagate as light does (independently of their frequency) i.e. they follow a straight line. If such a straight line exists between a sender and receiver it is called line-of-sight (LOS).

- Even if no matter exists between sender and receiver, the signal still experiences the free space loss. The received power P_r is proportional to $\frac{1}{d^2}$ where d is the distance between the sender and receiver.
- The received power also depends on the wavelength and the gain of receiver and transmitter antennas. If there is any matter between the ^{sender} transmitter and receiver, the situation becomes complex.

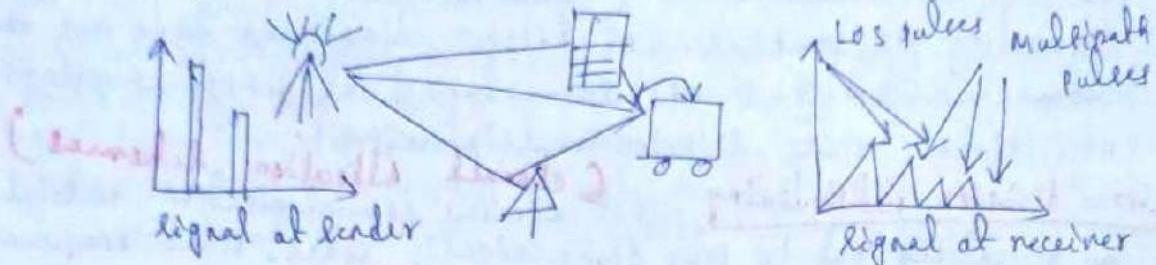
→ Most radio transmission takes place through the atmosphere. Signals travel through air, rain, snow, fog, dust particles, smog etc. While the path loss or attenuation does not cause too much trouble for short distances, e.g. for long distances heavily influences transmission over long distances, e.g. satellite transmission. Every mobile phone transmission is affected by weather conditions such as heavy rains. Rain can absorb much of the radiated energy of the antenna, so communication links may break down as soon as the rain lets in.

Additional signal propagation effects:

- Signal propagation in free space almost follows a straight line, like light.
- But in real life, we rarely have a line-of-sight between the sender and receiver of radio signals due to attenuation caused by the distance between sender and receiver, which are again very much frequency dependent.
- An extreme form of attenuation is blocking or shadowing of radio signals due to large obstacles.
- The higher the frequency of a signal, the more it behaves like light. Even small obstacles like a simple wall, a tree on the street or tree in an alley may block the signal.
- If an object is large compared to the wavelength of the signal, e.g. huge buildings, mountains, or the surface of the earth, the signal is reflected. The reflected signal is not as strong as the original, as objects can absorb some of the signal's power. Reflection helps transmitting signals as soon as no LOS exists. Signals transmitted from a sender may bounce off the walls of buildings several times before they reach the receiver. The more often the signal is reflected, the weaker it becomes.
- The third effect is due to refraction, this occurs because the velocity of the electromagnetic waves depends on the density of the medium through which it travels.
- Only in vacuum does it equal c. As waves that travel into a denser medium are bent towards the medium.
- This is the reason for LOS radio waves being bent towards the earth: the density of the atmosphere is higher closer to the ground.
- If the size of an obstacle is in the order of the wavelength or less, then waves can be scattered. An incoming signal is scattered into several weaker outgoing signals.

multi-path propagation :

- Together with the direct transmission from a sender to a receiver, the propagation effects lead to one of the most severe radio channel impairments, called multi-path propagation.
- Radio waves emitted by the sender can either travel along a straight line or they may be reflected at a large building or scattered at smaller obstacles.



- The above figure only shows three possible paths for the signal. In reality, many more paths with different lengths arrive at the receiver at different times.
- This effect caused by multi-path propagation is called delay spread: the original signal is spread due to different delays of parts of the signal.
- This delay spread is a typical effect of radio transmission because no wire guides the waves along a single path as in the case of wired networks. This effect has nothing to do with possible movements of the sender and receiver.
- Typical values for delay spread are approximately 3 μs in cities, up to 1μs can be observed. GSM, for example, can tolerate up to 16 μs of delay spread, i.e. almost a 5 Km path difference.
- Due to delay spread in real situation with hundreds of paths, this implies that a single impulse will result in many weaker impulses at the receiver. Each path has a different attenuation and the received pulses have different power, some of the received pulses are too weak that they can't be detected and act as noise.
- In the above figure the second impulse is separated from other at the sender side. At the receiver side both the impulses interfere i.e. they overlap in time. If each impulse represent a symbol or a bit then the energy intended for one symbol now spills over to the adjacent symbol, an effect that is called intersymbol interference (ISI). The higher the symbol rate to be transmitted, the worse the effects of ISI will be, as the original symbols are moved closer and closer to each other and it limits the bandwidth of a radio channel.

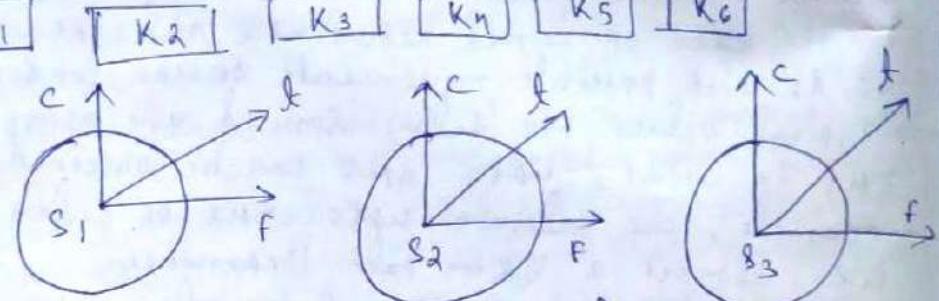
Multiplexing: multiplexing is not only a fundamental mechanism in communication systems but also in everyday life. Multiplexing describes how several users can share a medium with minimum or no interference.

→ one ex., the highways with several lanes. Many users use the same medium (highway) with hopefully no interference (accidents). This is possible due to the provision of several lanes (space division multiplexing) separating the traffic. In addition, different cars use the same medium (i.e. the same lane) at different points in time (time division multiplexing).

Space division multiplexing: For wireless communication, multiplexing can be carried out in four dimensions: space, time, frequency and code.

→ In this field, the task of multiplexing is to assign space, time, frequency and code to each communication channel with a minimum of interference and a maximum of medium utilization. The term communication channel here only refers to an association of sender and receiver who want to exchange data.

channels K_1 K_2 K_3 K_n K_5 K_6



→ In the above figure there are five channels and introduces a three dimensional co-ordinate system. This system shows the dimensions of code c , time t and frequency f .
→ For the SDM, the three dimensional space S_i is also shown. Here space is represented via circles indicating the interference range.

→ The channels K_1 to K_3 can be mapped onto the three spaces S_1 to S_3 which clearly separate the channels and prevent the interference ranges from overlapping. The space between the interference ranges is sometimes called guard space. Such a guard space is needed in all four multiplexing schemes presented.

→ For remaining channels (K_4 to K_6) three additional spaces would be needed. Although this procedure clearly represents a waste of space, this is exactly the principle used by the old analog telephone system! each subscriber is given a separate pair of copper

wired to the local exchange. In wireless transmission, FDM implies a separate channel for each communication channel with a wide enough distance between senders.

Frequency division multiplexing:

- FDM describes schemes to subdivide the frequency dimension into several non-overlapping frequency bands.
- Each channel K_i is now allotted its own frequency band as indicated. Senders using a certain frequency band can use this band continuously.
- Again guard spaces are needed to avoid frequency band overlapping. This scheme is used for radio stations within the same region, where each radio station has its own frequency. This very simple multiplexing scheme does not need complex coordination between sender and receiver. The receiver ~~has~~ only has to tune in to the specific sender.
- However, this scheme also has disadvantages. While radio stations broadcast 24 hours a day, mobile communication typically takes place for only a few minutes at a time. This results in tremendous waste of frequency resources.
- Additionally, the fixed assignment of a frequency to a sender makes the scheme very inflexible and limits the number of senders.

Time division multiplexing:

- A more flexible multiplexing scheme for typical mobile communications is time division multiplexing (TDM).
- Here a channel K_i is given the whole bandwidth for a certain amount of time, i.e. all senders use the same frequency but at different points in time.
- Again, guard spaces, which now represent time gaps, have to separate the different periods when the senders use the medium. In the highway example, this would refer to the gap between two cars.
- If two transmissions overlap in time, they are called co-channel interference (in the highway example, interference between two cars results in an accident).
- To avoid this type of interference, precise synchronization between different senders is necessary. This is clearly a disadvantage, as all senders need precise clocks or alternatively, a way has to be found to distribute a synchronization signal to all senders.
- The mobile phone standard GSM uses the combination of frequency and time division multiplexing for transmission between a mobile phone and a so-called base station.
- A disadvantage of this scheme is again the necessary coordination between different senders.

Code Division Multiplexing:

- CDMA is a relatively new scheme in commercial communication systems. First used in military applications due to its inherent security features, it now features in many civil wireless transmission scenarios thanks to the availability of cheap processing power.
- Here all channels use the same frequency at the same time for transmission. Separation is now achieved by assigning each channel its own code, guard spaces are realized by using codes with necessary distance in the code space e.g. orthogonal codes.
- The typical everyday example of CDMA is a party with many participants from different countries around the world who establish communication channels i.e. they talk to each other using the same frequency range at the same time.
- The main advantage of CDMA for wireless transmission is that it gives good protection against interference and tapping.
- Different codes have to be assigned but code spaces are huge compared to the frequency space.
- The main disadvantage of this scheme is the relatively high complexity of the receiver.

Modulation! $g(t) = A_t \cos(2\pi f_t t + \phi_t)$

This function has three parameters: amplitude A_t , frequency f_t and phase ϕ_t which may vary in accordance with data or another modulating signal.

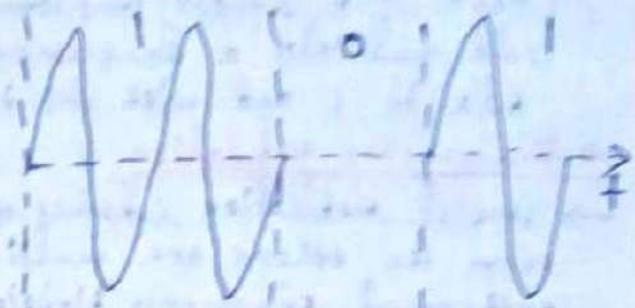
- For digital modulation, digital data (0 & 1) is translated into an analog signal (baseband signal).
- Digital modulation is required if digital data has to be transmitted over a medium that only allows for analog transmission.
- In wireless networks, however digital transmission can't be used. Hence the binary bit-stream has to be translated into an analog signal first.
- The three basic methods for this translation are amplitude shift keying (ASK), frequency shift keying (FSK) and phase shift keying (PSK).

Amplitude Shift Keying (ASK): It is the most simple digital modulation scheme. The two binary values 0 and 1, are represented by two different amplitudes.

- This simple scheme only requires low bandwidth, but is

very susceptible to interference - effects like multipath propagation, noise or path loss heavily influence the amplitude.

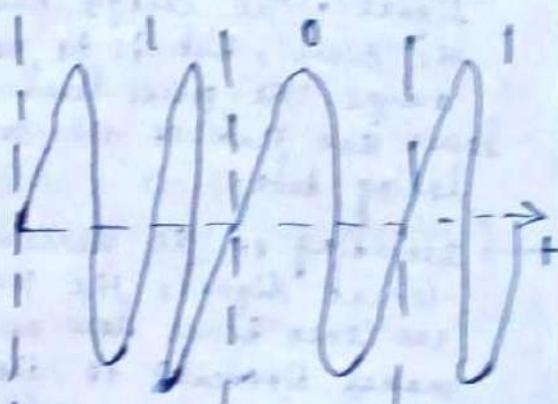
- In a wireless environment, a constant amplitude cannot be guaranteed, so ASK is basically not used for wireless radio transmission.



- However, the wired transmission scheme with the high bit performance, namely optical, transmission uses ASK. Here a light pulse represent a 1, while the absence of light represents a zero. ASK can also be applied to wireless infrared transmission.

Frequency Shift Keying (FSK): A modulation scheme often used for wireless transmission is frequency shift keying (FSK). It is also called binary FSK (BFSK); it assigns one frequency f_1 to the binary 1 and another frequency f_2 to the binary zero.

- A very simple scheme to implement FSK is to switch between two oscillators, one with frequency f_1 and the other with f_2 , depending upon the input.



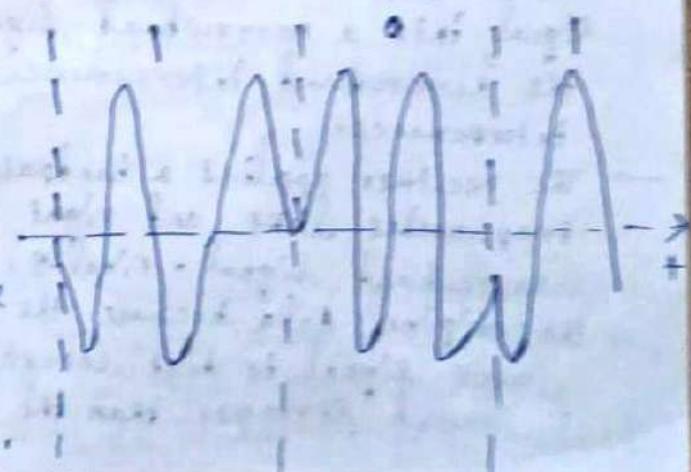
- A simple way to implement demodulation is by using two bandpass filters, one for f_1 and other for f_2 .

- FSK needs a larger bandwidth compared to ASK but is much less susceptible to errors.

Phase Shift Keying:

Finally, phase shift keying (PSK) uses shifts in the phase of a signal to represent data.

- Figure shows a phase shift of 180° or π at the 0 follows the 1 (the same happens as the 1 follows the 0).



→ This simple scheme, shifting the phase by 180° each time the value of data changes, is also called binary PSK (BPSK). A simple implementation of a BPSK modulator could multiply a frequency f with $+1$ if the binary data is 1 and with -1 if the binary data is 0.

Multi-carrier Modulation:

→ Several modulation schemes that stand somewhat apart from the others are multi-carrier modulation (MCM), orthogonal frequency division multiplexing (OFDM) or coded OFDM (COFDM) that are used in the context of the European digital radio system DAB and the WLAN standards IEEE 802.11a and HiperLAN2.

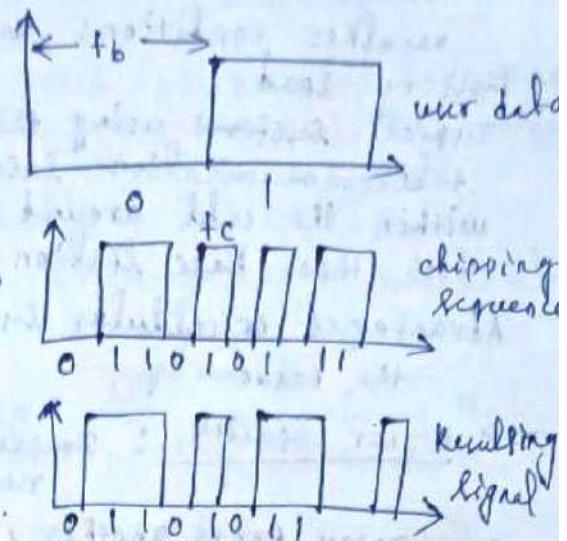
Spread Spectrum:

- As the name implies, spread spectrum techniques involve spreading the bandwidth needed to transmit data - which does not make sense at first sight.
- Spreading the bandwidth has several advantages. The main advantage is the resistance to narrowband interference.
- First the spreader ~~spreads~~ converts the narrowband signal into a broadband signal. The energy needed to transmit the signal is the same, but it is now spread over a larger frequency range. The power level of the spread signal can be much lower than that of the original narrowband signal without losing data.
- Depending on the generation and the reception of the spread signals, the power level of the user signal can even be as low as the background noise. This makes it difficult to distinguish between the background noise and the user signal and thus hard to detect.
- During transmission, narrowband and broadband interference add to the signal. The sum of interference and user signal is received. The receiver now knows how to de-spread the signal, converting the spread user signal into a narrowband signal again, while spreading the narrowband interference and leaving the broadband interference.
- The receiver applies a bandpass filter to cut off frequencies left and right of the narrowband of the narrowband signal. Finally, the ~~receiver~~ can reconstruct the original data because the power level of the user signal is high enough i.e. the signal is much stronger than the remaining interference.

① Direct Sequence Spread Spectrum:

Direct sequence spread spectrum (DSSS) systems take a user bit stream and perform an (XOR) with a so-called chipping sequence.

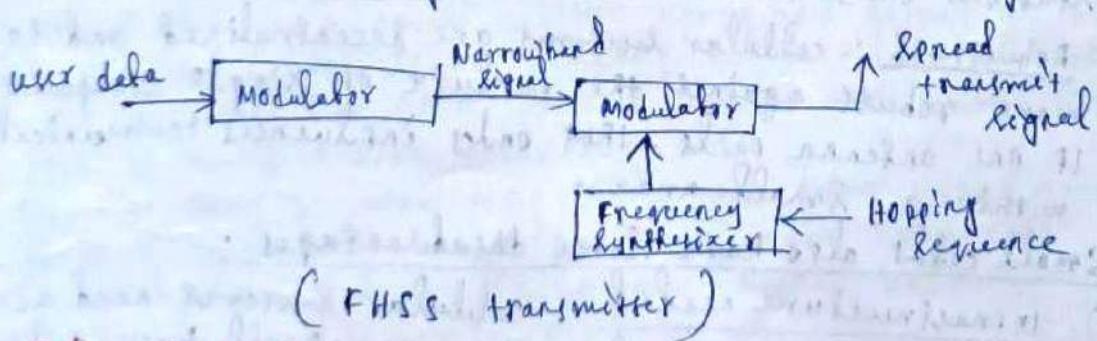
- While each user bit has a duration t_b , the chipping sequence consists of smaller pulses, called chips, with a duration t_c . If the chipping sequence is generated properly, it appears as random noise. This sequence is also sometimes called pseudo-noise sequence.



② Frequency hopping spread spectrum:

For frequency hopping spread spectrum (FHSS) systems, the total available bandwidth is split into many channels of smaller bandwidth plus guard spaces between the channels.

- Transmitter and receiver stay on one of these channels for a certain time and then hop to another channel.
- The system implements FDM and TDM. The pattern of channel usage is called the hopping sequence, the time spent on a channel with a certain frequency is called the dwell time. FHSS comes in two variants, slow and fast hopping.
- In slow hopping, the transmitter uses one frequency for several bit periods.
- For fast hopping, the transmitter changes the frequency several times during the transmission of a single bit.



Cellular systems:

- cellular systems for mobile communications implement SDM. Each transmitter typically called a base station, covers a certain area, a cell. cell radius can vary from tens of meters in buildings and hundreds

- of meters in cities, upto tens of kilometers in the country side.
 - The shapes of the cells are never perfect circles or hexagons, but depend on the environments, on weather conditions and sometimes even on user load.
 - Typical systems using this approach are mobile telecommunication systems, where a mobile station within the cell around a base station communicates with this base station and vice-versa.
- Advantages of cellular systems with small cells, are the following:
- Higher capacity: implementing SDM allows frequency reuse. If one transmitter is far away from another, i.e. outside the interference range, it can reuse the same frequencies. As most mobile phone systems allocate frequencies to certain users, this frequency is blocked for other users. But frequency is a scarce resource and the number of concurrent users per cell is very limited.

- (1) Less transmission power: while power aspects are not a big problem for base stations, they are indeed problematic for mobile stations. A receiver far away from a base station would need much more transmit power than the current new mobiles. But energy is a serious problem for mobile handheld devices.
- (2) Local Interference only: Having long distances between sender and receiver results in even more interference problems. With small cells mobile stations and base stations only have to deal with local interference.
- (3) Robustness: cellular systems are decentralized and so, more robust against the failure of single components. If one antenna fails, this only influences communication within a small area.

- Small cells also have some disadvantages:
- (1) Infrastructure needed: cellular systems need a complex infrastructure to connect all base stations. This include many antennas, switches for call forwarding, location registers to find a mobile station etc. which makes the whole system quite expensive.

② Handover needed: The mobile station has to perform a handover when changing from one cell to the another. Depending ~~upon~~ on the cell size and the speed of movement, this can happen quite often.

③ Frequency Planning: To avoid interference between transmitters using the same frequencies, frequencies have to be distributed carefully. On one hand, interference should be avoided, on the other hand, only a limited number of frequencies is available.

Medium Access Control (chapter 3)

→ Medium Access Control comprises all mechanisms that regulate user access to a medium using FDM, TDM, FDM or CDM.

→ MAC is thus similar to traffic regulations in the ~~in the~~ highway / multiplexing example.

→ MAC belongs to layer 2, the data link control layer (DLC) of the OSI / ISO reference model.

→ One example of MAC is CSMA / CD (carrier sense multiple access with collision detection) which works as follows. A sender senses the medium to see if it is free. If the medium is busy, the sender waits until it is free.

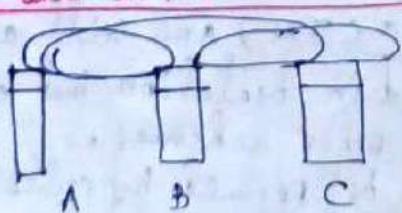
→ If the medium is free, the sender starts transmitting data and continues to listen into the medium. If the sender detects a collision while sending, it stops at once and sends a jamming signal.

→ But, this scheme fails in wireless networks because the strength of a signal decreases proportionally to the square of the distance to the sender.

→ The sender may apply carrier sense and detect an idle medium. The sender starts sending but a collision happens at the receiver due to a second sender. The same can happen to the collision detection.

→ So, this very common MAC schemes from wired network fails in a wireless scenario. Some more scenarios for which this scheme fails are listed below.

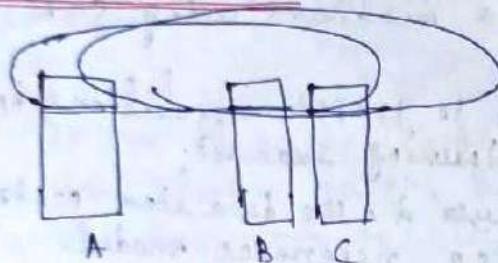
Hidden and exposed terminals:



Here the transmission range of mobile phone A reaches B, but not C (the detection range does not reach C either).

- The transmission range of C reaches B but not A. Finally the transmission range of B reaches A and C. I.e. A cannot detect C and vice-versa.
- A starts sending B, C does not receive this transmission. C also wants to send something to B and hence the medium. The medium appears to be free, the carrier sense fails. C also starts sending causing a collision at B. But A can't detect this collision at B and continues with its transmission. A is hidden for C and vice-versa.
- While hidden terminals may cause collision, the exposed terminals only causes unnecessary delay.

Near and far terminals:



- Here A and B are both sending with the same transmission power. As the signal strength decreases proportionally to the square of the distance, B's signal drowns out A's signal. As a result, C cannot receive A's transmission.
- The Near/Far effect is a severe problem of wireless networks using CSMA. All signals should arrive at the receiver with more or less the same strength.
- Otherwise, a person standing closer to somebody could always speak louder than a person further away. Even if the levels were separated by code, the closest one would simply drown out the others.

SDMA (Space Division Multiple Access):

- SDMA is used for allocating a separated space to users in wireless networks.
- A typical application involves assigning an optimal base station to a mobile phone user. The mobile phone may receive several base stations with different qualities.
- A MAC algorithm could now decide which base station to talk, taking into account which frequencies (FDMA), time slots (TDM) or code (CDMA) are still available.
- Typically, SDMA is never used in isolation but always in combination with one or more other schemes.
- The basis for SDMA algorithm is formed by cells and sectorized antennas.

FDMA (Frequency division multiple Access) :

- FDMA comprises all algorithms allocating frequencies to transmission channels according to the frequency division multiplexing (FDM).
- channels can be assigned to the same frequency at all times, i.e. pure FDMA or change frequencies according to a certain pattern, i.e., FDMA combined with TDMA.
- The latter example is the common practice for many wireless systems known as frequency hopping. Sender and receiver have to agree on a hopping pattern, otherwise the receiver could not tune into the right frequency.
- Hopping patterns are fixed at least for a longer period.
- furthermore, FDM is often used for simultaneous access to the medium by base station and mobile station in cellular networks. Here the two partners typically establish a duplex channel, i.e. a channel that allows for simultaneous transmission in both the directions.
- the two directions, mobile station to base station and vice-versa are now separated using different frequencies. This scheme is then called frequency division duplex (FDD).
- Again, both partners have to know the frequencies in advance, they cannot just listen into the medium. The two frequencies are also known as uplink, i.e., from mobile station to base station or from ground control to ~~to satellite~~ satellite, and as downlink, i.e., from base station to mobile station or from satellite to ground control.

TDMA (Time division multiple Access) :

- compared to FDMA, time division multiple access (TDMA) offers a much more flexible scheme, which comprises all technologies that allocate certain time slots for communication. Now tuning into a certain frequency is not necessary, that means the receiver can stay at the same frequency the whole time.
- using only one frequency, and thus very simple receivers and transmitters, many different algorithms exist to control medium access.
- listening to many channels separated in time at the same frequency is simple. Almost all MAC schemes for wired networks work according to this principle, e.g., Ethernet, TOKEN RING, ATM etc.
- Now, synchronization between sender and receiver has to be achieved in the time domain. It may be either a fixed pattern or dynamic allocation scheme.

- Dynamic allocation schemes require an identification for each transmission as TDMA is the case for typical wireless MAC schemes.
- MAC addresses are quite often used as identification. This enables a receiver in a broadcast medium to recognize if it really is the intended receiver or a merely.
- Fixed schemes do not need identification.

① Fixed TDM:

- The simplest algorithm for using TDM is allocating time slots for channels in a fixed pattern.
- This results in a fixed bandwidth and is the typical solution for wireless phone systems.
- MAC is quite simple, as the only crucial factor is accessing the reserved time slot at the right moment.
- If TDMA synchronization occurs, each mobile station knows its turn and no interference will happen.
- The fixed pattern can be assigned by the base station where competition between different mobile stations that want to access the medium is solved.
- Fixed access patterns fit perfectly well for connections with a fixed bandwidth.
- TDMA schemes with fixed access patterns are used for many digital mobile phone systems like IS-54, IS-136, GSM, DECT, PHS and PACS.
- Assigning different slots for uplink and downlink using the same frequency called time division duplex (TDD).

② Classical Aloha: (~~Wired stations no such exist~~) AMGT

- TDMA comprises all mechanisms controlling medium access according to TDM. But what happens if TDM is applied without controlling access? This is exactly what the classical Aloha scheme does; A scheme which was invented at the university of Hawaii and was used in the ALOHANET for wireless connection of several stations.
- Aloha neither coordinates medium access nor does it resolve contention on the MAC layer.
- Instead, each station can access the medium at any time. This is a random access scheme, without a central arbiter controlling access and without coordination among the stations.
- If two or more stations access the medium at the same time, a collision occurs and the transmitted data is destroyed.

→ The simple Aloha works fine for a light load and does not require any complicated access mechanisms.

③ Slotted Aloha:

- The first refinement of the classical Aloha scheme is provided by the introduction of time slots (Slotted Aloha).
- In this case, all senders have to be synchronized, transmission can only start at the beginning of a time slot.
- Here the introduction of slots raises the throughput from 18 percent to 36 percent.
- Here still access is not coordinated, both the Aloha principles occur in many systems that implement distributed access to a medium.
- Aloha systems work perfectly well under a light load but they can not give any hard transmission guarantees.
- However, even new mobile communication systems like UMTS have to rely on Slotted Aloha for medium access in certain situations.

④ carrier sense multiple Access (CSMA):

- One improvement to basic Aloha is hearing the carrier before accessing the medium. This is what CSMA schemes generally do.
- Hearing the carriers before accessing the medium reduces the chance of collision but hidden terminals can't be detected and if it transmits at the same time when another sender is sending the data then there collision occurs.
- This basic scheme is still used in most wireless LANs.
- Several versions of CSMA exists. In non-persistent CSMA, stations sense the carrier and start sending immediately if the medium is idle. If the medium is busy, the station pauses a random amount of time before sending the medium again and re-sampling the pattern.
- CSMA with collision avoidance (CSMA/CA) is one of the access schemes used in wireless LAN following the standard IEEE 802.11.
- Here sensing the carrier is combined with a back-off scheme in case of a busy medium to achieve some fairness among competing stations.

⑤ Demand assigned multiple Access:

- A general improvement of Aloha access systems can also be achieved by reservation mechanisms and combining with some (fixed) TDM tables.
- These schemes typically have a reservation period followed by a transmission period. During reservation periods, stations can reserve future slots in the transmission period.

- One basic scheme for demand assigned multiple access (DAMA) also called reservation Aloha, a scheme typical for satellite systems. DAMA has two modes.
- During a contention phase, all stations can try to reserve future slots.
- For example, 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.
- In successful, a time slot in the future is reserved and no other station is allowed to transmit during this slot.
- DAMA is an explicit reservation scheme. Each transmission slot has to be reserved explicitly.

Packet reservation multiple access (PRMA):

- An example for an implicit reservation scheme is packet reservation multiple access (PRMA); Here slots can be reserved implicitly according to the following scheme.
- A certain number of slots forms a frame. The frame is repeated in time i.e. a fixed TDM pattern is applied.
- A base station, which could be a satellite, now broadcasts the status of each slot to all mobile stations.
- All stations receiving this vector will then know which slot is occupied and which slot is currently free.
- PRMA constitutes yet another combination of fixed and random TDM schemes with reservation compared to the previous schemes.
- As soon as a station has succeeded with a reservation, all future slots are implicitly reserved for this station.
- This ensures transmission with a guaranteed data rate. The slotted aloha scheme is used for idle slots only, data transmission is not destroyed by collision.

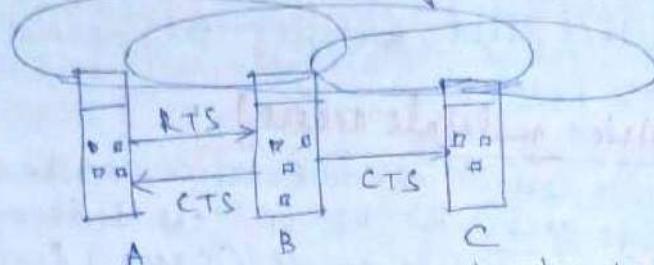
Reservation TDMA:

- An even more fixed pattern that still allows some random access is exhibited by reservation TDMA. In a fixed TDM scheme N mini-slots followed by $N \cdot K$ data slots form a frame that is repeated.
- This guarantees each station a certain bandwidth and a fixed delay.
- Using these free slots can be based on a simple round-robin scheme or can be ~~be uncoordinated~~ using an aloha scheme.

Multiple access with collision avoidance (MACA):

- MACA presents a simple scheme that solves the hidden terminal problem, does not need a base station and is still a random access Aloha scheme—but with dynamic reservation.
- Here, A and C both want to send to B. A has already started

the transmission, but is hidden for C, C also hears it with its transmission, thereby causing a collision at B.



- With MAC, A does not start with its transmission at once, but sends a request to send (RTS). First, B receives the RTS that contains the name of sender and receiver, as well as the length of the future transmission.
- This RTS is not heard by C, but triggers an acknowledgement from B, called clear to send (CTS).
- The CTS again contains the name of the sender (A) and receiver (B) of the user data and the length of the future transmission.
- This CTS is now heard by C and the medium for future use by A is now reserved for the duration of the transmission.
- After receiving a CTS, C is not allowed to send anything for the duration indicated in the CTS towards B.
- A collision cannot occur at B during data transmission and the hidden terminal problem is solved - provided that the transmission conditions remain the same.
- Still, collisions can occur during the sending of an RTS. Both A and C could send an RTS that collides at B. RTS is very small compared to the data transmission, so the probability of a collision is much lower.

Polling:

- where one station is to be heard by all others (e.g., the base station of a mobile phone network or any other dedicated station) polling schemes can be applied.
- Polling is a slightly centralized scheme with one master station and several slave stations.
- The master can poll the slaves according to many schemes: round-robin, randomly, according to reservations etc.
- The master could establish a list of stations waiting to transmit during a contention phase. After this phase, the station polls each station on the list. Similar schemes are used, e.g. in the Bluetooth wireless LAN.

Inhibit Sense Multiple-Access (ISMA):

- Another combination of different schemes is represented by ~~inhibit sense multiple access (ISMA)~~ inhibit sense multiple access (ISMA). This scheme is used for the packet data transmission service cellular digital packet data (CDPD) in the AMPS mobile phone system & also known as digital sense multiple access (DSMA).

- Here, the base station only signals a busy medium via a busy (called busy/CSIR indicator) on the downlink.
- After the busy tone loop, accessing the uplink is not coordinated any further.

CDMA (Code division multiple access) :

- Finally, codes with certain characteristics can be applied to the transmission to enable the use of code division multiplexing (CDM). Code division multiple access (CDMA) allows use exactly three codes to separate different users in the code space and to enable access to a shared medium without interference.
- The main problem is how to find "good" codes and how to separate the signal from noise generated by other signals and the environment.
- The code directly controls the spreading sequence.
- Then explain CDM.

(1) Spread Aloha multiple access :

- Using different codes with certain properties for spreading data results in a nice and powerful multiple access scheme namely CDMA. But CDMA senders and receivers are not really simple devices.
- Communicating with n devices requires programming of the receiver to be able to decode n different codes.
- For mobile phone systems, a lot of complexity needed for CDMA to integrate in the base stations. The wireless and mobile devices communicate with the base station only.
- The CDMA technique seems to pose too much overhead.
- No one wants to program many spreading codes for e.g. ad-hoc networks. On the other hand, Aloha was a very simple scheme, but could only provide a relatively low bandwidth due to collisions.
- If we use CDMA with only a single code, i.e. without CD? The resulting scheme is called spread Aloha multiple access (SAM) and is a combination of CDMA and TDMA.
- SAM works as follows: each sender uses the same spreading code. The same data can also be sent with higher power for a shorter period.
- The signal of an unsynchronized sender appears as noise.
- The main problem in using this approach is finding good spreading sequences ~~and it's very difficult~~ ~~it's very difficult~~ ~~it's very difficult~~

Comparison of S/T/F/CDMA :

- In real systems, the MAC schemes always occur in combinations. A very typical combination is constituted by SDMA/TDMA/FDMA as used in IS-54, GSM, DECT, PHS and PACS phone systems.

- Although many network providers and manufacturers have lower their expectations regarding the performance of CDMA compared to the early 1980s but CDMA is integrated into almost all third generation mobile phone systems either as W-CDMA (FOMA, UMTS) or CDMA 2000.
- CDMA can be used in combination with FDMA/TDMA access schemes to increase the capacity of a cell. In contrast to other schemes, CDMA has the advantage of a soft handover and soft capacity. Soft capacity in CDMA systems describes the fact that CDMA systems can add more and more users to a cell, i.e. there is no hard limit.
- For TDMA/FDMA systems, a hard upper limit exists - if no more time/frequency slots are available, the system rejects new users.
- Cell planning is more difficult in CDMA systems compared to the more fixed TDMA/FDMA schemes.
- Mobile phone systems using SDMA/TDMA/FDMA or SDMA/CDMA are centralized systems.
- Most distributed systems use some version of the basic Aloha.
- Simple CSMA is very efficient at low load, MACA can overcome the problem of hidden terminals and polling guarantees bandwidth. No single scheme combines all the benefits, which is why, for example, the wireless LAN standard IEEE 802.11 combines all three schemes. Polling is used to set up a time structure via a base station. A CSMA version is used to access the medium during uncoordinated periods, and additionally, MACA can be used to avoid hidden terminals or in cases where no base station exists.

(multiple user with CSMA with collision detection and avoidance mechanism based on CSMA/CA)

• CSMA/CA is a collision avoidance technique used in IEEE 802.11 wireless LANs. It is a variation of CSMA and is used in conjunction with the IEEE 802.11 standard. In CSMA/CA, a node will not transmit if it detects a signal on the channel. If a node wants to transmit, it will first listen to the channel for a short period of time. If no signal is detected, the node can transmit its data. If a collision occurs, the nodes will wait for a random amount of time before attempting to transmit again. This process continues until the data is successfully transmitted.

(multiple user with MACA with collision detection and avoidance mechanism based on CSMA/CA)

• MACA (Multiple Access with Collision Avoidance) is a collision avoidance technique used in IEEE 802.11 wireless LANs. It is a variation of CSMA and is used in conjunction with the IEEE 802.11 standard. In MACA, a node will not transmit if it detects a signal on the channel. If a node wants to transmit, it will first listen to the channel for a short period of time. If no signal is detected, the node can transmit its data. If a collision occurs, the nodes will wait for a random amount of time before attempting to transmit again. This process continues until the data is successfully transmitted.

(multiple user with CSMA/CA with collision detection and avoidance mechanism based on CSMA/CA)

• CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) is a collision avoidance technique used in IEEE 802.11 wireless LANs. It is a variation of CSMA and is used in conjunction with the IEEE 802.11 standard. In CSMA/CA, a node will not transmit if it detects a signal on the channel. If a node wants to transmit, it will first listen to the channel for a short period of time. If no signal is detected, the node can transmit its data. If a collision occurs, the nodes will wait for a random amount of time before attempting to transmit again. This process continues until the data is successfully transmitted.

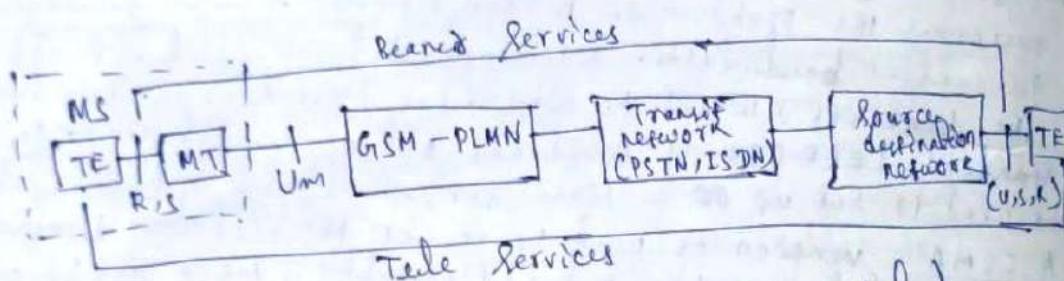
Telecommunication Systems

GSM (Global System for mobile communications) :

- GSM is the most successful mobile telecommunication system in the world today. It is used by thousands of millions of people in more than 190 countries.
- The primary goal of GSM was to provide a mobile phone system that allows users to roam throughout Europe and provides voice services compatible to ISDN and other PSTN systems.
- GSM is a second generation system, replacing the first generation analog systems but not offering the high worldwide data rates that the third generation systems, such as UMTS, are promising.

GSM mobile services:

- GSM permits the integration of different voice and data services and the interworking with existing networks.
- Services make a network interesting for customers.
- GSM has defined three different categories of services: bearer, tele and supplementary services.



(Bearer and tele services reference model)

- A mobile station (MS) is connected to the GSM public land mobile network (PLMN) via the Um interface.
- (GSM-PLMN is the infrastructure needed for GSM network)
- This network is connected to transit networks, e.g., integrated services digital network (ISDN) or traditional public switched telephone network (PSTN).
- There might be an additional network, the source/destination network before another terminal TE is connected.
- Bearer services now comprise all services that enable the transparent transmission of data between the interfaces to the network, i.e. S in case of the mobile station and a similar interface for the other terminal (e.g. so for ISDN terminals).
- Interfaces like V, S and R in case of ISDN have not been designed for all networks, so it depends on the specific network which interface is used as a reference for the transparent transmission of data.

- The bearer services of GSM only need the lower three layers of the ISO/OSI reference models.
- Within the mobile station MS, the mobile termination (MT) performs all network specific tasks (TMA, FOMA, coding etc.) and offers an interface for data transmission (S) to the terminal TE which can then be network independent.

Bearer Services:

- GSM specifies different mechanisms for data transmission.
- Bearer services permit transparent and non-transparent, synchronous or asynchronous data transmission.
- Synchronous bearer services only use the function of the physical layer (Layer 1) to transmit data.
- The transmission quality is increased by the use of the forward error correction (FEC), which codes redundancy into the data streams and helps to reconstruct the original data in case of transmission errors.
- Transparent bearer services do not try to recover lost data.
- Non-transparent bearer services use protocols of layers two and three to implement error correction and flow control. : 2nd protocol
- There are two types of transparent bearer services, adding a radio link protocol (RLP).
- This protocol comprises mechanisms of high-level data link control (HDLC).
- Using transparent and non-transparent services, GSM specifies several bearer services for interworking with PSTN, ISDN and packet switched public data networks (PSDN) like X.25, which is available worldwide.

Tele services:

- GSM mainly focuses on voice-oriented tele services.
- These comprise encrypted voice transmission, message services and basic data communications with terminals as known from the PSTN or ISDN (e.g. fax).
- However, as the main service is telephony, the primary goal of GSM was the provision of high-quality digital voice transmission, offering at least the typical bandwidth of 3.1 kHz of analog phone systems.
- Special codecs (coder/decoder) are used for voice transmission while other codecs are used for the transmission of analog data for communication with traditional computer modems used in, e.g. fax machines.
- Another service offered by GSM is the emergency number. The same number can be used throughout the country. This service is mandatory for all providers and free of charge.

- A useful service for very simple message transfer is the short message service (SMS) which offers transmission of messages of up to 160 characters.
- SMS messages do not use the standard data channel of GSM but exploit unused capacity in the signalling channels.
- Sending and receiving of SMS is possible during data or voice transmission.
- The successor of SMS, the enhanced message service (EMS) offers a larger message size (760 characters), formatted text and the transmission of animated pictures, small images, ring tones etc.
- MMS offers the transmission of larger pictures (GIF, JPG etc.) short video clips etc.
- Another non-voice tele service is group 3 fax, which is available worldwide. In this service, fax data is transmitted as digital data over the analog telephone network.

Supplementary Services:

- In addition to talk and bearer services, GSM providers can offer supplementary services.
- Some typical services are user identification, cell redirection, or forwarding of ongoing calls.
- Standard ISDN features such as closed user groups and multi party communication may be available.

System architecture:

- A GSM system consists of three subsystems, the radio subsystem (RSS), the network and switching subsystem (NSS) and the operation subsystem (OSS).

Radio Subsystem:

- As the name implies, the radio subsystem (RSS) comprises all radio specific facilities, i.e. the mobile station (MS) and the base station subsystem (BSS).
- A GSM network comprises many BSS, each controlled by a base station controller (BSC). The BSC performs all functions necessary to maintain radio connections to an MS.
- Base transceiver station (BTS) comprises all radio equipment i.e. antennas, signal processing, amplifiers necessary for radio transmission.
- It can form a radio cell or using sectorized antennas several cells.

- Base Station controller (BSC): It logically manages BSCs.
- reserves radio frequencies, handles ~~handover~~ the handover from one BSC to another within the BSS and performs paging of the MS.
- Mobile Station (MS): It comprises all user equipment and software needed for communication with a GSM network.
- An MS consists of user independent software and hardware and the Subscriber Identity Module (SIM) which stores all user-specific data that is relevant to GSM.
- An user can personalize any mobile station using his or her SIM.

(2) Network and switching subsystems:

- The heart of the GSM System is formed by the network and switching subsystems. The NSS connects the wireless network with standard public network, performs handovers between different BSSs, comprises functions for worldwide localization of users and supports changing, accounting and roaming of users between different providers in different countries. The NSS consists of following switches and databases:
- Mobile Service Switching centre (MSC): MSCs are high-performance digital ISDN switches. They set up connections to other MSCs and to the BSCs via the A interface, and form the backbone network of a GSM system. Typically, an MSC manages several BSCs in a geographical region.
- Home location register (HLR): The HLR is the most important database in a GSM system, as it stores all user relevant information. This comprises static information such as mobile subscriber ISDN number (MSISDN), subscribed services (e.g. call forwarding, roaming, GPRS) and the International mobile subscriber Identity (IMSI) etc.
- As soon as an MS leaves its current LA (local area), the information in the HLR is updated.
- Visitor location register (VLR): The VLR associated to each MSC is a dynamic database which stores all important information needed for the MS users currently in the LA that it is associated to the MSC. If a new MS comes into an LA the VLR is responsible for, it copies all the

relevant information for this user from the HLR.

③ operation subsystem: The third part of a GSM system, the operation subsystem (OSS), contains the necessary functions for network operations and maintenance.

→ operation and maintenance centre (OMC): It monitors and controls all other network entities via the I interface.

→ Typical OMC management functions are traffic monitoring, status reports of network entities, subscriber and security management or accounting and billing.

→ authentication centre (AVC): The AVC has been designed to protect user identity and data transmission. The AVC contains the algorithms for authentication and as well as keys for encryption.

→ Equipment Identity register (EIR): It stores all device identifications registered for the network. As MSs are mobile, they can be easily stolen. The EIR has a blacklist of stolen (or locked) devices.

→ In theory an MS is useless as soon as the owner has reported a theft.

→ It is a database for all IMEI.

Radio Interface :

→ The most interesting interface in a GSM system is Uu, the radio interface, as it comprises many mechanisms for multiplexing and media access.

→ GSM implements TDMA using cells with BTS and assigns an MS to BTS.

→ Furthermore, FDD is used to separate uplink and downlink.

→ Media access combines TDMA and FDMA.

→ Data is transmitted in small portions, called bursts. A normal burst as used for data transmission inside a time slot.

→ The guardspace is used to avoid overlapping with other bursts due to different path delays and to give the transmitter time to turn on and off.

→ The first and last three bits of a normal burst (tail) are all set to 0 and can be used to enhance the received performance.

→ A flag S indicates whether the data field contains user or network control data.

- Apart from the normal burst there are 4 more bursts are used for data transmission.
- A frequency correction burst allows the MS to correct local oscillator to avoid interference with neighbouring channels.
- A synchronization burst synchronizes the MS with BTS in time.
- An access burst is used for the initial connection setup between MS and BTS.
- A dummy burst is used if no data is available for a slot.
- To avoid frequency selective fading, GSM provides an optional slow frequency hopping mechanism. MS and BTS may change the carrier frequency after each frame based on a common hopping sequence. An MS changes its frequency between up and downlink slots respectively.
- GSM specifies two basic groups of logical channels i.e. traffic channels and control channels.
- Traffic channels (TCH): GSM uses a TCH to transmit user data (e.g. voice, fax). Two types of TCH have been defined i.e. full-rate TCH (TCH/F) and half-rate TCH (TCH/H).
- A TCH/F has a data rate of 22.8 Kbit/s, whereas TCH/H has a data rate of 11.4 Kbit/s.
- Improved codes allow for better voice coding, and can use a TCH/H. Using this, the capacity of the GSM system for voice transmission.
- Control channels (CCH):
- Many different CCCHs are used in a GSM system to control medium access, allocation of traffic channels or mobility management. Three groups of control channels have been defined, each again with subchannels.
- * Broadcast control channel (BcCH): A BTS uses this channel to signal information to all MSs within a cell. Information transmitted in this channel.
- * Common control channel (CcCH): All information regarding connection setup between MS and BS is exchanged via the CcCH. For calls toward an MS, the BTS uses the paging channel (PCH) for paging the appropriate MS.
- * Dedicated control channel (DcCH): While the previous channels have all been unidirectional, the following channels are bidirectional. This can comprise authentication, negotiation or other data needed

for setting up a TCH.

- However, these channels can't use some slots arbitrarily. GSM specifies a very elaborate multiplexing scheme that integrates several interleavers of frames.
- This periodic pattern of 20 slots occurs in all TDMA frames with a TCH. The combination of these frames is called traffic multiframe.

Protocols :

- Layer 1, the physical layer, handles all radio-specific functions. This includes the creation of bursts according to five different formats, multiplexing of bursts into a TDMA frame, synchronization with the BTS, detection of the idle channels and measurement of the channel quality on the downlink.
- The physical layer at Uu uses GMSK for digital modulation and performs encryption / decryption of data.
- Synchronization also includes the correction of the individual path delay between an MS and the BTS.
- All MSs within a cell use the same BTS and thus must be synchronized to this BTS.
- The main task of the physical layer comprises channel coding and error detection / correction which is directly combined with the coding mechanism.
- Channel coding makes extensive use of different forward error correction (FEC) schemes.
- Different logical channels of GSM use different coding schemes with different correction capabilities.
- Mobility Management (MM) contains functions for registration, authentication, identification, location updating and the provision of a temporary mobile subscriber identity (TMSI).
- Finally, the call management (CM) layer contains three entities: call control (CC), short message service (SMS) and supplementary service (SS).
→ Signaling bytes No. 7 (SS7) is used for signaling between an MSC and a BSC.

Localization and calling:

- One fundamental feature of the GSM system is the automatic, worldwide localization of users. The system always knows where a user currently is, and the same phone number is valid worldwide. To provide this service, GSM performs periodic location updates even if a user does not use the mobile station.
- The HLR always contains information about the current location and the VLR currently responsible for the MS informs the HLR about location changes.

→ As soon as an MS moves into the range of a new VLR, the HLR sends all user data needed to the new VLR. changing VLR with uninterrupted availability of all services is also called roaming.

→ Roaming can take place within the network of one provider, between two providers in one country (national roaming) or often not supported due to competition between operators) but also between different providers in different countries (international roaming). Thirdly, people associate international roaming with the term roaming as it is this type of roaming that makes GSM very attractive. To locate an MS and to address the MS, several numbers are needed:

* Mobile station International ISDN number (MSISDN)

→ The ~~most~~ only important number for a user of GSM is the phone number. The phone number is associated with the SIM not with a certain device.

→ The MSISDN follows the ITU-T standard. It consists of the country code (cc), the national destination code (NDC) and the subscriber number (SN).

* International mobile subscriber identity (IMSI):

→ GSM uses the IMSI for internal unique identification of a subscriber. IMSI consists of a mobile country code (Mcc), the mobile network code (Mnc) and finally the mobile subscriber identification number (MSIN).

* Temporary mobile subscriber identity (TMSI):

To hide the IMSI, which would give away the exact identity of the user signaling over the air interface, GSM uses the 4 byte TMSI for local subscriber identification.

* Mobile station roaming number (MSRN): Another temporary address that hides the identity and location of a subscriber is MSRN. MSRN contains the current visited country code (VCC), the visited national destination code (VNDC), the identification of the current VSC together with the subscriber number.

→ The MSRN helps the HLR to find a subscriber for an incoming call.

Handover:

→ cellular networks require handover procedures, as single cells do not cover the whole service area, but e.g. only up to 35 km around each antenna on the countryside and some hundred meters in cities.

→ The smaller the cell size and the faster the movement of a mobile station through the cells, the more handovers of ongoing calls are required. However, a handover should not cause a cut-off, also called call drop.

There are two reasons for a handover.

- The MS moves out of the range of a BTS or a certain antenna of a BTS respectively. The received signal decreases continuously until it falls below the minimal requirements for communication.
- The wired infrastructure (MSC, BSC) may decide that the traffic in one cell is too high and shift some MS to other cells with a lower load. Handover may be due to load balancing.

There four possible handover scenarios in GSM:

- intra-cell handover: within a cell, narrow-band interference could make transmission at a certain frequency impossible. So handover can be made.

- Inter-cell, intra-BSC handover:

This is a typical handover scenario. The mobile station moves from one cell to another, but stays within the control of same BSC. The BSC then performs a handover.

- Inter-BSC, intra-MS handover:

As a BSC only controls a limited number of cells, GSM also has to perform handovers between cells controlled by different BSCs. This handover then has to be controlled by MSC.

- inter-MS handover:

A handover could be required between two cells belonging to different MSCs. Now both MSCs perform the handover together.

Security: GSM offers several security services using confidential information stored in the AUC and in the individual SIM.

Access control and authentication: The first step includes the authentication of a valid user for the SIM.

The user needs a secret ~~key~~ PIN to access the SIM.

The next step is the subscriber authentication.

Confidentiality: All user-related data is encrypted.

MS applies encryption to voice, data and signaling.

The confidentiality exists between MS and BTS.

Anonymity: To provide user anonymity, all data is encrypted before transmission and user identifiers are not used over the air.

Three algorithms are used in GSM to provide security.

Algorithm A3 is used for authentication, A5 for encryption and A8 for the generation of a cipher key. Only algorithm A5 was publicly available whereas A3 and A8 were secret.

Authentication: Before a subscriber can use any service from the GSM network, he or she must be authenticated. Authentication is based on the SIM, which stores the individual authentication key K_i , the user identification IMSI, and the algorithms used for authentication A3. → For authentication, the VLR sends the random value RAND to the SIM.

Encryption: To ensure privacy, all messages containing user-related information are encrypted in GSM over the air interface.

- After authentication, MS and BSC can start using encryption by applying the cipher key K_c . K_c is generated using the individual key K_i and a random value by applying the algorithm A8.
- The key K_c itself is not transmitted over the air interface.

New Data Services:

- The standard bandwidth of 9.6 kbit/s available for data transmission is not sufficient for the requirements of today's computer.
- To enhance the data transmission capabilities of GSM, two basic approaches are possible. As the basic GSM is based on connection-oriented traffic channels e.g. with 9.6 kbit/s each, several channels could be combined to increase the bandwidth.

D) HSCSD: A straightforward improvement of GSM's data transmission capabilities is high-speed circuit-switched data (HSCSD), which is available with some providers.

- In HSCSD higher data rates are achieved by building several TCHs.
- An MS requests one or more TCHs from the GSM network, i.e. it allocates several TDMA slots within a TDMA frame.
- This allocation can be asymmetrical, i.e. more slots can be allocated on the downlink than on the uplink, which fits the typical user behaviour of downloading more data compared to uploading.
- HSCSD only requires software upgrade in an MS & MSC.
- It has the disadvantage that, it still uses the connection-oriented mechanisms of GSM. These are not at all efficient for computer data traffic, which is typically bursty and asymmetrical.
- For n channels, HSCSD requires n times signaling during handover, connection setup and release. Each channel is treated separately.

② GPRS :

- The next step toward more flexible and powerful data transmission avoid the problem of HSCSD by being fully-packet oriented. The general packet radio service (GPRS) provides packet mode transfer for applications that exhibit traffic patterns such as frequent transmission of small volumes (e.g. typical web requests) or infrequent transmission of small or medium volumes (e.g. typical web responses) according to the requirement specification.
- Compared to existing data transfer services, GPRS should use the existing network resources more effectively for packet mode applications and should provide a selection of QoS parameters for the service requesters.
- GPRS should also allow for broadcast, multicast and unicast service.
- The main benefit for users of GPRS is the 'always-on' characteristics - no connection has to be set up prior to data transfer.
- For the 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 pre-determined manner but on demand. All time slots can be shared by the active users; up- and down-link are allocated separately.
- Allocation of the slots is based on current load and operator preferences.
- Depending on the coding, a transfer rate up to 170 kbit/s is possible.
- The GPRS concept is independent of channel characteristics and of the type of channel and does not limit the maximum data rate.
- All GPRS services can be used in parallel to conventional services.
- In phase 1, GPRS offers a point-to-point (PTP) packet transfer service.
- Delay within a GPRS network is incurred by channel access delay, coding for error correction and transfer delay in the fixed and wireless part of the GPRS network. The delay introduced by external fixed networks is out of scope.
- Finally, GPRS includes several security services such as authentication, access control, user identity confidentiality and user information confidentiality.

- The GPRS architecture introduces two new network elements, which are called GPRS support nodes (GSN) and are in fact routers. All GSNs are integrated into the standard GSM architecture, and many new interfaces have been defined.
- The gateway GPRS support node (GGSN) is the interworking unit between the GPRS network and external packet data networks (PDN). This node contains routing information for users, performs address conversion and tunnels data to a user via encapsulation.
- The GPRS register (GR) keeps track of the individual MS's location, is responsible for collecting billing information (counting bytes).
- Before sending any data over the GPRS network, an MS must attach to it, following the procedures of the mobility management.
- The other new element is the serving GPRS support node (SGSN) which supports the MS via the Gp interface.
- In an idle mode an MS is not reachable and all context is deleted.
- GPRS tunnelling protocol (GTP) can use two different transport protocols either the reliable TCP (needed for reliable transfer of X.25 packets) or the non-reliable UDP (used for IP packets).
- The network protocol for the GPRS backbone is IP (using any lower layers).
- The radio link protocol (RLP) provides a reliable link while the MAC controls access with signalling procedures for the radio channel.
- MS can allocate up to eight packet data traffic channels (PDCHs).

a) DECT: Another fully digital cellular network is the digital enhanced cordless telecommunications (DECT) system.

- It replaces older analog cordless phone systems.
- DECT could also be used to bridge the last few hundred meters between a new network operator and customer.
- A big difference between DECT and GSM is in terms of cell diameter and cell capacity. While GSM is designed for outdoor use with a cell diameter of up to 70 Kms, the range of DECT is limited to about 300m from the base station.
- It can also handle handovers but it was not designed to work at a higher speed. DECT works at a frequency range of 1880 - 1990 MHz offering 120 full duplex channels.

System architecture

→ local networks in the DECT context offer local telecommunication services that can include everything from simple switching to intelligent call forwarding, address translation etc. Here there are home database (HDB) and visitor database (VDB) are also located.

Protocol architecture

The DECT protocol reference architecture follows the OSI reference model. It contains the physical layer, medium access control and data link control plus both the control plane (c-plane) and the user plane (U-plane).

Physical layer:

As in all wireless networks, the physical layer comprises all functions for modulation/demodulation, downlink signal detection, header/receiver synchronization and collection of status information for the management plane.

Medium access control layer:

The MAC layer establishes, maintains and releases channels for higher layers by partitioning and aggregating physical channels. MAC multiplexes several logical channels onto physical channels.

Data link control layer:

It creates and maintains reliable connections between the mobile terminal and the base station. Two services have been defined for the c-plane: a connectionless broadcast service for paging and a point-to-point protocol similar to LAPD in ISDN.

Network layer:

The network layer of DECT is similar to those in 2M ISDN and GSM and only exists for the c-plane. This layer provides services to request, check, reserve, control and release resources at the fixed station and the mobile terminal.

TETRA (Terrestrial trunked radio):

Trunked radio systems constitute another method of wireless data transmission. These systems use many different radio carriers but only allocates a specific carrier to a certain user for a short period of time according to demand.

- These types of radio systems typically offer interfaces to the fixed telephone network, i.e. voice and data services, but are not publicly accessible.
- These systems are not only simpler than most other networks, they are also reliable and relatively cheap to set up and operate.

→ Tetra also offers bearer services of up to 28.8 kbit/s for unprotected data transmission and 9.6 kbit/s for protected transmission.

→ In case of typical TDMA frame structure of TETRA, each frame consists of four slots. It consists of one control frame form a multiframe and finally a superframe contains 60 multiframes.

UMTS (Universal mobile telecommunications system) :

→ The European proposal for IMT-2000 prepared by ETSI is called universal mobile telecommunication system.

→ UMTS as initially proposed by ETSI rather represents an evolution from the second generation GSM system to the third generation than a completely new system.

→ The (IMT)-2000 - International mobile telecommunications tried to establish a common worldwide communication system that allowed for terminal and user mobility supporting the idea of universal personal telecommunication (UPT).

→ One initial enhancement of GSM toward UMTS was enhanced data rates for global evolution (EDGE), which uses enhanced modulation schemes.

→ UMTS fits into a bigger framework developed in the mid-nineties by ETSI, called global multimedia mobility (GMM).

→ UMTS should also provide several bearer services, real-time and non-real-time services, circuit and packet switched transmission and many different data rates.

→ Handover should be possible between UMTS cells, but also between UMTS and GSM or satellite networks.

→ UMTS should provide a variable division of uplink and downlink data rates.

→ The ITU standardized five groups of 3G radio access technologies.

* IMT-DS : The direct spread technology comprises wideband CDMA systems.

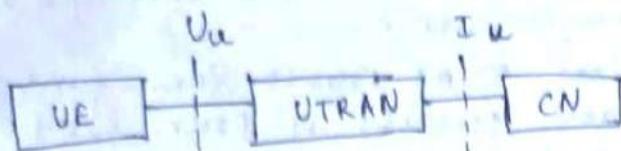
* IMT-TG : time code contained only the UTRA-TDD system.

* IMT-MC : multi-carrier technology.

* IMT-SC : single-carrier technology.

* IMT-FT : frequency-time technology.

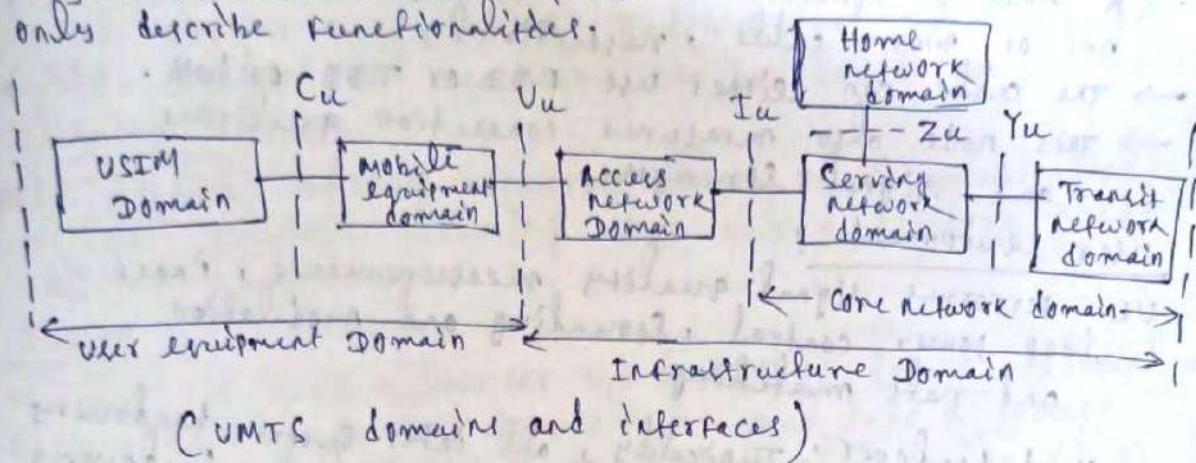
UMTS System Architecture



(Main components of the UMTS reference architecture)

- This UMTS reference architecture applies to both UTRA solutions (3GPP, 2000). The UTRA network (UTRAN) handles cell level mobility and comprises several radio network subsystems (RNS).
- The functions of the RNS include radio channel ciphering and deciphering, handover control, radio resource management etc.
- The UTRAN is connected to the user equipment (UE) via the radio interface Iu (which is comparable to the Um interface in GSM).
- Via the Iu interface (which is similar to the A interface in GSM), UTRAN communicates with the core network (CN).
- The CN contains functions for inter-system handover, gateways to other networks (fixed or wireless), and performs location management if there is no dedicated connection between UE and UTRAN.
- UMTS further subdivides the architecture into so-called domains. The user equipment domain is assigned to a single user and comprises all the functions that are needed to access UMTS services.
- The USIM domain contains the SIM for UMTS which performs functions for encryption and authentication of users and stores all necessary user-related data.
- The end device itself is in the mobile equipment domain. All functions for radio transmission as well as user interfaces are located here.
- The infrastructure domain is shared among all users and offers UMTS services to all accepted users. This domain consists of the access network domain, which contains the radio access network (RAN), and the core network domain can be separated into three domains with specific tasks.
- The serving network domain comprises all functions currently used by a user for accessing UMTS services.
- All functions related to the home network of a user, e.g. user data look-up, fall into the home network domain.

→ Finally, the transit network domain may be necessary if, for example, the serving network cannot directly contact the home network. All three domains within the core network may be in fact the same physical network. These domains only describe functionalities.



UMTS radio interface:

- The biggest difference between UMTS and GSM comes with the new radio interface (Vu). The duplex mechanisms are already well known from GSM (FDD) and DECT (TDD). However, the direct sequence (DS) CDMA used in UMTS.
- UMTS uses a constant chipping rate of 3.84 Mcihips/s. Different user data rates can be supported using different spreading factors.
- The first step in a feeder is spreading of user data using orthogonal spreading codes. Using orthogonal codes separates the different data streams of a feeder. UMTS uses so called orthogonal variable spreading factor (OVSF) codes.

UTRAN : (UMTS Terrestrial Radio Access Network)

- The UTRAN architecture consists of several radio network subsystems (RNS). Each RNS is controlled by a radio network controller (RNC) and comprises several components that are called node B.
- An RNC in UMTS can be compared with the BSC, a node B is similar to a BTS.
- Each node B can control several antennas which make a radio cell.
- RNC does the following tasks.
 - * cell admission control
 - * congestion control
 - * encryption / decryption
 - * ATM switching and multiplexing
 - * radio resource control
 - * code allocation
 - * power control
 - * management

Node B

The name node B was chosen during standardization until a new and better name was found.

- A node B connects to one or more antennas creating one or more cables, respectively.
- The cables can either use FDD or TDD or both.
- This node also measures connection qualities and signal strengths.

User Equipment

UE performs signal quality measurements, inner loop power control, spreading and modulation and rate matching.

- Hard handover: Typically, all inter system handovers are hard handovers in UMTS; this includes handovers to and from GSM or other IMT-2000 systems.

Soft handover:

Soft handovers are well known from traditional CDMA networks as they use macro diversity, a basic property of CDMA.

- Macro-diversity makes the transmission more robust with respect to fast fading, multi-path propagation and shadowing.

(Handover between two cells, no cell reselection done) : GARTU

Handover between two cells, no cell reselection done in GARTU case.

Handover between two cells, no cell reselection done in GARTU case.

Handover between two cells, no cell reselection done in GARTU case.

Handover between two cells, no cell reselection done in GARTU case.

Handover between two cells, no cell reselection done in GARTU case.

Handover between two cells, no cell reselection done in GARTU case.

Handover between two cells, no cell reselection done in GARTU case.

Wireless LAN

Advantages of WLANs are:

Flexibility: within radio coverage, nodes can communicate without further negotiation. Radio waves can penetrate walls. senders and receivers can be placed anywhere.

Planning:

only wireless ad-hoc networks allow for communication without previous planning, any wired network needs wiring plans.

Design:

wireless networks allow for the design of small, independent devices which can for example be put into a pocket. cables not only connects users but also designers of small PDA, Notepad etc.

Robustness: wireless networks can survive disasters, e.g. earthquakes or users pulling a plug. If the wireless device survive, people can still communicate.

Cost:

After providing wireless access to the infrastructure via an access point for the first user, adding additional users to a wireless network will not increase the cost. This is important for e.g. lecture halls, hotel lobbies or gate areas in airports where the numbers using the network may vary significantly.

Disadvantages:

Quality of Service: WLANs typically offer low quality than the wired counterparts. The main reasons for this are the lower bandwidth due to limitations in radio transmission.

Proprietary Solutions:

Due to slow standardization procedures, many companies have come up with proprietary solutions offering standardized functionality plus many enhanced features. However, these additional features only work in a homogeneous environment.

Restrictions: All wireless products have to comply with national regulations. Several government and non-government worldwide institutions regulate the operation and selected frequencies to minimize interference.

Safety and Security: using radio waves for data transmission might interfere with other high-tech equipment in e.g. hospital, senders and receivers are

operated by laymen and radiation has to be low. Special precautions have to be taken to prevent safety hazards.

Intra red vs. radio transmission:

Today, two different basic transmission technologies can be used to set up WLANs. One technology is based on the transmission of intra red light, the other one which is much more popular, uses radio transmission in the GHz range. Both technologies can be used to set up ad-hoc connections for work groups to connect, e.g. a desk-top with a printer without a wire, or to support mobility within a small area.

- Intra red technology uses diffuse light reflected at walls, furniture etc. or directed light if a LOS exists between the sender and the receiver. Senders can be simple ~~LED~~ LEDs or laser diodes. Photodiodes act as receivers.
- The main advantage of IR technology are its simple and extremely cheap senders and receivers which are integrated into nearly all mobile devices available today, e.g. PDAs, laptops, notebooks, mobile phones.
- Disadvantages of IR transmission are its low bandwidth compared to other LAN technologies. IR transmission cannot penetrate walls or other obstacles. Typically, for good transmission quality and high data rates a LOS, i.e. direct connection, is needed.

Radio transmission: Almost all networks described in use radio waves for data transmission, e.g., GSM at 900, 1800, and 1900 MHz, DECT at 18.80 MHz etc.

Advantages: The advantages of radio transmission include the long-term experiences made with radio transmission for WAN (e.g. microwave links) and mobile cellular phones.

- It can cover larger areas and can penetrate (through) walls, furniture, plants etc. Additional coverage is gained by reflection. Radio typically does not need a LOS if the frequencies are not too high.

Disadvantages:

Again, the main advantage is also a big disadvantage of radio transmission. Shielding is not so simple. Radio transmission can interfere with other senders or electrical devices can destroy data transmitted radio. Additionally, radio transmission is only permitted in certain frequency bands.

Infrastructure and ad-hoc networks:

- Many WLANs of today need an infrastructure network. Infrastructure networks not only provide access to other networks, but also include forwarding functions, medium access control etc. In these infrastructure-based wireless networks, communication typically takes place only between the wireless nodes and the access point, but not directly between the wireless nodes.
- The access point does not just control medium access, but also acts as a bridge to other wireless or wired networks. Several wireless networks may form one logical wireless network.
- Typically, the setup of infrastructure-based wireless networks is simpler because most of the network functionalities lies within the access point, whereas the wireless clients can remain quite simple.
- Handover may or may not occur.
- These networks cannot be used for disaster relief in cases where no infrastructure is left.

Ad-hoc networks:

- These wireless networks, do not need any infrastructure to work. Each node can communicate directly with other nodes, so no access point controlling medium access is necessary.
 - Nodes within an ad-hoc network can only communicate if they can reach each other physically, i.e. if they are within each other's radio range or if other nodes can forward message.
 - In ad-hoc networks, the complexity of each node is higher because every node has to implement medium access mechanisms & provide greatest flexibility.
 - Ad-hoc networks might only have selected nodes with with the capabilities of forwarding data. Most of the nodes have to connect to such a special node to transmit data if the receiver is out of their range.
- * IEEE802.11 and HyperLAN 2 are typically infrastructure-based networks which additionally support ad-hoc networking. Bluetooth is a typical wireless-ad-hoc WLAN.

Wireless Local Area Networks

IEEE 802.11

- The IEEE Standard 802.11 specifies the most famous family of WLANs in which many products are available. As the Standard's number indicates, this standard belongs to the group of 802.X LAN standards e.g. 802.3 Ethernet or 802.5 Token Ring.
- The primary goal of the standard was, the specification of a simple and robust WLAN which offers time-bounded and asynchronous services. The MAC layer should be able to operate with multiple physical layers, each of which exhibits a different medium scale and transmission characteristic.
- Additional features of the WLAN should include the support of power management to save battery power, the handling of hidden nodes and the ability to operate worldwide.

System architecture

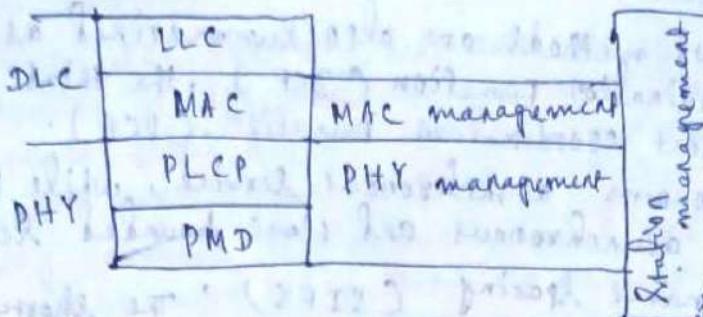
- Here several nodes, called stations (STA_i) are connected to access points (AP). Stations are terminals with access mechanisms to the wireless medium and radio contact to the AP.
- The stations and the AP which are within the same radio coverage form a basic service set (BSS_i). Then the BSS_i are connected via a distributed system.
- The distributed system connects the wireless networks via the APs, with a portal, which forms the WTI (interworking unit) to other LANs.
- Stations can select an AP and associate with it. The APs support roaming (i.e. changing access points), the distributed system handles data transfer between the different APs.
- APs provide synchronization within a BSS, support power management and can control medium access to support time-bounded service.
- In addition to infrastructure-based networks, IEEE 802.11 allows the building of ad-hoc networks between stations, thus forming one or more independent BSS_i.

Protocol architecture:

- The IEEE 802.11 standard only covers the physical layer PHY and medium access layer MAC like other 802.X LANs do.
- The physical layer is subdivided into the physical layer

convergence protocol (PLCP) and the physical medium dependent sublayer PMD. The basic tasks of the MAC layer comprise medium access, fragmentation of user data and encryption.

→ The upper part of the data link control layer, the logical link control (LLC), covers the differences of the medium access control layers needed for the different media. In many of today's networks, no explicit LLC layer is visible.



→ PLCP sublayer provides a carrier sense signal, called clear channel assessment (CCA), and provides a common PHY service access point (SAP) independent of the transmission technology.

→ Finally, the PMD sublayer handles modulation and encoding/decoding of signals.

Physical layer:

IEEE 802.11 supports three different physical layers: one layer based on infra red and two layers based on radio transmission. All PHY variants include the provision of the clear channel assessment signal (CCA). This is needed for the MAC mechanisms controlling medium access and indicates if the medium is currently idle.

→ Frequency hopping spread spectrum (FHSS)

→ Direct sequence spread spectrum (DSSS)

→ Infra red: The PHY layer, which is based on infra red transmission, uses near-visible light at 850–950nm. IR light is not regulated apart from safety restrictions. The standard does not require a line-of-sight between sender and receiver but should also work with diffuse light.

Medium access control layer:

→ The MAC layer has to fulfill several tasks. First of all, it has to control medium access, but it can also offer support for roaming, authentication and power conservation.

→ The basic services provided by the MAC layer are the ~~mandatory~~ mandatory asynchronous data service and an optional time-bounded service. 802.11 only offers the asynchronous service in ad-hoc network mode, both service types can be offered using an infrastructure-based network.

- The asynchronous service supports broadcast and multi-cast packets and packet exchange is based on the 'best effort' model i.e. no delay bounds can be given for transmission.
- The following three basic mechanisms have been defined for IEEE 802.11: the basic version of CSMA/CA, an optional method avoiding the hidden terminal problem, and finally a contention-free polling method for time bounded service.
- The first two methods are also summarized as distributed coordination function (DCF), the third method is called point coordination function (PCF).
- DCF only offers asynchronous service, while PCF offers both asynchronous and time bounded service.

Short-Inter Frame Spacing (SIFS): The shortest waiting time for medium access. (highest priority)

PCF Inter-frame Spacing (PIFS): A waiting time between SIFS and DIFS (and thus medium priority) is used for a time-bounded service.

DCF Inter-frame Spacing (DIFS): This parameter denotes the longest waiting time and has the lowest priority for medium access.

→ During a contention phase several nodes try to access the medium.

MAC frames: The basic structure of an IEEE 802.11 MAC data frame together with the content of the frame control field. The fields are:

- Frame control: The first 2 bytes
- Duration / ID
- Address 1 for: contain standard MAC addresses.
- Sequence control: ~~contain~~ a sequence number is used to filter duplicates.
- Data: MAC frame contains arbitrary data.
- CRC (Checksum)
- Protocol version
- Type
- Subtype
- Power management
- More data
- order
- More fragments

Roaming

- If a user walks around with a wireless station, the station has to move from one access point to another to provide uninterrupted service. Moving between access points is called ~~soft~~ roaming. The term handover or handoff as used in the context of mobile or cellular phone systems would be more appropriate as it is simply a change of the active cell. However, for WLANs roaming is more common.
- The steps for roaming between access points are:
 - * A station decides that the current link quality to its access point AP₁ is too poor. The station then starts scanning for another access point.
- Scanning involves the active search for another BSS and can also be used for setting up a new BSS in case of ad-hoc networks.
- IEEE 802.11 specifies scanning on single or multiple channels and different date between passive scanning and active scanning. Passive scanning simply means listening into the medium to find other networks. Active scanning comprises sending a probe on each channel and waiting for a response.
- The station then selects the best access point for roaming based on, e.g. signal strength, and sends an association request to the selected access point AP₂.
- The new access point AP₂ answers with an association response. If the response is successful, the station has roamed to the new ~~new~~ access point AP₂. Otherwise, the station has to continue scanning for new access points.
- The access point accepting an association request indicates the new station in its BSS to the distribution system (DS). The DS then updates its database, which contains the current location of the wireless stations.

802.11b :

- To avoid market segmentation, a common standard, IEEE 802.11b soon followed 802.11 and was added as supplement to the original standard.
- The standard describes a new PHY layer and is by far the most successful version of IEEE 802.11 available today.
- 802.11b hit the market before 802.11a.
- Depending on the current interference and the distance between sender and receiver 802.11b systems offer 11, 5.5, 2 or 1 Mbit/s. Maximum user data rate is approx 6 Mbit/s. The new data rates, 5.5 and 11 Mbit/s

- use 8-chip complementary code keying (CCK). The standard defines several packet formats for the physical layer.
- The mandatory format incorporates with the original versions of 802.11. The mandatory format is called long PLCP PPDU.
 - The optional versions provide a more efficient data transfer due to shorter headers/different coding schemes and can coexist with other 802.11 versions.
 - However, the standard states that control all frames shall be transmitted at one of the basic rates, so they will be understood by all stations in a BSS.
 - As IEEE 802.11b is the most widespread version, some more information is given for practical usage. The standard operates on certain frequencies in the 2.4 GHz ISM band. These depend on national regulations.
 - Although 14 channels have been defined, for each channel the centre frequency is given. This number of channels are used to minimize interference.
 - This is similar to the cell planning for mobile phone systems.

802.11a :

- IEEE 802.11a offers upto 54 Mbit/s using OFDM.
- The physical layer of IEEE 802.11a and the ETSI Standard HiperLAN2 has been jointly developed, so both physical layers are almost identical.
- However, HiperLAN2 differs in the MAC layer, the PHY layer packet formats and the offered services.
- Again, IEEE 802.11a uses the same MAC layer as all 802.11 physical layers do. To be able to offer data rates upto 54 Mbit/s, IEEE 802.11a uses many different technologies.
- The system uses 64 subcarriers (48 data + 4 pilot) that are modulated using BPSK, QPSK, 16-QAM etc.
- To reduce transmission errors, FEC is applied using coding rates of 1/2, 2/3 or 3/4.
- Depending on ~~national~~ national regulations, different sets of channels may be used.
- Eight channels have been defined for the lower two bands and four more are available in the high band.
- The PLCP preamble consists of 12 symbols and is used for frequency acquisition, channel estimation, and synchronization.

HiperLAN :

- in 1996, the ETSI standardized HiperLAN I as a WLAN allowing for node mobility and supporting ad-hoc and infrastructure-based topologies.
- get stands for high performance local area network.

HiperLAN I :

ETSI describes HiperLAN I as a wireless LAN supporting priorities and packet life time for data transfer at 23.5 Mbit/s, including forwarding mechanisms, topology discovery, user data encryption, network identification and power conservation mechanisms.

- HiperLAN I should operate at 5.1 - 5.3 GHz with a range of 50m in buildings at 1W transmit power.
- The service offered by a HiperLAN I is compatible with the standard MAC services known from IEEE 802.2 LANs. Addressing is based on standard 48 bit MAC addresses.
- Confidentiality is ensured by an encryption/decryption algorithms that requires the identical keys.
- A innovative feature of HiperLAN I, which many other wireless networks do not offer, is its ability to forward data packets using several relays. Relays can extend the communication on the MAC layer beyond the radio range.

Prioritization phase :

- HiperLAN I offers five different priorities for data packets ready to be sent. After one node has finished sending, many other nodes can compete for the right to lead.
- The first objective of the prioritization phase is to make sure that no node with a lower priority gains access to the medium while packets with higher priority are waiting at other nodes.
- In the first step of this phase, the priority detection, time is divided into five slots, slot 0 (highest priority) to slot 4 (lowest priority).

Elimination phase :

- Several nodes may now enter the elimination phase. The elimination phase now resolves contention by means of elimination bursting and elimination survival verification.
- The whole elimination phase will last for the duration of the longest elimination burst.

Yield phase :

- During the yield phase, the remaining nodes only listen to the medium without leading any additional bursts. Again, time is divided into slots, this time called yield slots.

Transmission phase:

A node that has survived the prioritization and contention phase can now send its data.

WATM: wireless ATM does not only describe a transmission technology but tries to specify a complete communication layer.

→ it is also called Mobile ATM.

→ Similar to other cellular networks, WATM networks must be able to locate a wireless terminal or a mobile user.

→ The network must provide mechanisms which search for new access points, set up new connections between intermediate buffers.

→ All extensions of protocol or other mechanisms also require an extension of ~~to~~ the management functions to control the network.

→ As for any wireless network, radio frequencies modulation schemes, antennas, channel coding etc. have to be determined.

→ Different media access schemes are possible, each with specific strengths and weaknesses.

→ During handover, cells cannot only be lost but can also be out of sequence. Cells must be re-severed and lost cells must be retransmitted if required.

WATM Services:

→ Office environments: This include all kinds of extensions for existing fixed networks offering a broad range of internet/intranet access, multi-media conferences, online multi-media database access.

→ Universities, schools, training centres: includes distance learning, wireless & mobile access to databases.

→ Industry: This include information retrieval, surveillance from database etc. which ~~is~~ involves the extension of intranet.

→ Hospitals: Application could include the transfer of medical images, remote access to patient records, remote monitoring of patients.

→ Home: many electronic devices at home (e.g. TV, radio equipment, PC with internet access) could be connected using WATM technology.

BRAN (Broadband radio access networks)

→ It can be used as RAL (radio access layer) for WATM.

→ The main motivation behind BRAN is the deregulation and privatization of the telecommunication system.

→ Different types of traffic are supported, one can multiplex traffic for higher efficiency and the connection can be asymmetrical.

- The primary market for BRAN includes private customers and small to medium-sized companies with Internet applications, multi-media conferencing and virtual private networks.
- The BRAN standard and IEEE 802.16 have similar goals.
- As an access network, BRAN technology is independent from the protocols of the fixed network. BRAN can be used for ATM and TCP/IP networks.

HiperLAN2:

- HiperLAN2 provides high-throughput transmission.
- It is connection-oriented. Prior to data transmission HiperLAN2 networks establish logical connections between a sender and a receiver. Connection set-up is used to negotiate QoS (Quality of Service) parameters. All connections are time-binded - multiplexed over the air interface.
- Each connection has its own set of QoS parameters.
- HiperLAN2 does not require frequency planning of cellular networks or standard IEEE 802.11 networks.
- Authentication as well as encryption are supported by HiperLAN2 for the security support.
- Mobile terminals can move around while transmission always takes place between the terminal and the access point with the best radio signal. Handover between access points is performed automatically.
- Mobile terminals can negotiate certain wake-up patterns to save power.
- If sector antennas are used for an AP, which is optional in the standard, the AP shall support sector handover. In case of radio handover, it is handled within the AP, no external interaction is needed.
- In case of network handover, the core network and higher layers are also involved and this is the most complex situation.
- HiperLAN networks can operate in two different modes. Those are centralized mode and base mode.
- HiperLAN has three layers, physical layer, data link layer, convergence layer.
- The data link layer has ~~three~~ six different so-called transport channels for data transfer. Those are:
 - ① Broadcast channel (BCH): conveys basic informⁿ for radio cell to all MTS.
 - ② Frame channel (FCH): contains directory for uplink and downlink phases.
 - ③ Access feedback channel (AICH) — gives FB to MTS.
 - ④ Long transport channel (LCH) — control data for d.s.c.u.l. (length 54 bytes)
 - ⑤ Short transport channel (SCH) (length 9 bytes)
 - ⑥ Harbor channel (RCH): here collision resolution is performed.

BLUETOOTH : Bluetooth technology is an ad-hoc network which are LANs with a very limited coverage and without the need for an infrastructure.

→ This is a different type of network as needed to connect different small devices in close proximity without expensive wiring or the need for a wireless infrastructure.

→ The necessary transceiver components should be cheap.

→ Many mobile phones, laptops, PDAs, video cameras etc. are equipped with bluetooth technology today.

Architecture :

→ Like IEEE 802.11b, Bluetooth operates in the 2.4 GHz ISM band.

→ However, MAC, physical layer and the offered services are completely different.

→ Bluetooth operates on 79 channels in the 2.4 GHz band with 1 MHz carrier spacing. Each device performs frequency hopping with 1600 hops/s.

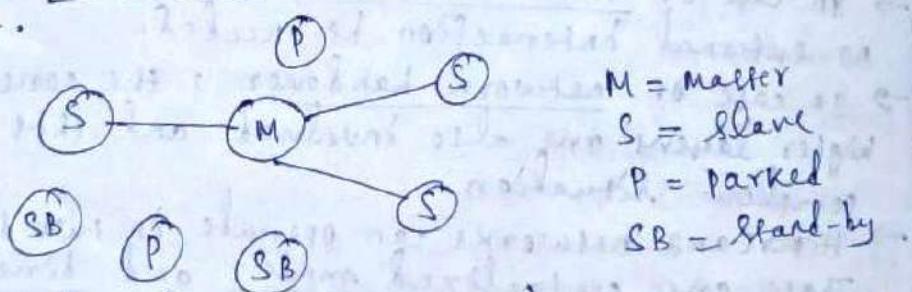
→ A very important term in the context of Bluetooth is a piconet. A piconet is a collection of bluetooth devices which are synchronized to the same hopping sequence.

→ One device in the piconet can act as master (M), all other devices connected to the master must act as slaves.

→ The master determines the hopping pattern in the piconet, and the slaves have to synchronize to this pattern.

→ Two additional types of devices are there. One is parked devices (P) can't actively participate in the piconet but can be reactivated within some microseconds.

~~The~~ devices in Stand-by (SB) do not participate in the piconet.



(Simple Bluetooth piconet)

→ All active devices are assigned a 3-bit active member address (AMA). All parked devices are an 8-bit parked member address (PMA). Devices in stand-by do not need an address.

Protocol Stack : The core protocols of Bluetooth comprise the following elements.

→ Radio : specification of the air interface.

→ Baseband : description of basic connection establishment, packet formats, timing and basic QoS parameters.

Link manager protocol: Link set-up and management between devices including security functions and parameter negotiation.

Logical link control and adaptation protocol (L2CAP):

Adaptation of higher layers to the baseband.

Service discovery protocol: Device discovery in close proximity plus querying of service characteristics.

→ On top of L2CAP is the cable replacement protocol RFCOMM that emulates a serial line interface. This allows for a simple replacement of serial line cables and enables many legacy applications and protocols to run over bluetooth.

Radio Layer: The radio specification is a rather short document and only defines the carrier frequencies and output power. Several limitations had to be taken into account when bluetooth's radio layer was designed.

→ Bluetooth devices will be integrated into typical mobile devices and rely on battery power. This requires small, low power chips which can be built into handheld devices.

→ Bluetooth has to support multimedia data.

→ Bluetooth uses the license-free frequency band at 2.4 GHz allowing for worldwide operation with some minor adaptations to national regulations.

→ Bluetooth transceivers use Gaussian FSK for modulation and are available in three classes: power class 1, power class 2 and power class 3.

PC1: max power is 100mW & min is 1mW.

PC2: max power is 2.5mW & nominal power is 1mW.

PC3: max power is 1mW.

Baseband Layer:

The functions of the baseband layer are quite complex as it not only performs frequency hopping for interference mitigation and medium access, but also defines physical links and many packet formats.

→ Remember that each device participating in a certain piconet hops at the same time to the same carrier frequency.

→ The time between two hops is called a slot.

→ Bluetooth also defines 3-slot and 5-slot packets for higher data rates (multi-slot packets).

→ If a master or a slave sends a packet covering three or five slots, the radio transmitter remains on the same frequency. No frequency hopping is performed within packets.

→ After transmitting the packet, the radio returns to the frequency required for its hopping sequence.

→ The components of a bluetooth packet of baseband layer consists of Access code, packet header, payload.

- The access code of a packet is needed for timing synchronization and piconet identification.
- The packet header field contains typical layer 2 features, address, packet type, flow and error control and checksum. The 3-bit active member address represents the active address of a slave.
- Link Manager Protocol:
 - LMP manages various aspects of the radio link between a master and a slave and the current parameter setting of the devices.
 - LMP enhances baseband functionality, but higher layers can still directly access the baseband. The following groups of functions are covered by the LMP:
 - * Authentication, pairing and encryption
 - * Synchronization
 - * capability negotiation
 - * quality of service negotiation
 - * power control
 - * Link supervision
 - * State and transmission mode change
 - A device wants to establish a piconet: A user of the device wants to scan for other devices in the radio range. The device starts the inquiry procedure by sending an inquiry access code (IAC) that is common to all Bluetooth devices.
 - Devices in Standby that listen periodically: devices in standby may enter the Inquiry mode periodically to search for IAC messages. When the device connected to the master then it becomes slave. If the inquiry was successful, a device enters the page mode. During the page state two roles are defined. After finding all required devices the master is able to set up connections to each device, i.e. setting up a piconet.
 - To save battery power, a Bluetooth device can go into one of three low power states:
 - ① Sniff State: it has the highest power consumption of the low power state. Here, the device listens to the piconet at a reduced rate.
 - ② Hold State: The device does not release its AMA (active member address) but stops asynchronous connectionless link (ACL) transmission. A slave may still exchange SCO packets.
 - ③ Park State: in this state the device has the lowest duty cycle and the lowest power consumption. The device releases its AMA and receives a parked member address (PMA).

L2CAP (Logical link control and adaptation protocol)

It is a data link control protocol on top of the baseband layer offering logical channels between Bluetooth devices with QoS properties. It is available for ACLs only.

→ It provides three different types of logical channels that are transported via the ACL between master and slave.

- ① connectionless (unidirectional channels are used)
- ② connection-oriented (each channel is bidirectional)
- ③ Signaling (exchange signaling messages)

→ Each channel is identified by its channel identifier (CID).

Security The main security features offered by Bluetooth include a challenge-response routine for authentication, a stream cipher for encryption and a session key generation.

→ Each connection may require a one-way, two-way or no authentication using challenge-response routines.

→ All these schemes have to be implemented in silicon.

→ The security algorithms use the public identity of a device, a secret private user key and a random key as input parameter.

→ The first step needed is pairing among two BT devices if they have never met before. It requires a secret PIN into both devices. This PIN can have a length of upto 16 bytes.

SDP (Service discovery protocol)

→ Bluetooth devices should work together with other devices in unknown environments in an ad-hoc fashion. It is essential to know what devices or more specifically what services are available in radio proximity.

→ To find new services, Bluetooth defined the service discovery protocol. SDP describes only the discovery of services, not their usage.

→ All the information an SDP server has about a service is contained in a service record. This consists of a list of service attributes and is identified by a 32-bit service record handle. SDP does not inform clients of any added or removed services. There is no service access control or service brokerage. A service attribute consists of an attribute ID and an attribute value.

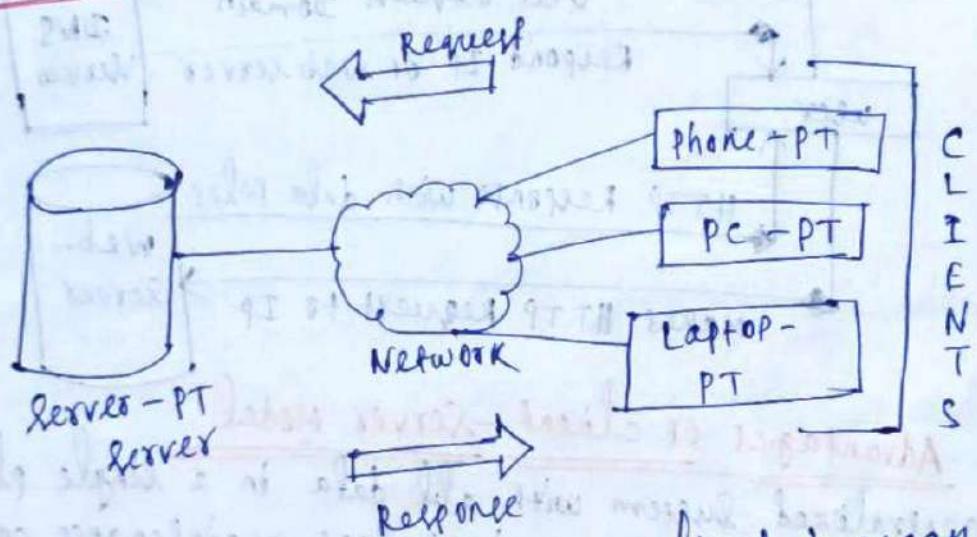
Introduction to Mobile development Framework

C/S Architecture : (client - Server Architecture)

- The client-server architecture is a distributed application structure that partitions task or workload between the providers of a resource or service, called servers, and service requesters called clients.
- In the client-server architecture, when the client computer sends a request for data to the server through the internet, the server accepts the requested process and delivers the data packets requested back to the client.
- Clients do not share any of their resources. Examples of client-server Model are Email, WWW etc.

Working of Client-Server Model

CPT - protocol type



Client: when we talk the word client, it mean to talk of a person or an organization using a particular service.

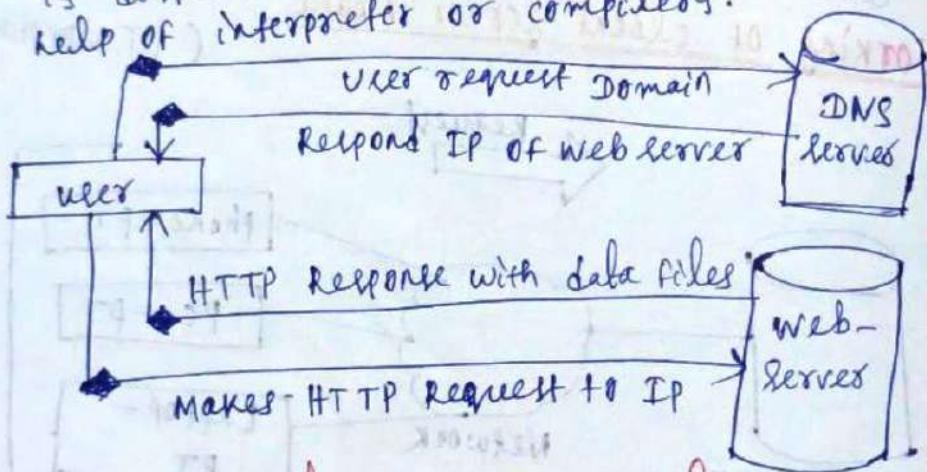
→ Similarly in the digital world a client is a computer (Host) i.e. capable of receiving information or using a particular service from the service providers (servers).

→ Servers: Similarly, when we talk the word servers, it mean a person or medium that serves something. Similarly in this digital world a server is a remote computer which provides

information (data) or access to particular services.
→ So, it's basically the client requesting something and the server serving it as long as it's present in the database.

Steps to interact Server with clients :

- user enters the URL (uniform resource locator) of the website or file. The browser then requests the DNS (Domain name system) server.
- DNS server lookup for the address of the web server.
- DNS server lookup for the address of the webserver.
- DNS server responds with the IP address of the web server.
- server sends over the necessary files of the website.
- Browser then renders the files and the website is displayed. This rendering is done with the help of interpreter or compilers.



Advantages of Client-Server Model:

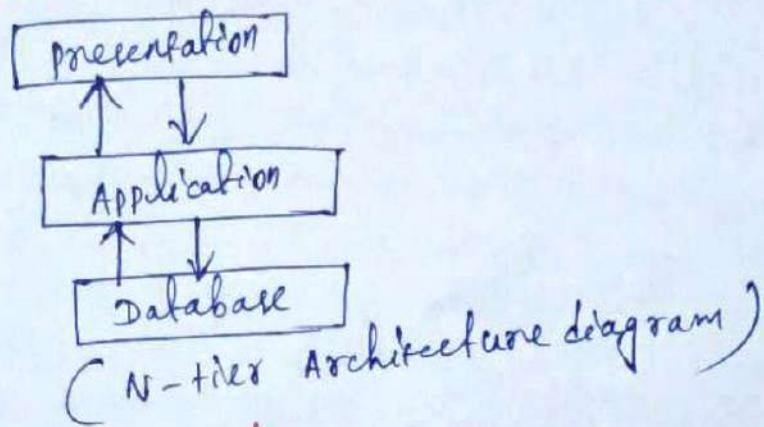
- centralized system with all data in a single place.
- cost efficient, requires less maintenance cost and data recovery is possible.
- The capacity of the client and servers can be changed separately.

Disadvantages:

- clients are prone to viruses.
- servers are prone to Denial of Service (DoS) attacks.
- Data packets may be modified during transmission.
- capturing login credentials or other useful information of the user are common and MITM (Man in the Middle) attacks are common.

N-TIER ARCHITECTURE

- An n-tier architecture application program is one that is distributed among three or more separate computers in a distributed network.
- The most-common form of n-tier is the 3-tier application, and it is classified into three categories.
- In N-tier, N refers to a number of tiers or layers are being used like 2-tier, 3-tier or n-tier, etc. It is also called "Multi-Tier architecture."



WWW (World Wide Web)

- The World wide web, or web for short, are the pages we see when we are at a device and online.
- But the internet is the network of connected computers that the web works on.
- The WWW is a network of online content that is formatted in HTML and accessed via HTTP.
- The term refers to all the interlinked HTML pages that can be accessed over the internet.
- WWW is an information system where documents and other web sources are identified by URLs (such as `http:// google.com`), which may be interlinked by hypertext, and are accessible over the internet.

WWW Architecture :

Wireless Telecom networks Rest part

IS-95: Interim Standard 95 (IS-95) was the first ever CDMA-based digital cellular technology.

→ It was developed by Qualcomm and later adopted as a standard by the telecommunications Industry Association published in 1995.

→ The proprietary name for IS-95 is cdmaOne.

→ It is a 2G mobile telecommunications standard that uses CDMA, a multiple access scheme for digital radio, to send voice, data and signaling data between mobile telephones and cell sites.

→ CDMA or "Code division multiple access" is a digital radio system that transmits stream of bits (PN codes). CDMA permits several radios to share the same frequencies.

→ Unlike TDMA, a competing system used in 2G GSM, all radios can be active all the time, because network capacity does not directly limit the number of active radios.

→ IS-95 defines the transmission of signals in both the forward (network-to-mobile) and reverse (mobile-to-network) directions.

→ In the forward direction, radio signals are transmitted by base stations (BTS). Every BTS is synchronized with a GPS receiver so transmissions are tightly controlled in time.

→ For the reverse direction, radio signals are transmitted by the mobile.

CDMA-2000: CDMA2000 is a code division multiple access (CDMA) of IMT-2000 specifications developed by International Telecomm. Union (ITU).

→ CDMA2000 is a family of technology for 3G mobile cellular communications for transmissions of voice, data and signals.

→ It supports mobile communications at speed between 144 kbps and 2Mbps.

- It applies multi-carrier modulation techniques to 3G networks. This gives higher data rate, greater bandwidth and better voice quality. It is also backward compatible with older CDMA versions.
- It has multi-mode, multi-band roaming features.
- CDMA 2000 compared to UMTS, a competing set of 3G standards, which is developed by 3GPP and used in Europe, Japan and China.

W-CDMA Wideband code division Multiple Access

(W-CDMA) is a third-generation (3G) standard that employs the direct-sequence CDMA channel access method and the FDD method to provide high-speed and high-capacity service.

→ WCDMA is the most commonly used variant of the Universal mobile telecommunications system (UMTS).

→ It was developed by Japan's NTT DOCOMO.

→ WCDMA features two modes:

* Frequency division Duplex (FDD): Separates users by employing both codes as well as frequencies. One frequency is used for the uplink, while another is used for the downlink.

* Time division Duplex (TDD): Separates users by employing codes, frequencies and time, where in the same frequency is used for both uplink and downlink.

→ Although WCDMA is designed to operate on evolved GSM core networks, it uses CDMA for its air interface.

→ The TDD mode of WCDMA actually employs a combination of TDMA and CDMA.

Wireless sensor networks:

→ Wireless sensor networks (WSNs) can be defined as a self-configured and infrastructure-less wireless networks to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion to cooperatively pass their data through the network to a main location or sink where the data can be observed and analyzed.

→ A sink or base station acts like an interface between users and the network.

UBIQUITOUS Wireless Transmission

Introduction To achieve the goal of ubiquitous communication, a universal platform is necessary to connect all the network facilities and make them communicate together.

→ The transmission of radio on fibre (ROF) has been realized as an attractive means to reach this target.

Scenario of Mobile communication :

- The different types of mobile communication systems are a mobile two-way radio, public land radio, mobile telephone radio.
- Mobile two-way radios are one-to-many communication systems that operate in half-duplex mode, i.e. push to talk.
- Mobile communication is the use of technology that allows us to communicate with others in different locations without the use of any physical connection (wires or cables).
- Mobile two-way communications uses the frequency range 26-27.1 MHz and having no channels of 10 kHz.
- It uses Amplitude modulation.
- Public land mobile radio is a two way FM radio system, used in police, fire and municipal agencies. It is limited to small geographical areas.
- Mobile telephones offer full-duplex transmission. These are one-to-one systems that permit two simultaneous transmissions.

Mobile communication Generations 1G to 3G

cellular concepts: The advent of cellular operations brought frequency reuse capabilities, advances in wireless access, DSP, integrated circuits, increased battery life, which leads to exponential growth in personal communication services.

→ The cellular system works as follows: An available frequency spectrum is divided into discrete channels, which are assigned in groups to geographic cells covering a service area.

→ The service area is allotted a radio frequency (RF) transmitter, whereas adjacent cells operate on different frequencies to avoid interference.

1G (1st Generation) cellular phone

→ Analog cellular systems fall in the first-generation (1G) category.

→ In 1970, Bell Labs in New Jersey proposed a cellular telephone concept as advanced mobile telephony system (AMPS).

→ AMPS is a standard cellular telephone service placed into operation on October 13, 1983, by Bell.

→ It uses narrow-band FM with a usable audio frequency band of 300-3 kHz and maximum frequency deviation of ± 12 kHz for 100% modulation.

→ AMPS uses FDMA, where transmissions are separated in the frequency domain.

→ Subscribers are assigned a pair of voice channels (forward and reverse) for the duration of their call. It uses BFSK.

2G (2nd Generation)

→ 2G is short for second-generation cellular network.

→ It was commercially launched on the GSM standard in Finland by Radiolinja.

→ Three benefits of 2G networks over its predecessors are:

* Digitally encrypted phone conversations at least between the mobile phone and the cellular base station but not necessarily in the rest of the network.

- * significantly more efficient use of the radio frequency spectrum enabling more users per frequency band.
 - * Data services for mobile, starting with SMS text messages.
- 2G technologies enabled the various networks to provide the services such as text messages, picture messages, and MMS.
- Radio signals on 2G networks are digital.
- With GPRS (General packet radio service), 2G offers a theoretical maximum transfer speed of 110 Kbit/s.
- With Edge (enhanced data rates for GSM evolution), there is a theoretical max^m speed of 284 Kbit/s.
- The most common 2G technology was the TDMA based GSM, originally from Europe.

3G Technology:

- 3G technology was launched by NTT DOCOMO, Japan in 2001. It was widely launched commercially on W-CDMA standard which is based on GSM.
- At the same time UMTS network spread 3G technology under 3GPP standards in European countries.
- 3G provided faster data-transmission speeds so facsimile line video calling came into feature.
- The max speed of 3G was estimated to be around 2Mbps for non-moving devices and 384 Kbps in moving vehicles.
- The theoretical max speed is 21.6 Mbps.
- It enabled smartphones to provide faster communication, send/receive large emails and texts, provide fast web browsing, video streaming and more security among others.

- It was widely based on CDMA 2000 and EDGE technologies.
- The main distinction between 2G and 3G that allowed media streaming to take place is that 3G utilizes packet switching data transmission rather than circuit switching.
- Data is broken down into small pieces or packets and then sent to the destination.
- Using this method of transmission greatly increases the speed, allowing one to send data through multiple channels in parallel rather than one channel in series.
- 3G changed the course of wireless communication services where in addition to voice telephony and SMS services, data services increased in use.
- 3G technology provides better voice quality and better connectivity due to broad ~~bandwidth~~ ^{internet} ~~bandwidth~~ PC bandwidth.
- 3G uses better encrypting/encoding techniques used to transmit data added a better data security.
- 3G devices became smaller in size and also battery life improved with better frequency and encoding technique.
- 3G networks could handle the first smartphones offering increased bandwidth and transfer rates to accommodate internet applications and audio and video files.

MOBILE IP

Mobile IP (Internet protocol) enables the transfer of information to and from mobile computers, such as laptops and wireless communications. The mobile computer can change its location to a foreign network and still access and communicate with ~~the~~ and through the mobile computer's home network.

- Mobile IP enables routing of IP datagrams to mobile nodes. The mobile node's home address always identifies the mobile node, regardless of its current point of attachment to the internet or an organization's network.

WORKING WITH MOBILE IP :

The mobile node's home address always identifies the mobile node, regardless of its current point of attachment to the internet or an organization's network.

- When away from home, a care-of address associates the mobile node with its home address by providing information about the mobile node's current point of attachment to the internet or an organization's network.
- Mobile IP uses a registration mechanism to register the care-of address with a home agent.
- The home agent redirects datagrams from the home network to the care-of address by constructing a new IP header that contains the mobile node's care of address as the destination IP address.
- This new header then encapsulates the original IP datagram, causing the mobile node's home address to have no effect on the encapsulated datagram's routing until it arrives at the care-of address. This type of encapsulation is also called tunneling.

→ After arriving at the care-of address, each datagram is de-encapsulated and then delivered to the mobile node.

→ IP address stands for Internet protocol address, it is an identifying number that is associated with a specific computer or computers network, when connected to the internet, the IP address allows the computers to send and receive information.

→ 192.168.0.0 is the beginning of the private IP address range that includes all IP addresses through 192.168.255.255. This IP address is usually not used on a network.

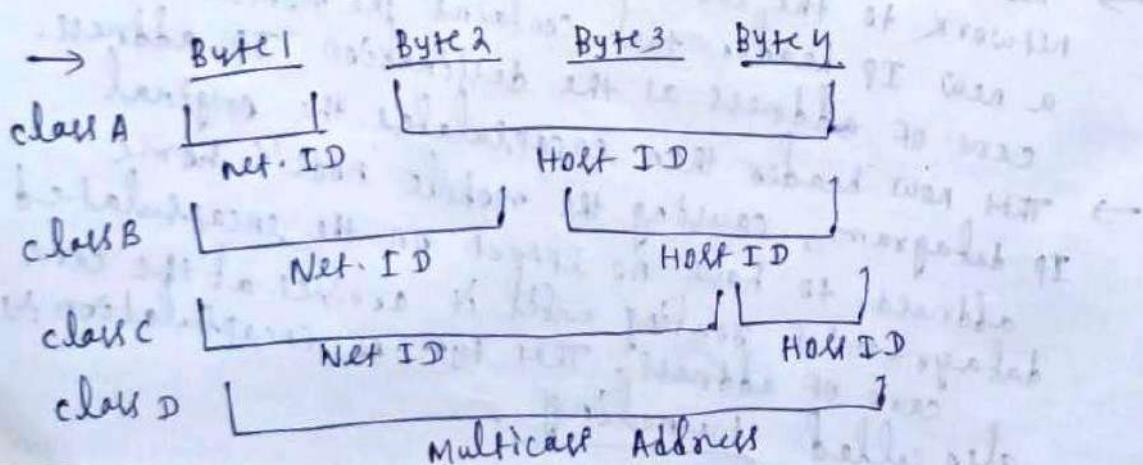
→ An IP address is a 32-bit number that uniquely identifies a host (computer or other device, such as a printer or router) on a TCP/IP network.

→ IP addresses are normally expressed in dotted-decimal format, with four numbers separated by periods, such as 192.168.123.132.

→ For example, the dotted-decimal IP address 192.168.123.132 is (in binary notation) the 32-bit number.

→ IP address is a 32-bit address and separated into 4 parts each part carries 8 bits and they are separated by periods, known as dotted decimal notation.

→ 192.168.1.20
↓
Network part → Host part



class A	Network	Host	Host	Host
Subnet Mask	255	0	0	0
class B	Network	Network	Host	Host
Subnet Mask	255	255	0	0
class C	Network	Network	Network	Host
Subnet Mask	255	255	255	0

- A subnet mask is a 32-bit number created by setting host bits to all 0's and setting network bits to all 1's.
- In this way, the subnet mask separates the IP address into the network and host addresses.
- The "255" address is always assigned to a broadcast address, and the "0" address is always assigned to a network address.

Mobile IP entities :

Mobile IP introduces the following new functional entities :

Mobile Node (MN) : Host or router that changes its point of attachment from one network to another.

Home Agent (HA) : Router on a mobile node's home network that intercepts datagrams destined for the mobile node, and delivers them through the care-of address. The Home agent also maintains current location information for the mobile node.

Foreign Agent (FA) : Router on a mobile node's visited network that provides routing services to the mobile node while the mobile node is registered.

Correspondent node (CN) : At least one partner is needed for communication. In the following the CN represents this partner for the MN. The CN can be a fixed or mobile node.

Core-of Address (COA): The COA defines the current location of the MN from an IP point of view. All IP packets sent to the MN are delivered to the COA, not directly to the IP address of the MN. packet delivery toward the MN ~~is~~ is done using a tunnel, i.e. the COA marks the tunnel endpoint, the address where the packets exit the tunnel. There are two different possibilities for the location of the COA:

Foreign Agent (COA): The COA could be located at the FA i.e., the COA is an IP address of the FA. The FA is the tunnel end-point and forward packets to the MN.

co-located COA: The COA is co-related if the MN temporarily acquired an additional IP address which acts as COA. This address is now ~~not~~ topologically correct, and the tunnel endpoint is at the MN. Co-located can be acquired using services such as DHCP.

IPv4

32-bit logical address / 4 octet
value 0 - 255

IP address \rightarrow Network ID + Host ID

Ex: 192.168.39.240

Class A: 20.100.200.15

Class B: 195.160.20.255

classes Class A \rightarrow 1.0.0.0 to 126.0.0.0

Class B \rightarrow 128.0.0.0 to 191.255.0.0

Class C \rightarrow 192.0.0.0 to 223.255.255.0

{ Class D \rightarrow 224-239 (Multicast) }

{ Class E \rightarrow 240-255 (Reserv) }

Class A is used for large network.

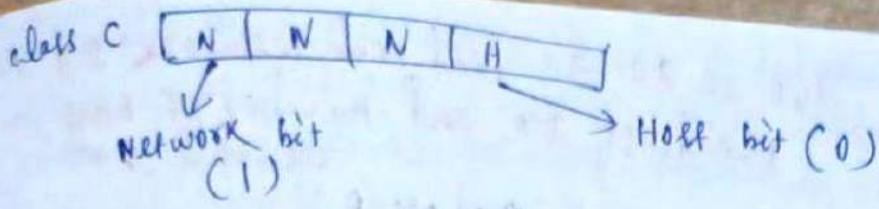
127 is used for special purpose and that is used as Loop back address (127.0.0.0)

Class A

N	H	H	H
---	---	---	---

Class B

N	N	H	H
---	---	---	---



- Ex
- 115.10.0.15 (class A)
 - 115.0.0.0 (Network ID)
 - 196.10.10.10 (class C)
 - 196.10.10.0 ~~196.10.10.0~~ (Network ID)
 - 150.10.0.0 (class B)
 - 150.10.0.0 ~~150.10.0.0~~ (Network ID)

Subnet Mask

115.10.10.20 (class A)

↓ ↓ ↓ ↓
N H H H

(8 bits reserved for network ID)

11111111 00000000 00000000 00000000 (Subnet Mask)

↓ ↓ ↓ ↓
255 0 0 0 (Subnet Mask)

160.10.20.10 (class B)

11111111 11111111 00000000 00000000 (Subnet Mask)

↓ ↓ ↓ ↓
255 255 0 0 (Subnet Mask)

Ex 192.168.37.200 (convert this IP address to binary)

2 ⁷	2 ⁶	2 ⁵	2 ⁴	2 ³	2 ²	2 ¹	2 ⁰
128	64	32	16	8	4	2	1

11000000 10101000 00100101 11001000

Private IP class A : 10.0.0.0

class B : 172.16.X.X
172.31.X.X

class C : 192.168.0.0 to 192.168.255.255

Public IP addresses need to be purchased but private IP not.

Example 150.10.20.30 find out Network ID ?
Broadcast ID and number of host
usable ?

150.10.20.30 (Class B)

150.10.0.0 (Network ID)

150.10.255.255 (Broadcast ID)

Number usable Host :

(16 bits R for Host here), ~~2~~ $2^{16} - 2 = 65,534$ IP

2 IPs are used for special purpose

one is for network ID and
another is for broadcast ID.

Example : 11.200.200.200 (find out Network
ID, broadcast ID and usable
Host)

11.200.200.200

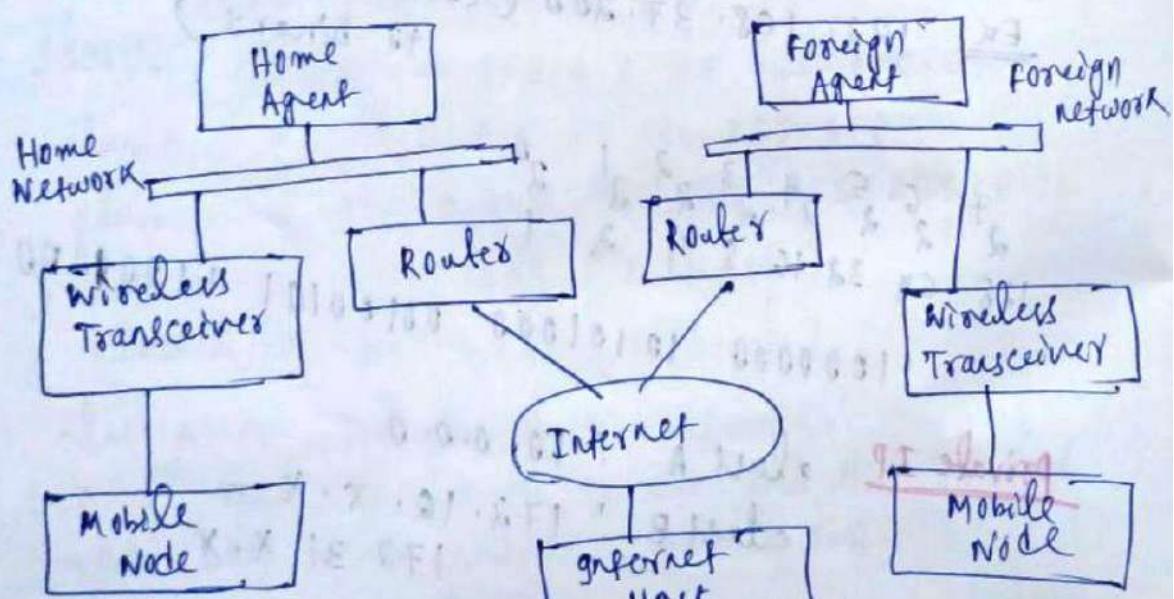
11.0.0.0 (Network ID)

11.255.255.255 (Broadcast ID)

Number of usable Host :

$$2^{24} - 2 = 16,777,214$$

Mobile IP



(mobile IP topology)

First of all, the internet host sends a datagram to the mobile node using the mobile node's home address (normal IP routing process).

- If the mobile node (MN) is on its home network, the normal IP process to the mobile node. Otherwise, the home agent picks up the datagram.
 - If the mobile node is on foreign network, the HA forwards the datagram to the FA.
 - The FA delivers the datagram to the MN.
 - Datagrams from the MN to the internet host are sent using normal IP routing procedures.
- If the MN is on a foreign network, the packets are delivered to the FA. The FA forwards the datagram to the internet host.
- In the case of wireless communications, the above illustrations depict the use of wireless transceivers to transmit the datagrams to the MN. Also, all datagrams between the internet host and the MN use the MN's home address regardless of whether the MN is on a home or foreign network.
 - The Care-Of-Address (COA) is used only for communication with mobility agents and is never seen by the internet host.

① Mobile Node: The mobile node is an end system or device such as a cell phone, PDA or laptop whose fw enables network roaming capabilities.

② Home Agent (HA): The HA provides several services for the mobile node and is located in the home network. The tunnel for packets towards the MN starts at home agent.

→ The HA maintains a location registry, i.e. it is informed of the MN's location by the current COA (care of address).

→ The HA can be implemented on a router that is responsible for the home network.

→ If changing the router's fw is not possible, the home agent could also be implemented on an arbitrary node in the subnet.

- ③ Foreign Agent (FA) The FA can provide several services to the MN during its visit to the foreign network. The FA can have the COA acting as a tunnel endpoint and forwarding packets to the MN. The foreign agent can be the default router for the MN.
→ Foreign agent can also provide security services because they belong to the foreign network as opposed to the MN which is only visiting.

- ④ care of Address (COA)
- The COA defines the current location of the MN from an IP point of view. All IP packets sent to the MN are delivered to the COA, not directly to the IP address of the MN.
→ packet delivery toward the MN is done using a tunnel.
→ To be more precise, the COA marks the endpoint of the tunnel, i.e. the address where packets exit the tunnel.
→ There are two diff. possibilities for the location of the care of address.
- * Foreign Agent COA: The COA could be located at the FA, i.e. the COA is an IP address of the FA.
 - * co-located COA: The COA is co-located if the MN temporarily acquired an additional IP address which acts as a COA.

- ⑤ correspondent node (CN)
- At least one partner is needed for communication. The correspondent node represents this partner for the MN. The correspondent node can be a fixed or mobile node.
- ⑥ Home Network: The home network is the subnet the MN belongs to with respect to its IP address. No mobile IP support is needed within this network.

⑦ Foreign Network The foreign network is the current subnet the MN visits and which is not the home network.

Process of Mobile IP:

The mobile IP process has following 3 main phases which are:

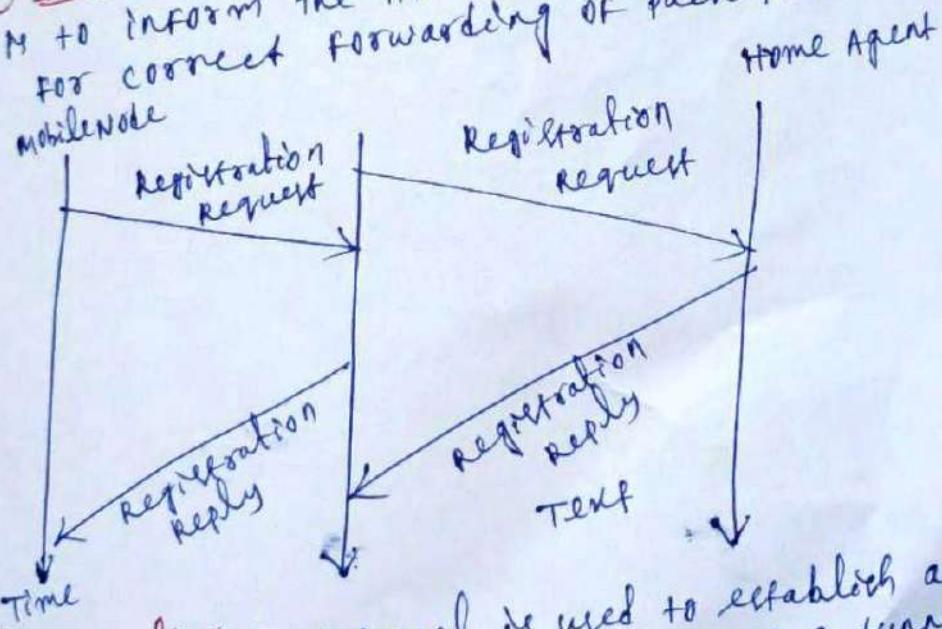
1. Agent Discovery: During the agent discovery phase the HA and FA advertise their services on the network using ICMP router discovery protocol (IRDP).

→ Mobile IP defines two methods.

① Agent advertisement: FA and HA advertise their presence periodically using special agent advertisement messages.

② Agent solicitation: If no agent advertisements are present or the inter arrival time is too high, and as MN has not received a COA, the mobile node must send agent solicitations.

③ Registration: The main purpose of the registration is to inform the HA of the current location for correct forwarding of packets.



④ Tunneling: A tunnel is used to establish a virtual pipe for data packets between a tunnel entry and a tunnel endpoint.

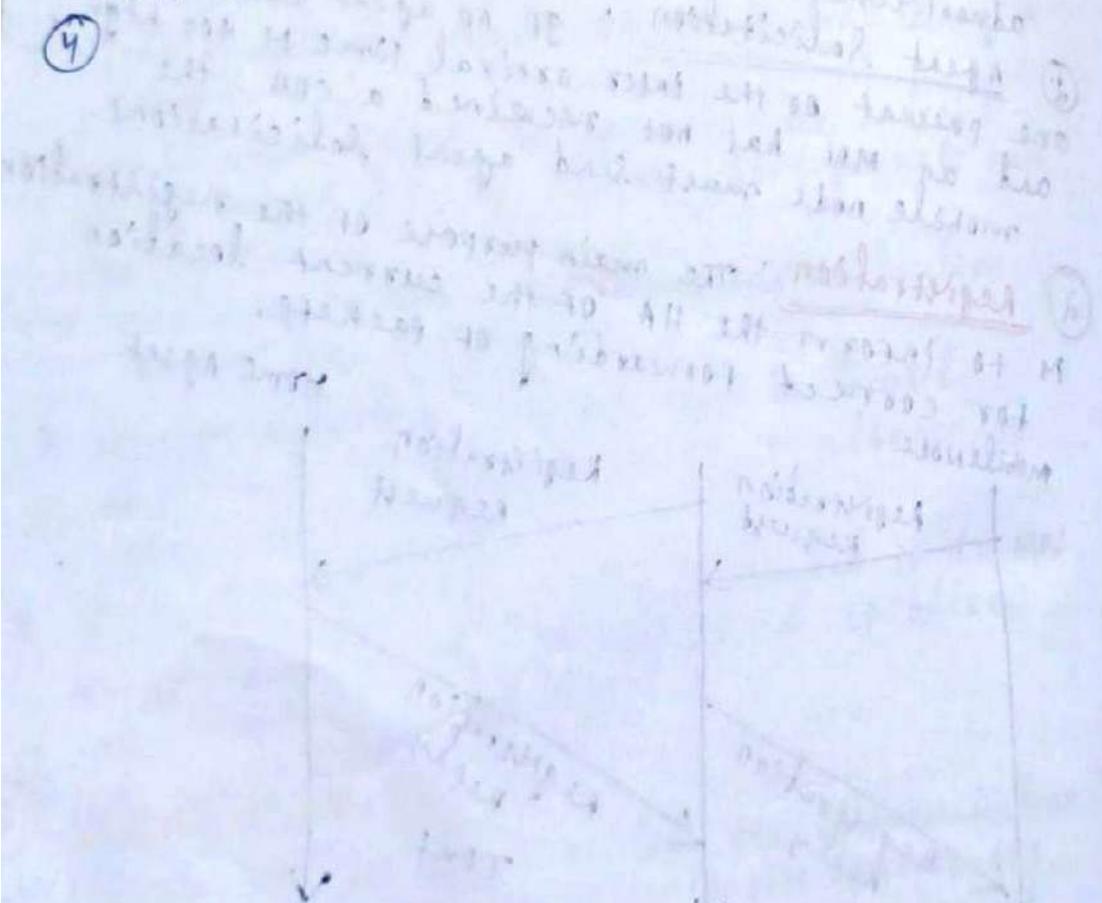
→ Packets which are entering in a tunnel are forwarded inside the tunnel and leave the tunnel unchanged. Tunneling, i.e., sending a packet through a tunnel is achieved with the help of encapsulation.

→ Tunneling is also known as "port forwarding".
is the transmission and data intended for use
only within a private, usually corporate network
through a public network.

IPv6 An IPv6 address is made of 128 bits,
divided into eight 16 bits segments or blocks.

Features

- ① Larger Address Space → approx 34×10^{38}
- ② Simplified Header → 40 byte (8 fields)
- ③ End to end connectivity → no need of NAT (Network address translation), Every host can directly reach each other.
- ④



Many a times it has to direct a packet to a particular host
so that it reaches to the correct host
so here we have to make a rule in the router
which will direct the packet to the correct host
the host to which the packet is directed
will receive the packet.