UNIT – 1

UNIT I INTRODUCTION 9

Wireless Transmission – signal propagation – Free space and two ray models – spread spectrum – Satellite Networks – Capacity Allocation – FDMA –TDMA- SDMA – DAMA

Wireless Transmission

Unguided transmission techniques commonly used for information communications include broadcast radio, terrestrial microwave, and satellite. Infrared transmission is used in some LAN applications. Three general ranges of frequencies are of interest in our discussion of wireless transmission.

Frequencies in the range of about 1 to 40 GHz are referred to as **microwave frequencies**. At these frequencies, highly directional beams are possible, and microwave is quite suitable for point-to-point transmission. Microwave is also used for satellite communications.

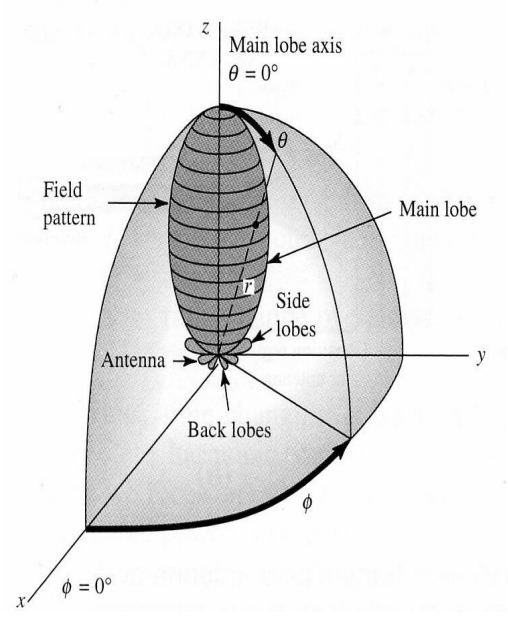
Frequencies in the range of 30 MHz to 1 GHz are suitable for omnidirectional applications. We refer to this range as the **radio** range.

Another important frequency range is the infrared portion of the spectrum, roughly from 3×10^{11} to 2×10^{14} Hz. Infrared is useful to local point-to-point and multipoint applications within confined areas, such as a single room.

Signal Propagation

Antenna

- ✓ An antenna is an electrical conductor or system of conductors.
  - Transmission - radiates electromagnetic energy into space
  - Reception - collects electromagnetic energy from space
- ✓ In two-way communication, the same antenna can be used for transmission and reception.
- ✓ Radiation pattern
  - Graphical representation of radiation properties of an antenna
  - Depicted as two-dimensional cross section



- ✓ Beam width (or half-power beam width)
  - Measure of directivity of antenna
- ✓ Reception pattern
  - Receiving antenna's equivalent to radiation pattern
- ✓ Types of Antenna
  - Isotropic antenna (idealized)
    - Radiates power equally in all directions
  - Dipole antennas
    - Half-wave dipole antenna (or Hertz antenna)
    - Quarter-wave vertical antenna (or Marconi antenna)
  - Parabolic Reflective Antenna
- ✓ Antenna gain
  - Power output, in a particular direction, compared to that produced in any direction by a perfect omnidirectional antenna (isotropic antenna)
- ✓ Effective area
  - Related to physical size and shape of antenna
- ✓ Relation between antenna gain and effective area
  - $$G = \frac{4\pi A_e}{\lambda^2} = \frac{4\pi f^2 A_e}{c^2}$$
  - G = antenna gain, Ae = effective area, f = carrier frequency, c = speed of light (» 3 ´ 108 m/s), λ= carrier wavelength.

11 (a) (ii) Wave Propagation Modes

- ✓ **Ground-wave propagation**
  - Follows contour of the earth
  - Can Propagate considerable distances
  - These are mainly used for transmission between the surface of the earth and the ionosphere.
  - Frequencies up to 2 MHz(low 30–300 kHz (30,000–300,000 Hz)and medium frequency300–3000 kHz (300,000–3,000,000 Hz) range of radio spectrum)
  - Beyond the horizon, the waves get blocked by the curvature of the earth and the signals are produced by the diffracted surface wave.

Frequency of ground waves depending on the type of ground

Type of ground	**f = 1 MHz**	**f = 10 MHz**	**f = 100 MHz**
Dry ground like desert	10^{-4}	10^{-4}	10^{-4}
Very moist ground like fields	10^{-2}	10^{-2}	2.10^{-2}
Fresh water at 20℃	3.10^{-3}	3.10^{-3}	5.10^{-3}
Sea water at 20℃	5	5	5

Advantages of Ground Wave Propagation

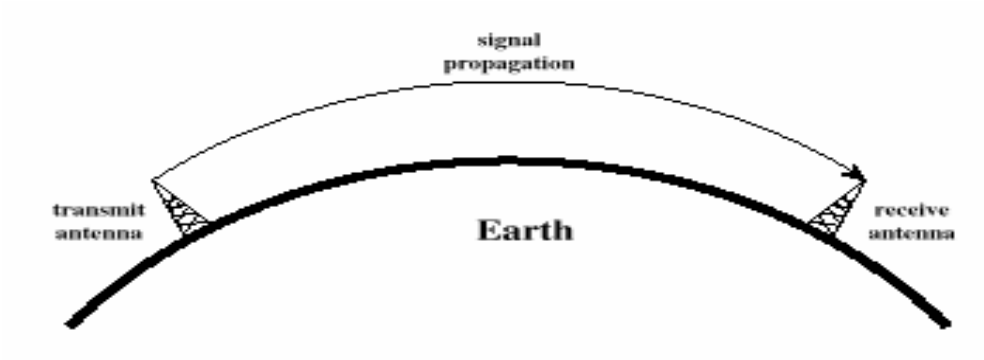
- These waves have the tendency to bend around the corners or obstructions during propagation which makes them more efficient and also these are not affected by the change in atmospheric conditions.

Disadvantages of Ground Wave Propagation

- High-frequency waves cannot be transmitted as the energy losses are more because of the absorption of energy in the earth's atmosphere.
- These are used to cover short ranges and also involves attenuation of waves as they interact with the eddy currents produced by the surface of the earth.

Applications Ground Wave Propagation

- These can be used for one-way communication from the military to submerged submarines as they penetrate to a significant depth into seawater.
- AM, FM and television broadcasting can be done with the help of ground waves.



- ✓ **Sky-wave propagation**
  - Signal reflected from ionized layer of atmosphere back down to earth
  - Signal can travel a number of hops, back and forth between ionosphere and earth's surface
  - Reflection effect caused by refraction
    Falls in high frequency range of radio spectrum 3–30 MHz (3,000,000–30,000,000 Hz)
    Advantages :

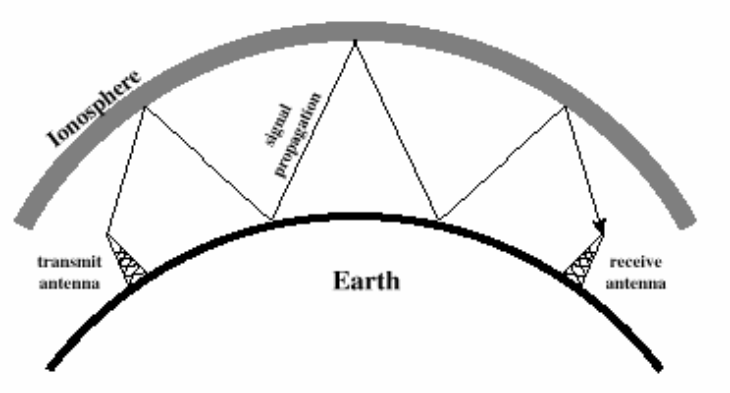
      - As it utilizes reflective property of ionosphere available above earth at higher frequencies, it is most simple mode of propagation and provides continuous support in communications.

    Disadvantages

      - Required large power for transmission, Ionoshere is present near or far during night time and day time respectively. Due to this, Sky waves can travel longer or smaller distances.
      - Required large antennas, Transmitter signal travels multiple hops before reaching the receiver. This reduces signal strength considerably if distances are larger between transmitter and receiver antennas.

- limited frequency range of propagation

  - Examples
  - amateur radio operators
  - commercial marine and aircraft communications, and also to shortwave broadcasters



✓ Line-of-sight propagation

- Transmitting and receiving antennas must be within line of sight
  - Satellite communication – signal above 30 MHz not reflected by ionosphere
  - Ground communication – antennas within effective line of site due to refraction
- Refraction – bending of microwaves by the atmosphere
  - Velocity of electromagnetic wave is a function of the density of the medium
  - When wave changes medium, speed changes
  - Wave bends at the boundary between mediums

Optical line of sight Effective,

$d = 3.57\sqrt{h}$

or radio, line of sight $d = 3.57\sqrt{kh}$

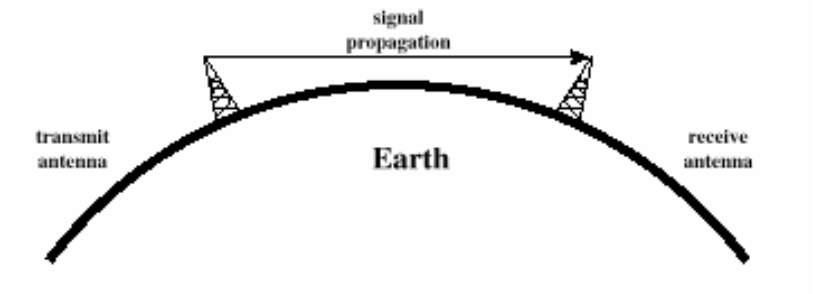
• d = distance between antenna and horizon (km) •

h = antenna height (m)

• K = adjustment factor to account for refraction, rule of thumb K = 4/3

Application:

As the signal can travel only to lesser distances in this mode, this transmission is used for **infrared** or **microwave transmissions**.



LOS Wireless Transmission Impairments

Attenuation

Free space loss

Distortion

Dispersion

Noise

Other effects:

Atmospheric absorption

Multipath

Refraction

- ✓ **Free space path loss model**
- ✓ Consider a signal transmitted through free space to a receiver located at distance d from the transmitter. Assume there are no obstructions between the transmitter and receiver and the signal propagates along a straight line between the two. The channel model associated with this transmission is called a line-of-sight (LOS) channel, and the corresponding received signal is called the LOS signal or ray. Free-space path loss introduces a complex scale factor , resulting in the received signal.
- ✓
- ✓ $$r(t) = \Re\left\{\frac{\lambda\sqrt{G_l}e^{-j2\pi d/\lambda}}{4\pi d}u(t)e^{j2\pi f_c t}\right\}$$
- ✓ where$\sqrt{G_l}$ is the product of the transmit and receive antenna field radiation patterns in the LOS direction. The phase shift e^−j2πd/λ is due to the distance d the wave travels.
- ✓ The power in the transmitted signal s(t) is P_t, so the ratio of received to transmitted power
- ✓ $$\frac{P_r}{P_t} = \left[\frac{\sqrt{G_l}\lambda}{4\pi d}\right]^2$$ 0
- ✓ Thus, the received signal power falls off inversely proportional to the square of the distance d between the transmit and receive antennas. We will see in the next section that for other signal propagation models, the received signal power falls off more quickly relative to this distance. The received signal power is also proportional to the square of the signal wavelength, so as the carrier frequency increases, the received power decreases. This dependence of received power on the signal wavelength λ is due to the effective area of the receive antenna. However, directional antennas can be designed so that receive power is an increasing function of frequency for highly directional links. The received power can be expressed in dBm as

$$P_r \text{ dBm} = P_t \text{ dBm} + 10\log_{10}(G_l) + 20\log_{10}(\lambda) - 20\log_{10}(4\pi) - 20\log_{10}(d).$$

Free-space path loss is defined as the path loss of the free-space model:

$$P_L \text{ dB} = 10\log_{10}\frac{P_t}{P_r} = -10\log_{10}\frac{G_l\lambda^2}{(4\pi d)^2}.$$

The **free-space path gain** is thus

$$P_G = -P_L = 10\log_{10}\frac{G_l\lambda^2}{(4\pi d)^2}.$$

Two ray model

The two-ray model is used when a single ground reflection dominates the multipath effect, as illustrated in Figure 2.4. The received signal consists of two components: the LOS component or ray, which is just the transmitted signal propagating through free space, and a reflected component or ray, which is the transmitted signal reflected off the ground.

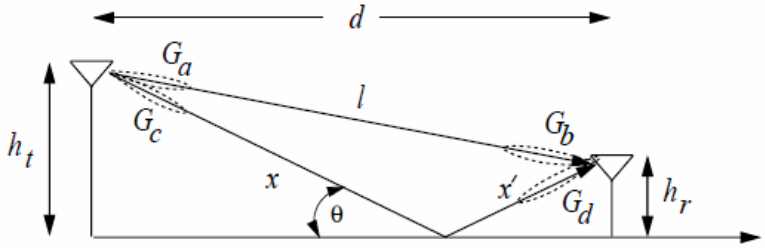


Figure 2.4: Two-Ray Model.

The received LOS ray is given by the free-space propagation loss formula (2.6). The reflected ray is shown in Figure 2.4 by the segments x and x'. If we ignore the effect of surface wave attenuation[2] then, by superposition, the received signal for the two-ray model is

$$r_{2ray}(t) = \Re\left\{\frac{\lambda}{4\pi}\left[\frac{\sqrt{G_l}u(t)e^{-j2\pi l/\lambda}}{l} + \frac{R\sqrt{G_r}u(t-\tau)e^{-j2\pi(x+x')/\lambda}}{x+x'}\right]e^{j2\pi f_c t}\right\}, \tag{2.11}$$

where $\tau = (x + x' - l)/c$ is the time delay of the ground reflection relative to the LOS ray, $\sqrt{G_l} = \sqrt{G_a G_b}$ is the product of the transmit and receive antenna field radiation patterns in the LOS direction, R is the ground reflection coefficient, and $\sqrt{G_r} = \sqrt{G_c G_d}$ is the product of the transmit and receive antenna field radiation patterns corresponding to the rays of length x and x', respectively. The **delay spread** of the two-ray model equals the delay between the LOS ray and the reflected ray: $(x + x' - l)/c$.

If the transmitted signal is narrowband relative to the delay spread ($\tau << B_u^{-1}$) then $u(t) \approx u(t-\tau)$. With this approximation, the received power of the two-ray model for narrowband transmission is

$$P_r = P_t\left[\frac{\lambda}{4\pi}\right]^2\left|\frac{\sqrt{G_l}}{l} + \frac{R\sqrt{G_r}e^{-j\Delta\phi}}{x+x'}\right|^2, \tag{2.12}$$

where $\Delta\phi = 2\pi(x + x' - l)/\lambda$ is the phase difference between the two received signal components. Equation (2.12) has been shown to agree very closely with empirical data [15]. If d denotes the horizontal separation of the antennas, h_t denotes the transmitter height, and h_r denotes the receiver height, then using geometry we can show that

$$x + x' - l = \sqrt{(h_t + h_r)^2 + d^2} - \sqrt{(h_t - h_r)^2 + d^2}. \tag{2.13}$$

When d is very large compared to $h_t + h_r$ we can use a Taylor series approximation in (2.13) to get

$$\Delta\phi = \frac{2\pi(x + x' - l)}{\lambda} \approx \frac{4\pi h_t h_r}{\lambda d}. \tag{2.14}$$

The ground reflection coefficient is given by [2, 16]

$$R = \frac{\sin\theta - Z}{\sin\theta + Z}, \tag{2.15}$$

where

$$Z = \begin{cases} \sqrt{\epsilon_r - \cos^2\theta}/\epsilon_r & \text{for vertical polarization} \\ \sqrt{\epsilon_r - \cos^2\theta} & \text{for horizontal polarization} \end{cases}, \tag{2.16}$$

and ϵ_r is the dielectric constant of the ground. For earth or road surfaces this dielectric constant is approximately that of a pure dielectric (for which ϵ_r is real with a value of about 15).

We see from Figure 2.4 and (2.15) that for asymptotically large d, $x + x' \approx l \approx d$, $\theta \approx 0$, $G_l \approx G_r$, and $R \approx -1$. Substituting these approximations into (2.12) yields that, in this asymptotic limit, the received signal power is approximately

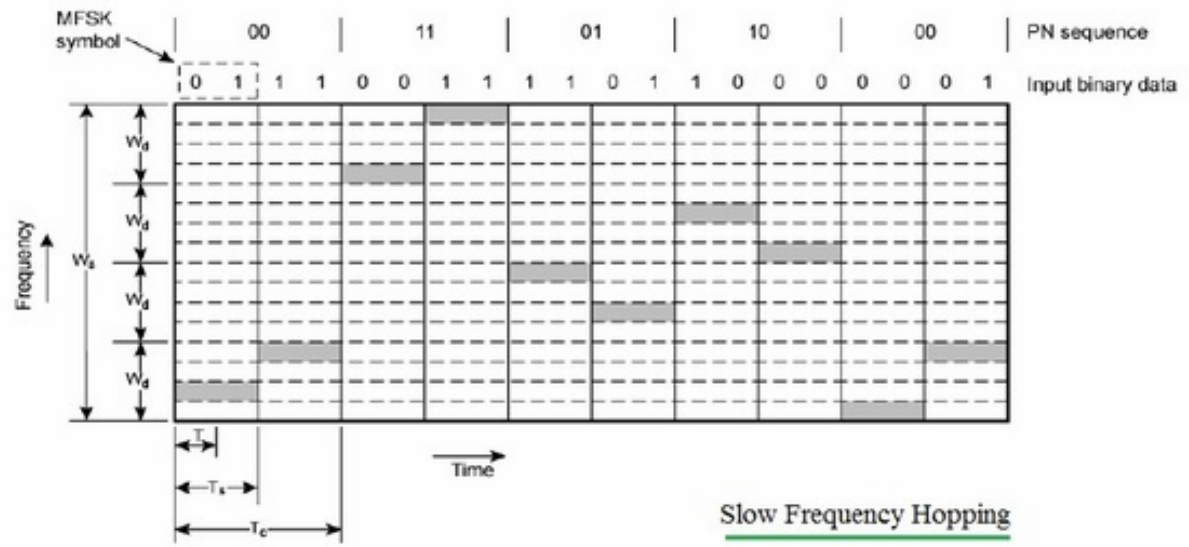
$$P_r \approx \left[\frac{\lambda\sqrt{G_l}}{4\pi d}\right]^2 \left[\frac{4\pi h_t h_r}{\lambda d}\right]^2 P_t = \left[\frac{\sqrt{G_l} h_t h_r}{d^2}\right]^2 P_t, \tag{2.17}$$

or, in dB, we have

$$P_r \text{ dBm} = P_t \text{ dBm} + 10\log_{10}(G_l) + 20\log_{10}(h_t h_r) - 40\log_{10}(d). \tag{2.18}$$

Spread Spectrum

Slow FHSS



MFSK example with M = 4

During T_s, 2 bit signal elements are transmitted

Each pair of columns corresponds to the selection of a **frequency band** based on a **2-bit PN sequence**.

Thus, for the first pair of columns, governed by PN sequence 00, the **lowest band** of frequencies is used.

For the second pair of columns, governed by PN sequence 11, the **highest band** of frequencies is used.

Here we have *M = 4, which means that four different frequencies are used to* encode the data input 2 bits at a time.

Each **signal element** is a **discrete frequency tone** , and the total MFSK bandwidth is $W_d = M f_d$.

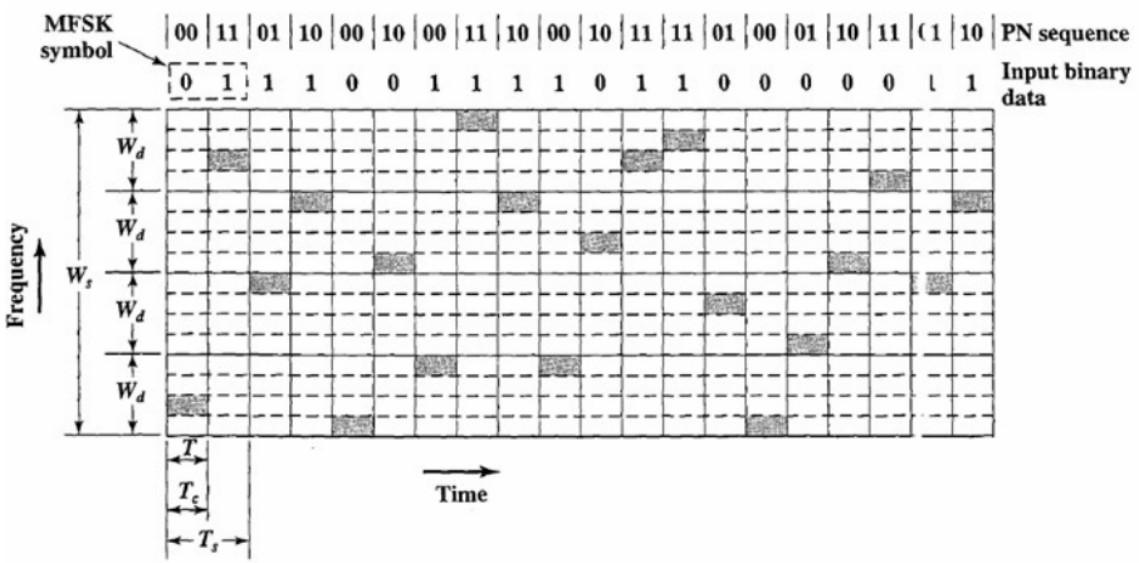
We use an FHSS scheme with $k = 2$. *That is, there are* $4 = 2^k$ ***different channels, each of width*** W_d .

The total **FHSS bandwidth** is $W_s = 2^k W_d$.

Each 2 bits of the PN sequence is used to select ***one*** **of the four channels (bands).**

That **band is held for a duration of two signal elements** , or **four bits** $(T_c = 2 T_s = 4T)$.

Fast FHSS

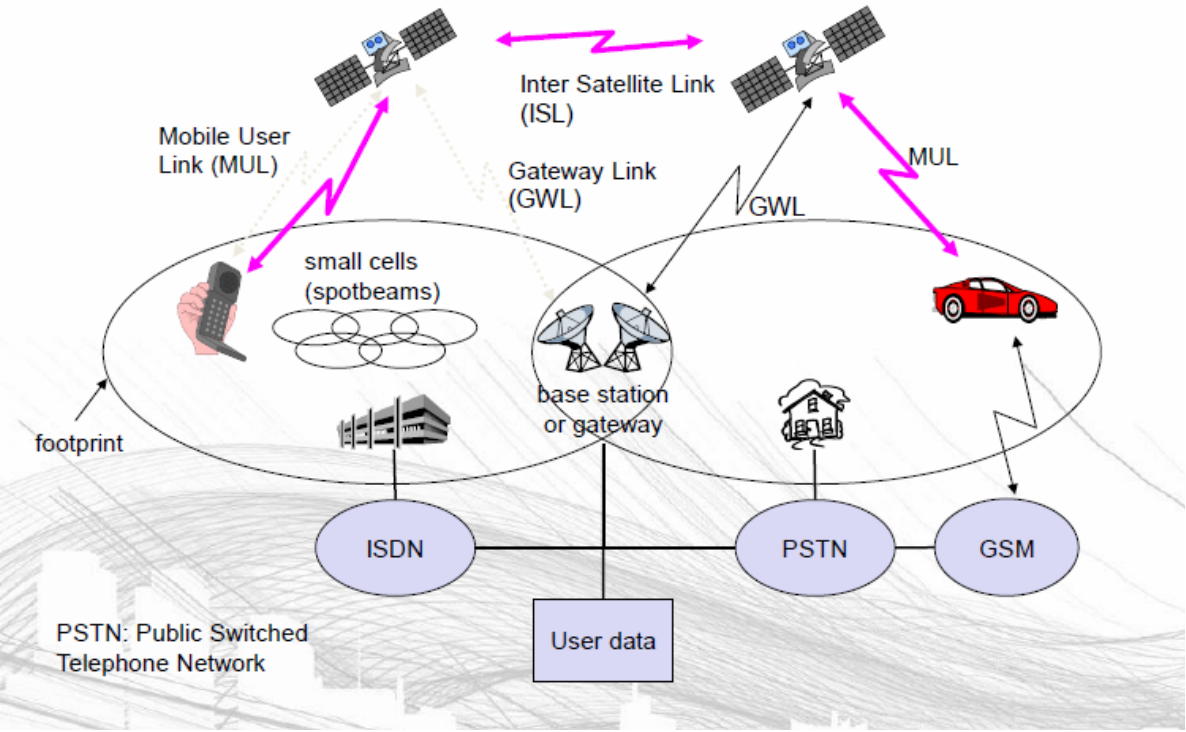


Again, $M = 4$ *and* $k = 2$.

In this case, however, each signal element is represented by two frequency bands tones .

Again, $W_d = M f_d$ *and* $W_s = 2^k W_d$. *In this example* ($T_s = 2 T_c = 2T$).

In general, fast FHSS provides improved performance compared to slow FHSS in the face of noise or jamming.



Satellite Network

- ✓ Satellites in circular orbits
  - –attractive force $F_g = m\, g\, (R/r)^2$
  - –centrifugal force $F_c = m\, r\, \omega^2$
  - –m: mass of the satellite
  - –R: radius of the earth (R = 6370 km)
  - –r: distance to the center of the earth
  - –g: acceleration of gravity (g = 9.81 m/s²)
  - – ω: angular velocity = 2 π f, f: rotation frequency)

- Stable orbit
  - $F_g = F_c$

$$r = \sqrt[3]{\frac{gR^2}{(2\pi f)^2}}$$

- ✓ Earth Stations – antenna systems on or near earth

- Uplink – transmission from an earth station to a satellite
- Downlink – transmission from a satellite to an earth station
- Transponder – electronics in the satellite that convert uplink signals to downlink signals.

✓ Coverage area
- Global, regional, national

✓ Service type
- Fixed service satellite (FSS)
- Broadcast service satellite (BSS)
- Mobile service satellite (MSS)

✓ General usage
- Commercial, military, amateur, experimental

✓ Circular or elliptical orbit
- Circular with center at earth's center
- Elliptical with one foci at earth's center

✓ Orbit around earth in different planes
- Equatorial orbit above earth's equator
- Polar orbit passes over both poles
- Other orbits referred to as inclined orbits

✓ Altitude of satellites
- Geostationary orbit (GEO)
- Medium earth orbit (MEO)
- Low earth orbit (LEO)

✓ LEO
- Circular/slightly elliptical orbit under 2000 km
- Orbit period ranges from 1.5 to 2 hours
- Diameter of coverage is about 8000 km
- Round-trip signal propagation delay less than 20 ms
- Maximum satellite visible time up to 20 min
- System must cope with large Doppler shifts
- Atmospheric drag results in orbital deterioration

✓ MEO
- Circular orbit at an altitude in the range of 5000 to 12,000 km
- Orbit period of 6 hours
- Diameter of coverage is 10,000 to 15,000 km
- Round trip signal propagation delay less than 50 ms
- Maximum satellite visible time is a few hours

✓ GEO
- A geostationary orbit can be achieved only at an altitude very close to 35,863 kilometres (22,236 miles) and directly above the equator.
- This equates to an orbital speed of 3.07 kilometres per second (1.91 miles per second) and an orbital period of 1,436 minutes, one sidereal day.

Capacity Allocation

Approach	SDMA	TDMA	FDMA	CDMA

Idea	Segment spaced into cells or sectors.	Segments 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 or one sector.	All terminals are active for short periods of time on 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 time domain	Filtering in the frequency domain.	Code plus special receivers.
Transmission scheme	Continuous	Discontinuous	Continuous	Continuous
Cell capacity	Depends on cell area	Limited	Limited	No absolute limit on channel capacity but it is an interference limited system
Advantages	Very simple, increases capacity per	Established fully digital, flexible	Simple, established, robust	Flexible, less frequency planning needed, soft handover
Disadvantages	Inflexible, antennas typically fixed	Guard space needed (multipath propagation), synchronization difficult	Inflexible, frequencies are scarce resource	Complex receivers, needs more complicated power control for senders
Comment	Only in combination with TDMA, FDMA or CDMA useful	Standards in fixed networks, together with FDMA or SDMA used in many mobile networks	Typically combined with TDMA and SDMA	Still faces some problems, higher complexity, lowered expectations, will be integrated with TDMA or FDMA

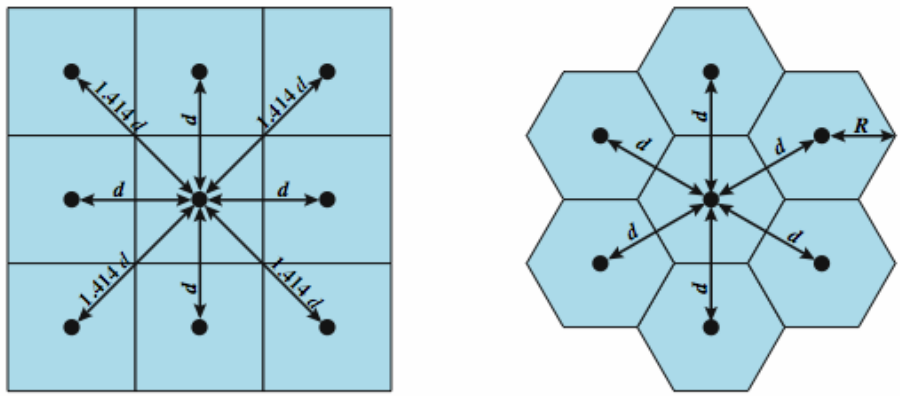
Unit – 2

UNIT II MOBILE NETWORKS **9**

Cellular Wireless Networks – GSM – Architecture – Protocols – Connection Establishment – Frequency Allocation – Handover – Security – GPRA.

Cellular Wireless Networks

Of all the tremendous advances in data communications and telecommunications, perhaps the most revolutionary is the development of cellular networks. Cellular technology is the underlying technology for mobile telephones, personal communications systems, wireless Internet and wireless Web applications, and much more. It is a technique developed to **increase the capacity** available for mobile radio telephone service. Contrast with the older mobiles using large area, high-power transmitters. The essence of a cellular network is the use of multiple low-power transmitters. The area to be covered is divided into cells in a hexagonal tile pattern that provide full coverage of the area. Because the range of such a transmitter is small, an area can be divided into cells, each one served by its own antenna. Each cell is allocated a band of frequencies and is served by a **base station**, consisting of transmitter, receiver, and control unit. Adjacent cells are assigned different frequencies to avoid interference or crosstalk. However, cells sufficiently distant from each other can use the same frequency band.



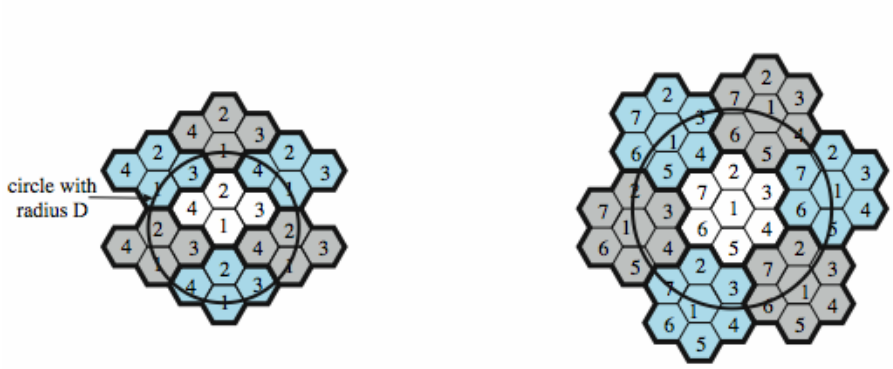
(a) Square pattern (b) Hexagonal pattern

The first design decision to make is the shape of cells to cover an area. A matrix of square cells would be the simplest layout to define. However, this geometry is not ideal. If the width of a square cell is *d*, then a cell has four neighbors at a distance *d* and four neighbors at a distance *d*. As a mobile user within a cell moves toward the cell's boundaries, it is best if all of the adjacent antennas are equidistant. This simplifies the task of determining when to switch the user to an adjacent antenna and which antenna to choose.

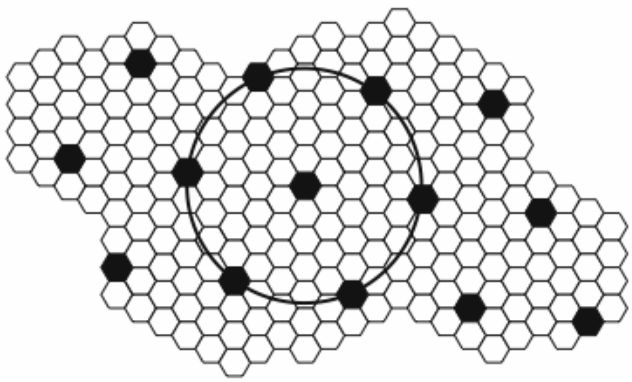
A hexagonal pattern provides for equidistant antennas. The radius of a hexagon is defined to be the radius of the circle that circumscribes it (equivalently, the distance from the center to each vertex; also equal to the length of a side of a hexagon). For a cell radius *R*, the distance between the cell center and each adjacent cell center is $d = R$. In practice, a precise hexagonal pattern is not used. Variations from the ideal are due to topographical limitations, local signal propagation conditions, and practical limitation on siting antennas.

Frequency Reuse

With a wireless cellular system, you are limited in how often you can use the same frequency for different communications because the signals, not being constrained, can interfere with one another even if geographically separated. Systems supporting a large number of communications simultaneously need mechanisms to conserve spectrum. In a cellular system, each cell has a base transceiver. The transmission power is carefully controlled (to the extent that it is possible in the highly variable mobile communication environment) to allow communication within the cell using a given frequency while limiting the power at that frequency that escapes the cell into adjacent ones. The objective is to use the same frequency in other nearby cells, thus allowing the frequency to be used for multiple simultaneous conversations. Generally, 10 to 50 frequencies are assigned to each cell, depending on the traffic expected.



(a) Frequency reuse pattern for $N = 4$ **(b) Frequency reuse pattern for $N = 7$**



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

With a wireless cellular system, you are limited in how often you can use the same frequency for different communications because the signals, not being constrained, can interfere with one another even if geographically separated. Systems supporting a large number of communications simultaneously need mechanisms to conserve spectrum. In a cellular system, each cell has a base transceiver. The transmission power is carefully controlled (to the extent that it is possible in the highly variable mobile communication environment) to allow communication within the cell using a given frequency while limiting the power at that frequency that escapes the cell into adjacent ones. The objective is to use the same frequency in other nearby cells, thus allowing the frequency to be used for multiple simultaneous conversations. Generally, 10 to 50 frequencies are assigned to each cell, depending on the traffic expected.

The essential issue is to determine how many cells must intervene between two cells using the same frequency so that the two cells do not interfere with each other. Various patterns of frequency reuse are possible. If the pattern consists of N cells and each cell is assigned the same number of frequencies, each cell can have K/N frequencies, where K is the total number of frequencies allotted to the system. For AMPS $K = 395$, and $N = 7$ is the smallest pattern that can provide sufficient isolation between two uses of the same frequency. This implies that there can be at most 57 frequencies per cell on average.
In a hexagonal cell pattern, only the following values of N are possible:

$N = I^2 + J^2 + (I \times J)$, 1,1 = 0, 1,2,3, ...
Hence, possible values of N are 1,3,4,7,9,12,13,16,19,21, and so on. The following relationship holds:

$$\frac{D}{R} = \sqrt{3N}$$

This can also be expressed as $D/d = \sqrt{N}$.

Assume a system of 32 cells with a cell radius of 1.6 km, a total of 32 cells, a total frequency bandwidth that supports 336 traffic channels, and a reuse factor of $N = 7$. If there are 32 total cells, what geographic area is covered, how many channels are there per cell, and what is the total number of concurrent calls that can be handled? Repeat for a cell radius of 0.8 km and 128 cells.

The area of a hexagon of radius R is $1.5R^2\sqrt{3}$. A hexagon of radius 1.6 km has an area of 6.65 km^2, and the total area covered is $6.65 \times 32 = 213$ km^2. For $N = 7$, the number of channels per cell is 336/7 = 48, for a total channel capacity of $48 \times 32 = 1536$ channels.

the area covered is $1.66 \times 128 = 213$ km^2. The number of channels per cell is 336/7 = 48, for a total channel capacity of $48 \times 128 = 6144$ channels.

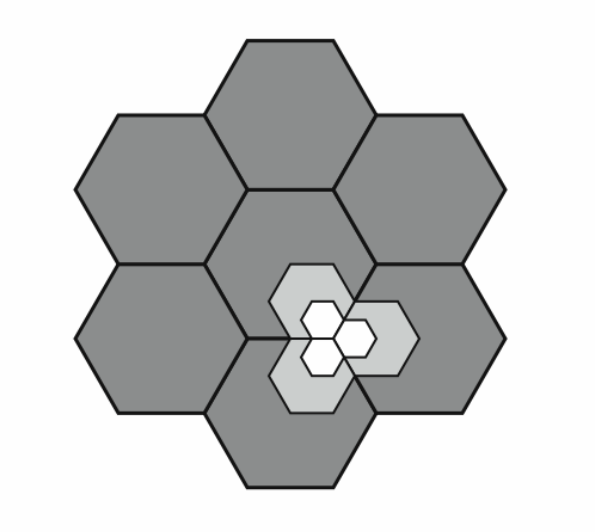
Increasing Capacity

In time, as more customers use the system, traffic may build up so that there are not enough frequencies assigned to a cell to handle its calls. A number of approaches have been used to cope with this situation, including the following:

- **Adding new channels:** Typically, when a system is set up in a region, not all of the channels are used, and growth and expansion can be managed in an orderly fashion by adding new channels.

- **Frequency borrowing:** In the simplest case, frequencies are taken from adjacent cells by congested cells. The frequencies can also be assigned to cells dynamically.

- **Cell splitting:** In practice, the distribution of traffic and topographic features is not uniform, and this presents opportunities for capacity increase. Cells in areas of high usage can be split into smaller cells.



Additional approaches to increase capacity include:

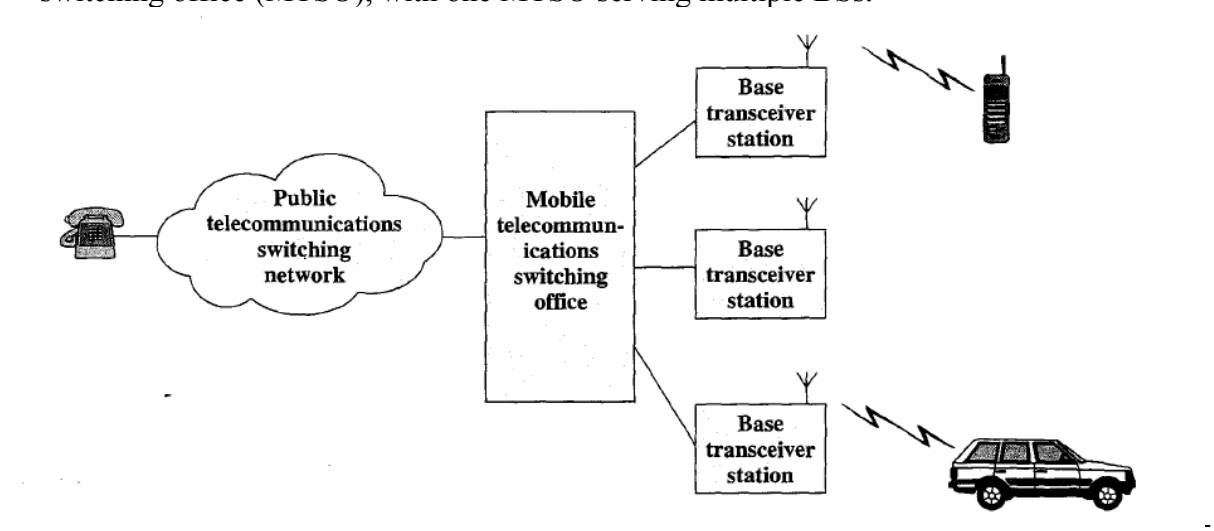
- **Cell sectoring:** With cell sectoring, a cell is divided into a number of wedge-shaped sectors, each with its own set of channels, typically three or six sectors per cell. Each sector is assigned a separate subset of the cell's channels, and directional antennas at the base station are used to focus on each sector.
- **Microcells:** As cells become smaller, antennas move from the tops of tall buildings or hills, to the tops of small buildings or the sides of large buildings, and finally to lamp posts, where they form microcells. Each decrease in cell size is accompanied by a reduction in the radiated power levels from the base stations and the mobile units. Microcells are useful in city streets in congested areas, along highways, and inside large public buildings.
- The use of smaller cells enables the use of lower power and provides superior propagation conditions.

Typical Parameters for Macrocells and Microcells [ANDE95]

	Macrocell	**Microcell**
Cell radius	1 to 20 km	0.1 to 1 km
Transmission power	1 to 10 W	0.1 to 1 W
Average delay spread	0.1 to 10 μs	10 to 100 ns
Maximum bit rate	0.3 Mbps	1 Mbps

Operation of Cellular Systems

Figure shows the principal elements of a cellular system. In the approximate center of each cell is a base station (BS). The BS includes an antenna, a controller, and a number of transceivers, for communicating on the channels assigned to that cell. The controller is used to handle the call process between the mobile unit and the rest of the network. At any time, a number of mobile units may be active and moving about within a cell, communicating with the BS. Each BS is connected to a mobile telecommunications switching office (MTSO), with one MTSO serving multiple BSs.



Typically, the link between an MTSO and a BS is by a wire line, although a wireless link is also possible. The MTSO connects calls between mobile units. The MTSO is also connected to the public telephone or telecommunications network and can make a connection between a fixed subscriber to the public network and a mobile subscriber to the cellular network. The MTSO assigns the voice channel to each call, performs handoffs (discussed subsequently), and monitors the call for billing information.

The use of a cellular system is fully automated and requires no action on the part of the user other than placing or answering a call. Two types of channels are available between the mobile unit and the base station (BS):

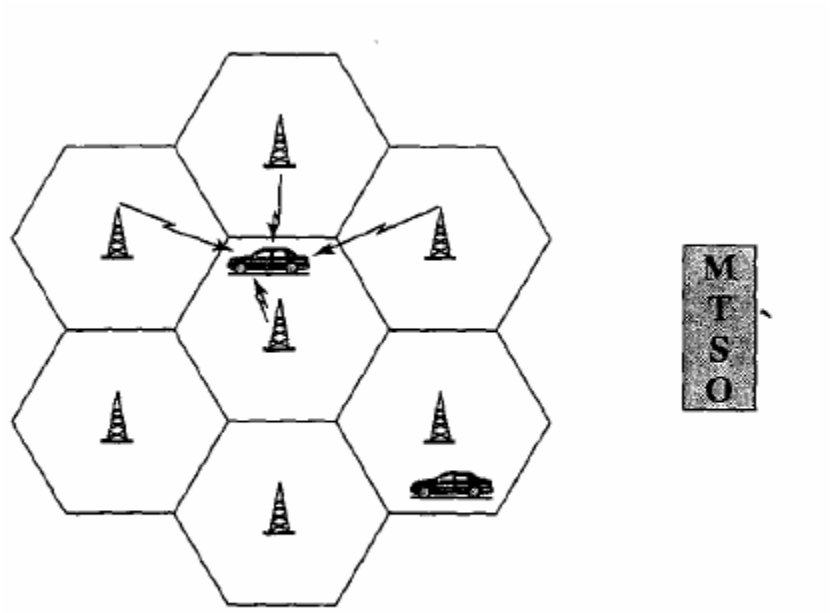
- control channels
- traffic channels.

Control channels are used to exchange information having to do with setting up and maintaining calls and with establishing a relationship between a mobile unit and the nearest BS.
Traffic channels carry a voice or data connection between users.

The steps in a typical call between two mobile users within an area controlled by a single MTSO:

Mobile unit initialization: When the mobile unit is turned on, it scans and selects the strongest setup control channel used for this system. Cells with different frequency bands repetitively broadcast on different setup channels.
The receiver selects the strongest setup channel and monitors that channel. The effect of this procedure is that the mobile unit has automatically selected the BS antenna of the cell within which it will operate.

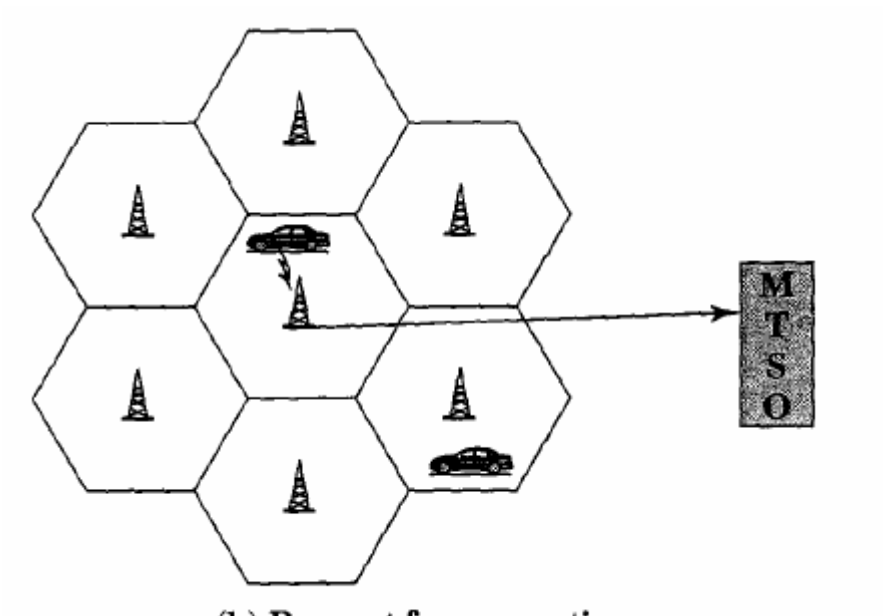
Then a handshake takes place between the mobile unit and the MTSO controlling this cell, through the BS in this cell.
The handshake is used to identify the user and register its location. As long as the mobile unit is on, this scanning procedure is repeated periodically to account for the motion of the unit.



(a) Monitor for strongest signal

Mobile-originated call:

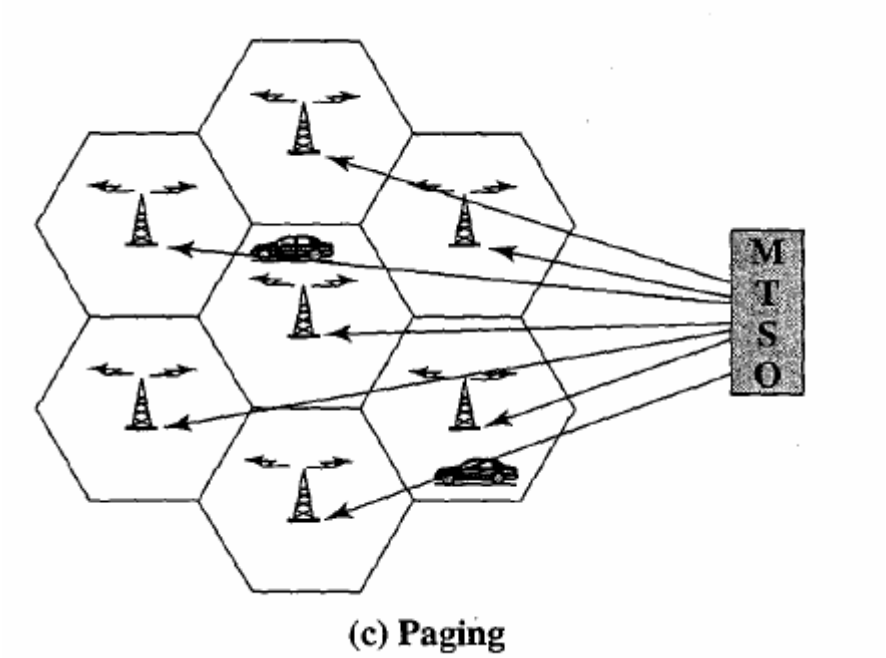
- A mobile unit originates a call by sending the number of the called unit on the preselected setup channel.
- The receiver at the mobile unit first checks that the setup channel is idle by examining information in the forward (from the BS) channel. When an idle is detected, the mobile unit may transmit on the corresponding reverse (to BS) channel.
- The BS sends the request to the MTSO.



(b) Request for connection

Paging:

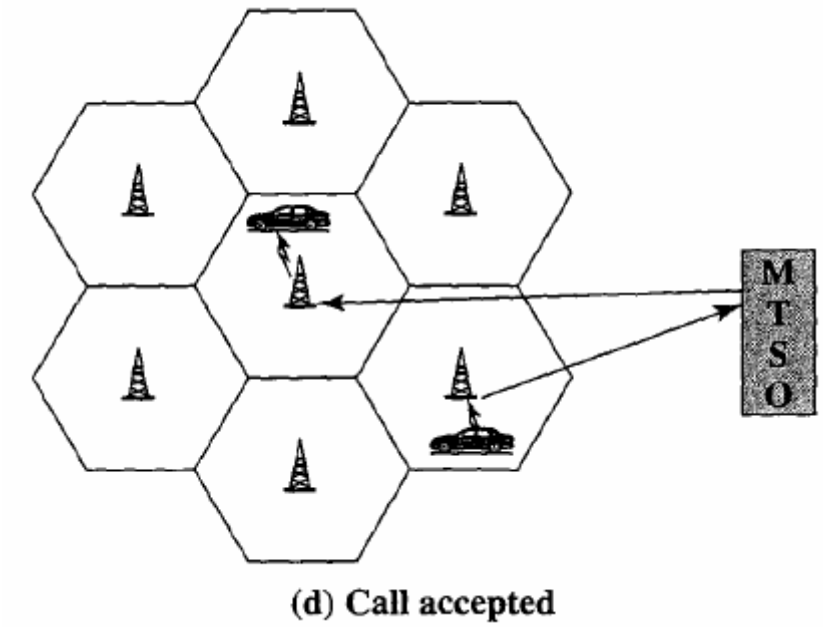
- The MTSO then attempts to complete the connection to the called unit. The MTSO sends a paging message to certain BSs depending on the called mobile unit number.
- Each BS transmits the paging signal on its own assigned setup channel.



(c) Paging

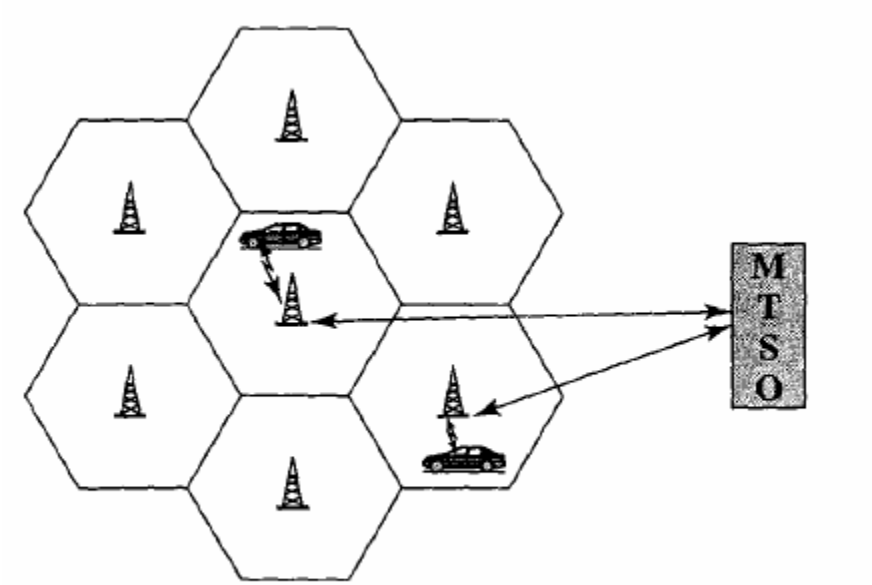
Call accepted:

- The called mobile unit recognizes its number on the setup channel being monitored and responds to that BS, which sends the response to the MTSO.
- The MTSO sets up a circuit between the calling and called BSs. At the same time, the MTSO selects an available traffic channel within each BS's cell and notifies each BS, which in turn notifies its mobile unit.
- The two mobile units tune to their respective assigned channels.



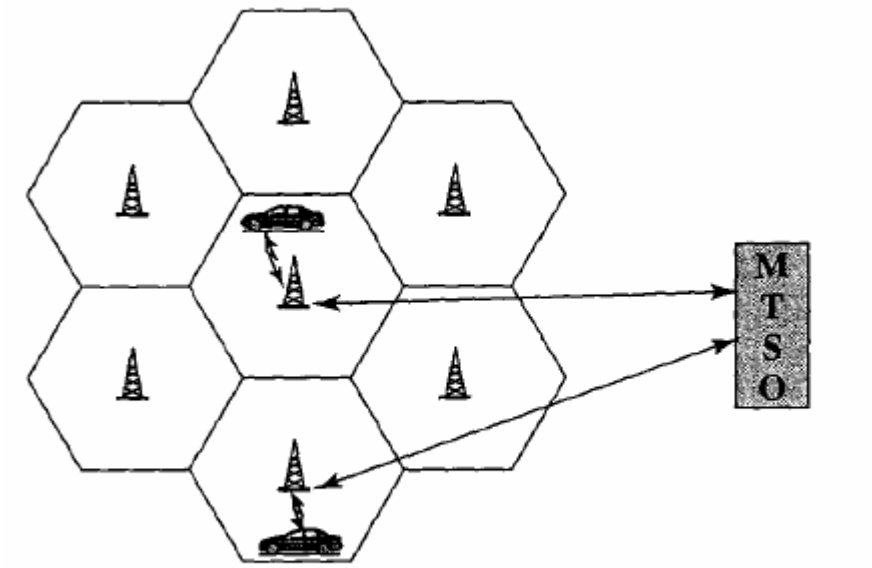
(d) Call accepted

Ongoing call: While the connection is maintained, the two mobile units exchange voice or data signals, going through their respective BSs and the MTSO.



(e) Ongoing call

Handoff: If a mobile unit moves out of range of one cell and into the range of another during a connection, the traffic channel has to change to one assigned to the BS in the new cell.The system makes this change without either interrupting the call or alerting the user.



(f) Handoff

GSM

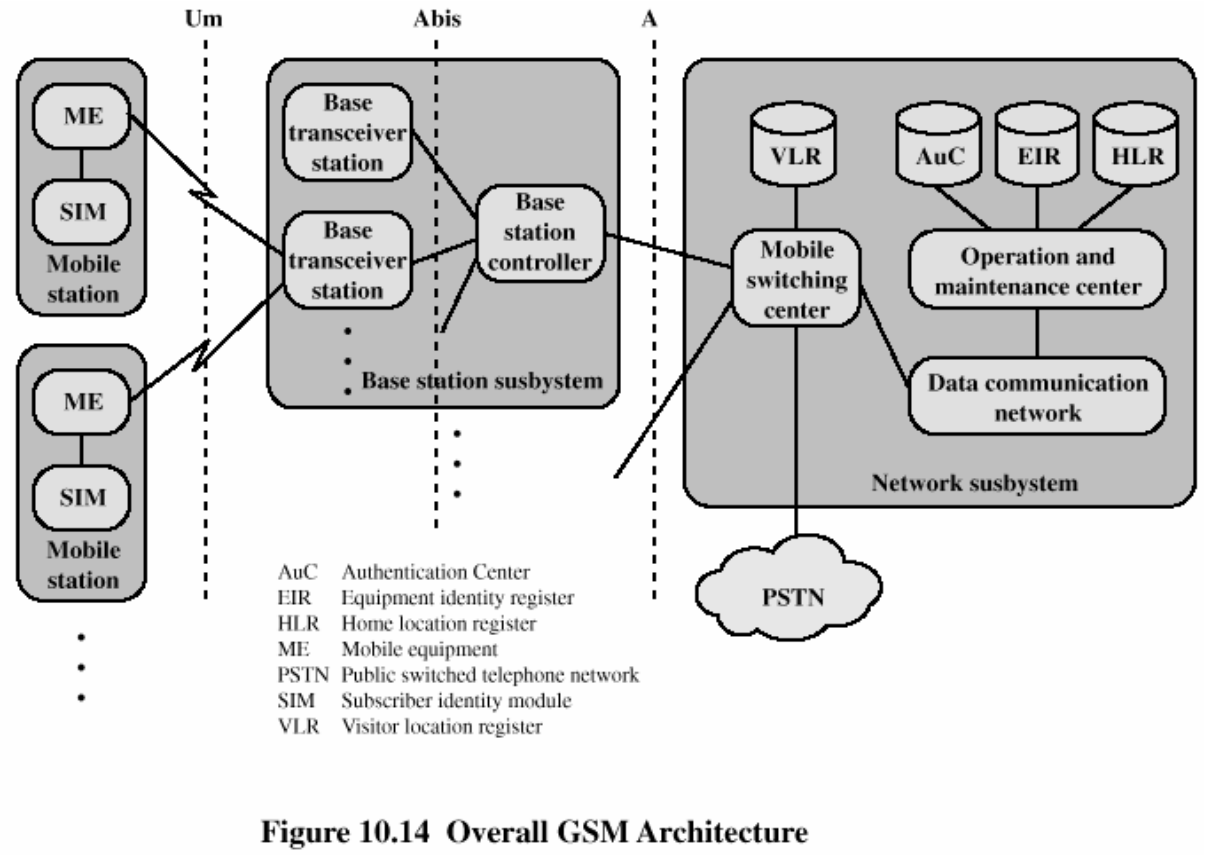


Figure 10.14 Overall GSM Architecture

Construction and working

- ✓ Mobile station communicates across Um interface (air interface) with base station transceiver in same cell as mobile unit
- ✓ Mobile equipment (ME) – physical terminal, such as a telephone or PCS
    - ME includes radio transceiver, digital signal processors and subscriber identity module (SIM)
- ✓ GSM subscriber units are generic until SIM is inserted
    - SIMs roam, not necessarily the subscriber devices
- ✓ Base Station Subsystem (BSS) consists of base station controller and one or more base transceiver stations (BTS)
- ✓ Each BTS defines a single cell
    - Includes radio antenna, radio transceiver and a link to a base station controller (BSC)
- ✓ BSC reserves radio frequencies, manages handoff of mobile unit from one cell to another within BSS, and controls paging
- ✓ NS provides link between cellular network and public switched telecommunications networks
    - Controls handoffs between cells in different BSSs
    - Authenticates users and validates accounts
    - Enables worldwide roaming of mobile users
- ✓ Central element of NS is the mobile switching centre (MSC)
- ✓ Inside MSC we have,
- ✓ Home location register (HLR) database – stores information about each subscriber that belongs to it

- ✓ Visitor location register (VLR) database – maintains information about subscribers currently physically in the region.
- ✓ Authentication center database (AuC) – used for authentication activities, holds encryption keys.
- ✓ Equipment identity register database (EIR) – keeps track of the type of equipment that exists at the mobile station.

GSM Connection establishment

The number dialled to reach a mobile subscriber (MSISDN) contains no information at all about the current location of the subscriber. In order to establish a complete connection to a mobile subscriber, however, one must determine the current location and the locally responsible switch (MSC). In order to be able to route the call to this switch, the routing address to this subscriber (MSRN) has to be obtained. This routing address is assigned temporarily to a subscriber by its currently associated VLR. At the arrival of a call at the GMSC, the HLR is the only entity in the GSM network which can supply this information, and therefore it must be interrogated for each connection setup to a mobile subscriber. An ISDN switch recognizes from the MSISDN that the called subscriber is a mobile subscriber, and therefore can forward the call to the GMSC of the subscriber's home PLMN based on the CC and NDC in the MSISDN. This GMSC can now request the current routing address (MSRN) for the mobile subscriber from the HLR using the MAP . By way of the MSRN the call is forwarded to the local MSC, which determines the TMSI of the subscriber and initiates the paging procedure in the relevant location area . After the MS has responded to the paging call, the connection can be switched through several variants for determining the route and interrogating the HLR exist, depending on how the MSRN was assigned and stored, whether the call is national or international and depending on the capabilities of the associated switching centers.

MOBILE STATION INTERNATIONAL ISDN NUMBER (MSISDN):

The only important number from the user of GSM is phone number. Remember that the phone number is not associated with certain device but with the SIM, which is personalized for user. The number consist of country code(CC) as eg.+49 179 1234567 with 49 for germany. National Destination Code (NDC) is used to locate the network provider and Subscriber number.

INTERNATIONAL MOBILE SUBSCRIBER IDENTITY(IMSI):

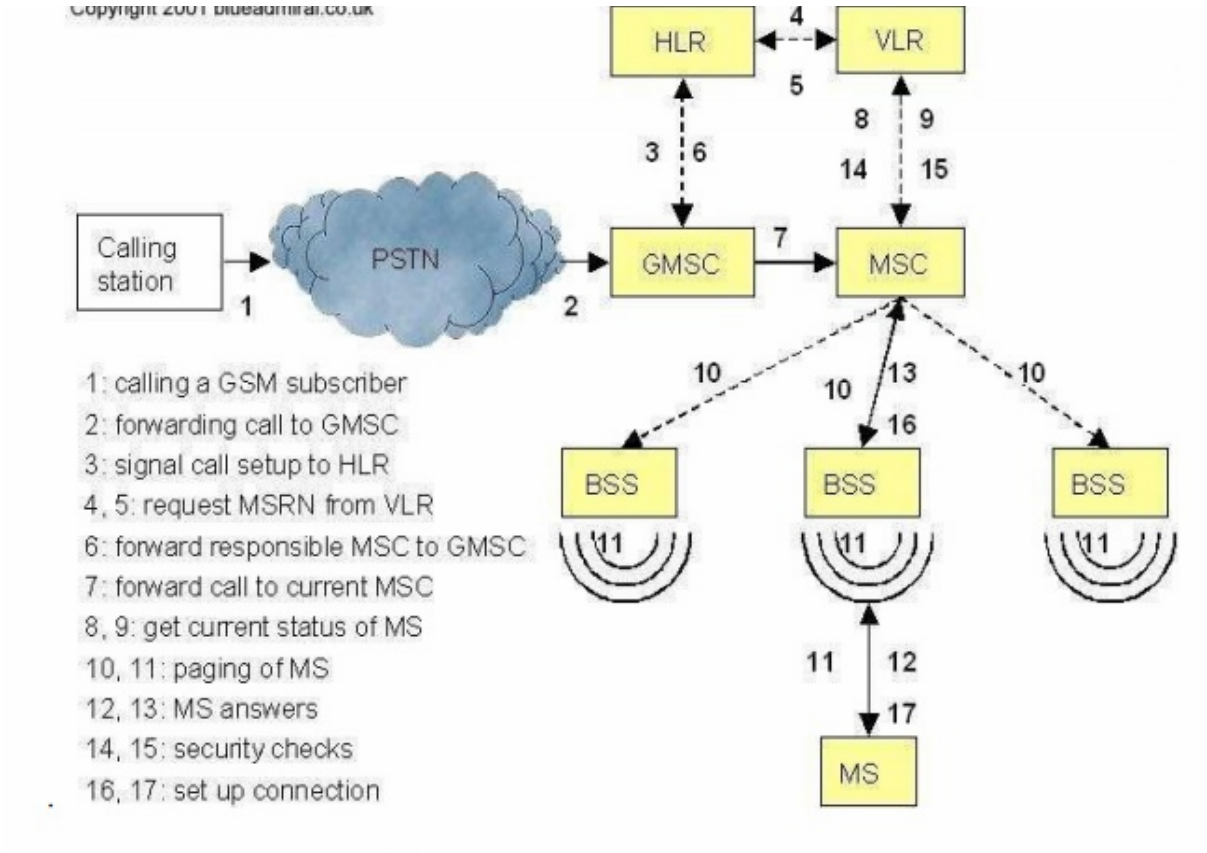
GSM uses the IMSI for internal unique identification of a subscriber. IMSI consist of a mobile country code (MCC) and mobile network code(MNC) and finally the mobile subscriber identification number(MSIN).

TEMPORARY MOBILE SUBSCRIBE IDENTITY(TMSI):

To hide the IMSI, which would give away the exact identity of user signalling over the air interface, GSM uses the 4 byte.TMSI is selected by current VLR and is only valid temporarily and within location area of VLR.

MOBILE STATION ROAMING NUMBER (MSRN):

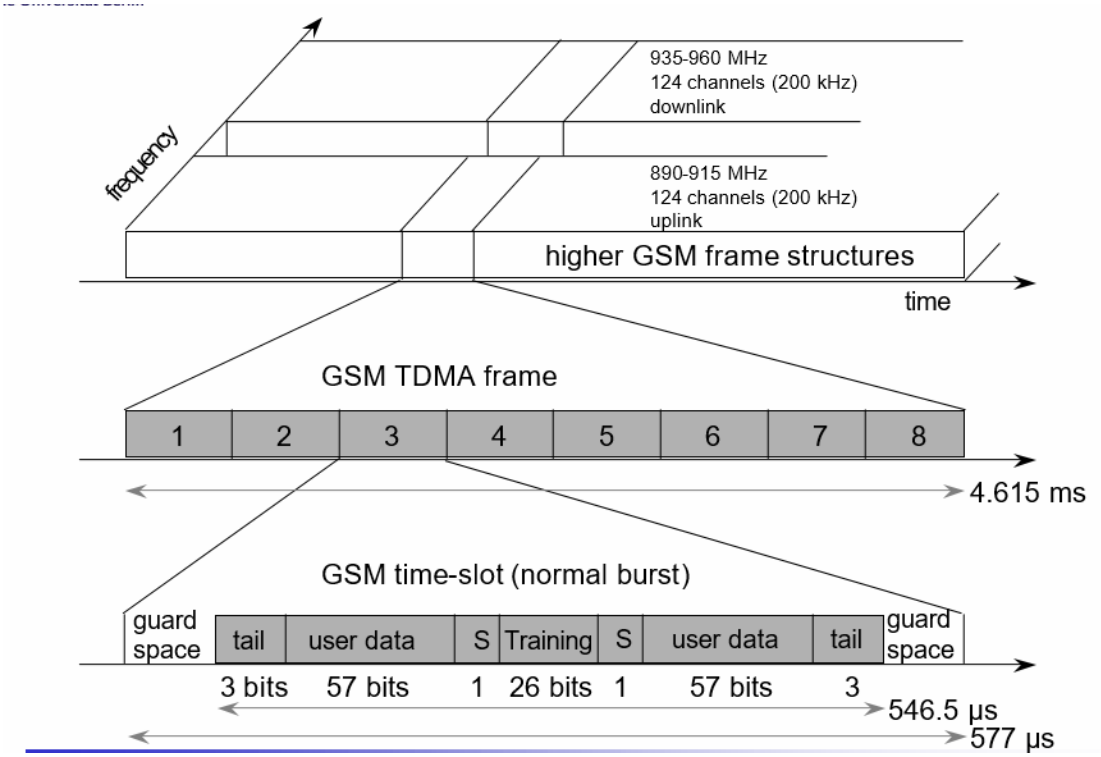
Another temporary address which hides the identity and location of a subscriber is MSRN. The VLR generates this address on request from MSC, and the address is stored in the HLR . MSRN contains current visitory and visitor national destination code(VNDC).



GSM frequency allocation

Type	Channels	Uplink [MHz]	Downlink [MHz]
GSM 850 (Americas)	128-251	824-849	869-894
GSM 900 classical extended	0-124, 955-1023 124 channels +49 channels	876-915 890-915 880-915	921-960 935-960 925-960
GSM 1800	512-885	1710-1785	1805-1880
GSM 1900 (Americas)	512-810	1850-1910	1930-1990
GSM-R exclusive	955-1024, 0-124 69 channels	876-915 876-880	921-960 921-925

Additionally: GSM 400 (also named GSM 450 or GSM 480 at 450-458/460-468 or 479-486/489-496 MHz - Please note: frequency ranges may vary depending on the country - Channels at the lower/upper edge of a frequency band are typically not used



GSM handover and security

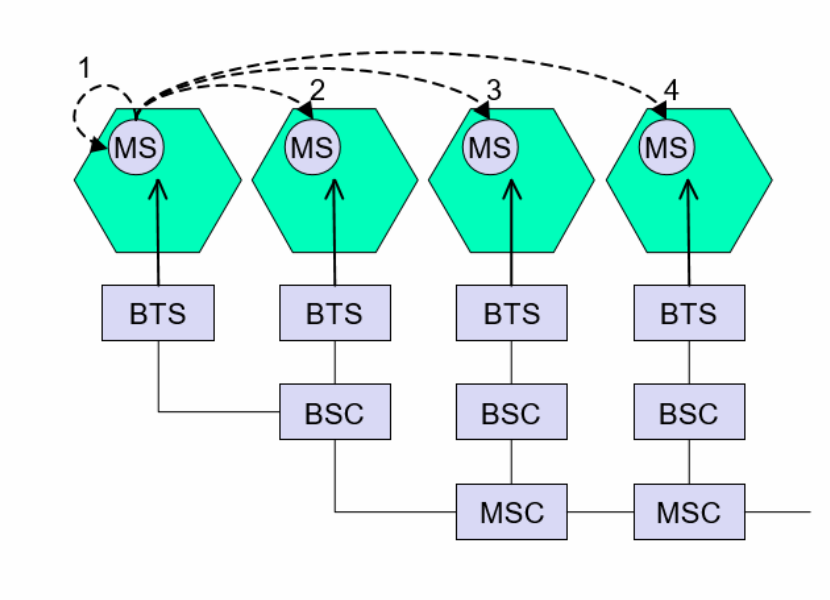
One of the key elements of a mobile phone or cellular telecommunications system, is that the system is split into many small cells to provide good frequency re-use and coverage. However as the mobile moves out of one cell to another it must be possible to retain the connection. The process by which this occurs is known as handover or handoff. The term handover is more widely used within Europe, whereas handoff tends to be use more in North America. Either way, handover and handoff are the same process.

Requirements for GSM handover

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

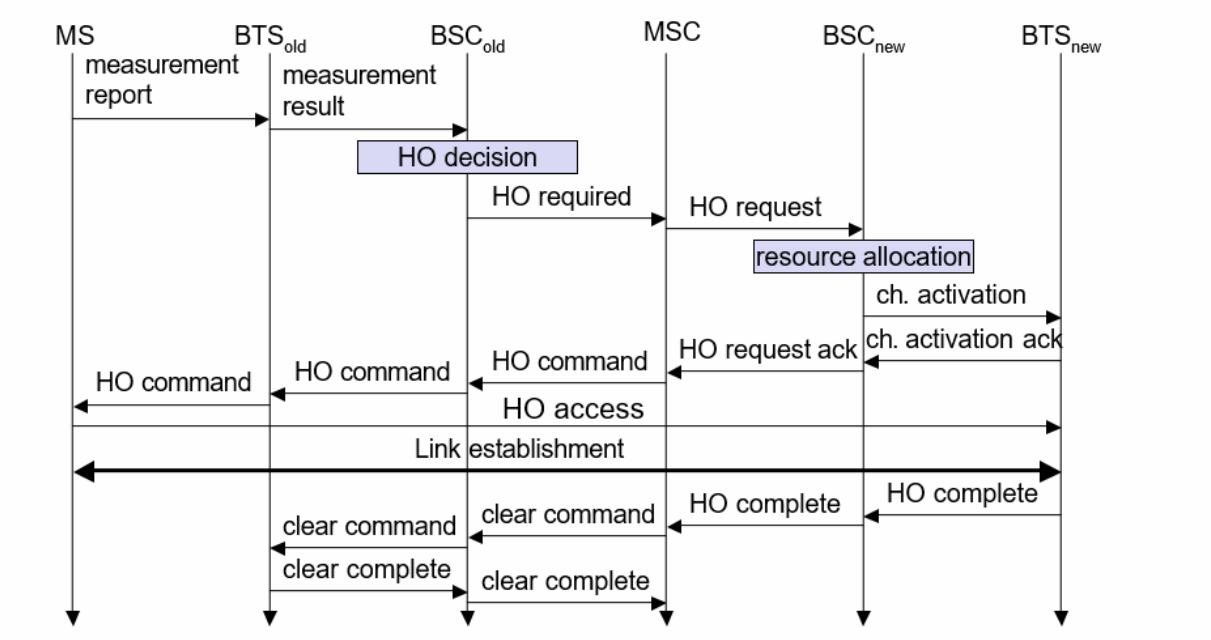
Types of GSM handover

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



- ***Intra-BTS handover:*** This form of GSM handover occurs if it is required to change the frequency or slot being used by a mobile because of interference, or other reasons. In this form of GSM handover, the mobile remains attached to the same base station transceiver, but changes the channel or slot.
- ***Inter-BTS Intra BSC handover:*** This form of GSM handover or GSM handoff occurs when the mobile moves out of the coverage area of one BTS but into another controlled by the same BSC. In this instance the BSC is able to perform the handover and it assigns a new channel and slot to the mobile, before releasing the old BTS from communicating with the mobile.
- ***Inter-BSC handover:*** When the mobile moves out of the range of cells controlled by one BSC, a more involved form of handover has to be performed, handing over not only from one BTS to another but one BSC to another. For this the handover is controlled by the MSC.
- ***Inter-MSC handover:*** This form of handover occurs when changing between networks. The two MSCs involved negotiate to control the handover.

GSM handover process



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

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

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

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

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

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

- ***Old and new BTSs synchronised:*** In this case the mobile is given details of the new physical channel in the neighbouring cell and handed directly over. The mobile may optionally transmit four access bursts. These are shorter than the standard bursts and thereby any effects of poor synchronisation do not cause overlap with other bursts.

However in this instance where synchronisation is already good, these bursts are only used to provide a fine adjustment.

- ***Time offset between synchronised old and new BTS:*** In some instances there may be a time offset between the old and new BTS. In this case, the time offset is provided so that the mobile can make the adjustment. The GSM handover then takes place as a standard synchronised handover.
- ***Non-synchronised handover:*** When a non-synchronised cell handover takes place, the mobile transmits 64 access bursts on the new channel. This enables the base station to determine and adjust the timing for the mobile so that it can suitably access the new BTS. This enables the mobile to re-establish the connection through the new BTS with the correct timing.

Inter-system handover

With the evolution of standards and the migration of GSM to other 2G technologies including to 3G UMTS / WCDMA as well as HSPA and then LTE, there is the need to handover from one technology to another. Often the 2G GSM coverage will be better then the others and GSM is often used as the fallback. When handovers of this nature are required, it is considerably more complicated than a straightforward only GSM handover because they require two technically very different systems to handle the handover.

These handovers may be called intersystem handovers or inter-RAT handovers as the handover occurs between different radio access technologies.

The most common form of intersystem handover is between GSM and UMTS / WCDMA. Here there are two different types:

- ***UMTS / WCDMA to GSM handover:*** There are two further divisions of this category of handover:
  - Blind handover: This form of handover occurs when the base station hands off the mobile by passing it the details of the new cell to the mobile without linking to it and setting the timing, etc of the mobile for the new cell. In this mode, the network selects what it believes to be the optimum GSM based station. The mobile first locates the broadcast channel of the new cell, gains timing synchronisation and then carries out non-synchronised intercell handover.
  - Compressed mode handover: using this form of handover the mobile uses the gaps I transmission that occur to analyse the reception of local GSM base stations using the neighbour list to select suitable candidate base stations. Having selected a suitable base station the handover takes place, again without any time synchronisation having occurred.

Handover from GSM to UMTS / WCDMA: This form of handover is supported within GSM and a "neighbour list" was established to enable this occur easily. As the GSM / 2G network is normally more extensive than the 3G network, this type of handover does not normally occur when the mobile leaves a coverage area and must quickly find a new base station to maintain contact. The handover from GSM to UMTS occurs to provide an improvement in performance and can normally take place only when the conditions are right. The neighbour list will inform the mobile when this may happen.

Security in GSM

Security services

1.access control /authentication

- User -- SIM (Subscriber Identity Module): secret PIN (personal identification number)
- SIM network: challenge response method

2.confidentiality

- voice and signalling encrypted on the wireless link (after successful authentication)

3. anonymity

- temporary identity TMSI (Temporary Mobile Subscriber Identity)
- newly assigned at each new location update (LUP)
- encrypted transmission

Three algorithms specified in GSM

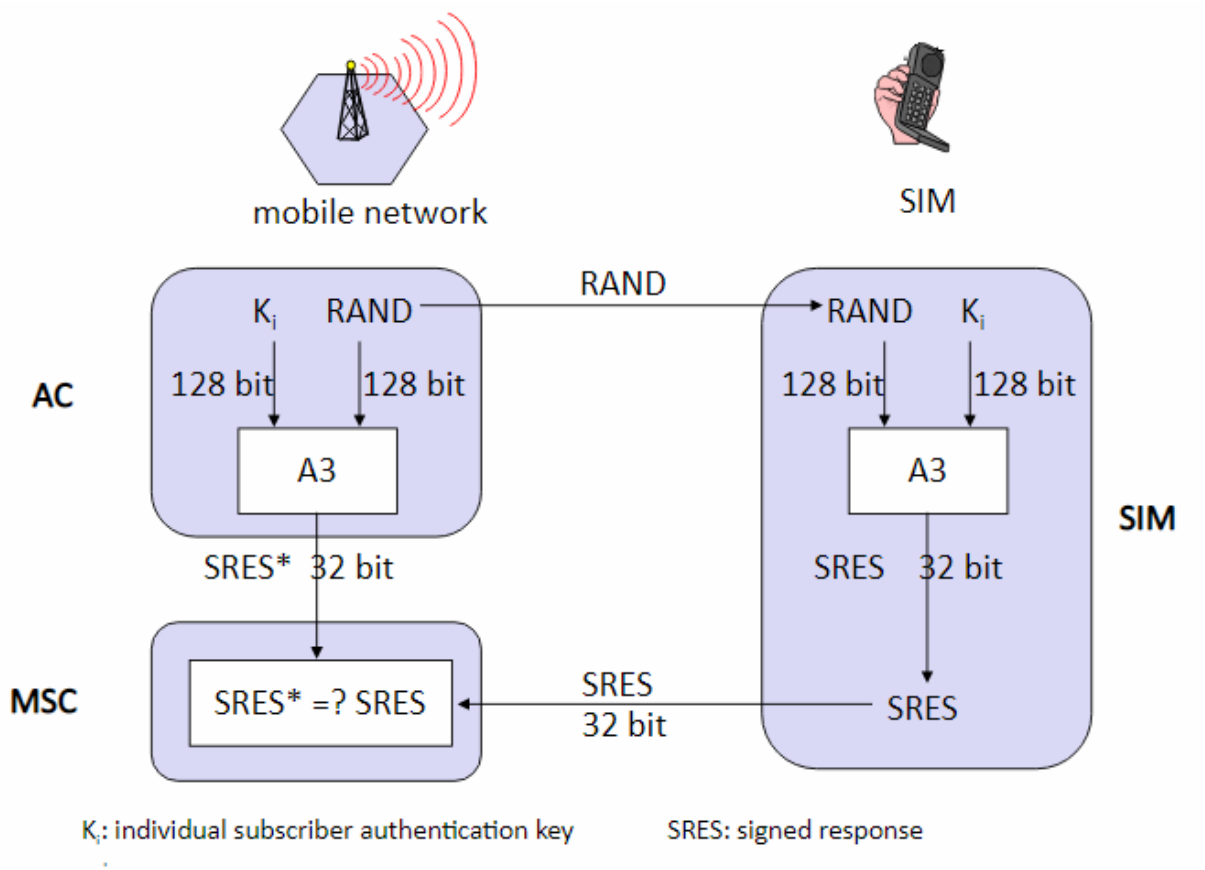
- A3 for authentication (“secret”, open interface)
- A5 for encryption (standardized)
- A8 for key generation (“secret”, open interface)

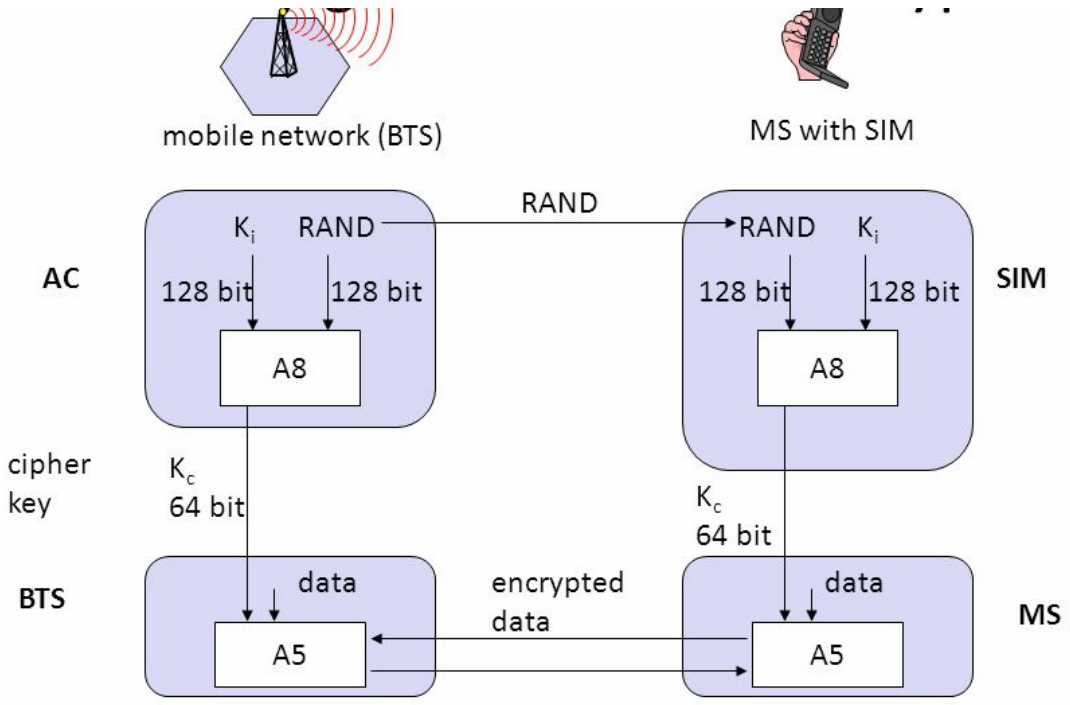
“secret”: • A3 and A8 available via the Internet • network providers can use stronger mechanisms.

Authentication

authentication is based on SIM , which stores individual authentication key Ki, user identification IMSI and algorithm A3.

Challenge response method.


mobile network
SIM
AC
K_i
RAND
RAND
K_i
128 bit
128 bit
128 bit
128 bit
A3
A3
SIM
SRES* 32 bit
SRES 32 bit
MSC
SRES* =? SRES
SRES
32 bit
SRES
K_i: individual subscriber authentication key
SRES: signed response


mobile network (BTS)
MS with SIM
AC
K_i
RAND
RAND
K_i
SIM
128 bit
128 bit
128 bit
128 bit
A8
A8
cipher
key
K_c
64 bit
K_c
64 bit
BTS
data
encrypted
data
data
MS
A5
A5

GPRS network architecture

***General Packet Radio Service** (**GPRS**) is a packet oriented mobile data standard on the 2G and 3G cellular communication network's global system for mobile communications (GSM).

*GPRS was established by European Telecommunications Standards Institute (ETSI) in response to the earlier CDPD and i-mode packet-switched cellular technologies. It is now maintained by the 3rd Generation Partnership Project

GPRS extends the GSM Packet circuit switched data capabilities and makes the following services possible:

- SMS messaging and broadcasting
- "Always on" internet access
- Multimedia messaging service (MMS)
- Push-to-talk over cellular (PoC)
- Instant messaging and presence—wireless village
- Internet applications for smart devices through wireless application protocol (WAP)
- Point-to-point (P2P) service: inter-networking with the Internet (IP)
- Point-to-multipoint (P2M) service: point-to-multipoint multicast and point-to-multipoint group calls

If SMS over GPRS is used, an SMS transmission speed of about 30 SMS messages per minute may be achieved. This is much faster than using the ordinary SMS over GSM, whose SMS transmission speed is about 6 to 10 SMS messages per minute.

The main concepts of GPRS are as follows (ETSI, 1998b). For the new GPRS radio channels, the GSM system can allocate between one and eight time slots within a TDMA frame.

Time slots are not allocated in a fixed, pre-determined manner but on demand. All time slots can be shared by the active users; up- and downlink are allocated separately. Allocation of the slots is based on current load and operator preferences.

Protocols supported

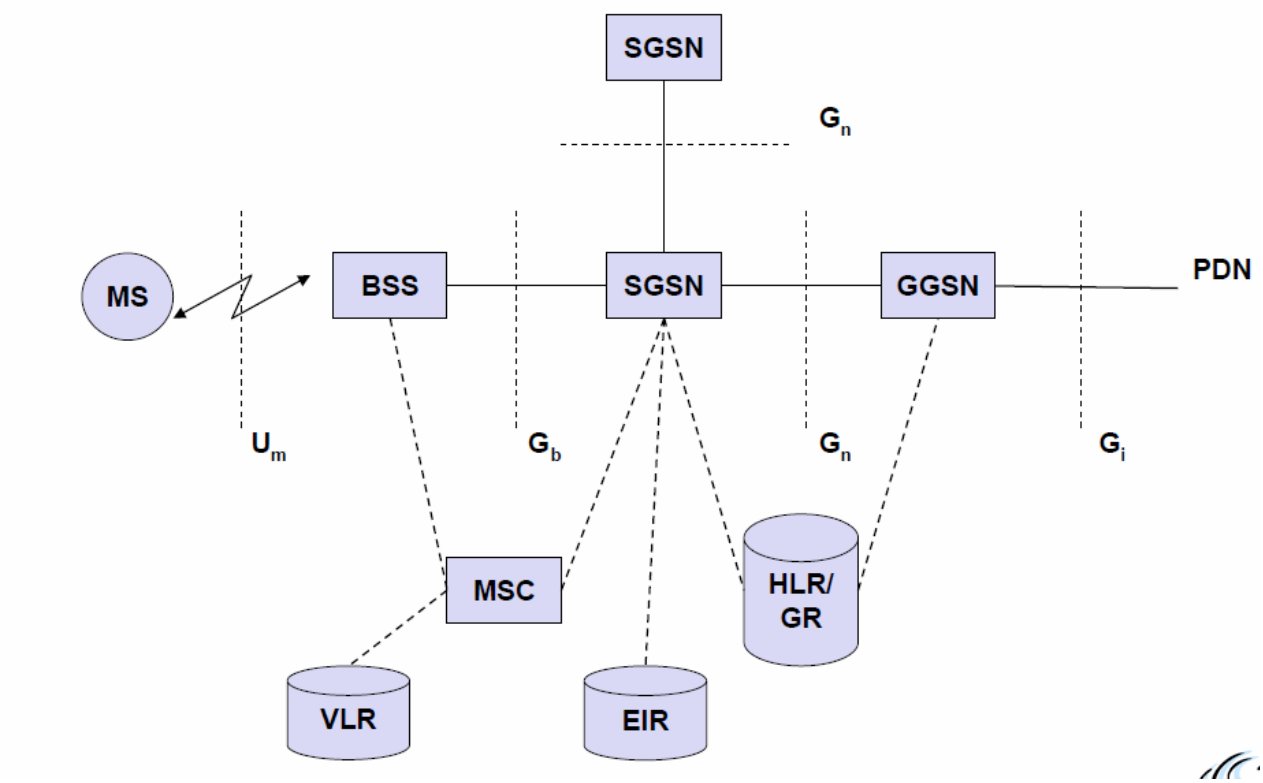
GPRS supports the following protocols:

- **Internet Protocol (IP).** In practice, built-in mobile browsers use IPv4 before IPv6 is widespread.
- **Point-to-Point Protocol (PPP**) is typically not supported by mobile phone operators but if a cellular phone is used as a modem for a connected computer, PPP may be used to tunnel IP to the phone. This allows an IP address to be dynamically assigned (using IPCP rather than DHCP) to the mobile equipment.
  - In phase 1, GPRS offers a point-to-point (PTP) packet transfer service (ETSI,1 98c). One of the PTP versions offered is the PTP connection oriented network service (PTP-CONS), which includes the ability of GPRS to maintain a virtual circuit upon change of the cell within the GSM network.
  - The other PTP version offered is the PTP connectionless network service (PTP-CLNS), which supports applications that are based on the Internet Protocol IP.
- **X.25** connections are typically used for applications like wireless payment terminals, although it has been removed from the standard. X.25 can still be supported over PPP, or even over IP, but this requires either a network-based router to perform encapsulation or software built into the end-device/terminal; e.g., user equipment (UE).

Coding scheme	1 slot	2 slots	3 slots	4 slots	5 slots	6 slots	7 slots	8 slots
CS-1	9.05	18.2	27.15	36.2	45.25	54.3	63.35	72.4
CS-2	13.4	26.8	40.2	53.6	67	80.4	93.8	107.2
CS-3	15.6	31.2	46.8	62.4	78	93.6	109.2	124.8
CS-4	21.4	42.8	64.2	85.6	107	128.4	149.8	171.2

Table shows the typical data rates available with GPRS if it is used together with GSM. In the beginning, only coding schemes CS-1 and CS-2 are available. The system chooses a coding scheme depending on the current error rate (CS-4 provides no error correction capabilities).

Users of GPRS can specify a **QoS-profile**. This determines the **service precedence** (high, normal, low), **reliability class** and **delay class** of the transmission, and **user data throughput**.



Construction and working

- ✓ GPRS (General Packet Radio Service):
  - Packet switching

- Using free slots only if data packets ready to send (e.g., 115 Kbit/s using 8 slots temporarily)
- Standardization 1998, introduction 2001
- Advantage: one step towards UMTS, more flexible
- Drawback: more investment needed (new hardware)

✓ GPRS network elements: –

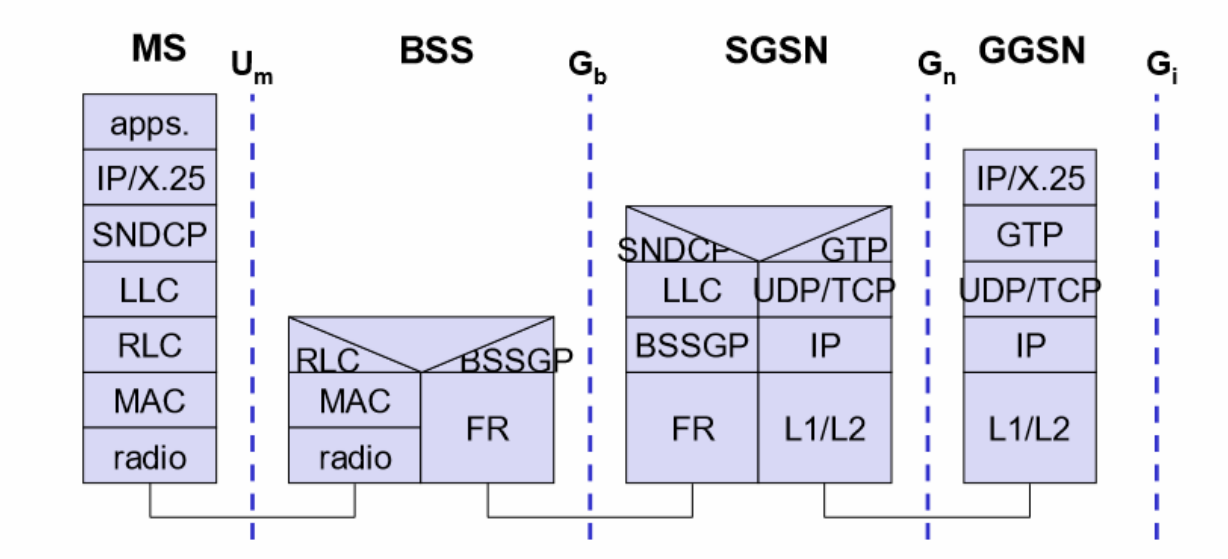
- GSN (GPRS Support Nodes):
  - Act as router
  - GGSN and SGSN
- GGSN (Gateway GSN)
  - Used for address translation
  - Inter-working unit between GPRS and PDN (Packet Data Network) via the Gi interface and transfers packets to the SGSN via an IP-based GPRS backbone network (Gn interface).
- SGSN (Serving GSN)

The SGSN, for example, requests user addresses from the **GPRS register (GR)**, keeps track of the individual MSs' location, is responsible for collecting billing information (e.g., counting bytes), and performs several security functions such as access control.

  - Used for accounting and access control
  - Supports the MS (location, billing, security) which supports the MS via the Gb interface.

- GR (GPRS Register)
  - Stores user addresses
  - The GR, which is typically a part of the HLR, stores all GPRS-relevant data.

GPRS protocol Architecture



Construction and Working

- ✓ GTP (GPRS tunnelling protocol)- All data within the GPRS backbone, i.e., between the GSNs, is transferred using the GTP
  GPRS tunnelling protocol (GTP)
  - Used to differentiate transport protocols
  - TCP or UDP

- ✓ SNDCP (subnetwork dependant convergence protocol) - To adapt to the different characteristics of the underlying networks
  - Used to transfer data between SGSN and MS
- ✓ LLC (logical link layer)
  - Used for high reliable packet data transfer between SGSN and MS.
- ✓ BSSGP (base station subsystem GPRS protocol)
  - Used to convey routing and QoS related information between BSS and SGSN.
  - Does not perform error correction. works on top of a **frame relay (FR)** network.

- ✓ **MAC** controls access with signaling procedures for the radio channel and the mapping of LLC frames onto the GSM physical channels

- ✓ RLC (radio link protocol)
  - To transfer data over U_m interface and provides reliable link.
- ✓ FR (frame relay)
  - The BSS and the SGSN are connected by the G_b interface with Frame Relay.

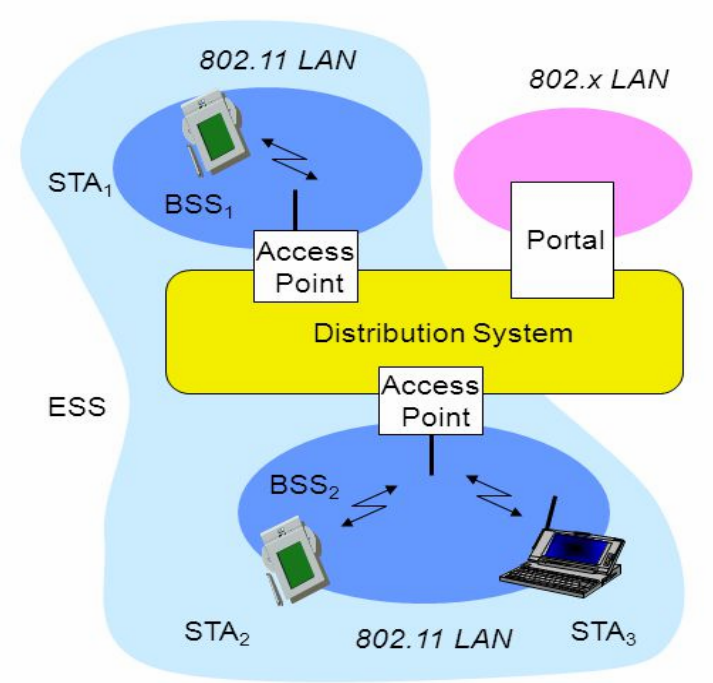
Unit3

UNIT III WIRELESS NETWORKS **9**

Wireless LAN – IEEE 802.11 Standard-Architecture – Services – HiperLAN, Bluetooth

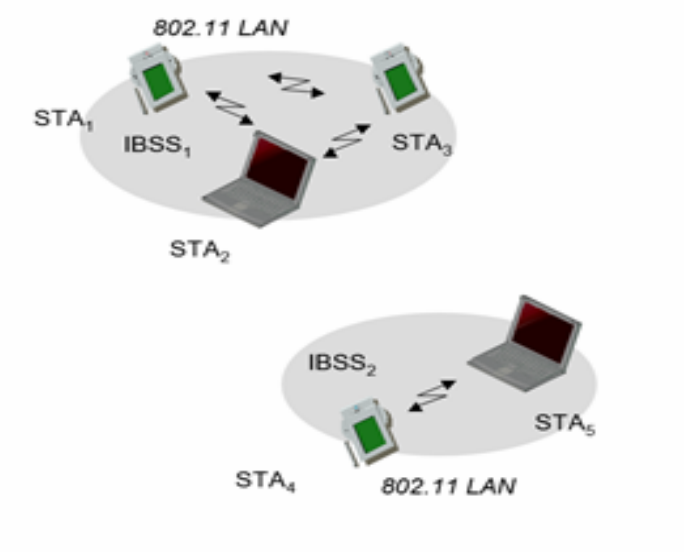
WLAN – Wireless Local Area Network – IEEE 802.11

- ✓ Two types of network architecture
  - Infrastructure based network
  - Adhoc network
- ✓ IEEE 802.11 Infrastructure based network



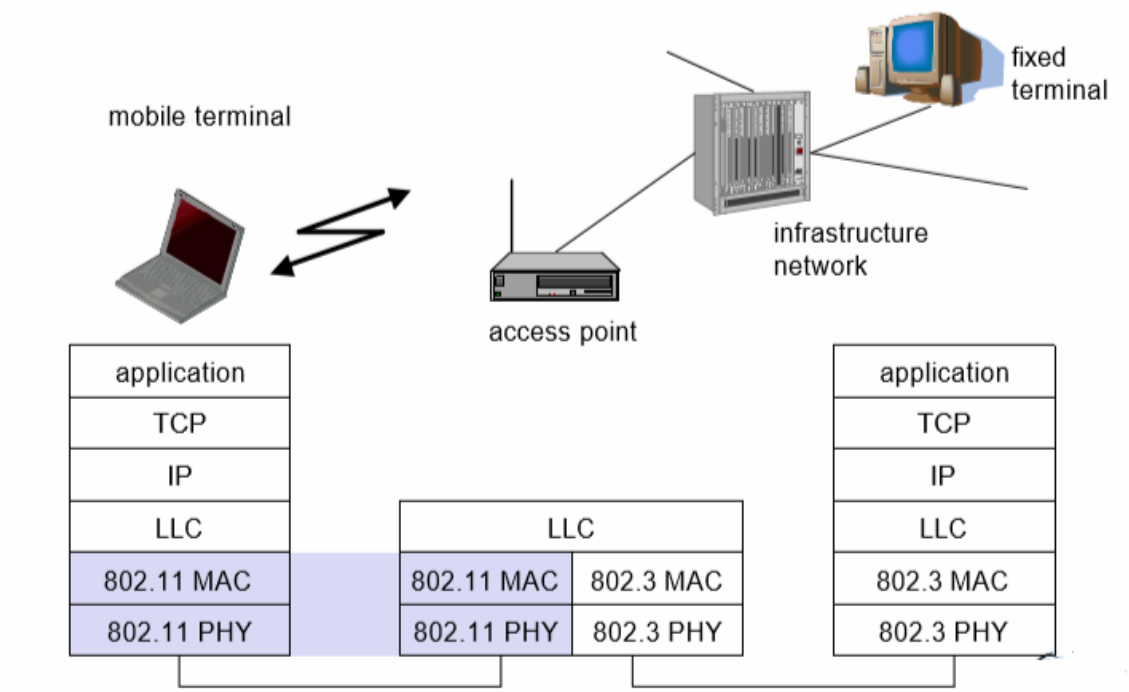
- Station (STA)
  - terminal with access mechanisms to the wireless medium and radio contact to the access point
- Basic Service Set (BSS)
  - group of stations using the same radio frequency
- Access Point
  - station integrated into the wireless LAN and the distribution system
- Portal
  - bridge to other (wired) networks
- Distribution System
  - interconnection network to form one logical network (EES: Extended Service Set) based on several BSS.

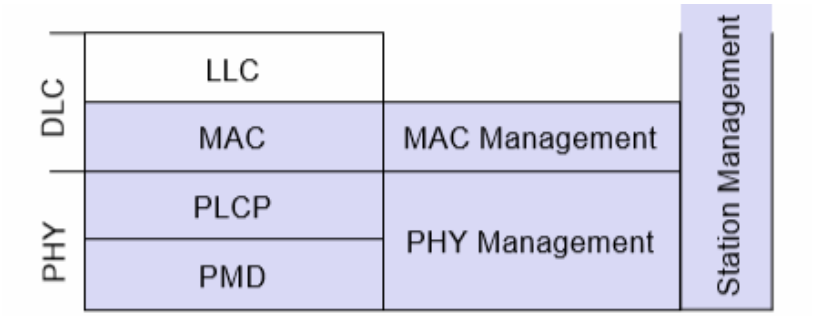
✓ IEEE 802.11 Adhoc network



- Direct communication within a limited range
  - Station (STA): terminal with access mechanisms to the wireless medium.
  - Independent Basic Service Set (IBSS): group of stations using the same radio frequency.

✓ Protocol Architecture

- 

- MAC
  - Access mechanisms, fragmentation, encryption
- MAC Management.
  - synchronization, roaming, MIB, power management.
- 

- PLCP Physical Layer Convergence Protocol
  - clear channel assessment signal (carrier sense)
- PMD Physical Medium Dependent
  - modulation, coding
- PHY Management
  - channel selection, MIB
- Station Management
  - coordination of all management functions

✓ IEEE 802.11 physical layer

- data rates 1 or 2 Mbit/s
- FHSS (Frequency Hopping Spread Spectrum)
  - spreading, despreading, signal strength, typ. 1 Mbit/s
  - min. 2.5 frequency hops/s, two-level GFSK modulation
- DSSS (Direct Sequence Spread Spectrum)
  - DBPSK modulation for 1 Mbit/s (Differential Binary Phase Shift Keying),
  - DQPSK for 2 Mbit/s (Differential Quadrature PSK)

        - preamble and header of a frame is always transmitted with 1 Mbit/s, rest of transmission 1 or 2 Mbit/s
        - chipping sequence: +1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1 (Barker code)
        - max. radiated power 1 W (USA), 100 mW (EU), min. 1mW
    - Infrared
        - 850-950 nm, diffuse light, typ. 10 m range
        - carrier detection, energy detection, synchronization

WLAN Spread Spectrum

Spread spectrum is currently the most widely used transmission technique for wireless LANs. It was initially developed by the military to avoid jamming and eavesdropping of the signals. This is done by spreading the signal over a range of frequencies, that consist of the industrial, scientific, and medical (ISM) bands of the electromagnetic spectrum. The ISM bands include the frequency ranges at 902 MHz to 928 MHZ and at 2.4 GHz to 2.484 GHz, which do not require an FCC license.

Two types

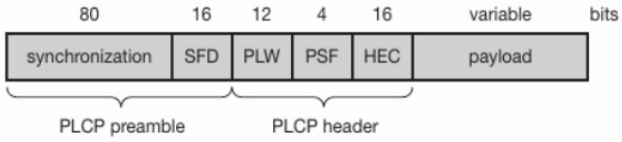
Frequency Hopping Spread Spectrum (FHSS)

Direct Sequence Spread Spectrum (DSSS)

FHSS

- ✓ spreading, despreading, signal strength, typ. 1 Mbit/s
- ✓ 79 hopping channels for North America and Europe
- ✓ 25 hopping channels for Japan.
- ✓ two-level GFSK modulation for 1 Mbits/s (1 bit is mapped into one frequency)
- ✓ a 4 level GFSK used for 2 Mbits/s.
- ✓ Maximum transmit power is 1 W in the US, 100 mW EIRP (equivalent isotropic radiated power) in Europe and 10 mW/MHz in Japan.
- ✓ Frame of the physical layer of WLAN used with FHSS consists of two parts
    - PLCP part (preamble and header)
    - Payload part
- ✓ PLCP transmitted at 1 Mbits/s while payload can use 1 or 2 Mbits/s.
- ✓ MAC data is scrambled using polynomial $s(z) = z^7+z^4+1$ for DC blocking and whitening of spectrum.
- ✓ FHSS frame structure

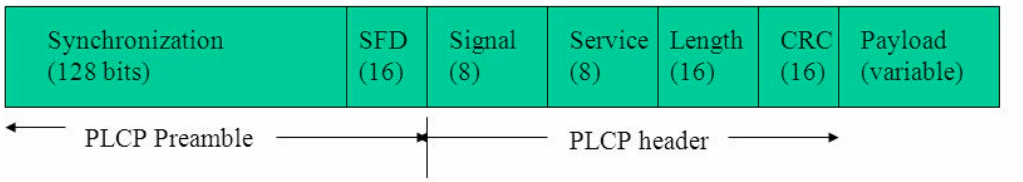
✓



- **Synchronization** – 80 bit SYN (010101….), used to SYN potential receiver.
- **Start frame delimiter (SFD)** – indicate the start of frame.
- **PLCP_PDU length word (PLW)** – length of payload
- **PLCP Signalling field (PSF)** – indicate data rate of payload 0000 – 1Mbits/sec, granularity 500 Kbits/sec.
- **Header error check (HEC)** – 16 bit checksum

DSSS

- ✓ DBPSK modulation for 1 Mbit/s (Differential Binary Phase Shift Keying), DQPSK for 2 Mbit/s (Differential Quadrature PSK)
- ✓ preamble and header of a frame is always transmitted with 1 Mbit/s, rest of transmission 1 or 2 Mbit/s
- ✓ chipping sequence: +1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1 (Barker code)
- ✓ max. radiated power 1 W (USA), 100 mW (EU), min. 1mW.



✓

- ✓ Synchronization – gain setting, energy detection and frequency offset compensation.
- ✓ Start Frame Delimiter (SFD) – synchronization field contains scrambled 1 bits.
- ✓ Signal – 0x0A indicates 1 Mbits/s data rate (DBPSK), 0x14 indicates 2 Mbits/s (DQPSK).
- ✓ Service – reserved for future use.
- ✓ Length – 16 bits for payload length in microsecond.

Header Error Check (HEC) – 16 bit checksum

WLAN Services

Service	Provider	Category
Association	Distribution system	MSDU delivery
Authentication	Station	LAN access and security
Deauthentication	Station	LAN access and security
Disassociations	Distribution system	MSDU delivery
Distribution	Distribution system	MSDU delivery

Integration	Distribution system	MSDU delivery
MSDU delivery	Station	MSDU delivery
Privacy	Station	LAN access and security
Reassocation	Distribution system	MSDU delivery

Categorizing services

1. Station services implemented in every 802.11 station
2. Including AP stations
3. Distribution services provided between BSSs
4. Three services used to control access and confidentiality
5. Six services used to support delivery of MAC service data units (MSDUs) between stations
6. Block of data passed down from MAC user to MAC layer
7. Typically LLC PDU
8. If MSDU too large for MAC frame, fragment and transmit in series of frames.

Association Related Services

1. Purpose of MAC layer transfer MSDUs between MAC entities
2. Fulfilled by distribution service (DS)
3. DS requires information about stations within ESS
    a. Provided by association-related services
    b. Station must be associated before communicating
4. Three transition types of based on mobility
    a. No transition: Stationary or moves within range of single BSS
    b. BSS transition: From one BSS to another within same ESS
        i. Requires addressing capability be able to recognize new location
5. ESS transition: From BSS in one ESS to BSS in another ESS
    a. Only supported in sense that the station can move
    b. Maintenance of upper-layer connections not guaranteed
    c. Disruption of service likely.

Access and Privacy Services

1. On wireless LAN, any station within radio range other devices can transmit
2. Any station within radio range can receive
3. Authentication: Used to establish identity of stations to each other
    a. Wired LANs assume access to physical connection conveys authority to connect to LAN
    b. Not valid assumption for wireless LANs
        i. Connectivity achieved by having properly tuned antenna
    c. Authentication service used to establish station identity
    d. 802.11 supports several authentication schemes
        i. Allows expansion of these schemes
    e. Does not mandate any particular scheme
    f. Range from relatively insecure handshaking to public-key encryption schemes
    g. 802.11 requires mutually acceptable, successful authentication before association.

HiperLAN

HIPERLAN (HIgh PERformance wireless Local Area Network)

- ✓ ETSI (European Telecommunications Standards Institute) standard
  - European standard, cf. GSM, DECT, ...
  - Enhancement of local Networks and interworking with fixed networks
  - integration of time-sensitive services from the early beginning
- ✓ HIPERLAN family
  - one standard cannot satisfy all requirements
    - range, bandwidth, QoS support
    - commercial constraints
  - HIPERLAN 1 standardized since 1996

Fundamentals of WLANs

1. HiperLAN

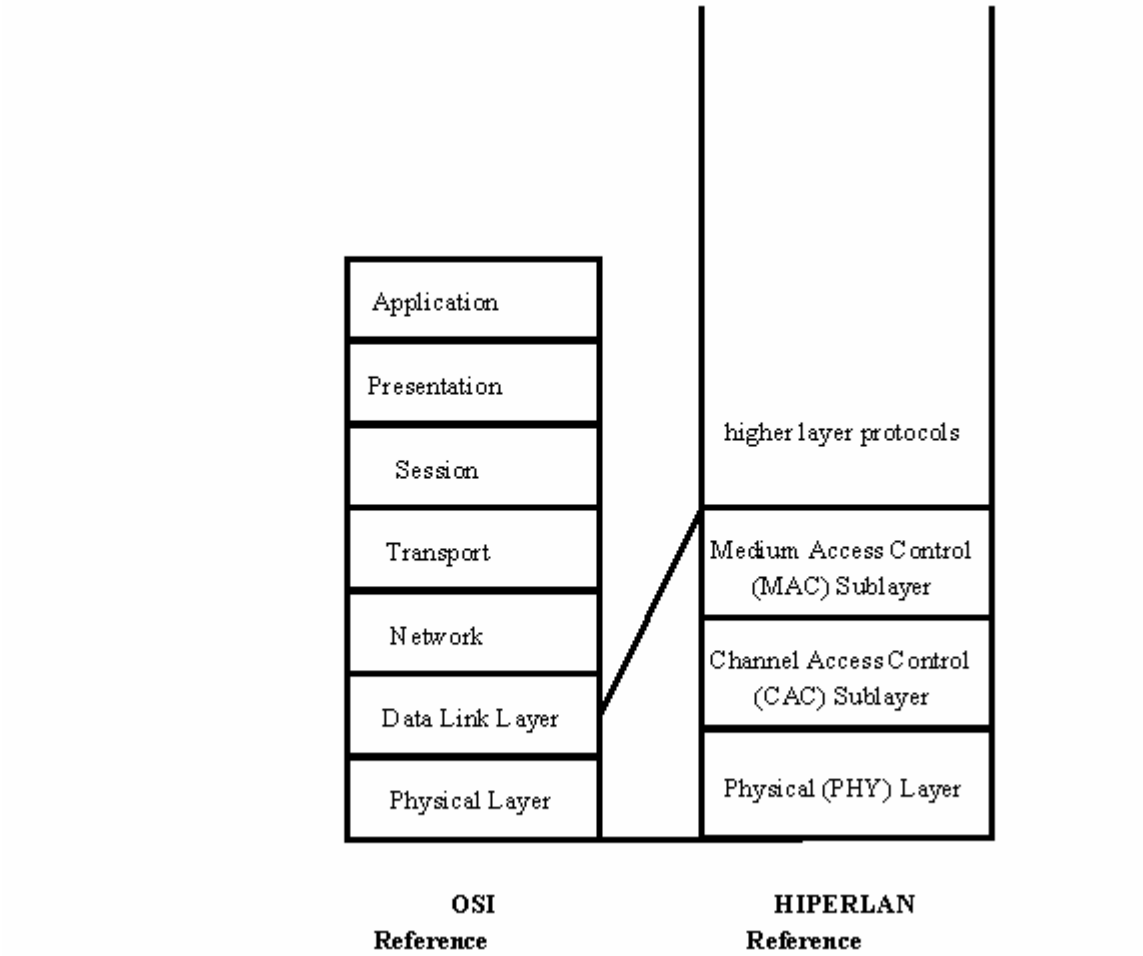
- HiperLAN stands for High performance LAN. While all of the previous technologies have been designed specifically for an adhoc environment, HiperLAN is derived from traditional LAN environments and can support multimedia data and asynchronous data effectively at high rates (23.5 Mbps).
- A LAN extension via access points can be implemented using standard features of the HiperLAN/1 specification. However, HiperLAN does not necessarily require any type of access point infrastructure for its operation.
- HiperLAN was started in 1992, and standards were published in 1995. It employs the 5.15GHz and 17.1 GHz frequency bands and has a data rate of 23.5 Mbps with coverage of 50m and mobility< 10 m/s.
- It supports a packet-oriented structure, which can be used for networks with or without a central control (BS-MS and ad-hoc). It supports 25 audio connections at 32kbps with a maximum latency of 10 ms, one video connection of 2 Mbps with 100 ms latency, and a data rate of 13.4 Mbps.
- HiperLAN/1 is specifically designed to support adhoc computing for multimedia systems, where there is no requirement to deploy a centralized infrastructure. It effectively supports MPEG or other state of the art real time digital audio and video standards.
- The HiperLAN/1 MAC is compatible with the standard MAC service interface, enabling support for existing applications to remain unchanged.
- HiperLAN 2 has been specifically developed to have a wired infrastructure, providing short-range wireless access to wired networks such as IP and ATM.

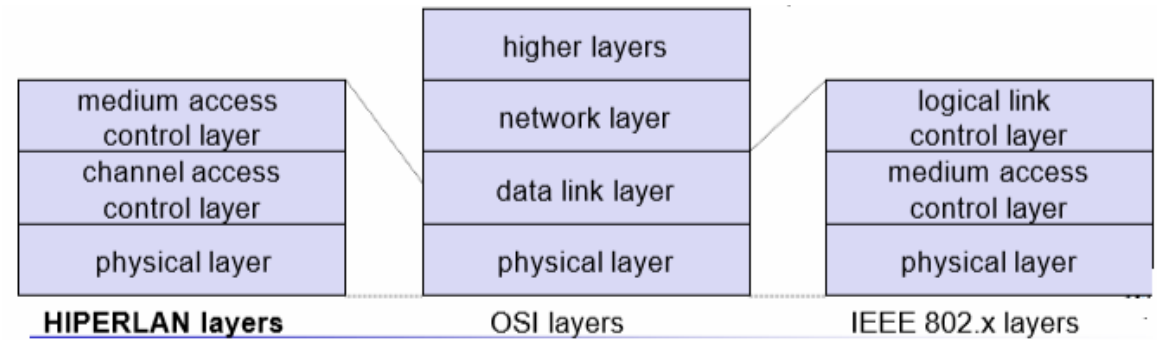
HIPERLAN requirements

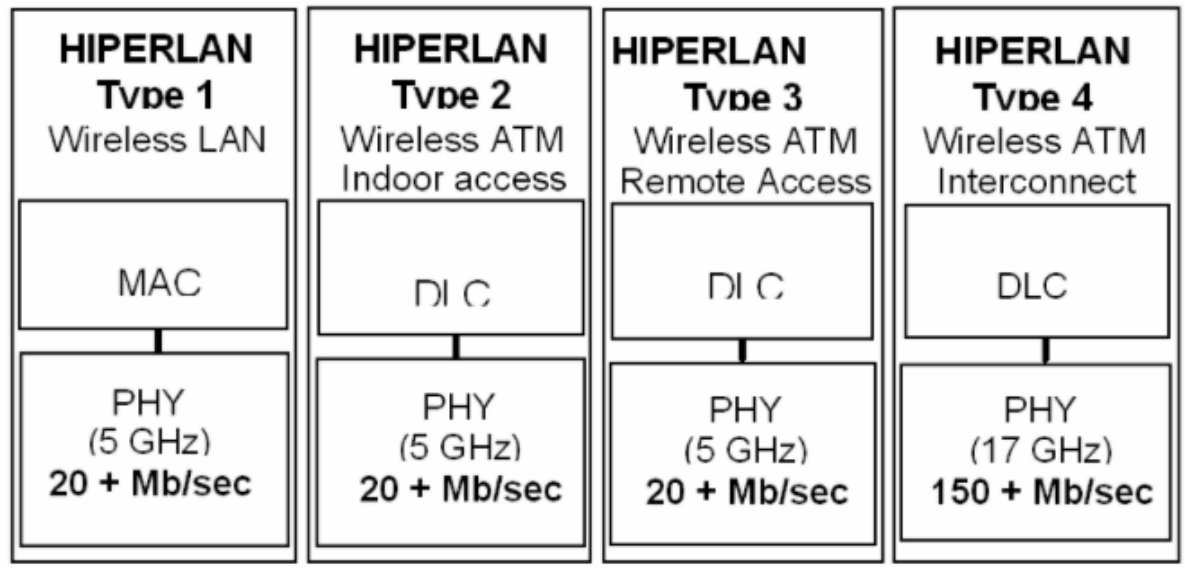
- Short range - 50m
- Low mobility - 1.4m/s
- Networks with and without infrastructure
- Support isochronous traffic
- audio 32kbps, 10ns latency
- video 2Mbps, 100ns latency
- Support asynchronous traffic
- data 10Mbps, immediate access

The goals of HiperLAN are as follows:

- QoS (to build multiservice network)
- Strong security
- Handoff when moving between local area and wide areas
- Increased throughput
- Ease of use, deployment, and maintenance
- Affordability
- Scalability

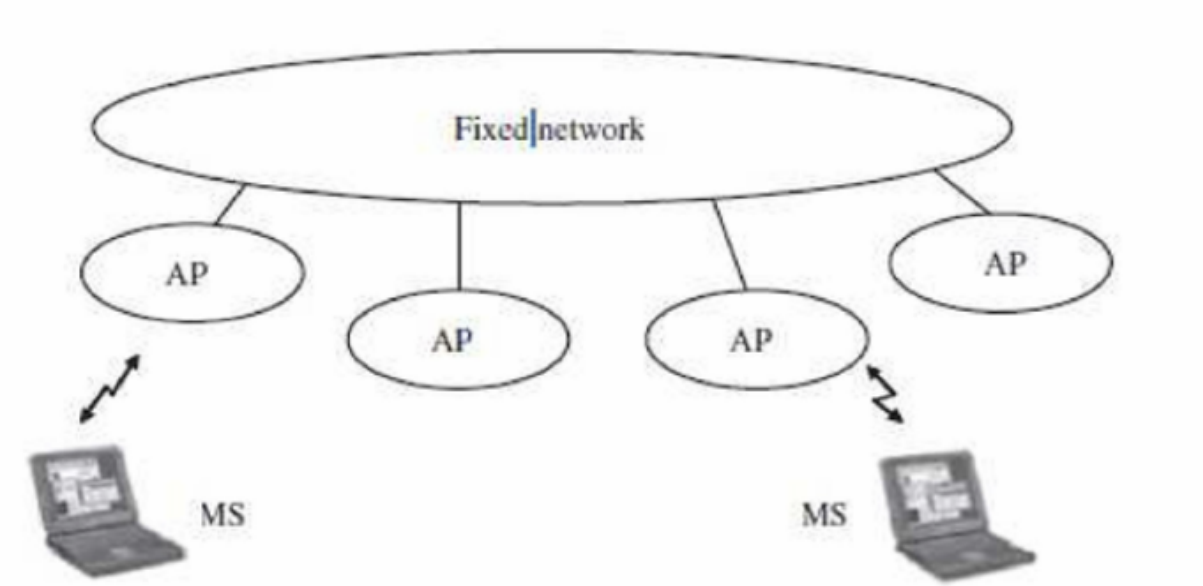



higher layers
medium access control layer
network layer
logical link control layer
channel access control layer
data link layer
medium access control layer
physical layer
physical layer
physical layer
HIPERLAN layers
OSI layers
IEEE 802.x layers


HIPERLAN Type 1
Wireless LAN
MAC
PHY (5 GHz) 20 + Mb/sec
HIPERLAN Type 2
Wireless ATM Indoor access
DLC
PHY (5 GHz) 20 + Mb/sec
HIPERLAN Type 3
Wireless ATM Remote Access
DLC
PHY (5 GHz) 20 + Mb/sec
HIPERLAN Type 4
Wireless ATM Interconnect
DLC
PHY (17 GHz) 150 + Mb/sec

-

	HIPERLAN 1	HIPERLAN 2	HIPERLAN 3	HIPERLAN 4
Application	wireless LAN	access to ATM fixed networks	wireless local loop	point-to-point wireless ATM connections
Frequency	5.1-5.3GHz			17.2-17.3GHz
Topology	decentralized ad-hoc/infrastructure	cellular, centralized	point-to-multipoint	point-to-point
Antenna	omni-directional		directional	
Range	50 m	50-100 m	5000 m	150 m
QoS	statistical	ATM traffic classes (VBR, CBR, ABR, UBR)		
Mobility	<10m/s		stationary	
Interface	conventional LAN	ATM networks		
Data rate	23.5 Mbit/s	>20 Mbit/s		155 Mbit/s
Power conservation	yes		not necessary	



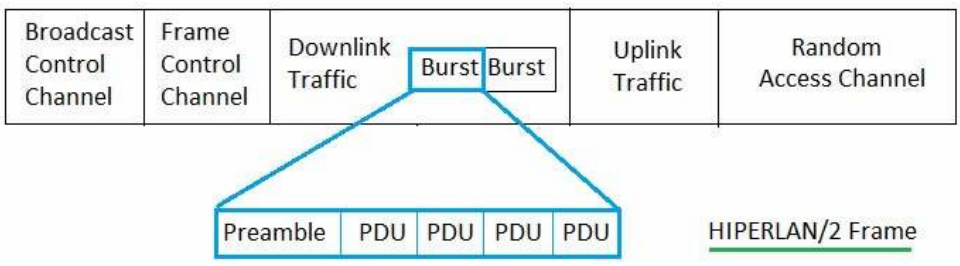
The HiperLAN/2 architecture shown in the figure allows for interoperation with virtually any type of fixed network, making the technology both network and application independent.

HiperLAN/2 networks can be deployed at "hot spot" areas such as airports and hotels, as an easy way of offering remote access and internet services.

- ✓ HIPERLAN 1
  - Data transmission
    - point-to-point, point-to-multipoint, connectionless
    - 23.5 Mbit/s, 1 W power, 2383 byte max. packet size
  - Services
    - asynchronous and time-bounded services with hierarchical priorities
    - compatible with ISO MAC
  - Topology
    - infrastructure or ad-hoc networks

        - transmission range can be larger then coverage of a single node
    - Further mechanisms
        - power saving, encryption, checksums.
- ✓ HIPERLAN 1 - CAC sublayer
    - Channel Access Control (CAC)
        - assure that terminal does not access forbidden channels
        - priority scheme, access with EY-NPMA
        - 3 EY-NPMA phases: priority resolution, contention resolution, transmission
    - Priorities
        - 5 priority levels for QoS support
        - QoS is mapped onto a priority level with the help of the packet lifetime (set by an application).
- ✓ HIPERLAN 1 - MAC layer
    - Compatible to ISO MAC
    - Supports time-bounded services via a priority scheme
    - Packet forwarding
        - support of directed (point-to-point) forwarding and broadcast forwarding (if no path information is available)
        - support of QoS while forwarding
    - Encryption mechanisms.
        - mechanisms integrated, but without key management
    - Power conservation mechanisms
        - mobile terminals can agree upon awake patterns (e.g., periodic wake-ups to receive data)
        - additionally, some nodes in the networks must be able to buffer data for sleeping terminals and to forward them at the right time (so called stores).

HIPERLAN/2 Frame Structure



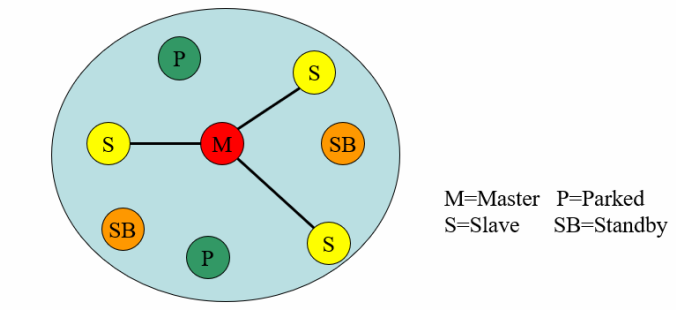
HIPERLAN/2 Frame

The basic frame structure in HIPERLAN/2 consists of broadcast, frame control, downlink, uplink and random access. Transmission format in HIPERLAN/2 is burst which consists of preamble and data fields (i.e. PDUs).

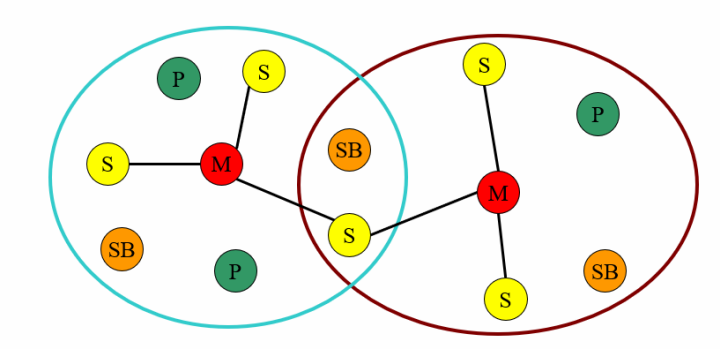
- ✓ Difference between WLAN and HIPERLAN

Parameters	HIPERLAN	802.11 WLAN
Application	Access to ATM fixed network	Wireless networks
Frequency, Band	5 GHz	2.4 GHZ
Maximum Data rate	54 Mbps	2 Mbps
Topology	Cellular, centralized	Can be adhoc or infra-based
Error control	Arq/fec phy layer	ARQ
Range	50-100m	100 m
Interface	high	medium
Medium Access method	AP centralized	CSMA/CA
Connectivity	Connection oriented	Connectionless
QoS (Quality of Service	ATM /802.1p/RSVP	PCF (optional)
Frequency Selection	dynamic frequency selection (DSS)	Frequency hopping or DSSS
Typical Outdoor Range	—	—
Encryption	DES, 3DES	40 bit RC4
Authentication	X.509	No

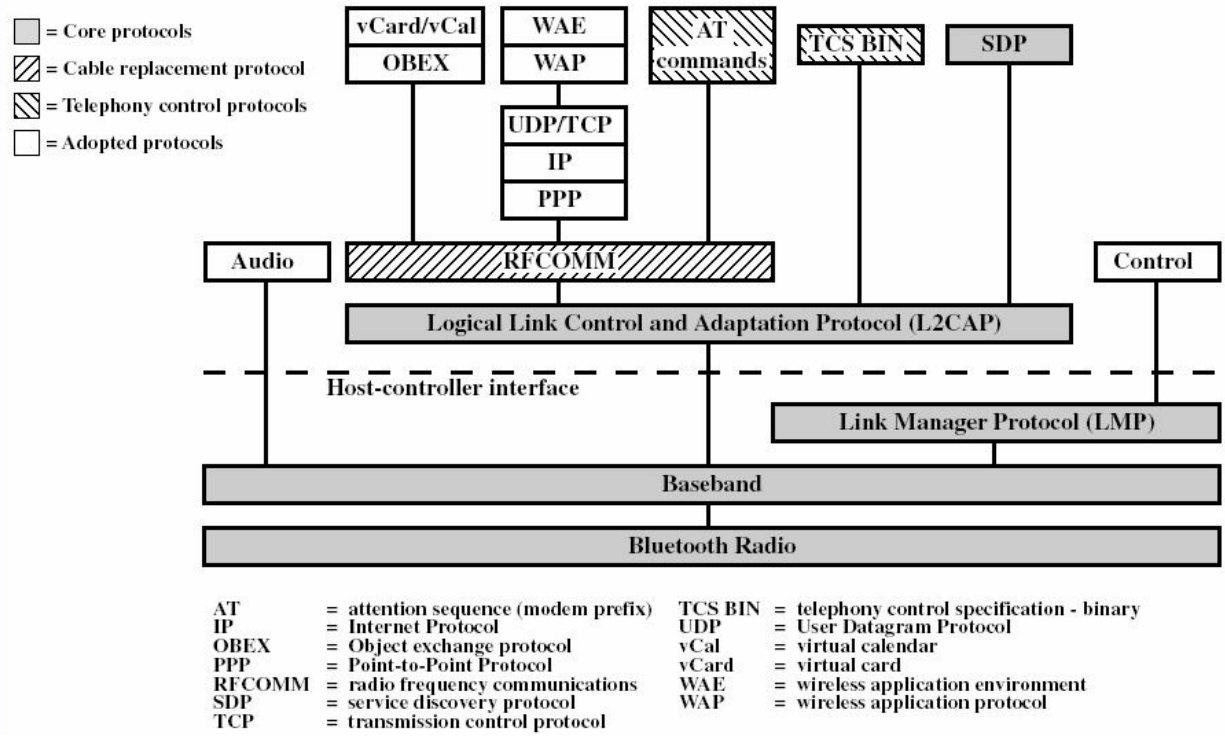
Bluetooth

- ✓ Bluetooth
  - Uses the radio range of 2.45 GHz
  - Theoretical maximum bandwidth is 1 Mb/s
  - Several Bluetooth devices can form an ad hoc network called a "piconet"
  - In a piconet one device acts as a master (sets frequency hopping behaviour) and the others as slaves
  - Example: A conference room with many laptops wishing to communicate with each other
- ✓ Bluetooth Architecture
- ✓ Piconet
  - Each piconet has one master and up to 7 simultaneous slaves
  - Master : device that initiates a data exchange.
  - Slave : device that responds to the master
  - 

- ✓ Scatternet
  - Linking of multiple piconets through the master or slave devices
  - Bluetooth devices have point-to-multipoint capability to engage in Scatternet communication.



✓ Bluetooth Protocol Architecture



✓ **Bluetooth Radio** : specifics details of the air interface, including frequency, frequency hopping, modulation scheme, and transmission power.

✓ **Baseband**: concerned with connection establishment within a piconet, addressing, packet format, timing and power control.

✓ **Link manager protocol (LMP)**: establishes the link setup between Bluetooth devices and manages ongoing links, including security aspects (e.g. authentication and encryption), and control and negotiation of baseband packet size

✓ **Logical link control and adaptation protocol (L2CAP)**: adapts upper layer protocols to the baseband layer. Provides both connectionless and connection-oriented services.

✓ **Service discovery protocol (SDP)**: handles device information, services, and queries for service characteristics between two or more Bluetooth devices.

- ✓ **Host Controller Interface (HCI)**: provides an interface method for accessing the Bluetooth hardware capabilities. It contains a command interface, which acts between the Baseband controller and link manager.

- ✓ **TCS BIN (Telephony Control Service):** bit-oriented protocol that defines the call control signalling for the establishment of voice and data calls between Bluetooth devices.

- ✓ **OBEX(OBject EXchange)** : Session-layer protocol for the exchange of objects, providing a model for object and operation representation

- ✓ **RFCOMM:** a reliable transport protocol, which provides emulation of RS232 serial ports over the L2CAP protocol

- ✓ **WAE/WAP:** Bluetooth incorporates the wireless application environment and the wireless application protocol into its architecture.

Unit 4

UNIT IV ROUTING **9**

Mobile IP- SIP – DHCP – AdHoc Networks – Proactive and Reactive Routing Protocols – Multicast Routing - WSN routing – LEACH- SPIN- PEGASIS

Mobile IP

- ✓ RFC 3344 standard
- ✓ Motivation
    - Routing
        - based on IP destination address, network prefix (e.g. 129.13.42.99) determines physical subnet.
    - Specific routes to end-systems
        - change of all routing table entries to forward packets to the right destination.
    - Changing the IP-address
        - adjust the host IP address depending on the current location

REQUIREMENTS

Compatibility:

Mobile IP has to remain compatible with all lower layers used for the standard, non-mobile, IP.

Mobile IP must not require special media or MAC/LLC protocols, so it must use the same interfaces and mechanisms to access the lower layers as IP does.

Transparency:

Mobility should remain 'invisible' for many higher layer protocols and applications. Besides maybe noticing a lower bandwidth and some interruption in service, higher

layers should continue to work even if the mobile computer has changed its point of attachment to the network.

Clearly, many of today's applications have not been designed for use in mobile

environments, so the only effects of mobility should be a higher delay and lower

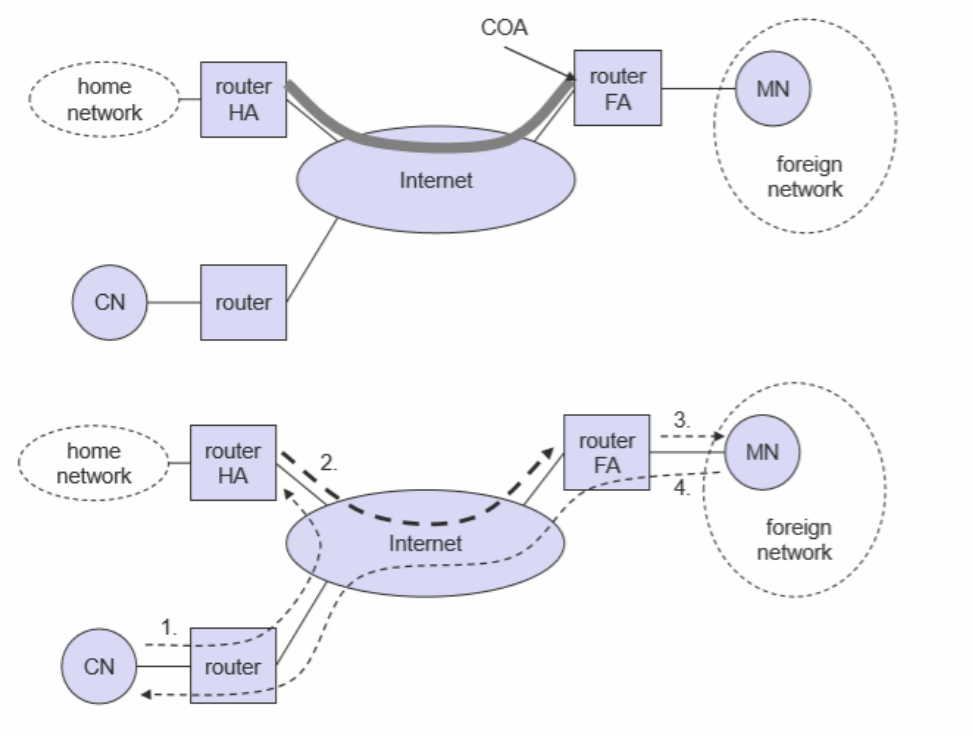
bandwidth. However, there are some applications for which it is better to be 'mobility aware'.

Scalability and efficiency:

It is crucial for a mobile IP to be scalable over a large number of participants in the whole internet, worldwide. Introducing a new mechanism to the internet must not jeopardize its efficiency. Enhancing IP for mobility must not generate too many new messages flooding the whole network. Special care has to be taken considering the lower bandwidth of wireless links.
Looking at the number of computers connected to the internet and at the growth rates of mobile communication, it is clear that myriad devices will participate in the internet as mobile components.

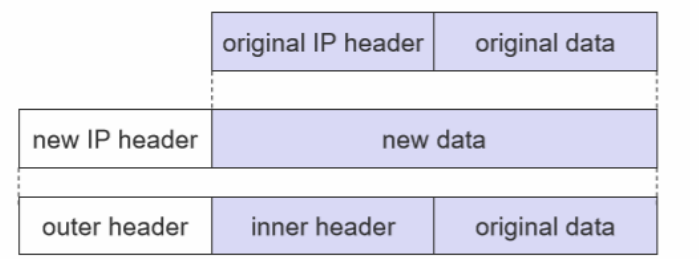
Security:

- ✓ Terminology

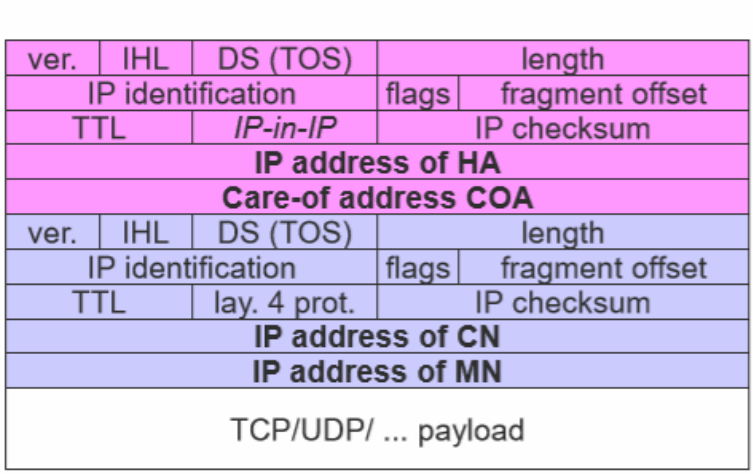


  - Mobile Node (MN)
    - system (node) that can change the point of connection to the network without changing its IP address
  - Home Agent (HA)
    - system in the home network of the MN, typically a router
    - registers the location of the MN, tunnels IP datagrams to the COA
  - Foreign Agent (FA)

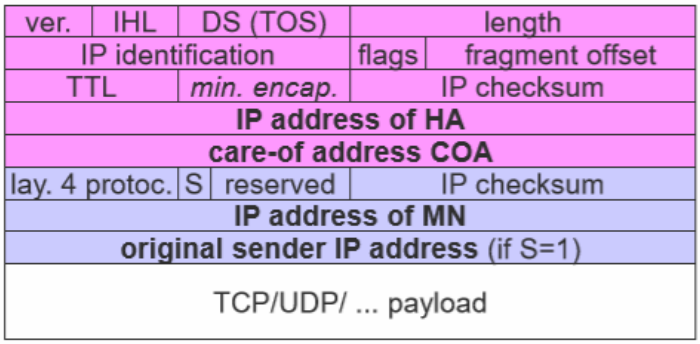
        - system in the current foreign network of the MN, typically a router
        - forwards the tunnelled datagrams to the MN, typically also the default router for the MN.
    - Care-of Address (COA)
        - address of the current tunnel end-point for the MN (at FA or MN).
        - actual location of the MN from an IP point of view -can be chosen, e.g., via DHCP.
    - Correspondent Node (CN)
        - communication partner
- ✓ Data transfer to mobile node
    - Sender sends to the IP address of MN, HA intercepts packet (proxy ARP)
    - HA tunnels packet to COA, here FA, by encapsulation
    - FA forwards the packet to the MN.
- ✓ Data transfer from mobile node
    - Sender sends to the IP address of the receiver as usual, FA works as default route.
- ✓ Network Integration
    - Agent Advertisement
        - HA and FA periodically send advertisement messages into their physical subnets
        - MN listens to these messages and detects, if it is in the home or a foreign network (standard case for home network)
        - MN reads a COA from the FA advertisement messages
    - Registration (always limited lifetime!)
        - MN signals COA to the HA via the FA, HA acknowledges via FA to MN
        - these actions have to be secured by authentication
    - Advertisement
        - HA advertises the IP address of the MN (as for fixed systems), i.e. standard routing information
        - routers adjust their entries, these are stable for a longer time (HA responsible for a MN over a longer period of time)
        - packets to the MN are sent to the HA,
        - independent of changes in COA/FA.
- ✓ Encapsulation



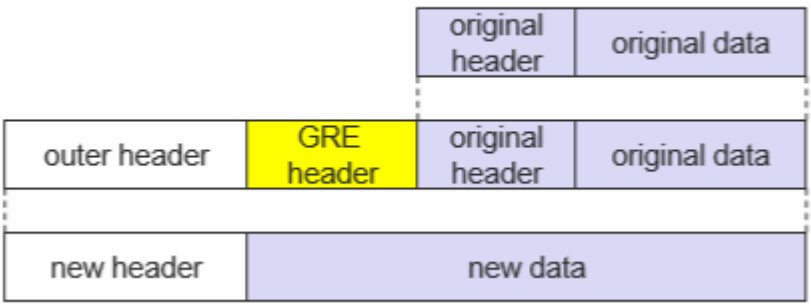
    -
    - Encapsulation of one packet into another as payload -e.g. IPv6 in IPv4 (6Bone), Multicast in Unicast (Mbone).
    - IP-in-IP encapsulation
        - IP-in-IP-encapsulation (mandatory, RFC 2003) -tunnel between HA and COA.



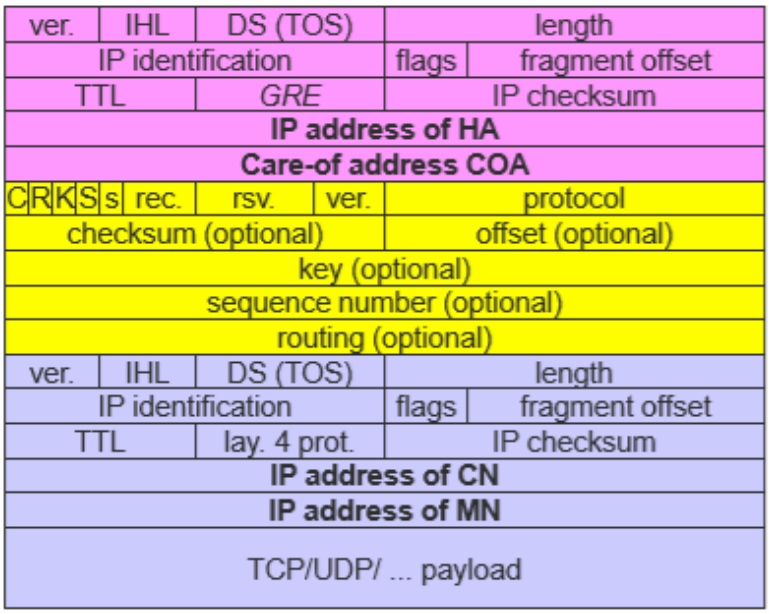
- Minimal encapsulation
  - avoids repetition of identical fields -e.g. TTL, IHL, version, DS (RFC 2474, old: TOS).
  - only applicable for non-fragmented packets, no space left for fragment identification.



- Generic Routing Encapsulation
  - Allows encapsulation of one protocol suite into the payaload portion of the packet of another protocol suite.



  - Contains several flags – Checksum bit (c), routing field (R), Key field (k), sequence number field (S), strict source routing (s).



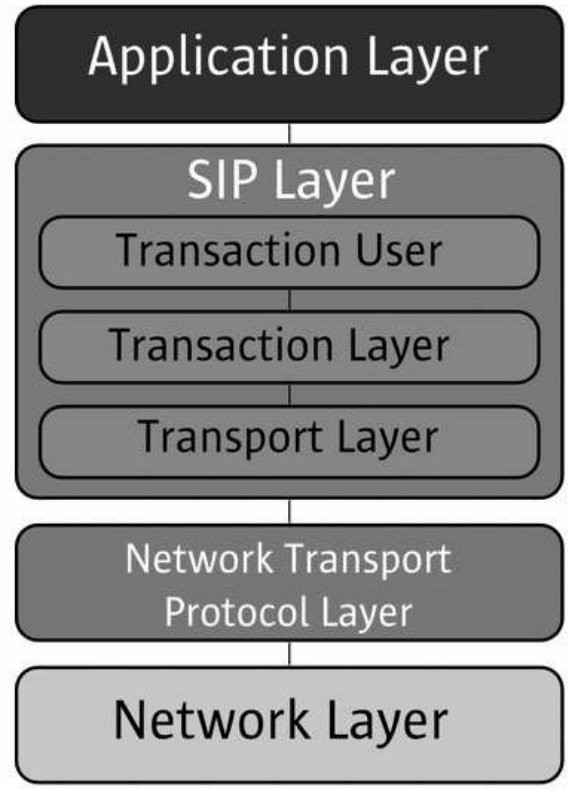
SIP

Session Initiation Protocol (SIP) is one of the most common protocols used in VoIP technology. It is an application layer protocol that works in conjunction with other application layer protocols to control multimedia communication sessions over the Internet.

- SIP is a signalling protocol used to create, modify, and terminate a multimedia session over the Internet Protocol. A session is nothing but a simple call between two endpoints. An endpoint can be a smartphone, a laptop, or any device that can receive and send multimedia content over the Internet.
- SIP is an application layer protocol defined by IETF (Internet Engineering Task Force) standard. It is defined in **RFC 3261**.
- SIP embodies client-server architecture and the use of URL and URI from **HTTP** and a text encoding scheme and a header style from **SMTP**.
- SIP takes the help of SDP (Session Description Protocol) which describes a session and RTP (Real Time Transport Protocol) used for delivering voice and video over IP network.
- SIP can be used for two-party (unicast) or multiparty (multicast) sessions.
- Other SIP applications include file transfer, instant messaging, video conferencing, online games, and streaming multimedia distribution.

Basically SIP is an application layer protocol. It is a simple network signalling protocol for creating and terminating sessions with one or more participants. The SIP protocol is designed to be independent of the underlying transport protocol, so SIP applications can run on TCP, UDP, or other lower-layer networking protocols.

The following illustration depicts where SIP fits in in the general scheme of things −



Typically, the SIP protocol is used for internet telephony and multimedia distribution between two or more endpoints. For example, one person can initiate a telephone call to another person using SIP, or someone may create a conference call with many participants.

The SIP protocol was designed to be very simple, with a limited set of commands. It is also text-based, so anyone can read a SIP message passed between the endpoints in a SIP session.

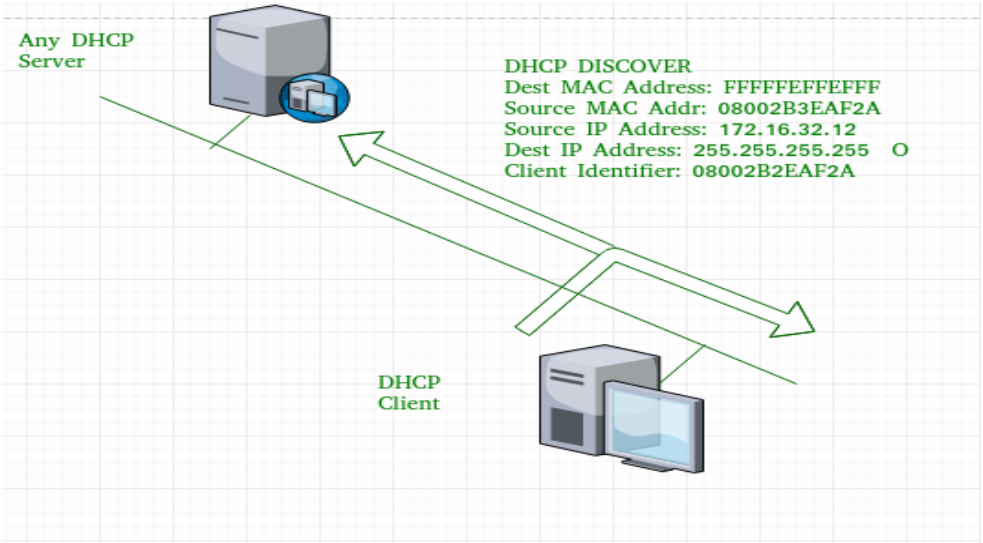
DHCP

Dynamic Host Configuration Protocol(DHCP) is an application layer protocol which is used to provide:- **simplify the installation and maintenance of networked computers**

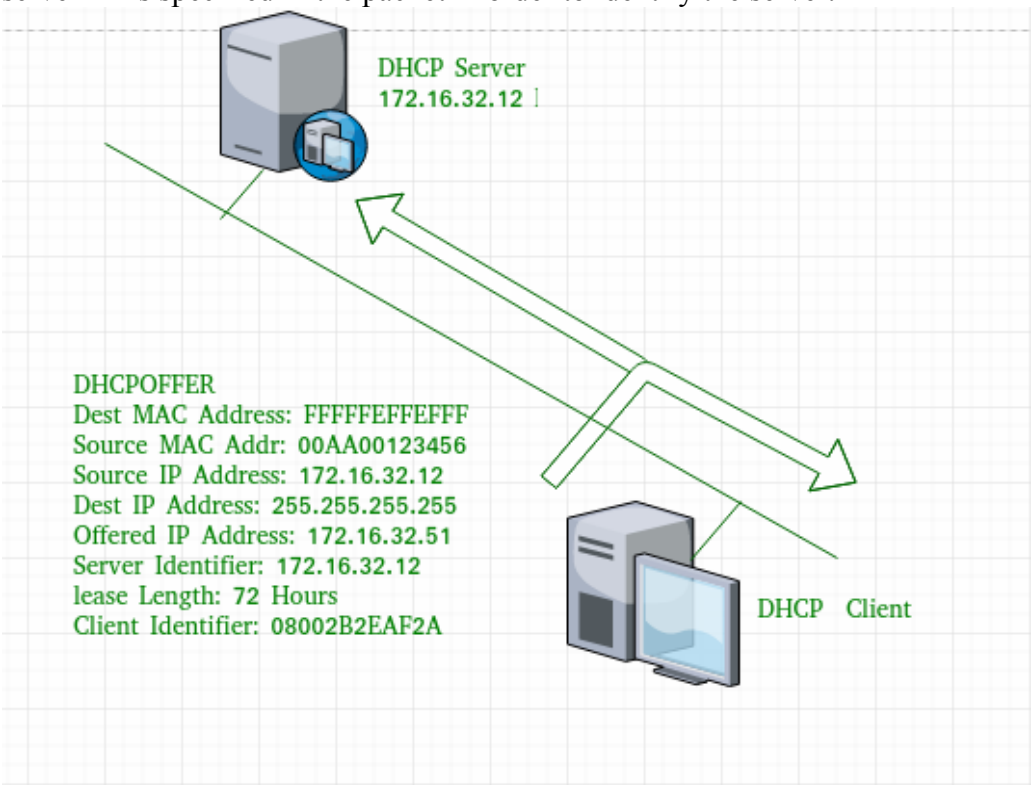
1. Subnet Mask (Option 1 – e.g., 255.255.255.0)
2. Router Address (Option 3 – e.g., 192.168.1.1)
3. DNS Address (Option 6 – e.g., 8.8.8.8)
4. Vendor Class Identifier (Option 43 – e.g., 'unifi' = 192.168.1.9 ##where unifi = controller)

DHCP is based on a client-server model and based on discovery, offer, request, and ACK.

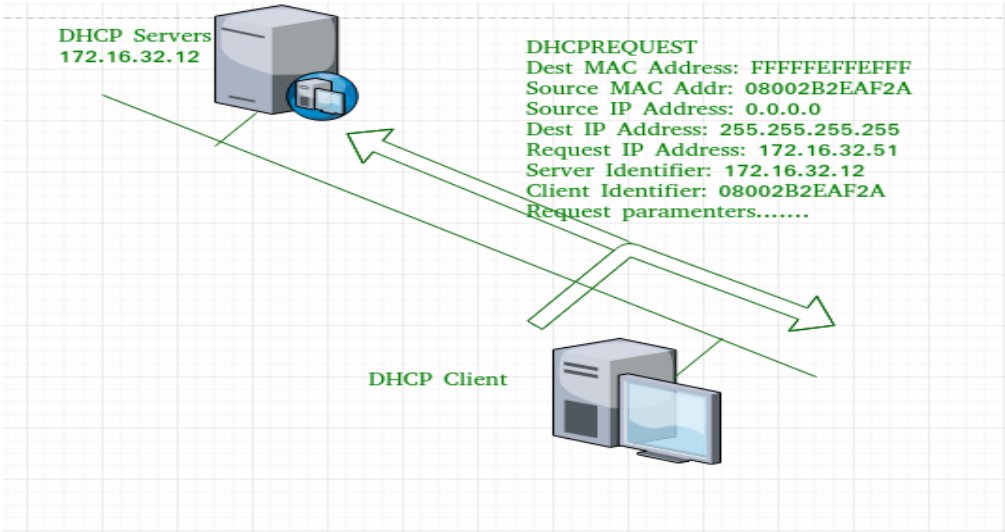
DHCP discover message –This is a first message generated in the communication process between server and client. This message is generated by Client host in order to discover if there is any DHCP server/servers are present in a network or not. This message is broadcasted to all devices present in a network to find the DHCP server. This message is 342 or 576 bytes long



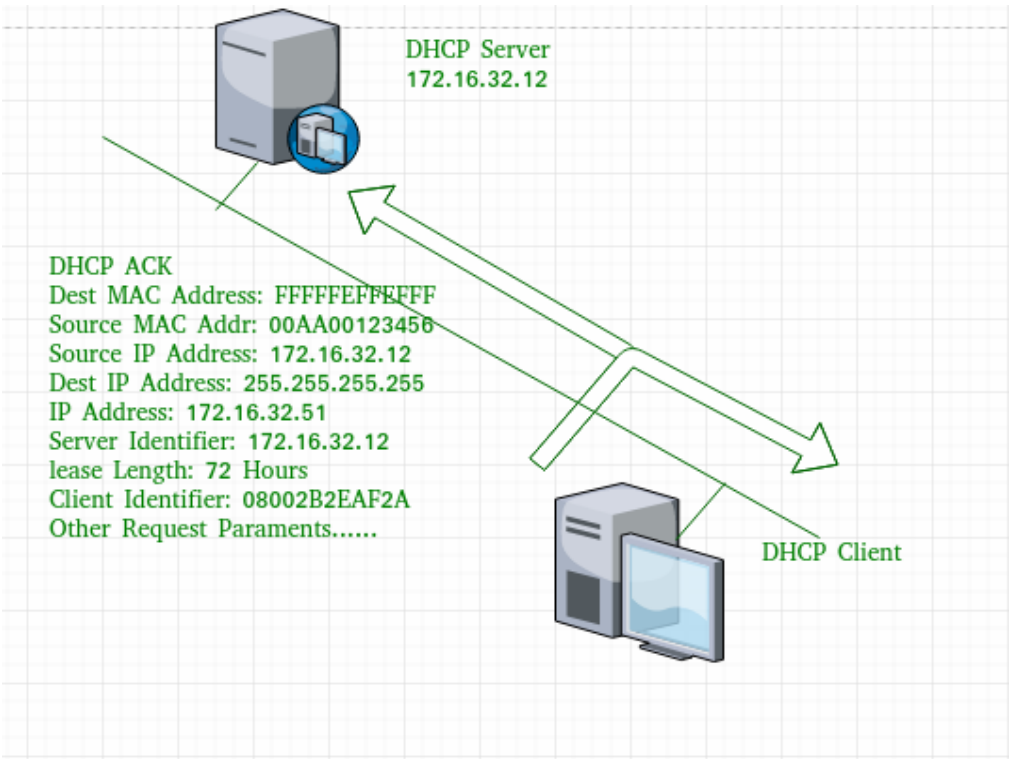
DHCP offer message –The server will respond to host in this message specifying the unleased IP address and other TCP configuration information. This message is broadcasted by server. Size of message is 342 bytes. If there are more than one DHCP servers present in the network then client host will accept the first DHCP OFFER message it receives. Also a server ID is specified in the packet in order to identify the server.



DHCP request message –When a client receives a offer message, it responds by broadcasting a DHCP request message. The client will produce a gratuitous ARP in order to find if there is any other host present in the network with same IP address. If there is no reply by other host, then there is no host with same TCP configuration in the network and the message is broadcasted to server showing the acceptance of IP address .A Client ID is also added in this message.



DHCP acknowledgement message –In response to the request message received, the server will make an entry with specified client ID and bind the IP address offered with lease time. Now, the client will have the IP address provided by server.



DHCP negative acknowledgement message – Whenever a DHCP server receives a request for IP address that is invalid according to the scopes that is configured with, it send DHCP Nak message to client. Eg-when the server has no IP address unused or the pool is empty, then this message is sent by the server to client.

DHCP decline –If DHCP client determines the offered configuration parameters are different or invalid, it sends DHCP decline message to the server .When there is a reply to the gratuitous ARP by any host to the client, the client sends DHCP decline message to the server showing the offered IP address is already in use.

DHCP release –A DHCP client sends DHCP release packet to server to release IP address and cancel any remaining lease time.

DHCP inform –If a client address has obtained IP address manually then the client uses a DHCP inform to obtain other local configuration parameters, such as domain name. In reply to the DHCP inform message, DHCP server generates DHCP ack message with local.

Mobile ad-hoc networks

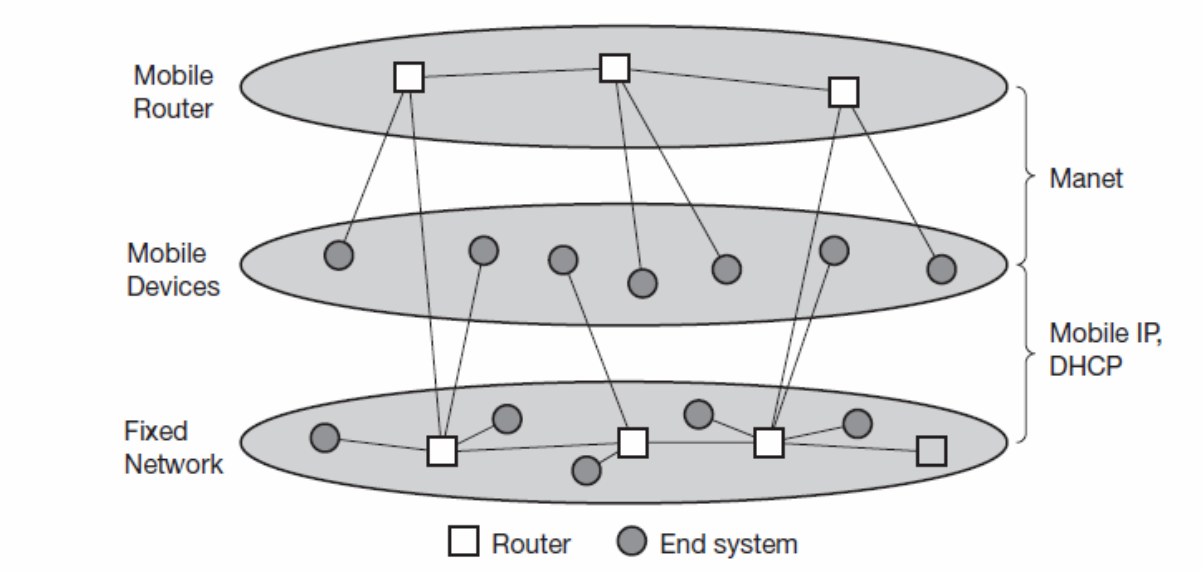
Mobility support relies on the existence of atleast some infrastructure. Mobile IP requires, e.g., a home agent, tunnels, and default routers. DHCP requires servers and broadcast capabilities of the medium reaching all participants or relays to servers. Cellular phone networks require base stations, infrastructure networks etc. However, there may be several situations where users of a network cannot rely on an infrastructure, it is too expensive, or there is none at all. In these situations mobile ad-hoc networks are the only choice.

Instant infrastructure: Unplanned meetings, spontaneous interpersonal communications etc. cannot rely on any infrastructure. Infrastructures need planning and administration. It would take too long to set up this kind of infrastructure; therefore, ad-hoc connectivity has to be set up.

Disaster relief: Infrastructures typically break down in disaster areas. Hurricanes cut phone and power lines, floods destroy base stations, fires burn servers. Emergency teams can only rely on an infrastructure they can set up themselves. No forward planning can be done, and the set-up must be extremely fast and reliable. The same applies to many military activities, which is, to be honest, one of the major driving forces behind mobile ad-hoc networking research.

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. If, for example, only connection oriented cellular networks exist, but an application sends only a small status information every other minute, a cheaper ad-hoc packet-oriented network might be a better solution. Registration procedures might take too long, and communication overheads might be too high with existing networks. Application-tailored ad-hoc networks can offer a better solution.

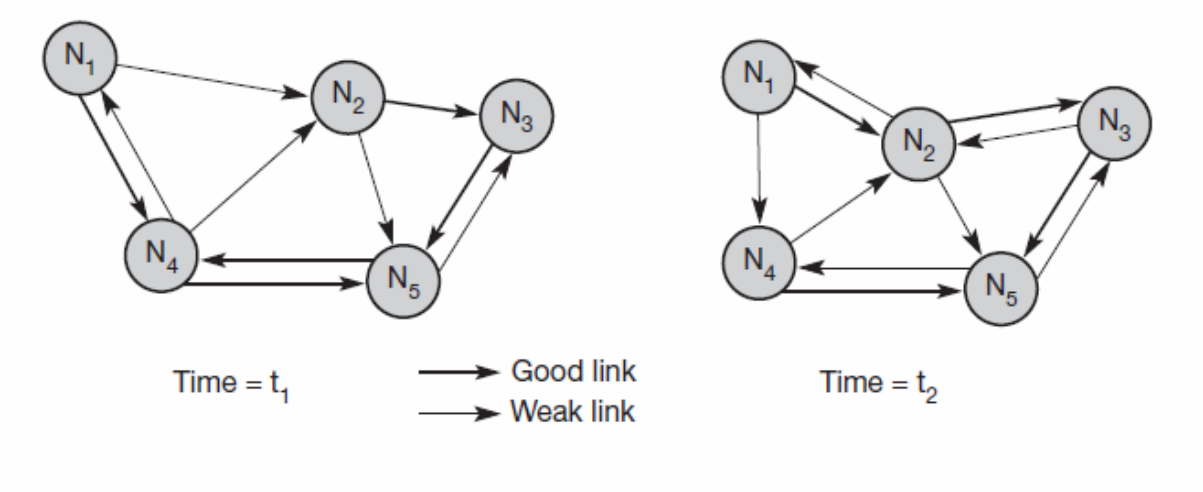


Over the last few years ad-hoc networking has attracted a lot of research interest. This has led to creation of a working group at the IETF that is focussing on **mobile ad-hoc networking**, called **MANET** (MANET, 2002), (Corson, 1999).
While mobile IP and DHCP handle the connection of mobile devices to a fixed infrastructure, MANET comprises mobile routers, too.
Mobile devices can be connected either directly with an infrastructure using Mobile IP for mobility support and DHCP as a source of many parameters, such as an IP address.
MANET research is responsible for developing protocols and components to enable ad-hoc networking between mobile devices.

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. This made an easy connection possible to the ARPAnet, the starting point of today's Internet. Twenty radio channels between 1718.4–1840 MHz were used offering 100 or 400 kbit/s. The system used DSSS with 128 or 32 chips/bit.

Routing
While in wireless networks with infrastructure support a base station always reaches all mobile nodes, this is not always the case in an ad-hoc network. A destination node might be out of range of a source node transmitting packets.

Routing is needed to find a path between source and destination and to forward the packets appropriately

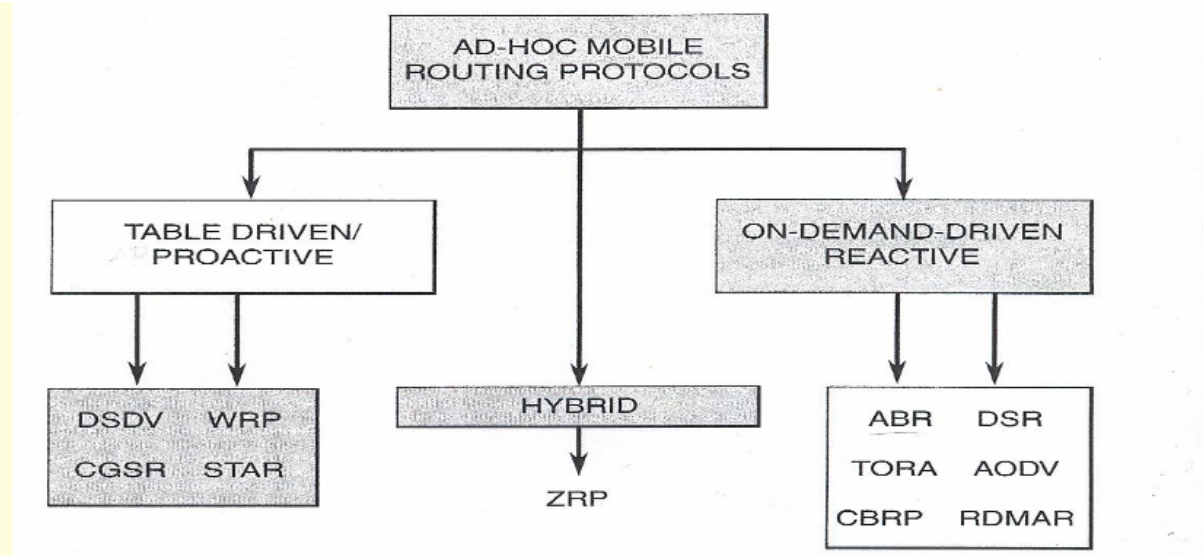


Example of adhoc network

Fundamental differences between wired networks and ad-hoc wireless networks related to routing.

***Asymmetric links**
***Redundant links**
***Interference**
***Dynamic topology**

Proactive and Reactive routing protocols



Multicast Routing

Multicast routing is special case of broadcast routing with significance difference and challenges. In broadcast routing, packets are sent to all nodes even if they do not want it. But in Multicast routing, the data is sent to only nodes which wants to receive the packets.

Routing is the process of selecting paths in a network along which to send network Traffic. Routing is performed for many kinds of networks, including the telephone network, electronic data networks (such as the Internet), and transportation networks. In packet switching networks, routing directs packet forwarding, the transit of logically addressed packets from their source toward their ultimate destination through intermediate nodes;

typically hardware devices called routers, bridges, gateways, firewalls, or switches. Multicast (delivers a message to a group of nodes that have expressed interest in receiving the message). With a multicast design, applications can send one copy of each packet and address it to the group of computers that want to receive it. This technique addresses packets to a group of receivers rather than to a single receiver, and it depends on the network to forward the packets to only the networks that need to receive them. Path selection involves applying a routing metric to multiple routes, in order to select the best route. In the case of computer networking, the metric is computed by a routing algorithm, and can cover such information as bandwidth, network delay, hop count, path cost, load, reliability, and communication cost.

DVMRP is a distance vector style algorithm that builds source based multicast trees. When a DVMRP router receives a multicast packet, it sends the packet to all attached routers and waits for a response. Routers with no group members return a ―prune‖ message, which eventually prevents further multicast messages for that group from reaching the router. The prune state is soft, that is, it will time-out within a set time interval. If after sending a prune and before the state can time-out, the host wants to join the group, it has to send a graft message upstream. DVMRP is inefficient when the number of receivers in the group is sparsely distributed. DVMRP builds its own routing table instead of reusing the existing unicast routing table for RPF checking of incoming packets. DVMRP has been used to build the MBONE—a multicast backbone across the public Internet—by building tunnels between DVMRP-capablemachines. The MBONE is used widely in the research community to transmit the proceedings of various conferences and to permit desktop conferencing. A packet is assumed to have arrived on the RPF interface if a router receives it on an interface that it uses to send unicast packets to the source. If the packet arrives on the RPF interface, then router forwards it out the interfaces that are present in the outgoing interface list of a multicast routing table entry.

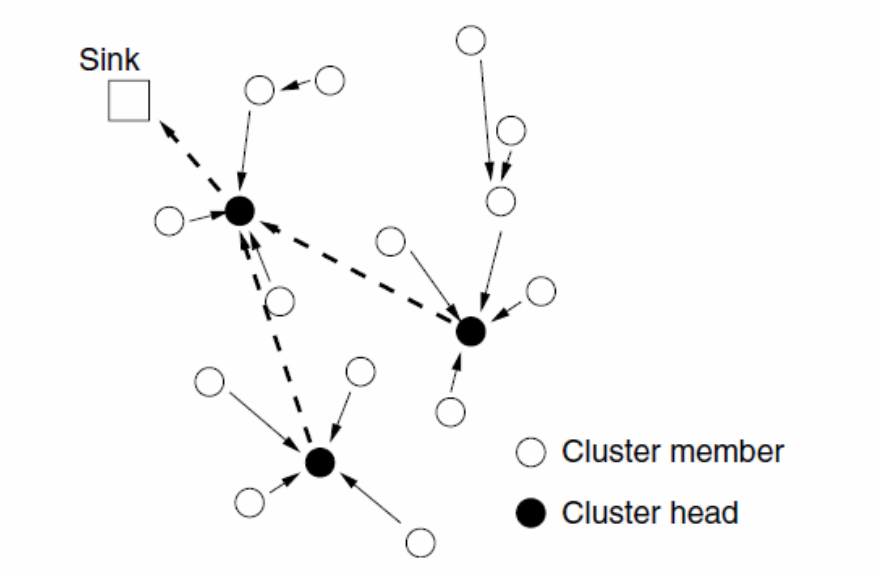
IGMPThe Internet Group Management Protocol, version 2[RFC 2236], operates between a host and its directly attached router (informally, think of the directly attached router as thefirst-hoprouter that a host would see on a path to any other host outside its own local network, or thelast-hop router on any path to that host), IGMP provides the means for a host to inform its attached router that an application running on the host wants to join a specific multicast groupIGMP interaction is limited to a host and its attached router, another protocol is clearly required to coordinate the multicast routers (including the attached routers) throughout the Internet, so that multicast datagram are routed to their final destinations. IGMP version 2 [RFC 2236] has only three message types. A general membership query message is sent by a router to all hosts on an attached interface (for example, to all hosts on a local area network) to determine the set of all multicast groups that have been joined by the hosts on that interface. A router can also determine whether a specific multicast group has been joined by hosts on an attached interface using a specific membership query. The specific query includes the multicast address of the group being queried in the multicast group address field of the IGMP membership query message

WSN Protocols

LEACH PROTOCOL

The LEACH (*Low-Energy Adaptive Clustering Hierarchy*)protocol aims to minimize energy consumption in WSNs through a cluster-based operation. The goal of LEACH is to dynamically select sensor nodes as cluster heads and form clusters in the network. The communications inside the clusters are directed to the cluster head, which performs aggregation. Cluster heads then directly communicate with the sink to relay the collected information from each cluster. LEACH also changes the cluster head role dynamically such that the high-energy consumption in communicating with the sink is spread to all sensor nodes in the network.

The operation of LEACH is controlled through *rounds*, which consist of several phases. During each round, each cluster formation stays the same, and the cluster heads are selected at the beginning of each round. A round is separated into two phases, the *setup phase* and *steady state phase*. During the setup phase, cluster heads are selected, clusters are formed, and the cluster communication schedule is determined. During the steady state phase, data communication between the cluster members and the cluster head is performed. The duration of the steady state phase is longer than the duration of the setup phase in order to minimize the overhead.



The setup phase of LEACH consists of three phases: advertisement, cluster setup, and schedule creation. LEACH aims to randomly select sensors as cluster heads during the beginning of each round. The cluster head selection is performed through the advertisement phase, where the sensor nodes broadcast a cluster head advertisement message. Firstly, a sensor node chooses a random number between 0 and 1. If this random number is less than a threshold T(n), the sensor node becomes a cluster head.

$$T(n) = \begin{cases} \dfrac{P}{1 - P[r \bmod (1/P)]} & \text{if } n \in G \\ 0 & \text{otherwise} \end{cases}$$

where P is the desired percentage to become a cluster head, r is the current round, and G is the set of nodes that have not been selected as a cluster head in the last 1/P rounds. The

selected cluster heads then advertise to their neighbours in the network that they are the new cluster heads. For this operation, LEACH relies on a CSMA-based random access scheme to avoid advertisement collisions from multiple cluster heads. Once the sensor nodes receive the advertisement, they determine the cluster that they belong to.

If a node receives an advertisement from a single cluster head, then it automatically becomes a member of that cluster. However, if a sensor node receives advertisements from multiple cluster heads, the cluster selection is performed based on the signal strength of the advertisement from the cluster heads to the sensor nodes. The cluster head with the highest signal strength is selected.

After the advertisement phase, the sensor nodes inform the associate cluster head that they will be members of the cluster, which is called the cluster setup phase. Again, LEACH relies on a CSMA-based random access scheme to prevent collisions between packets sent by each node. Finally, the schedule creation phase is performed, where the cluster heads assign the time during which the sensor nodes can send data to the cluster heads. This selection is based on a time division multiple access (TDMA)approach, which is followed throughout the steady state phase.

Once the cluster formation is completed in the setup phase, LEACH switches to the steady state phase. During this phase, the sensor nodes can begin sensing and transmitting data to the cluster heads. The cluster heads also aggregate data from the nodes in their cluster before sending these data to the sink. At the end of the steady state phase, the network goes into the setup phase again to enter into another round of selecting the cluster heads. As a result, energy consumption due to the cluster head duty is equally distributed among sensor nodes.

The advantages and disadvantages of Leach protocol

LEACH is a MAC protocol, it contains many advantages like it does not need any control information, it **saves energy**, it is completely distributed and also contain many disadvantages like if cluster head dies then cluster become useless, clusters are divided randomly etc.

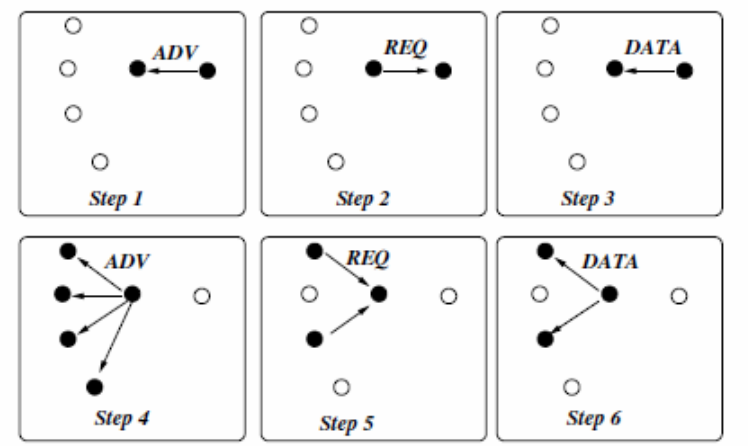
ADVANTAGES AND DISADVANTAGES The various advantages of LEACH protocol are:

1. The Cluster Heads aggregates the whole data which lead to reduce the traffic in the entire network].
2. As there is a single hop routing from nodes to cluster head it results in saving energy.
3. It increases the lifetime of the sensor network.
4. In this, location information of the nodes to create the cluster is not required.
5. LEACH is completely distributed as it does not need any control information from the base station as well as no global knowledge of the network is required.

Besides the advantages of LEACH [9] it also has some Demerits which are as follows:

1. LEACH does not give any idea about the number of cluster heads in the network.
2. One of the biggest disadvantage of LEACH is that when due to any reason Cluster head dies, the cluster will become useless because the data gathered by the cluster nodes would never reach its destination i.e. Base Station .
3. Clusters are divided randomly, which results in uneven distribution of Clusters. For e.g. some clusters have more nodes and some have lesser nodes. Some cluster heads at the center of the cluster and some cluster heads may be in the edge of the cluster [10]; this phenomenon can cause an increase in energy consumption and have great impact on the performance of the entire network.

SPIN (*Sensor Protocols for Information via Negotiation*)is a family of routing protocols designed to address the deficiencies of flooding by negotiation and resource adaptation. For this purpose, two main approaches are followed. Firstly, instead of sending all the data, sensor nodes negotiate with each other through packets that describe the data. Consequently, the observed information is only sent to interested sensor nodes as a result of this negotiation. Secondly, each node monitors its energy resource, which is used to perform energy-aware decisions.



Before sending a DATA packet, a node advertises its intent by broadcasting an ADV packet (Step 1).The ADV packet contains a description of the DATA packet to be sent, which is much smaller in size than the DATA packet. Then, if a neighbour is interested in the ADV packet, it replies back with a REQ message (Step 2). Finally, the DATA packet is sent to the node that requests it (Step 3). Data propagation in WSNs is coordinated through this mechanism at each hop. As shown in Steps 4, 5, and 6, multiple nodes can send REQ messages back to a node, which sends DATA to each node until all the nodes get a copy. As a result of the SPIN protocol, the sensor nodes in the entire sensor network which are interested in the data will get a copy.

The above figure referred to as the point-to-point SPIN protocol (SPINPP).In addition to SPIN-PP, several variations have been proposed to address some of the disadvantages of SPIN-PP. SPIN with energy consumption awareness(SPIN-EC), SPIN for broadcast networks (SPIN-BC), and SPIN with reliability (SPIN-RL).

SPIN-PP does not address the resource-blindness problem of conventional flooding or gossiping protocols. Although the DATA packet transmission is limited to nodes that provide interest, energy consumption is still a concern. SPIN-EC addresses this through a simple energy conservation heuristic such that whenever the residual energy of a node is lower than a threshold, the node does not participate in the protocol operation, i.e., it does not send a REQ packet if it does not have enough energy to transmit the REQ packet and receive a DATA packet. Since node participation is dependent on the residual energy, if a node has plenty of energy SPIN-EC behaves like SPIN-PP.

Another disadvantage of SPIN-PP is shown in Steps 5 and 6 from the above figure. Whenever there is more than one node that sends REQ packets, the DATA packet is sent to each node individually. Considering the broadcast nature of the wireless channel, this approach is a waste of resources since each neighbour of a node can receive the packet in each unicast.

Furthermore, SPIN-PP does not provide any mechanism to prevent collisions when multiple REQ packets are send. This is addressed through SPIN-BC, which is developed for broadcast

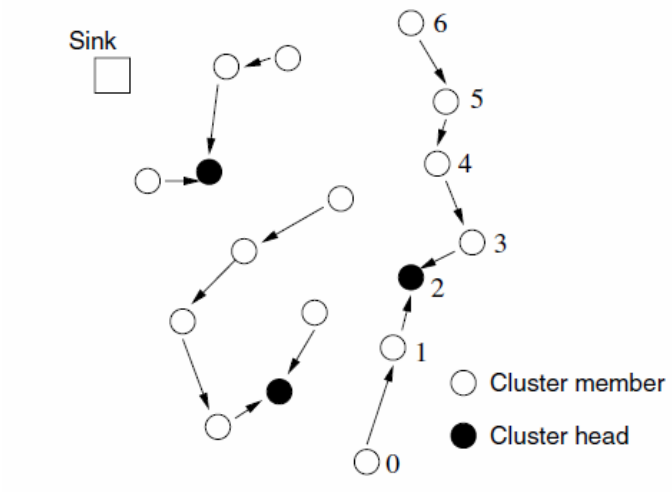
networks. In contrast to SPIN-PP, SPIN-BC introduces a randomized back off mechanism for the nodes before transmitting a REQ packet. As a result, if a node has an interest in a packet but hears a REQ packet related to that particular packet, it drops its REQ packet and waits for the DATA packet. Upon receiving a REQ packet, a transmitter node broadcasts a single DATA packet which can be received by all the interested neighbours. As a result, SPIN-BC decreases the energy consumption and overhead caused by multiple interested neighbours.

SPIN-RL provides a reliability mechanism to the SPIN-BC protocol such that if a node receives an ADV packet but does not receive a DATA packet followed by it (due to wireless channel errors),it requests the DATA packet from the neighbours that may have received the DATA packet. Moreover, SPIN-RL limits the retransmission period of the nodes such that they do not retransmit a DATA packet before a specified period.

Disadvantages:
1.The sending of data towards the sink node from the source node takes very long time.
2.If a node has more computation power then it will consume more energy as compared to other node in the network.
3.If a node is used many times then it will lose energy early then the other nodes in the network.
4.If a node is sitting idle then its energy will be reduced without transmission of data.

PEAGSIS PROTOCOL

The PEGASIS protocol aims to provide improvements to the LEACH protocol. PEGASIS aims to address the overhead caused by the cluster formation in LEACH by constructing chains of nodes instead of clusters. The chain construction is performed according to a greedy algorithm, where nodes select their closest neighbours as next hops in the chain. It is assumed that the nodes have a global knowledge of the network and the chain construction starts from the nodes that are farthest from the sink.



As a result of chain operation, instead of maintaining cluster formation and membership, each node only keeps track of its previous and next neighbour in the chain. Communication in the chain is performed sequentially such that each node within a chain aggregates data from its neighbour until all the data are aggregated at one of the sensor nodes, i.e., chain leader. The chain leader controls the communication order by passing a token among the nodes.
The chain leader in this example is node 2. Node 2 first passes the token to node 0 to initiate communication. Node 0 transmits its data to node 1, which aggregates these data with its own to create a packet of the same length. This packet is transmitted to node 2. Once node 2 receives the packet from node 1, it passes the token to the other end of the chain, i.e., node 6. Information from nodes 6, 5, 4, and 3 is also aggregated and sent to node 2 in the same

fashion. Upon receiving the aggregated information in the chain, node 2 uses a single hop communication to transmit the data to the sink.

Unit 5

UNIT V TRANSPORT AND APPLICATION LAYERS
9
TCP over Adhoc Networks – WAP – Architecture – WWW Programming Model – WDP – WTLS – WTP – WSP – WAE – WTA Architecture – WML – WML scripts.

TCP over Adhoc Network

The transmission control protocol (TCP) is the most predominant transport layer protocol in the Internet today. It transports more than 90% percent of the traffic on the Internet. Its reliability, end-to-end congestion control mechanism, byte-stream transport mechanism, and, above all, its elegant and simple design have not only contributed to the success of the Internet, but also have made TCP an influencing protocol in the design of many of the other protocols and applications. Its adaptability to the congestion in the network has been an important feature leading to graceful degradation of the services offered by the network at times of extreme congestion. TCP in its traditional form was designed and optimized only for wired networks. Extensions of TCP that provide improved performance across wired and single-hop wireless networks were discussed . Since TCP is widely used today and the efficient integration of an ad hoc wireless network with the Internet is paramount wherever possible, it is essential to have mechanisms that can improve TCP's performance in ad hoc wireless networks. This would enable the seamless operation of application-level protocols such as FTP, SMTP, and HTTP across the integrated ad hoc wireless networks and the Internet.

Problems with TCP
• TCP attributes packet losses to congestion.
• What does it do when it perceives a packet loss ?
• It goes back to the Slow Start Phase and restarts with one packet.
• This would result in a degradation of TCP throughput.
• Notice that packet losses could be due to fading/mobility.

Feedback-based TCP (TCP-F)

TCP-F requires the following to enhance performance:
• support of reliable data-link layer protocols;
• routing support to inform the TCP sender about path breaks;
• routing protocol is expected to repair the broken path within a reasonable time.
The aim of TCP-F: minimize the throughput degradation resulting from path breaks.

TCP with explicit link failure notification (TCP-ELFN)

According to TCP-ELFN an explicit link failure notification is used.

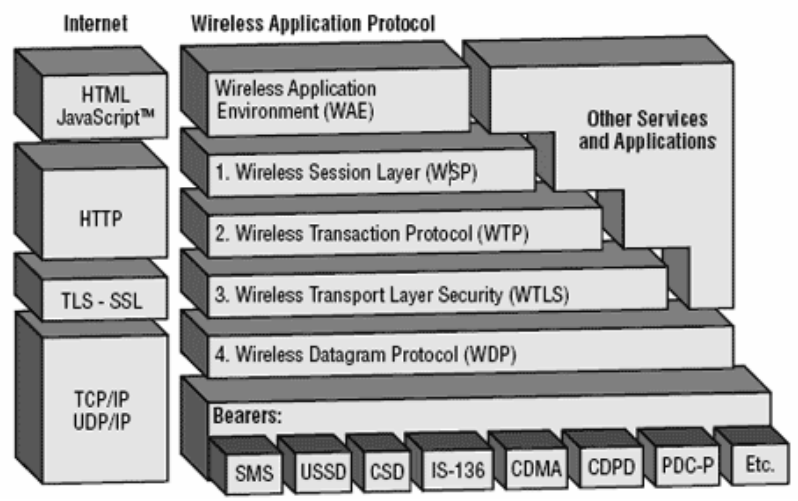
When an intermediate node detects a link failure:
• sends an explicit link failure notification (ELFN) to TCP-ELFN sender: – either sending an ICMP destination unreachable message (DUR); – or inserting info regarding link break in Route Error message of the routing protocol.

Once the TCP-ELFN sender receives the ELFN packet:

• it disables its retransmission timer and CW;
• enters a standby state.

Being in standby state the TCP-ELFN sender:
• periodically originates probe packets to see if a new route is established;
• when ACK for a probe packet is received TCP-ELFN continues to perform as usual.

WAP protocol architecture



Theory

Application Layer

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

Session Layer

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

Transaction Layer

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

Security Layer

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

Transport Layer

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

Each of these layers provides a well-defined interface to the layer above it. This means that the internal workings of any layer are transparent or invisible to the layers above it. The layered architecture allows other applications and services to utilise the features provided by

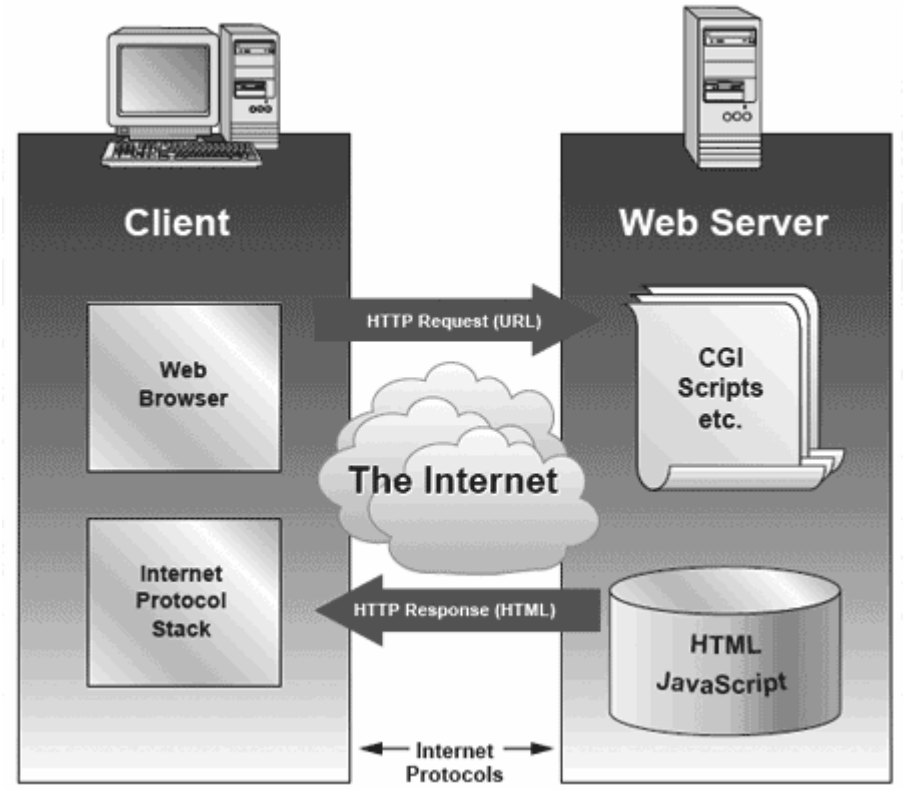
the WAP-stack as well. This makes it possible to use the WAP-stack for services and applications that currently are not specified by WAP.

WWW Programming model

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

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

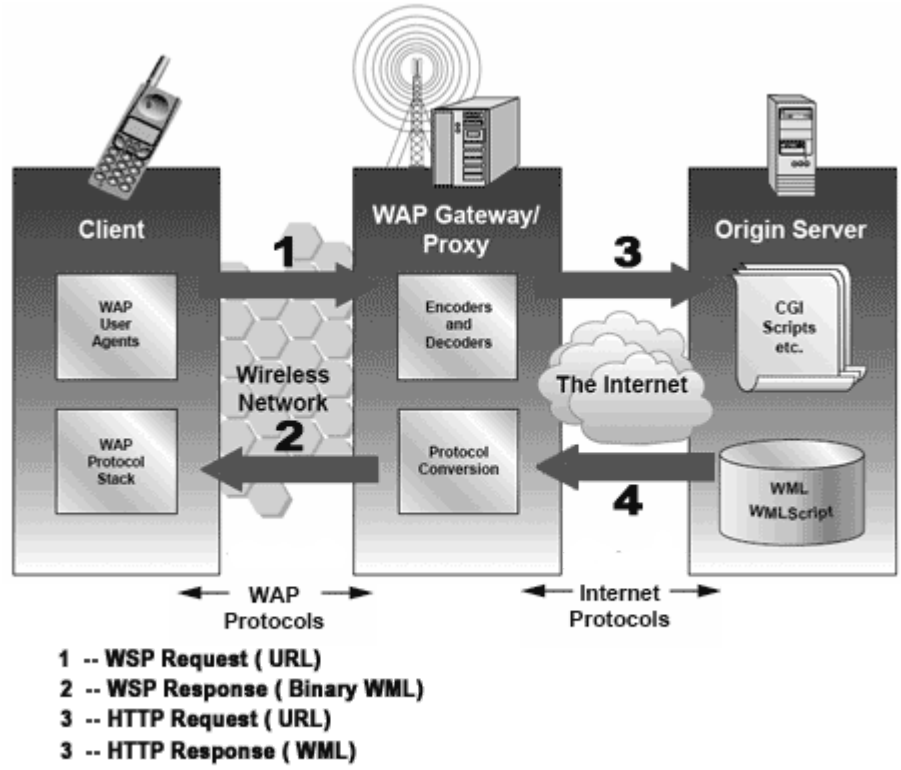
The figure below shows how a WWW client request a resource stored on a web server. On the Internet standard communication protocols, like HTTP and Transmission Control Protocol/Internet Protocol (TCP/IP) are used.



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

The WAP Model

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



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

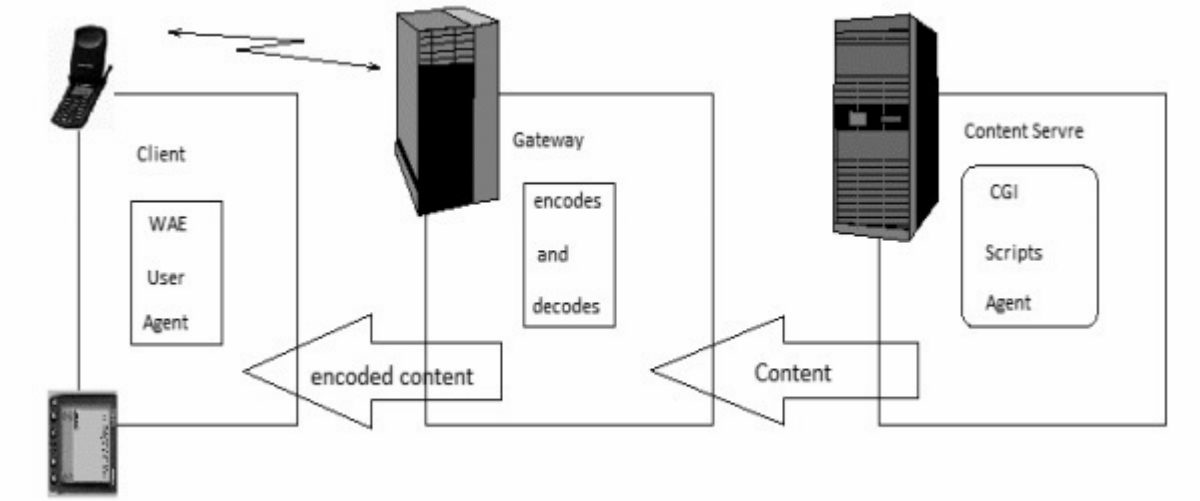
A **markup language** − the Wireless Markup Language (WML) has been adapted to develop optimized WAP applications. In order to save valuable bandwidth in the wireless network, WML can be encoded into a compact binary format. Encoding WML is one of the tasks performed by the WAP Gateway/Proxy.

How WAP Model Works?

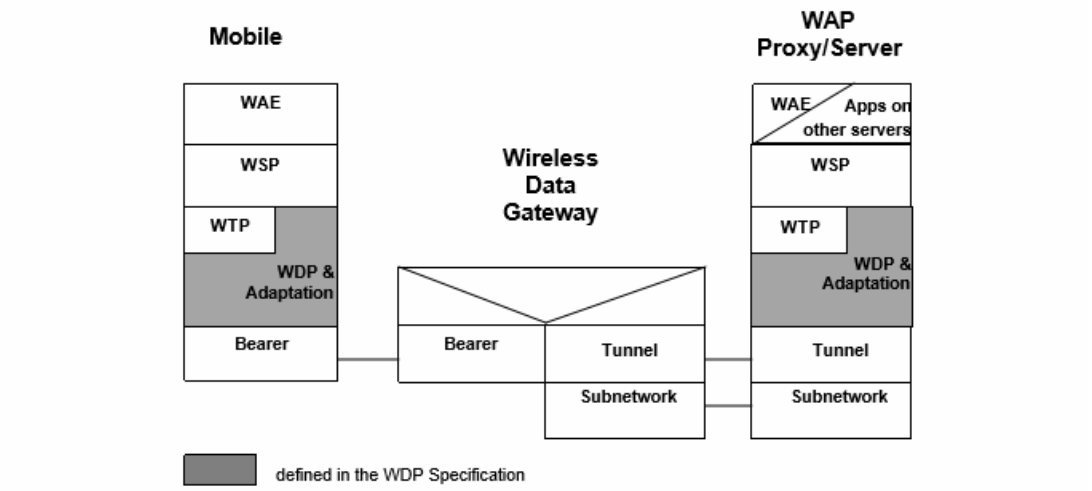
When it comes to actual use, WAP works as follows −

- The user selects an option on their mobile device that has a URL with Wireless Markup language (WML) content assigned to it.
- The phone sends the URL request via the phone network to a WAP gateway using the binary encoded WAP protocol.
- The gateway translates this WAP request into a conventional HTTP request for the specified URL and sends it on to the Internet.
- The appropriate Web server picks up the HTTP request.
- The server processes the request just as it would any other request. If the URL refers to a static WML file, the server delivers it. If a CGI script is requested, it is processed and the content returned as usual.
- The Web server adds the HTTP header to the WML content and returns it to the gateway.
- The WAP gateway compiles the WML into binary form.
- The gateway then sends the WML response back to the phone.
- The phone receives the WML via the WAP protocol.

- The micro-browser processes the WML and displays the content on the screen.



WDP



The WDP layer operates above the data capable bearer services supported by the various network types. As a general datagram service, WDP offers a consistent service to the upper layer protocol (Security, Transaction and Session) of WAP and communicate transparently over one of the available bearer services.

WDP supports several simultaneous communication instances from a higher layer over a single underlying WDP bearer service. The port number identifies the higher layer entity above WDP. This may be another protocol layer such as the Wireless Transaction Protocol (WTP) or the Wireless Session Protocol (WSP) or an application such as electronic mail. By reusing the elements of the underlying bearers, WDP can be implemented to support multiple bearers and yet be optimised for efficient operation within the limited resources of a mobile device.

At the Mobile the WDP protocol consists of the common WDP elements shown by the layer labelled WDP. The Adaptation Layer is the layer of the WDP protocol that maps the WDP protocol functions directly onto a specific bearer. The Adaptation Layer is different for each bearer and deals with the specific capabilities and characteristics of that bearer service. The Bearer Layer is the bearer service such as GSM SMS, or USSD, or ANSI-136 R-Data, or CDMA Packet Data. At the Gateway the Adaptation Layer terminates and passes the WDP packets on to a WAP Proxy/Server via a Tunnelling protocol, which is the interface between the Gateway that supports the bearer service and the WAP Proxy/Server. For example if the bearer were GSM SMS, the Gateway would be a GSM SMSC and would support a specific protocol (the Tunnelling protocol) to interface the SMSC to other servers. The SubNetwork

is any common networking technology that can be used to connect two communicating devices, examples are wide-area networks based on TCP/IP or X.25, or LANs operating TCP/IP over Ethernet. The WAP Proxy/Server may offer application content or may act as a gateway between the wireless WTP protocol suites and the wired Internet.

WSP (Wireless Session Protocol)

Goals

- HTTP 1.1 functionality
- Request/reply, content type negotiation, etc
- support of client/server, transactions, push technology
- key management, authentication, Internet security services
- session management (interruption, resume, etc)

WSP protocols

Types

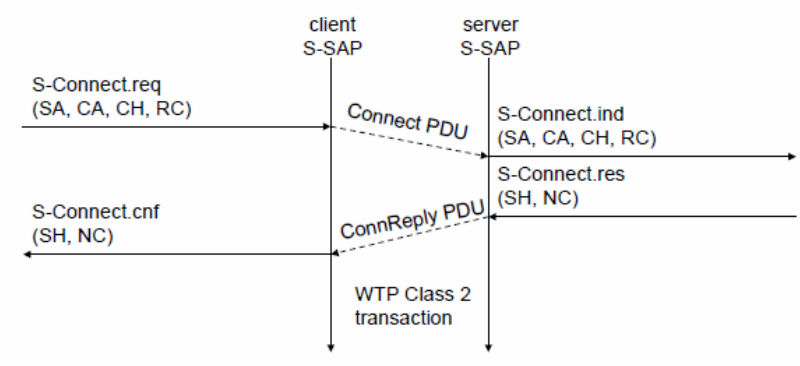
Connection mode (uses WTP)

- Session Management (class 0, 2)
- Method Invocation (class 2)
- Error Report
- Push (class 0)
- Confirmed Push (class 1)
- Session suspend/resume (class 0, 2)

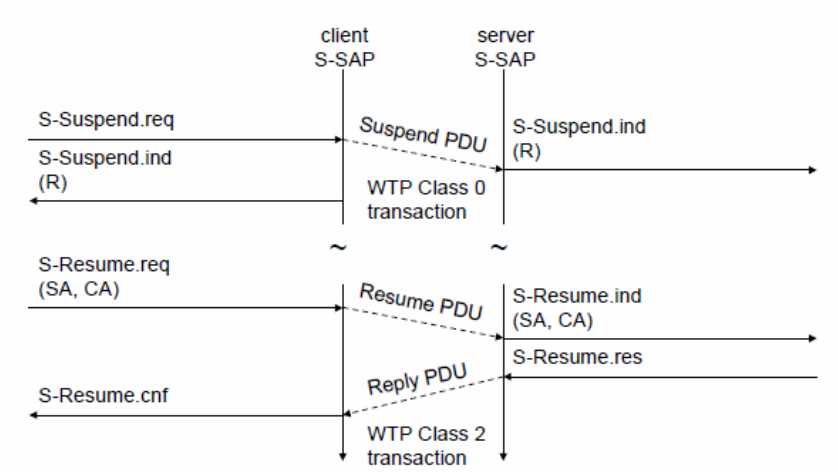
Connectionless mode (uses WDP or WTLS)

- Method Invocation
- Push (in general unreliable)

WSP/B session establishment



WSP/B session suspend/resume



WAE (Wireless Application Environment)

Goals

1. Network independent application environment for low-bandwidth,wireless devices
2. Integrated Internet/WWW programming model with high interoperability

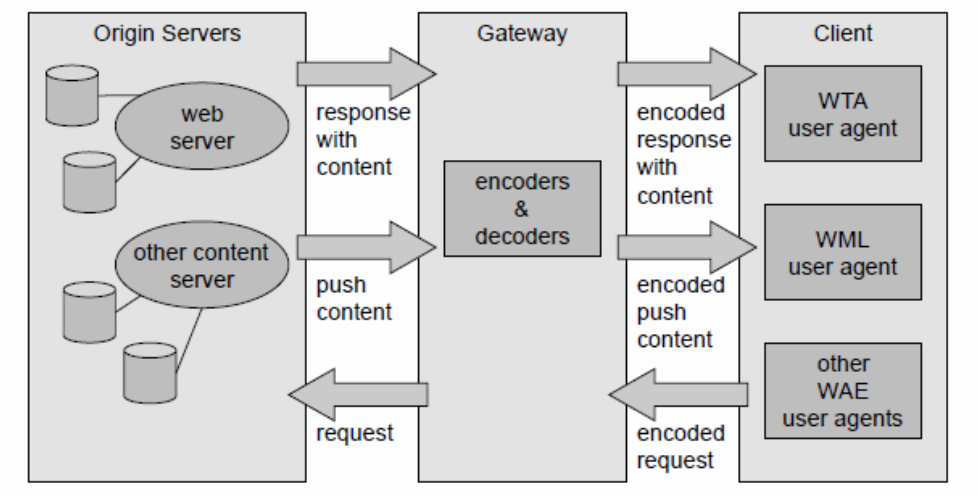
Requirements

1. device and network independent, international support
2. manufacturers can determine look-and-feel, user interface
3. considerations of slow links, limited memory, low computing power,
4. small display, simple user interface (compared to desktop computers)

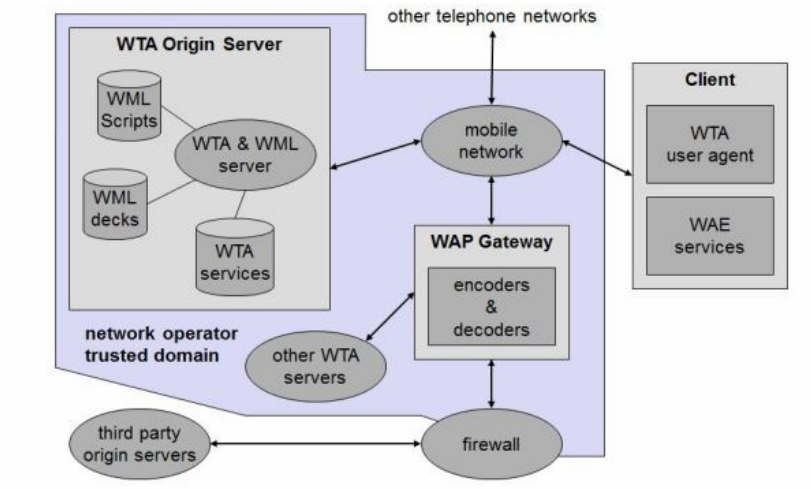
Components

1. architecture: application model, browser, gateway, server
2. WML: XML-Syntax, …
3. WMLScript: procedural, loops, conditions, ... (similar to JavaScript)
4. WTA: telephone services, such as call control, text messages, phonebook, ... (accessible from WML/WMLScript)
5. content formats: vCard, vCalendar, Wireless Bitmap, WML, ...

WAE logical model

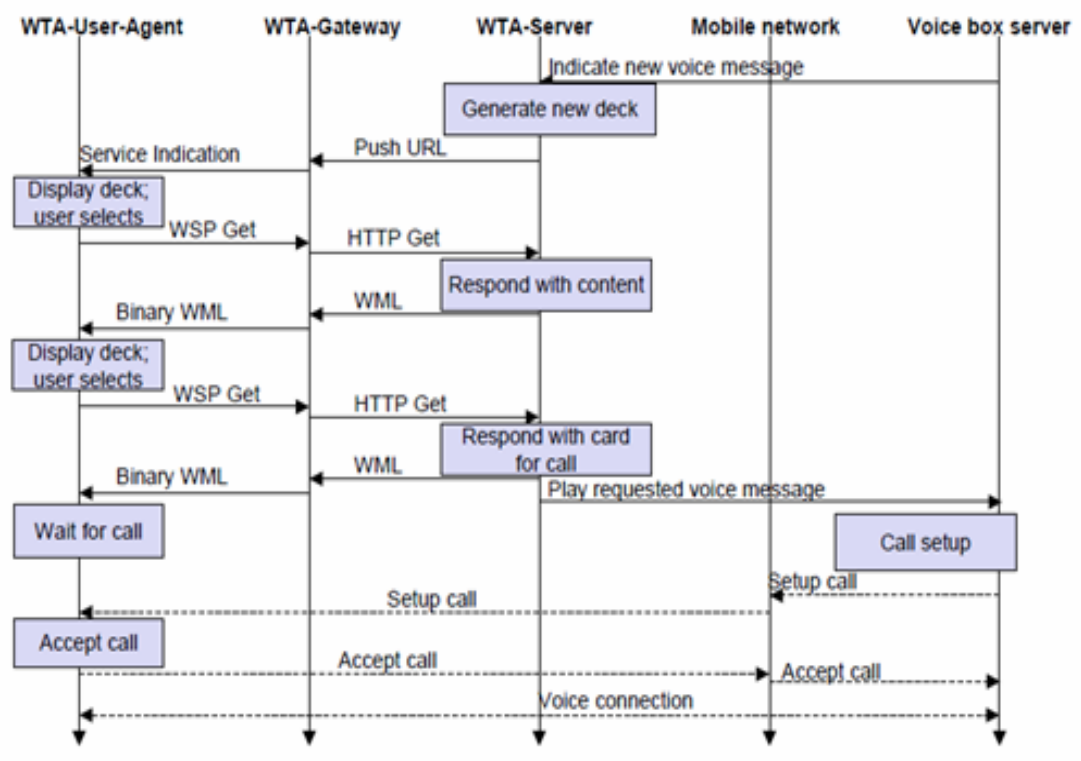


WTA logical architecture



Theory

- ✓ Stands for Wireless Telephony Application
- ✓ WTA is a collection of telephony specific extensions for call and feature control mechanisms, merging data networks and voice networks.
- ✓ It is an Extension of basic WAE application model with following features
    - network model for interaction
        - client requests to server
        - event signalling: server can push content to the client
    - event handling
        - table indicating how to react on certain events from the network
        - client may now be able to handle unknown events
    - telephony functions
        - some application on the client may access telephony functions
    - Example
        - calling a number (WML)
            - wtai://wp/mc;07216086415
        - calling a number (WMLScript)
            - WTAPublic.makeCall("07216086415");
- ✓ WTA voice box example with definition

- 

✓ Push/Pull services in WAP I

- Service Indication
  - Service announcement using a pushed short message
  - Service usage via a pull
  - Service identification via a URI

```
<?xml version="1.0"?>
  <!DOCTYPE si PUBLIC "-//WAPFORUM//DTD SI 1.0//EN"
    "http://www.wapforum.org/DTD/si.dtd">
<si>
  <indication href="http://www.piiiizza4u.de/offer/salad.wml"
     created="2000-02-29T17:45:32Z"
     si-expires="2000-02-29T17:50:31Z">
     Salad special: The 5 minute offer
  </indication>
</si>
```

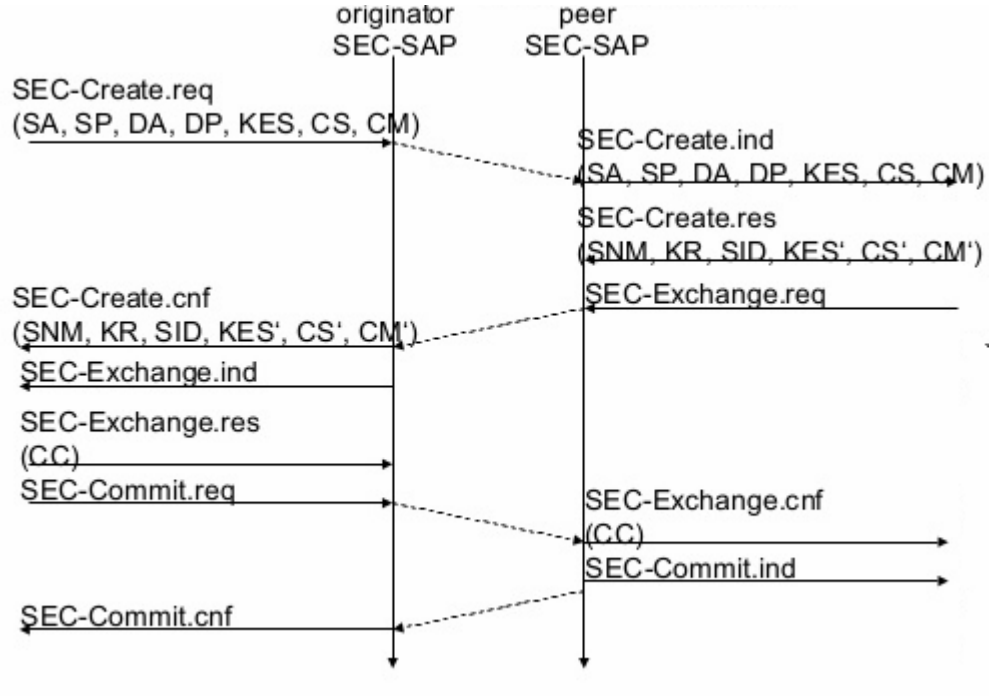
Wireless Transport Layer Security (WTLS)

Goals

- data integrity
  - prevention of changes in data.
- privacy
  - prevention of tapping.
- authentication
  - creation of authenticated relations between a mobile device and a server.
- protection against denial-of-service attacks
  - protection against repetition of data and unverified data.

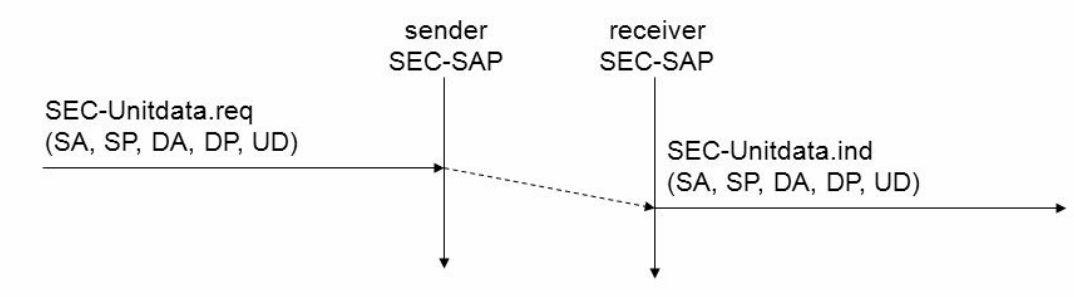
✓ WTLS

- is based on the TLS (Transport Layer Security) protocol (former SSL, Secure Sockets Layer)
- optimized for low-bandwidth communication channels.
- WTLS establishing a secure session



- This session establishment consists of several steps
- The first step is to initiate the session with the SEC-Create primitive.
- Parameters are source address (SA), source port (SP) of the originator, destination address (DA), destination port (DP) of the peer.
- The originator proposes a key exchange suite (KES) (e.g., RSA, DH, ECC, a cipher suite (CS) (e.g., DES, IDEA, and a compression method (CM) (currently not further specified).
- The peer answers with parameters for the sequence number mode (SNM), the key refresh cycle (KR) (i.e., how often keys are refreshed within this secure session), the session identifier (SID) (which is unique with each peer), and the selected key exchange suite (KES‘), cipher suite (CS‘), compression method (CM‘).
- The peer also issues a SEC-Exchange primitive. This indicates that the peer wishes to perform public-key authentication with the client, i.e., the peer requests a client certificate (CC) from the originator.

✓ **WTLS datagram transfer**



- After setting up a secure connection between two peers, user data can be exchanged. This is done using the simple SEC-Unit data primitive as shown in figure.
- SEC-Unit transfers a datagram between a sender and a receiver.
- The parameters are: source address (SA), source port (SP), destination address (DA), destination port (DP), and user data (UD).

Key features of WML

- ✓ Text and images
  - Hints how text and images are presented to a user.
  - Provides set of mark-up elements (bold, italic, etc.,) and tab columns for tabbing alignment.
- ✓ User Interaction
  - Provides text entry column for text and password entry.
  - Option selection or control for task invocation
- ✓ Navigation
  - Navigation through browsing history with HTML browser
  - Hyperlinks
- ✓ Context management
  - Saving the state between different decks without server interaction.

WML Scripts

- ✓ WML stands for Wireless Markup Language. It is a mark-up language inherited from HTML, but WML is based on XML, so it is much stricter than HTML.WML is used to create pages that can be displayed in a WAP browser. Pages in WML are called DECKS. Decks are constructed as a set of CARDS. WMLScript is the scripting language used in WML pages.
  Key features of WML
  - used to generate message boxes and dialog boxes locally, to view error messages and confirmations faster
  - used to access facilities of the user agent
  - used to validate user input
  - used for the extension of device software
  - It is the scripting language used in WML pages
  - Light version of the JavaScript language
  - Only contains references to script URLs
  - Is compiled into byte code on the server before it is sent to the WAP browser
  - Part of the WAP specification
- ✓ WML script example program
- ✓ WML libraries
  - The are six standard libraries totally.
    - Lang − The Lang library provides functions related to the WMLScript language core.

    - Example Function − abs(),abort(), characterSet(),float(), isFloat(), isInt(), max(), isMax(), min(), minInt(), maxInt(), parseFloat(), parseInt(), random(), seed()
- Float − The Float library contains functions that help us perform floating-point arithmetic operations.
    - Example Function − sqrt(), round(), pow(), ceil(), floor(), int(), maxFloat(), minFloat()
- String − The String library provides a number of functions that help us manipulate strings.
    - Example Function − length(), charAt(), find(), replace(), trim(), compare(), format(), isEmpty(), squeeze(), toString(), elementAt(), elements(), insertAt(), removeAt(), replaceAt()
- URL − The URL library contains functions that help us manipulate URLs.
    - Example Function − getPath(), getReferer(), getHost(), getBase(), escapeString(), isValid(), loadString(), resolve(), unescapeString(), getFragment()
- WMLBrowser − The WMLBrowser library provides a group of functions to control the WML browser or to get information from it.
    - Example Function − go(), prev(), next(), getCurrentCard(), refresh(), getVar(), setVar()
- Dialogs − The Dialogs library Contains the user interface functions.
    - Example Function − prompt(), confirm(), alert().