SOLUTION Prepared by Dr. RN Rajotiya

Under Prepration:

MDU Examination May 2015

Mobile Communication

Paper : ECE-419-F

Time : 3 Hours MM: 100

Before answering the question, candidate should ensure that they have been supplied the correct and complete question paper. No complaint in this regard, will be entertained after the examination.

Note: Question no. 1 is compulsory. Attempt any five questions by selecting at least one question from each section.

1. (a) What is far-field region 4

The region far from an antenna compared to the dimensions of the antenna and the wavelength of the radiation. Also known as far field;far region; far zone; radiation zone. In this region, the radiation pattern does not change shape with distance(although the field still die off as 1/R, the power density dies off as ($1/R^2$). Also, this region is dominated by radiated fields, with the E- and H-fields orthogonal to each other and the direction of propagation as with plane waves.
If the maximum linear dimension of an antenna is D, then the following 3 conditions must all be satisfied to be in the far field region:

$R > 2D^2/\lambda$. i.

$R >> D$ ii

$R >> \lambda$

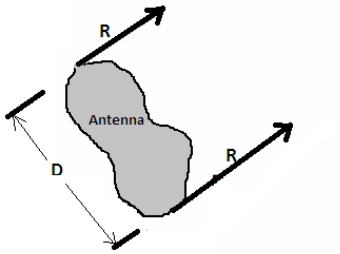


Fig: The Rays from any Point on the Antenna are Approximately Parallel in the Far Field

The 1st and the 2nd eqn above ensure that the power radiated in a given direction from distinct parts of the antenna are approximately parallel as shown in figure below. This helps ensure the fields in the far-field region behave like plane waves. Note that $R >> D$, or $R >> \lambda$ means "R is much more greater i.e. 10 times than the RHS"
Finally, where doesthe third far-field equation come from? Near a radiating antenna, there are reactive fields that typically have the E-fields and H-fiels die off with distance $1/R^2$ and $1/R^3$. The third equation above ensures that these near fields are gone,and we are left with the radiating fields, which fall off with distance as 1/R.
The far field region is sometimes referred to as Fraunhofer region, a carryover term from optics.

(b) What are the security threats to wireless networks? 4

There are a number of main threats that exist to wireless LANS, these include:

- Rogue Access Points/Ad-Hoc Networks
- Denial of Service
- Configuration Problems (Mis-Configurations/Incomplete Configurations)
- Passive Capturing

i. Rogue Access Points/Ad-Hoc Networks

One method that is often used by attackers targeting wireless LANS is to setup a rogue access point that is within the range of the existing wireless LAN. The idea is to 'fool' some of the legitimate devices into associating to this access point over the legitimate access points. To really be effective, this type of attack requires some amount of physical access; If an attacker is able to gain access to a physical port on a company network and then hook the access point into this port, it is possible to get devices to associate with the rogue access point and capture data through it for an extended period of time.

ii. Denial of Service

DoS is one of the simplest network attacks to perpetrate because it only requires limiting access to services. This can be done by simply sending a large amount of traffic at a specific target. However, the flooding of traffic is not the only way to limit access to services; for wireless networks it can be much easier as the signal can be interfered with through a number of different techniques. When a wireless LAN is using the 2.4 GHz band, interference can be caused by something as simple as a microwave oven or a competing access point on the same channel. Because the 2.4 GHz band is limited to only 3 non-overlapping channels (U.S.), an attacker just needs to cause enough interference into these three channels to cause service interruption.

iii. Configuration Problems

Simple configuration problems are often the cause of many vulnerabilities, this is because many consumer/SOHO grade access points ship with no security configuration. A novice user can set up one of these devices quickly and gain access. However they also open up their network to external use without further configuration. Other potential issues with configuration include weak passphrases, weak security deployments (i.e. WEP vs WPA vs WPA2), and default SSID usage among others.

iv. Passive Capturing

Passive capturing is performed by simply getting within range of a target wireless LAN and then listening and capturing data. This information can be used for a number of things including attempting to break existing security settings and analyzing non-secured traffic. It is almost impossible to really prevent this type of attack because of the nature of a wireless network; what can be done is to implement high security standards using complex parameters.

(c) What are the effects of fading? 4

Multipath Fading Effects In principle, the following are the main multipath effects:

1 Fading Effects due to Multipath Time Delay Spread

Flat Fading

Such types of fading occurs when the bandwidth of the transmitted signal is less than the coherence bandwidth of the channel. Equivalently if the symbol period of the signal is more than the rms delay spread of the channel, then the fading is flat fading.

Frequency Selective Fading

Frequency selective fading occurs when the signal bandwidth is more than the coherence bandwidth of the mobile radio channel or equivalently the symbols duration of the signal is less than the rms delay spread.

2 Fading Effects due to Doppler Spread

Fast Fading

In a fast fading channel, the channel impulse response changes rapidly within the symbol duration of the signal. Due to Doppler spreading, signal undergoes frequency dispersion leading to distortion. Therefore a signal undergoes fast fading if $T_S >> T_C$; where T_C is the coherence time and $B_S >> B_D$; where B_D is the Doppler spread. Transmission involving very low data rates suffer from fast fading.

Slow Fading

In such a channel, the rate of the change of the channel impulse response is much less than the transmitted signal. We can consider a slow faded channel a channel in which channel is almost constant over atleast one symbol duration. Hence $T_S << T_{C;}$ and $B_S >> B_D$

(d) What is mobility management? 4

Mobility Management :

A MS is assigned a home network, commonly known as location area. When an MS migrates out of its current BS into the footprint of another, a procedure is performed to maintain service continuity, known as Handoff management. An agent in the home network, called home agent, keeps track of the current location of the MS. The procedure to keep track of the user's current location is referred to as Location management. Handoff management and location management together are referred to as Mobility management.

Handoff: At any instant, each mobile station is logically in a cell and under the control of the cell's base station. When a mobile station moves out of a cell, the base station notices the MS's signal fading away and requests all the neighbouring BSs to report the strength they are receiving. The BS then transfers ownership to the cell getting the strongest signal and the MSC changes the channel carrying the call. The process is called handoff.

Location Management; location update and paging. When a Mobile Station (MS) enters a new Location Area, it performs a location updating procedure by making an association between the foreign agent and the home agent. One of the BSs, in the newly visited Location Area is informed and the home directory of the MS is updated with its current location. When the home agent receives a message destined for the MS, it forwards the message to the MS via the foreign agent. An authentication process is performed before forwarding the message.

(e) What advantages does the use of IPv6 offer for mobility? 4

SOLUTION

While mobile IP was originally designed for IP version 4, IP version makes life much easier. The advantages are:

i. Several mechanisms that had to be specified separately for mobility support come free in IPv6.
ii. Security with regard to authentication, is now a required featurefor all IPv6 nodes. No special mechanisms as add-ons are needed for securing mobile IP registration.
iii. Every IPv6 node masters address auto configuration – the mechanisms for acquiring a COA are already built in.
iv. Neighbor discovery as a mechanism mandatory for every node is also included in the specification; special foreign agents are no longer needed to advertise services.
v. Combining the features of auto configuration and neighbor discovery means that every mobile node is able to create or obtain a topologically correct address for the current point of attachment.
vi. Every IPv6 node can send binding updates to another node, so the MN can send its current COA directly to the CN and HA. These mechanisms are an integral part of IPv6.
vii. A soft handover is possible with IPv6. The MN sends its new COA to the old router servicing the MN at the old COA, and the old router encapsulates all incoming packets for the MN and forwards them to the new COA.
viii. Altogether, mobile IP in IPv6 networks requires very few additional mechanisms of a CN, MN, and HA.
ix. The FA is not needed any more. A CN only has to be able to process binding updates, i.e., to create or to update an entry in the routing cache.
x. The MN itself has to be able to decapsulate packets, to detect when it needs a new COA, and to determine when to send binding updates to the HA and CN. A HA must be able to encapsulate packets.

SECTION-A

2.(a) What are the applications of cellular mobile communications? 10

SOLUTION:

The application areas are discussed below:

i. Vehicle: many of the new vehicle that are appearing in the market are already fitted with such technology. It helps communication while on moving in a vehicle. In urban areas cellular systems help maintain te uninterrupted communication while in remote areas satellite communication can be used, while the current position of the car can be determined using the global positioning system. Other services as music, news, road condition, weather report and other broadcast services are received via digital audio broadcasting with 1.5 Mbps.

ii. Emergencies: Ambulance may be fitted with high quality wireless connectivity with hospital for better medical help.

iii. Business: Cellular communication has brought the concept of m-commerce and m-business, and this is a reality these days that many of the meetings, audio conferences help business activity while on move without actually meeting the other party.

iv. Replacement of wired networks: This gives a better solution to get rid of all wires in home and offices, thus giving a neat and clean outlook, flexibility, mobility etc.

v. Infotainment : Internet everywhere, is not possible without wireless and cellular technology. It has given the freedom to do business with electronic cash. Today service like mpaisa is available that transfer money to another location. Cashless recharge of mobile. Airtel has offered a service to transfer balance to other mobile.

vi. Location dependent services: Today we are able to move and get connected through another access point hiding the fact that you have changed your location. Mobile IP allows to transmit the packet through other access points keeping the same home IP.

vii. Mobile and Wireless devices:

a. Sensor (Sensing the Door)
b. Embedded controllers (keyboard, washing machines)
c. Pager (Display short message)
d. Mobile Phones (Migrate, Color graphic display touch screen)
e. Personal Digital assistant (Accompany calendar, notepad)
f. Pocket computer Notebook / Laptop

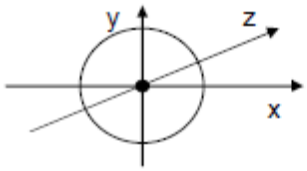
(b)Describe in brief the Antennas used in mobile communication. 10

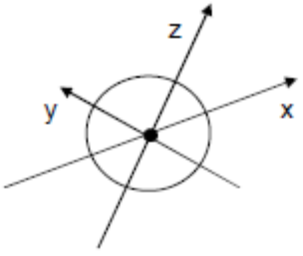
The antennas are used for Radiation and reception of electromagnetic waves, coupling of wires to space for radio transmission. The following types of antennas are used in mobile communication

• 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



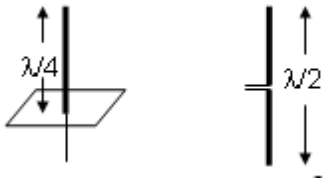


Ideal isotropic radiator

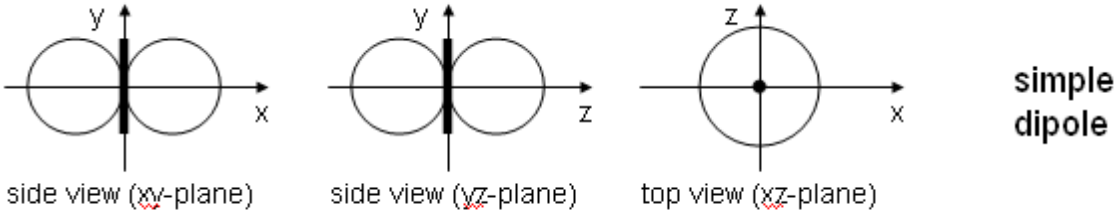
Antennas: simple dipoles

• 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

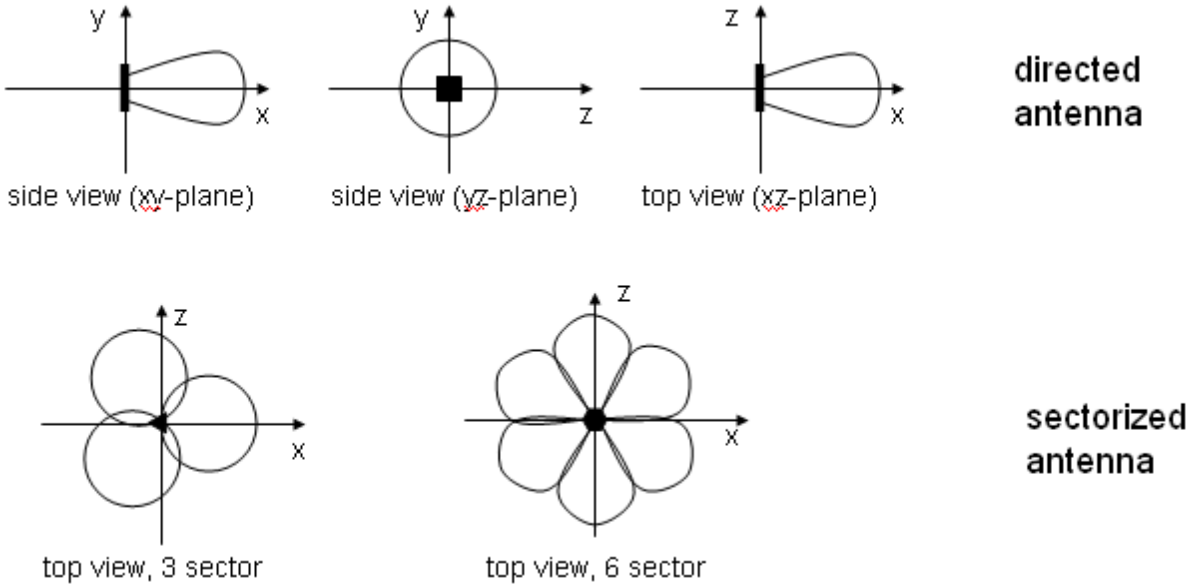


Example: Radiation pattern of a simple Hertzian dipole



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)



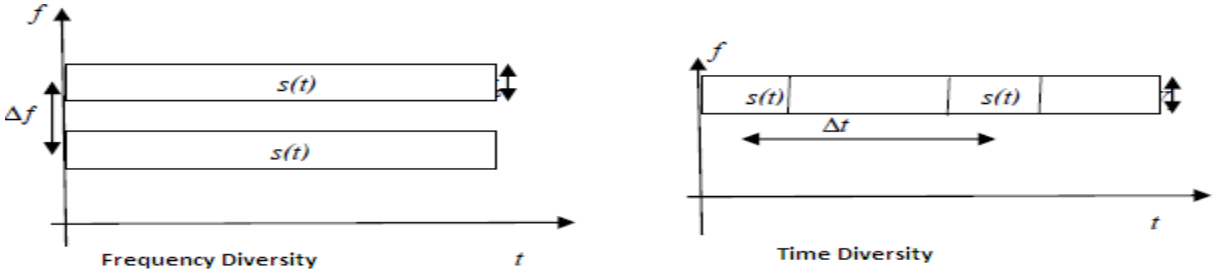
3. (a) What do you mean by diversity? How many type of diversity are present? 10

Diversity is the technique used in wireless communications systems to improve the performance over a fading radio channel. Here receiver is provided with multiple copies of the same information signal which are transmitted over two or more real or virtual communication channels. Diversity exploits the random nature of the radio propagation by finding independent signal paths for communication. Thus the basic idea of diversity is repetition or redundancy of information. In virtually all the applications, the diversity decisions are made by the receiver and are unknown to the transmitter.

Types of Diversity : Small-scale fades are characterized by deep and rapid amplitude fluctuations which occur as the mobile moves over distances of just a few wavelengths. For narrow-band signals, this typically results in a Rayleigh faded envelope. In order to prevent deep fades from occurring, microscopic diversity techniques can exploit the rapidly changing signal. Large scale fading, caused due to shadowing, can be combated using macroscopic diversity wherein the distances of consideration are of the order of the distances between two base stations.

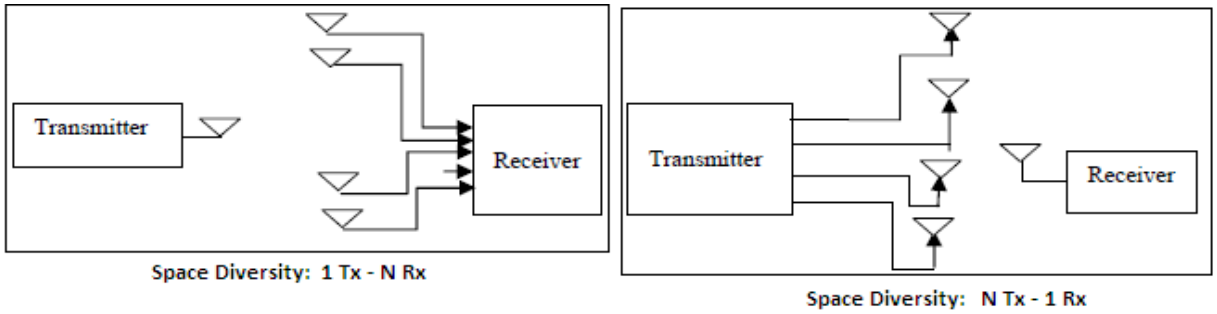
i. **Diversity techniques**: Diversity techniques are effective when the branches considered are assumed to be independently faded or the envelopes are uncorrelated. There are mainly five techniques of diversity practically used:

ii. **Frequency Diversity:** The same information signal is transmitted on different carriers, the frequency separation between them being at least the coherence bandwidth.



iii. **Time Diversity:** The information signal is transmitted repeatedly in time at regularly intervals. The separation between the transmit times should be greater than the coherence time, Tc. The time interval depends on the fading rate, and increases with the decrease in the rate of fading.

iv. **Space Diversity:** In Space diversity, there are multiple receiving antennas placed at different spatial locations, resulting in different (possibly independent) received signals.



v. **Polarization diversity:** Here, the electric and magnetic fields of the signal carrying the information are modified and many such signals are used to send the same information. Thus orthogonal type of polarization is obtained. It enables detection of smaller radar cross-section (RCS) targets, and avoids the physical, mathematical, and engineering challenges of timeof-arrival coherent combining. The advantage of polarization diversity over spatial diversity is that diversity gains are possible with collocated antennas.

vi. **Angle Diversity:** The angular diversity schemes may be applied at the base station or at the Mobile unit.

- At the Base station
  - In time Angular Diversity Combine the two received signals at the same time in order to achieve Diversity Gain. It is a microscopic diversity.

- Out of time Angular Diversity The signal strength of the mobile unit is constantly monitored at the base station by each beam of a multi-beam antenna system. The strongest beam is used for the traffic link at the time.

➢ At the Mobile unit-If the received signal arrives at the Antenna via several paths, each with a different angle of arrival, the signal components can be isolated by means of directive antennas. Each directive antenna will isolate a different angular component and signals received from different directive antennas are uncorrelated.

(b) Define the followings: 10

(a) Doppler Spread.

Doppler spread B_D is a measure of the spectral broadening caused by the time rate of change of the mobile radio channel and is defined as the range of frequencies over which the received Doppler spectrum is essentially non-zero. When a pure sinusoidal tone of frequency f_c is transmitted, the received signal spectrum, called the Doppler spectrum, will have components in the range $f_c - f_d$ *to* $f_c + f_d$ *,where* f_d *is the Doppler shift. The amount of spectral broadening depends on* f_d *which is a function of the relative velocity of the mobile, and the angle* θ *between the direction of motion of the mobile and direction of arrival of the scattered waves. If the baseband signal bandwidth is much greater than* B_D *the effects of Doppler spread are negligible at the receiver*.

(b) Coherence Time

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,

$$Tc = \frac{1}{f_m}$$

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.

If the coherence time is defined as the time over which the time correlation function is above 0.5, then the coherence time is approximately [Ste94]

$$Tc = \frac{9}{16\pi f_m}$$

where f_m is the maximum Doppler shift given by $fm = v/\lambda$. In practice, (5.40.a) suggests a time duration during which a Rayleigh fading signal may fluctuate wildly, and (5.40.b) is often too restrictive. A popular rule of thumb for modern digital communications is to define the

coherence time as the geometric mean of Equations (5.40.a) and (5.40.b). That is,

$$Tc = \sqrt{\frac{9}{16\pi (fm)^2}}$$

The definition of coherence time implies that two signals arriving with a time separation greater than T_C are affected differently by the channel.

(c) Coherence bandwidth

SOLUTION:

The coherence Bc is the bandwidth for which either amplitudes or phases of two receiver signals have a high degree of similarity. Bc is a statistical measure of range of frequencies over which the channel passes all spectral components with approximately equal gain and linear phase.

$$Bc = \frac{1}{\tau_{dmax}}$$

More useful measurement is often expressed in terms of " rms" delay spread τdrms . Two fading signal with frequencies f1 and f2, where Δf= | f1-f2 |, if correlation function nbetween two faded signal R(Δf)=0.5, then

$$\Delta f > Bc = \frac{1}{2\pi\tau_{drms}}$$

More popular approximation is $\Delta f > Bc = \frac{1}{5\pi\tau_{drms}}$

Bc<1/Ts=Bw corresponds to frequency-selective (all freq. components are not affected by channel a similar manner)channel

Bc>1/Ts=Bw corresponds to flat fading (all freq. components are affected by channel a similar manner)channel channel

(d) Doppler Shift

Doppler shift occurs when the transmitter of a signal is moving in relation to the receiver. The relative movement shifts the frequency of the signal, making it different at the receiver than at the transmitter. In other words, the frequency perceived by the receiver differs from the one that was originally emitted. It's easy to understand and observe this phenomena with sound waves. A good example is the sound of a race car that passes by you. When the car is getting closer, the sound has a higher pitch. When the car passes you and starts going away, the pitch suddenly becomes lower.

This occurs because the source emits sound waves at a constant frequency but as it moves toward the observer, the distance between the waves in the signal becomes shorter. The waves travel at a speed v and are emitted at a frequency f(cycles/seconds). In our example, the emitter has moved a distance of d towards the receiver between the emission of two succeeding cycles. The cycles thus arrive at the observer at a frequency higher than the emission frequency. The opposite applies when the transmitter is moving away; the distance between each peak (or cycles) increases, and since the wave is moving at the same v speed, the perception of the observer is that the frequency has diminished.

For a vehicle moving in a straight line at constant velocity v , the Doppler frequency shift, fd is given by:

$$fd = \left(\frac{2\pi}{\lambda}\right)||v||\cos(\theta(t))$$

SECTION-B

4. (a) Explain in detail the free space loss model. 10

The free space propagation model assumes a transmit antenna and a receive antenna to be located in an otherwise empty environment. Neither absorbing obstacles nor reflecting surfaces are considered. In particular, the influence of the earth surface is assumed to be entirely absent.

For propagation distances d much larger than the antenna size, the far field of the electromagnetic wave dominates all other components. That is, we are allowed to model the radiating antenna as a point source with negligible physical dimensions. In such case, the energy radiated by an omni-directional antenna is spread over the surface of a sphere. This allows us to analyse the effect of distance on the received signal power.

The surface area of a sphere of radius d is $4\pi d^2$. The power density w at distance d from a transmitter with power p_T and antenna gain G_t is

$w = p_T G_t / (4 \pi d^2)$.

The available power p_R at a receive antenna with gain G_R is

$$P_R = \frac{P_T G_T}{4\pi d^2}.A = \frac{\lambda^2}{(4\pi d)^2} G_T P_T G_R$$

where A is the effective area or `aperture' of the antenna, with $G_R = 4 \pi A / \lambda^2$. The wavelengthC is c / f_c with c the velocity of light and f_c the carrier frequency. The product $G_t p_T$ is called the effectively radiated power (ERP) of the transmitter.

20 log *d* Path Loss Law

As the propagation distance increases, the radiated energy is spread over the surface of a sphere of radius d, so the power received decreases proportional to d^{-2}. Expressed in dB, the received power is :

$$P_{dB} = P_v - 20\, log\frac{d}{d_v}$$

(b) Explain Okumara propagation model. 10

SOLUTION:

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)

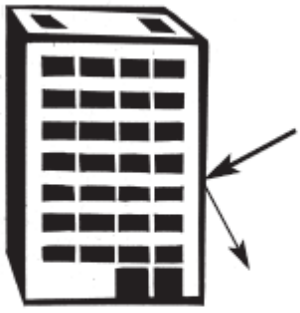
The remaining terms on the right hand side of eqn for L_{50} above are provided in a graphical form as the

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.

5. (a) Explain the basic propagation mechanisms in detail, which impact propagation in mobile communication. 10

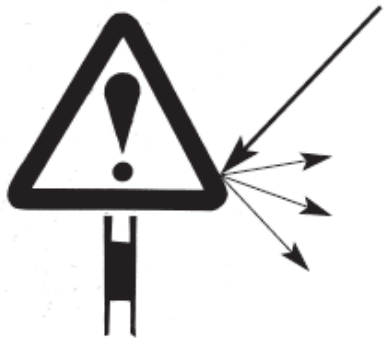
Reflection, diffraction and scattering are the three fundamental phenomena that cause signal propagation in a mobile communication system, apart from LoS communication. The most important parameter, predicted by propagation models based on above three phenomena, is the received power. The physics of the above phenomena may also be used to describe small scale fading and multipath propagation. The following subsections give an outline of these phenomena

Reflection : Reflection occurs when an electromagnetic wave falls on an object, which has very large dimensions as compared to the wavelength of the propagating wave. For example, such objects can be the earth, buildings and walls. When a radio wave falls on another medium having different electrical properties, a part of it is transmitted into it, while some energy is reflected back. Let us see some special cases. If the medium on which the e.m. wave is incident is a dielectric, some energy is reflected back and some energy is transmitted. If the medium is a perfect conductor, all energy is reflected back to the first medium. The amount of energy that is reflected back depends on the polarization of the e.m. wave.



Reflection

Diffraction: It is the phenomenon due to which an EM wave can propagate beyond the horizon, around the curved earth's surface and obstructions like tall buildings. As the user moves deeper into the shadowed region, the received field strength decreases. But the diffraction field still exists an it has enough strength to yield a good signal



Scattering

Diffraction

Scattering: The actual received power at the receiver is somewhat stronger than claimed by the models of reflection and diffraction. The cause is that the trees, buildings and lampposts scatter energy in all directions. This provides extra energy at the receiver. Roughness is tested by a Rayleigh criterion, which defines a critical height hc of surface protuberances for a given angle of incidence θi, given by, $h_c = \lambda / 8\sin\theta_i$.

(b) Define Brewster angle. 10

Brewster angle is the angle at which no reflection occurs in the medium of origin. It occurs when the incident angle Θ_B is such that the reflection coefficient (Γ) is equal to zero. The Brewster angle is given by the value of Θ_B which satisfies:

$$\text{Sin}(\Theta_B) = \sqrt{\frac{\varepsilon 1}{\varepsilon 1 + \varepsilon 2}}$$

For the case when the first medium is free space and the second medium has a relative permittivity $\varepsilon r, then\ the\ above\ equation\ can\ be\ expressed\ as$:

$$\text{Sin}(\Theta_B) = \sqrt{((\varepsilon r - 1)/(\varepsilon_r^2 - 1))}$$

The Brewster angle occur only for vertical polarization i.e. the maximum polarization of the reflected ray occurs when the reflected ray is perpendicular to the refracted ray.

SECTION-C

6. (a) Explain forward and reverse channel parameters of IS-95 CDMA. 10

IS-95 channels in the Forward link

The IS-95 forward link channels and their functions and make-up are summarized below:

- ***Pilot channel (PC):*** The pilot channel is transmitted as a reference by the base station to provide timing and phase reference for the mobiles, and carries no real data. The "data" carried by the channel is a continuous stream of zeros which is spread by Walsh code zero, which itself a stream of zeros. This is further spread by a pair of quadrature PN sequences. This means that the pilot channel is effectively the PN sequence with its associated offset. A measurement of the

signal-to-noise ratio of the pilot channel also gives the mobile an indication of which is the strongest serving sector.

- ***Paging channels (PCH):*** This IS-95 channel is used to carry information to enable mobiles to be paged. Data carried by this IS-95 channel includes system parameters, voice pages, SMS and other broadcast messages. It occupies Walsh codes 1 - 7 dependent upon the system requirements. The PCH carries data at either 4.8 or 9.6 kbps - a field in the Sync Channel indicates the data rate being transmitted.

  As with other channels there are a number of stages taken to produce the final channel. First the baseband information is error protected. After this the data is repeated if it is at a rate of 4.8 kbps, otherwise it is left as it is. Following this the data is interleaved and then scrambled by the decimated long PN sequence, and finally spread by the Walsh code for the particular channel assignment. In this process the long PN code is itself masked with a code which is specific to the channel being used. In this way the long PN code for Paging Channel 1 (using Walsh Code 1) is different to Paging Channel 4 (using Walsh Code 4).

- ***Synchronisation channel (SC):*** This IS-95 channel is used to provide the timing reference to access the cell . This IS-95 channel always uses Walsh code 32. Each base station has a fixed timing offset to reduce the interference between adjacent base-stations.

  The Sync channel incorporates an 80 mS superframe structure. This is divided into three 26.667 mS frames which correspond to the same length as the short PN sequences. This means that they align with the timing on the Pilot channel.

  This IS-95 channel is allocated the least power of the overhead channels in the overall CDMA transmission. The data that is transmitted on this channel includes the system time, pilot PN of the base station, long code state, system ID, and the network ID.

- ***Forward Traffic Channel (FTC):*** As the name implies, the Forward Traffic Channel is used to carry voice, user data, and also signalling information.

  IS-95 channels in the reverse link

  The IS-95 channels for the reverse link are quite different to those in the forward link. There are only two basic channels:

- Access channel
- Reverse traffic channel

  The way in which these IS-95 channels are structured and assembled is also different. This is because they are generated within the mobile rather than the base station. In terms of the modulation, OQPSK is used where a half chip delay is introduced onto the Q channel of the modulation.

  The two IS-95 channels in the reverse link are summarized below:

- ***Access channel (AC):*** This IS-95 channel is used by the mobile to communicate with the base station when no traffic channel has been set up. This IS-95 channel is therefore used for gaining acess toth e network, call origination requests and also for sending responses to paging commands that might be sent bythe network.

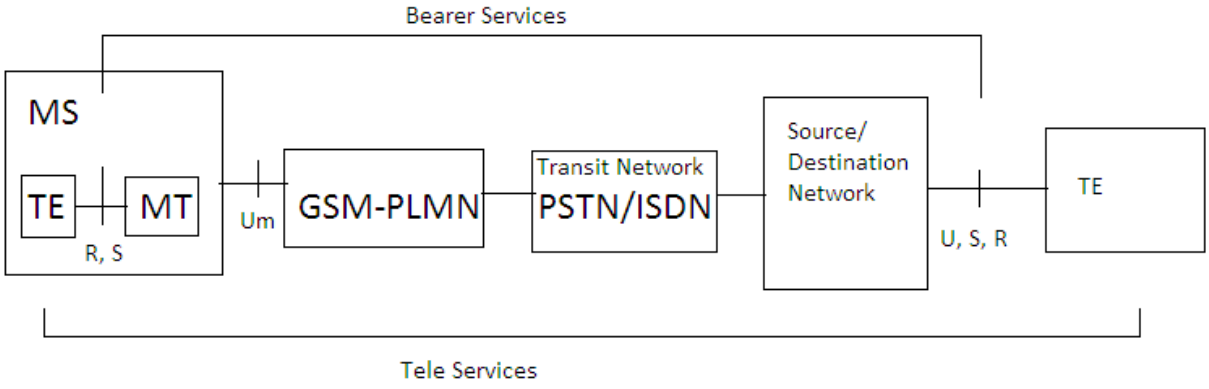
  There can be up to 32 Access Channels on the IS-95 reverse link for each Paging Channel on

forward link. Each AC uses the same PN but they are time shifted to enable the mobile to be uniquely identified. Data is sent at 4800 bps in a 20 mS time frame so that each frame contains 96 bits.

- ***Reverse traffic channel (RTC):*** Like the Forward Traffic Channel, this reverse link IS-95 channel is used to carry variable rate voice data, user data and signaling.

(b) What are the different GSM services and features? 10

- The GSM service permits integration of different voice and data services and interworking with existing networks.
- Here bearer services comprise all services that enable transparent transmission of data between the interface to the network (S in case of Mobile station).These services are connection oriented and may be circuit or packet switched and need lower 3 layer of OSI,
- Tele services are application specific and may need all 7 layers of OSI



i. Bearer Services:

- Bearer service permit transparent, non- transparent, synchronous, asynchronous data transmission. Original GSM offered data rate of 9.6Kbps.
- Transparent bearer services use layer 1 of OSI
- Use forward Error correction(FEC), do not try to recover loss of data due to shadowing, intruptions etc.

  Non Transparent services use OSI layer 2,3 to implement error correction and flow control. These services use transparent bearer services adding radio link protocol(RLP). This protocol comprise mechanism of HDLC, thus achieved bit error rate(BER) $<10^{-7}$

- Using transparent and non-transparent services, GSM specifies several bearer services for internetworking with PSTN, ISDN, packet switched public data networks (PSPDN) like X.25.

- Data transmission can be full duplex, synchronous with data rate 2.4.4.8,9.6Kbps, asynchronous from 300-9600bps.
- Low data rate reflect only small % of data servivces, but this relation of data and voice services is changing with data becoming mor and mor important

ii. Tele Services:

GSM mainly focuses on voice-oriented services, which comprises encrypted voice transmission, message services, and basic data communication with terminals as known from the PSTN and ISDN,. However as the main service is telephony, primary goal of GSM was the provision of high quality digital voice transmission, offering at least typical bandwidth of 3.1KHz that of analog telephony.

Non-voice Services offered: These services are: Emergency call, Short message service upto 160 characters, Enhanced Message service (EMS) upt 760 characters, Multimedia message service(MMS)-offered GIF, JPG, WBMP, short video clip come with phone with camera, Group 3 fax: in this fax data is transmitted as digital data over analog telephone network

iii. Supplementary Services

- Similar to ISDN these service offer various enhancements for std. telephony service such as :
- user identification
- Redirection
- Call Forwarding
- Closed user group
- and multi-party

7. (a) How do IEEE 802.11, HyperLAN2 and Bluetooth, respectively, solve the hidden terminal problem? 8

Solution:

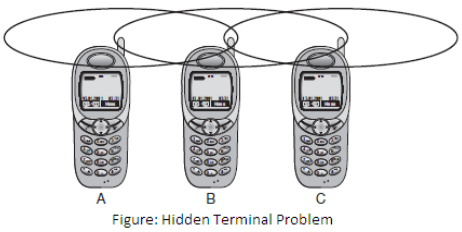


Figure: Hidden Terminal Problem

First o let us define what is Hidden terminals. Consider the scenario with three mobile phones as shown in below. The transmission range of A reaches B, but not C (the detection range does not reach C either). The transmission range of C reaches B, but not A. Finally, the transmission range of B reaches A and C, i.e., A cannot detect C and vice versa. A starts sending to B, C does not receive this transmission. C also wants to send something to B and senses the medium. The medium appears to be free, the carrier sense fails. C also starts sending causing a collision at B. But A cannot detect this collision at B and continues with its transmission. A is **hidden** for C and vice versa.

Solution in IEEE 802.11: To deal with this problem, the standard defines an additional mechanism
using two control packets, RTS and CTS. The use of the mechanism is optional; however, every 802.11 node has to implement the functions to react properly upon reception of RTS/CTS control packets.

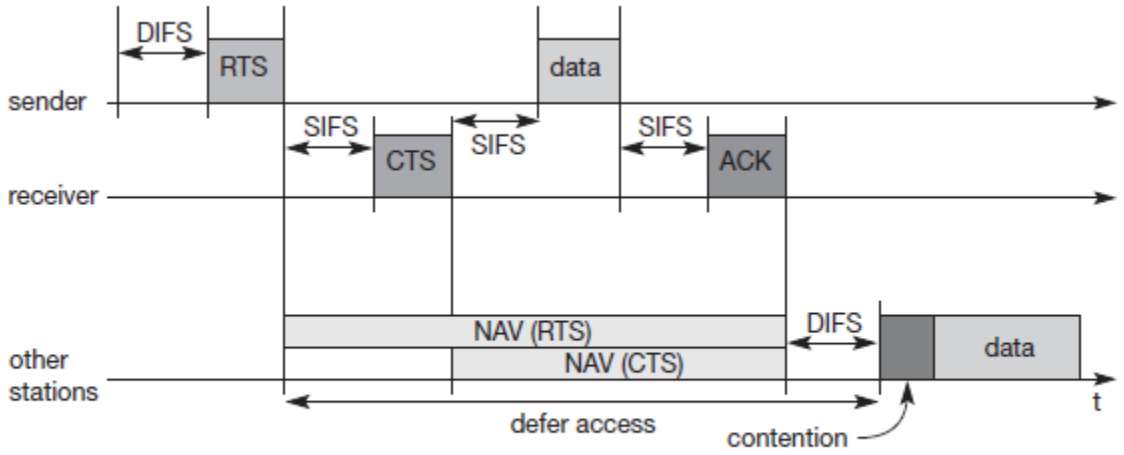


Figure: Solution of Hidden terminal in IEEE 802.11

RTS packet is received by all MTs in one-hop neighborhood of the sender:
– they set their network allocation vector (NAV);
– NAV specifies the earliest time when the station is permitted to attempt transmission.
• the intended receiver of a packet does the following:
– waits for SIFS (high priority!);
– response with clear-to-send (CTS) packet;
– CTS contains the duration field.
• CTS packet is received by all MTs in one-hop neighborhood of the receiver:
– they set their network allocation vector (NAV);
– if the set of stations receiving RTS and CTS are different, hidden terminals exist.

• All stations are informed and the medium is reserved for one sender exclusively;
• The sender starts its transmission after waiting for SIFS;
• The receiver receives packets, waits for SIFS and responds with ACK;
• The NAV in each node marks the medium as free.

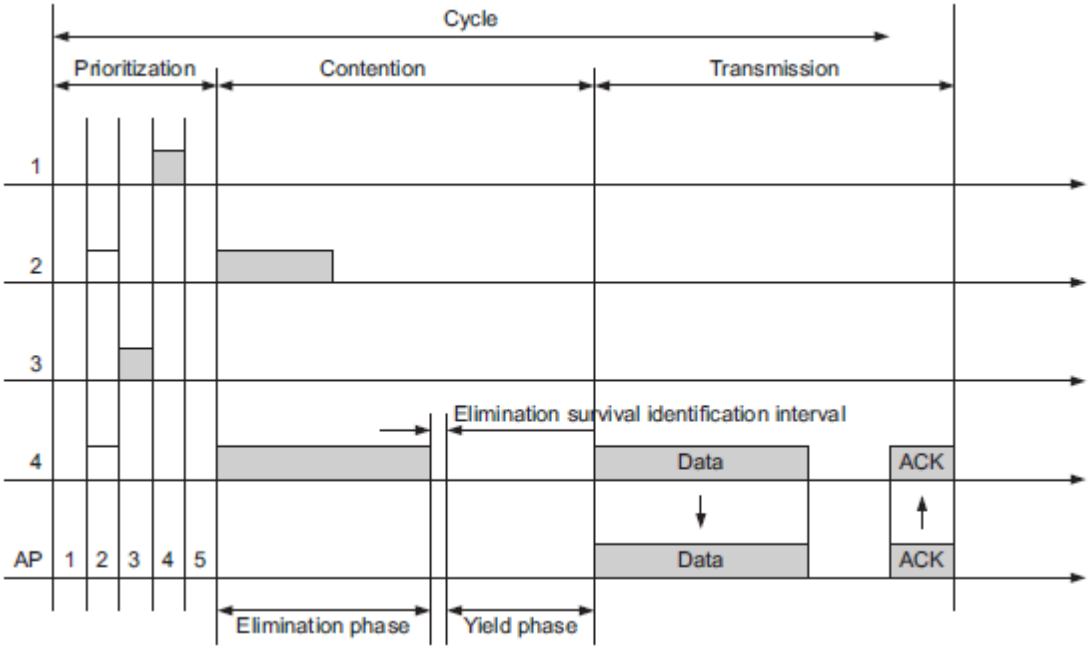
Solution in HyperLAN: The hyperLAN also supports 'channel access in the hidden elimination condition' to handle the problem of hidden terminals

- PRIORITIZATION: The aim of this phase is to detect nodes having packets with the highest CAM priority. Two stages:
    - priority detection: A node listens channel for a number of slots proportional to the CAM priority of its packet.
    - priority assertion : A node asserts its priority sending a signal in the slot corresponding to the packet priority.

Nodes having packets with low CAM priority detects nodes with the higher priority packets.

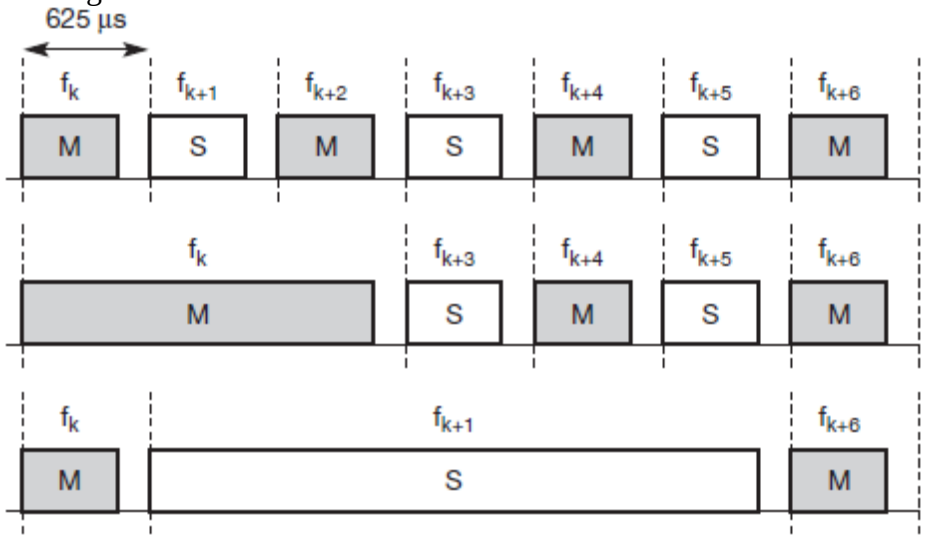
- CONTENTION: The aim is to eliminate as many nodes as possible to minimize the collision:
    - Elimination phase: In this phase
        - a node transmits signal for geometrically distributed number of slots (0:5k,k is the CAM);
        - it senses the media for one slot;

        - if transmissions in this slot are detected, a node stops contention process;
        - if no, it goes to yield phase.
    - Yield phase:
        - A node listens channel for a number of slots. If it is idle, the node is chosen for transmission.
- TRANSMISSION:
    - The successful delivery is acknowledged using ACK packets.



Solution in BLUETOOTH :

Remember that each device participating in a certain piconet hops at the same time to the same carrier frequency. If, for example, the master sends data at fk, then a slave may answer at fk+1. This scenario shows another feature of Bluetooth. **TDD** is used forvseparation of the transmission directions. The upper part of figure shows so-called **1-slot packets** as the data transmission uses one 625 μs slot. Within each slot the master or one out of seven slaves may transmit data in an alternating fashion.



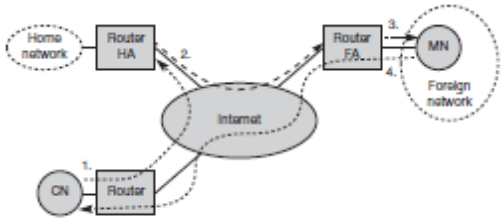
The control of medium access will be described later. Bluetooth also defines **3-slot** and **5-slot** packets for higher data rates (multi slot packets). If a master or a slave sends a packet covering

three or five slots, the radio transmitter remains on the same frequency. No frequency hopping is performed within packets. After transmitting the packet, the radio returns to the frequency required for its hopping sequence. The reason for this is quite simple: not every slave might receive a transmission (hidden terminal problem) and it can not react on a multi-slot transmission. Those slaves not involved in the transmission will continue with the hopping sequence. This behavior is important so that all devices can remain synchronized, because the piconet is uniquely defined by having the same hopping sequence with the same phase.

(b) What are the advantages and problems of forwarding mechanisms in Bluetooth networks regarding security, power saving, and network mobility? 12

SECTION-D

8. (a) List the entities of mobile IP and describe data transfer from mobile node and vice versa. Why and where is encapsulation needed? 10



Various entities are:

i. Mobile node (MN): A mobile node is an end-system or router that can change its point of attachment to the internet using mobile IP

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

iii. Home network: The home network is the subnet the MN belongs to with respect to its IP address. No mobile IP support is needed within the home network.

iv. Foreign network: The foreign network is the current subnet the MN visits and which is not the home network

v. Foreign agent (FA): The FA can provide several services to the MN during its visit to the foreign network. The FA can have the COA acting as tunnel endpoint and forwarding packets to the MN. The FA can be the default router for the MN. FAs can also provide security services because they belong to the foreign network as opposed to the MN which is only visiting. For mobile IP functioning, FAs are not necessarily needed. Typically, an FA is implemented on a router for the subnet the MN attaches to.

vi. Care-of address (COA): The COA defines the current location of the MN from an IP point of view. All IP packets sent to the MN are delivered to the COA, not directly to the IP address of the MN. Packet delivery toward the MN is done using a tunnel, as explained later. To be more precise, the COA marks the tunnel endpoint.

vii. Foreign agent COA: The COA could be located at the FA, i.e., the COA is an IP address of the FA. The FA is the tunnel end-point and forwards packets to the MN. Many MN using the FA can share this COA as common COA.

viii. Home agent (HA): The HA provides several services for the MN and is located in the home network. The tunnel for packets toward the MN starts at the HA. The HA maintains a location registry, i.e., it is informed of the MN's location by the current COA.

IP packet delivery to and from the MN : A correspondent node CN wants to send an IP packet to the MN.

step 1 : One of the requirements of mobile IP was to support hiding the mobility of the MN. CN does not need to know anything about the MN's current location and sends the packet as usual to the IP address of MN. This means that CN sends an IP packet with MN as a destination address and CN as a source address.

step 2: The internet, not having information on the current location of MN, routes the packet to the router responsible for the home network of MN. This is done using the standard routing mechanisms of the internet. The HA now intercepts the packet, knowing that MN is currently not in its home network. The packet is not forwarded into the subnet as usual, but encapsulated and tunnelled to the COA. A new header is put in front of the old IP header showing the COA as new destination and HA as source of the encapsulated packet.

step 3: The foreign agent now decapsulates the packet, i.e., removes the additional header, and forwards the original packet with CN as source and MN as destination to the MN. Again, for the MN mobility is not visible. It receives the packet with the same sender and receiver address as it would have done in the home network.

step 4: At first glance, sending packets from the MN to the CN is much simpler. The MN sends the packet as usual with its own fixed IP address as source and CN's address as destination. The router with the FA acts as default router and forwards the packet in the same way as it would do for any other node in the foreign network. As long as CN is a fixed node the remainder is in the fixed internet as usual. If CN were also a mobile node residing in a foreign network, the same mechanisms as described in steps 1 through 3 would apply now in the other direction.

(b) Write short note on mobile adhoc networks. Distinguish some of the adhoc routing protocols. 10

SOLUTION:

A mobile ad-hoc network (MANET) is an infrastructure less network, i.e. this type of network does not require big infrastructure like BTS, BSC, MSC etc as in the case of cellular systems. The mobile nodes in an MANET depend on their own transmission/receiving power and are used in a short range. These types of networks are established in emergency and where there is no infrastructure existing.

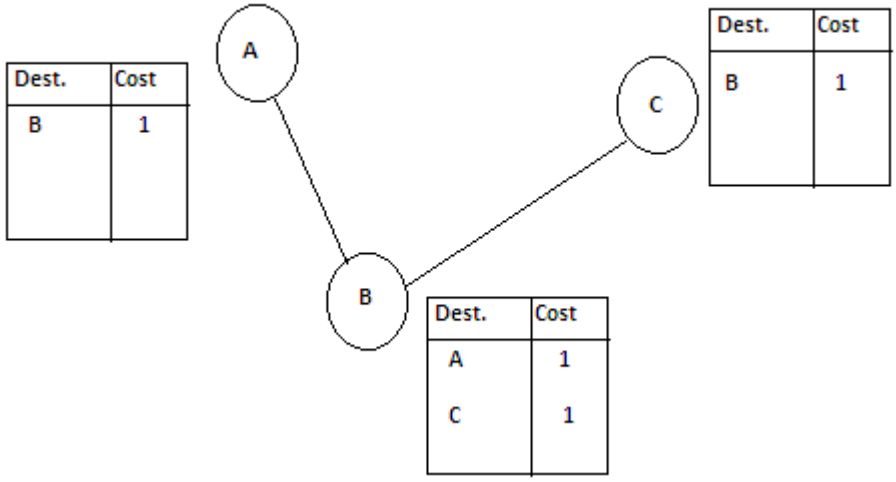
These networks should be mobile and use wireless communications. Examples for the use of such mobile, wireless, multi-hop ad-hoc networks, which are only called ad-hoc networks here for simplicity, are:

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.

Routing protocols:
Routing is needed to find a path between source and destination and to forward the packets appropriately. In wireless networks using an infrastructure, cells have been defined. Within a cell, the base station can reach all mobile nodes without routing via a broadcast. In the case of ad-hoc networks, each node must be able to forward data for other nodes. This creates many additional problems that are discussed in the following paragraphs. Some of the routing protocols are described below:
Distance Vector Routing(DVR):
Every node keep a maintain a routing table containing the following information:



Every node share their routing table with every other node in its visibility area. Thus the nodes will update their routing table and will contain information of every other node. The problem with this routing protocol is that there is a great amount of overhead of routing information and lead to congestion and packet drops, count-to-infinity in case of broken link, battery usage is high which is not desirable feature in MANET.

Destination sequence distance vector(DSDV):Some of the above problems are solved in DSDV protocol. This protocol add two things to the distance vector algorithm:
Sequence numbers: Each routing advertisement comes with a sequence number. Within ad-hoc networks, advertisements may propagate along many paths. Sequence numbers help to apply the advertisements in correct order. This avoids the loops that are likely with the unchanged distance vector algorithm.
● **Damping:** Transient changes in topology that are of short duration should not destabilize the routing mechanisms. Advertisements containing changes in the topology currently stored are therefore not disseminated further. A node waits with dissemination if these changes are probably unstable. Waiting time depends on the time between the first and the best announcement of a path to a certain destination.
The routing table of DSDV protocol is shown below:
Dynamic Source Routing:
The DVR, DSDV algorithms maintain routes between all nodes, although there may currently be no data exchange at all. This causes unnecessary traffic and prevents nodes from saving battery power. **Dynamic source routing (DSR)**, therefore, divides the task of routing into two separate problems:
● **Route discovery:** A node only tries to discover a route to a destination if it has to send something to this destination and there is currently no known route.

● **Route maintenance:** If a node is continuously sending packets via a route, it has to make sure that the route is held upright. As soon as a node detects problems with the current route, it has to find an alternative.

The basic principle of source routing is also used in fixed networks, e.g. token rings. Dynamic source routing eliminates all periodic routing updates and works as follows. If a node needs to discover a route, it broadcasts a route request with a unique identifier and the destination address as parameters. Any node that receives a route request does the following.

● If the node has already received the request (which is identified using the unique identifier), it drops the request packet.

● If the node recognizes its own address as the destination, the request has reached its target.

● Otherwise, the node appends its own address to a list of traversed hops in the packet and broadcasts this updated route request.

Using this approach, the route request collects a list of addresses representing a possible path on its way towards the destination. As soon as the request reaches the destination, it can return the request packet containing the list to the receiver using this list in reverse order. One condition for this is that the links work bi-directionally. If this is not the case, and the destination node does not currently maintain a route back to the initiator of the request, it has to start a route discovery by itself.

9. (a) Explain characteristics of TCP over 2.5/3G wireless networks. 10

The focus on 2.5G/3G for transport of internet data is important as already more than 1 billion people use mobile phones and it is obvious that the mobile phone systems will also be used to transport arbitrary internet data. The following characteristics have to be considered when deploying applications over 2.5G/3G wireless links:

i. **Data rates:** While typical data rates of today's 2.5G systems are 10–20 kbit/s uplink and 20–50 kbit/s downlink, 3G and future 2.5G systems will initially offer data rates around 64 kbit/s uplink and 115–384 kbit/s downlink. Typically, data rates are asymmetric as it is expected that users will download more data compared to uploading. Uploading is limited by the limited battery power. In cellular networks, asymmetry does not exceed 3–6 times, however, considering broadcast systems as additional distribution media (digital radio, satellite systems), asymmetry may reach a factor of 1,000. Serious problems that may reduce throughput dramatically are bandwidth oscillations due to dynamic resource sharing. To support multiple users within a radio cell, a scheduler may have to repeatedly allocate and deallocate resources for each user. This may lead to a periodic allocation and release of a high-speed channel.

ii. **Latency:** All wireless systems comprise elaborated algorithms for error correction and protection, such as forward error correction (FEC), check summing, and interleaving. FEC and interleaving let the round trip time (RTT) grow to several hundred milliseconds up to some seconds. The current GPRS standard specifies an average delay of less than two seconds for the transport class with the highest quality (see chapter 4).

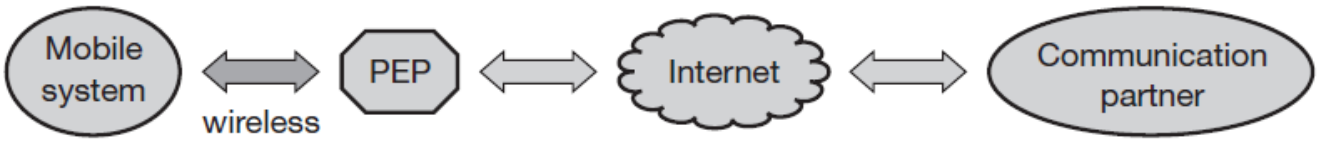
iii. **Jitter:** Wireless systems suffer from large delay variations or 'delay spikes'. Reasons for sudden increase in the latency are: link outages due to temporal loss of radio coverage, blocking due to high-priority traffic, or handovers. Handovers are quite often only virtually seamless with outages reaching from some 10 ms (handover in GSM systems) to several seconds (intersystem handover, e.g., from a WLAN to a cellular system using Mobile IP without using additional mechanisms such as multicasting data to multiple access points).

iv. **Packet loss:** Packets might be lost during handovers or due to corruption. Thanks to link-level retransmissions the loss rates of 2.5G/3G systems due to corruption are relatively low (but still

orders of magnitude higher than, e.g., fiber connections!). However, recovery at the link layer appears as jitter to the higher layers. Based on these characteristic

(b) Explain some performance enhancing proxies beneficial for wireless and mobile internet access. 10

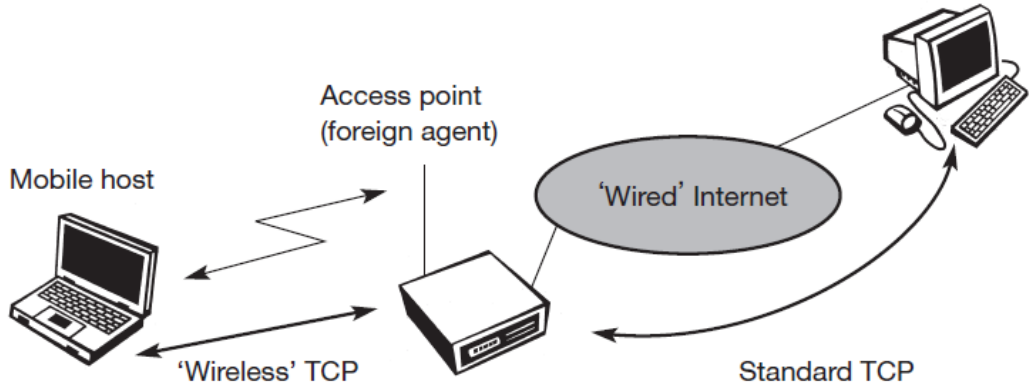
Performance Enhancing Proxies are used to to Mitigate Link-Related Degradations' and are also beneficial for wireless and mobile internet access.
Transport layer proxies : The transport layer proxies are 'snooping TCP' and 'indirect TCP'. The transport layer proxies are typically used for local retransmissions, 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:

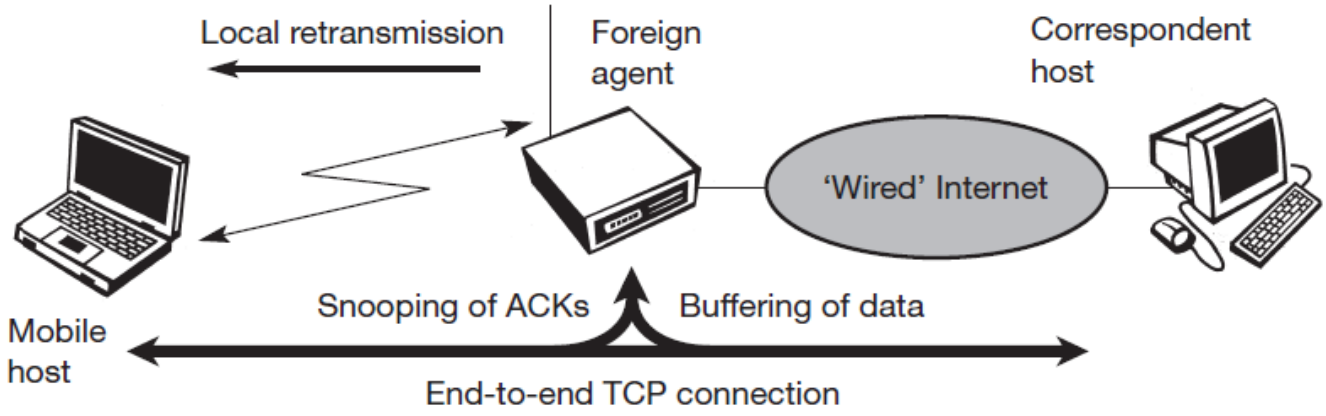
Indirect TCP:

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.



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