18CS702

Hall Ticket Number:

IV/IV B.Tech (Regular/Supplementary) DEGREE EXAMINATION

November, 2022 **Computer Science & Engineering**

Seventh Semester **Wireless Networks**

Time: Three Hours **Maximum:** 50 Marks

Answer Question No.1 compulsorily. (10X1 = 10 Marks)

Answer ONE question from each unit. (4X10=40 Marks)

1	a)	What is meant by spread spectrum?	CO1	L1	
	b)	List out any 2 features of FDMA.	CO1	L2	
	c)	List applications of Wireless networks.	CO1	L4	
	d)	What is handover?	CO2	L3	
	e)	Define wireless LAN	CO2	L2	
	f)	What is meant by mobile IP?	CO2	L1	
	g)	Differentiate Infra-red and Radio transmission.	CO3	L3	
	h)	What led to the development of Indirect TCP?	CO3	L1	
	i)	What are all the various flavors of TCP available?	CO4	L4	
	j)	Outline the challenging issues in ad hoc network maintenance.	CO4	L1	
		Unit –I			
2	a)	Explain about the historical background of Wireless Communications	CO1	L2	5M
	b)	Discuss in detail about spread spectrum techniques	CO1	L1	5M
		(OR)			
3	a)	What is modulation? Explain ASK with neat diagrams?	CO1	L3	5M
	b)	Compare FDMA,TDMA	CO1	L1	5M
		Unit –II			
4	a)	Explain in detail about mobile services defined by GSM.	CO2	L4	5M
	b)	Explain the following satellite applications. i. GPS. ii. Satellite Navigational system.	CO2	L2	5M
		(OR)			
5		What is GSM and explain the architecture of GSM System.	CO2	L3	10M
		Unit –III			
6	a)	Briefly explain about the system and protocol architecture of 802.11.	CO3	L1	5M
	b)	Explain in detail the Dynamic host configuration protocol.	CO3	L2	5M
		(OR)			
7		State the entities and terminologies used in Mobile IP along with tunneling and also explain the three types of encapsulation mechanisms used in mobile IP.	CO3	L1	10M
		Unit –IV			
8	a)	Discuss the architecture of wireless application protocol	CO4	L1	5M
	b)	Write short notes on time-out freezing and selective re-transmission	CO4	L1	5M
		(OR)			
9	a)	Explain the traditional TCP .What are the improvements that are made into the classical TCP?	CO4	L2	5M
	b)	Write about (i) Wireless Transport Layer Security (ii) Wireless Session protocol	CO4	L3	5M

Scheme

a) What is meant by spread spectrum?

Definition

In which a signal is transmitted in a bandwidth considerably greater than the frequency content of the original information.

b) List out any 2 features of FDMA.

Any 2 features

- Frequency division multiple access (FDMA) comprises all algorithms allocating frequencies to transmission channels according to the frequency division multiplexing (FDM) scheme.
- Allocation can either be fixed or dynamic.
- FDM is often used for simultaneous access to the medium by base station and mobile station in cellular networks.

c) List applications of Wireless networks.

Any 2 applications

Vehicles , Emergencies, Business, Replacement of wired networks, Infotainment and more, Location dependent services

d) What is handover?

Definition

A handover is a process in telecommunications and mobile communications in which a connected cellular call or a data session is transferred from one cell site (base station) to another without disconnecting the session.

e) Define wireless LAN

Definition

A wireless LAN (WLAN) is a wireless computer network that links two or more devices using wireless communication to form a local area network (LAN) within a limited area such as a home, school, computer laboratory, campus, or office building.

f) What is meant by mobile IP?

Definition

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

g) Differentiate Infra-red and Radio transmission.

Any 2 differences

Infrared	Radio
❑ uses IR diodes, diffuse light, multiple reflections (walls, furniture etc.)	❑ typically using the license free ISM band at 2.4 GHz
Advantages	Advantages
❑ simple, cheap, available in many mobile devices	❑ experience from wireless WAN and mobile phones can be used
❑ no licenses needed	❑ coverage of larger areas possible (radio can penetrate walls, furniture etc.)
❑ simple shielding possible	

h) What led to the development of Indirect TCP?

Importance

TCP performs poorly together with wireless links

TCP within the fixed network cannot be changed.

This led to the development of I-TCP which segments a TCP connection into a fixed part and a wireless part.

i) What are all the various flavours of TCP available?

Features

Congestion control

Slow start

Fast re-transmission

j) Outline the challenging issues in ad hoc network maintenance.

Any 2 issues

Limited wireless range.

Packet losses.

Energy conservation because of limited batteries.

Low-quality communications.

Hidden-node problem creates collision if two device try to communicate with same receiver.

Exposed-node problem.

Lack of security.

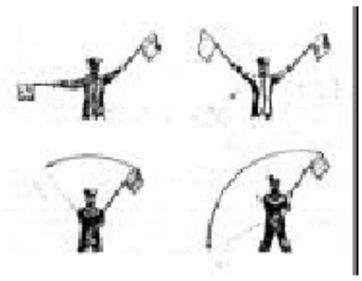
Unit –I

2. a) Explain about the historical background of Wireless Communications

Evolution -5M

Many people in history used light for communication

- heliographs, flags („semaphore"), ...
- 150 BC smoke signals for communication; (Polybius, Greece)
- 1794, optical telegraph, Claude Chappe



Here electromagnetic waves are of special importance:

- 1831 Faraday demonstrates electromagnetic induction
- J. Maxwell (1831-79): theory of electromagnetic Fields, wave equations (1864)
- H. Hertz (1857-94): demonstrates with an experiment the wave character of electrical transmission through space (1886, in Karlsruhe, Germany, at the location of today's University of Karlsruhe)

1895 Guglielmo Marconi

- first demonstration of wireless telegraphy (digital!)
- long wave transmission, high transmission power necessary (> 200kw)

1907 Commercial transatlantic connections

- huge base stations (30 100m high antennas)

1915 Wireless voice transmission New York - San Francisco

1920 Discovery of short waves by Marconi

- reflection at the ionosphere
- smaller sender and receiver, possible due to the invention of the vacuum tube (1906, Lee DeForest and Robert von Lieben)

1926 Train-phone on the line Hamburg - Berlin

- wires parallel to the railroad track

1928 many TV broadcast trials (across Atlantic, color TV, TV news)

1933 Frequency modulation (E. H. Armstrong)

1958 A-Netz in Germany

- analog, 160MHz, connection setup only from the mobile station, no handover, 80% coverage, 1971 11000 customers

1972 B-Netz in Germany

- analog, 160MHz, connection setup from the fixed network too (but location of the mobile station has to be known)
- available also in A, NL and LUX, 1979 13000 customer in D

1979 NMT at 450MHz (Scandinavian countries)

1982 Start of GSM-specification

- goal: pan-European digital mobile phone system with roaming

1983 Start of the American AMPS (Advanced Mobile Phone System, analog)

1984 CT-1 standard (Europe) for cordless telephones

1986 C-Netz in Germany

- analog voice transmission, 450MHz, hand-over possible, digital signaling, automatic location of mobile device
- still in use today (as T-C-Tel), services: FAX, modem, X.25, e-mail, 98% coverage

1991 Specification of DECT

- Digital European Cordless Telephone (today: Digital Enhanced Cordless Telecommunications)
- 1880-1900MHz, ~100-500m range, 120 duplex channels, 1.2Mbit/s data transmission, voice encryption, authentication, up to several 10000 user/km^2, used in more than 40 countries

1992 Start of GSM

- in D as D1 and D2, fully digital, 900MHz, 124 channels
- automatic location, hand-over, cellular
- roaming in Europe - now worldwide in more than 100 countries
- services: data with 9.6kbit/s, FAX, voice, ...

1994 E-Netz in Germany

- GSM with 1800MHz, smaller cells, supported by 11 countries
- as Eplus in D (1997 98% coverage of the *population*)

1996 HiperLAN (High Performance Radio Local Area Network)

- ETSI, standardization of type 1: 5.15 - 5.30GHz, 23.5Mbit/s
- recommendations for type 2 and 3 (both 5GHz) and 4 (17GHz) as wireless ATM-networks (up to 155Mbit/s)

1997 Wireless LAN - IEEE802.11

- IEEE-Standard, 2.4 - 2.5GHz and infrared, 2Mbit/s
- already many products (with proprietary extensions)

1998 Specification of GSM successors

- for UMTS (Universal Mobile Telecommunication System) as European proposals for IMT-2000

Iridium

- 66 satellites (+6 spare), 1.6GHz to the mobile phone

b) Discuss in detail about spread spectrum techniques

Definition -2M spread spectrum techniques -3M

Problem of radio transmission:

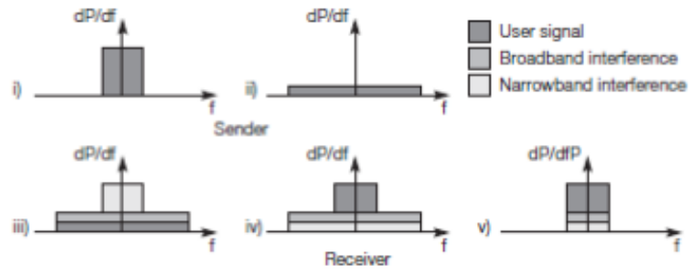
frequency dependent fading can wipe out narrow band signals for duration of the interference

Solution:

- spread the narrow band signal into a broad band signal using a special code
- protection against narrow band interference

The following Figure shows

i) Shows an idealized narrowband signal from a sender of user data (here power density dP/df versus frequency f). • The sender now spreads the signal in step ii), i.e., converts the narrowband signal into a broadband signal. The energy needed to transmit the signal (the area shown in the diagram) is the same, but it is now spread over a larger frequency range. The power level of the spread signal can be much lower than that of the original narrowband signal without losing data.



step iii). During transmission, narrowband and broadband interference add to the signal The sum of interference and user signal is received. The receiver now knows how to despread the signal, converting the spread user signal into a narrowband signal again, while spreading the narrowband interference and leaving the broadband interference. In step v) the receiver applies a bandpass filter to cut off frequencies left and right of the narrowband signal. Finally, the receiver can reconstruct the original data because the power level of the user signal is high enough, i.e., the signal is much stronger than the remaining interference.

Spreading the spectrum can be achieved in two different ways.

- Direct sequence spread spectrum
- Frequency hopping spread spectrum

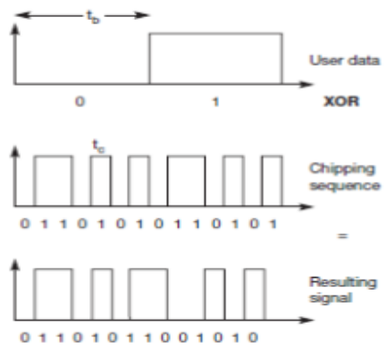
Direct Sequence Spread Spectrum:-

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

The example shows that the result is either the sequence 0110101 (if the user bit equals 0) or its complement 1001010 (if the user bit equals 1). While each user bit has a duration tb, the chipping sequence consists of smaller pulses, called chips, with a duration tc.

If the chipping sequence is generated properly it appears as random noise: this sequence is also sometimes called **pseudo-noise** sequence.

The **spreading factor** s = tb/tc determines the bandwidth of the resulting signal. If the original signal needs a bandwidth w, the resulting signal needs s·w after spreading.



DSSS need additional components as shown in the simplified block diagrams in below figure

The **first step in a DSSS transmitter, the spreading of the user data with the chipping sequence (digital modulation)**.

Assuming for example a user signal with a bandwidth of 1 MHz. **Spreading with the above 11-chip Barker code would result in a signal with 11 MHz bandwidth**. The radio carrier then shifts this signal to the carrier frequency (e.g., 2.4 GHz in the ISM band).

Frequency Hopping Spread Spectrum :-

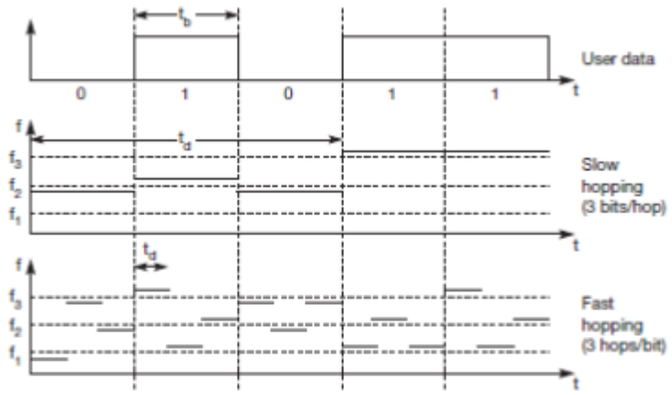
For frequency hopping spread spectrum (FHSS) systems, the total available bandwidth is split into many channels of smaller bandwidth plus guard spaces between the channels.

Transmitter and receiver stay on one of these channels for a certain time and then hop to another channel.

This system implements FDM and TDM.

The pattern of channel usage is called the **hopping sequence**, the time spend on a channel with a certain frequency is called the **dwell time**.

FHSS comes in two variants, **slow** and **fast hopping**.



In **slow hopping**, the transmitter uses one frequency for several bit periods. Above figure shows five user bits with a bit period tb. Performing slow hopping, the transmitter uses the frequency f2 for transmitting the first three bits during the dwell time td. Then, the transmitter hops to the next frequency f3. Slow hopping systems are typically cheaper and have relaxed tolerances, but they are not as immune to narrowband interference as fast hopping systems.

For **fast hopping** systems, the transmitter changes the frequency several times during the transmission of a single bit. In the above figure, the transmitter hops three times during a bit period. Fast hopping systems are more complex to implement because the transmitter and receiver have to stay synchronized within smaller tolerances to perform hopping at more or less the same points in time. However, these systems are much better at overcoming the effects of narrowband interference and frequency selective fading as they only stick to one frequency for a very short time.

The below Figures show simplified block diagrams of FHSS transmitters and receivers respectively.

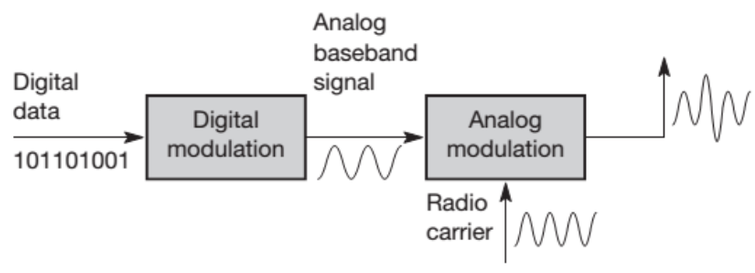
OR

3. a) What is modulation? Explain ASK with neat diagrams?

Definition -1M ASK Definition -1M diagrams-1.5M Explanation-1.5M

The following diagram shows a simplified block diagram of a radio transmitter for digital data.

Figure 2.21 Modulation in a transmitter



The first step is the digital modulation of data into the analog baseband signal.

The analog modulation then shifts the center frequency of the analog signal up to the radio

carrier. This signal is then transmitted via the antenna. The receiver receives the analog radio signal via its antenna and demodulates the signal into the analog baseband signal with the help of the known carrier. This would be all that is needed for an analog radio tuned in to a radio station.

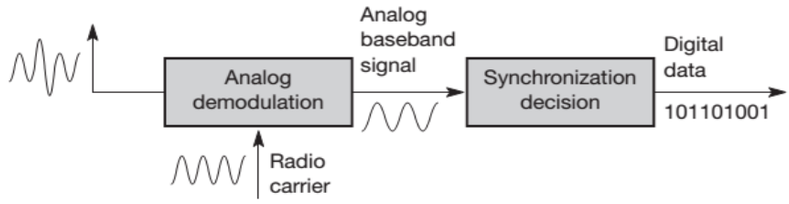


Figure 2.22
Demodulation and data reconstruction in a receiver

For digital data, another step is needed. Bits or frames have to be detected, i.e., the receiver must synchronize with the sender. How synchronization is achieved, depends on the digital modulation scheme. After synchronization, the receiver has to decide if the signal represents a digital 1 or a 0, reconstructing the original data.

Amplitude shift keying

Amplitude shift keying, the most simple digital modulation scheme.

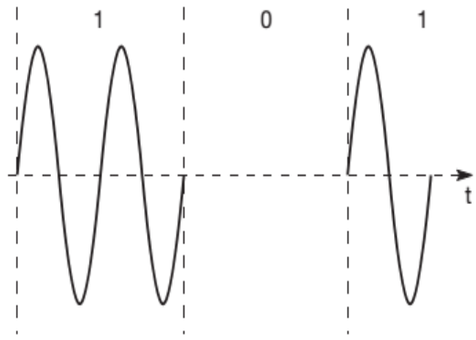


Figure 2.23
Amplitude shift keying (ASK)

It has two binary values, 1 and 0, are represented by **two different amplitudes**.

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, constant **amplitude** cannot be guaranteed, so ASK is typically **not** used for **wireless radio transmission**.

b) Compare FDMA,TDMA

Any 5 Comparison

Approach	SDMA	TDMA	FDMA	CDMA
Idea	segment space into cells/sectors	segment sending time into disjoint time-slots, demand driven or fixed patterns	segment the frequency band into disjoint sub-bands	spread the spectrum using orthogonal codes
Terminals	only one terminal can be active in one cell/one sector	all terminals are active for short periods of time on the same frequency	every terminal has its own frequency, uninterrupted	all terminals can be active at the same place at the same moment, uninterrupted
Signal separation	cell structure, directed antennas	synchronization in the time domain	filtering in the frequency domain	code plus special receivers
Advantages	very simple, increases capacity per km²	established, fully digital, flexible	simple, established, robust	flexible, less frequency planning needed, soft handover
Disadvantages	inflexible, antennas typically fixed	guard space needed (multipath propagation), synchronization difficult	inflexible, frequencies are a scarce resource	complex receivers, needs more complicated power control for senders
Comment	only in combination with TDMA, FDMA or CDMA useful	standard in fixed networks, together with FDMA/SDMA used in many mobile networks	typically combined with TDMA (frequency hopping patterns) and SDMA (frequency reuse)	higher complexity, lowered expectations; integrated with TDMA/FDMA

Unit –II

4. a) Explain in detail about mobile services defined by GSM?

Explanation-5M

Mobile Services :-

- GSM provide 3 types of services
- Bearer Services
- Tele Services
- Supplementary Services

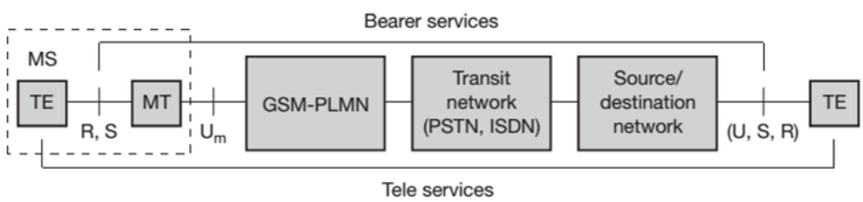


Figure 4.3 Bearer and tele services reference model

Bearer Services :-

GSM mainly focus on data transmission services.

Various data transmission services offered by GSM are

- Transparent bearer service
- Non-transparent bearer service

Transparent bearer service:-

- It uses the functions of the physical layer to transmit data.
- It uses Forward Error Correction (FEC) to increase the transmission quality.

Non - Transparent bearer service :-

- It uses the functions of the data link layer and Network layer.
- It uses error control and flow control techniques for data transmission.

Tele services :-

GSM mainly focus on voice oriented tele services.

Various tele services offered by GSM are

- Telephony
- Emergency Number
- Short Message Services (SMS)
- Enhanced Message Services (EMS)
- Multimedia Message Services (MMS)
- Group 3 Fax

Telephony :-

Provides High Quality data transmission.

Emergency Number :-

The same number can be used throughout the country. This service is mandatory for all providers and free of charge. This connection is also has the highest priority pre-empting other connections and will automatically be set up with the closest emergency centre.

Short Message Service (SMS) :-

Provides transmission of messages up to 160 characters.

Enhanced Message Service (EMS) :-

Provides transmission of messages up to 760 characters, transmission of animated pictures, small images, ring tones etc.

Multimedia Message Service (MMS):-

Provides transmission of larger pictures, shot videos etc.

Group 3 fax :-

Provides non - tele services i.e. fax data.

Supplementary Services :-

In addition to Bearer and Tele services there exists Supplementary services like

User Identification

Call forwarding

Blocking a call

Conference call

Locking a Mobile terminal

b) Explain the following satellite applications. i. GPS. ii. Satellite Navigational system.

GPS -3M Satellite Navigational system-2M

Global Positioning System (GPS) is a navigation system based on satellite. It has created the revolution in navigation and position location. It is mainly used in positioning, navigation, monitoring and surveying applications.

The major **advantages** of satellite navigation are real time positioning and timing synchronization. That's why satellite navigation systems have become an integral part in most of the applications, where mobility is the key parameter.

A complete operational GPS space segment contains twenty-four satellites in MEO. These satellites are made into six groups so that each group contains four satellites. The group of four satellites is called as one **constellation**. Any two adjacent constellations are separated by 60 degrees in longitude.

The **orbital period** of each satellite is approximately equal to **twelve hours**. Hence, all satellites revolve around the earth two times on every day. At any time, the GPS receivers will get the signals from at least four satellites.

GPS Codes and Services

Each GPS satellite transmits two signals, **L_1 and L_2** are of different frequencies. **Trilateration** is a simple method for finding the position (Latitude, Longitude, Elevation) of GPS receiver. By using this method, the position of an unknown point can be measured from three known points

GPS Codes

Following are the two types of GPS codes.

- Coarse Acquisition code or C/A code
- Precise code or P code

The signal, L_1 is modulated with 1.023 Mbps pseudo random bit sequence. This code is called as Coarse Acquisition code or **C/A code** and it is used by the public.

The signal, L_2 is modulated with 10.23 Mbps pseudo random bit sequence. This code is called as Precise code or **P code** and it is used in military positioning systems. Generally, this P code is transmitted in an encrypted format and it is called as **Y code**

The P code gives better measurement accuracy when compared to C/A code, since the bit rate of P code is greater than the bit rate of C/A code.

GPS Services

Following are the two types of services provided by GPS.

- Precise Positioning Service (PPS)
- Standard Positioning Service (SPS)

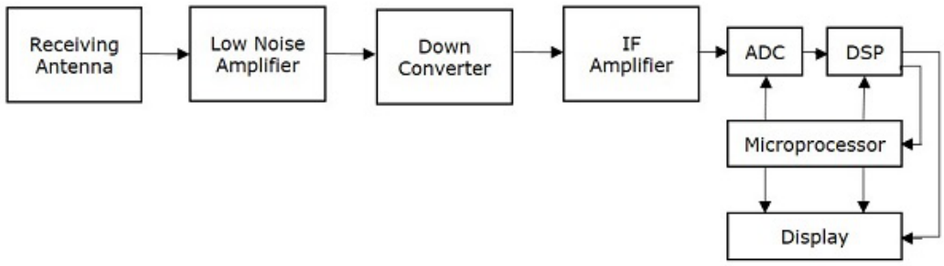
PPS receivers keep tracking of both C/A code and P code on two signals, L_1 and L_2. The Y code is decrypted at the receiver in order to obtain P code.

SPS receivers keep tracking of only C/A code on signal, L_1.

GPS Receiver

There exists only one-way transmission from satellite to users in GPS system. Hence, the individual user does not need the transmitter, but only a **GPS receiver**. It is mainly used to find the accurate location of an object. It performs this task by using the signals received from satellites.

The **block diagram** of GPS receiver is shown in below figure.



OR

5. a) What is GSM and explain the architecture of GSM System.

Definition -1M diagrams-3M Explanation-6M

GSM is the most successful digital mobile telecommunication system. It was introduced in 1980 by Europe companies like Nokia, Motorola etc. The primary goal of GSM was to provide,

Mobile phone system that allows users to roam throughout the country.

Data and voice services compatible to ISDN or PSTN systems.

GSM is the second generation system replacing the first generation analog systems.

GSM contains FDMA and TDMA. GSM can operate at 3 frequency ranges GSM 900, GSM 1800, GSM 1900.

<u>System Architecture :-</u>

A GSM system consists of 3 sub-systems

Radio Sub System (RSS)

Network and Switching Sub system (NSS)

Operation Sub System (OSS)

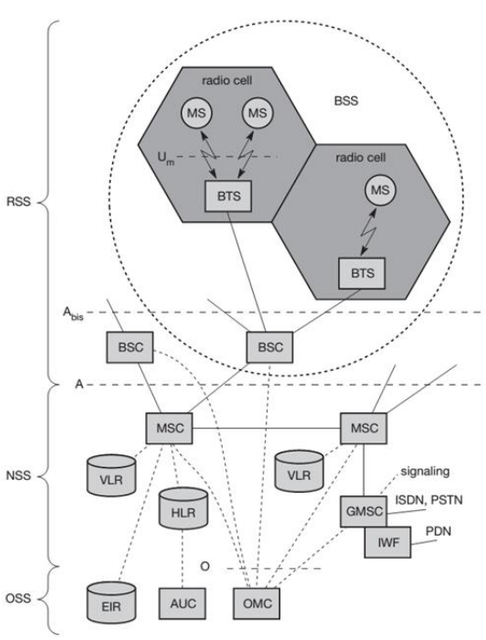


Figure 4.4
Functional architecture of a GSM system

The Radio Station Subsystem (RSS) is used for receiving signals from Base station. The Network Switching Subsystem (NSS) is used for switching from one Network to another Network. The Operating Support Subsystem (OSS) is used for handling the complete operating setup of mobile device.

The RSS and NSS is connected via "A" interface. The NSS and OSS is connected via "O" interface.

Radio Station Subsystem (RSS) :-

Radio Station Subsystem contains all radio specific entities. i.e. Mobile Stations (MS) and Base Station Subsystems (BSS).

Base Station Subsystem (BSS) :-

GSM consists of many BSSs and those are controlled by Base Station Controller (BSC).

BSS provides functions like

- Maintaining radio connections to Mobile Station.
- Coding/Decoding of voice.
- BSS contains several BTSs.

Base Transceiver Station (BTS) :-

It contains all radio equipment like antennas, signal processing, amplifiers required during radio transmission.

BTS can form radio cell and it is connected to the MS via Um interface. Um interface provides mechanisms for wireless transmission(TDMA, FDMA etc).

BTS connected to BSC via Abis interface contains 16 or 64 Kbits/sec connections.

Base Station Controller (BSC) :-

BSC basically manages the BTSs.

It reserves radio frequencies, handover from one BTS to another with in the BSS.

It multiplexes radio channels on to the fixed network at the A interface.

Mobile Station (MS) :-

It contains all user equipment and software needed for communication with in a network.

It contains Subscriber Identity Module (SIM) which stores all user specific data related to GSM.

MS can be identified by the via the IMEI (International Mobile Equipment Identity).

SIM provides user-specific mechanisms like charging and authentication etc.

IMEI provides device-specific mechanisms like theft protection etc.

SIM card contains

- Card – type
- List of subscriber services
- Personal Identity Number (PIN)
- PIN Unblocking Key (PUK)
- Authentication Key (Ki)
- IMSI (International Mobile Subscriber Identity)

Network Switching Subsystem (NSS) :-

It is the heart of GSM system.

It performs handover between different BSS and includes functions like worldwide localization users, support charging, accounting, roaming of users between different providers in different countries.

NSS contains

- Mobile Service Switching Center (MSC)

Home Location Register (HLR)

Visitors Location Register (VLR)

Mobile Service Switching Center (MSC) :-

MSC manages all BSCs in a geographical region via A interface.

MSC contains

GMSC (Gateway MSC) :- By using GMSC, MSC connects to all PSTN and ISDN networks.

IWF (Internetworking Functions):- By using IWF, MSC connects to all PDN (Public Data Networks) such as X.25.

SS7 (Standard Signalling System No.7):- By using SS7, MSC handles all signalling needed for connection setup, connection release and handover of connections to other MSCs.

MSC also performs functions needed for supplementary services such as call forwarding, conference call, blocking call, user identification etc.

Home Location Register (HLR) :-

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

It contains user's static information like Mobile Subscriber ISDN number (MSISDN), subscribed services (call forwarding, roaming restrictions, GPRS) and International Mobile Subscriber Identity (IMSI).

It contains the dynamic information like Location Area (LA) of MS, Mobile Subscriber Roaming Number (MSRN), the current VLR and MSC.

Visitor Location Register (VLR) :-

VLR is the most important database in GSM system as it stores all important information needed for the MS users currently in LA that is associated to the MSC. i.e. used to track the location of a user.

If a new MS comes into an LA the VLR is responsible for, it copies all relevant information for this user from the HLR.

Operating Support Subsystem (OSS) :-

It contains the necessary functions for network operation and maintenance.

It contains

OMC (Operation and Maintenance Center):-

It monitors and controls all other network entities via 'O' interface.

OMC can handle traffic monitoring, status report of network entities, subscriber and security management.

Authentication Center (AuC):-

Authentication Center (AuC) has been defined to protect user identity and data transmission.

Equipment Identity Register (EIR) :-

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

The EIR contains a list of valid IMEIs (white list) and list of malfunctioning devices (gray list)

Unit –III

6. a) Briefly explain about the system and protocol architecture of 802.11.

Architecture -3M **Explanation-2M**

Wireless Networks can exhibit two different basic system architectures

Infrastructure based architecture.

Adhoc based architecture.

Infrastructure Base Architecture :-

The following are the components used in this architecture.

Station (STAi) :- stations are nothing but mobile nodes.

Access Point (AP) :- stations are connected to Access Points.Stations are terminals with access mechanisms to wireless medium and radio contact to the AP.

Basic Service Set (BSS) :- The stations and AP are within the same radio coverage for a BSS.

Extended Service Set (ESS) :- Several BSSs are connected thorough Access Points, All BSSs are within the ESS.

Two BSSs are connected via a distribution system.

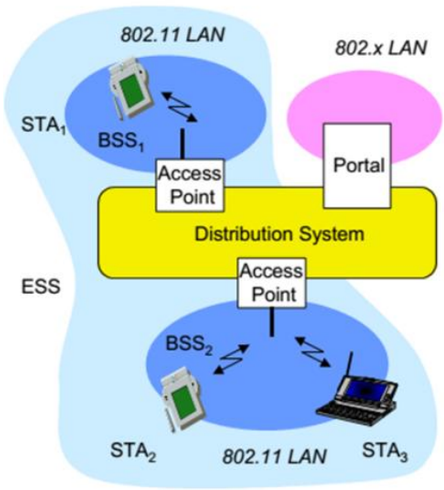
A Distribution System connects several BSSs via Access Points to form a single network and that network is called as Extended Service Set (ESS) Network.

Each Network has its own identifier called ESSID.

ESSID is the name of the network which is used to separate different networks.

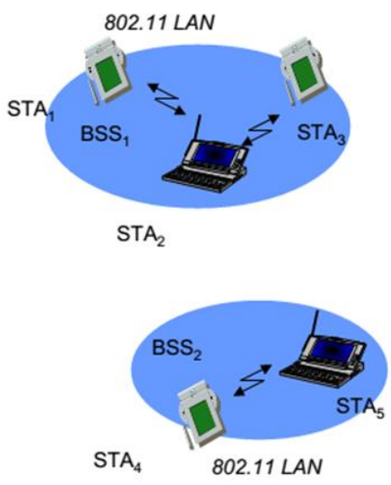
Without knowing ESSID it is not possible to participate in WLAN

Portal : Bridge to a Wired Network.



Adhoc Based Architecture :-

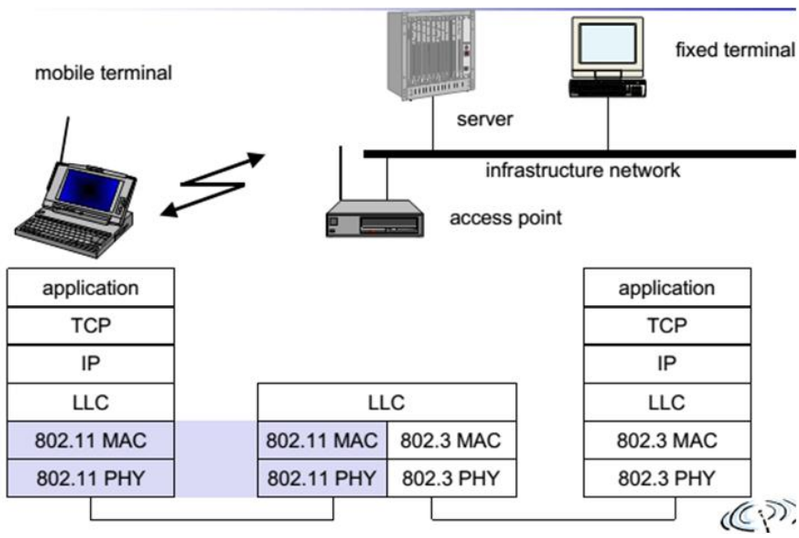
In this case, Independent BSS (IBSS) comprise group of stations using same radio frequency.



Stations STA1 , STA2 and STA3 are in IBSS1, STA4 and STA5 are in IBSS2.

This means for example that STA3 can communicate directly with STA2 but not with STA5.

Protocol Architecture :-



IEEE 802.11 wireless LAN connected to a switched ethernet 802.3 via switch. Applications running on source and destination systems, they do not know what happening inside the network apart from lower band width.

Both wireless and wired nodes have same higher layers (Application, Transport and Network layers).

LLC in the data link layer covers the difference of the Medium Access Control layers need for different media.

Physical Layer is subdivided into

Physical Layer Convergence Protocol (PLCP).

Physical Medium Dependent (PMD) sub layer.

PLCP provides a carrier signal, called Clear Channel Assessment (CCA) provides a PHY common Service Access Point (SAP) independent of the transmission technology.

PMD handles modulation and encoding/decoding of signals.

b) Explain in detail the Dynamic host configuration protocol.

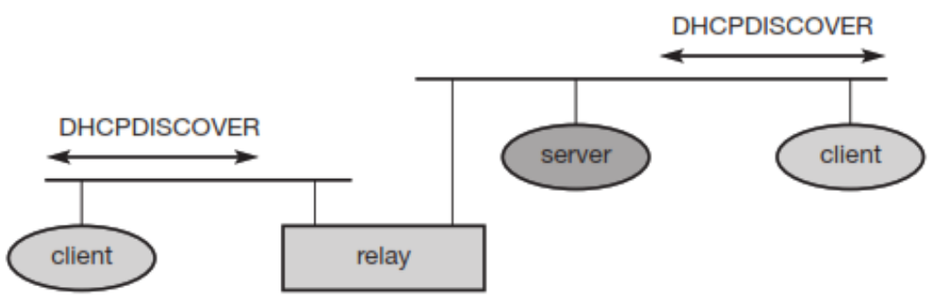
Explanation-5M

Dynamic Host Configuration Protocol

It is a method for assigning Internet Protocol (IP) addresses permanently or to individual computers in an organization's network.

DHCP lets a network administrator supervise and distribute IP addresses from a central point and automatically sends a new IP address when a computer is plugged into a different place in the network.

DHCP is based on a client/server model as shown in the following figure.



DHCP clients send a request to a server (DHCPDISCOVER in the example) to which

the server responds. A client sends requests using MAC broadcasts to reach all devices in the LAN. A DHCP relay might be needed to forward requests across inter-working units to a DHCP server.

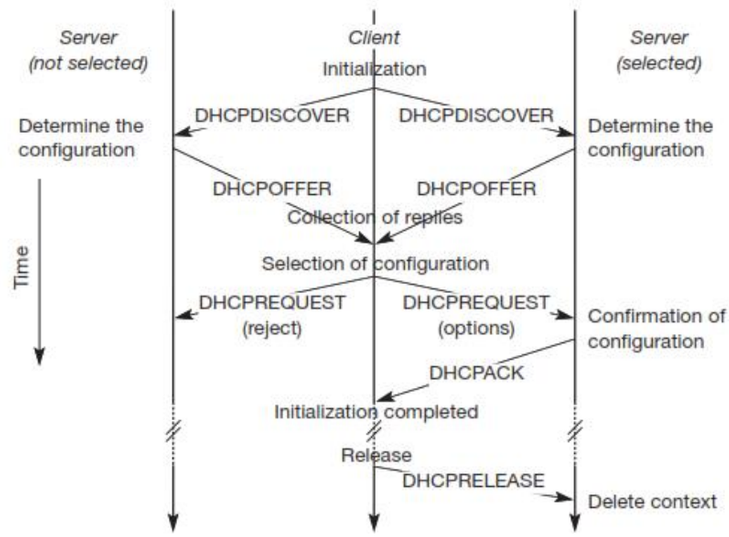


Figure 8.18
Client initialization via DHCP

The figure shows one client and two servers.

As described above, the client broadcasts a DHCPDISCOVER into the subnet.

There might be a relay to forward this broadcast. In the case shown, two servers receive this broadcast and determine the configuration they can offer to the client. One example for this could be the checking of available IP addresses and choosing one for the client. Servers reply to the client's request with DHCPOFFER and offer a list of configuration parameters.

The client can now choose one of the configurations offered.

The Client in turn replies to the servers, accepting one of the configurations and rejecting the others using DHCPREQUEST.

If a server receives a DHCPREQUEST with a rejection, it can free the reserved configuration for other possible clients.

The server with the configuration accepted by the client now confirms the configu- ration with DHCPACK.

This completes the initialization phase.

If a client leaves a subnet, it should release the configuration received by the server using DHCPRELEASE.

Now the server can free the context stored for the client and offer the configuration again.

The configuration a client gets from a server is only leased for a certain amount of time, it has to be reconfirmed from time to time. Otherwise the server will free the configuration. This timeout of configuration helps in the case of crashed nodes or nodes moved away without releasing the context.

OR

7. a) State the entities and terminologies used in Mobile IP along with tunneling and also explain the three types of encapsulation mechanisms used in mobile IP.

entities and terminologies -4M Explanation-6M

Entities and Terminology of Mobile IP**:-**

The following are the different components of Mobile IP.

Mobile Node (MN)

Correspondent Node (CN)

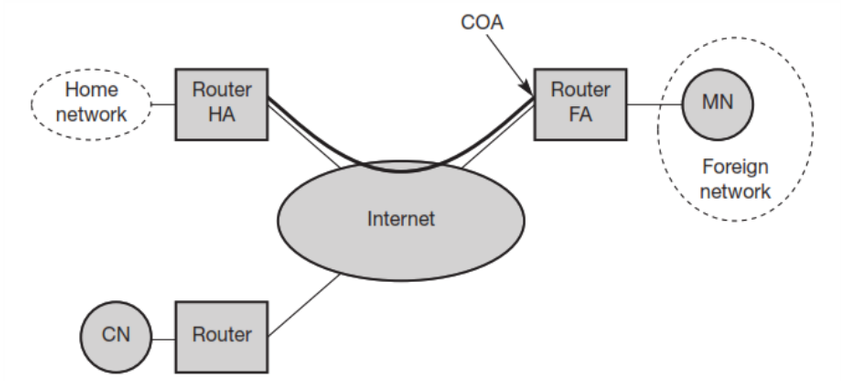
Home Network

Foreign Network

Foreign Agent

Care - Of - Address

Home Agent



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 without changing its IP address.

Correspondent Node (CN) :- [Other Device for communication. i.e. server]

Mobile Node (MN) needs at least one partner for communication.

CN represents this partner for MN.

The CN can be fixed or Mobile node.

Home Network :-

Home Network is the subnet in which the MN belongs to with respect to its IP address.

Foreign Network :-

Foreign Network is the current subnet in which the MN visits and which is not in the home network.

Foreign Agent (FA) :-

When MN is in Foreign Network it provides several services like

It acts as default router for MN.

It has COA, acting as tunnel end point forwarding packets to Mobile Node.

It also provides security services.

Care - Of - Address (COA) :-

Defines the current location of Mobile Node (MN) in terms of IP addresses.

All IP packets sent to the MN are delivered to the COA, not directly to the IP addresses of MN.

COA marks the tunnel end-point i.e. addresses where packets exit the tunnel.

There are 2 different possibilities for the location of COA.

Foreign Agent COA :- The COA could be located at the foreign agent. i.e. COA is the IP address of FA.

Co-located COA :- MN requires temporary IP address that address acts as COA.

Home Agent (HA) :-

When MN is in Home Network it provides several services like

Tunnel for packets toward the MN starts at the HA.

HA maintain a location registry i.e. it is informed of the MN's location by the current COA.

<u>Tunnelling and Encapsulation</u> :-

Tunnelling is a mechanism used for forwarding data packets in between Home agent (Tunnel Entry) and Foreign Agent (Tunnel end point).

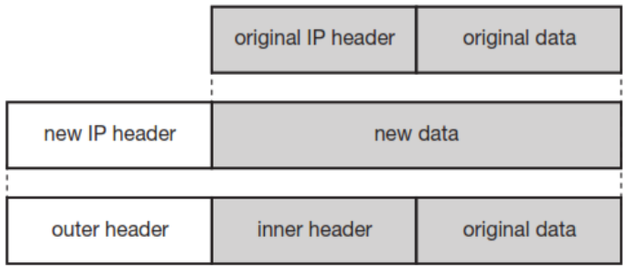
Tunnelling is achieved by encapsulation.

Encapsulation is the mechanism of taking a packet consisting of packet header and data

putting into the data part of a new packet.

The reverse operation taking a packet out of the data part of another packet is called as decapsulation.

Encapsulation and decapsulation takes place when a packet is transferred from higher to lower layers.



There are different ways of encapsulation needed for the tunnel between the HA and COA.

IP-in-IP Encapsulation

Minimal Encapsulation

Generic Routing Encapsulation

IP-in-IP Encapsulation :-

The following diagram shows a packet inside the tunnel by using IP-in-IP encapsulation

ver.	IHL	DS (TOS)	length
IP identification		flags	fragment offset
TTL	*IP-in-IP*	IP checksum	
IP address of HA			
Care-of address of COA			
ver.	IHL	DS (TOS)	length
IP identification		flags	fragment offset
TTL	lay. 4 prot.	IP checksum	
IP address of CN			
IP address of MN			
TCP/UDP/ … payload			

The fields of Outer Header are set as follows:

Ver : it contains value 4 for IPV4 version.
IHL (Internet Header Length) :- Length of the outer header in 32 bit words.
DS(TOS)[Type Of Service] :- it just copied from the inner header.
Length :- Length of the encapsulated packet.
TTL :- must be high enough so that packet can reach the tunnel end point.
Next field is the type of protocol is used in the IP Payload with IP-in-IP and this field is set to 4.
IP checksum : used for error detection and error correction.
IP address of HA :- tunnel entry point which is source address.
Care-of-address of COA :- tunnel end point which is destination address.
If no options follow the outer header, the inner header starts with the same fields as just explained.
This header remains almost unchanged during encapsulation, thus showing the original sender CN and receiver MN of the packet.
The only change is TTL which is decremented by 1.

Minimal Encapsulation :-

Several fields are redundant in IP-in-IP encapsulation.

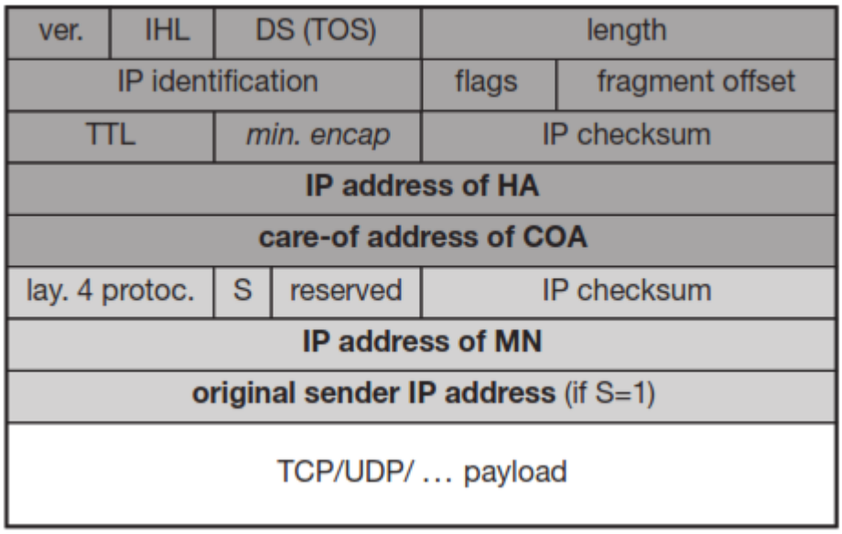
In order to remove redundancy minimal encapsulation is used.

The minimal encapsulation is an optional encapsulation method for mobile IP.

The value for Minimal encapsulation protocol is 55.

The inner header is different for minimal encapsulation

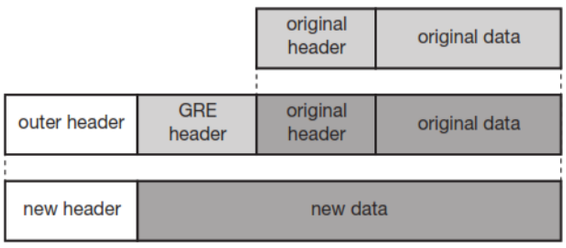
Minimal encapsulation does not work with already fragmented packets.



Generic Routing Encapsulation (GRE) :-

While IP-in-IP encapsulation and minimal encapsulation work only for IP, Generic Routing Encapsulation (GRE) supports another network layer protocol including IP.

Generic Routing Encapsulation (GRE) allows the encapsulation of packets of one protocol suite into the payload portion of a packet of another protocol suite.

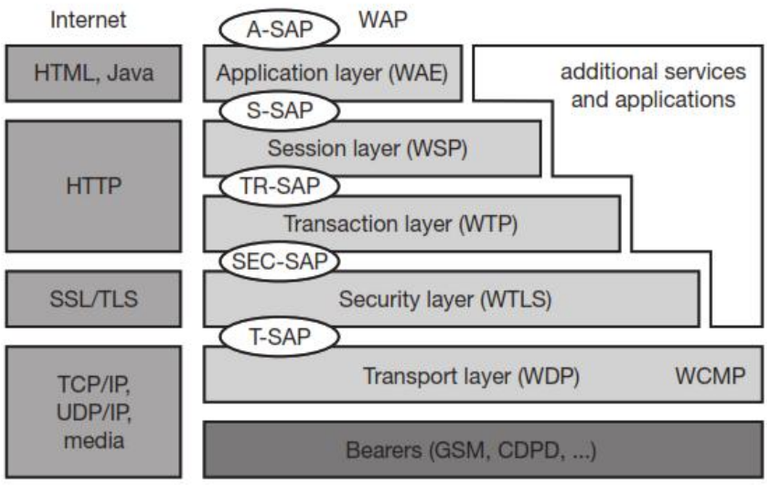


Unit –IV

8. a) Discuss the architecture of wireless application protocol

Architecture -2M Explanation-3M

Wireless Application Layer Protocol Architecture:-



WAP protocol stack is divided into 5 layers:

Application Layer(WAE)

Session Layer(WSP)

Transaction Layer(WTP)

Security Layer(WTLS)

Transport Layer(WDP)

Application Layer (WAE-Wireless Application Environment):-

It contains mobile device specifications and content development programming languages like WML and WML script.

It is general purpose environment based on combination of WWW and mobile telephony technologies.

Its primary goal is to develop a frame work that allows operators and service providers can able to build applications that can reach wide variety of wireless platforms.

Session Layer (WSP - Wireless Session layer Protocol):-

It provides reliable and organized exchange of content between client and server.

It provides fast connection suspension and reconnection.

It also supports asynchronous requests.

Transaction Layer (WTP - Wireless Transaction Protocol):-

It offers transaction support.

WTP is a part of TCP/IP which provides a simplified protocol suitable for low bandwidth wireless stations.

Each transaction has unique identifiers, acknowledgements, duplicate removal and retransmission.

It has no security mechanisms and no explicit connection set-up.

Security Layer [WTLS - Wireless Transport Layer Security]:-

It is based on Transport Layer Security (TLS).

It provides data integrity, privacy, authentication, Denial-of-Service Protection.

Transport Layer (WDP - Wireless Datagram Protocol):-

It provides application addressing port numbers, Optional segmentation, reassembly and error detection.

WAP is designed to operate over a variety of different services like SMS, GPRS, CSD, USSD etc.

b) Write short notes on time-out freezing and selective re-transmission

time-out freezing- 3M selective re-transmission -2M

<u>time-out freezing:-</u>

The MAC layer can inform the TCP layer of an upcoming loss of connection or that the current interruption is not caused by congestion. TCP can now stop sending and 'freezes' the current state of its congestion window and further timers. If the MAC layer notices the upcoming interruption early enough, both the mobile and correspondent host can be informed. With a fast interruption of the wireless link, additional mechanisms in the access point are needed to inform the correspondent host of the reason for interruption. Otherwise, the correspondent host goes into slow start assuming congestion and finally breaks the connection.

As soon as the MAC layer detects connectivity again, it signals TCP that it can resume operation at exactly the same point where it had been forced to stop. For TCP time simply does not advance, so no timers expire.

The advantage of this approach is that it offers a way to resume TCP connections even after longer interruptions of the connection. It is independent of any other TCP mechanism, such as acknowledgements or sequence numbers, so it can be used together with encrypted data.

However, this scheme has some severe disadvantages. Not only does the software on the mobile host have to be changed, to be more effective the correspondent host cannot remain unchanged. All mechanisms rely on the capability of the MAC layer to detect future interruptions. Freezing the state of TCP does not help in case of some encryption schemes that use time-dependent

random numbers. These schemes need resynchronization after interruption.

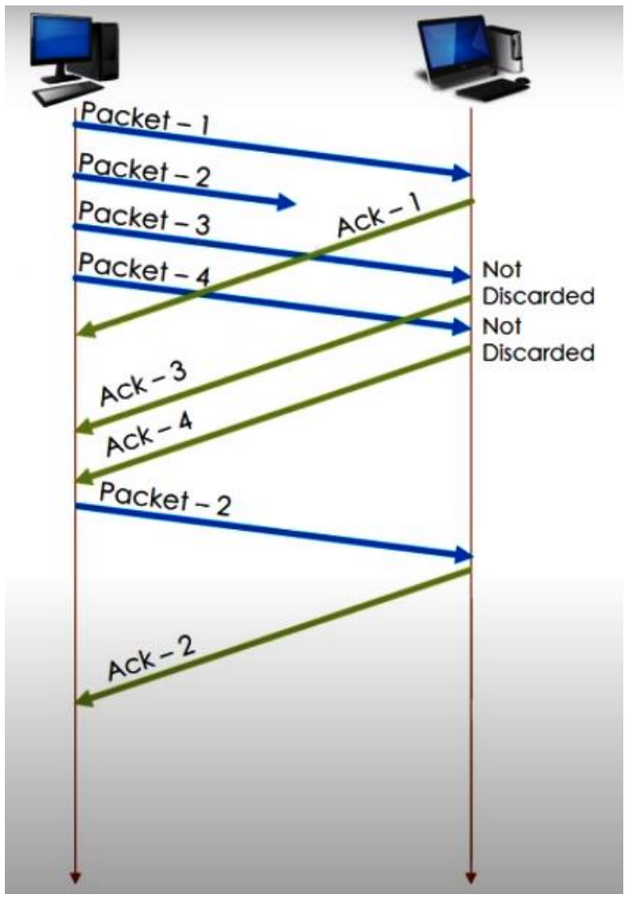
Selective Retransmission :-

A very useful extension of TCP is the use of selective retransmission.

TCP acknowledgements are cumulative.

If a single packet is lost, the sender has to retransmit everything starting from the lost packet (Go-Back-N Protocol). This type mechanism obviously wastes bandwidth.

To overcome the above drawback selective retransmission introduced.



With this method, TCP can indirectly request a selective retransmission of packets.

In selective retransmission, the receiver can acknowledge single packet, not only trains of in-sequence packets.

The sender can now determine precisely which packet is needed and can retransmit it.

Advantages:

A sender retransmits only the lost packets.

Disadvantage:

More complex software on the receiver side must maintain.

OR

9. a) Explain the traditional TCP .What are the improvements that are made into the classical TCP?

Definition -1M improvements-4M

TCP is a connection Oriented i.e. Before one application process can begin to send data to another, the two processes must "handshake" with each other.

TCP connection provides full-duplex service.

TCP connection is always point-to-point Between a single sender and single receiver.

So -called "Multicasting" - the transfer of data from one sender to many receivers in a single send operations - is not possible with TCP.

Mechanisms of traditional TCP

Congestion control

Slow start

Fast Retransmit/Fast Recovery

Implication on mobility

Classical TCP improvements :-

If we use traditional TCP for wireless communication, then the efficiency decreases.

The reason for this is the use of slow start under wrong assumptions.

From a missing acknowledgment, TCP concludes a congestion situation.

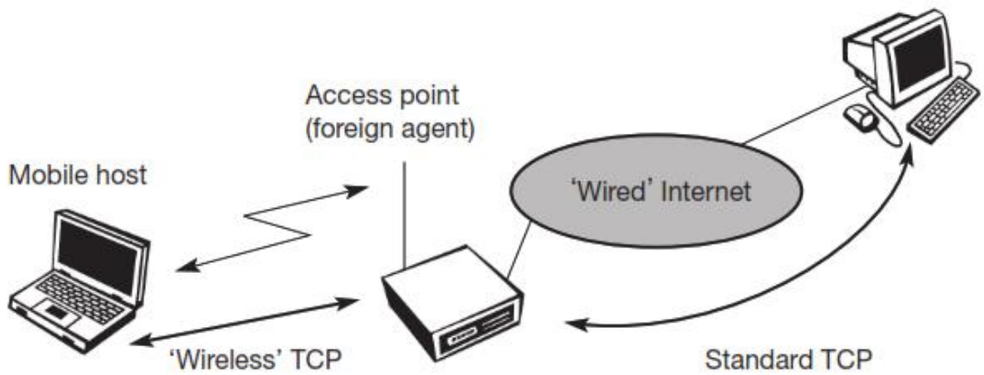
But in wireless communication because of mobility also there exists packet loss.

Indirect TCP :-

Two reason that led down the development of Indirect TCP (I-TCP)

- TCP performs poorly together with wireless links
- TCP within the fixed network cannot be changed.

I-TCP segments a TCP connection in to fixed part and a wireless part.



Standard TCP is used between the fixed computer and the access point.

The correspondent host in fixed network does not notice the wireless link.

The foreign agent acts as a proxy and relays all data in both directions.

If the correspondent host sends a packet, the foreign agent acknowledges this packet and tries to forward the packet to the mobile host.

If the mobile host receives the packet, it acknowledges the packet.

However, this acknowledge is only used by the foreign agent.

If a packet is lost on the wireless link due to transmission error, the correspondent host would not notice this.

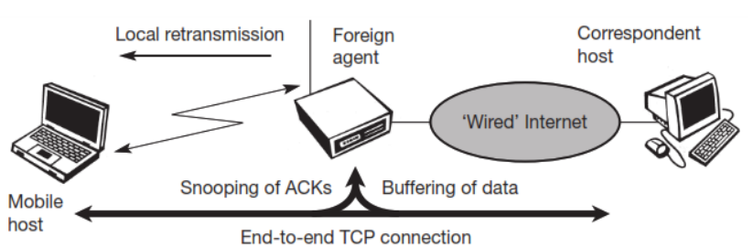
In this case foreign agent tries to retransmit this packet locally to maintain reliable data transport.

Snooping TCP :-

One of the drawbacks of I-TCP is the segmentation of the single TCP connection into two TCP connections.

These losses the original end-to-end TCP semantics.

Snooping TCP enhances the technique and leaves the TCP end-to-end connection intact.



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 enable the foreign agent to perform local retransmission in case of packet loss on the wireless link.

The foreign agent buffers every packet until it receives an acknowledgment 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 acknowledgment has been lost.

Alternatively, the foreign agent could receive a duplicate ACK which also shows the loss of a packet.

Now the foreign agent retransmits the packet directly from the buffer, performing a much faster retransmission compared to the correspondent host.

The foreign agent must not acknowledge data to the correspondent host.

If the foreign agent now crashes, the time-out of the correspondent host still works and triggers a retransmission.

When the data transfer from the mobile host to correspondent host, the foreign agent snoops into the packet stream to detect gaps in the sequence numbers of TCP.

As soon as the foreign agent detects a missing packet, it returns a negative acknowledgment (NACK) to the mobile host.

The mobile host can now retransmit the missing packet immediately.

Mobile TCP :-

In wireless networks packets may be dropped because of handover mechanism or mobile host moves out of the coverage area.

What happens to standard TCP in case of disconnection?

A TCP sender tries to retransmit data controlled by a retransmission timer that doubles with each unsuccessful retransmission attempt, up to maximum of one minute.

What happens in the case of I-TCP if the mobile is disconnected?

The proxy(Access Point) has to buffer more and more data, so the longer the period of disconnection, the more buffer is needed.

If a handover follows the disconnection, which is typical, even more state has to be transferred to the new proxy.

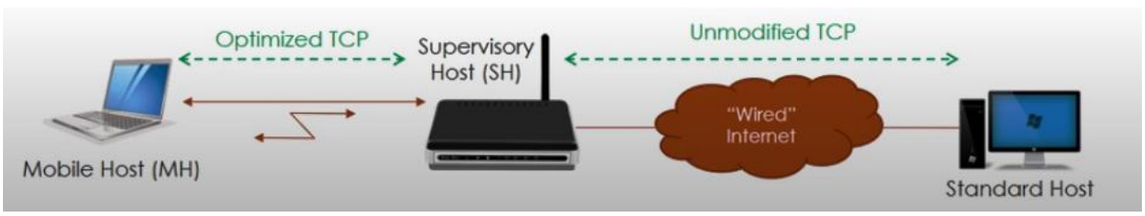
What happens in the case of Snooping TCP if the mobile is disconnected?

The mobile will not be able to send ACKs so, snooping cannot help in this situation.

The M-TCP (Mobile TCP) approach has the same goals as I-TCP and snooping TCP.

M-TCP wants to improve overall throughput, to lower the delay, to maintain end-to-end semantics of TCP, and to provide a more efficient handover.

M-TCP is especially adapted to the problems arising from lengthy or frequent disconnection.



M-TCP splits the TCP connection into two parts as I-TCP does.

An unmodified TCP is used on Standard host - Supervisory Host (SH) connection, while an optimized TCP is used on the SH-MH connection.

The Supervisory host is responsible for exchanging data between both parts similar to the proxy in I-TCP.

The M-TCP assumes a relatively low bit error rate on the wireless link, so there is no buffering/retransmission of via the SH.

If a packet is lost on the wireless link, it has to be retransmitted by the original sender. This maintains the TCP end-to-end semantics.

The SH monitors all packet sent to the MH and ACKs are returned from the MH.

If the SH does not receive an ACK for some time, it assumes that MH is disconnected.

It then chokes the sender by setting the sender's window size to 0.

Setting the window size to 0 forces the sender to go into persistent mode. i.e. sender will not try to retransmit data.

As soon as the SH detects connectivity again , it reopens the window of the sender to the old value.Then the sender can continue sending at full speed.

b) Write about (i) Wireless Transport Layer Security (ii) Wireless Session protocol

Wireless Transport Layer Security -3M **Wireless Session protocol-2M**

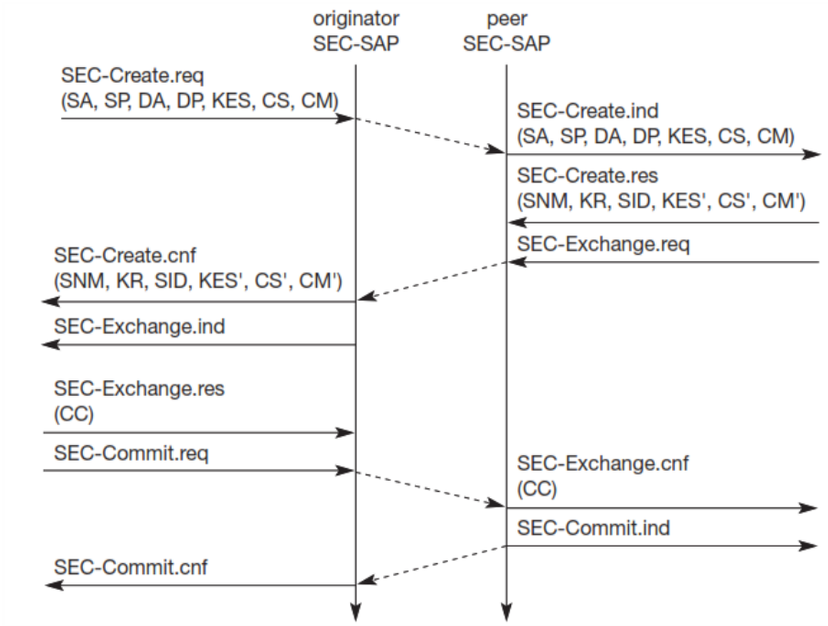
Wireless Transport Layer Security : -(WTLS)

It is based on Transport Layer Security (TLS).

It provides data integrity, privacy, authentication, Denial-of-Service Protection.

Before data can be exchanged via WTLS, a secure session has to be established.

This Session establishment consists of several steps:



Step1 :- Initiate the session with SEC-Create Primitive : SEC-Create.req.

Parameters:-

- SA : Source Address
- SP : Source Port
- DA : Destination Address
- DP : Destination Port
- KES : Key Exchange Suite (Ex: RSA, DH etc)
- CS : Cipher Suite (Ex : DES)
- CM : Compression Method

Step2 :- After receiving request peer also responds with : SEC-Create.res

Parameters:

- SNM : Sequence Number Mode
- KR : Key Refresh Cycle (keys are refreshed with in secure session)
- SID : Session Identifier
- KES` : Selected Key Exchange Suite
- CS` : Selected Cipher Suite
- CM` : Selected Compression Method

The Peer also issues a SES-Exchange Primitive

- Peer wishes to perform public key authentication with the client. i.e. peer requests a Client Certificate (CC) from the originator.

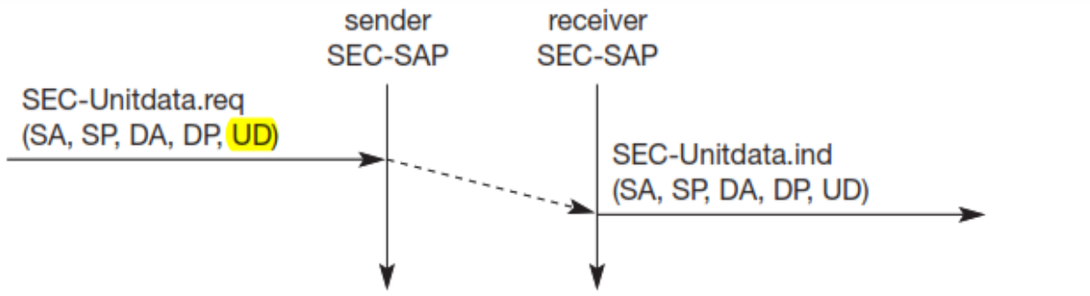
Step 3:- Originator issues SEC-Commit.req primitive.

- Originator answers with its certificate
- Indicates that handshake is completed

Step 4 :- SEC-Commit.ind

- Indicates that certificate is delivered.
- Conclude the full handshake.

After setting up a secure connection between two peers, user data can be exchanged.



It is same as T-DUnit data on the WDP layer.

The parameters are the same here : Source Address (SA), Source Port (SP), Destination Address (DA), Destination Port (DP), and User Data (UD).

Wireless Session Protocol :-

It provides reliable and organized exchange of content between client and server.

It provides fast connection suspension and reconnection.

It also supports asynchronous requests.

WSP offers the following needed for content exchange between cooperating clients and servers.

Session Management :-

WSP introduces sessions that can be established from client to a server.

The capabilities of suspending and resuming a session are important to mobile applications.

Assuming a mobile device is being switched off - it would be useful for a user to be able to continue operation at exactly the point where the device was switched off.

Capability negotiation :-

Clients and servers can agree upon a common level of protocol functionality during session establishment.

During session establishment some may be negotiated which does not affect the transaction.

WSP contains WSP/B protocol which is useful for browsing type applications.

WSP/B offers the following functions:

- HTTP/1.1 functions:
  - WSP/B supports the HTTP/1.1 functions, such as
    - Extensible request/replay methods
    - Composite objects
    - Content type negotiation
- Exchange of session headers:
  - Client and server can exchange request/replay headers that remain constant over the lifetime of the session.
  - WSP/B will not interpret header information but passes all headers directly to service users.
- Push and Pull data transfer:
  - Pulling data from a server is supported by WSP/B using the request/response mechanism.

- WSP/B supports three mechanisms for data transfer:
    - A confirmed data push within an existing session context.
    - A non-confirmed data push within an existing session context.
    - A non-confirmed data push without an existing session context.
- Asynchronous requests:
    - WSP/B supports a client that can send multiple requests to a serve simultaneously.

Signature of the HOD

Internal Evaluators :-

Name Signature

External Evaluators:-

Name Signature