ANNAI WOMEN'S COLLEGE (ARTS & SCIENCE)

(Affiliated to bharathidasan university, Tiruchirappalli)

PUNNAMCHATRAM , KARUR.

Department of Computer Science

I M.Sc(CS)

MOBILE COMMUNICATION (COURSE MATERIAL)

Prepared by,
Mrs. V. SARANYA, M.Sc., M.Phil.,
Assistant professor
Department of Computer Science & Applications

Mobile Communication

Chapter-I

Introduction:

There are two different kinds of mobility:

- ✓ User mobility
- ✓ Device portability

User mobility:

- User mobility can access to the same or similar telecommunication services at different places.

Device portability:

- The communication device moves (with or without a user).

Characteristics:

1. **Fixed and wired:**
- This configuration describes the typical desktop computer in an office.
- The devices allow for mobile usage.

2. **Mobile and wired:**
- Many of today"s laptops fall into this category .
- Company"s network via the telephone network and a modem.

3. **Fixed and wireless:**
- This mode is used for installing networks.
- In historical buildings to avoid damage by installing wires.

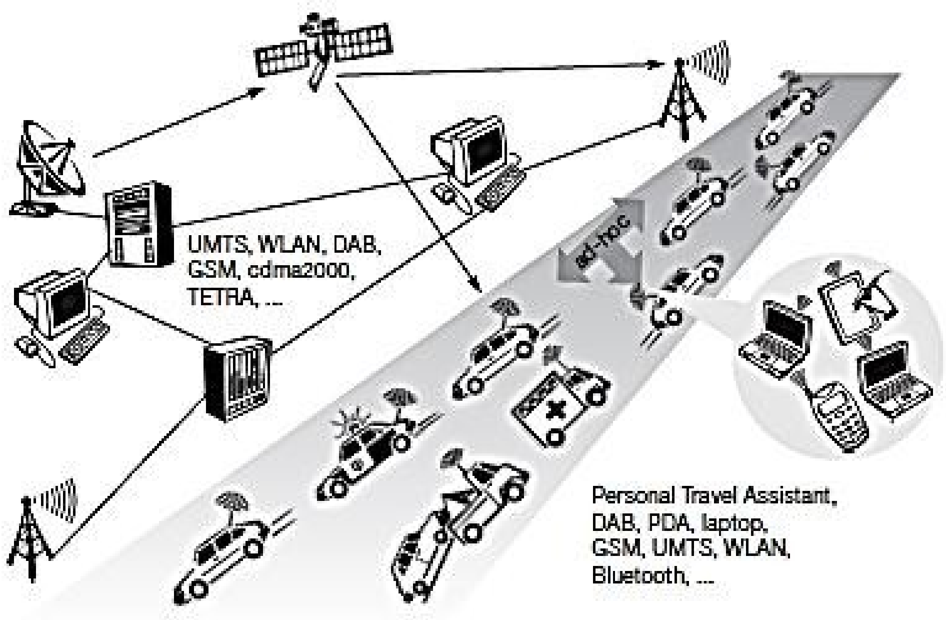
4. **Mobile and wireless:**
- This is the most interesting case.
- No cable restricts the user, who can roam between different wireless networks.

Applications:

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

1. Vehicles:

- Many wireless communication systems and mobility aware applications.
- Music, news, road conditions, weather reports, and other broadcast information are received via digital audio broadcasting (DAB)
- Personal communication, a universal mobile telecommunications system (UMTS).
- The phone might be available offering voice and data connectivity with 384 Kbit/s.
- Remote areas, satellite communication can be used, while the current position of the car is determined via the global positioning system (GPS).

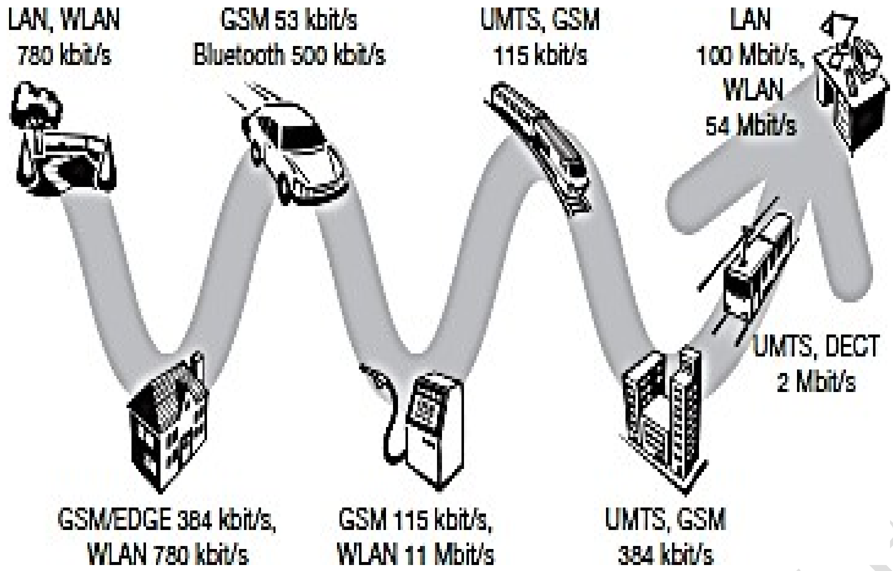


2. Emergencies:

- The possibilities of an ambulance with a high-quality wireless connection to a hospital.
- Vital information about injured persons can be sent to the hospital from the scene of the accident.
- Wireless networks are the only means of communication in the case of natural disasters such as hurricanes or earthquakes.

3. Business:

- A travelling salesman today needs instant access to the company"s database.
- Wireless access, the laptop can be turned into a true mobile office.
- Efficient and powerful synchronization mechanisms are needed to ensure data consistency.



4. Replacement of wired networks:

- Wireless networks can also be used to replace wired networks. (e.g., remote sensors, for tradeshows, or in historic buildings).
- Computer fairs use WLANs as a replacement for cabling.
- Other cases for wireless networks are computers, sensors, or information displays in historical buildings.

5 Infotainment and more:

- Static information might be loaded via CD-ROM, DVD, or even at home via the Internet.
- Wireless networks can provide up-to-date information at any appropriate location.
- Another growing field of wireless network applications lies in entertainment and games.

6. Location dependent services:

- Mobile computing and wireless networks try to hide the fact that the network access has been changed.
- A wireless link is more error prone than a wired one.

Mobile and wireless devices:

- 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.

Categories:

Sensor:

- A very simple wireless device is represented by a sensor transmitting state information.
- A switch sensing the office door.

Embedded controllers:

- Many appliances already contain a simple or some times more complex controller.
- Keyboards, mice, head sets, washing machines, coffee machines, hair dryers.

Pager:

- As a very simple receiver, a pager can only display short text messages, has a tiny display, and cannot send any messages.
- Pagers can even be integrated into watches.

Mobile phones:

- The traditional mobile phone only had a simple black and white text display.
- Send/receive voice or short messages.
- Mobile phones with full color graphic display, touch screen, and Internet browser are easily available.

Personal digital assistant:

- PDAs typically accompany a user and offer simple versions of office software (calendar, note-pad, mail).

Pocket computer:

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

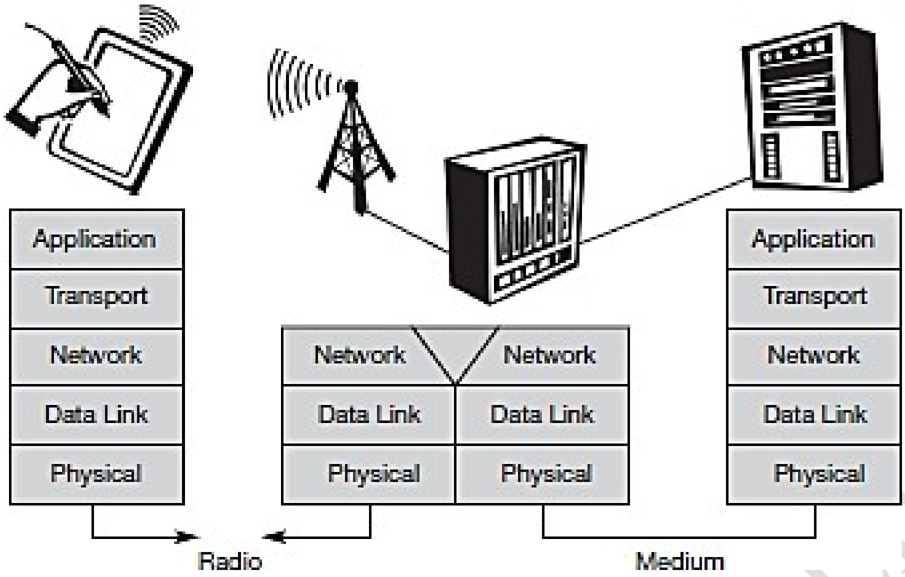
  (Text processing, spreadsheets etc.).

Notebook/laptop:

- The laptops offer more or less the same performance as standard desktop computers.
- They use the same software – the only technical difference being size, weight, and the ability to run on a battery.

A Simplified Reference Model:

- The basic reference model used to structure communication systems.
- A personal digital assistant (PDA) which provides an example for a wireless and portable device.
- This PDA communicates with a base station in the middle of the picture.
- The base station consists of a radio transceiver (sender and receiver) and an interworking unit connecting the wireless link with the fixed link.
- The communication partner of the PDA, a conventional computer, is shown on the right-hand side.



1. **Physical layer:**
- The conversion of a stream of bits into signals that can be transmitted on the sender side.
- The physical layer is responsible for frequency selection, generation of the carrier frequency, signal detection.

2. **Data link layer:**
- This layer include accessing the medium, multiplexing of different data streams.
- Correction of transmission errors, and synchronization.
- The data link layer is responsible for a reliable point-to-point connection.

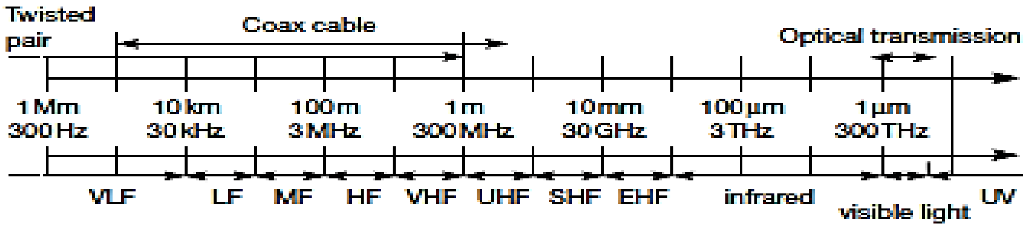
3. **Network layer:**
- This is responsible for routing packets through a network.
- Establishing a connection between two entities over many other intermediate systems.

4. **Transport layer:**
- This layer is used in the reference model to establish an end-to-end connection.
- Transport protocols known from the Internet, TCP and UDP, are to be used over a wireless link.

5. **Application layer:**
- The applications are situated on top of all transmission oriented layers.

Wireless Transmission:

- This is an important topic in wireless transmission.
- The frequencies used for transmission are all regulated basic facts about signals, antennas, and signal propagation.
- The varying propagation characteristics create particular complications for radio transmission.
- Frequently causing transmission errors.



Frequencies for radio transmission:

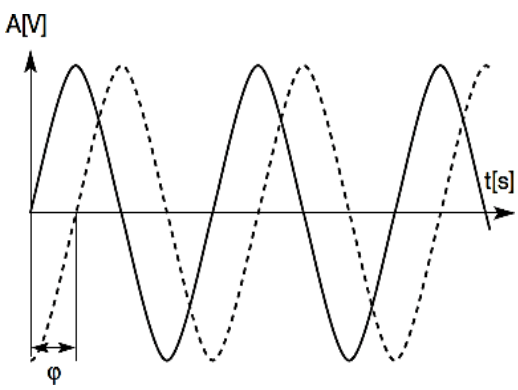
- Radio transmission can take place using many different frequency bands. Each frequency bands.
- Directly coupled to the frequency is the wavelength λ via the equation **λ = c/f**.
- Radio transmission starts at several kHz, the very low frequency (VLF) range.
- These are very long waves. Waves in the low frequency (LF) range are used by submarines.
- The medium frequency (MF) and high frequency (HF) ranges are typical for transmission of hundreds of radio stations.
- Conventional analog TV is transmitted in ranges of 174–230 MHz and 470–790 MHz using the very high frequency (VHF) and ultra-high frequency (UHF) bands.
- In this range, digital audio broadcasting (DAB) takes place as well (223–230 MHz and 1452-1472 MHz) and digital TV is planned or currently being installed analog TV.
- Super high frequencies (SHF) are typically used for directed microwave links.
- The extremely high frequency (EHF) range which comes close to infra-red.

Signals:

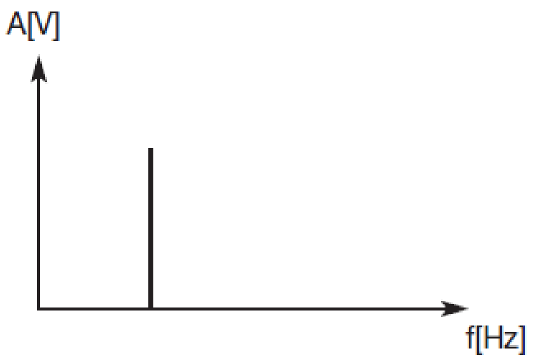
- Signals are the physical representation of data.
- Users of a communication system can only exchange data through the transmission of signals.
- Signals are functions of time and location.
- Signal parameters represent the data values.
- The most interesting types of signals for radio transmission are periodic signals, especially sine waves as carriers.

The general function of sine wave:

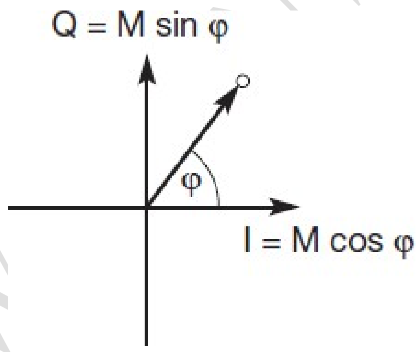
$$g(t) = A_t \sin(2\pi f_t t + \varphi_t)$$



- The amplitude as a factor of the function g may also change over time, thus At,
- The frequency f expresses the periodicity of the signal with the period T = 1/f.
- The phase shift determines the shift of the signal relative to the same signal.
- The representations in the time domain are problematic if a signal consists of many different frequencies better representation of a signal is the **frequency domain.**

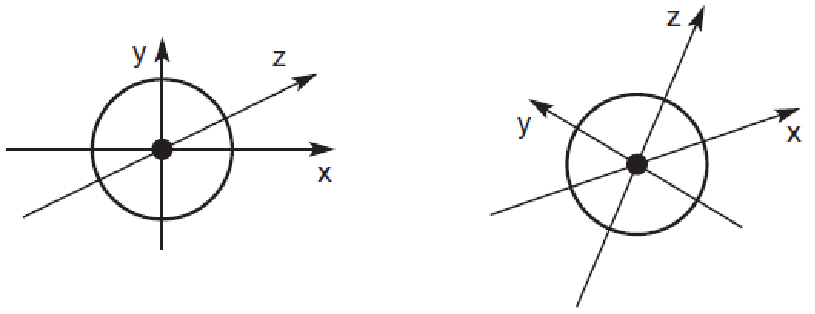


- This representation, also called phase state or signal constellation diagram.
- The length of the vector represents the amplitude.

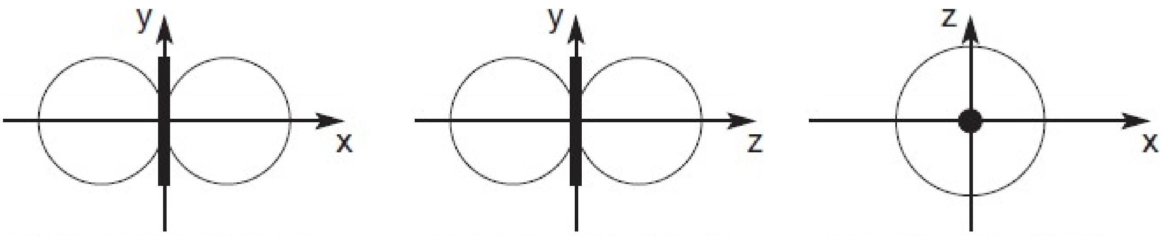


Antennas:

- Antennas couple electromagnetic energy to and from space to and from a wire or coaxial cable.
- The radiation pattern is symmetric in all directions a two dimensional cross-section of the real three-dimensional pattern.

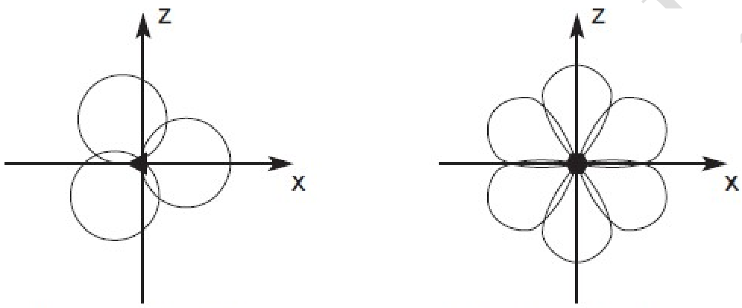


- The intensity of radiation is not the same in all directions from the antenna.
- The uniform or Omni-directional radiation pattern.



Side view (xy-plane) Side view (zy-plane) Top view (xz-plane)

- Directed antennas are typically applied in cellular system can be combined on a single pole to construct a sectorized antenna.



Top view, 3 sector Top view, 6 sector

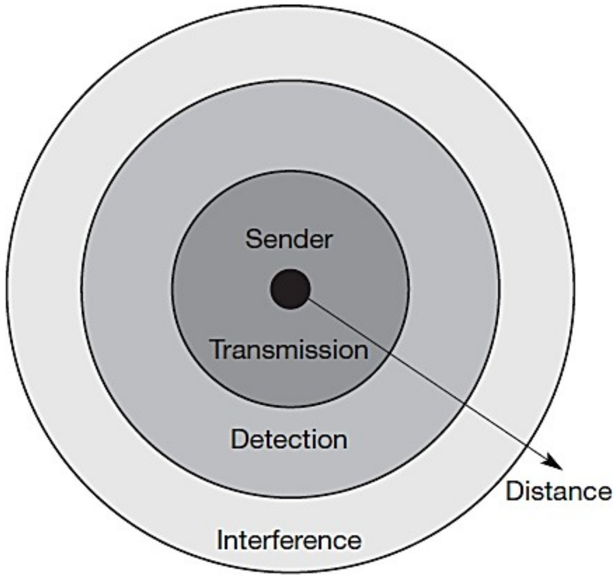
- Two or more antennas can be also being combined to improve reception by countering the negative effects of multi-path propagation.
- These antennas also called "multi-element antenna array".

Different diversity schemes are:

1. Switched diversity
2. Selection diversity

Signal propagation:

- Wired networks, wireless communication networks also have senders and receivers of signals.
- In connection with signal propagation, these two networks exhibit considerable differences.
- Wired networks only travel along the wire can be twisted pair copper wires, a coax cable, but also a fiber optics.



1. **Transmission range:**
   - The signals with an error rate low enough to be able to communicate and can also act as sender.

2. **Detection range:**
   - The transmitted power is large enough to differ from background noise. The error rate is too high to establish communication.

3. **Interference range:**
   - The interfere with other transmission by adding to the background noise.

Path loss of radio signals:

- In free space radio signals propagate as light do they follow a straight line.
- A straight line exists between a sender and a receiver it is called line-of-sight (LOS).
- The surface area s grows with the increasing distance d from the center according to the equation s = 4π d2.
- Most radio transmission takes place through the atmosphere – signals travel through air, rain, snow, fog, dust particles, smog.

Ground wave (<2 MHz):

- Waves with low frequencies follow the earth‟s surface and can propagate long distances.

  These waves are used for, **e.g., submarine communication or AM radio**.

Sky wave (2–30 MHz):

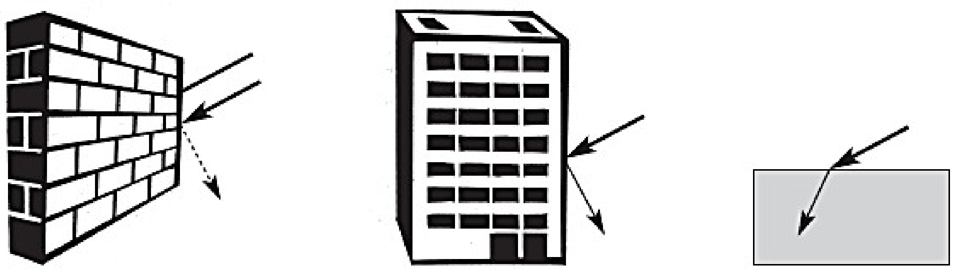
- This way the waves can bounce back and forth between the ionosphere and the earth"ssurface, travelling around the world.

Line-of-sight (>30 MHz):

- Mobile phone systems, satellite systems, cordless telephones.
- Use even higher frequencies.

Additional signal propagation effects:

- Mobile phones are typically used in big cities with skyscrapers, on mountains, inside buildings.
- In addition to the attenuation caused by the distance between sender and receiver.
- An extreme form of attenuation is blocking or shadowing of radio signals due to large obstacles.



Shadowing   Reflection   Refraction

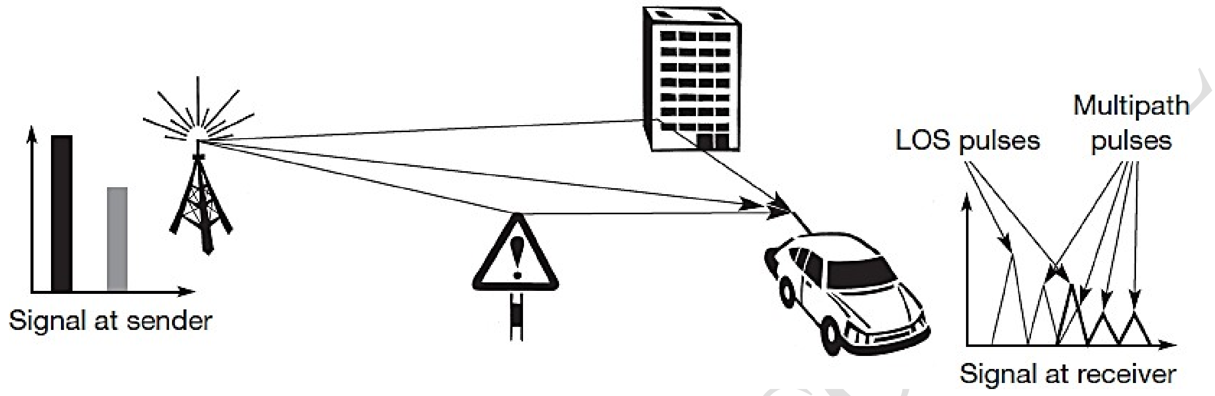
- The reflection of signals as shown in the middle If an object is large compared to the wavelength of the signal.
- The effects of refraction occur because the velocity of the magnetic waves depends on density.
- The medium through which it travels.

Scattering   Diffraction

- The size of an obstacle is in the order of the wave length or less,then waves can be scattered.
- The effect of diffraction very similar to scattering radio waves will be deflected at an edge and propagation.

Multi-path propagation:

- The direct transmission from a sender to a receiver, the propagation effects mentioned in the previous section.
- Lead to one of the most severe radio channel impairments, called multi-path propagation.



- A sender on the left and one possible receiver on the right.
- Radio waves emitted by the sender can either travel along a straight line.
- A large building, or scattered at smaller obstacles.
- Many more paths are possible.
- Signals travelling along different paths with different lengths arrive at the receiver at different times. This effect is called delay spread.

Multiplexing:

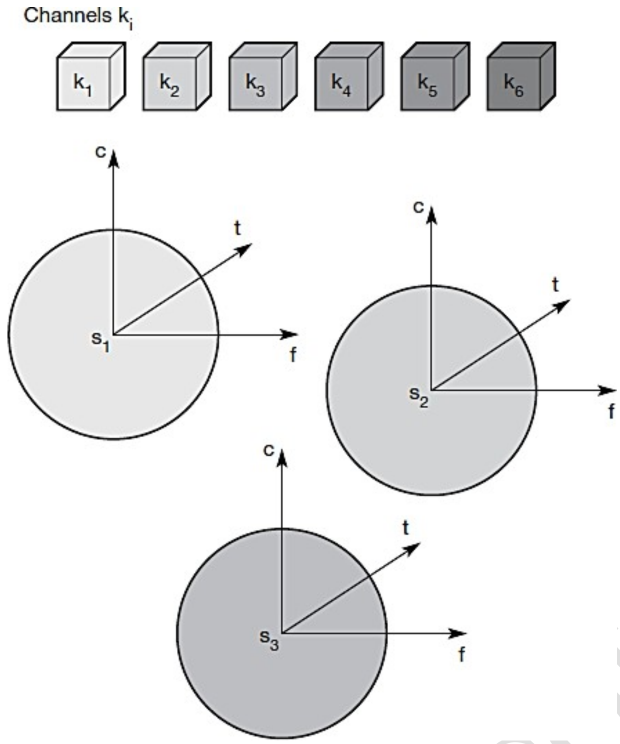
- Multiplexing is not only a fundamental mechanism in communication systems but also in everyday life.
- Multiplexing describes how several users can share a medium with minimum or no interference.

Space division multiplexing:

- Wireless communication, multiplexing can be carried out in four dimensions.

  Space, time, frequency, and code.

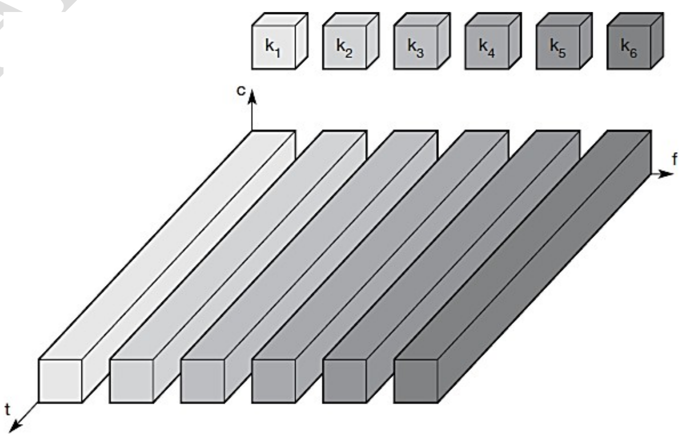
- In this field, the task of multiplexing is to assign space, time, frequency, and code to each communication.
- A minimum of interference and a maximum of medium utilization.



- This first type of multiplexing, space division multiplexing (SDM), the (three dimensional) space si.
- The space is represented via circles indicating the interference range.
- The channels k1 to k3 can be mapped onto the three „spaces" s1 to s3.
- The space between the interference ranges is sometimes called guard space.

Frequency division multiplexing:

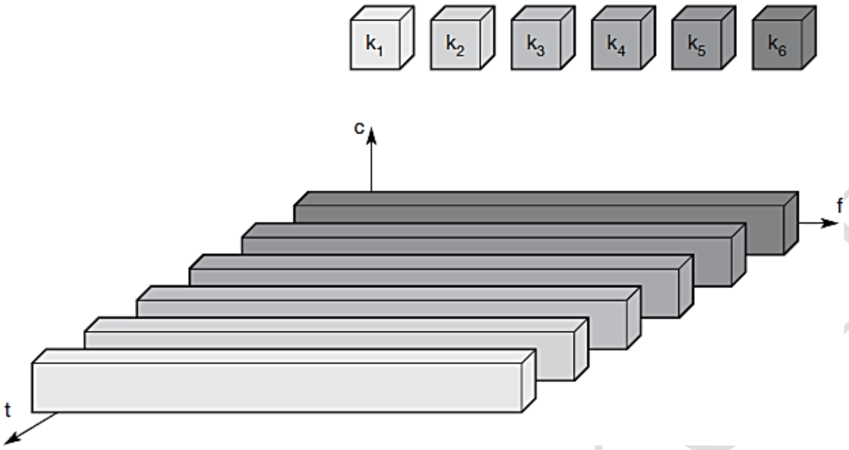
- Frequency division multiplexing (FDM) describes schemes to subdivide the frequency dimension into several non-overlapping frequency bands.
- This very simple multiplexing scheme does not need complex coordination between sender and receiver.



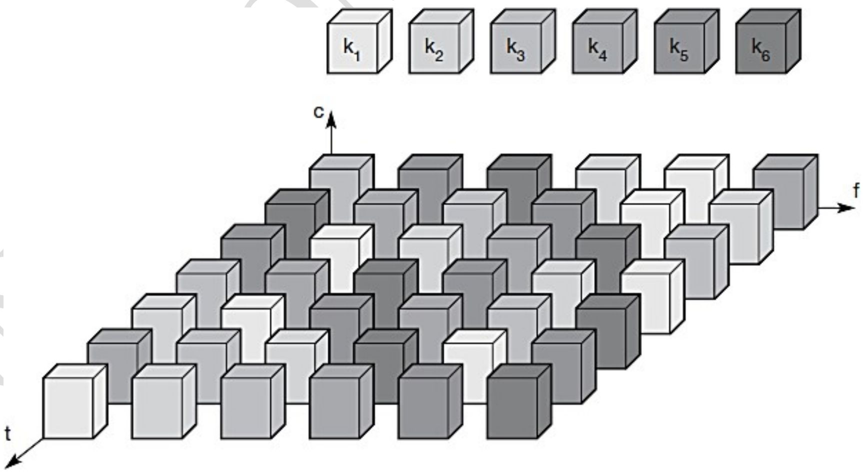
- While radio stations broadcast 24 hours a day, mobile communication typically takes place for only a few minutes at a time.

Time division multiplexing:

- A more flexible multiplexing scheme for typical mobile communications is time division multiplexing (TDM).
- All senders use the same frequency but at different points in time.
- If two transmissions overlap in time, this is called co-channel interference.

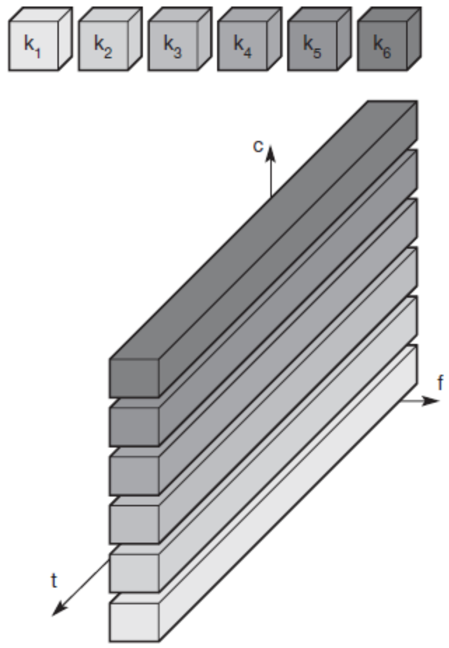


- Frequency and time division multiplexing can be combined.
- The sequence of frequencies and the time of changing to another frequency.



Code division multiplexing:

- The code division multiplexing (CDM) is a relatively new scheme in commercial communication systems.
- It is used in military applications due to its inherent security features spread spectrum techniques.



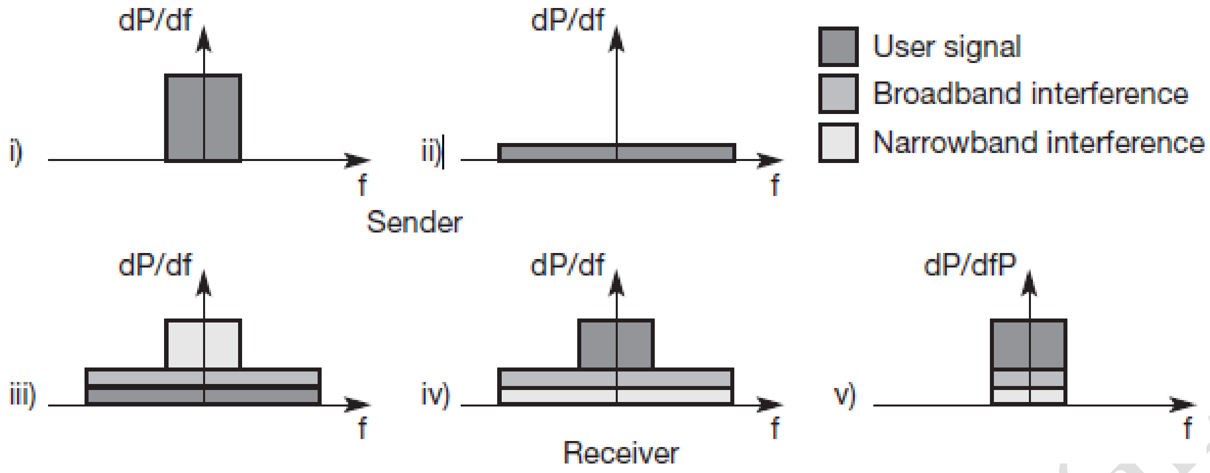
- All channels ki use the same frequency at the same time for transmission.
- The main advantage of CDM for wireless transmission is that it gives good protection against interference and tapping.

Spread spectrum:

- Spread spectrum techniques involve spreading the bandwidth needed to transmit data.

The main advantage is the resistance to narrowband interference.

- Idealized narrowband signal from a sender of user data.
- Converts the narrowband signal into a broadband signal.
- The sum of interference and user signal is received.
- The receiver applies a band pass filter to cut off frequencies left and right of the narrowband signal.
- Spread spectrum helps to deal with narrowband interference for a single channel.



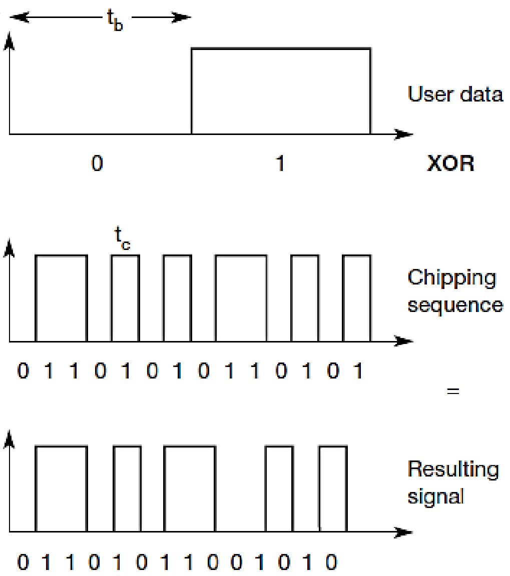
- Spread spectrum technologies also exhibit drawbacks.
- The effect of spread spectrum if a secret code is used for spreading.

Two different ways:

- Direct sequence spread spectrum.
- Frequency hopping spread spectrum.

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.
- The chipping sequence consists of smaller pulses, called chips.
- The chipping sequence is generated properly it appears as random noise. this sequence is also sometimes called pseudo-noise sequence.



- The original signal needs a bandwidth w, the resulting signal needs s·w after spreading.
- The first step in a DSSS transmitter, the spreading of the user data with the chipping sequence.
- The DSSS receiver is more complex than the transmitter.
- The receiver only has to perform the inverse functions of the two transmitter modulation steps.

Frequency hopping spread spectrum:

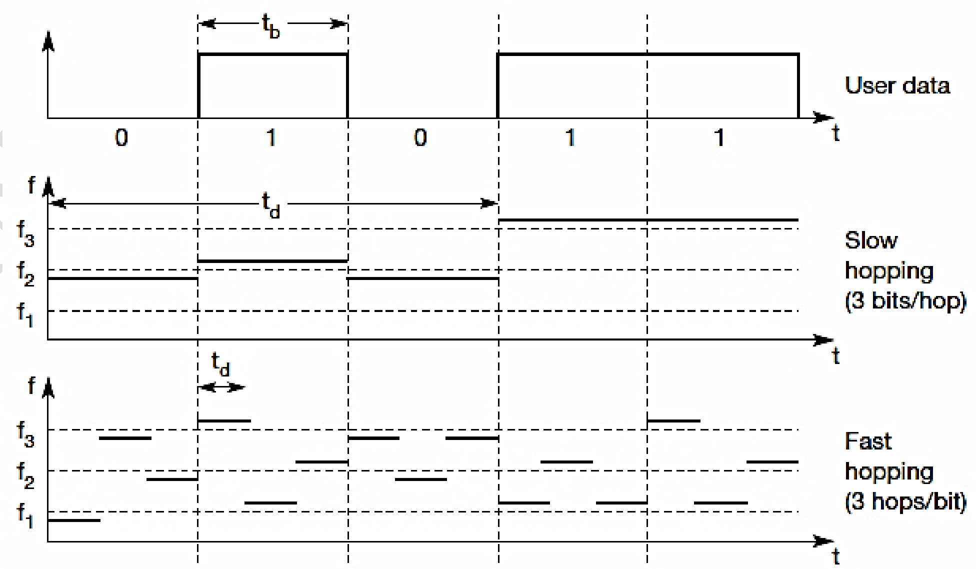
- Frequency hopping spread spectrum (FHSS) systems, the total available bandwidth is split into many channels of smaller bandwidth plus guard spaces between the channels.
- This system implements FDM and TDM.
- The pattern of channel usage is called the hopping sequence.
- The time spend on a channel with a certain frequency is called the dwell time.

FHSS comes in two variants.

- Slow hopping
- Fast hopping

Slow hopping:

- The transmitter uses one frequency for several bit periods.
- Then the transmitter hops to the next frequency f3.
- Slow hopping systems are typically cheaper and have relaxed tolerances.
- They are not as immune to narrowband interference as fast hopping systems.

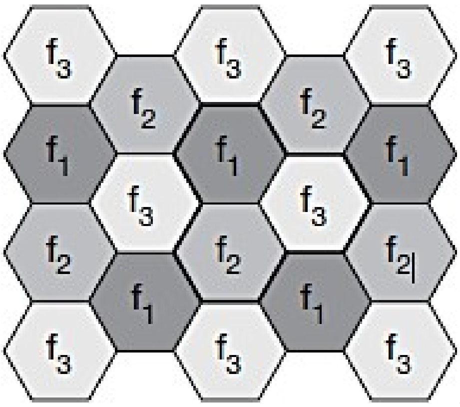


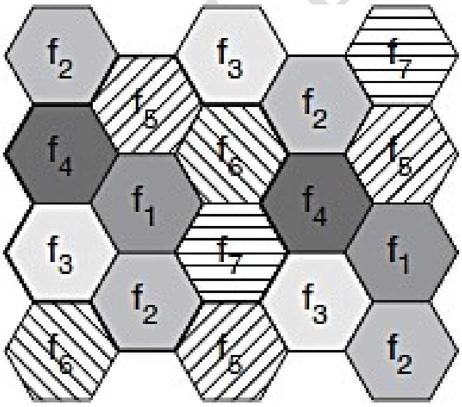
Fast hopping systems:

- The transmitter changes the frequency several times during the transmission of a single bit.
- Fast hopping systems are more complex to implement because the transmitter and receiver have to stay synchronized within smaller tolerances.

Cellular systems:

- Cellular systems for mobile communications implement SDM.
- Each transmitter typically called a base station covers a certain area a cell.
- The shape of cells are never perfect circles or hexagons.
- A mobile station within the cell around a base station communicates with this base station and vice versa.





Advantages:

Higher capacity:

- Implementing SDM allows frequency reuse. If one transmitter is far away from another.
- Outside the interference range, it can reuse the same frequencies.
- This frequency is blocked for other users.
- The number of concurrent users per cell is very limited.

Less transmission power:

- A receiver far away from a base station would need much more transmit power than the current few Watts.

Local interference only:

- Having long distances between sender and receiver results in even more interference problems.
- Small cells mobile stations and base stations only have to deal with „local" interference.

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.

Disadvantages:

Infrastructure needed:

- Cellular systems need a complex infrastructure to connect all base stations.

This includes:

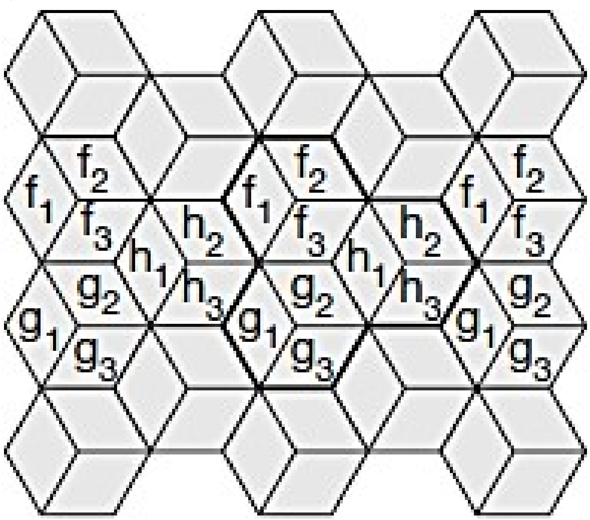
- Many antennas
- Switches for call forwarding.
- Location registers

Handover needed:

- The mobile station has to perform a handover when changing from one cell to another.
- Depending on the cell size and the speed of movement.

Frequency planning:

- To avoid interference between transmitters using the same frequencies, frequencies have to be distributed carefully.
- Interference should be avoided, on the other, only a limited number of frequencies is available.
- To reduce interference even further sectorized antennas can be used.
- The use of three sectors per cell in a cluster with three cells.



- Cells with more traffic are dynamically allotted more frequencies.
- This scheme is known as borrowing channel allocation (BCA).
- The first fixed scheme is called fixed channel allocation (FCA).
- FCA is used in the GSM system as it is much simpler to use, but it requires careful traffic analysis before installation.
- A dynamic channel allocation (DCA) scheme has been implemented in DECT.
- These frequencies can only be borrowed, but it is also possible to freely assign frequencies to cells.
- Cellular systems using CDM instead of FDM do not need such elaborate channel allocation schemes.
- Separated through the code they use, not through the frequency.

Medium access control:

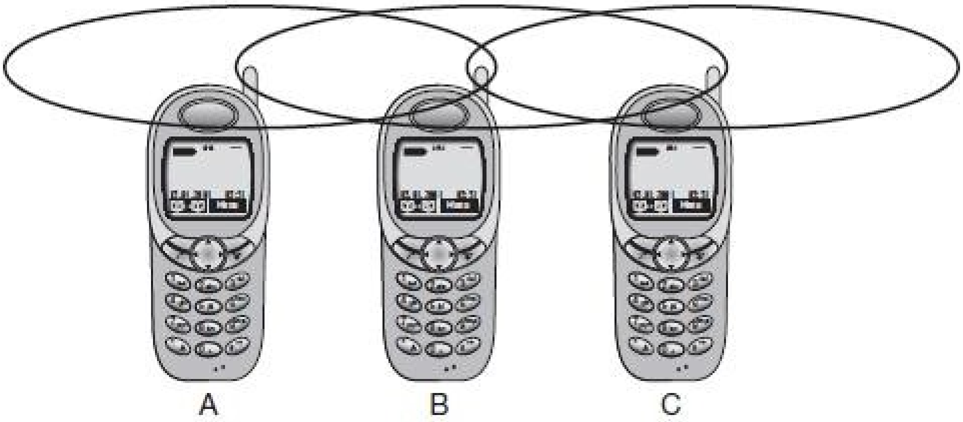
- Medium access control comprises all mechanisms that regulate user access to a medium using SDM, TDM, FDM, or CDM.

Motivation for a specialized MAC:

- The main question in connection with MAC in the wireless is whether.
- It is possible to use elaborated MAC schemes from wired networks.
- CSMA/CD as used in the original specification of IEEE 802.3 networks.
- Consider carrier sense multiple access with collision detection,
- A sender senses the medium (a wire or coaxial cable) to see if it.
- 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.

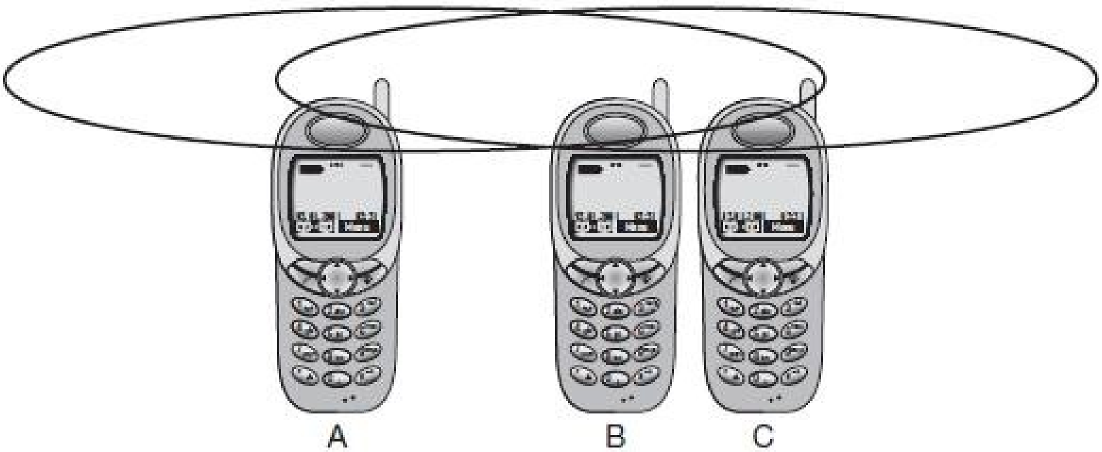
1. Hidden and exposed terminals:

- The transmission range of A reaches B, but not C.
- The transmission range of C reaches B, but not A.
- Finally, then transmission range of B reaches A and C.
- A starts sending to B, C does not receive this transmission.
- C also wants to send.
- B senses the medium.
- The medium appears to be free, the carrier sense fails.
- C also starts sending causing a collision at B.
- But A cannot detect this collision at B and continues with its transmission.
- A is hidden for C.
- A is outside the interference range of C, waiting is not necessary.
- C is exposed to B.



2. **Near and far terminals:**

- 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.
- The near/far effect is a severe problem of wireless networks using CDM.
- All signals should arrive at the receiver with more or less the same strength.



- A person standing closer to somebody could always speak louder than a person further away.

SDMA (Space Division Multiple Access):

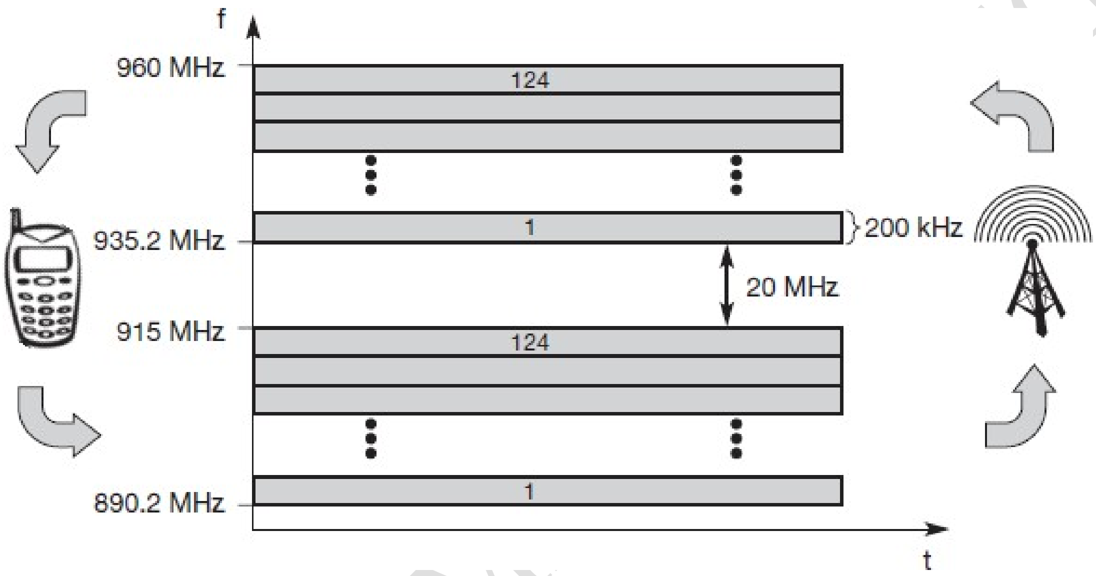
- Space Division Multiple Access (SDMA) is used for allocating a separated space to users in wireless networks.
- A typical application involves assigning an optimal base station to a mobile phone user.
- The mobile phone may receive several base stations with different quality.
- SDMA is never used in isolation but always in combination with one or more other schemes.
- The basis for the SDMA algorithm is formed by cells and sectorized antennas which constitute the infrastructure implementing space division multiplexing (SDM).
- Single users are separated in space by individual beams.

FDMA (Frequency Division Multiple Access):

- Frequency division multiple access (FDMA) comprises all algorithms allocating frequencies to transmission channels according to the frequency division multiplexing (FDM).
- Allocation can either be fixed dynamic.

  (i.e., demand driven).

- Channels can be assigned to the same frequency at all times.
- FDMA combined with TDMA.
- FDM is often used for simultaneous access to the medium by base station and mobile station in cellular networks.



- 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).

There are two frequencies:

- Uplink
- Downlink

Uplink:

- From mobile station to base station or from ground to control satellite.

Downlink:

- From base station to mobile station or from satellite to ground control.

TDMA (Time Division Multiple Access):

- Time division multiple access (TDMA) offers a much more flexible scheme, which comprises all technologies that allocate certain time slots for communication.
- The compared with FDMA.

- The receiver can stay at the same frequency the whole time.
- Only one frequency and thus very simple receiver and transmitter.
- Many different algorithms exist to control medium access.

CDMA (Code Division Multiple Access):

- Code division multiple access (CDMA) systems use exactly these codes to separate different users in
- 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.

Comparison of S/T/F/CDMA:

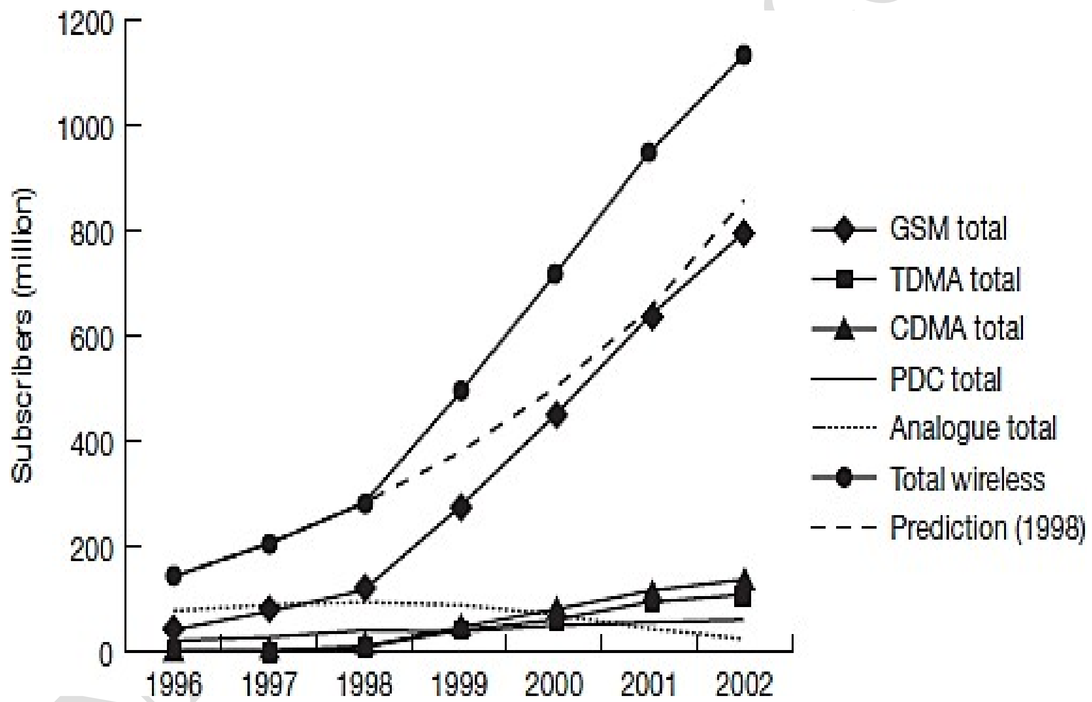
Approach	SDMA	TDMA	FDMA	CDMA
Idea	Segment space into cells/sectors	Segment sending time into disjoint time-slots, demand driven or fixed patterns	Segment the frequency band into disjoint sub-bands	Spread the spectrum using orthogonal codes
Terminals	Only one terminal can be active in one cell/one sector	All terminals are active for short periods of time on the same frequency	Every terminal has its own frequency, uninterrupted	All terminals can be active at the same place at the same moment, uninterrupted
Signal separation	Cell structure directed antennas	Synchronization in the time domain	Filtering in the frequency domain	Code plus special receivers
Advantages	Very simple, increases capacity per km^2	Established, fully digital, very flexible	Simple, established, robust	Flexible, less planning needed, soft handover
Disadvantages	Inflexible, antennas typically fixed	Guard space needed (multi-path propagation), synchronization difficult	Inflexible, frequencies are a scarce resource	Complex receivers, needs more complicated power control for senders
Comment	Only in combination with TDMA, FDMA or CDMA useful	Standard in fixed networks, together with FDMA/SDMA used in many mobile networks	Typically combined with TDMA (frequency hopping patterns) and SDMA (frequency reuse)	Used in many 3G systems, higher complexity, lowered expectations; integrated with TDMA/FDMA

Mobile Communication

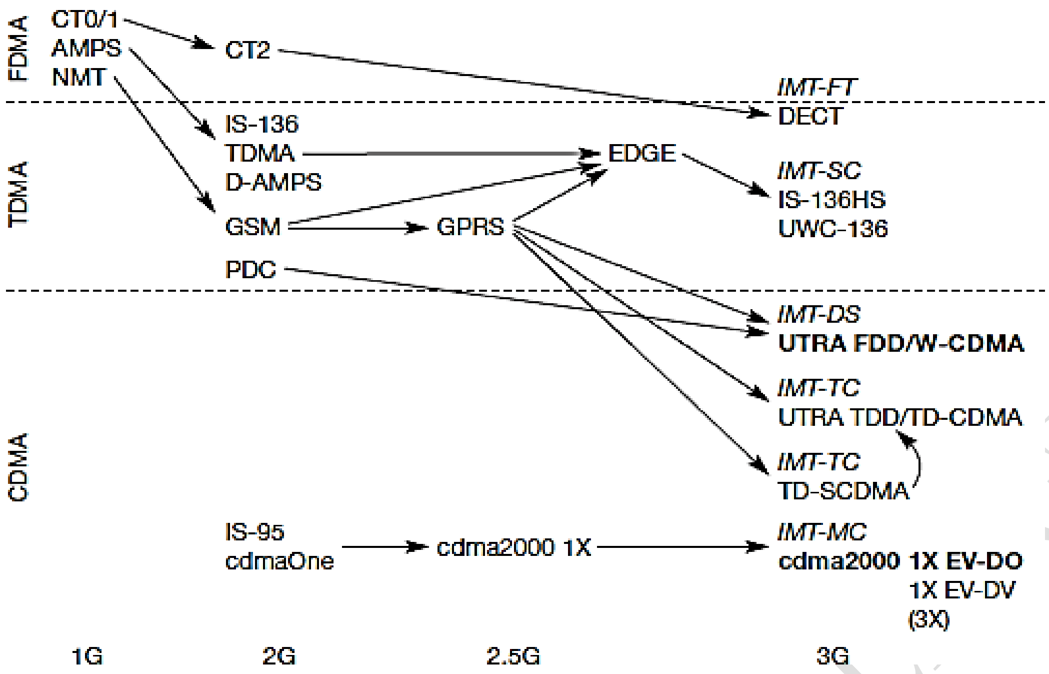
Chapter-II

Telecommunication systems:

- They are the wireless extensions of traditional PSTN or ISDN networks.
- The most popular digital system is GSM, with approximately 70 per cent market share.
- The analog AMPS system still holds three per cent.
- The Japanese PDC holds five per cent (60 million users).
- The remainder is split between CDMA (12 percent) and TDMA (10 per cent) systems.
- Here, the digital market is split into TDMA, CDMA, and GSM.
- 107 million -TDMA
- 135 million- CDMA
- 16 million –GSM



- The following sections present prominent examples for second generation (2G) mobile phone networks, cordless telephones, and trunked radio systems.
- Third generation (3G) mobile phone networks.
- A system like GSM has many open interfaces and network entities defined in the specification.
- One reason for this is their system architecture which is similar to GSM.



- The diagram is divided into the three main multiplexing schemes, FDMA, TDMA, and CDMA.
- The technologies into three generations.
- The first generation comprises analog systems, which typically rely on FDMA.
- The first 2G systems hit the market in the early nineties.
- The second and third generation there is no real revolutionary step.

GSM:

- GSM is the most successful digital mobile telecommunication.
- It is used by over 800 million people in more than 190 countries.
- To avoid this situation for a second generation fully digital system, the groupe special mobile GSM) was founded in 1982.
- This system was soon named the global system for mobile communications (GSM).
- The whole development process of GSM was transferred to 3GPP and further development is combined with 3G development.
- GSM has initially been deployed in Europe using 890–915 MHz for uplinks and 935–960 MHz for downlinks – this system is also called GSM 900.
- GSM at 1800 MHz (1710–1785 MHz uplink, 1805–1880 MHz downlink), also called DCS (digital cellular system)
- GSM at 1900 MHz (1850–1910 MHz uplink, 1930–1990 MHz downlink), also called PCS (personal communications service)

- The architecture, services, and protocols of GSM that are common to all three major solutions, GSM 900, GSM 1800, and GSM 1900.
- GSM has mainly been designed for this and voice services and this still constitutes the main use of GSM systems.

Mobile services:

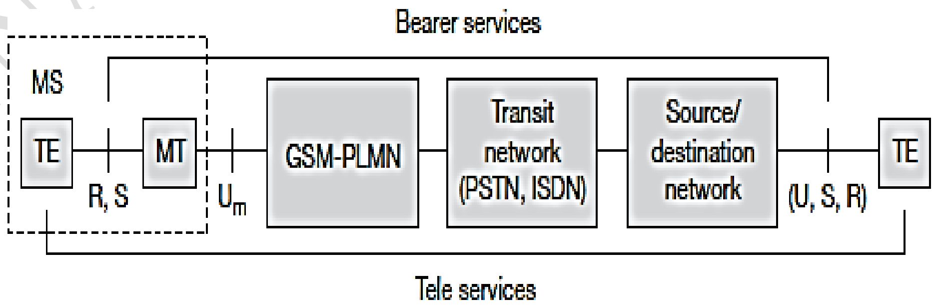
GSM has defined three different categories of services:

- ✓ Bearer service
- ✓ Tele service
- ✓ Supplementary services

- A mobile station MS is connected to the GSM public land mobile network (PLMN).
- This network is connected to transit networks, e.g., integrated services digital network (ISDN) or traditional public switched telephone network (PSTN).
- The mobile termination (MT) performs all network specific tasks TDMA, FDMA, and offers an interface for data transmission.

Bearer services:

- GSM specifies different mechanisms for data transmission, the original GSM allowing for data rates of up to 9600 bit/s for non-voice services.
- Bearer services permit transparent and non-transparent, synchronous or asynchronous data transmission.
- Transparent bearer services only use the functions of the physical layer to transmit data.



- Non-transparent bearer services use protocols of layers two and three to implement error correction and flow control.
- These services use the transparent bearer services, adding a radio link protocol (RLP).
- This protocol comprises mechanisms of high-level data link control (HDLC).

Tele services:

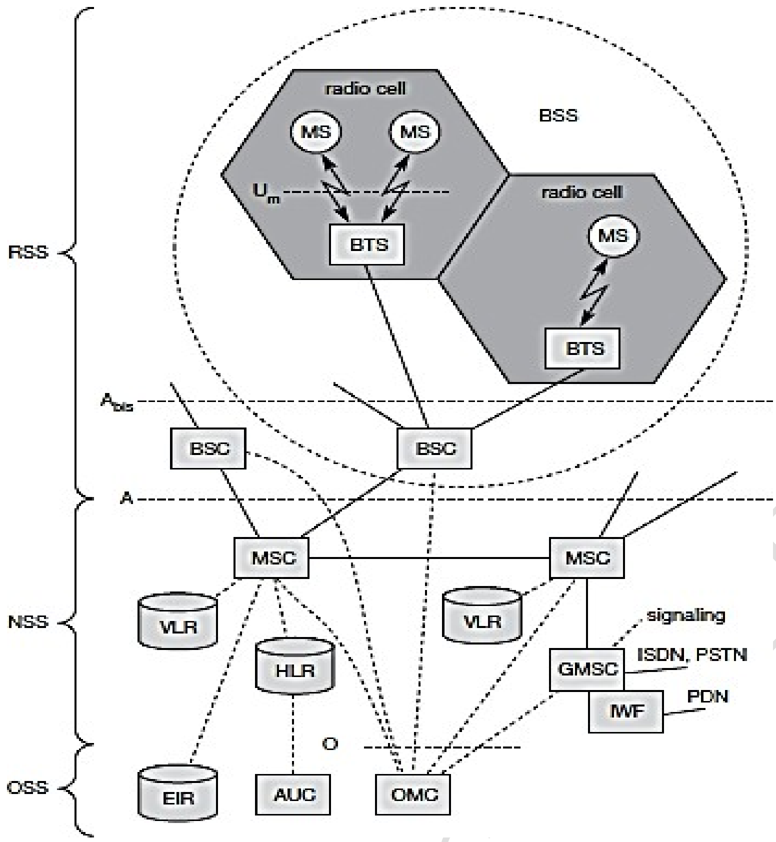
- GSM mainly focuses on voice-oriented tele services.
- These comprise encrypted voice transmission, message services, and basic data communication with terminals as known from the PSTN or ISDN
- The primary goal of GSM was the provision of high-quality digital voice transmission.
- At least the typical bandwidth of 3.1 kHz of analog phone systems.
- 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 channels of GSM but exploit unused capacity in the signaling channels.
- The enhanced message service (EMS).
- The multimedia message service (MMS).

Supplementary services:

- GSM providers can offer supplementary services.
- These services offer various enhancements for the standard telephony service, and may vary from provider to provider.
- The services are user identification, call redirection, or forwarding of ongoing calls.
- Standard ISDN features such as closed user groups and multiparty communication may be available.

System architecture:

- All systems in the telecommunication area, GSM comes with a hierarchical, complex system architecture comprising many entities, interfaces, and acronyms.
- A GSM system consists of three subsystems.
  - ✓ Radio sub system (RSS)
  - ✓ Network and switching subsystem (NSS)
  - ✓ Operation subsystem (OSS)
- The mobile stations (MS) and some antenna masts of the base transceiver stations (BTS).



1. Radio subsystem:

- As the name implies, the radio subsystem (RSS) comprises all radio specific Entities.
- The mobile stations (MS) and the base station subsystem (BSS).
- The connection between the RSS and the NSS via the A interface and the connection to the OSS via the O interface.

Base station subsystem (BSS):

- The BSS performs all functions necessary to maintain radio connections to an MS.

Base transceiver station (BTS):

- A BTS comprises all radio equipment, antennas, signal processing, amplifiers necessary for radio transmission.

Base station controller (BSC):

- The BSC basically manages the BTSs.
- It reserves radio frequencies, handles the handover from one BTS to another BS.

Mobile station (MS):

- The MS comprises all user equipment and software needed for communication with a GSM network.
- An MS consists of user independent hard- and software and of the subscriber identity module (SIM).

2. Network and switching subsystem:

- The "heart" of the GSM system is formed by the network and switching subsystem (NSS).

Mobile services switching center (MSC):

- MSCs are high-performance digital ISDN switches. They set up connections to other MSCs and to BSCs.
- A gateway MSC (GMSC) has additional connections to other fixed networks, such as PSTN and ISDN.

Home location register (HLR):

- The HLR is the most important database in a GSM system as it stores all user-relevant information

Visitor location register (VLR):

- The VLR associated to each MSC is a dynamic database which stores all important information needed for MS
- The VLR is responsible for, it copies all 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 operation and maintenance.

Operation and maintenance center (OMC):

- The OMC monitors and controls all other network entities via the O interface.
- OMC management functions are traffic monitoring, status reports of network entities, subscriber and security management, or accounting and billing.

Authentication Centre (AuC):

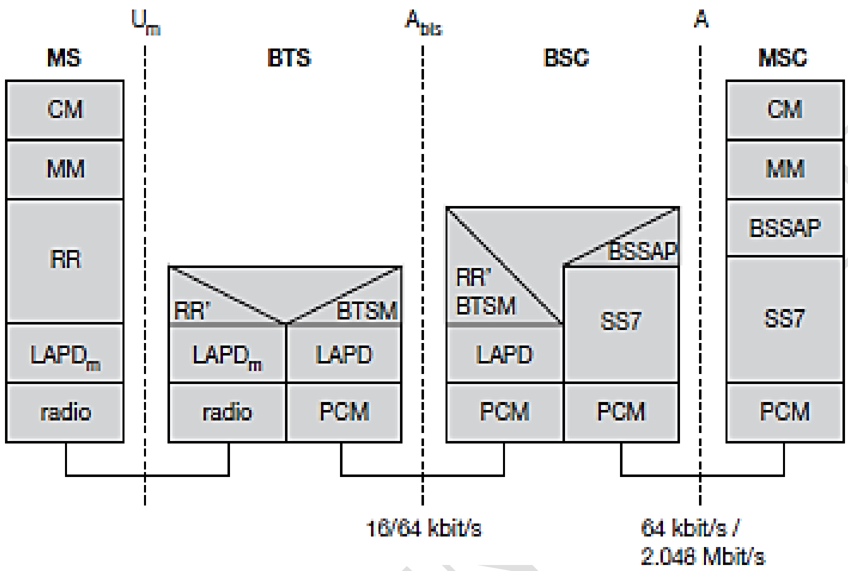
- A separate AuC has been defined to protect user identity and data transmission.
- The AuC contains the algorithms for authentication as well as the keys for encryption and generates the values needed for user authentication in the HLR.

Equipment identity registers (EIR):

- The EIR is a database for all IMEIs .it stores all device identifications registered for this network.

Protocols:

The protocol architecture of GSM with signaling protocols, interfaces, as well as the entities.



Layer 1:

- Physical-radio
- The main tasks of the physical layer comprise channel coding and error detection/correction.

Layer 2:

- LAPD
- LAPD offers reliable data transfer over connections, re-sequencing of data frames, and flow control.

Layer 3:

- RR- Radio Resource management
- The functions of RR" are supported by the BSC via the BTS management (BTSM).
- The main tasks of RR are setup, maintenance, and release of radio channels.

Layer 4:

- MM-Mobility Management
- Mobility management (MM) contains functions for registration, authentication ,identification, location updating, and the provision of a temporary mobile subscriber identity (TMSI).

Layer 5:

- CM-Call Management
- The call management (CM) layer contains three entities
- Call control (CC)
- Sort message service (SMS)
- Supplementary service (SS)

PCM-Pulse Code Modulation

- Data transmission at the physical layer typically uses pulse code modulation (PCM) systems.

SS7-Singnaling System NO.7

- Used for signaling between an MSC and a BSC.
- This protocol also transfers all management information between MSCs, HLR, VLRs, AuC, EIR, and OMC. An MSC can also control a BSS via a BSS application part (BSSAP).

HANDOVER AND SECURITY:

Handover:

- Cellular systems require handover procedures, as single cells do not cover the whole service area.
- A handover should not cause a cut-off, also called call drop.

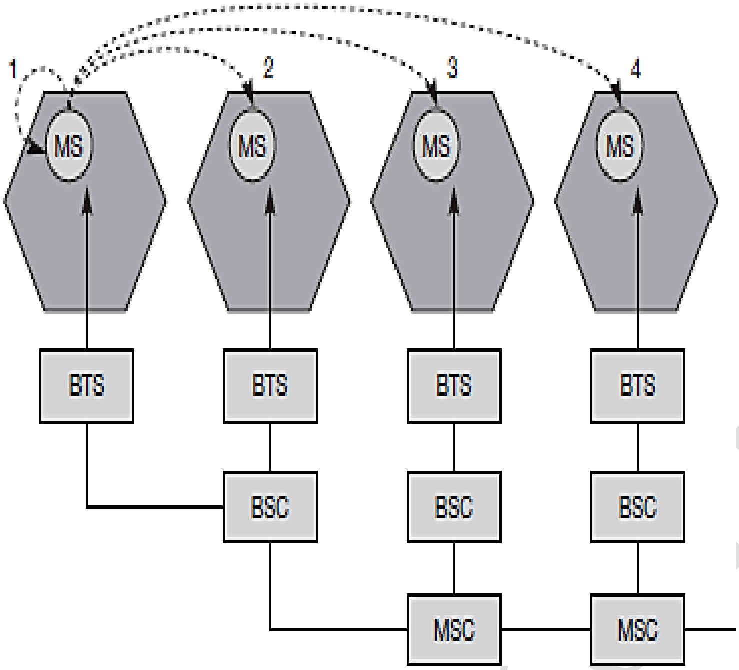
There are two basic reasons for a handover:

- The mobile station moves out of the range of a BTS or a certain antenna of a BTS respectively.
- The received signal level 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.

Four possible handover scenarios in GSM:

1. **Intra-cell handover:**

- Within a cell, narrow-band interference could make transmission at a certain frequency impossible.
- The BSC could then decide to change the carrier frequency.



2. Inter-cell, intra-BSC handover:

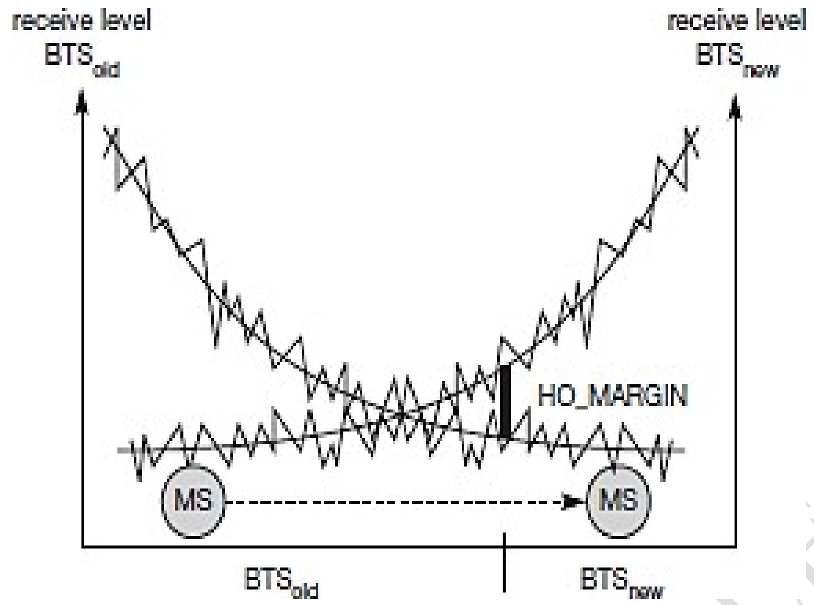
- The mobile station moves from one cell to another, but stays within the control of the same BSC.
- The BSC then performs a handover, assigns a new radio channel in the new cell and releases the old one.

3. Inter-BSC, intra-MSC 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 the MSC.

4. Inter MSC handover:

- A handover could be required between two cells belonging to different MSCs.



- MS moves away from one BTS (BTS old) closer to another one (BTS new).
- The handover margin (HO_MARGIN), which includes some hysteresis to avoid a ping- pong effect.
- The MS sends its periodic measurements reports, the BTS old forwards these reports to the BSC old together with its own measurements.

Security:

- GSM offers several security services using confidential information stored in the AuC and in the individual SIM.

The security services offered by GSM are:

- ✓ Access Control and authentication
- ✓ Confidentiality
- ✓ Anonymity

Access control and authentication:

- The first step includes the authentication of a valid user for the SIM. The user needs a secret PIN to access the SIM.

Confidentiality:

- All user-related data is encrypted. After authentication, BTS and MS apply encryption to voice, data, and signaling.

Anonymity:

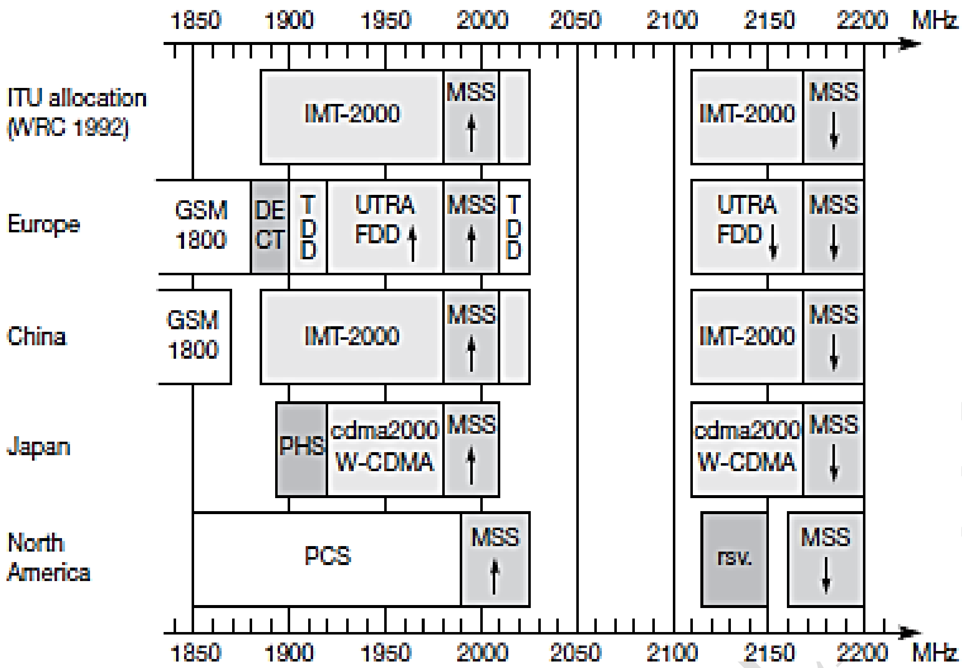
- All data is encrypted before transmission, and user identifiers are not used over the air.

Three algorithms have been specified to provide security services in GSM:

- Algorithm A3 is used for authentication.
- Algorithm A5 for encryption.
- Algorithm A8 for the generation of a cipher key.

UMTS and IMT-2000

- The International Telecommunication Union (ITU) made a request for proposals for radio transmission technologies (RTT) for the international mobile telecommunications (IMT) 2000.
- IMT-2000 includes different environments such as indoor use, vehicles, satellites and pedestrians.
- The world radio conference (WRC) 1992 identified 1885–2025 and 2110–2200 MHz as the frequency bands.
- In Europe, some parts of the ITU"s frequency bands for IMT-2000 are already allocated for DECT.
- The remaining frequencies have been split into bands for
- UTRA-FDD
- Uplink: 1920–1980 MHz,
- Downlink: 2110–2170 MHz
- UTRA-TDD
- Uplink: 1900–1920 MHz
- Downlink: 2010–2025 MHz
- Global multimedia mobility (GMM). GMM provides an architecture to integrate mobile and fixed terminals, many different access networks (GSM BSS, DECT, ISDN, UMTS, LAN, WAN, CATV, MBS)



ITU standardized five groups of 3G radio access technologies:

1. **IMT-DS:**
   - The direct spread technology comprises wideband CDMA (WCDMA) systems.
   - This is the technology specified for UTRA-FDD and used by all European providers and the Japanese.

2. **IMT-TC:**
   - The time code contained only the UTRA-TDD system which uses time-division CDMA (TD-CDMA).
   - TD- synchronous CDMA (TD-SCDMA).

3. **IMT-MC:**
   - A multi-carrier technology standardized by 3GPP2.It used by cdma 2000.

4. **IMT-SC:**
   - The UWC-136 is a single carrier technology originally promoted by the Universal Wireless Communications Consortium (UWCC).

5. **IMT-FT:**
   - As frequency time technology, an enhanced version of the cordless telephone standard DECT.

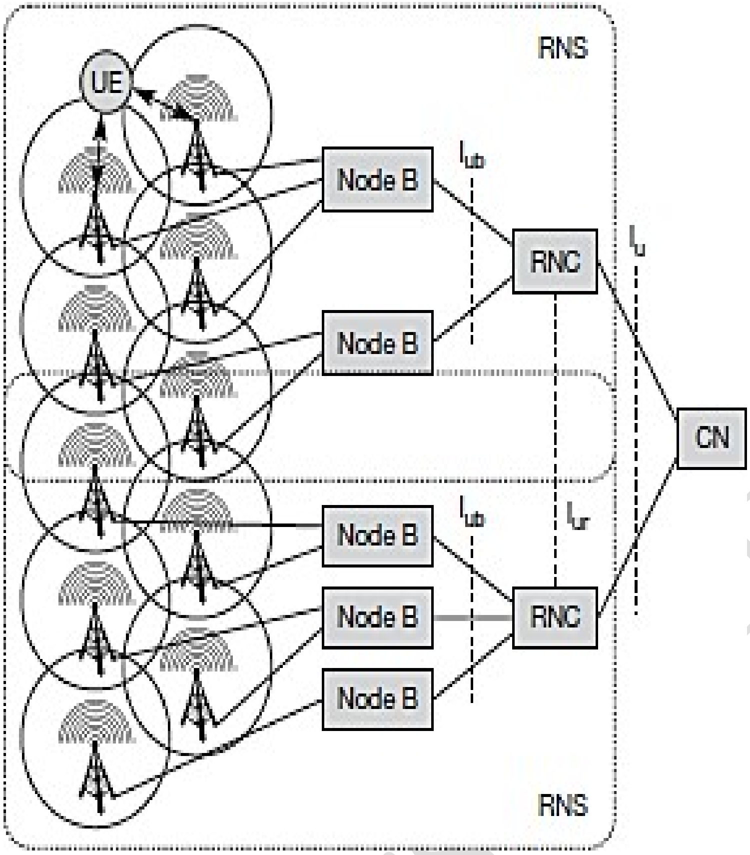
UMTS system architecture:

- UMTS reference architecture which applies to both UTRA solutions.
- 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.

- The UTRAN is connected to the user equipment (UE).
- The user equipment domain is assigned to a single user and comprises all the functions that are needed to access UMTS services.
- The end device itself is in the mobile equipment domain. All functions for radio transmission as well as user interfaces are located here.
- This domain consists of the access network domain, which contains the radio access networks (RAN).
- The serving network domain comprises all functions currently used by a user for accessing UMTS service.

UTRAN:

- The basic architecture of the UTRA network this consists of several radio network subsystems (RNS).
- Each RNS is controlled by a radio network controller (RNC).
- The mobile device, UE, can be connected to one or more antennas as will subsequently handover.
- Each RNC is connected with the core network (CN).
- The use of this interface is explained together with the UMTS handover mechanisms.



Core network:

- The core network (CN) basically the same as already explained in the context of GSM and GPRS .

Circuit switched domain (CSD):

- The circuit switched domain (CSD) comprises the classical circuit switched services including signaling.

Packet switched domain (PSD):

- The packet switched domain (PSD) uses the GPRS components SGSN and GGSN and connects to the RNS via the IuPS part of the Iu interface.

Handover:

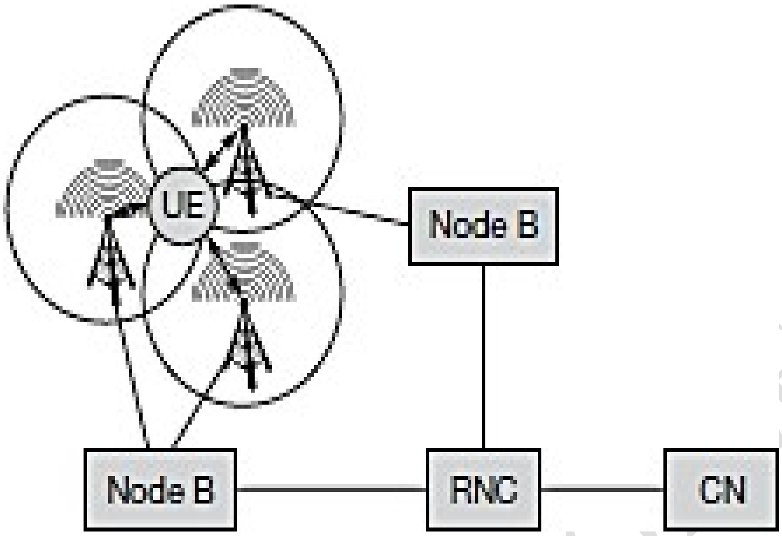
UMTS knows two basic classes of handovers:

- ✓ Hard handover
- ✓ Soft handover

Hard handover:

- This handover type is already known from GSM and other TDMA/FDMA systems.

- Switching between different antennas or different systems is performed at a certain point in time.

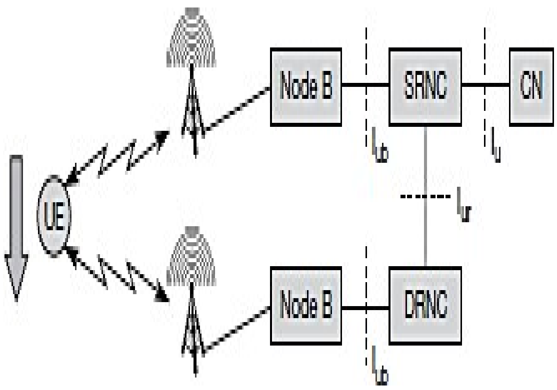


Soft handover:

- This is the real new mechanism in UMTS compared to GSM and is only available in the FDD mode.
- Soft handovers are well known from traditional CDMA networks as they use macro diversity, a basic property of CDMA.

Serving RNC and Drift RNC:

- If the UE moves in the example from the upper cell to the lower cell.
- The upper RNC acts as a serving RNC (SRNC) while the other is the drift RNC (DRNC).



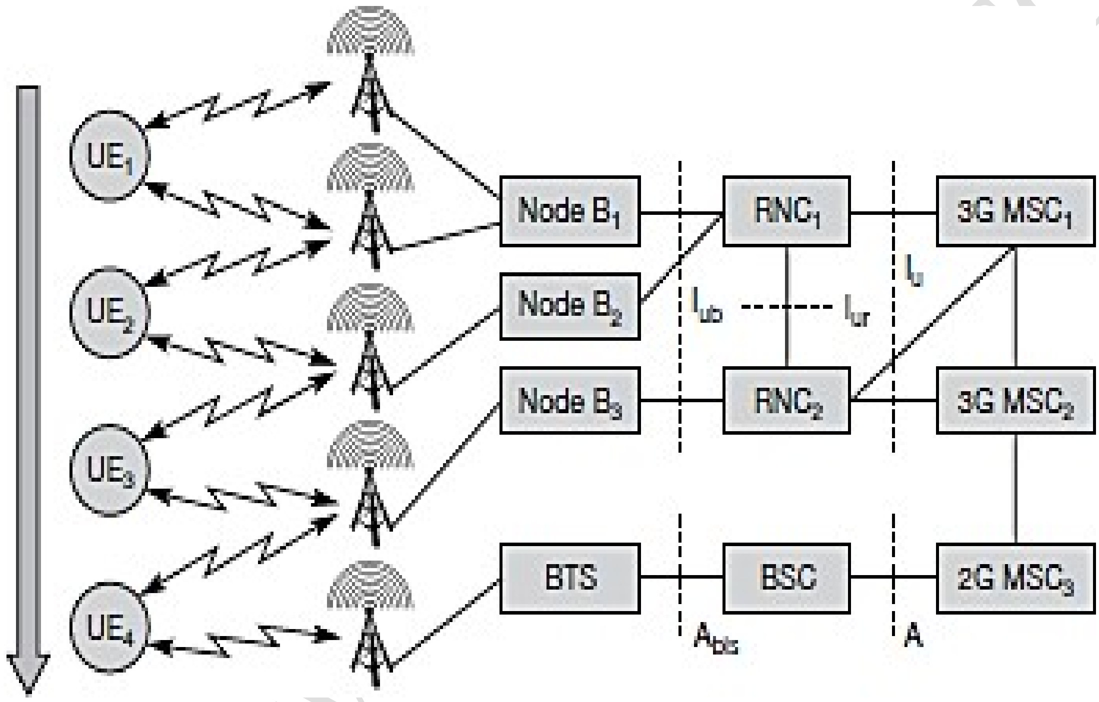
Different types of handover:

1. **Intra-node B, intra-RNC:**

- UE1 moves from one antenna of node B1 to another antenna. This type of handover is called softer handover.

2. **Inter-node B, intra-RNC:**

- UE2 moves from node B1 to node B2. In this case RNC1 supports the soft handover by combining and splitting data.



3. **Inter-RNC:**

- UE3 moves from node B2 to node B3 two different types of handover can take place.
  - ✓ The internal inter-RNC
  - ✓ External inter-RNC

4. **Inter-MSC:**

- It could be also the case that MSC2 takes over and performs a hard handover of the connection.

5. **Inter-system:**

- UE4 moves from a 3G UMTS network into a 2G GSM network.

Satellite Systems:

- Satellite communication introduces another system supporting mobile communications.
- Several restrictions and application requirements result in three major classes of satellites.

  - ✓ GEO
  - ✓ MEO
  - ✓ LEO

Applications:

1. **Weather forecasting:**
- Several satellites deliver pictures of the earth using, e.g, infra-red or visible light.

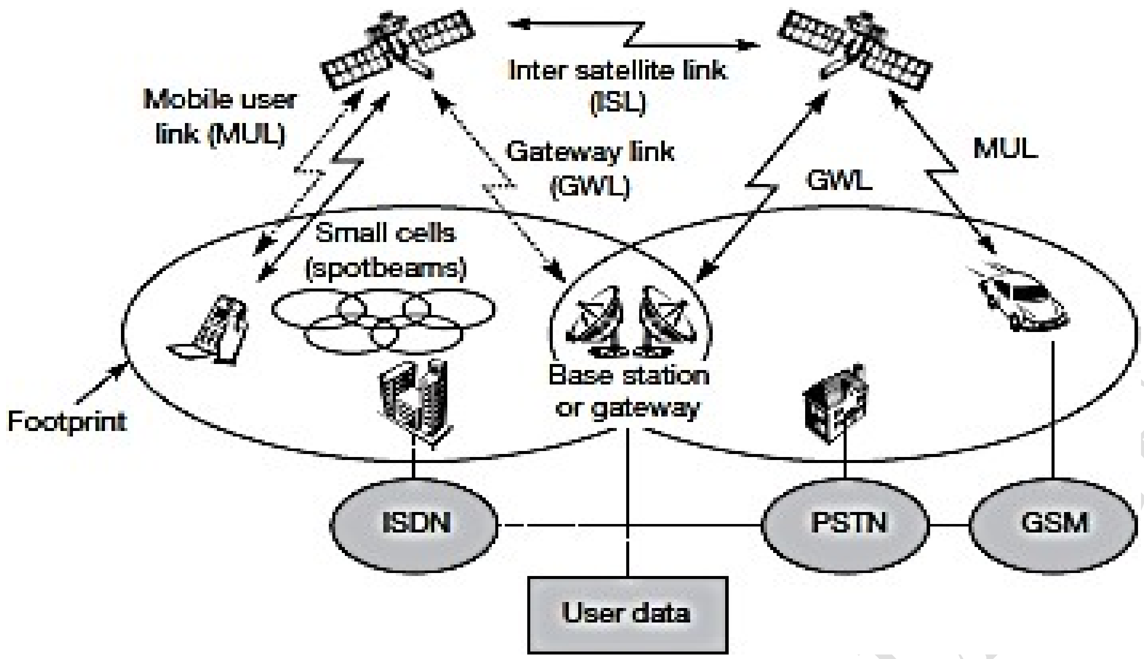
2. **Radio and TV broadcast satellites:**
- Hundreds of radio and TV programs are available via satellite.
- This technology competes with cable in many places.

3. **Military satellites:**
- One of the earliest applications of satellites was their use for carrying out espionage.
- Many communication links are managed via satellite because they are much safer from attack by enemies.

4. **Satellites for navigation:**
- The global positioning system (GPS) is nowadays well-known and available for everyone.

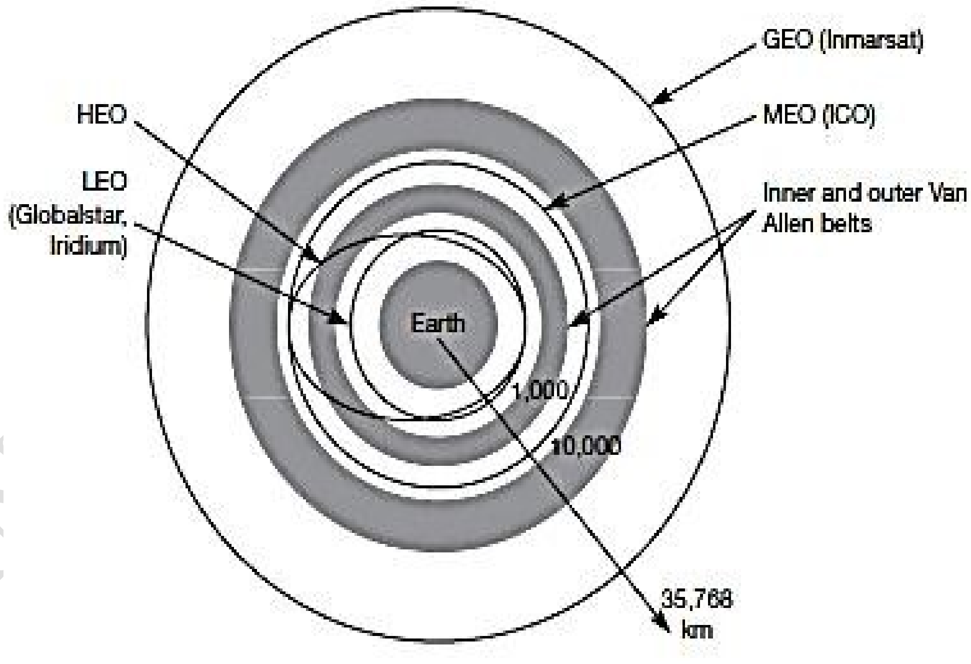
5. **Global telephone backbones:**
- One of the first applications of satellites for communication was the establishment of international telephone backbones.
- Instead of using cables it was sometimes faster to launch a new satellite.

6. **Connections for remote or developing areas:**
- Due to their geographical location many places all over the world do not have direct wired connection to the telephone network or the internet.



7. **Global mobile communication:**

- The latest trend for satellites is the support of global mobile data communication.
- The high latency geostationary satellites are not ideal for this task.



Basics:

Geostationary (or geosynchronous) earth orbit (GEO):

- GEO satellites have a distance of almost 36,000 km to the earth.

  Eg : TV and radio broadcast satellites.

Medium earth orbit (MEO):

- MEOs operates at a distance of about 5,000–12,000 km.

  Eg: ICO

Low earth orbit (LEO):

- The new satellite systems now rely on this class using altitudes of 500–1,500 km.

Highly elliptical orbit (HEO):

- This class comprises all satellites with noncircular orbits.

GEO:

- If a satellite should appear fixed in the sky, it requires a period of 24 hours.

Advantages:

- Three GEO satellites are enough for a complete coverage of almost any spot on earth.
- Senders and receivers can use fixed antenna positions, no adjusting is needed.

Disadvantages:

- Northern or southern regions of the earth have more problems receiving these satellites.
- larger antennas are needed in this case.

LEO:

- As LEOs circulate on a lower orbit, it is obvious that they exhibit a much shorter period (the typical duration of LEO periods are 95 to 120 minutes).

Advantages:

- LEOs even provide this bandwidth for mobile terminals with omni-directional antennas using low transmit power in the range of 1W.
- LEOs can provide a much higher elevation in Polar Regions and so better global coverage.

Disadvantages:

- The biggest problem of the LEO concept is the need for many satellites if global coverage is to be reached.
- LEOs is the short lifetime of about five to eight years due to atmospheric drag.

MEO:

- MEOs can be positioned somewhere between LEOs and GEOs.

Advantages:

- These satellites move more slowly relative to the earth"s rotation allowing a simpler system design.

Disadvantages:

- The larger distance to the earth, delay increases to about 70–80 m s.
- The satellites need higher transmit power and special antennas for smaller footprints.

Routing:

- The data transmissions from one user to another as any other network .
- Routing in the fixed segment (on earth) is achieved as usual, while two different solutions exist for the satellite network in space.
- This last satellite now sends the data down to the earth.
- This means that only one uplink and one downlink per direction is needed.
- Routing takes place in fixed networks as usual until another gateway is reached.
- Which is responsible for the satellite above the receiver.

Localization:

- Localization of users in satellite networks is similar to that of terrestrial cellular networks.
- The gateways of a satellite network maintain several registers.
- Home Location Register(HLR).
- Visitor Location Register(VLC).
- Satellite User Mapping Register(SUMR).
-

Handover:

- An important topic in satellite systems using MEOs and in particular LEOs is handover.

1. **Intra-satellite handover:**

- A user might move from one spot beam of a satellite to another spot beam of the same satellite.

2. **Inter-satellite handover:**

- Inter-satellite handover can also take place between satellites if they support ISLs.

3. **Gateway handover:**

- The mobile user and satellite might still have good contact, the satellite might move away from the current gateway.

4. **Inter-system handover:**

- Satellite systems are used in remote areas if no other network is available.

Mobile Communication

Chapter-III

Wireless LAN:

- WLANs are typically restricted in their diameter to buildings, a campus, single rooms etc. and are operated by individuals not by large-scale network providers.

Advantages of WLANs are:

Flexibility:

- Within radio coverage, nodes can communicate without further restriction. 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.

Robustness:

- Wireless networks can survive disasters, e.g., earthquakes or users pulling a plug.

Cost:

- After providing wireless access to the infrastructure via an access point for the first user.

WLANs also have several disadvantages:

Quality of service:

- 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.

Restrictions:

- All wireless products have to comply with national regulations. Several government and non-government institutions worldwide regulate.

Safety and security:

- Using radio waves for data transmission might interfere with other high-tech equipment in, e.g., hospitals.

WLANs to ensure their commercial success:

Global operation:

- WLAN products should sell in all countries so, national and international frequency regulations have to be considered.

Low power:

- Devices communicating via a WLAN are typically also wireless devices running on battery power.

License-free operation:

- LAN operators do not want to apply for a special license to be able to use the product.

Robust transmission technology:

- If they use radio transmission, many other electrical devices can interfere with them (vacuum cleaners, hairdryers, train engines etc.).

Simplified spontaneous cooperation:

- To be useful in practice, WLANs should not require complicated setup routines but should operate spontaneously after power-up.

Easy to use:

- In contrast to huge and complex wireless WANs, wireless LANs are made for simple use.

Protection of investment:

- A lot of money has already been invested into wired LANs.

Safety and security:

- Wireless LANs should be safe to operate, especially regarding low radiation if used, e.g., in hospitals.

Transparency for applications:

- Existing applications should continue to run over WLANs, the only difference being higher delay and lower bandwidth.

Infra-red vs radio transmission:

Infra-red:

- Infra-red technology uses diffuse light reflected at walls, furniture etc. or directed light if a line-of-sight (LOS) exists between sender and receiver.
- Senders can be simple light emitting diodes (LEDs) or laser diodes.

Advantages:

- The main advantages of infra-red technology are its simple and extremely cheap senders and receivers which are integrated into nearly all mobile devices available.
- The data rates of up to 115 Kbit/s.

Disadvantages:

- The infra-red transmissions are its low bandwidth compared to other LAN technologies.
- The main disadvantage is that infra-red is quite easily shielded.

Radio Transmission:

- Radio waves for data transmission, e.g., GSM at 900, 1,800, and 1,900 MHz, DECT at 1,880 MHz etc.

Advantages:

- Radio transmission includes the long-term experiences made with radio transmission for wide area networks (e.g., microwave links) and mobile cellular phones.
- Higher transmission rates (e.g., 54 Mbit/s).

Disadvantages:

- 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 via radio.

3.2 IEEE 802.11:

- IEEE- Institute of Electrical and Electronic Engineering.
- The IEEE standard 802.11 specifies the most famous family of WLANs in which many products are available.
- This standard belongs to the group of 802.x LAN standards, 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 original standard for higher data rates, 802.11a (up to 54 Mbit/s at 5 GHz) and 802.11b.

System architecture:

- Wireless networks can exhibit two different basic system architectures:
  - ✓ Infrastructure – based
  - ✓ Ad - hoc.

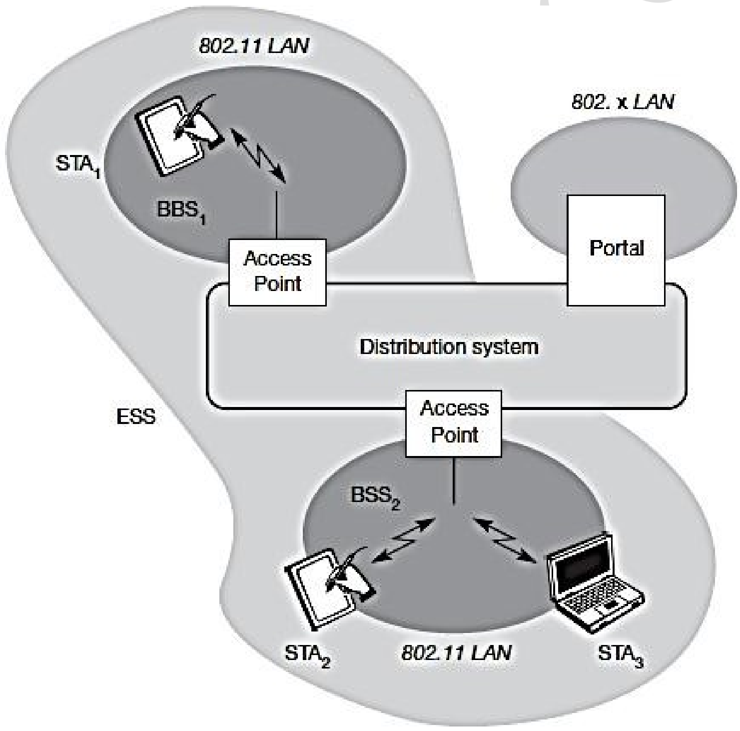
Infrastructure based IEEE 802.11:

- The components of an infrastructure and a wireless part as specified for IEEE 802.11.

Several Modes:

- ✓ Station(STA)
- ✓ Access Point(AP)
- ✓ Basic Server Set(BSS)
- ✓ Extended Service(ESS)
- ✓ Portal

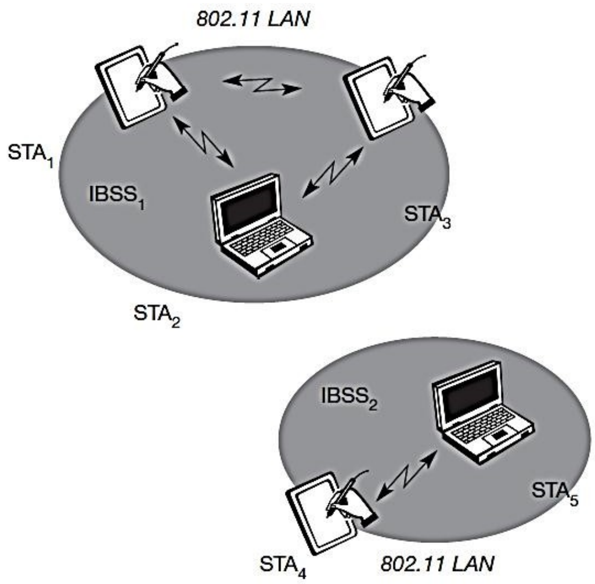
- Stations are terminals with access mechanisms to the wireless medium and radio contact to the AP.



- The stations and the AP which are within the same radio coverage form a basic service set (BSSi).
- Shows two BSSs – BSS1 and BSS2 – which are connected via a distribution system.
- A distribution system connects several BSSs via the AP to form a single network and thereby extends the wireless coverage area. This network is now called an extended service set (ESS).
- The distribution system connects the wireless networks via the APs with a portal, which forms the interworking unit to other LANs.

Ad-hoc Networks:

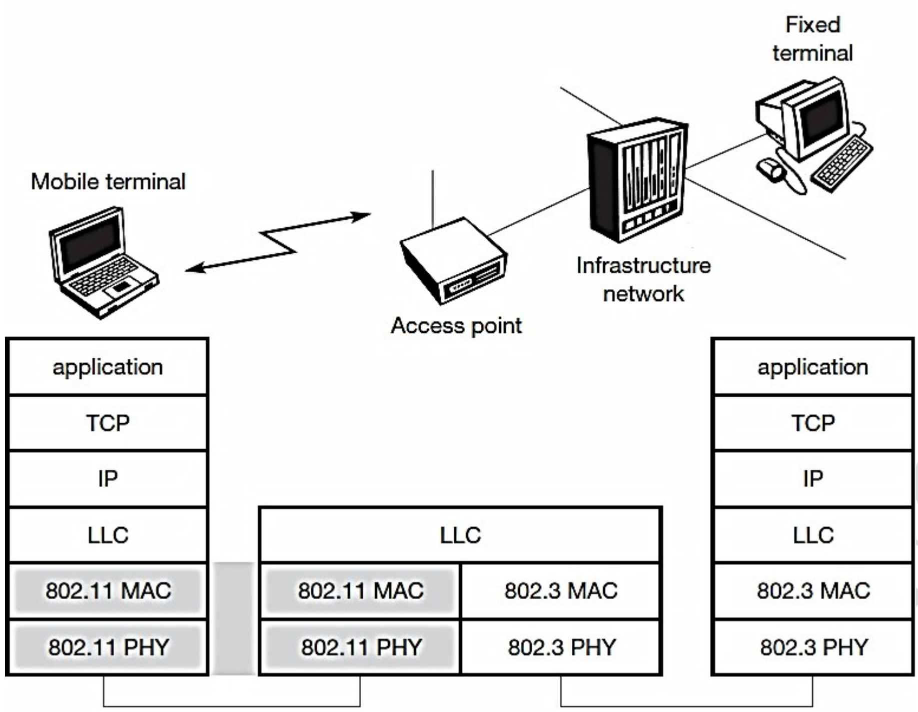
- Infrastructure-based networks, IEEE 802.11 allows the building of ad-hoc networks between stations.
- Thus forming one or more independent BSSs (IBSS).
- An IBSS comprises a group of stations using the same radio frequency.



- Stations STA1, STA2, and STA3 are in IBSS1, STA4 and STA5 in IBSS2.
- For example that STA3 can communicate directly with STA2 but not with STA5.

Protocol architecture:

- IEEE 802.11 wireless LAN connected to a switched IEEE 802.3 Ethernet via a bridge.
- The higher layers (application, TCP, IP) look the same for wireless nodes as for wired nodes.
- The upper part of the data link control layer, the logical link controls (LLC).
- The differences of the medium access control layers needed for the different media.



- The physical layer PHY and medium access layer MAC like the other 802.x LANs.
- The physical layer is sub divided into the physical layer convergence protocol (PLCP) and the physical medium dependent sub layer PMD.

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).
- The PHY layer offers a service access point (SAP) with 1 or 2 Mbit/s transfer rate.

Frequency hopping spread spectrum:

- Frequency hopping spread spectrum (FHSS) is a spread spectrum technique which allows for the coexistence of multiple networks in the same area by separating different networks using different hopping sequences.

The Functions are:

- ✓ Synchronization
- ✓ Start frame delimiter (SFD)
- ✓ PLCP_PDU length word (PLW)
- ✓ PLCP signaling field (PSF)

Direct sequence spread spectrum:

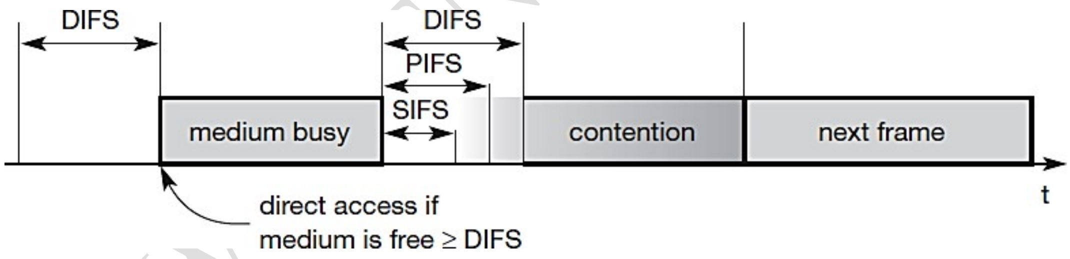
- Direct sequence spread spectrum (DSSS) is the alternative spread spectrum method separating by code and not by frequency.

The Functions are:

- ✓ Synchronization
- ✓ Start frame delimiter (SFD)
- ✓ Signal
- ✓ Service
- ✓ Length
- ✓ Header error check (HEC)

Medium access control layer:

- The MAC layer has to fulfill several tasks.
- 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 asynchronous data service and an optional time-bounded service.
- The following three basic access mechanisms have been defined for IEEE 802.11
- The first two methods are also summarized as distributed coordination function (DCF)
- The third method is called point coordination function (PCF).



Short inter-frame spacing (SIFS):

- The shortest waiting time for medium access (so the highest priority) is defined for short control messages

PCF inter-frame spacing (PIFS):

- A waiting time between DIFS and SIFS 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.

MAC management:

- MAC management plays a central role in an IEEE 802.11 station as it more or less controls all functions related to system Integration.

Synchronization:

- Functions to support finding a wireless LAN, synchronization of internal clocks, generation of beacon signals.
- To synchronize the clocks of all nodes, IEEE 802.11 specifies a timing synchronization function (TSF).

Power management:

- Functions to control transmitter activity for power conservation, e.g., periodic sleep, buffering
- Wireless devices are battery powered (unless a solar panel is used). Therefore, power-saving mechanisms are crucial for the commercial success of such devices.
- The basic idea of IEEE 802.11 power management is to switch off the transceiver whenever it is not needed.

Roaming:

- Functions for joining a network (association), changing access points, scanning for access points.
- 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 roaming.

The Steps For Roming:

- ✓ Scanning
- ✓ Passive Scanning
- ✓ Active Scanning
- ✓ Association Request
- ✓ Association Response

HIPERLAN:

HIPERLAN - High Performance Local Area Network.

- The key feature of all four networks is their integration of time-sensitive data transfer services.
- The names have changed and the former HIPERLANs 2, 3, and 4 are now called HiperLAN2, HIPERACCESS, and HIPERLINK.

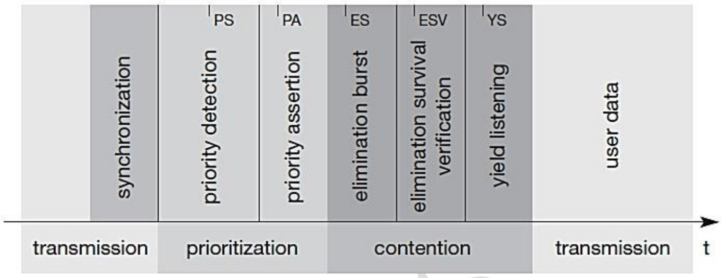
HIPERLAN 1:

- HIPERLAN 1 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 1 should operate at 5.1–5.3 GHz with a range of 50 m in buildings at 1 W transmit power.
- The following describes only the medium access scheme of HIPERLAN 1, a scheme that provides QoS and a powerful prioritization scheme.

Three Phases:

- ✓ Prioritization
- ✓ Contention
- ✓ Transmission



Prioritization:

- Determine the highest priority of a data packet ready to be sent by competing nodes.

Contention:

- Eliminate all but one of the contenders, if more than one sender has the highest current priority.

Transmission:

- Finally, transmit the packet of the remaining node.

Prioritization phase:

- 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.

Elimination phase:

- The whole elimination phase will last for the duration of the longest elimination burst among the contending nodes plus the survival verification time.
- One or more nodes will survive this elimination phase, and can then continue with the next phase.

Yield phase:

- The yield phase is determined by the shortest yield-listening period among all the contending nodes.
- At least one node will survive this phase and can start to transmit data.

Transmission phase:

- In case of a unicast transmission, the sender expects to receive an immediate acknowledgement from the destination, called an acknowledgement HCPDU

WATM:

Wireless ATM

- WATM; sometimes also called wireless, mobile ATM, wmATM
- Many WATM aspects come from the telecommunication industry.
- This specific situation can be compared to the case of competition and merging with regard to the concepts TCP/IP and ATM

Motivation for WATM:

- Several reasons led to the development of WATM:
- The need for seamless integration of wireless terminals into an ATM network.
- ATM networks scale well from LANs to WANs – and mobility is needed in local and wide area applications.
- ATM to be successful, it must offer a wireless extension.
- WATM could offer QoS for adequate support of multi-media data streams.
- One goal in this context is the seamless integration of mobility into B-ISDN

Need to be considered for a mobile ATM:

Location management:

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

Mobile routing:

- Even if the location of a terminal is known to the system, it still has to route the traffic through the network to the access point currently responsible for the wireless terminal.

Handover signaling:

- The network must provide mechanisms which search for new access points

QoS and traffic control:

- In contrast to wireless networks offering only best effort traffic, and to cellular networks offering only a few different types of traffic.

Network management:

- All extensions of protocols or other mechanisms also require an extension of the management functions to control the network.

WATM services:

- WATM systems had to be designed for transferring voice, classical data, video , multimedia data, short messages etc.

Office environments:

- This includes all kinds of extensions for existing fixed networks offering a broad range of Internet/Intranet access, multi-media conferencing, online multi-media database access, and telecommuting.

Universities, schools, training centers:

- The main foci in this scenario are distance learning, wireless and mobile access to databases, internet access,

Industry:

- WATM may offer an extension of the Intranet supporting database connection, information retrieval, surveillance

Hospitals:

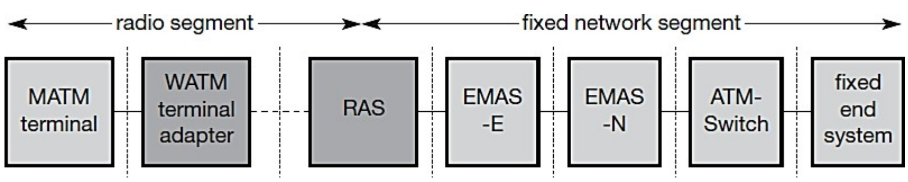
- Applications could include the transfer of medical images, remote access to patient records, remote monitoring of Patients.

Home:

- Many electronic devices at home could be connected using WATM technology. e.g., TV, radio equipment, CD player.

Networked vehicles:

- All vehicles used for the transportation of people or goods will have a local network and network access in the future.



Handover:

- One of the most important topics in a WATM environment is handover.
- Connectionless, best-effort protocols supporting handover, such as mobile IP on layer 3 and IEEE 802.11.
- The main problem for WATM during the handover is rerouting all connections and maintaining connection quality.

Many different requirements have been set up for handover:

Handover of multiple connections:

- As ATM is a connection-oriented technology where end-systems can support many connections at the same time, handover in WATM must support more than only one connection.

Handover of point-to-multi-point connections:

- Seamless support of point-to-multi-point connections is one of the major advantages of the ATM technology.

QoS support:

- Handover should aim to preserve the QoS of all connections during handover. However, due to limited resources, this is not always possible.

Data integrity and security:

- Security associations between the terminal and the network should not be compromised by handover.

Signaling and routing support:

- WATM must provide the means to identify mobility-enabled switches in the network,

Performance and complexity:

- The fact that WATM systems are complex by nature is mainly due to their support of connections with QoS.

Mobile quality of service:

- Quality of service (QoS) guarantees is one of the main advantages envisaged for WATM networks compared to e.g., mobile IP working over packet radio networks.

  - ✓ Wired Qos
  - ✓ Wireless Qos
  - ✓ Handover Qos

BRAN:

BRAN - The broadband radio access networks .

- The main motivation behind BRAN is the deregulation and privatization of the telecommunication sector in Europe.
- One possible technology to provide network access for customers is radio. The advantages of radio access are high flexibility and quick installation.
- The primary market for BRAN includes private customers and small to medium-sized companies with Internet Applications.

BRAN has specified four different network types:

HIPERLAN 1:

- This high-speed WLAN supports mobility at data rates above 20 Mbit/s. Range is 50 m, connections are multi-point-to-multi-point using ad-hoc or infrastructure networks.

HIPERLAN/2:

- This technology can be used for wireless access to ATM or IP networks and supports up to 25 Mbit/s user data rate in a point-to-multi-point configuration.
- Transmission range is 50 m.

HIPERACCESS:

- This technology could be used to cover the „last mile" to a customer via a fixed radio link.
- Transmission range is up to 5 km, data rates of up to 25 Mbit/s are supported.

HIPERLINK:

- HIPERLINK provides a fixed point-to-point connection with up to 155 Mbit/s.

HiperLAN2:

- HiperLAN2 offers data rates of up to 54 Mbit/s including QoS support and enhanced security features.

High-throughput transmission:

- HiperLAN2 not only offers up to 54 Mbit/s at the physical layer but also about 35 Mbit/s at the network layer.
- HiperLAN2 uses MAC frames with a constant length of 2 m s.

Connection-oriented:

- Prior to data transmission HiperLAN2 networks establish logical connections between a sender and a receiver.

Quality of service support:

- The help of connections, support of QoS is much simpler. Each connection has its own set of QoS parameters bandwidth, delay, jitter, bit error rate etc.,

Dynamic frequency selection:

- All access points have built-in support which automatically selects an appropriate frequency within their coverage area.

Security support:

- Authentication as well as encryption is supported by HiperLAN2. Both, mobile terminal and access point can authenticate each other.

Mobility support:

- Mobile terminals can move around while transmission always takes place between the terminal and the access point with the best radio signal.

Application and network independence:

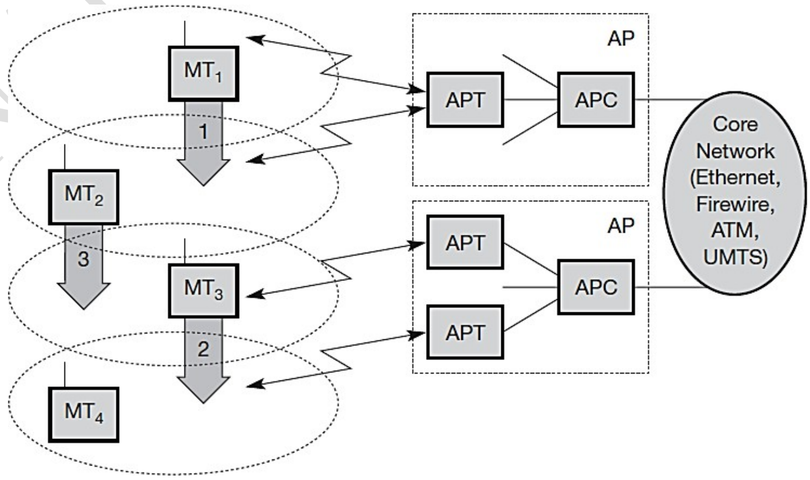
- HiperLAN2 was not designed with a certain group of applications or networks in mind.

Power save:

- Mobile terminals can negotiate certain wake-up patterns to save power.

Reference model and configurations:

- The standard architecture of an infrastructure-based HiperLAN2 network.
- Two access points (AP) are attached to a core network.
- Each AP consists of an access point controller (APC) and one or more access point transceivers (APT).



- APT can comprise one or more sectors Finally, four mobile terminals (MT).

Three handover situations may occur:

Sector handover (Inter sector):

- If sector antennas are used for an AP, which is optional in the standard, the AP shall support sector handover.

Radio handover (Inter-APT/Intra-AP):

- As this handover type, too, is handled within the AP, no external interaction is needed.

Network handover (Inter-AP/Intra-network):

- MT2 moves from one AP to another.
- In this case, the core network and higher layers are also involved.

HiperLAN2 networks can operate in two different modes:

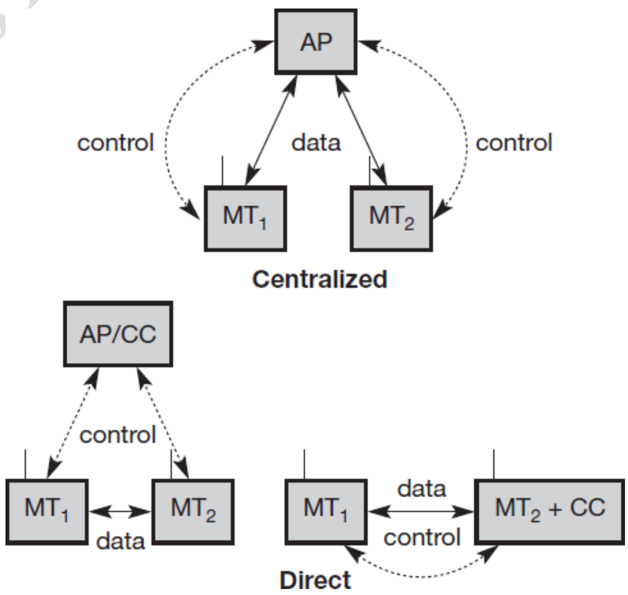
- ✓ Centralized mode (CM)
- ✓ Direct mode (DM)

Centralized mode (CM):

- All APs are connected to a core network and MTs are associated with APs. Even if two MTs share the same cell, all data is transferred via the AP.

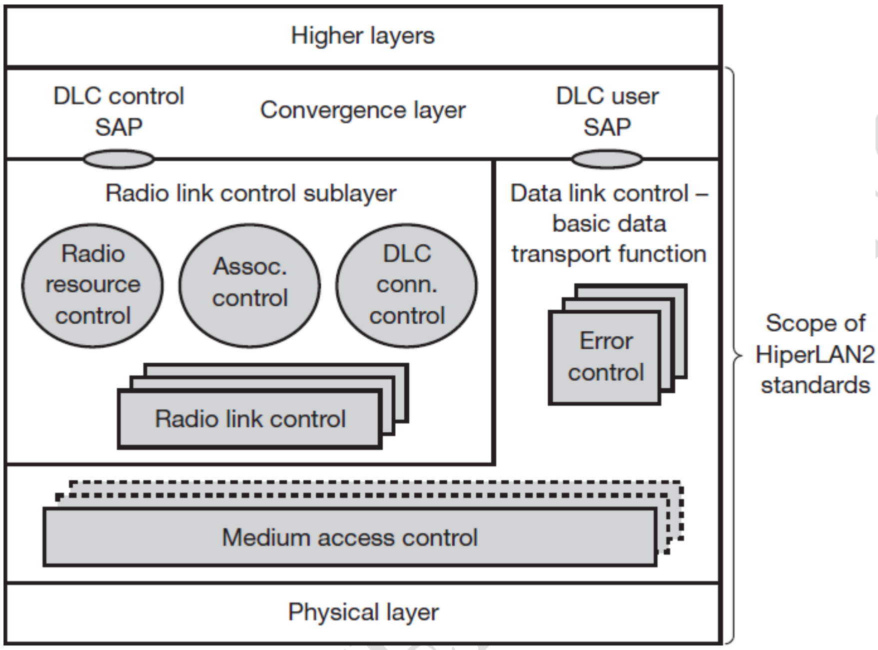
Direct mode (DM):

- Data is directly exchanged between MTs if they can receive each other, but the network still has to be controlled.
- This can be done via an AP that contains a central controller (CC).



HiperLAN2 Protocol Stack:

- HiperLAN2 protocol stack as used in access points.
- The lowest layer, the physical layer, handles as usual all functions related to modulation, forward error correction, signal detection, synchronization.



- The data link control (DLC) layer contains the MAC functions, the RLC sublayer and error control functions.
- The user part contains error control mechanisms. HiperLAN2 offers reliable data transmission using acknowledgements and retransmissions.
- The radio link control (RLC) sub layer comprises most control functions in the DLC layer.
- On top of the DLC layer there is the convergence layer. This highest layer of HiperLAN2 standardization may comprise segmentation.

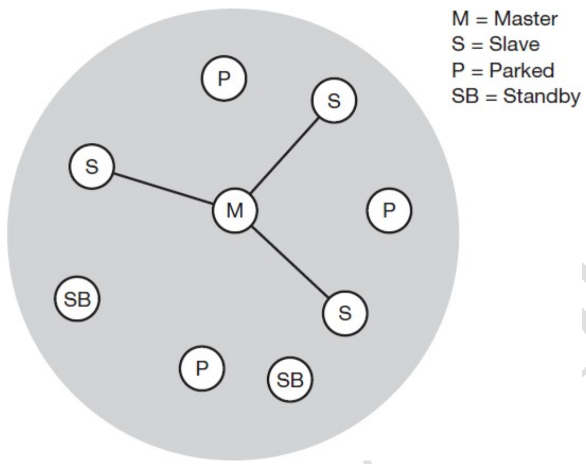
Bluetooth:

- Bluetooth technology discussed here aims at so-called ad-hoc piconets.
- The envisaged gross data rate is 1 Mbit/s, asynchronous (data) and synchronous (voice) services should be available.
- Wireless personal area networks (WPAN) under the following five criteria.

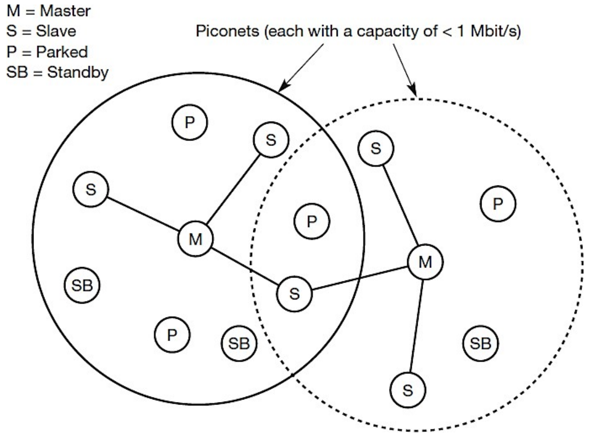
  - ✓ Market Potential
  - ✓ Compatibility
  - ✓ Distinct Identity
  - ✓ Technical Feasibility
  - ✓ Economic Feasibility

Architecture:

- 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 (s).



- Each piconet has unique hopping pattern.
- Two additional types of devices are shown: parked devices (P) cannot actively participate in the piconet
- But are known and can be reactivated within some milliseconds
- Devices in stand-by (SB) do not participate in the piconet.
- Each piconet has exactly one master and up to seven simultaneous slaves.
- More than 200 devices can be parked.
- All active devices are assigned a 3-bit active member address (AMA).
- All parked devices use an 8-bit parked member address (PMA).



- A groups of piconets called scatternet the scatternet consists of two piconets.
- In which one device participates in two different piconets.
- A master can also leave its piconet and act as a slave in another piconet.
- It is clearly not possible for a master of one piconet to act as the master of another piconet as this would lead to identical behavior.

Protocol stack:

- The Bluetooth specification already comprises many protocols and components.
- The Bluetooth protocols but many adaptation function and enhancements.
- The Bluetooth protocol stack can be divided into a core specification
- Which describes the protocols from physical layer to the data link control together with management functions, and profile specifications.

The core protocols of Bluetooth comprise the following elements:

Radio:

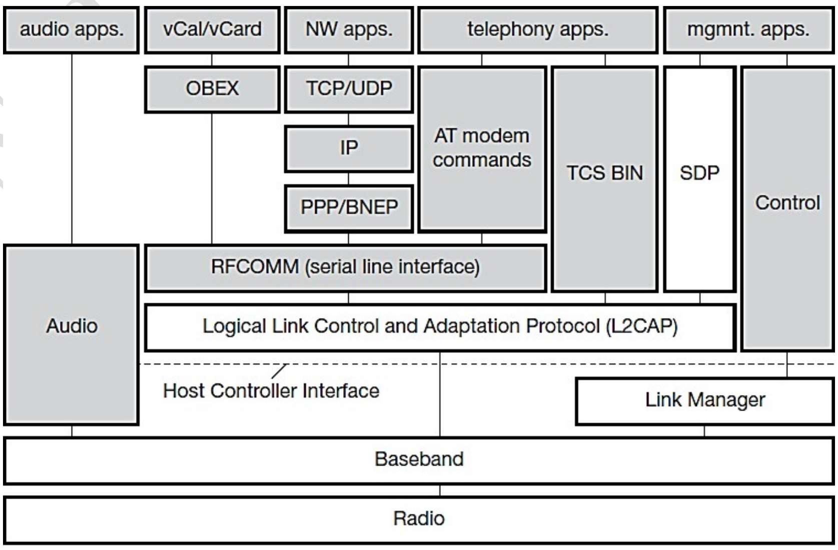
- Specification of the air interface, i.e., frequencies, modulation, and transmit power

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.



AT: attention sequence
OBEX: object exchange
TCS BIN: telephony control protocol specification – binary
BNEP: Bluetooth network encapsulation protocol
SDP: service discovery protocol
RFCOMM: radio frequency comm.

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.

Link manager protocol:

- The 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.

The following groups of functions are covered by the LMP:

Authentication, pairing, and encryption:

- Although basic authentication is handled in the baseband, LMP has to control the exchange of random numbers and signed responses.

Synchronization:

- Precise synchronization is of major importance within a Bluetooth network. The clock offset is updated each time a packet is received from the master.

Capability negotiation:

- Not all Bluetooth devices will support all features that are described in the standard devices have to agree the usage of, e.g., multi-slot packets.

Quality of service negotiation:

- Different parameters control the QoS of a Bluetooth device at these lower layers.

Power control:

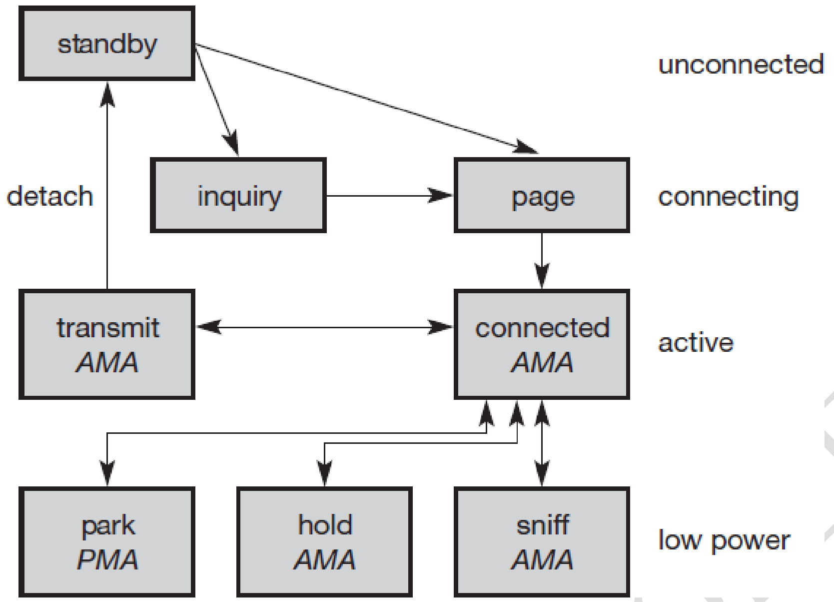
- A Bluetooth device can measure the received signal strength. Depending on this signal level the device can direct the sender of the measured signal to increase or decrease its transmit power

Link supervision:

- LMP has to control the activity of a link, it may set up new SCO links, or it may declare the failure of a link.

State and transmission mode change:

- Devices might switch the master/slave role, detach themselves from a connection, or change the operating mode.



A Bluetooth device can go into one of three low power states:

Sniff state:

- The sniff state has the highest power consumption of the low power states.

Hold state:

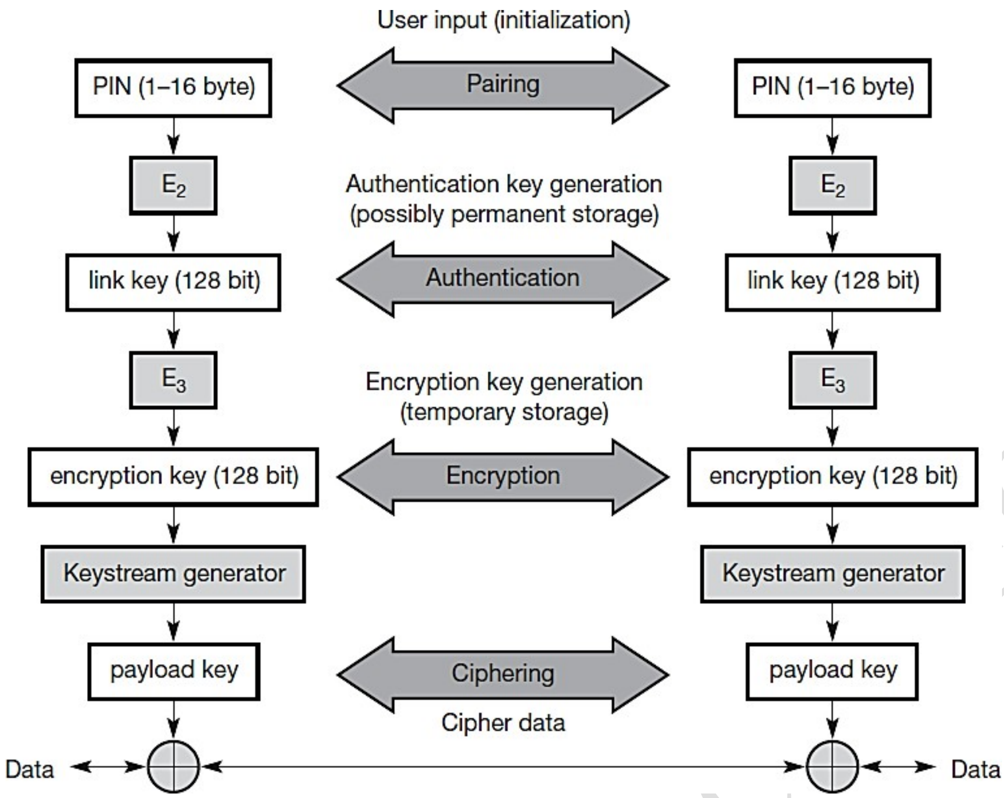
- The device does not release its AMA but stops ACL transmission. A slave may still exchange SCO packets.

Park state:

- In this state the device has the lowest duty cycle and the lowest power consumption.

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 the challenge-response routine.



- The security algorithms use the public identity of a device, a secret private user key, and an internally generated random key as input parameters.
- Several keys can be computed which can be used as link key for authentication.
- The authentication is a challenge-response process based on the link key
- The current clock a payload key is generated for ciphering user data.
- The payload key is a stream of pseudo-random bits.

Mobile Communication

Chapter-IV

Mobile IP:

- Overall view of Mobile IP, and the extensions needed for the internet to support the mobility of hosts.

Goals, assumptions and requirement:

- As shown in chapter 1, mobile computing is clearly the paradigm of the future. The internet is the network for global data communication with hundreds of millions of users.
- A host sends an IP packet with the header containing a destination address with other fields.
- As long as the receiver can be reached within its physical subnet, it gets the packets.
- As soon as it moves outside the subnet.
- A host needs a so-called "**topologically correct address".**

Requirements:

- A more general architecture had to be designed. Many field trials and proprietary systems finally led to mobile IP as a standard to enable mobility in the internet.

Several requirements:

- ✓ Compatibility
- ✓ Transparency
- ✓ Scalability and efficiency
- ✓ Security

Compatibility:

- The installed base of Internet computers, i.e., computers running TCP/IP and connected to the internet, is huge.
- Mobile IP has to be integrated into existing operating systems or at least work with them routing.

Transparency:

- Mobility should remain „invisible" for many higher layer protocols and applications.
- The mobile computer has changed its point of attachment to the network.
- The only effects of mobility should be a higher delay and lower bandwidth.

Scalability and efficiency:

- Introducing a new mechanism to the internet must not jeopardize its efficiency.
- Special care has to be taken considering the lower bandwidth of wireless links.
- The number of computers connected to the internet and at the growth rates of mobile communication.

Security:

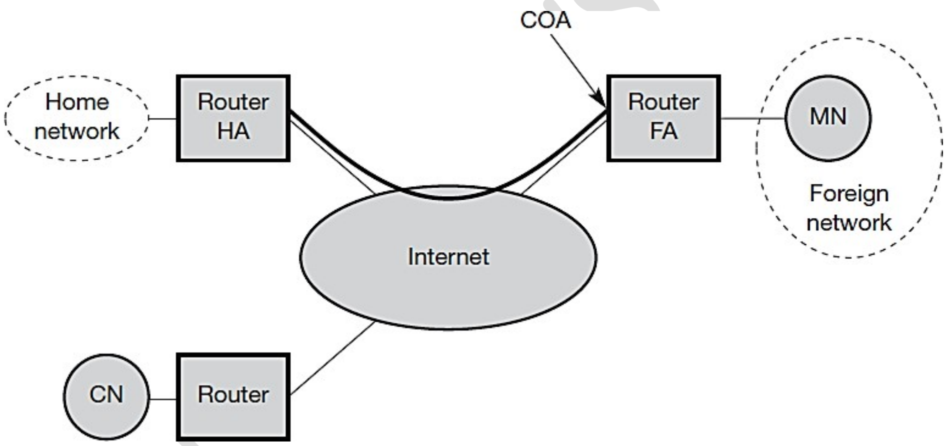
- Mobility poses many security problems. The minimum requirement is that of all the messages related to the management of Mobile IP are authenticated.

Entities and terminology:

- The following defines several entities and terms needed to understand mobile IP.

Mobile node (MN):

- A mobile node is an end-system or router that can change its point of attachment to the internet using mobile IP.



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.

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 the home network.

Foreign network:

- The foreign network is the current subnet the MN visits and which is not the home network.

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 tunnel endpoint and forwarding packets to the MN.

Care-of addresses (COA):

- The COA defines the current location of the MN from an IP point of view.

There are two different possibilities

- ✓ Foreign Agent COA
- ✓ Co-located COA

Foreign agent COA:

- The COA could be located at the FA 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 COA.

Home agent (HA):

- The HA provides several services for the MN and is located in the home network.

Three alternatives for the implementation of an HA.

- The HA can be implemented on a router that is responsible for the home network.
- If changing the router"s software is not possible, the HA could also be implemented on an arbitrary node in the Subnet.
- Finally, a home network is not necessary at all. The HA could be again on the „router" but this time only acting as a Manager.

IP packet delivery:

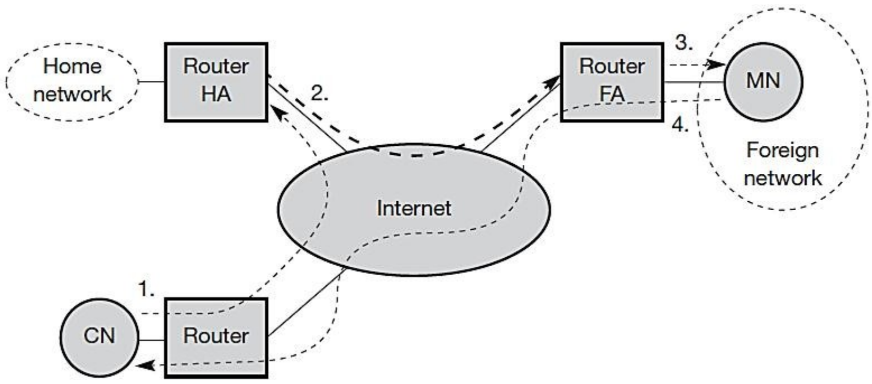
- A correspondent node CN wants to send an IP packet to the MN.

Step 1:

- CN does not need to know anything about the MN"s current location and sends the packet as usual to the IP address of MN.

Step 2:

- A new header is put in front of the old IP header showing the COA as new destination and HA as source of the encapsulated packet.



Step 3:

- The additional header and forwards the original with CN as source and MN as destination to the MN.

Step 4:

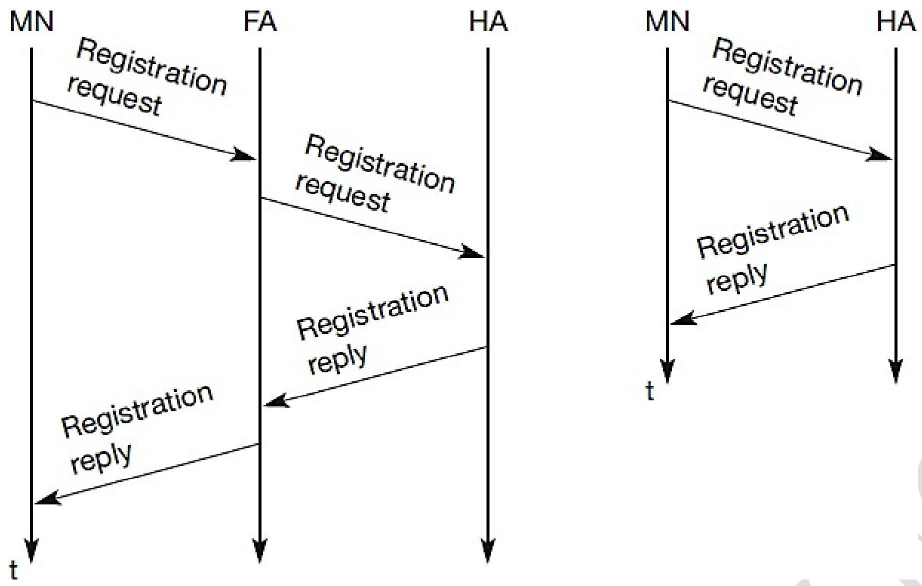
- The MN sends the packet as usual with its own fixed IP address as source and CN"s address as destination.

Registration:

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

Registration can be done in two different ways:

- The MN sends its registration request containing the COA to the FA which is forwarding the request to the HA.
- The HA now sets up a **mobility binding** containing the mobile node"s home IP address and the current COA.
- The MN may send the request directly to the HA. This by the way is also the registration procedure for MNs returning to their home network.



Tunneling and encapsulation:

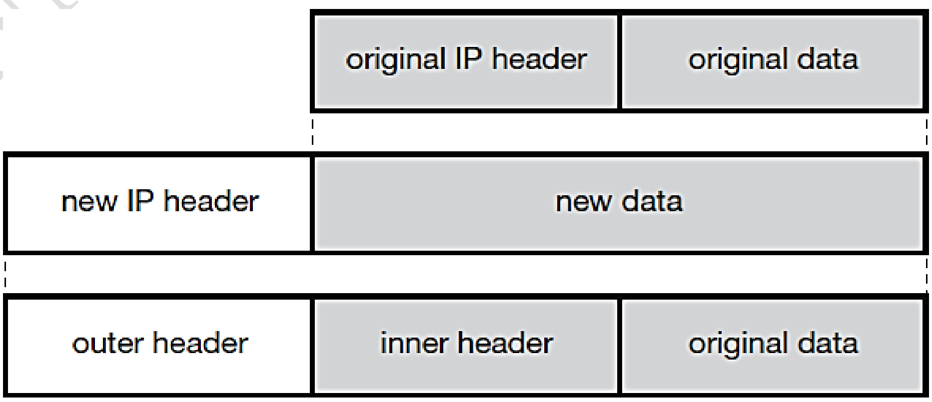
- The tunnel establishes a virtual pipe for data packets between a tunnel entry and a tunnel endpoint.
- Packets entering a tunnel are forwarded inside the tunnel and leave the tunnel unchanged.
- Sending a packet through a tunnel is achieved by using encapsulation.

Encapsulation:

- The mechanism of taking a packet consisting of packet header and data and putting it into the data part of a new packet.

Decapsulation.

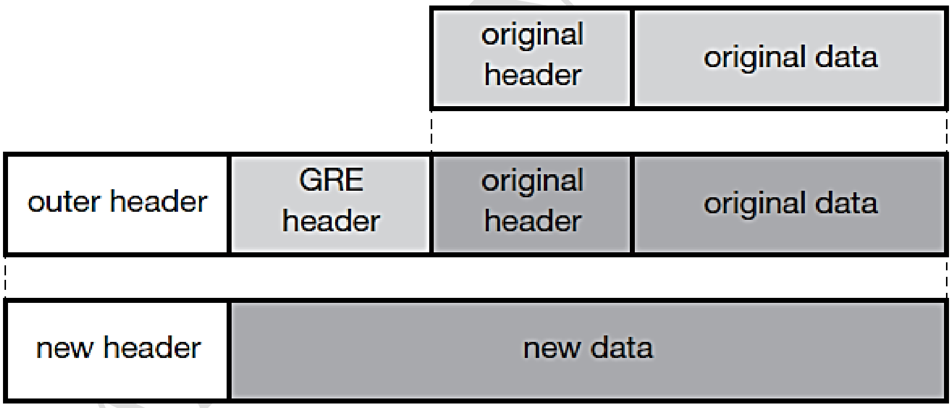
- The reverse operation talking a packet out of the data part of another is called decapsulation.



- Encapsulation and decapsulation are the operations typically performed when a packet is transferred from a higher protocol layer to a lower layer or from a lower to a higher layer respectively.
- The data part of a new packet and sets the new IP header in such a way that the packet is routed to the COA. The new header is also called the **outer header** for obvious reasons.
- Which can be identical to the original header as this is the case for IP-in-IP encapsulation, or the inner header can be computed during encapsulation.
- There are different ways of performing the encapsulation needed for the tunnel between HA and COA.

Generic routing encapsulation:

- IP-in-IP encapsulation and minimal encapsulation work only for IP, the following encapsulation scheme also supports other network layer protocols in addition to IP.
- **Generic routing encapsulation** (GRE) allows the encapsulation of packets of one protocol suite into the payload portion of a packet of another protocol.



Optimizations:

- One way to optimize the route is to inform the CN of the current location of the MN.
- The CN can learn the location by caching it in a **binding cacher.**
- Which is a part of the local routing table for the CN.

The optimized mobile IP protocol needs four additional messages.

- ✓ Binding request
- ✓ Binding update
- ✓ Binding acknowledgement
- ✓ Binding warning

Binding request:

- Any node that wants to know the current location of an MN can send a binding request to the HA.

Binding update:

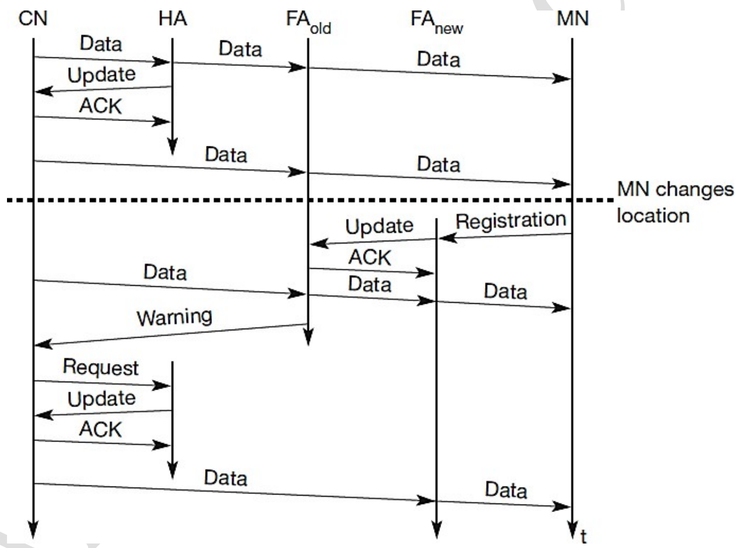
- This message sent by the HA to CNs reveals the current location of an MN.

Binding acknowledgement:

- If requested, a node returns this acknowledgement after receiving a binding update message.

Binding warning:

- If a node decapsulates a packet for an MN, but it is not the current FA for this MN, this node sends a Binding warning.



- The CN can request the current location from the HA. If allowed by the MN.
- The HA returns the COA of the MN via an update message.
- The CN acknowledges this update message and stores the mobility binding.
- The CN can send its data directly to the current foreign agent FA old.
- FA old forwards the packets to the MN.
- The MN might now change its location and register with a new foreign agent, FAnew.
- This registration is also forwarded to the HA to update its location database.
- Furthermore, FAnew informs FAold about the new registration of MN.
- MN"s registration message contains the address of FAold for this purpose.
- FAold might now forward these packets to the new COA of MN which is FAnew.

Reverse tunneling:

- The MN can directly send its packets to the CN as in any other standard IP situation.
- The destination address in the packets is that of CN.

Firewalls:

- Almost all companies and many other institutions secure their internal networks connected to the Internet with the help of a firewall.

Multi-cast:

- While the nodes in the home network might participate in a multi-cast group, an MN in a foreign network cannot transmit multi-cast packets in a way that they emanate from its home network without a reverse tunnel.

TTL:

- An MN sending packets with a certain TTL while still in its home network.
- The TTL might be low enough so that no packet is transmitted outside a certain region.

Mobile ad-hoc networks:

- It is important to note that this section focuses on so-called multi-hop ad-hoc networks when describing ad-hoc networking.
- The ad-hoc setting up of a connection with an infrastructure is not the main issue here.
- These networks should be mobile and use wireless communications.
- The use of such mobile, wireless, multi-hop ad-hoc networks.

Ad-hoc networks here for simplicity, here:

- ✓ Instant infrastructure
- ✓ Disaster relief
- ✓ Remote areas
- ✓ Effectiveness

Instant infrastructure:

- Unplanned meetings, spontaneous interpersonal communications etc. cannot rely on any infrastructure.
- Infrastructures need planning and administration.

Disaster relief:

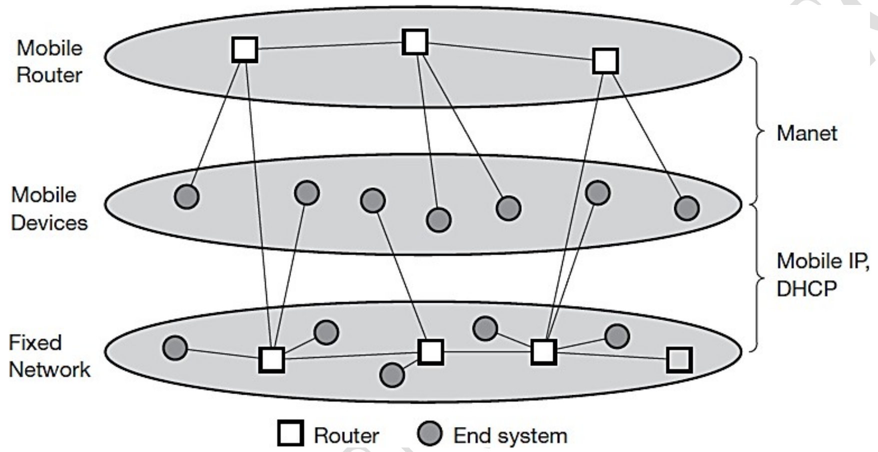
- Infrastructures typically break down in disaster areas. Hurricanes cut phone and power lines, floods destroy base stations, fires burn servers.

Remote areas:

- Even if infrastructures could be planned ahead, it is sometimes too expensive to set up an infrastructure in sparsely populated areas.
- Depending on the communication pattern, ad-hoc networks or satellite infrastructures can be a solution.

Effectiveness:

- Services provided by existing infrastructures might be too expensive for certain applications.

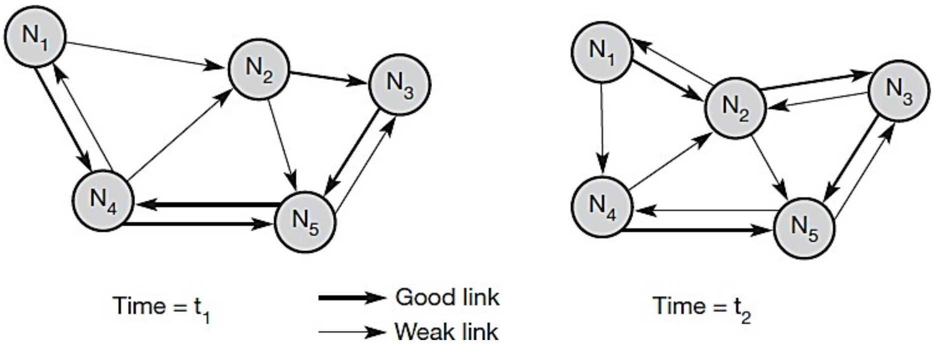


- Over the last few years ad-hoc networking has attracted a lot of research interest.
- This has led to creation of a working group at the IETF that is focusing on **mobile ad-hoc networking**, called **MANET.**
- The reason for having a special section about ad-hoc networks within a the network layer is that routing of data is one of the most difficult issues in ad-hoc networks.
- One of the first ad-hoc wireless networks was the packet radio network started by ARPA in 1973.

- It allowed up to 138 nodes in the ad-hoc network and used IP packets for data transport.
- A variant of distance vector routing was used in this ad-hoc network

Routing:

- The case in an ad-hoc network. A destination node might be out of range of a source node transmitting packets.
- Within a cell, the base station can reach all mobile nodes without routing via a broadcast.
- In the case of ad-hoc networks, each node must be able to forward data for other nodes.



- Five nodes, N1 to N5, are connected depending on the current transmission.
- N4 can receive N1 over a good link.
- N1 receives N4 only via a weak link
- N1 cannot receive N2 at all, N2 receives a signal from N1.
- N1 cannot receive N4 any longer, N4 receives N1 only via a weak link.
- But now N1 has an asymmetric but bi-directional link to N2 that did not exist before.

❖ Asymmetric links
❖ Redundant links
❖ Interference
❖ Dynamic topology

Asymmetric links:

- Node A receives a signal from node B. But this does not tell us anything about the quality of the connection in reverse.

Redundant links:

- Wired networks, too, have redundant links to survive link failures.
- There is only some redundancy in wired networks, which, Additionally, are controlled by a network administrator.

Interference:

- In wired networks links exist only where a wire exists, and connections are planned by network administrators.

Dynamic topology:

- The greatest problem for routing arises from the highly dynamic topology.
- The mobile nodes might move as or medium characteristics might change.

Time t1:

- Which is not always the case in ad-hoc networks, it would choose the path N1, N2, N3, for this requires only two hops.

Time t2:

- The topology has changed. Now N3 cannot take the same path to send acknowledgements back to N1, while N1 can still take the old path to N3.

Mobile Communication

Chapter-V

Wireless application protocol:

- The **wireless application protocol (WAP)** version 1. x is the main part.
- WAP is a common effort of many companies and organizations to set up a framework for wireless and mobile web access using many different transport systems.
- WAP combines the telephone network and the internet by integrating telephony applications into the web using its own wireless markup language (WML) and scripting language (WML Script).

File systems:

- The general goal of a file system is to support efficient, transparent, and consistent access to files.

Efficiency:

- **Efficiency** is of special importance for wireless systems as the bandwidth is low so the protocol overhead and updating operations.

Transparency:

- **Transparency** addresses the problems of location- dependent views on a file system.

Consistency:

- The main problem is **consistency** .General problems are the limited resources on portable devices and the low bandwidth of the wireless access.

Wireless application protocol (version 1.x):

- The growth of the internet, internet applications, and mobile communications led to many early proprietary solutions providing internet services for mobile, wireless devices.
- The **wireless application protocol forum (WAP Forum)** was founded in June 1997 by Ericsson, Motorola, Nokia, and Unwired Planet.
- The open mobile architecture forum and the SyncML initiative formed the **open mobile alliance.**

- The basic objectives of the WAP Forum and now of the OMA are to bring diverse internet content and other data services to digital cellular phones and other wireless, mobile terminals.
- A protocol suite should enable global wireless communication across different wireless network technologies.

Interoperable:

- Terminals and software from different vendors to communicate with networks from different providers.

Scaleable:

- Protocols and services should scale with customer needs and number of customers.

Efficient:

- Provision of QoS suited to the characteristics of the wireless and mobile networks.

Reliable:

- Provision of a consistent and predictable platform for deploying services.

Secure:

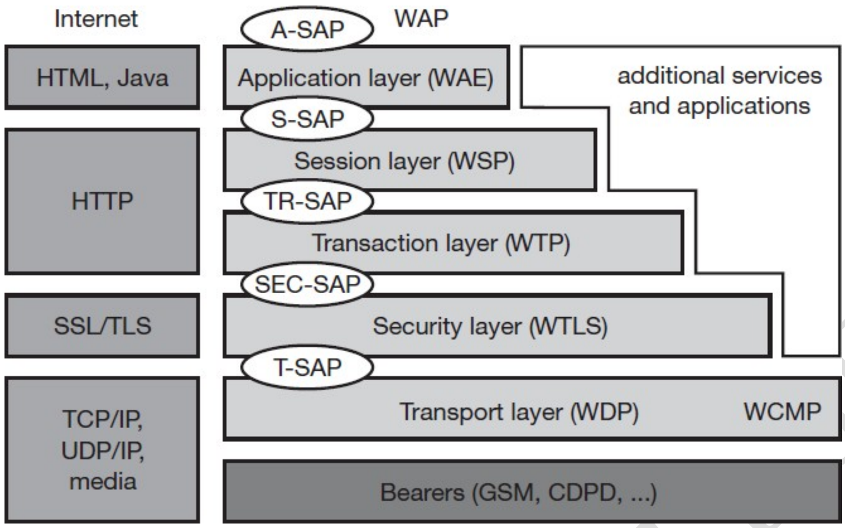
- Preservation of the integrity of user data, protection of devices and services from security problems.

Architecture:

- The WAP architecture, its protocols and components, and compares this architecture with the typical internet architecture when using the World Wide Web.
- This comparison is often cited by the WAP Forum and it helps to understand the architecture.
- This comparison can be misleading as not all components and protocols shown at the same layer are comparable.

Bearer services:

- The basis for transmission of data is formed by different **bearer services**.
- WAP does not specify bearer services, but uses existing data services and will integrate further services.



Transport layer:

- The **transport layer** with its **wireless datagram protocol (WDP)** and the additional **wireless control message protocol (WCMP),** because the adaptation of these protocols are bearer-specific.
- Datagram-oriented service to the higher layers of the WAP architecture.
- Communication is done transparently over one of the available bearer services.

Security layer:

- The **security layer** with its **wireless transport layer security** protocol **WTLS** offers its service at the **security SAP (SEC-SAP)**.
- WTLS is based on the transport layer security already known from the www.

Transaction layer:

- The WAP **transaction layer** with its **wireless transaction protocol (WTP)** offers a lightweight transaction service at the **transaction SAP (TR-SAP)**.

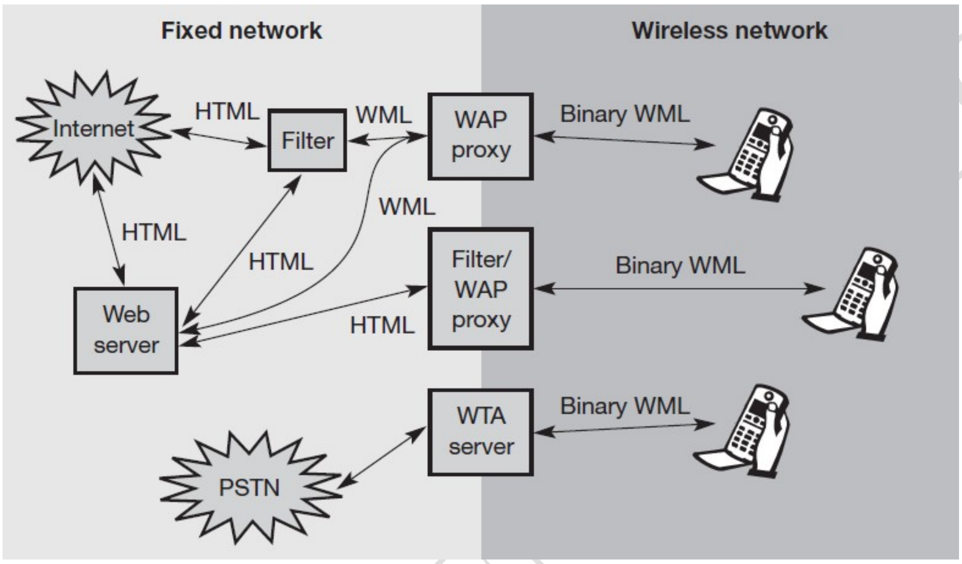
- This service efficiently provides reliable or unreliable requests and asynchronous transactions.

Session layer:

- The **session layer** with the **wireless session protocol (WSP)** currently offers two services at the **session-SAP (S-SAP)**.
- One connection-oriented and one connectionless if used directly on top of WDP.

Application layer:

- The **application layer** with the **wireless application environment (WAE)** offers a framework for the integration of different www and mobile telephony applications.
- The WAP transport layer together with the bearers can be (roughly) compared to the services offered by TCP or UDP.
- WAP does not always force all applications to use the whole protocol architecture.



- The current www in the internet offers web pages with the help of HTML and web servers.
- Special filters within the fixed network can now translate HTML into WML.
- Web servers can already provide pages in WML, or the gateways between the fixed and wireless network can translate HTML into WML.
- In a similar way, a special gateway can be implemented to access traditional telephony services via binary WML.
- This wireless telephony application (WTA) server translates, signaling of the telephone network.

Wireless markup language:

- The **wireless markup language (WML)** is based on the standard HTML.
- When designing WML, several constraints of wireless handheld devices had to be taken into account.
- Current handheld devices have small displays, limited user input facilities, limited memory, and only low performance computational resources.
- WML follows a deck and card metaphor. A WML document is made up of multiple **cards**.
- Cards can be grouped together into a **deck**.

- A WML deck is similar to an HTML page, in that it is identified by a URL and is the unit of content transmission.
- The WML browser fetches decks as required from origin servers.
- Either these decks can be static files on the server or they can be dynamically generated.
- It is important to note that WML does not specify how the implementation of a WML browser has to interact.

WML includes several basic features:

Text and images:

- WML gives, as do other mark-up languages, hints how text and images can be presented to a user.
- WML only provides a set of mark-up elements, such as emphasis elements (bold, italic, etc.) for text, or tab Columns for tabbing alignment.

User interaction:

- WML supports different elements for user input.
- The user agent is free to choose how these inputs are implemented. They could be bound to, e.g., physical keys, soft keys, or voice input.

Navigation:

- As with HTML browsers, WML offers a history mechanism with navigation through the browsing history, hyperlinks and other inter card navigation elements.

Context management:

- WML allows for saving the state between different decks without server interaction.

Ex.Prog:

```
<?xml version="1.0"?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.1//EN"
"http://www.wapforum.org/DTD/wml_1.1.xml">
<wml>
<card id="card_one" title="Simple example">
<do type="accept">
<go href="#card_two"/>
</do>
<p>
This is a simple first card!
```

```
<br/>
On the next one you can choose ...
</p>
</card>
<card id="card_two" title="Pizza selection">
<do type="accept" label="cont">
<go href="#card_three"/>
</do>
<p>
... your favourite pizza!
<select value="Mar" name="PIZZA">
<option value="Mar">Margherita</option>
<option value="Fun">Funghi</option>
<option value="Vul">Vulcano</option>
</select>
</p>
</card>
<card id="card_three" title="Your Pizza!">
<p>
Your personal pizza parameter is <b>$(PIZZA)</b>!
</p>
</card>
</wml>
```

WMLScript:

- WMLScript complements to WML and provides a general scripting capability in the WAP architecture.

WMLScript offers several capabilities not supported by WML.

- ✓ Validity check of user input.
- ✓ Access to device facilities.
- ✓ Local user interaction.

Validity check of user input:

- WMLScript can check the validity and save bandwidth and latency in case of an error.

Access to device facilities:

- WMLScript offers functions to access hardware components and software functions of the device.

Local user interaction:

- Without introducing round-trip delays WMLScript can directly and locally interact with a user, show.
- Messages or prompt for input.

Extensions to the device software:

- With the help of WMLScript a device can be configured and new functionality can be added even after deployment.
- WMLScript is based on JavaScript but adapted to the wireless environment.
- A WMLScript compiler is used to generate this byte code. This compiler may be located in a gateway or the origin servers store pre-compiled WMLScript byte code.
- WMLScript can set and read WML variables.
- WMLScript provides many features known from standard programming languages such as functions, expressions, or while, if,for, return etc.
- The WMLScript compiler can compile one or more such scripts into a **WMLScript compilation unit**.

Ex.Prog:

```
function pizza_test(pizza_type)
{
var taste = "unknown";
if (pizza_type = "Mar")
{
taste = "well... ";
}
else
{
if (pizza_type = "Vul")
{
taste = "quite hot";
};
};
return taste;
};
```

There are six libraries:

Lang:

- This library provides functions closely related to WMLScipt itself.

Float:

- Many typical arithmetic floating-point operations are in this library.

String:

- Many string manipulation functions are in this library.

URL:

- This library provides many functions for handling URLs

WMLBrowser:

- This library provides several functions typical for a browser, such as prev to go back one card or refresh to update the context of the user interface.

Dialogs:

- For interaction with a user, this library has been defined.

Wireless telephony application:

- Browsing the web using the WML browser is only one application for a handheld device user.
- This is where the **wireless telephony application (WTA)**.
- The **WTA user agent** and the **wireless telephony application interface.**
- WTA is a collection of telephony specific extensions for call and feature control mechanisms, merging data networks and voice networks.
- The WTA framework integrates advanced telephony services using a consistent user interface
- To allows network operators to increase accessibility for various special services in their network.
- WTA should enable third-party developers as well as network operators to create network-independent content that accesses the basic features of the bearer network.

WTA extends the basic WAE application model in several ways:

Content push:

- A WTA origin server can push content, WML decks or WMLScript, to the client.
- A push can take place without prior client request.

Access to telephony functions:

- The **wireless telephony application interface** provides many functions to handle telephony events.

Repository for event handlers:

- The repository represents a persistent storage on the client for content required to offer WTA services.

Security model:

- Mandatory for WTA is a security model as many frauds happen with wrong phone numbers or faked services.

Three classes of libraries have been defined:

Common network services:

- The **call control** library contains, functions to set up, accept, and release calls.
- **Network text** contains functions to send, read, and delete text messages.
- **Phonebook** allows for the manipulation of the local phonebook entries.

Network specific services:

- Libraries in this class depend on the capabilities of the mobile network.

Public services:

- This class contains libraries with publicly available functions.
- The third-party providers may use, not just network operators.
- One example is "make call" to set up a phone call.

XML:

XML-Extensible Markup Language:

- XML it is important to understand as a document.
- The family of markup language that includes XML.
- XML the markup takes the form of „tags"enclosed inangle-brackets<>.

Tags are used in pairs:

<tag>

</tag>

Ex:

<Title>

<Welcome>

</title>

XML"s major role in Data representation and exchange.

Example Program:

```
<Bank>
    <account>
        <ac.no>A-101</ac.no>
        <branch-name>Downtown</branch-name>
        <balance>500</balance>
        </account>
</bank>
```

Structure Of XML Data:

- XML document is the „element".
- XML specifies the notion of an attribute.
- Element- **"Start and End tags"**

XML document must properly:

<account>….<balance>….</balance>….</account>

XML document not properly:

<account>….<balance>….</account>….</balance>

Storage Of XML Data:

- The many application requires storage of XML data.
- One way to store XML data convert is „relational representation".
- Another way to store XML data is „relational database'.

Relational Database:

- The relational database is widely used in exchange application.
    1. Store as string
    2. Tree representation
    3. Map to relations

Store as string:

- A simple way to store XML data is to store the top element in separate tuple.

Ex:

Elements (data)

Data-tuple

Tree representation:

XML data can be modeled as a tree and stored using pair of relation.

Ex:

Nodes (id,type,label,value)

Map to relations:

- XML elements whose schema is mapped to relations & attributes.

XML Application:

- XML document are designed to be exchanged between application.

Two application of XML:

1. Exchange of data
2. Data mediation

Exchange of data:

- XML representation of data for variety of specialized application.

Data Mediation:

- XML data from HTML web pages.
- Mediator application used to extracted information.