B.Tech 7th Semester Examination May 2014

Mobile Communication

Paper:ECE-419-F

Time: 3 Hours MM: 100

Note: Questio no. 1 is compulsory. Attempt one question from each section.

1. (a) What is multiplexing. Explain briefly. 4
   (b) What is coherence time? 4
   (c) Explain free space path loss 4
   (d) What do you mean by IEEE standards 4
   (e) What do you understand by optimization 4

UNIT-1

2. (a) Explain various types of antennas required for a mobile radio system. 10
   (b) What is modulation. Explain various types of modulation techniques briefly. 10

3. (a) Explain multipath characteristics of radio waves. 10

   (b)

UNIT=-2

4. Explain Okumara and Hata model in detail 20
5. Write short notes on: 20
   (a) Microcell Model
   (b) PCS Model

UNIT-3

6. (a) What is GSM. Explain the architecture of GSM. 10
   b) Compare various data networks standards like GPRS, IS-95, and WCDMA. 10
7. (a) Explain HyperLAN in detail 10
   (b) Explain Bluetooth. 10

UNIT-4

8. (a) What is performance enhancing proxies? Explain 10
   (b) What is reverse Tunnelling? Explain 10
9. Write short Note on: 20

SOLUTION:

B.Tech 7th Semester Examination May 2014

Mobile Communication

Paper:ECE-419-F

Time: 3 Hours MM: 100

Note: Questio no. 1 is compulsory. Attempt one question from each section.

1. (a) What is multiplexing. Explain briefly. 4

Multiplexing describes how several users can share a medium with minimum or no interference Different types of multiplexing are: For wireless communication, multiplexing can be carried out in four dimensions: space, time, frequency, and code. In this field, the task of multiplexing is to assign space, time, frequency, and code to each communication channel with a minimum of interference and a maximum of medium utilization. Accordingly, multiplexing are of the following types:

Space division multiplexing (SDM): The channels can be mapped onto the three 'spaces' s1 to s3 which clearly separate the channels and prevent the interference ranges from overlapping.

Frequency division multiplexing (FDM): Each channel is provided at different frequency with space guards to prevent interference.

Time division multiplexing (TDM): in this scheme channels gain access at different instants but with full bandwidth.

Code division multiplexing (CDM): Separation is now achieved by assigning each channel its own 'code', guard spaces are realized by using codes with the necessary 'distance' in code space, e.g., orthogonal codes.

(b) What is coherence time? 4

Coherence time T_c is the time domain dual of Doppler spread and is used to characterize the time varying nature of the frequency dispersiveness of the channel in the time domain. The Doppler spread and coherence time are inversely proportional to one another. That is,

$$Tc = \frac{1}{f_m} \qquad (a)$$

Coherence time is actually a statistical measure of the time duration over which the channel impulse response is essentially invariant, and quantifies the similarity of the channel response at different times. In other words, coherence time is the time duration over which two received signals have a strong potential for amplitude correlation. If the reciprocal bandwidth of the baseband signal is greater than the coherence time of the channel, then the channel will change during the transmission of the baseband message, thus causing distortion at the receiver.

(c) Explain free space path loss 4

The free space path loss, also known as FSPL is the loss in signal strength that occurs when an electromagnetic wave travels over a line of sight path in free space. In these circumstances there are no obstacles that might cause the signal to be reflected refracted, or that might cause additional attenuation.

The free space path loss calculations only look at the loss of the path itself and do not contain any factors relating to the transmitter power, antenna gains or the receiver sensitivity levels which are required when calculating a link budget and these will also be used within radio and wireless survey tools and software.

To understand the reasons for the free space path loss, it is possible to imagine a signal spreading out from a transmitter. It will move away from the source spreading out in the form of a sphere. As it does so, the surface area of the sphere increases. As this will follow the law of the conservation of energy, as the surface area of the sphere increases, so the intensity of the signal must decrease.

As a result of this it is found that the signal decreases in a way that is inversely proportional to the square of the distance from the source of the radio signal in free space.

$$\text{Signal} = \frac{1}{Distance\ ^2}$$

Whilst the free space path loss is taken to be inversely proportional to the square of the distance, in most terrestrial (non-free space) cases this basic formula has to be altered because of the effects of the earth and obstacles including trees, hills, buildings, etc..

(d) What do you mean by IEEE standards 4

IEEE stands for Institute of Electrical and Electronic Engineers. IEEE primarily innovates new electronic products and services, designs the standards that govern them and imparts, publishes and promotes industry knowledge through publications, conferences and partnering with academic institutes. The prime areas of focus for IEEE are electrical, electronics, computer engineering, computer science, information technology and most of their related disciplines.

IEEE in computing is widely popular for the development of standards for computer networking and its suite of services. IEEE develops many different standards, such as IEEE 802 and IEEE 802.11 (commonly known as Wi-Fi), and provides ongoing innovation, amendments and maintenance services for these standards. Some of the IEEE standards are given below:

- 802.1: Bridging & Management
- 802.2: Logical Link Control
- 802.3: Ethernet
- 802.11: Wireless LANs
  - ***802.11a*** - Wireless network bearer operating in the 5 GHz ISM band with data rate up to 54 Mbps.
  - ***802.11b*** - Wireless network bearer operating in the 2.4 GHz ISM band with data rates up to 11 Mbps. ***802.11e*** - Quality of service and prioritisation

- ***802.11f*** - Handover
- ***802.11g*** - Wireless network bearer operating in 2.4 GHz ISM band with data rates up to 54 Mbps.
- ***802.11h*** - Power control
- ***802.11i*** - Authentication and encryption
- ***802.11j*** - Interworking
- ***802.11k*** - Measurement reporting
- ***802.11n*** - Wireless network bearer operating in the 2.4 and 5 GHz ISM bands with data rates up to 600 Mbps.
- ***802.11s*** - Mesh networking
- ***802.11ac*** - Wireless network bearer operating below 6GHz to provide data rates of at least 1Gbps per second for multi-station operation and 500 Mbps on a single link.
- ***802.11ad*** - Wireless network bearer providing very high throughput at frequencies up to 60GHz.
- ***802.11af*** - Wi-Fi in TV spectrum white spaces (often called White-Fi).
- ***802.11ah*** - Wi-Fi using unlicensed spectrum below 1 GHz to provide long range communications and support for the Internet of Everything.
- 802.15: Wireless PANs
- 802.16: Broadband Wireless MANs
- 802.17: Resilient Packet Rings
- 802.19: TV White Space Coexistence Methods
- 802.20: Mobile Broadband Wireless Access

(e) What do you understand by optimization 4

With the basic mobile IP protocol all packets to the MN have to go throughthe HA. This can cause unnecessary overheads for the network between CN and HA, but also between HA and COA, depending on the current location of the MN. As the example shows, latency can increase dramatically. This is particularly unfortunate if the MNs and HAs are separated by, e.g., transatlantic links.

One way to optimize the route is to inform the CN of the current location of the MN. The CN can learn the location by caching it in a **binding cache** which is a part of the local routing table for the CN. The appropriate entity to inform the CN of the location is the HA. The optimized mobile IP protocol needs four additional messages.

● **Binding request:** Any node that wants to know the current location of an MN can send a binding request to the HA. The HA can check if the MN has allowed dissemination of its current location. If the HA is allowed to reveal the location it sends back a binding update.

● **Binding update:** This message sent by the HA to CNs reveals the current location of an MN. The message contains the fixed IP address of the MN and the COA. The binding update can request an acknowledgement.

● **Binding acknowledgement:** If requested, a node returns this acknowledgement after receiving a binding update message.

● **Binding warning:** If a node decapsulates a packet for an MN, but it is not the current FA for this MN, this node sends a binding warning. The warning contains MN's home address and a target node address, i.e., the address of the node that has tried to send the packet to this MN. The recipient of the warning then knows that the target node could benefit from obtaining a fresh binding for the MN. The recipient can be the HA, so the HA should now send a binding update to the node that obviously has a wrong COA for the MN.

UNIT-1

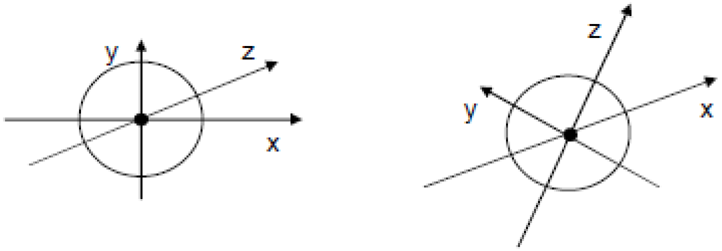
2. (a) Explain various types of antennas required for a mobile radio system. 10

The antennas are used for Radiation and reception of electromagnetic waves, coupling of wires to space for radio transmission. The following types of antennas are used in mobile communication

• Isotropic radiator: equal radiation in all directions (three dimensional) - only a theoretical reference antenna

• Real antennas always have directive effects (vertically and/or horizontally)

• Radiation pattern: measurement of radiation around an antenna

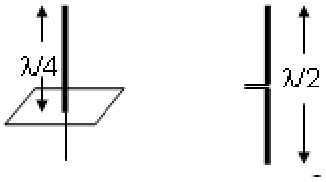


Ideal isotropic radiator

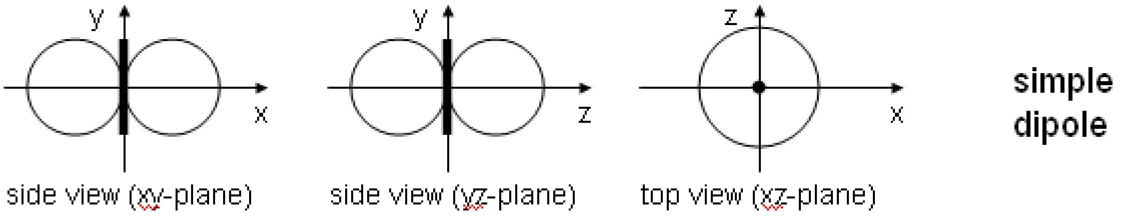
Antennas: simple dipoles

• Real antennas are not isotropic radiators but, e.g., dipoles with lengths /4 on car roofs or /2 as Hertzian dipole

shape of antenna proportional to wavelength

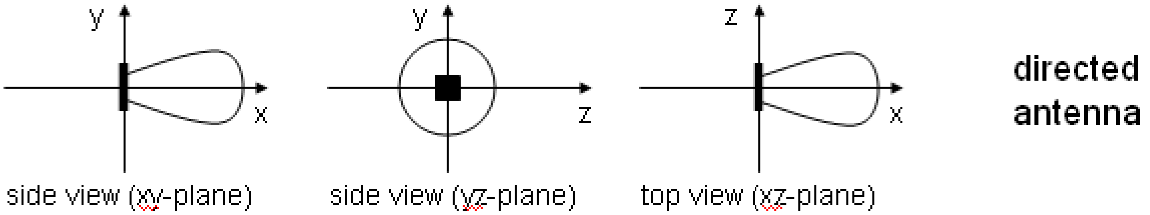


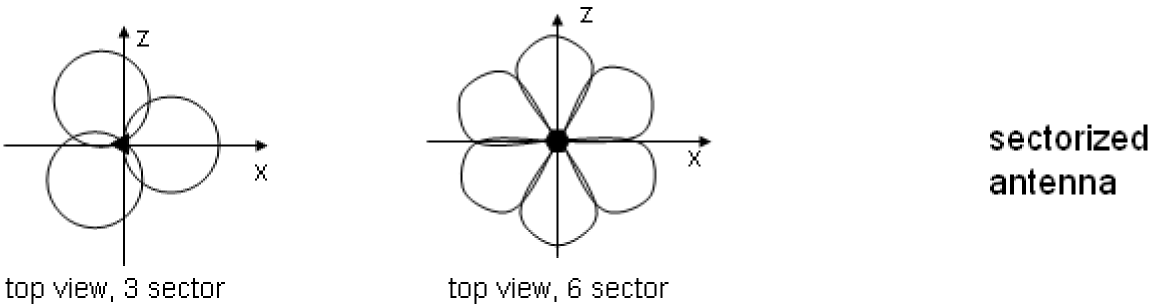
Example: Radiation pattern of a simple Hertzian dipole



Gain: maximum power in the direction of the main lobe compared to the power of an isotropic radiator (with the same average power)

• Often used for microwave connections or base stations for mobile phones (e.g., radio coverage of a valley)





(b) What is modulation. Explain various types of modulation techniques briefly. 10

Modulation is the process by which some characteristics of the carrier are varied in accordance with modulating wave. The three characteristics of the carrier are amplitude, frequency and phase. So one of these are varied in proportion with the modulating signal. The message signal is referred as modulating signal and the modified signal is the modulated signal. It is important to note that the information is contained in the varied characteristics of the carrier and not in the carrier itself.

Advantage of Modulation:

Modulation is used to overcome the limitation of base band transmission. In the process of modulation, the base band signal is shifted from low frequency to high frequency spectrum. It has the following advantages:

i. Reduction in height of antenna (antenna height=λ/4)

ii. Avoids mixing of signals

iii. Improves quality of signal

iv. Increases range of communication

The most fundamental digital modulation techniques are based on keying:

- PSK (phase-shift keying): a finite number of phases are used.
- FSK (frequency-shift keying): a finite number of frequencies are used.
- ASK (amplitude-shift keying): a finite number of amplitudes are used.
- QAM (quadrature amplitude modulation): a finite number of at least two phases and at least two amplitudes are used.

i. **Amplitude Shift Keying (ASK): It is** the most simple digital modulation scheme. The two binary values, 1 and 0, are represented by two different amplitudes. In the example, one of the amplitudes is 0 (representing the binary 0). This simple scheme only requires low bandwidth, but is very susceptible to interference. Effects like multi-path propagation, noise, or path loss heavily influence the amplitude. In a wireless environment, a constant amplitude cannot be guaranteed, so ASK is typically not used for wireless radio transmission. However, the wired transmission scheme with the highest performance,

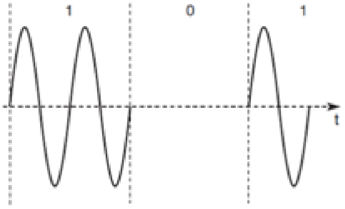


Figure 2B-i: ASK

Frequency Shift Key (FSK): The simplest form of FSK, also called binary FSK (BFSK), assigns one frequency f1 to the binary 1 and another frequency f2 to the binary 0. A very simple way to implement FSK is to switch between two oscillators, one with the frequency f1 and the other with f2, depending on the input. To avoid sudden changes in phase, special frequency modulators with continuous phase modulation, (CPM) can be used.

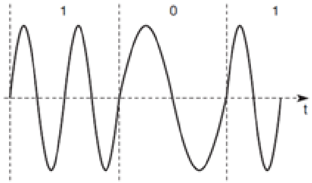


Figure : 2B-ii FSK

Phase Shift Keying (PSK): PSK uses shifts in the phase of a signal to represent data. Figure 2.25 shows a phase shift of 180° or π as the 0 follows the 1 (the same happens as the 1 follows the 0). This simple scheme, shifting the phase by 180° each time the value of data changes, is also called binary PSK (BPSK). A simple implementation of a BPSK modulator could multiply a frequency f with +1 if the binary data is 1 and with –1 if the binary data is 0.

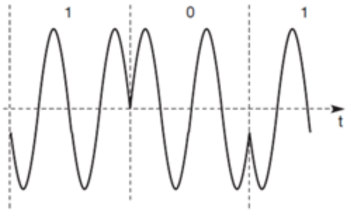
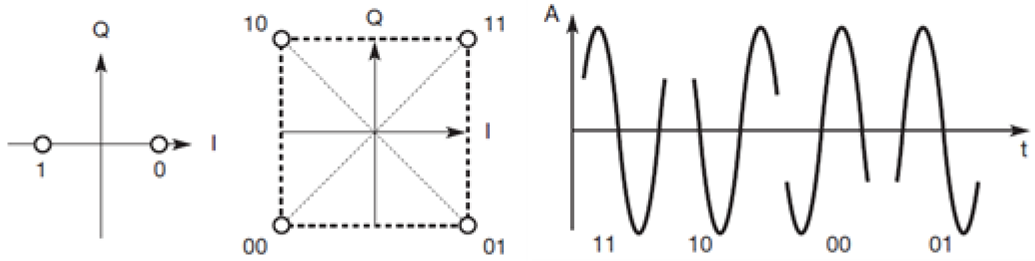


Figure 2B-iii: PSK

Quadrature PSK (QPSK): The basic BPSK scheme only uses one possible phase shift of 180°. Figure 2B-iv (a) shows BPSK in the phase domain. Figure (b) shows quadrature PSK (QPSK), one of the most common PSK schemes. Here, higher bit rates can be achieved for the same bandwidth by coding two bits into one phase shift. Alternatively, one can reduce the bandwidth and still achieve the same bit rates as for BPSK. QPSK can be realized in two variants. The phase shift can always be relative to a **reference signal** (with the same frequency). If this scheme is used, a phase shift of 0 means that the signal is in phase with the reference signal. A QPSK signal will then exhibit a phase shift of 45° for the data 11, 135° for 10, 225° for 00, and 315° for 01 with all phase shifts being relative to the reference signal. The transmitter 'selects' parts of the signal as shown in Figure (c) and concatenates them. To reconstruct data, the receiver has to compare the incoming signal with the reference signal. One problem of this scheme involves producing a reference signal at the receiver. Transmitter and receiver have to be synchronized very often.

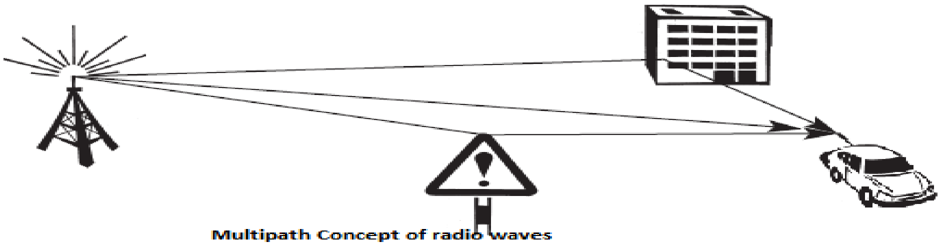


(a) BPSK in phase domain (b) QPSK (c) QPSK in time domain

Figure: 2B-iv: QPSK

3. **(a) Explain multipath characteristics of radio waves.** 10

One of the multipath characteristic of the radio wave is fading, which is the distortion that a carrier modulated signal experiences over certain propagation media. In wireless fading is due to multipath propagation and is sometimes referred to as multipath induced fading.



Multipath Concept of radio waves

In wireless communication, the presence of reflectors in the environment surrounding a transmitter and receiver create multiple paths that a transmitted signal can traverse. Radio waves emitted by the sender can either travel along a straight line, or they may be reflected at a large building, or scattered at smaller obstacles. This simplified figure only shows three possible paths for the signal. In reality, many more paths are possible. As a result, the receiver sees the superposition of multiple copies of the transmitted signal, each traversing a different path.
Each signal copy will experiences differences in attenuation, delay and phase shift while travelling from the transmitter to receiver. This can result in either constructive or destructive interference, amplifying or attenuating the signal power seen at the receiver.

Strong destructive interference is frequently referred to as deep fade and may result in temporary failure of communication due to severe drop in the channel signal-to-noise ration.

delay spread : Due to the finite speed of light, signals travelling along different paths with different lengths arrive at the receiver at different times. This effect (caused by multi-path propagation) is called **delay spread**: the original signal is spread due to different delays of parts of the signal.

interference (ISI): As seen in figure that there are multipath, On the sender side, both impulses are separated. At the receiver, both impulses interfere, i.e., they overlap in time. Now consider that each impulse should represent a symbol, and that one or several symbols could represent a bit. The energy intended for one symbol now spills over to the adjacent symbol, an effect which is called **intersymbol interference (ISI)**. The higher the symbol rate to be transmitted, the worse the effects of ISI will be, as the original symbols are moved closer and closer to each other. ISI limits the bandwidth of a radio channel with multi-path propagation (which is the standard case). Due to this interference, the signals of different symbols can cancel each other out leading to misinterpretations at the receiver and causing transmission errors.

(b)

UNIT=2

4. Explain Okumara and Hata model in detail **20**

SOLUTION

1. Okumara Model:

Okumura's model is a graphical model and is one of the most frequently and easiest to use macroscopic propagation models. It was developed during the mid 1960's as the result of large-scale studies conducted in and around Tokyo. The model was designed for use in the frequency range 200 up to 1920 MHz and mostly in an urban propagation environment.

Okumura's model assumes that the path loss between the TX and RX in the terrestrial propagation environment can be expressed as:

$L_{50} = L_{FS} + A_{mu} + H_{tu} + H_{ru}$

where:

L_{50} - Median path loss between the TX and RX expressed in dB

L_{FS} - Path loss of the free space in dB

A_{mu} - "Basic median attenuation" – additional losses due to propagation in urban environment in dB

H_{tu} - TX height gain correction factor in dB

H_{xu} - RX height gain correction factor in dB

The free space loss term can be calculated analytically using:

$L_{FS} = 32.45 + 20 \log (\frac{d}{1\ km}) + 20 \log (\frac{f}{1\ MHz}) – 10\log(G\ t)$ - 10log(G r)

where:

d - Distance between the TX and RX in km

f - Operating frequency in MHz

G_t, G_r - TX and RX antenna gains (linear)

The remaining terms on the right hand side of eqn for L_{50} above are provided in a graphical form as the

family of curves such as Basic median attenuation as a function of frequency and path distance, Base station height correction gain and Mobile station height correction gain graphs.

2. Hata –Okumara Model : Hata model is an empirical formulation of the graphical path loss data provided by Okumara and is valid from 150 MHz to 1500 MHz. Hatapresented the urban area propagation loss as a standard formula and supplied correction equation for application to other situations.

a. Urban area

L50(urban)= 69.55+26.16log fc-13.82log hte - a(hre) + (44.9 - 6.55log hte)log d

L50 – median path loss with dB;
fc=150-1500 MHz -frequency range;
hte=30-200m-base station antenna height;
d=1-20km distance from BS

a(hre) is the correction factor for mobile antenna height which is a function of the size of the coverage area.

For a small or medium-sized le antenna correction factor is :

a(hre)=(1.1fc - 0.7)hm - (1.56 log fc-0.8) dB;
hre=1-10 m-mobile antenna height
for a large city, a(hre)is given by:
a(hre) = 8.29(log 1.54 hre)^2 – 1.1 dB for fc <= 300 MHz
a(hre) = 3.2(log 11.75 hre)2 -4.97 dB for fc >= 300MHz

To obtain the path loss in suburban area, the standard Hata Formula L50(Urban) given above is modified as:

Suburban area L50= L50(urban) - 2[log (fc/28)2-5.4] dB

b. Open area

L_{50}= L_{50}(urban)-4.78log (fc)2+18.33log fc-40.94] dB

5. **Write short notes on: 20**

a. Microcell Model

Work of Feuerstein used a 20 MHz pulsed transmitter at 1900 MHz to measure path loss, outage, and delay spread in typical microcellular systems in San Fransico and Oakland. Using base station antenna heights of 3.7m, 8.5m, and 13.3 m, and a mobile receiver with an antenna height of 1.7 m above ground, statistics for path loss, multipath, and coverage area were developed from extensive measurements in line-of-sight and obstructed environment. This work revealed that a two-ray ground reflection model is a good estimate for path loss in line-of-sight microcells, and a simple log-distance path loss model holds well for obstructed environments.

For flat earth ground reflection model, the distance df at which the first Fresnel zone just becomes obstructed by the ground (first Fresnel zone clearance) is given by:

$$df = \frac{1}{\lambda}\sqrt{[\,(\Sigma^2 - \Delta^2)^2 - 2\,(\Sigma^2 + \Delta^2)\,(\tfrac{\lambda}{2})^2 + (\tfrac{\lambda}{2})^4]}$$

$$= \frac{1}{\lambda}\sqrt{[\,16ht^2\,hr^2 - \lambda^2\,(ht^2 + hr^2)\frac{\lambda^4}{16}\,]}$$

For LOS cases, a double regression path loss model that uses a regression breakpoint at the first Fresnel zone clearance was shown to fit well to measurements. The model assumes omni-directional vertical antennas and predicts average path loss as:

$$(\overline{\mathrm{PL}}\,(\mathrm{d}) = \begin{matrix} 10\,\mathrm{n1}\log(d) + p1 & for\ 1 < d < df \\ 10\mathrm{n2}\log\left(\frac{\mathrm{d}}{\mathrm{df}}\right) + 10\mathrm{n1}\log(\mathrm{df}) + \mathrm{p1} & \text{for } \mathrm{d} > df \end{matrix}$$

Where p1 = $\overline{\mathrm{PL}}\,(\mathrm{d0})$ (the path loss in decibels at the reference distance of d0=1m), d is in meters and n1,n2 are path loss exponents which are a function of transmitter height.

b. PCS Model

The Europian cooperative for scientific and Technical research formed the working committee named COST-231 to develop an extended version of the HATA Model. COST-231 committee proposed the following formula to extend Hata's model to 2GHz.

The Hata Model is extended to the following range:

f	:	1500MHz to 2000 MHz
hte	:	30 m to 200m
hre	:	1 m to 10m
d	:	1 km to 20 km

The proposed model for path loss is:

$L_{50}(\text{urban}) = 46.3 + 33.9 \log f_c - 13.82 \log h_{te} - a(h_{re}) + (44.9 - 6.55 \log h_{tu}) \log d + C_M$

Where $a(h_{re})$ is defined as:

a(hre)=(1.1fc - 0.7)hm - (1.56 log fc-0.8) dB;

hre=1-10 m-mobile antenna height

for a large city, a(hre)is given by:

$a(hre) = 8.29(\log 1.54\, hre)^2 - 1.1$ dB for fc <= 300 MHz

a(hre) = 3.2(log 11.75 hre)2 -4.97 dB for fc >= 300MHz

and

$$C_M = \begin{matrix} 0 \text{ dB for medium sized city and suburban area} \\ 3\ dB\ for\ metropolitan\ centers \end{matrix}$$

UNIT-3

6. (a) What is GSM. Explain the architecture of GSM. **10**

SOLUTION:

System Architecture of GSM System:

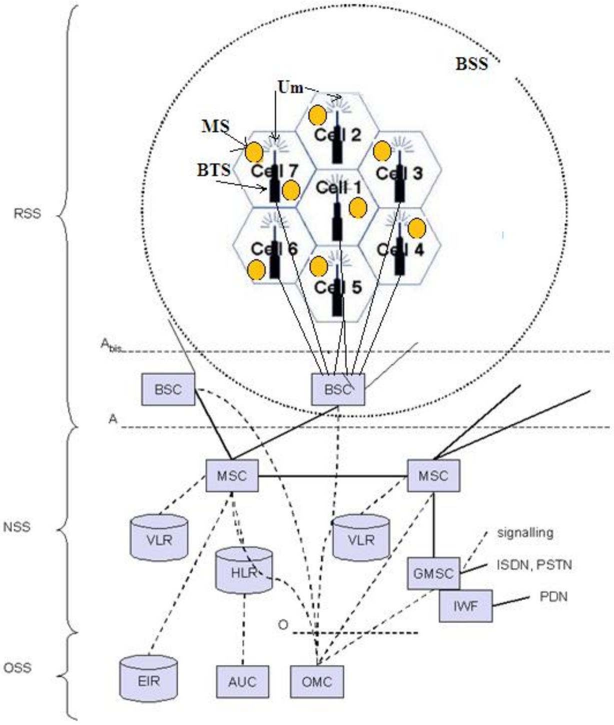
GSM system architecture is a hierarchical architecture comprising of the following three subsystems:

i. Radio Subsystem (RSS)

ii. Network and Switching Subsystem (NSS)

iii. Operational Subsystem (OSS)

As a matter of fact the use of the mobile service practically see only a small part of the architecture, may be a mobile handset (MS), Mobile Towers carrying some antennas. Rest of the system is hidden to a common user. The three major subsystems are explained below with the help of the architecture given in figure-1



1. Radio Subsystem:

   The radio subsystem consist of the Mobile stations(or mobile handsets), Base Transceiver System (BTS), and Base Station Controller.

Base station subsystem(BSS) : BSS is the contain the end user stations called mobile stations(MS), the base transceiver stations(BTS), a base station controller(BSC). BTS installed in cells providing the necessary connectivity to the MS via the Um interface and to BSC via Abis interface.

2. Networking and Switching Subsystem:

The main function of NSS is to provide the handover among the different BSS and other functions such as worldwide location management of users, charging, accounting and roaming of users. It consist of MSC, HLR and VLR. HLR stores Static Information such as mobile subscriber ISDN number, subscriber services such as (call forwarding, roaming restriction, GPRS). Visitor Location Register (VLR) is associated with each MSC is a dynamic database that stores , when a new MS enter the LA, its VLR is updated by copying information from its HLR.

3. Operation Subsystem contain services for network operation and management. Operations and Management Center is responsible for traffic monitoring, status report of network elements, accounting and billing , subscriber and security management. Authentication center(AuC) protects user identity and data transmission. Equipment Identity Register (EIR) is a database for device identity (IMEI), blacklist of locked devices. This database is not synchronized among the other operators and hence device may be misused.

(b) Compare various data networks standards like GPRS, IS-95, and WCDMA. 10

GPRS:

The **general packet radio service (GPRS)** provides packet mode transfer for applications that exhibit traffic patterns such as frequent transmission of small volumes or infrequent transmissions of small or medium volumes according to the requirement specification. Compared to existing data transfer services, GPRS should use the existing network resources more efficiently for packet mode applications, and should provide a selection of QoS parameters for the service requesters. GPRS should also allow for broadcast, multicast, and unicast service. Network providers typically support this model by charging on volume and not on connection time as is usual for traditional GSM data services and for HSCSD.

The main benefit for users of GPRS is the ‘always on’ characteristic – no connection has to be set up prior to data transfer. Clearly, GPRS was driven by the tremendous success of the packet-oriented internet, and by the new traffic models and applications. However, GPRS, needs additional network elements, i.e., software and hardware.

The main concepts of GPRS is that, 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. Depending on the coding, a transfer rate of up to 170 kbit/s is possible. For

GPRS, operators often reserve at least a time slot per cell to guarantee a minimum data rate. The GPRS concept is independent of channel characteristics and of the type of channel (traditional GSM traffic or control channel), and does not limit the maximum data rate (only the GSM transport system limits the rate). All GPRS services can be used in parallel to conventional services.

The **GPRS architecture** introduces two new network elements, which are called **GPRS support nodes (GSN)** and are in fact routers. All GSNs are integrated into the standard GSM architecture, and many new interfaces have been defined (see Figure 4.16). The **gateway GPRS support node (GGSN)** is the interworking unit between the GPRS network and external **packet data networks (PDN)**. This node contains routing information for GPRS users, performs address conversion, and tunnels data to a user via encapsulation. The GGSN is connected to external networks (e.g., IP or X.25) via the Gi interface and transfers packets to the SGSN via an IP-based GPRS backbone network (Gn interface).

The other new element is the **serving GPRS support node (SGSN)** which supports the MS via the Gb interface. 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. The SGSN is connected to a BSC via frame relay and is basically on the same hierarchy level as an MSC. The GR, which is typically a part of the HLR, stores all GPRS-relevant data. GGSNs and SGSNs can be compared with home and foreign agents, respectively,
in a mobile IP network

IS-95

First commercial CDMA standard, developed by Qualcomm, ratified in 1995 ƒ Still forms basis for CDMA voice access ƒ 1.23 MHz of bandwidth ƒ Total spreading factor of 128 (full-rate voice)

IS-95 (promoted as cdmaOne) is based on CDMA, which is a completely different medium access method. Before deployment, the system was proclaimed as having many advantages over TDMA systems, such as its much higher capacity of users per cell, e.g., 20 times the capacity of AMPS. Today, CDMA providers are making more realistic estimates of around five times as many users. IS-95 offers soft handover, avoiding the GSM ping-pong effect. However, IS-95 needs precise synchronization of all base stations (using GPS satellites which are military satellites, so are not under control of the network provider), frequent power control, and typically, dual mode mobile phones due to the limited coverage. The basic ideas of CDMA have been integrated into most 3G systems.

WCDMA:

Wideband Code-Division Multiple-Access (W-CDMA) is one of the main technologies for the implementation of third-generation (3G) cellular systems. It is base on radio access technique proposed by ETSI Alpha group and the specifications was finalised 1999.

The implementation of W-CDMA will be a technical challenge because of it's complexity and versatility. The complexity of W-CDMA systems can be viewed from different angles: the complexity of each single algorithm, the complexity of the overall system and the computational complexity of a receiver. W-CDMA link-level simulations are over 10 times more compute-intensive than current second-generation simulations. In W-CDMA interface different users can simultaneously transmit at different data rates and data rates can even vary in time. UMTS networks need to support all current second generation services and numerous new applications and services.

7. (a)Explain HyperLAN in detail 10

In 1996, the ETSI standardized HIPERLAN 1 as a WLAN allowing for node mobility and supporting ad-hoc and infrastructure-based topologies (ETSI 1996). (HIPERLAN stands for **high performance local area network**.) **HIPERLAN-1** was originally one out of four HIPERLANs envisaged, as ETSI decided to have different types of networks for different purposes. The key feature of all four networks is their integration of time-sensitive data transfer services. Over time, names have changed and the former HIPERLANs 2, 3, and 4 are now called HiperLAN2, HIPERACCESS, and HIPERLINK.

HIPERLAN 1is a wireless LAN that support priorities and packet life time for data transfer at 23.5 Mbit/s, including forwarding mechanisms, topology discovery, user data encryption, network identification and power conservation mechanisms. HIPERLAN 1 should operate at 5.1–5.3 GHz with a range of 50 m in buildings at 1 W transmit power.

The service offered by a HIPERLAN 1 is compatible with the standard MAC services known from IEEE 802.x LANs. Addressing is based on standard 48 bit MAC addresses. A special HIPERLAN 1 identification scheme allows the concurrent operation of two or more physically overlapping HIPERLANs without mingling their communication. Confidentiality is ensured by an encryption/decryption algorithm that requires the identical keys and initialization vectors for successful decryption of a data stream encrypted by a sender.

An innovative feature of HIPERLAN 1, which many other wireless networks do not offer, is its ability to forward data packets using several relays. Relays can extend the communication on the MAC layer beyond the radio range. For power conservation, a node may set up a specific wake-up pattern. This pattern determines at what time the node is ready to receive, so that at other times, the node can turn off its receiver and save energy.

The following describes only the medium access scheme of HIPERLAN 1, a scheme that provides QoS and a powerful prioritization scheme.

Elimination-yield non-preemptive priority multiple access (EY-NPMA) is not only a complex acronym, but also the heart of the channel access providing priorities and different access schemes. EY-NPMA divides the medium access of different competing nodes into three phases:

● **Prioritization:** Determine the highest priority of a data packet ready to be sent by competing nodes.

● **Contention:** Eliminate all but one of the contenders, if more than one sender has the highest current priority.

● **Transmission:** Finally, transmit the packet of the remaining node.

In a case where several nodes compete for the medium, all three phases are necessary (called ‘channel access in **synchronized channel condition**’). If the channel is free for at least 2,000 so-called high rate bit-periods plus a dynamic extension, only the third phase, i.e. transmission, is needed (called ‘channel access in **channel-free condition**’).

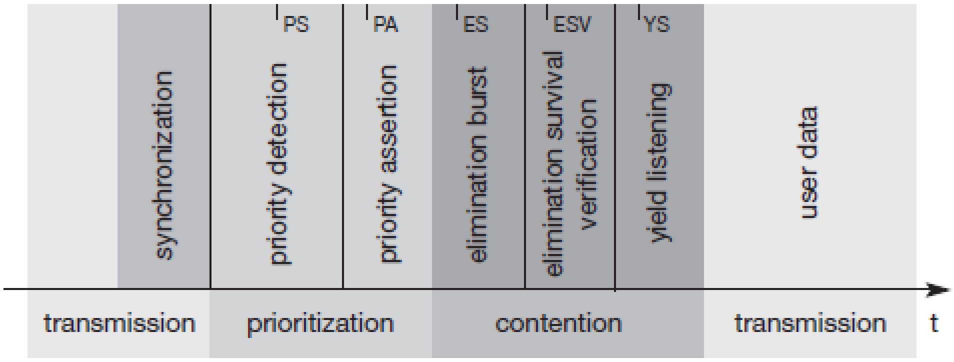


Figure: Phases of the HIPERLAN 1 EY-NPMA access scheme

The dynamic extension is randomly chosen between 0 and 3 times 200 high rate bit-periods with equal likelihood. This
extension further minimizes the probability of collisions accessing a free channel if stations are synchronized on higher layers and try to access the free channel at the same time. HIPERLAN 1 also supports ‘channel access in the **hidden elimination condition**’ to handle the problem of hidden terminals.

The contention phase is further subdivided into an **elimination phase** and a **yield phase**. The purpose of the elimination phase is to eliminate as many contending nodes as possible (but surely not all). The result of the elimination phase is a more or less constant number of remaining nodes, almost independent of the initial number of competing nodes. Finally, the yield phase completes the work of the elimination phase with the goal of only one remaining node. Figure above gives an overview of the three main phases and some more details which will be explained in the following sections. For every node ready to send data, the access cycle starts with synchronization to the current sender. The first phase, prioritization, follows. After that, the elimination and yield part of the contention phase follow. Finally, the remaining node can transmit its data. Every phase has a certain duration which is measured in numbers of slots and is determined by the variables IPS, IPA, IES, IESV, and IYS.

(b) Explain Bluetooth. **10**

This is a different type of network is needed to connect different small devices in close proximity (about 10 m) without expensive wiring or the need for a wireless infrastructure (Bisdikian, 1998). The envisaged gross data rate is 1 Mbit/s, asynchronous (data) and synchronous (voice) services should be available.

Architecture

Like IEEE 802.11b, Bluetooth operates in the 2.4 GHz ISM band. However, MAC, physical layer and the offered services are completely different.

Networking

To understand the networking of Bluetooth devices a quick introduction to its key features is necessary. Bluetooth operates on 79 channels in the 2.4 GHz band with 1 MHz carrier spacing. Each device performs frequency hopping with 1,600 hops/s in a pseudo random fashion. Bluetooth applies FHSS for interference mitigation.

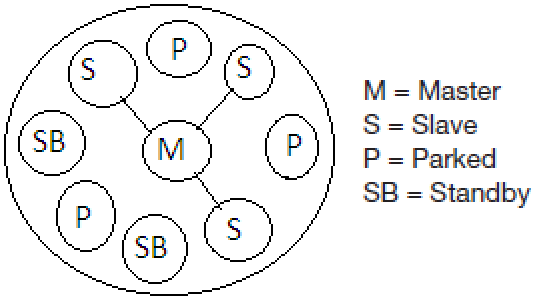


Figure: Bluetooth Piconet

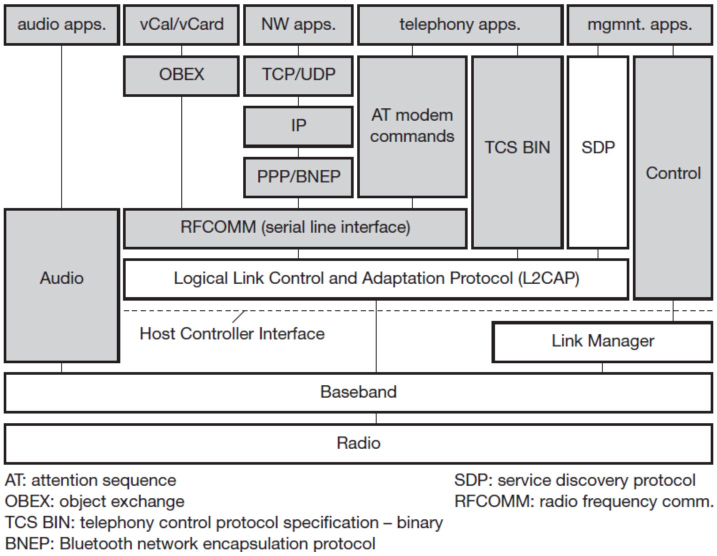
A very important term in the context of Bluetooth is a **piconet**. A piconet is a collection of Bluetooth devices which are synchronized to the same hopping sequence. Figure 7.41 shows a collection of devices with different roles. One device in the piconet can act as **master** (M), all other devices connected to the master must act as **slaves** (S). The master determines the hopping pattern in the piconet and the slaves have to synchronize to this pattern. Each piconet has a unique hopping pattern. If a device wants to participate it has to synchronize to this. Two additional types of devices are shown: parked devices (P) can not actively participate in the piconet (i.e., they do not have a connection), but are known and can be reactivated within some milliseconds.

Devices in stand-by (SB) do not participate in the piconet. Each piconet has exactly one master and up to seven simultaneous slaves. More than 200 devices can be parked. The reason for the upper limit of eight active devices, is the 3-bit address used in Bluetooth. If a parked device wants to communicate and there are already seven active slaves, one slave has to switch to park mode to allow the parked device to switch to active mode.

Bluetooth Protocol Stack:

The Bluetooth protocol stack can be divided into a **core specification** (Bluetooth, 2001a), which describes the protocols from physical layer to the data link control together with management functions, and **profile specifications** (Bluetooth, 2001b). The latter describes many protocols and functions needed to adapt the wireless Bluetooth technology to legacy and new applications.

The **core protocols** of Bluetooth comprise the following elements:


audio apps.
vCal/vCard
NW apps.
telephony apps.
mgmnt. apps.
OBEX
TCP/UDP
IP
PPP/BNEP
AT modem commands
TCS BIN
SDP
Control
Audio
RFCOMM (serial line interface)
Logical Link Control and Adaptation Protocol (L2CAP)
Host Controller Interface
Link Manager
Baseband
Radio
AT: attention sequence
OBEX: object exchange
TCS BIN: telephony control protocol specification – binary
BNEP: Bluetooth network encapsulation protocol
SDP: service discovery protocol
RFCOMM: radio frequency comm.

● **Radio:** Specification of the air interface, i.e., frequencies, modulation, and transmit power.

● **Baseband:** Description of basic connection establishment, packet formats, timing, and basic QoS parameters.

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

● **Logical link control and adaptation protocol (L2CAP):** Adaptation of higher layers to the baseband (connectionless and connection-oriented services.

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

On top of L2CAP is the **cable replacement protocol** RFCOMM that emulates a serial line interface following the EIA-232 (formerly RS-232) standards. This allows for a simple replacement of serial line cables and enables many legacy applications and protocols to run over Bluetooth. RFCOMM supports multiple serial ports over a single physical channel. The **telephony control protocol specification – binary** (TCS BIN) describes a bit-oriented protocol that defines call control signaling for the stablishment of voice and data calls between Bluetooth devices. It also describes mobility and group management functions. The **host controller interface** (HCI) between the baseband and L2CAP provides a command interface to the baseband controller and link manager, and access to the hardware status and control registers. The HCI can be seen as the hardware/software boundary.

Many **protocols** have been **adopted** in the Bluetooth standard. Classical Internet applications can still use the standard TCP/IP stack running over PPP or use the more efficient Bluetooth network encapsulation protocol (BNEP). Telephony applications can use the AT modem commands as if they were using a standard modem. Calendar and business card objects (vCalendar/vCard) can be exchanged using the object exchange protocol (OBEX) as common with IrDA interfaces. A real difference to other protocol stacks is the support of **audio**. Audio applications may directly use the baseband layer after encoding the audio signals.

UNIT-4

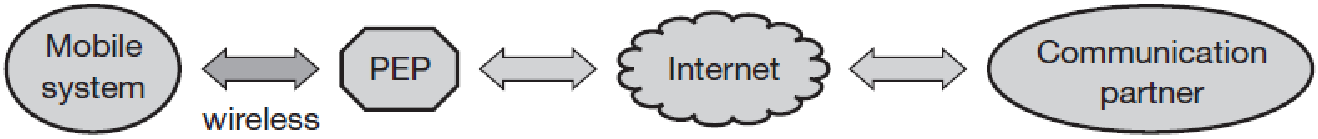
8. (a) What is performance enhancing proxies? Explain 10

Performance Enhancing Proxies are used to Mitigate Link-Related Degradations' and are also beneficial for wireless and mobile internet access.

Transport layer proxies: The transport layer proxies are 'snooping TCP' and 'indirect TCP'. The transport layer proxies are typically used for local retransmissions, local acknowledgements, TCP acknowledgement filtering or acknowledgement handling in general.

Application level proxies: Application layer proxies can be used for content filtering, content-aware compression, picture downscaling etc. Prominent examples are internet/WAP gateways making at least some of the standard web content accessible from WAP devices.

In principle, proxies can be placed on any layer in a communication system but the one located in located in the transport and application layer are discussed here. One of the key features of a proxy is its transparency with respect to the end systems, the applications and the users. Figure shows the general architecture of a wireless system connected via a proxy with the internet.

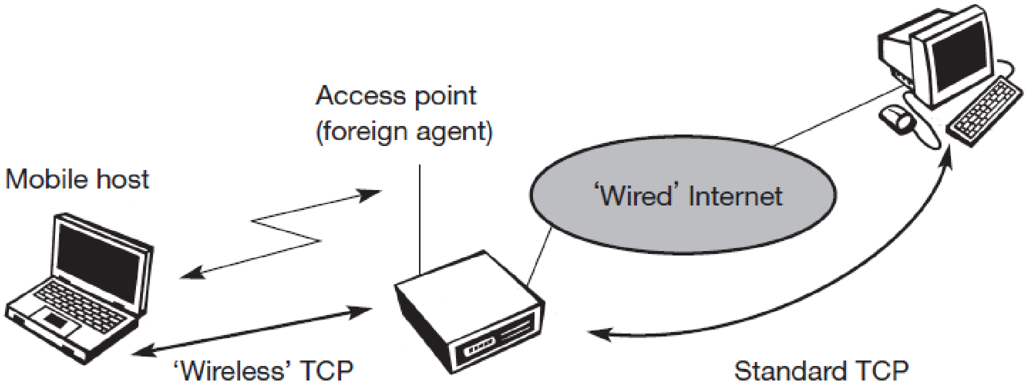


However, all proxies share a common problem as they break the end-to-end semantics of a connection. The most detrimental negative implication of breaking the end-to-end semantics is that it disables end-to-end use of IP security. Using IP security with ESP (encapsulation security payload) the major part of the IP packet including the TCP header and application data is encrypted so is not accessible for a proxy.

Transport layer Proxies:

Indirect TCP:

I-TCP segments a TCP connection into a fixed part and a wireless part. Figure below shows an example with a mobile host connected via a wireless link and an access point to the 'wired' internet where the correspondent host resides.



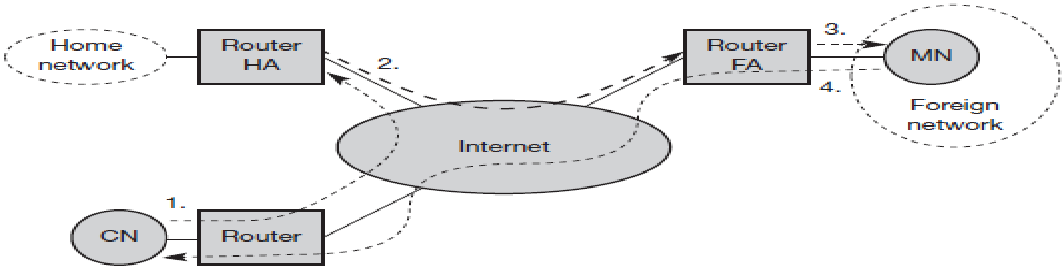
Standard TCP is used between the fixed computer and the access point. No computer in the internet recognizes any changes to TCP. Instead of the mobile host, the access point now terminates the standard TCP connection, acting as a proxy. This means that the access point is now seen as the mobile host for the fixed host and as the fixed host for the mobile host. Between the access point and the mobile host, a special TCP, adapted to wireless links, is used.

Snooping TCP:

In this approach, the foreign agent buffers all packets with **destination mobile host** and additionally 'snoops' the packet flow in both directions to recognize acknowledgements. The reason for buffering packets toward the mobile node is to enable the foreign agent to perform a local retransmission in case of packet loss on the wireless link. The foreign agent buffers every packet until it receives an acknowledgement from the mobile host. If the foreign agent does not receive an acknowledgement from the mobile host within a certain amount of time, either the packet or the acknowledgement has been lost.

(b) What is reverse Tunnelling? Explain 10

We have seen how a correspondent node communicated with the mobile node through the router HA and COA as also seen in the following figure:



At first glance, the return path from the MN to the CN shown in figure above looks quite simple. The MN can directly send its packets to the CN as in any other standard IP situation. The destination address in the packets is that of CN.

But there are several severe problems associated with this simple solution.

i. **Firewalls:** Almost all companies and many other institutions secure their internal networks (intranet) connected to the internet with the help of a firewall. All data to and from the intranet must pass through the firewall. Besides many other functions, firewalls can be set up to filter out malicious addresses from an administrator's point of view. Quite often firewalls only allow packets with topologically correct addresses to pass. This provides at least a first and simple protection against misconfigured systems of unknown addresses. However, MN still sends packets with its fixed IP address as source which is not topologically correct in a foreign network. Firewalls often filter packets coming from outside containing a source address from computers of the internal network. This avoids other computers that could use internal addresses and claim to be internal computers. However, this also implies that an MN cannot send a packet to a computer residing in its home network. Altogether, this means that not only does the destination address matter for forwarding IP packets, but also the source address due to security concerns. Further complications arise through the use of private addresses inside the intranet and the translation into global addresses when communicating with the internet. This **network address translation** is used by many companies to hide internal resources (routers, computers, printers etc.) and to use only some globally available addresses.

ii. **Multi-cast:** Reverse tunnels are needed for the MN to participate in a multicastgroup. While the nodes in the home network might participate in a multi-cast group, an MN in a foreign network cannot transmit multi-cast packets in a way that they emanate from its home network without a reverse tunnel. The foreign network might not even provide the technical infrastructure for multi-cast communication.

iii. **TTL:** Consider an MN sending packets with a certain TTL while still in its home network. The TTL might be low enough so that no packet is transmitted outside a certain region. If the MN now moves to a foreign network, this TTL might be too low for the packets to reach the same nodes as before. Mobile IP is no longer transparent if a user has to adjust the TTL while moving. A reverse tunnel is needed that represents only one hop, no matter how many hops are really needed from the foreign to the home network.

9. Write short Note on: **20**

Under progress

Reference:

1. http://www.wirelesscommunication.nl/reference/chaptr03/fsl.htm
2. Mobile Communication by Schiller

3. Wireless Communication by Rapaport
4. http://www.iitg.ernet.in/scifac/qip/public_html/cd_cell/chapters/a_mitra_mobile_communication/chapter5.pdf
5. www.care4you.in
6. https://en.wikipedia.org/wiki/Fading
7. http://www.antenna-theory.com/basics/fieldRegions.php