SYLLABUS

MOBILE COMPUTING

UNIT-I

Mobile Physical Layer: Review of generation of mobile services, overview of wireless telephony, cellular concept, GSM: air-interface, channel structure, location management: HLR-VLR, hierarchical, handoffs, channel allocation in cellular systems, CDMA, GPRS.

Mobile Computing Architecture: Issues in mobile computing, three tier architecture for mobile computing, design considerations, Mobile file systems, Mobile databases. WAP: Architecture, protocol stack, Data gram protocol, Wireless transport layer security, Wireless transaction protocol, wireless session protocol, application environment, and applications. **[T1] [T2][T3] [No. of Hrs. 12]**

UNIT-II

Mobile Data Link Layer: Wireless LAN over view, IEEE 802.11, Motivation for a specialized MAC, Near & far terminals, Multiple access techniques for wireless LANs such as collision avoidance, polling, Inhibit sense, spread spectrum, CDMA , LAN system architecture, protocol architecture, physical layer MAC layer and management, Hiper LAN.

Blue Tooth: IEEE 802.15 Blue tooth User scenarios, physical, MAC layer and link management.

Local Area Wireless systems: WPABX, IrDA, ZigBee, RFID, WiMax.

[T1] [T2][T3] [No. of Hrs. 11]

UNIT-III

MOBILE IP Network Layer: IP and Mobile IP Network Layer- Packet delivery and Handover Management-Location Management- Registration- Tunnelling and Encapsulation-Route Optimization- Dynamic Host Configuration Protocol, Ad Hoc networks, localization, MAC issues, Routing protocols, global state routing (GSR), Destination sequenced distance vector routing (DSDV), Dynamic source routing (DSR), Ad Hoc on demand distance vector routing (AODV), VoIP –IPSec.

Mobile Transport Layer: Traditional TCP/IP, Transport Layer Protocols-Indirect, Snooping, Mobile TCP. **[T1] [T2][T3] [No. of Hrs. 11]**

UNIT-IV

Support for Mobility: Data bases, data hoarding, Data dissemination, UA Prof and Caching, Service discovery, Data management issues, data replication for mobile computers, adaptive clustering for mobile wireless networks, Mobile devices and File systems, Data Synchroni-zation, Sync ML.

Introduction to Wireless Devices and Operating systems: Palm OS, Windows CE, Symbion OS, Android, Mobile Agents. Introduction to Mobile application languages and tool kits.

[T1] [T2][T3] [No. of Hrs. 11]

END TERM EXAMINATION [MAY-JUNE 2017]
EIGHTH SEMESTER [B.TECH.]
MOBILE COMPUTING [ETIT–402]

Time : 3 Hrs. **M.M. : 75**

Note: *Attempt any five questions including Q. No. 1 which is compulsory.*

Q.1. Answer following in brief:

Q.1. (a) Explain Data dissemination issues in mobile Networks. (5)

Ans. Data Dissemination

Some related aspects of wireless sensor networks including the protocols and software employed are as follows:-

Data dissemination after aggregation, compaction, and fusion

Data dissemination by sensor nodes is carried out after aggregation, compaction, and fusion.

1. Aggregation refers to the process of joining together present and previously received data packets after removing redundant or duplicate data.

2. Compacting means making information short without changing the meaning or context, for example, transmitting only the incremental data so that information sent is short.

3. Fusion means formatting the information received in parts through various data packets and several types of data (or data from several sources), removing redundancy in the received data, and presenting the formatted information created from the information parts in cases when the individual records are not required and/or are not retrievable later.

Q.1. (b) Explain the WAP Architecture in brief. (5)

Ans. Fig. (1) gives an overview of the WAP architecture, its protocols and components, and compares this architecture with the typical internet architecture when using the world wide web.

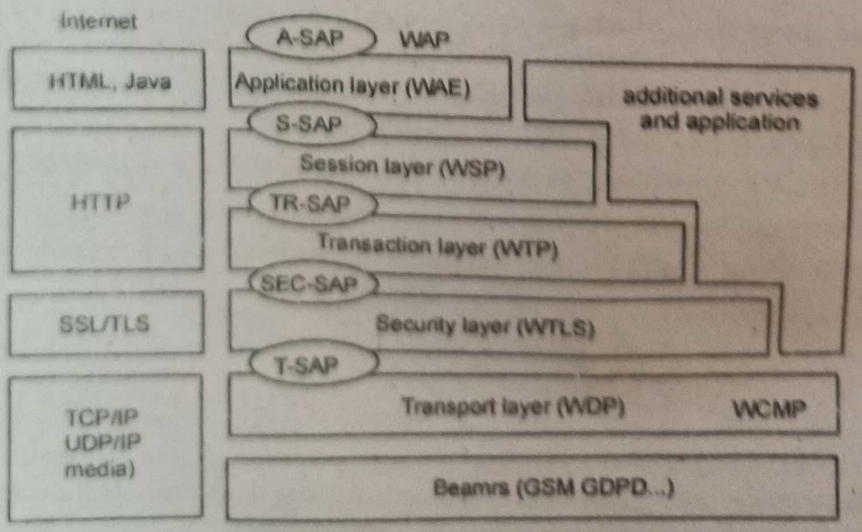


Fig.1. Components and interface of the WAP 1. architecure

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

The transport layer service access point (T-SAP) is the common interface to be used by higher layers independent of the underlying network.

The next higher layer, the security layer with its wireless transport layer security protocol WTLS offers its service at the security SAP (SEC-SAP). WTLS is based on the transport layer security (TLS, formerly SSL, secure sockets layer) already known from the www. WTLS has been optimized for use in wireless net-works with narrow-band channels.

The WAP **transaction layer** with its **wireless transaction protocol** (WTP) offers a lightweight transaction service at the transaction SAP (TR-SAP). This service efficiently provides reliable or unreliable requests and asynchronous transactions. The **session layer** with the **wireless session protocol** (WSP) currently offers two services at the **session-SAP** (S-SAP), one connection-oriented and one connectionless if used directly on top of WDP. A special service for browsing the web (WSP/B) has been defined that offers HTTP/1.1 functionality, long-lived session state, session suspend and resume, session migration and other features needed for wireless mobile access to the web.

Finally the **application layer** with the wireless **application environment** (WAE) offers a framework for the integration of different www and mobile telephony applications.The main issues here are scripting languages, special markup languages, interfaces to telephony applications, and many content formats adapted to the special requirements of small, handheld, wireless devices.

Q.1. (c) What is "Slow Start" in mobile computing? **(5)**

Ans. A transport layer protocol such as TCP has been designed for fixed networks with fixed end- systems. Congestion may appear from time to time even in carefully designed networks. The packet buffers of a router are filled and the router cannot forward the packets fast enough because the sum of the input rates of packets destined for one output link is higher than the capacity of the output link. The only thing a router can do in this situation is to drop packets. A dropped packet is lost for the transmission, and the receiver notices a gap in the packet stream. Now the receiver does not directly tell the sender which packet is missing, but continues to acknowledge all in-sequence packets up to the missing one. The sender notices the missing acknowledgement for the lost packet and assumes a packet loss due to congestion. Retransmitting the missing packet and continuing at full sending rate would now be unwise, as this might only increase the congestion. To mitigate congestion, TCP slows down the transmission rate dramatically. All other TCP connections experiencing the same congestion do exactly the same so the congestion is soon resolved

Slow start

TCP's reaction to a missing acknowledgement is quite drastic, but it is necessary to get rid of congestion quickly. The behavior TCP shows after the detection of congestion is called slow start.

The sender always calculates a congestion window for a receiver. The start size of the congestion window is one segment (TCP packet). The sender sends one packet and waits for acknowledgement. If this acknowledgement arrives, the sender increases the

congestion window by one, now sending two packets (congestion window = 2). This scheme doubles the congestion window every time the acknowledgements come back, which takes one round trip time (RTT). This is called the exponential growth of the congestion window in the slow start mechanism.

But doubling the congestion window is too dangerous. The exponential growth stops at the Congestion threshold.

As soon as the congestion window reaches the congestion threshold, further increase of the transmission rate is only linear by adding 1 to the congestion window each time the acknowledgements come back.

Linear increase continues until a time-out at the sender occurs due to a missing acknowledgement, or until the sender detects a gap in transmitted data because of continuous acknowledgements for the same packet. In either case the sender sets the congestion threshold to half of the current congestion window. The congestion window itself is set to one segment and the sender starts sending a single segment. The exponential growth starts once more up to the new congestion threshold, then the window grows in linear fashion.

Q.1. (d) Differentiate between tunneling and reverse tunneling? (5)

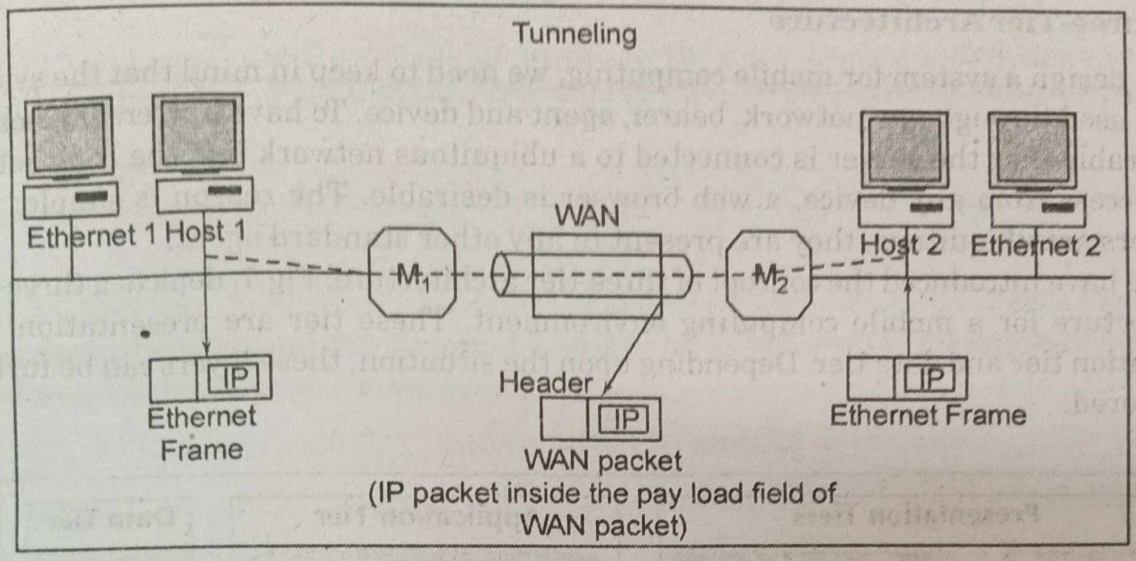
Ans. Tunneling

Tunneling is an internetworking strategy that is used when source and destination networks of same type are connected through a network of different type.

- In such a case, the packet from one network reaches the other network via different kind pf network that interconnects them.

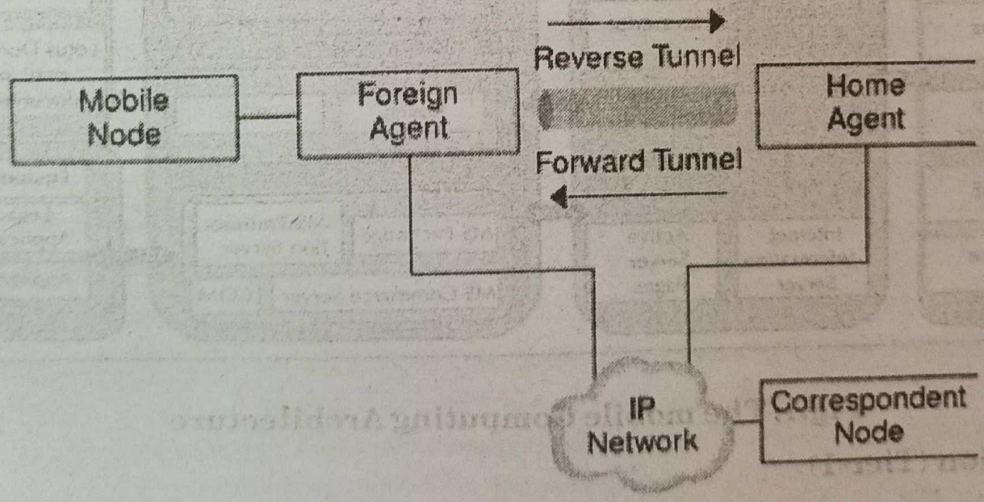
To understand tunneling, let an Ethernet is to be connected to another Ethernet via a WAN.

- The IP packets are to be sent from host 1 of Ethernet 1 to host 2 of Ethernet 2 via a WAN.
- To send an IP packet to host 2, host 1 constructs the packet containing the IP address of host 2.
- It then inserts this packet into an Ethernet frame. This frame is addressed to the multi-protocol router M_1 and is placed on Ethernet.
- When this packet reaches, multiprotocol router M_1, it removes the IP packet and insert it in the payload field of the WAN network layer packet.
- This WAN network layer packet is then addressed to multi-protocol router M_2.
- When this packet reaches M_2, it removes the IP packet and inserts it into the Ethernet frame and sends it to host 2.
- In the above process, IP packets do not have to deal with WAN, they just travel from one end of the tunnel to the other end. The host 1 and host 2 on two Ethernet also do not have to deal with WAN.
- The multi-protocol routers M_1 & M_2 understand about IP and WAN packets.



Reverse Tunneling

Mobile IP assumes that the routing within the Internet is independent of the data packet's source address. However, intermediate routers might check for a topologically correct source address. If an intermediate router does check, you should set up a reverse tunnel. By setting up a reverse tunnel from the mobile node's care-of address to the home agent, you ensure a topologically correct source address for the IP data packet. A mobile node can request a **reverse tunnel** between its foreign agent and its home agent when the mobile node registers. A reverse tunnel is a tunnel that starts at the mobile node's care-of address and terminates at the home agent. The following illustration shows the Mobile IP topology that uses a reverse tunnel.



Q.1. (e) With the help of neat protocol stack. Draw and explain three tier architecture for mobile computing. What are mobile nodes? Explain. (5)

Ans. A mobile node is an Internet-connected device whose location and point of attachment to the Internet may frequently be changed. This kind of node is often a cellular telephone or handheld or laptop computer, although a mobile node can also be a router. Special support is required to maintain Internet connections for a mobile node as it moves from one network or subnet to another, because traditional Internet routing assumes a device will always have the same IP address. Therefore, using standard routing procedures, a mobile user would have to change the device's IP address each time they connected through another network or subnet.

Three-Tier Architecture

To design a system for mobile computing, we need to keep in mind that the system will be used through any network, bearer, agent and device. To have universal access, it is desirable that the server is connected to a ubiquitous network like the Internet. To have access from any device, a web browser is desirable. The reason is simple: web browsers are ubiquitous, they are present in any other standard agent.

We have introduced the concept of three-tier architecture. Fig.1. depicts a three-tier architecture for a mobile computing environment. These tier are presentation tier, application tier and data tier. Depending upon the situation, these layers can be further sublayered.

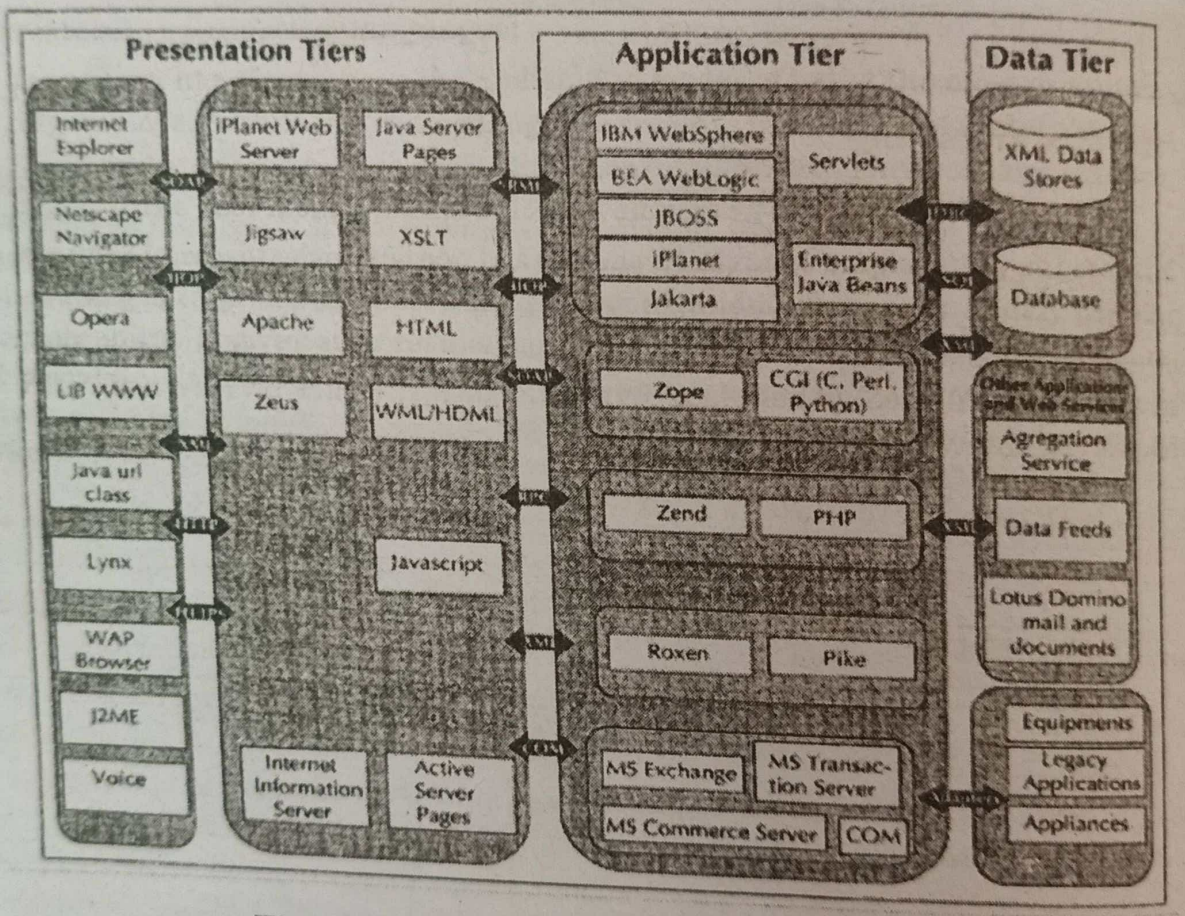


Fig.1. The mobile Computing Architecture

Presentation (Tier-1)

This is the user facing system in the first tier. This is the layer of agent applications and systems. These applications run on the client device and offer all the user interfaces. This tier is responsible for presenting the information to the end user. Humans generally use visual and audio means to receive information from machines.

Application (Tier-2)

The application tier or middle tier is the "engine" of a ubiquitous application. It performs the business logic of processing user input, obtaining data, and making decision. In certain cases, this layer will to the transcoding of data for appropriate rendering in the presentation tier. The application tier may include technology like CGIs, Java, JSP, .NET services, PHP or coldfusion, deployed in products like Apache, Websphere, Weblogic, iPlanet, Pramati, JBOSS or ZEND.

Data (Tier-3)

The Data tier is used to store data needed by the application and acts as a repository for both temporary and permanent data. The data can be stored in any form of datastore or database.

These can range from sophisticated relational database, legacy hierachical database, to even simple text files. The data can also be stored in XML format for interoperability with other systems and datasources.

A legacy application can also be considered as a data source or a document through a communication middle ware.

Q.2. (a) Explain location management in mobile networks. **(6)**

Ans. Mobile wireless devices with wireless connection facilities are changing the way people think about the use of computing and communication. These wireless devices can communicate with one another even though the user is mobile. People carrying a mobile computer will be able to access information regardless of the time and their current position. Over 100 million wireless Internet users were recorded as of September 2003 with the majority in Japan and Korea, while fast growth rates were recorded in Europe. Significant growth is expected in specialized mobile services such as driving directions, traffic report, tour guides, and commerce services such as mobile shopping. However, Location Management (LM) will be an important issue in these situations because wireless devices can change location while connected to a wireless network. New strategies must be introduced to deal with the dynamic changes of a mobile deviceís network address. The ability to change locations while connected to the network creates a dynamic environment. This means that data, which is static for stationary computing, becomes dynamic for mobile computing. There are a few questions that must be answered when looking at a LM scheme. What happens when a mobile user changes location? Who should know about the change? How can you contact a mobile host? Should you search the whole network or does anyone know about the mobile users moves? LM schemes are essentially based on users' mobility and incoming call rate characteristics. The main task of LM is to keep track of a users' location all the time while operating and on the move so that incoming messages (calls) can be routed to the intended recipient.

LM consists mainly of:

1. Location Tracking and Updating (Registration): A process in which an end-point initiates a change in the Location Database according to its new location. This procedure allows the main system to keep track of a users' location so that for example an incoming call could be forwarded to the intended mobile user when a call exists or maybe bring a user's profile near to its current location so that it could provide a user with his/her subscribed services.

2. Location Finding (Paging): The process of which the network initiates a query for an end point's location. This process is implemented by the system sending beacons to all cells so that one of the cells could locate the user. This might also result in an update to the location register.

As we can see, the main difference between location tracking and paging is in who initiates the change. While location tracking is initiated by a mobile host, paging is initiated by the base system. Most LM techniques use a combination of location tracking and location finding to select the best trade-off between the update overhead and the paging delay. LM methods are classified into two groups:

Transport Layer

The *Transport layer* (also known as the Host-to-Host Transport layer) is responsible for providing the Application layer with session and datagram communication services. The core protocols of the Transport layer are *Transmission Control Protocol* (TCP) and the *User Datagram Protocol* (UDP).

- TCP provides a one-to-one, connection-oriented, reliable communications service. TCP is responsible for the establishment of a TCP connection, the sequencing and acknowledgment of packets sent, and the recovery of packets lost during transmission.
- UDP provides a one-to-one or one-to-many, connectionless, unreliable communications service. UDP is used when the amount of data to be transferred is small (such as the data that would fit into a single packet), when the overhead of establishing a TCP connection is not desired or when the applications or upper layer protocols provide reliable delivery.

The Transport layer encompasses the responsibilities of the OSI Transport layer and some of the responsibilities of the OSI Session layer.

Application Layer

The *Application layer* provides applications the ability to access the services of the other layers and defines the protocols that applications use to exchange data. There are many Application layer protocols and new protocols are always being developed.

The most widely-known Application layer protocols are those used for the exchange of user information:

- The Hypertext Transfer Protocol (HTTP) is used to transfer files that make up the Web pages of the World Wide Web.
- The File Transfer Protocol (FTP) is used for interactive file transfer.
- The Simple Mail Transfer Protocol (SMTP) is used for the transfer of mail messages and attachments.
- Telnet, a terminal emulation protocol, is used for logging on remotely to network hosts.

Additionally, the following Application layer protocols help facilitate the use and management of TCP/IP networks:

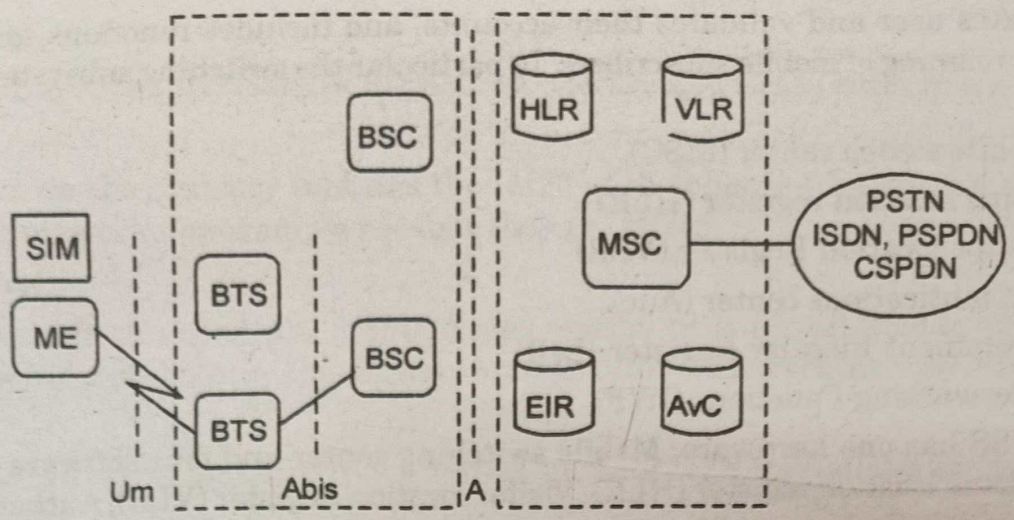
- The Domain Name System (DNS) is used to resolve a host name to an IP address.
- The Routing Information Protocol (RIP) is a routing protocol that routers use to exchange routing information on an IP internetwork.
- The Simple Network Management Protocol (SNMP) is used between a network management console and network devices (routers, bridges, intelligent hubs) to collect and exchange network management information.

Examples of Application layer interfaces for TCP/IP applications are Windows Sockets and NetBIOS. Windows Sockets provides a standard application programming interface (API) under Windows 2000. NetBIOS is an industry standard interface for accessing protocol services such as sessions, datagram, and name resolution.

Q.3. (a) Explain the architecture of GSM and discuss GSM services and security in brief. **(6.5)**

Ans.

- The GSM network architecture consists of three major subsystems:
- Mobile Station (MS)
- Base Station Subsystem (BSS)



SIM subscriber Identity Module	BSC Base Station Controller	MSC Mobile service switching center
ME Mobile Equipment	HLR Home Location Register	EIR Equipment Identity Register
BTS Base Transreceiver station	VLR Victor Location Register	AuC Authentication Center

- Network and Switching Subsystem (NSS)
- The wireless link interface between the MS and the Base Transceiver Station (BTS), which is a part of BSS. Many BTSs are controlled by a Base Station Controller (BSC). BSC is connected to the Mobile Switching Center (MSC), which is a part of NSS. Figure shows the key functional elements in the GSM network architecture.

1. Mobile Station (MS):

A mobile station communicates across the air interface with a base station transceiver in the same cell in which the mobile subscriber unit is located. The MS communicates the information with the user and modifies it to the transmission protocols if the air-interface to communicate with the BSS. The user's voice information is interfaced with the MS through a microphone and speaker for the speech, keypad, and display for short messaging, and the cable connection for other data terminals. The MS has two elements. The Mobile Equipment (ME) refers to the physical device, which comprises of transceiver, digital signal processors, and the antenna. The second element of the MS is the GSM is the Subscriber Identity Module (SIM). The SIM card is unique to the GSM system. It has a memory of 32 KB.

2. Base Station Subsystem (BSS):

A base station subsystem consists of a base station controller and one or more base transceiver station. Each Base Transceiver Station defines a single cell. A cell can have a radius of between 100m to 35km, depending on the environment. A Base Station Controller may be connected with a BTS. It may control multiple BTS units and hence multiple cells. There are two main architectural elements in the BSS – the Base Transceiver Subsystem (BTS) and the Base Station Controller (BSC). The interface that connects a BTS to a BSC is called the A-bis interface. The interface between the BSC and the MSC is called the A interface, which is standardised within GSM.

3. Network and switching subsystem (NSS)

The NSS is responsible for the network operation. It provides the link between the cellular network and the Public switched telecommunicates Networks (PSTN or ISDN or Data Networks). The NSS controls handoffs between cells in different BSSs,

authenticates user and validates their accounts, and includes functions for enabling worldwide roaming of mobile subscribers. In particular the switching subsystem consists of:

- Mobile switch center (MSC)
- Home location register (HLR)
- Visitor location Register (VLR)
- Authentications center (Auc)
- Equipment Identity Register (EIR)
- Interworking Functions (IWF)

The NSS has one hardware, Mobile switching center and four software database element: Home location register (HLR), Visitor location Register (VLR), Authentications center (Auc) and Equipment Identity Register (EIR). The MSC basically performs the switching function of the system by controlling calls to and from other telephone and data systems. It includes functions such as network interfacing and common channel signalling.

HLR:

The HLR is database software that handles the management of the mobile subscriber account. It stores the subscriber address, service type, current locations, forwarding address, authentication/ciphering keys, and billings information. In addition to the ISDN telephone number for the terminal, the SIM card is identified with an International Mobile Subscribes Identity (IMSI) number that is totally different from the ISDN telephone number. The HLR is the reference database that permanently stores data related to subscribers, including subscriber's service profile, location information, and activity status.

VLR:

The VLR is temporary database software similar to the HLR identifying the mobile subscribers visiting inside the coverage area of an MSC. The VLR assigns a Temporary mobile subscriber Identity (TMSI) that is used to avoid using IMSI on the air. The visitor location register maintains information about mobile subscriber that is currently physically in the range covered by the switching center. When a mobile subscriber roams from one LA (Local Area) to another, current location is automatically updated in the VLR. When a mobile station roams into a new MSC area, if the old and new LA's are under the control of two different VLRs, the VLR connected to the MSC will request data about the mobile stations from the HLR. The entry on the old VLR is deleted and an entry is created in the new VLR by copying the database from the HLR.

AuC:

The AuC database holds different algorithms that are used for authentication and encryptions of the mobile subscribers that verify the mobile user's identity and ensure the confidentiality of each call. The AuC holds the authentication and encryption keys for all the subscribers in both the home and visitor location register.

EIR:

The EIR is another database that keeps the information about the identity of mobile equipment such the International mobile Equipment Identity (IMEI) that reveals the details about the manufacturer, country of production, and device type. This information is used to prevent calls from being misused, to prevent unauthorised or defective MSs, to report stolen mobile phones or check if the mobile phone is operating according to the specification of its type.

White list:

This list contains the IMEI of the phones who are allowed to enter in the network.

Black list:

This list on the contrary contains the IMEI of the phones who are not allowed to enter in the network, for example because they are stolen.

Grey list:

This list contains the IMEI of the phones momentarily not allowed to enter in the network, for example because the software version is too old or because they are in repair.

IWF-

Interworking Function: It is a system in the PLMN that allows for non speech communication between the GSM and the other networks. The tasks of an IWF are particularly to adapt transmission parameters and protocol conversions. The physical manifestations of an IWF may be through a modem which is activated by the MSC dependent on the bearer service and the destination network. The OSS (Operational Support Systems) supports operation and maintenance of the system and allows engineers to monitor, diagnose, and troubleshoot every aspect of the GSM network.

GSM services:

GSM services are classified as either teleservices or data services. Teleservices include standard mobile telephony and mobile-originated traffic. Data services include computer to computer communication and packet switched traffic. User services may be divided into three major categories.

A. **Telephone services:** These include emergency calling and facsimile. GSM also supports Videotex and Teletex.

B. **Bearer services or data services:** These are limited to layer 1,2 and 3 of the open system interconnection (OSI) reference model. Supported services include packet switched protocols and data rates from 300bps to 9.6 kbps. Data may be transmitted using transparent or non transparent mode.

C. **Supplementary ISDN services:** these are digital in nature and include call diversion, closed user groups and caller identification, and are not available in analog mobile networks. Supplementary services also include short messaging service (SMS) which allows GSM subscribers and base station to transmit alphanumeric pages of limited length while simultaneously carrying normal voice traffic. SMS provides cell broadcast also can be used for safety and advisory applications such as the broadcast of highway or weather information to all GSM subscribers.

The **GSM security** mechanism is covered with following:

- Authentication (used for billing purposes)
- Confidentiality
- Anonymity(used to identify users)
- PIN Lock, EIR, personalization etc.

Authentication process helps GSM network authenticate the right user. This process is based on exchanged secret key K_i which is known to AuC (Authentication Center) and SIM card. There is no provision to read the key K_i from the SIM.

The second important concept in GSM security is identity **confidentiality**. This protects user from any intrusion. This is provided to the GSM subscriber using TMSI (temporary mobile subscriber identity). TMSI can be provided to the GSM mobile either during location update procedure (LAU) or during TMSI reallocation procedure.

Anonymity: Here IMSI is associated with a unique user (SIM), after the initial registration, a TMSI is assigned to the subscriber. The TMSI is stored along with the IMSI in the network HLR.

Q.3. (b) What are various handover procedure available in GSM? Explain. (6)

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

When a mobile user travels from one area of coverage or cell to another cell within a call's duration the call should be transferred to the new cell's base station. Otherwise, the call will be dropped because the link with the current base station becomes too weak as the mobile recedes. Indeed, this ability for transference is a design matter in mobile cellular system design and is call *handoff*.

With hard handoff, the link to the prior base station is terminated before or as the user is transferred to the new cell's base station. That is to say that the mobile is linked to no more than one base station at a given time. Initiation of the handoff may begin when the signal strength at the mobile received from base station 2 is greater than that of base station 1. The signal strength measures are really signal levels averaged over a chosen amount of time.

In cellular telephone communication, soft handoff refers to the overlapping of repeater coverage zones, so that every cell phone set is always well within range of at least one repeater (also called a base station). In some cases, mobile sets transmit signals to, and receive signals from, more than one repeater at a time.

Soft handoff technology is used by code-division multiple access (CDMA) systems. Older networks use frequency division multiplex (FDM) or time division multiplex (TDM). In CDMA, all repeaters use the same frequency channel for each mobile phone set, no matter where the set is located. Each set has an identity based on a code, rather than on a frequency (as in FDM) or sequence of time slots (as in TDM). Because no change in frequency or timing occurs as a mobile set passes from one base station to another, there are practically no dead zones. As a result, connections are almost never interrupted or dropped.

Types of GSM handover

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

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

only from one BTS to another but one BSC to another. For this the handover is controlled by the MSC.

- ***Inter-MSC handover:*** This form of handover occurs when changing between networks. The two MSCs involved negotiate to control the handover.

Q.4. (a) What is UMTS? Explain UMTS in detail. Explain the UMTS networks and list the advantages of third generation wireless standard. (6.5)

Ans. UMTS (Universal Mobile Telecommunications Service) is a third-generation (3G) broadband, packet-based transmission of text, digitized voice, video, and multimedia at data rates up to 2 megabits per second (Mbps). UMTS offers a consistent set of services to mobile computer and phone users, no matter where they are located in the world. UMTS is based on the Global System for Mobile (GSM) communication standard. It is also endorsed by major standards bodies and manufacturers as the planned standard for mobile users around the world. Once UMTS is fully available, computer and phone users can be constantly attached to the Internet wherever they travel and, as they roam, will have the same set of capabilities. Users will have access through a combination of terrestrial wireless and satellite transmissions. Until UMTS is fully implemented, users can use multi-mode devices that switch to the currently available technology (such as GSM 900 and 1800) where UMTS is not yet available.

UMTS network constituents

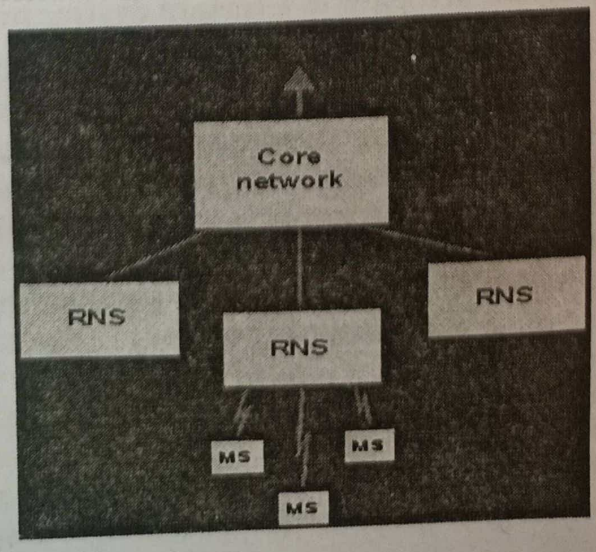
The UMTS network architecture can be divided into three main elements:

1.User Equipment (UE): The User Equipment or UE is the name given to what was previous termed the mobile, or cellphone. The new name was chosen because the considerably greater functionality that the UE could have. It could also be anything between a mobile phone used for talking to a data terminal attached to a computer with no voice capability.

2. Radio Network Subsystem (RNS): The RNS also known as the UMTS Radio Access Network, UTRAN, is the equivalent of the previous Base Station Subsystem or BSS in GSM. It provides and manages the air interface fort he overall network.

3.Core Network: The core network provides all the central processing and management for the system. It is the equivalent of the GSM Network Switching Subsystem or NSS.

The core network is then the overall entity that interfaces to external networks including the public phone network and other cellular telecommunications networks.



Advantages of 3G:

a. Overcrowding is relieved in existing systems with radio spectrum

b. Bandwidth, security and reliability are more

c. Provides interoperability among service providers

d. Availability of fixed and variable rates

e. Support to devices with backward compatibility with existing networks

f. Always online devices – 3G uses IP connectivity which is packet based

g. Rich multimedia services are available

Q.4. (b) Differentiate between DSDV, DSR and AODV routing mechanism. (6)

Ans. DSDV- Destination sequence distance vector

Destination sequence distance vector (DSDV) routing is an enhancement to distance vector routing for ad-hoc networks. DSDV can be considered historically, however, an on-demand version (ad-hoc on-demand distance vector, AODV) is among the protocols. Distance vector routing is used as routing information protocol (RIP) in wired networks. It performs extremely poorly with certain network changes due to the count-to-infinity problem. Each node exchanges its neighbour table periodically with its neighbours. Changes at one node in the network propagate slowly through the network (step-by-step with every exchange). The strategies to avoid this problem which are used in fixed networks (poisoned-reverse/split horizontal) do not help in the case of wireless ad-hoc networks due to the rapidly changing topology. This might create loops or unreachable regions within the network.

DSDV now adds 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. Anode waits with dissemination if these changes are probably unstableWaiting time depends on the time between the first and the best annoucement of a path to a certain destination.

DSR- This protocol uses a reactive approach which eliminates the need to periodically flood the network with table update messages which are required in a table-driven approach. In a reactive (on-demand) approach such as this, a route is established only when it is required and hence the need to find routes to all other nodes in the network as required by the table-driven approaches eliminated. The intermediate nodes also utilize . the route cache information efficiently to reduce the control overhead. The disadvantage of this protocol is that the route maintenance mechanism does not locally repair a broken link. Stale route cache information could also result in inconsistencies during the route reconstruction phase. The connection setup delay is higher than in table-driven protocols. Even though the protocol performs well in static and low-mobility environments, the performance degrades rapidly with increasing mobility. Also, considerable routing overhead is.involved due to the source-routing mechanism employed in DSR. This routing overhead is directly proportional to the path length.

AODV- Ad-hoc On-demand Distance Vector Routing (AODV) Protocol

AODV is reactive protocol. It reacts to the changes. It maintains only the active routes in the caches or tables for a pre-specified expiration time. These routes are found and are expected to be available at a given instant. It also performs unicast routing.

Distance vector means a set of distant nodes, which defines the path to destination. For example, *D-E-F-G* is a distance vector for source-destination pair D and G. In AODV, a distance vector is provided on demand during forwarding of *a* packet to destination by a node in the path and not by the route cache providing path through the header in the source data packet.

Phase 1 in AODV Protocol: The next hop routing table is generated as follows: A node uses hello messages to notify its existence to its neighbours. Therefore, the link status to the next hop in an active route is continuously monitored. When any node discovers a link disconnection, it broadcasts a route error (RERR) packet to its neighbours, who in turn propagate the RERR packet towards those nodes whose routes may be affected by the disconnected link. Then, the affected source can be informed. Following example considers the MANET. Assume that it deploys AODV routing protocol for discovering the distance vector *D-E-F-G*. It shows how hello message are used.

Phase 2 in AODV protocol: A source node initiates a route discovery process if no route is available in the routing table. It broadcasts the demand through the RREQ packets. Each RREQ has an ID and the addresses of the source and destination in its header. It expects return acknowledgement from destination. Anode identifies the last observed sequence number of the destination from the ID. Each RREQ starts with a small TTL value. If the destination is not found during the TTL, the TTL is increased in subsequent RREQ packets. The node also identifies the sequence number of the source node.

Sequence numbers ensure loop-free and up-to-date routes. Loop-free means that there is no bouncing of a packet to the node once it transmits to intermediate hops. Each node rejects the RREQ which it had observed before. This reduces flooding which means it reduces too many RREQs which may be present in the network at a given instant. That was the case in case of the DSR protocol.

Q.5. (a) Differentiate between fixed assignment schemes and random assignment schemes. **(6)**

Ans. FIXED ASSIGNMENT SCHEMES

TDMA

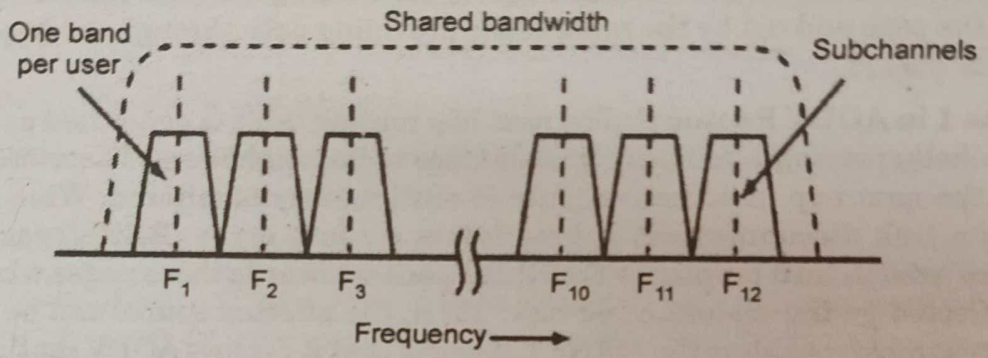
Time Division Multiple Access (TDMA) is a digital wireless telephony transmission technique. TDMA allocates each user a different time slot on a given frequency. TDMA divides each cellular channel into three time slots in order to increase the amount of data that can be carried.

CDMA

Code Division Multiple Access (CDMA) is a digital wireless technology that uses spread-spectrum techniques. CDMA does not assign a specific frequency to each user. Instead, every channel uses the full available spectrum. Individual conversations are encoded with a pseudo-random digital sequence. CDMA consistently provides better capacity for voice and data communications than other commercial mobile technologies, allowing more subscribers to connect at any given time, and it is the common platform on which 3G technologies are built.

FDMA

FDMA is the process of dividing one channel or bandwidth into multiple individual bands, each for use by a single user. Each individual band or channel is wide enough to accommodate the signal spectra of the transmissions to be propagated. The data to be transmitted is modulated on to each subcarrier, and all of them are linearly mixed together.



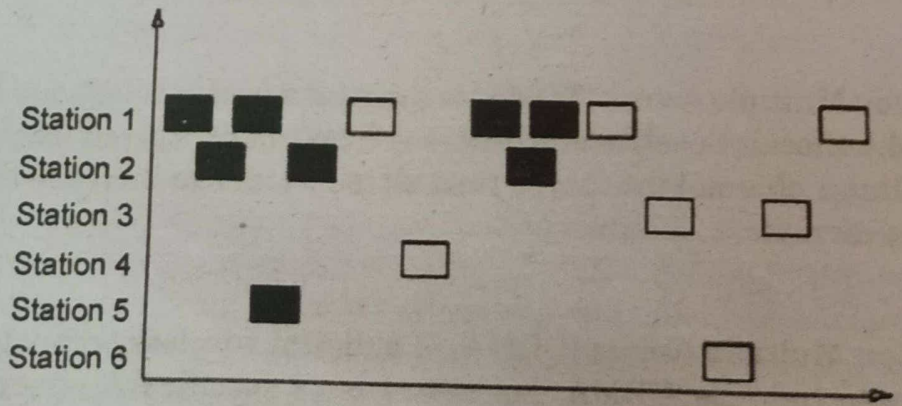
SDMA

Space-division multiple access (SDMA) is a channel access method based on creating parallel spatial pipes next to higher capacity pipes through spatial multiplexing and/or diversity, by which it is able to offer superior performance in radio multiple access communication systems. In traditional mobile cellular network systems, the base station has no information on the position of the mobile units within the cell and radiates the signal in all directions within the cell in order to provide radio coverage.

RANDOM ASSIGNMENT SCHEMES

Pure Aloha

With Pure Aloha, stations are allowed access to the channel whenever they have data to transmit. Because the threat of data collision exists, each station must either monitor its transmission on the rebroadcast or await an acknowledgment from the destination station. By comparing the transmitted packet with the received packet or by the lack of an acknowledgement, the transmitting station can determine the success of the transmitted packet. If the transmission was unsuccessful it is resent after a random amount of time to reduce the probability of re-collision.

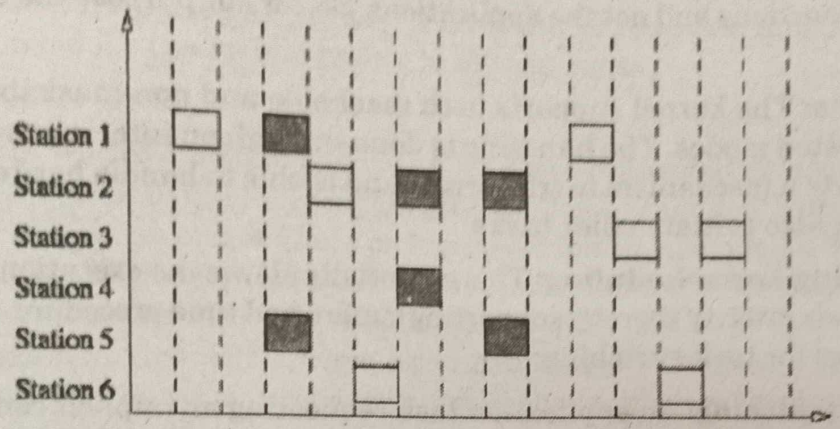


Time (shaded slots indicate collisions)

Slotted Aloha

The first of the contention based protocols we evaluate is the Slotted Aloha protocol. The channel bandwidth is a continuous stream of slots whose length is the time necessary

to transmit one packet. A station with a packet to send will transmit on the next available slot boundary. In the event of a collision, each station involved in the collision retransmits at some random time in order to reduce the possibility of recollision.



CSMA

CSMA is a network access method used on shared network topologies such as Ethernet to control access to the network. Devices attached to the network cable listen (carrier sense) before transmitting. If the channel is in use, devices wait before transmitting. MA (Multiple Access) indicates that many devices can connect to and share the same network. All devices have equal accéss to use the network when it is clear.

Q.5. (b) Explain the architecture palm OS. Difference between Paging and Location update. **(6.5)**

Ans. As shown in the heart of the OS is the kernel. Essentially the kernel handles all low-level communication with the process or interrupts, multitasking facilities and messaging to the OS atop it. The kernel interfaces to the hardware via the hardware abstraction layer. On top of the kernel there are the system services. Each service has a manager.

Later versions of the OS also contain a PACE (Palm application compatibility environment) which is an emulator for the older application ensuring backward compatibility, readers to explore the features supported by the model on which the application is to be deployed of the users are advice. Some important features supported by the kernel are listed below.

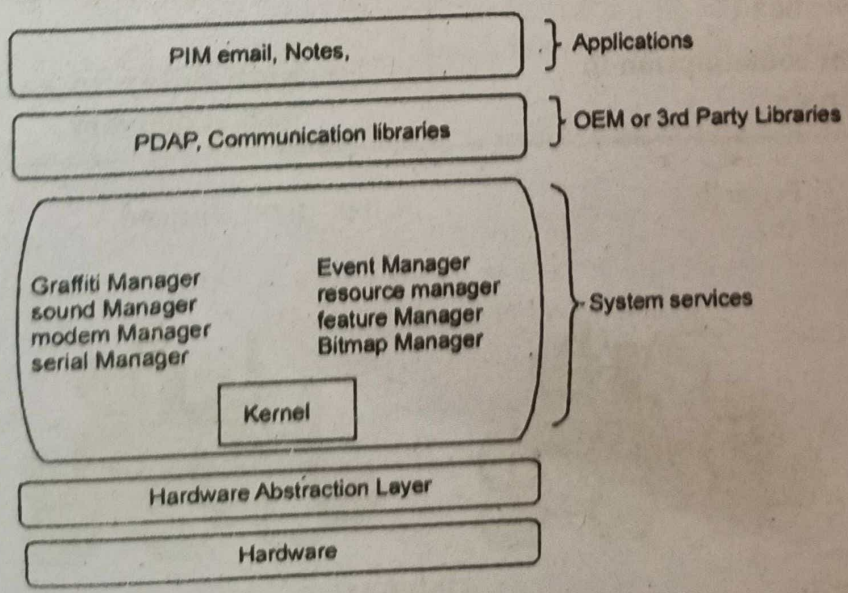


Fig. Architecture of Palm OS

Kernel Features

Multitasking: The kernel itself supports advanced multitasking, including semaphores. But certain licensing limitations cause mere features to be available only to the system functions and not the applications. So, for our purpose the OS is essentially single-tasked.

Interrupts: The kernel supports both maskable and non-maskable interrupts in normal and nested modes. The handling is done through an interrupt specially written for it. It supports a mechanism to trap errors and is able to handle hardware interrupts. Interrupts can also initiate odier tasks.

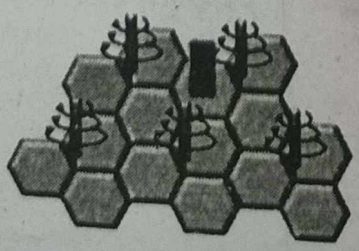
Time slicing and scheduling: This essentially allows the execution of several tasks according to their priority thereby supporting timers and time procedure. There are three types of triggers for task switching:

- Context switching: An application task requesting an implicit context switching,
- Hardware interrupt: There is an interrupt controller inside the Palm hardware system.
- Timer expiration: Each networking function has a timeout value to prevent the system from being idle in waiting state forever.

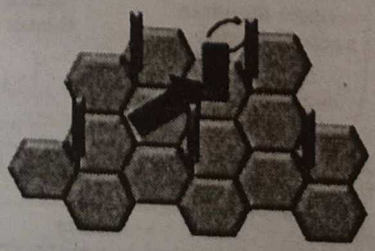
Differences between paging and Location Update

Mobility Management based on pure Location Update:	Mobility Management based on pure paging
• Each time the user crosses cell boundaries a location update is triggered	• If a call arrives terminal is paged in all cells of the mobile network
• Paging is not required	• Location update is not required
• As location updates must be initialized whenever crossing cell boundaries	• As paging must be executed in all cells of the network for each arriving calls/ SMS/data packet
• high signaling and database update overhead	• high signaling overhead
• high power consumption in the terminals	• high delay in call/SMS/data-packet delivery

• Paging



• Location Update



Q.6. Explain following terms with reference to mobile IP: (2.5×5=12.5)

Q.6. (a) Home address:

Ans. Home Address: The "normal", permanent IP address assigned to the mobile node. This is the address used by the device on its home network, and the one to which datagrams intended for the mobile node are always sent.

Q.6. (b) Mobile node

Ans. Mobile Node: A mobile node is an Internet-connected device whose location and point of attachment to the Internet may frequently be changed. This kind of node is often a cellular telephone or handheld or laptop computer, although a mobile node can also be a router. Special support is required to maintain Internet connections for a mobile node as it moves from one network or subnet to another, because traditional Internet routing assumes a device will always have the same IP address. Therefore, using standard routing procedures, a mobile user would have to change the device's IP address each time they connected through another network or subnet.

Q.6. (c) Foreign Node:

Ans. A mobile node when moves to foreign network becomes the foreign node. If a Mobile node determines that it is connected to foreign network, it acquires a care of address. Two types of care of addresses exist:

(*i*) Care of address acquired from a Foreign Agent.

(*ii*) Colocated care of address.

Q.6. (d) Foreign Network.

Ans. Foreign Network: In the Mobile Internet Protocol (Mobile IP), a foreign network is any network other than the home network to which a mobile device may be connected. Because standard Internet routing mechanisms deliver all traffic to a device's home network, it was once necessary to change a mobile device's IP address each time it connected through a foreign network.

Q.6. (e) Home Network.

Ans. Home Network: A home network is two or more computers interconnected to form a local area network (LAN) within the home. In the United States, for example, it is estimated that 15 million homes have more than one computer. A home network allows computer owners to interconnect multiple computers so that each can share files, programs, printers, other peripheral devices, and Internet access with other computers, reducing the need for redundant equipment and, in general, making everything easier to use.

Q.7. (a) What are the multiplexing techniques (Space, Frequency, Code division) and definition of each? (6)

Ans. TDMA: Time Division Multiple Access (TDMA) is a digital wireless telephony transmission technique. TDMA allocates each user a different time slot on a given frequency. TDMA divides each cellular channel into three time slots in order to increase the amount of data that can be carried.

TDMA technology was more popular in Europe, Japan and Asian countries, where as CDMA is widely used in North and South America. But now a days both technologies are very popular through out of the world.

Advantages of TDMA:

- TDMA can easily adapt to transmission of data as well as voice communication.

- TDMA has an ability to carry 64 kbps to 120 Mbps of data rates.
- TDMA allows the operator to do services like fax, voice band data, and SMS as well as bandwidth-intensive application such as multimedia and video conferencing.
- Since TDMA technology separates users according to time, it ensures that there will be no interference from simultaneous transmissions.
- TDMA provides users with an extended battery life, since it transmits only portion of the time during conversations.
- TDMA is the most cost effective technology to convert an analog system to digital.

Disadvantages of TDMA

- Disadvantage using TDMA technology is that the users has a predefined time slot. When moving from one cell site to other, if all the time slots in this cell are full the user might be disconnected.
- Another problem in TDMA is that it is subjected to multipath distortion. To overcome this distortion, a time limit can be used on the system. Once the time limit is expired the signal is ignored.

CDMA

Code Division Multipie Access (CDMA) is a digital wireless technology that uses spread-spectrum techniques. CDMA does not assign a specific frequency to each user. Instead, every channel uses the full available spectrum. Individual conversations are encoded with a pseudo-random digital sequence. CDMA consistently provides better capacity for voice and data communications than other commercial mobile technologies, allowing more subscribers to connect at any given time, and it is the common platform on which 3G technologies are built.

Advantages of CDMA

- One of the main advantages of CDMA is that dropouts occur only when the phone is at least twice as far from the base station. Thus, it is used in the rural areas where GSM cannot cover.
- Another advantage is its capacity; it has a very high spectral capacity that it can accommodate more users per MHz of bandwidth.

Disadvantages of CDMA

- Channel pollution, where signals from too many cell sites are present in the subscriber. s phone but none of them is dominant. When this situation arises, the quality of the audio degrades.
- When compared to GSM is the lack of international roaming capabilities.
- The ability to upgrade or change to another handset is not easy with this technology because the network service information for the phone is put in the actual phone unlike GSM which uses SIM card for this.
- Limited variety of the handset, because at present the major mobile companies use GSM technology.

FDMA

FDMA is the process of dividing one channel or bandwidth into multiple individual bands, each for use by a single user. Each individual band or channel is wide enough to accommodate the signal spectra of the transmissions to be propagated. The data to be transmitted is modulated on to each subcarrier, and all of them are linearly mixed together.

FDMA divides the shared medium bandwidth into individual channels. Subcarriers modulated by the information to be transmitted occupy each sub channel.

The best example of this is the cable television system. The medium is a single coax cable that is used to broadcast hundreds of channels of video/audio programming to homes. The coax cable has a useful bandwidth from about 4 MHz to 1 GHz. This bandwidth is divided up into 6-MHz wide channels. Initially, one TV station or channel used a single 6-MHz band. But with digital techniques, multiple TV channels may share a single band today thanks to compression and multiplexing techniques used in each channel.

This technique is also used in fibre optic communications systems. A single fibre optic cable has enormous bandwidth that can be subdivided to provide FDMA. Different data or information sources are each assigned a different light frequency for transmission. Light generally isn't referred to by frequency but by its wavelength (ë). As a result, fiber optic

FDMA is called wavelength division multiple access (WDMA) or just wavelength division multiplexing (WDM).

One of the older FDMA systems is the original analog telephone system, which used a hierarchy of frequency multiplex techniques to put multiple telephone calls on single line. The analog 300-Hz to 3400-Hz voice signals were used to modulate subcarriers in 12 channels from 60 kHz to 108 kHz. Modulator/mixers created single sideband (SSB) signals, both upper and lower sidebands. These subcarriers were then further frequency multiplexed on subcarriers in the 312-kHz to 552-kHz range using the same modulation methods. At the receiving end of the system, the signals were sorted out and recovered with filters and demodulators.

SDMA

Space-division multiple access (SDMA) is a channel access method based on creating parallel spatial pipes next to higher capacity pipes through spatial multiplexing and/or diversity, by which it is able to offer superior performance in radio multiple access communication systems. In traditional mobile cellular network systems, the base station has no information on the position of the mobile units within the cell and radiates the signal in all directions within the cell in order to provide radio coverage.

This results in wasting power on transmissions when there are no mobile units to reach, in addition to causing interference for adjacent cells using the same frequency, so called co-channel cells. Likewise, in reception, the antenna receives signals coming from all directions including noise and interference signals. By using smart antenna technology and differing spatial locations of mobile units within the cell, space-division multiple access techniques offer attractive performance enhancements.

The radiation pattern of the base station, both in transmission and reception, is adapted to each user to obtain highest gain in the direction of that user. This is often done using phased array techniques. In GSM cellular networks, the base station is aware of the distance (but not direction) of a mobile phone by use of a technique called "timing advance" (TA). The base transceiver station (BTS) can determine how distant the mobile station (MS) is by interpreting the reported TA.

Q.7.(b) Define WPABX, IrDA, Zigbee, RFID, WiMax in brief. (6.5)

Ans. WPBX systems integrate wireless telephones with a PBX switching system. Wireless PBX telephones (handsets) communicate through wired base stations (fixed radio transmitters) to the WPBX switching system. Most WPBX systems have automatic

switching call transfer that allows wireless handsets to transfer their calls to other base stations as the move through the WPBX radio coverage areas. Base stations are strategically located around the served area (both inside and/or outside) to provide contiguous radio coverage. WPBX systems can be completely, or partially, wireless between the system and the telephone instruments.

WPBX systems fill a need where all, or part, of the work force is highly mobile in a relatively small area such as a building/plant or a small commercial campus. Hospitals and manufacturing plants tend to have several types of personnel that tend to be constantly on the move: medical emergency personnel, maintenance personnel, and production-line supervisors to name a few. Such people are frequently away from their desk or other fixed telephone station set location; however, it is often quite important that they be contacted quickly.

There are several different types of WPBX systems industry standard systems and proprietary systems. Some of the standard WPBX systems include digital enhanced cordless telephone (DECT) and cordless telephony second generation (CT2). A WPBX radio system allows for voice or data communications on either an analog (typically FM) or digital radio channel. The radio channel typically allows multiple mobile telephones to communicate on the same frequency at the same time by special coding of their radio signals.

IrDA (Infrared Data Association)

Refer Q.4. (b) (iii) of First Term 2017.

ZigBee

Refer Q.4. (b) (i) First Term 2017.

WiMAX

Refer Q.4. (b) (iii) First Term 2017.

RFID(Radio Frequency Identification) is a radio transponder carrying an ID that can be read through radio frequency interfaces. These transponders are commonly known as RFID tags or simply tags. A RFID system comprises different functions are

(i) Means of reading or interrogating the data in the tag.

(ii) Mechanism to filter some of the data.

(iii) Means to communicate the data in the tag with a host computer..

(iv) Means for updating or entering customized data into the tag.

Q.8. (a) Difference between Hidden and Exposed Terminal, Near and Far Terminals. **(6)**

Ans.A significant difference between wired and wireless LANs is the fact that, in general a fully connected topology between the WLAN nodes cannot b assumed. This problem gives rise to 'hidden' and 'exposed' station problems.

Hidden Terminal:

- As seen in the above problem, the transmission range of A reaches B but not C. Similarly, the range of C reaches B but not A. Also the range of B reaches both A and C.
- Now, the node A starts to send something to B and C doesn't receive this transmission.
- Now C also wants to send data to B and senses the carrier. As it senses it to be free, it also starts sending to B.

• Hidden terminal problem occurs when two nodes that are outside each other's range performs simultaneous transmission to a node that is within the range of each of them resulting in a collision.

• That means the data from both parties A and C will be lost during the collision.

• Hidden nodes mean increased probability of collision at receiver end.

• One solution to avoid this is to have the channel sensing range much greater than the receiving range. Another solution is to use the Multiple Access with Collision Avoidance (MACA).

Exposed Terminal:

• Consider the same above diagram. Here imagine a situation wherein the B node is currently sending some data to node A.

• Now the other node C which is right now free want to send data to some node D(not in diag) which is outside the range of A and B.

• Now before starting transmission it senses the carrier and realizes that the carrier is busy (due to interference of B's signal).

• Hence, the C node postpones the transmission to D until it detects the medium to be idle.

• However such a wait was un-necessary as A was outside the interference range of C.

• Also a collision at B will be a weak enough to be unable to penetrate into C

• Exposed terminal problem occurs when the node is within the range of a node that is transmitting and it cannot be transmitted to any node.

• Exposed node means denied channel access unnecessarily which ultimately results in under-utilization of bandwidth resources.

• It also results in wastage of time-resource.

Near and far terminals

Consider the situation shown below. A and B are both sending with the same transmission power.

• Signal strength decreases proportional to the square of the distance

• So, B's signal drowns out A's signal making C unable to receive A's transmission

• If C is an arbiter for sending rights, B drown out A's signal on the physical layer making C unable to hear out A.

The **near/far effect** is a severe problem of wireless networks using CDM. All signals should arrive at the receiver with more or less the same strength for which Precise power control is to be implemented.

Q.8. (b) What are the various methods for data synchronization? Explain. **(6.5)**

Ans. SynchML is a data synchronization language based on XML. SynchML-based software synchronized data for PIM (email, calender, tasks-to-do list, or contacts list) databases and files for data.

SynchML is an open stanard based on XML. Use of a common and standard language enables interoperability. It also provides specifications for the protocols for sending message from one node to another and representation of the messages.

SynchML has revolutionized mobile application–development, services, and devic
The SynchML data engine performs the following tasks:

- SynchML code generation
- parsing of received synchML data
- validation of DTA in WBXML and XML formats of data
- base-64 encoding/dedcoding
- notification message passing
- credential checks.
- security operations and
- HMAC data integrity check.

FIRST TERM EXAMINATION [FEB. 2018]
EIGHTH SEMESTER [B.TECH]
MOBILE COMPUTING [ETIT-402]

Time : 1½ hrs. **M.M. : 30**

Note: *Attempt any three question in all and Q. 1. is Compulsory.*

Q.1. What is handover? Why is it required? What are handover scenarios in GSM? How the handover decisions take place depending on receiver signal strength? **(10)**

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

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

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

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

GSM handover process:

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

In GSM which uses TDMA techniques the transmitter only transmits for one slot in eight, and similarly the receiver only receives for one slot in eight. As a result the RF section of the mobile could be idle for 6 slots out of the total eight. This is not the case

because during the slots in which it is not communicating with the BTS, it scans the other radio channels looking for beacon frequencies that may be stronger or more suitable. In addition to this, when the mobile communicates with a particular BTS, one of the responses it makes is to send out a list of the radio channels of the beacon frequencies of neighbouring BTSs via the Broadcast Channel (BCCH).

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

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

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

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

- ***Old and new BTSs synchronised:*** In this case the mobile is given details of the new physical channel in the neighbouring cell and handed directly over. The mobile may optionally transmit four access bursts. These are shorter than the standard bursts and thereby any effects of poor synchronisation do not cause overlap with other bursts. However in this instance where synchronisation is already good, these bursts are only used to provide a fine adjustment.

- ***Time offset between synchronised old and new BTS:*** In some instances there may be a time offset between the old and new BTS. In this case, the time offset is provided so that the mobile can make the adjustment. The GSM handover then takes place as a standard synchronised handover.

- ***Non-synchronised handover:*** When a non-synchronised cell handover takes place, the mobile transmits 64 access bursts on the new channel. This enables the base station to determine and adjust the timing for the mobile so that it can suitably access the new BTS. This enables the mobile to re-establish the connection through the new BTS with the correct timing.

Handover scenarios in GSM systems

Intracell handover: The easiest type of handover is intracell handover where either the physical channel or the associated timeslot configuration is changed. This may become necessary if the connection on a physical channel is impaired. To evaluate connection quality, the mobile phone continuously transmits the measured RXLev (receive level measured by the telephone) and RXQual (bit error ratio determined) values to the base station. If the base station wants to hand over the telephone to another physical channel, all it needs to do is to inform the telephone about the new channel number and the new timeslot configuration. The telephone changes directly to the new channel and is able to maintain both its previous settings for timing and the base station parameters.

Intercell handover: If the mobile phone moves from one cell to another during a call, it must be handed over to the new cell. If the neighbour cell is time-synchronous with the current cell, the base station is able to effect a finely synchronized intercell handover. In this case, the mobile phone is transmitted on the new physical channel in the neighbour cell. Moreover, the mobile phone must be informed about the vital parameters of the new cell.

The mobile phone then optionally transmits four access bursts on the new channel. Compared to the normal bursts, these are shortened which is why they cannot cause interference with other calls even if the timing is slightly incorrect. If necessary, timing is corrected in a next step and the call continued. If the two cells with time offset are synchronous, the base station will effect a pseudo-synchronized or presynchronized intercell handover. This handover is similar to the finely synchronized intercell handover, but differs in that the mobile phone is provided with information about the time offset. Usually, however, a non-synchronized intercell handover takes place. In this case, the mobile phone transmits up to 64 access bursts on the new channel by means of which the new base station determines the timing and hands it over to the mobile phone. The mobile phone then reestablishes the call connection with the correct timing.

The base station requires the mobile phone's help in order to know the new cell to hand it over to. By means of the neighbour cell list, the base station informs the mobile phone about the RF channels for the BCCH that are used by the neighbour cells. The mobile phone now cyclically measures the RF level on these channels and transmits the measurement results to the base station. Based on this information, the base station determines the point in time at which the mobile phone is handed over to which cell. Changing the physical channel both for the call and for the BCCH information is key to intercell handover.

Intersystem handover: If the mobile phone leaves a cell and no new cell can be found in the same system, the base station can hand over an appropriately equipped mobile phone to a cell in another system. These intersystem handovers are highly complex because two technically disparate systems must be combined with each other. Basically, there are two handover options from WCDMA to GSM: In the case of blind handover, the base station simply transmits the mobile phone with all relevant parameters to the new cell. The mobile phone changes "blindly" to the GSM cell, i.e. it has not yet received any information about the timing there. It will first contact the transmitted BCCH channel, where it tries to achieve the frequency and time synchronization within 800 ms. Next, it will switch to the handed-over physical voice channel, where it will carry out the same sequence as with the non-synchronized intercell handover.

For the second type of handover from WCDMA to GSM, the compressed mode is used within the WCDMA cell; in this mode, transmission and reception gaps occur during the transmission between base station and mobile phone. During these gaps, the mobile phone can measure and analyze the nearby GSM cells. For this purpose, the base station, similar to the GSM system, provides a neighbour cell list, and the mobile phone transfers the measurement results to the base station. The actual handover in the compressed mode is basically analogous to blind handover.

There is, of course, an intersystem handover from GSM to WCDMA. A special neighbour cell list for WCDMA cells was established in GSM to support this handover.

Q.2. Explain the architecture of mobile computing. (10)

Ans.Three-Tier Architecture

To design a system for mobile computing, we need to keep in mind that the system will be used through any network, bearer, agent and device. To have universal access, it is desirable that the server is connected to a ubiquitous network like the Internet. To have access from any device, a web browser is desirable. The reason is simple: web browsers are ubiquitous, they are present in any other standard agent.

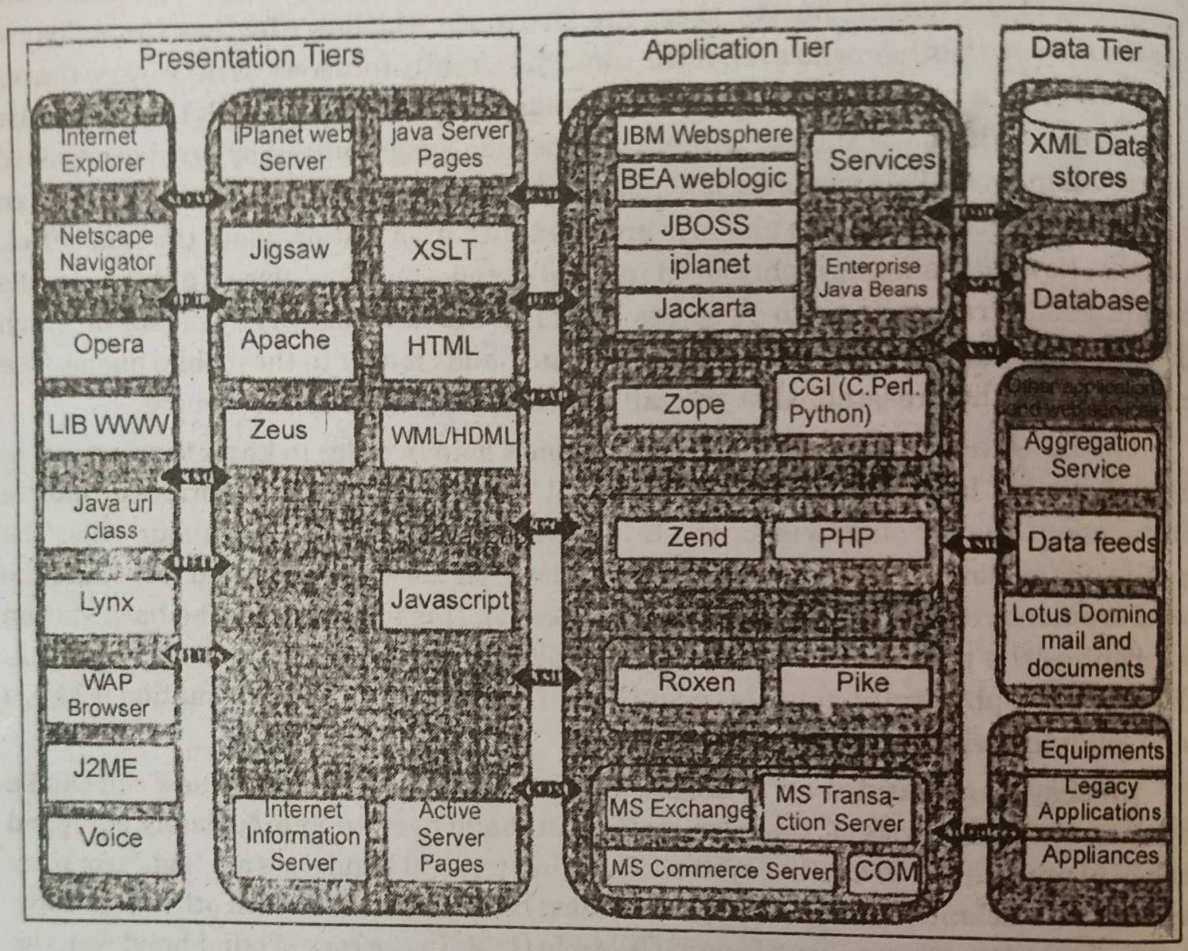


Fig. The mobile Computing Architecture

We have introduced the concept of three-tier architecture. Fig.1. depicts a three-tier architecture for a mobile computing environment. These tier are presentation tier, application tier and data tier. Depending upon the situation, these layers can be further sublayered.

Presentation (Tier-1): This is the user facing system in the first tier. This is the layer of agent applications and systems. These applications run on the client device and offer all the user interfaces. This tier is responsible for presenting the information to the end user. Humans generally use visual and audio means to receive information from machines.

Application (Tier-2): The application tier or middle tier is the "engine" of a ubiquitous application. It performs the business logic of processing user input, obtaining data, and making decision. In certain cases, this layer will to the transcoding of data for appropriate rendering in the presentation tier. The application tier may include technology like CGIs, Java, JSP, .NET services, PHP or coldfusion, deployed in products like Apache, Websphere, Weblogic, iPlanet, Pramati, JBOSS or ZEND.

Data (Tier-3): The Data tier is used to store data needed by the application and acts as a repository for both temporary and permanent data. The data can be stored in any form of datastore or database.

These can range from sophisticated relational database, legacy hierarchical database, to even simple text files. The data can also be stored in XML format for interoperability with other systems and datasources.

A legacy application can also be considered as a data source or a datastore through a communication middle ware.

Q.3. Name the mechanism to improve web access for handheld devices. What is their common problem and what led finally to the development of WAP? (10)

Ans. Caching, content transformation, picture downscaling, content selection, textual descriptions of pictures are some of the mechanism to improve web access for handheld devices. Many of the proposed solutions during the nineties were proprietary. WAP is the first standardized common solution supported by many network providers and device manufacturers.

A Brief History of WAP: The Wireless Application Protocol is a global standard for bringing Internet content and services to mobile phones and other wireless devices. The WAP standards suite is maintained by an industry consortium called the WAP Forum. Founded by Ericsson, Motorola, Nokia, and Openwave (then known as Unwired Planet) in June 1997, the WAP Forum now includes hundreds of member companies that are infrastructure providers, software companies, and content providers. The goal of the WAP Forum is to address the problems of wireless Internet access, ensuring that access is not limited by vendor or underlying network technology. Since its creation, the Wireless Application Protocol has passed through minor revisions (from 1.0 to 1.1, 1.2, and 1.2.1). WAP 2 is the first major revision since 1998.

The problems solved by WAP include the following:

- **Protocol mismatch**—Unlike the Internet, mobile networks (such as GSM and TDMA) are not inherently IP-based; they do not support the protocol of the Internet.
- **Device limitations**—Mobile devices (cellular phones, pagers, and palmtops) are not ideal Web clients.
- **Usability**—Usability is an issue, particularly with the limited size of mobile phones and pagers.

To address these issues, WAP defines a set of optimized protocols that can run over a wide variety of underlying cellular networks. It also specifies an application environment suited to small handled devices, including a display markup language (Wireless Markup Language, WML) and associated scripting language (WMLScript). Other standards cover push applications (useful for sending alerts and paging services) and telephony integration (such as initiating a voice call from a WML display page). For more information on WAP, check out the InformIT article "A WAP Primer."

The Wireless Application Protocol (WAP) is a system designed to format and filter Internet content for use in mobile devices. By linking the two 'hot-topics' in communication - the Internet and mobile technology - WAP provides a very valuable service. Motorola, Nokia, Ericsson and Phone.com set up the WAP Forum in mid 1997 with a view to establishing this standard, which has been widely accepted by over 200 members of the Forum.

As a scalable standard, WAP is designed to work with any mobile handset network type. It will function with GSM (Global System for Mobile Communication), CDMA (Code Division Multiple Access) and PDC (Personal Digital Cellular). It will also be compatible with any data transmission service e.g. SMS (Short Message Service) or GPRS (General Packet Radio Service). Later versions of the standard have evolved to make use of the more advanced technologies available.

WAP TECHNOLOGY: WAP incorporates a simple microbrowser, designed to work on the limited platforms of mobile handsets, with a central WAP gateway that performs the more processor-heavy operations. It defines a standard for data transmission to the handset, WDP (WAP datagram protocol), which is a variation of the internet standard transmission protocol, HTTP (Hypertext Transport Protocol), but redesigned for wireless network characteristics. WDP mostly differs from HTTP by stripping out much of the text information, replacing it with more efficient binary information for the low-bandwidth connection. The WAP data can be sent over any available network, be it the circuit-switched connection of TDMA (Time Division Multiple Access) IS-136 or packet-switched GPRS.

Added to this core transmission protocol are several scalable layers that can develop independently. The wireless transport layer security (WTLS) layer adds optional encryption facilities that enable secure transactions. WTP (WAP transaction protocol) adds transaction support, adding to the datagram service of WPD, while WSP (WAP session protocol) allows efficient data exchange between applications.

WAP also defines an application environment (WAE) that enables third-party developers to develop more advanced services and applications, along with the microbrowser used to access web pages on the handset itself.

To access internet content, the user's handset sends a request to the WAP gateway, which retrieves the information in either HTML (Hypertext Markup Language) or WML (Wireless Markup Language) from the host server. WML is a variation of HTML, designed specifically to enable viewing on the limited mobile terminal platform. If the information retrieved is in HTML, a filter in the gateway will attempt to convert it to WML. The information will then be transmitted to the handset over whatever network is available, using the transmission protocols described above.

In some cases, where HTML data is generated using a style sheet to convert XML data using an XSL processor, a WML style sheet can be added to the system to generate seamless information in the correct format for wireless viewing.

FUTURE OF WAP: Because WAP is a protocol designed to work over any mobile network, its use will continue to increase as more sophisticated data transmission technologies are introduced (e.g. GPRS, EDGE (Extended Data for Global Evolution) and W-CDMA (Wideband-CDMA)). As the bandwidth available to mobile terminals and the quality of displays improve, WAP can be enhanced to provide as effective an internet viewing experience as is possible on fixed terminals.

Q.4. What is CDMA? Explain in detail. **(10)**

Ans. Code Division Multiple Access (CDMA) is a sort of multiplexing that facilitates various signals to occupy a single transmission channel. It optimizes the use of available bandwidth. The technology is commonly used in ultra-high-frequency (UHF) cellular telephone systems, bands ranging between the 800-MHz and 1.9-GHz.

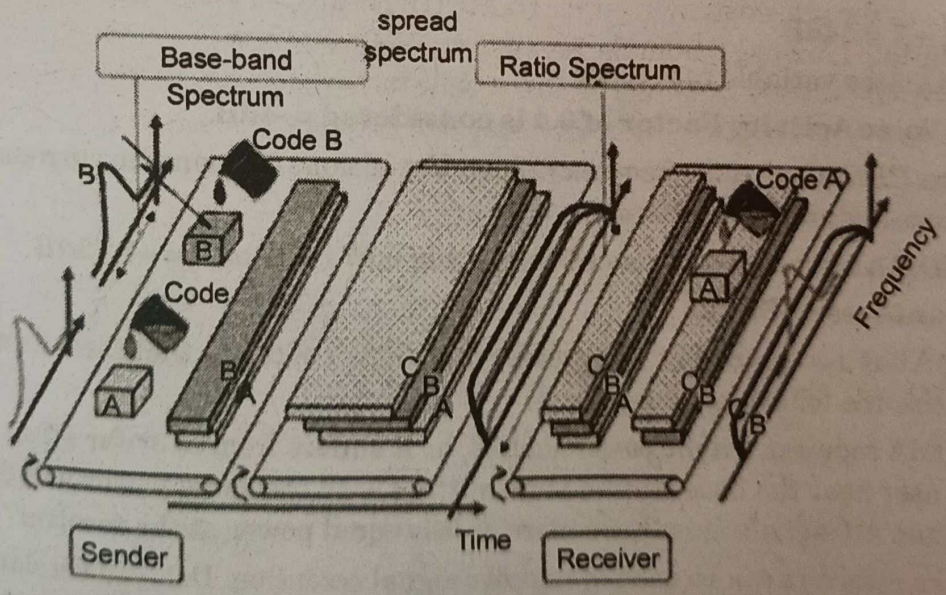
CDMA Overview: Code Division Multiple Access system is very different from time and frequency multiplexing. In this system, a user has access to the whole bandwidth for the entire duration. The basic principle is that different CDMA codes are used to distinguish among the different users.

Techniques generally used are direct sequence spread spectrum modulation (DS-CDMA), frequency hopping or mixed CDMA detection (JDCDMA). Here, a signal is generated which extends over a wide bandwidth. A code called **spreading code** is used to perform this action. Using a group of codes, which are orthogonal to each other, it is possible to select a signal with a given code in the presence of many other signals with different orthogonal codes.

How Does CDMA Work?: CDMA allows up to 61 concurrent users in a 1.2288 MHz channel by processing each voice packet with two PN codes. There are 64 Walsh codes available to differentiate between calls and theoretical limits. Operational limits and quality issues will reduce the maximum number of calls somewhat lower than this value.

In fact, many different "signals" baseband with different spreading codes can be modulated on the same carrier to allow many different users to be supported. Using different orthogonal codes, interference between the signals is minimal. Conversely, when signals are received from several mobile stations, the base station is capable of isolating each as they have different orthogonal spreading codes.

The following figure shows the technicality of the CDMA system. During the propagation, we mixed the signals of all users, but by that you use the same code as the code that was used at the time of sending the receiving side. You can take out only the signal of each user.



CDMA Capacity

The factors deciding the CDMA capacity are–

- Processing Gain
- Signal to Noise Ratio
- Voice Activity Factor
- Frequency Reuse Efficiency

Capacity in CDMA is soft, CDMA has all users on each frequency and users are separated by code. This means, CDMA operates in the presence of noise and interference.

In addition, neighboring cells use the same frequencies, which means no re-use. So, CDMA capacity calculations should be very simple. No code channel in a cell, multiplied by no cell. But it is not that simple. Although not available code channels are 64, it may not be possible to use a single time, since the CDMA frequency is the same.

Centralized Methods

- The band used in CDMA is 824 MHz to 894 MHz (50 MHz + 20 MHz separation).
- Frequency channel is divided into code channels.
- 1.25 MHz of FDMA channel is divided into 64 code channels.

Processing Gain: CDMA is a spread spectrum technique. Each data bit is spread by a code sequence. This means, energy per bit is also increased. This means that we get a gain of this.

P (gain) = 10log (W/R)

W is Spread Rate

R is Data Rate

For CDMA P (gain) = 10 log (1228800/9600) = 21dB

This is a gain factor and the actual data propagation rate. On an average, a typical transmission condition requires a signal to the noise ratio of 7 dB for the adequate quality of voice.

Translated into a ratio, signal must be five times stronger than noise.

Actual processing gain = P (gain) – SNR

= 21 – 7 = 14dB

CDMA uses variable rate coder

The Voice Activity Factor of 0.4 is considered = -4dB.

Hence, CDMA has 100% frequency reuse. Use of same frequency in surrounding cells causes some additional interference.

In CDMA frequency, reuse efficiency is 0.67 (70% eff.) = –1.73dB

Advantages of CDMA

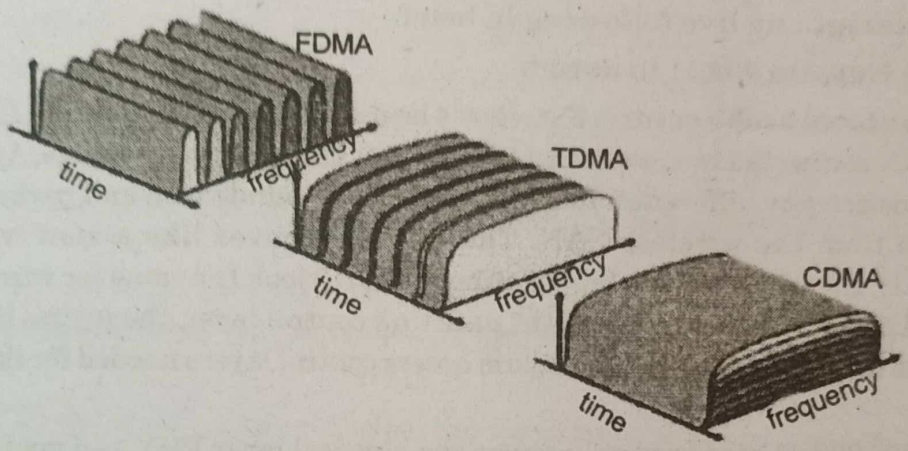
CDMA has a soft capacity. The greater the number of codes, the more the number of users. It has the following advantages

- CDMA requires a tight power control, as it suffers from near-far effect. In other words, a user near the base station transmitting with the same power will drown the signal latter. All signals must have more or less equal power at the receiver
- Rake receivers can be used to improve signal reception. Delayed versions of time (a chip or later) of the signal (multipath signals) can be collected and used to make decisions at the bit level.
- Flexible transfer may be used. Mobile base stations can switch without changing operator. Two base stations receive mobile signal and the mobile receives signals from the two base stations.
- Transmission Burst– reduces interference.

Disadvantages of CDMA

The disadvantages of using CDMA are as follows–

- The code length must be carefully selected. A large code length can induce delay or may cause interference.
- Time synchronization is required.
- Gradual transfer increases the use of radio resources and may reduce capacity.
- As the sum of the power received and transmitted from a base station needs constant tight power control. This can result in several handovers.



END TERM EXAMINATION [MAY-JUNE 2018]
EIGHTH SEMESTER [B.TECH]
MOBILE COMPUTING [ETIT–402]

Time : 3 hrs. **M.M. : 75**

Note: *Attempt any five questions including Q. No. 1 which is compulsory.*

Q.1. Attempt any five following in brief: **(5)**

Q.1. (a) Explain 802.11 in detail.

Ans. Protocol architecture: Fig. shows he most common scenario: an IEEE 802.11 wireless LAN connected to a, switched IEEE 802.3 Ethernet via a bridge, Applications should not notice any difference apart from the lower bandwidth and perhaps, higher access time from the wireless LAN. The WLAN behaves like a slow wired LAN. Consequently, the higher layers (application, TCP, IP) look the same for wireless nodes as for wired nodes The upper part of the data link control layer, the logical link control (LLC),covers the differences of the medium access control layers needed for the different media.

The IEEE 802.11 standard only covers the physical layer PHY and medium access layer MAC like the other 802.x LANs do. The physical layer is subdivided into the **physical layer convergence protocol (PLCP)** and the physical **medium dependent sublayer** PMD (see Figure). The basic tasks of the MAC layer comprise medium access, fragmentation of user data, and encryption. The PLCP sublayer provides a carrier sense signal, called clear channel assessment (CCA), and provides a common PHY service access point (SAP) independent of the transmission technology. Finally, the PMD sublayer handles modulation and encoding/decoding of signals.

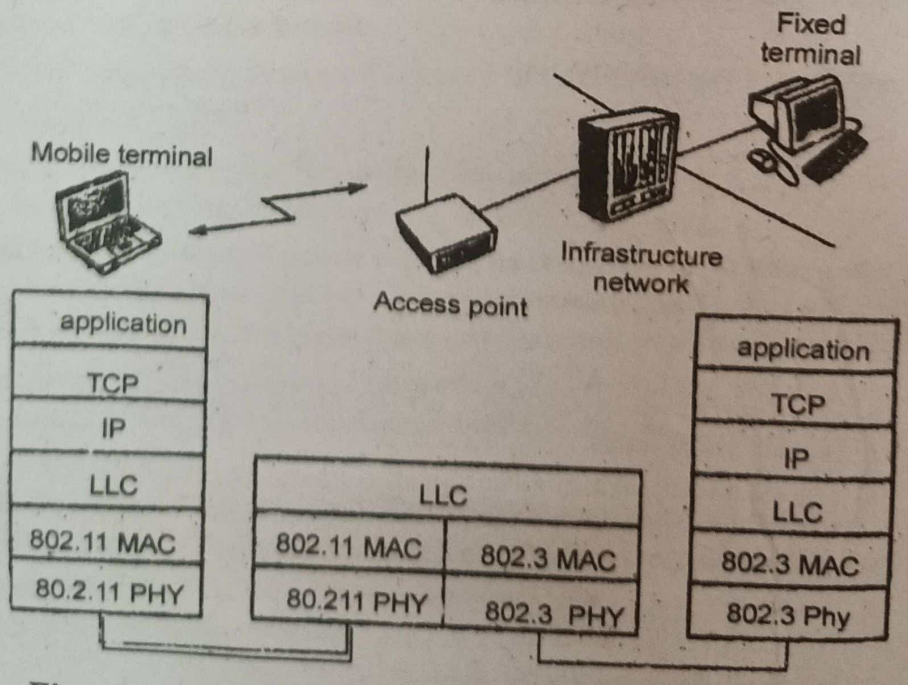


Fig. IEEE 802.11 protocol architecture and bridging

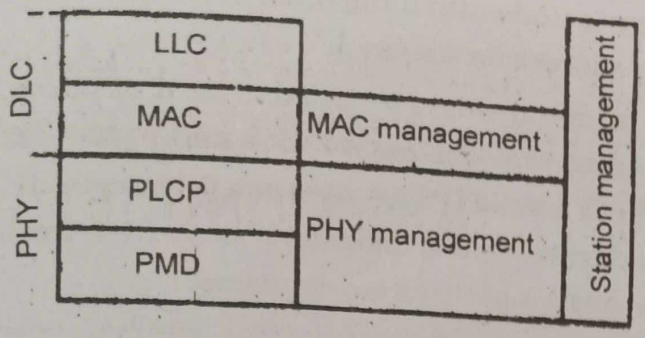


Fig. Detailed IEEE 802.11 protocol architecture and management

Q.1. (b) Differentiate between hidden terminal and exposed terminal. (5)

Ans. Refer to Q.8. (a) End Term Examination 2017, (pg: 30-2017)

Q.1. (c)Differentiate between Aloha and Slotted Aloha. (5)

Ans. Refer to Q.5. (a) End Term Examination 2017, (pg: 24-1017)

Q.1. (d) Differentiate between distance vector routing and dynamic source routing. (5)

Ans. Refer to Q.4. (b) End Term Examination 2017, (pg: 22-2017)

Q.1. (e) Differentiate between IP and Mobile IP.

Ans. IP

Internet Protocol (IP) is the principal set (or communications protocol) of digital message formats and rules for exchanging messages between computers across a single network or a series of interconnected networks, using the Internet Protocol Suite (often referred to as TCP/IP). Messages are exchanged as datagram, also known as data packets or just packets.

IP is the primary protocol in the Internet Layer of the Internet Protocol Suite, which is a set of communications protocols consisting of four abstraction layers: link layer (lowest), Internet layer, transport layer and application layer (highest).

The main purpose and task of IP is the delivery of datagram from the source host (source computer) to the destination host (receiving computer) based on their addresses. To achieve this, IP includes methods and structures for putting tags (address information, which is part of metadata) within datagram. The process of putting these tags on datagram is called encapsulation.

Think of an analogy with the postal system. IP is similar to the U.S. Postal System in that it allows a package (a datagram) to be addressed (encapsulation) and put into the system (the Internet) by the sender (source host). However, there is no direct link between sender and receiver.

The package (datagram) is almost always divided into pieces, but each piece contains the address of the receiver (destination host). Eventually, each piece arrives at the receiver, often by different routes and at different times. These routes and times are also determined by the Postal System, which is the IP. However, the Postal System (in the transport and application layers) puts all the pieces back together before delivery to the receiver (destination host).

Mobile IP: Mobile IP communication protocol refers to the forwarding of Internet traffic with a fixed IP address even outside the home network. It allows users having wireless or mobile devices to use the Internet remotely.

Mobile IP is mostly used in WAN networks, where users need to carry their mobile devices across different LANs with different IP addresses. Mobile IP is not a wireless protocol. However, it could be employed for the IP infrastructure of cellular networks.

A simple analogy to understand the concept is a person who has left vacation and set his a forwarding address for his mail.

When a mobile terminal enters a visited area, it requires the services of a foreign agent. The foreign agent provides registration and packet-forwarding services to the visiting terminals. Each mobile IP host uses one permanent IP address (home address) and one temporary address (care-of address) if away from the home network. Thus, the IP packet exchange consists of three mechanisms:

1. Discovering the care-of address.
2. Registering the care-of address with the home agent.
3. The home agent redirecting the received datagram to the foreign network using care-of address.

Care-of IP addresses are temporary IP addresses are given by the network outside the home network so devices can stay connected while on the move. The device gets a new care-of address if the user moves to another network.

Q.1. (f) What is the function of IOS? Write a note on Android and list the four layer structure of Android. (5)

Ans. Function of iOS: iOS is a mobile operating system developed by Apple. It was originally named the iPhone OS, but was renamed to the iOS in June, 2009. The iOS currently runs on the iPhone, iPod touch, and iPad.

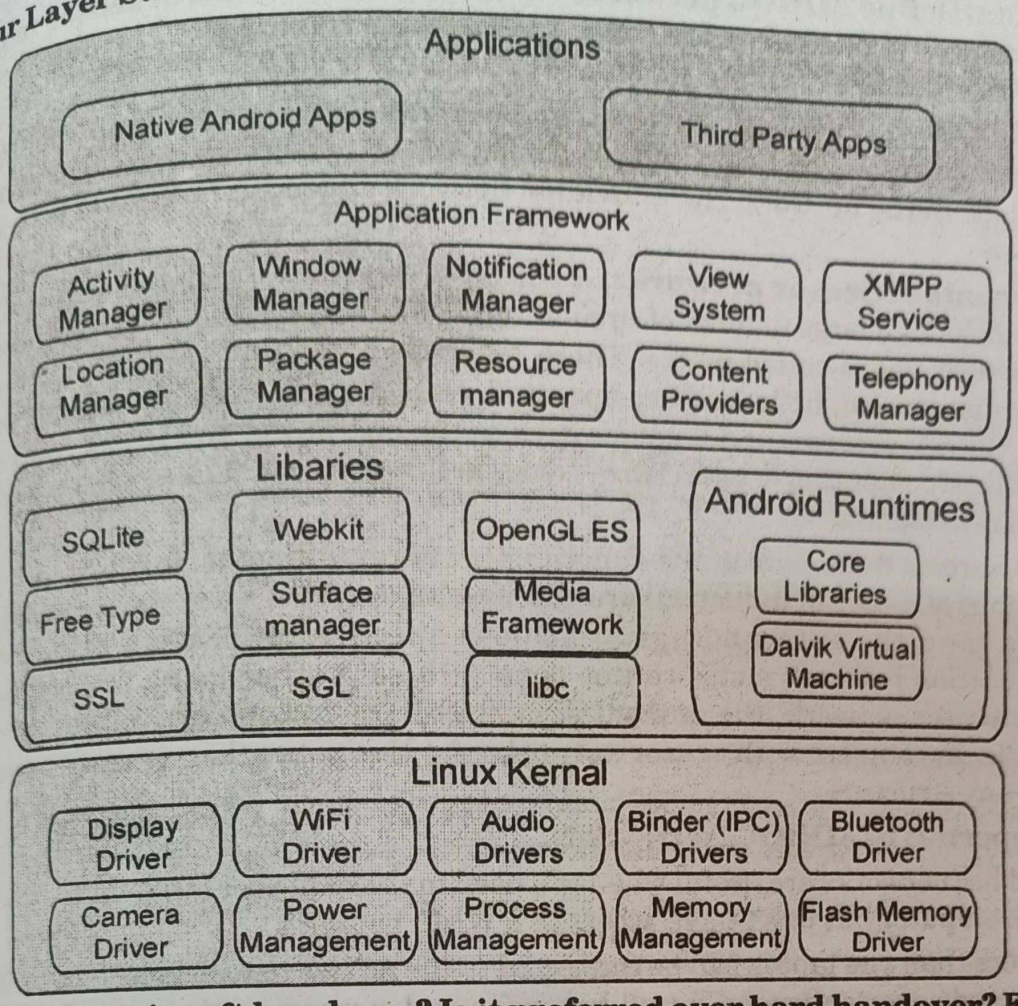
Like modern desktop operating systems, iOS uses a graphical user interface, or GUI. However, since it is a mobile operating system, iOS is designed around touchscreen input, rather than a keyboard and mouse.

Since iOS is designed to be simple and easy to use, it does not include several features found in a traditional operating system. For example, you cannot manage files and folders like you can in Mac OS X or Windows. You also have limited access to iOS system settings. Instead of modifying application preferences from within each program, most settings need to be adjusted within the Settings app. Additionally, while you can run multiple programs at once, you can only view one open program at a time.

Note on Android: Android is a Linux based operating system it is designed primarily for touch screen mobile devices such as smart phones and tablet computers. The operating system has developed a lot in last 15 years starting from black and white phones to recent smart phones or mini computers. One of the most widely used mobile OS these days is android. The android is software that was founded in Palo Alto of California in 2003.

The android is a powerful operating system and it supports large number of applications in Smartphones. These applications are more comfortable and advanced for the users. The hardware that supports android software is based on ARM architecture platform. The android is an open source operating system means that it's free and any one can use it. The android has got millions of apps available that can help you managing your life one or other way and it is available low cost in market at that reasons android is very popular.

Four Layer Structure of Android



Q.1. (g) What is soft handover? Is it preferred over hard handover? Explain. **(5)**

Ans . Hard handoff: It means that all the old radio links in the MS are removed before the new radio links are established. In GSM, it is general. we can say Break before Make. So in this case higher rates of call drops is found.

Soft Handoff: It means the radio links are added and removed in a way that the MS always keeps at least one radio link to the UTRAN. In CDMA this technique is performed. In simple words we can say Make before Break. To lower the rates of call drops, this technique is used.

Softer Handoff: It is a special case of soft handover where the radio links that are added and removed belong to the same site of co-located base stations from which several sector-cells are served i.e. Node B.

But in a simpler way it can be said as below:

Hard Handover:- When mobile(in Call) switches to a new sector/Cell which is on different frequency , then it performs hard Handover. It is basically an inter-frequency handover.

Soft Handover:- When mobile (in Call) switches to a new sector/cell which is on the same frequency then it is called a soft handover.

Soft handover is preferred over hard handover because call drops are less in case of soft handover. It overlaps of repeater coverage zones, so that every cell phone set is always well within range of at least one repeater (also called a base station). In some cases, mobile sets transmit signals to, and receive signals from, more than one repeater at a time.

Q.2. (a)Define ADHOC networks. What are the elements of sensor networks? Enlist various properties of ADHOC networks. What are the various challenges in ADHOC network? (6)

Ans. An ad-hoc network is a local area network (LAN) that is built spontaneously as devices connect. Instead of relying on a base station to coordinate the flow of messages to each node in the network, the individual network nodes forward packets to and from each other.

Elements of Sensor networks: A Wireless Sensor Network is one kind of wireless network includes a large number of circulating, self-directed, minute, low powered devices named sensor nodes called motes. These networks certainly cover a huge number of spatially distributed, little, battery-operated, embedded devices that are networked to caringly collect, process, and transfer data to the operators, and it has controlled the capabilities of computing & processing. Nodes are the tiny computers, which work jointly to form the networks.

The sensor node is a multi-functional, energy efficient wireless device. The applications of motes in industrial are widespread. A collection of sensor nodes collects the data from the surroundings to achieve specific application objectives. The communication between motes can be done with each other using transceivers. In a wireless sensor network, the number of motes can be in the order of hundreds/ even thousands. In contrast with sensor networks, Ad Hoc networks will have fewer nodes without any structure.

Properties of ADHOC Networks:

- Ad hoc networks are useful when you need to share files or other data directly with another computer but don't have access to a Wi-Fi network.
- More than one laptop can be connected to the ad hoc network, as long as all of the adapter cards are configured for ad-hoc mode and connect to the same SSID (service state identifier). The computers need to be within 100 meters of each other.
- If you are the person who sets up the ad hoc network, when you disconnect from the network, all the other users are also disconnected. An ad hoc network is deleted when everyone on it disconnects—which can be good or bad, depending on your view; it's truly a spontaneous network.
- You can use an ad hoc wireless network to share your computer's internet connection with another computer.

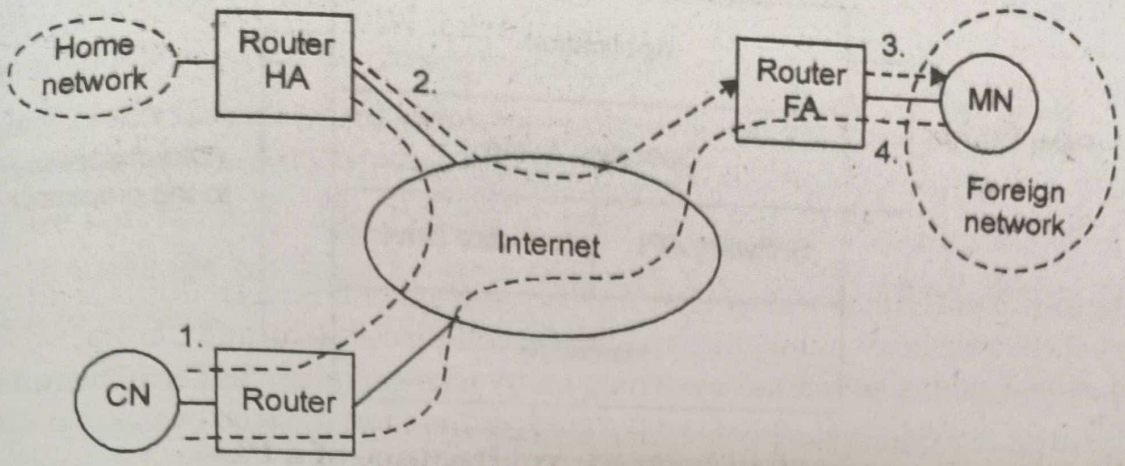
Challenges in ADHOC Networks:

The ad hoc networks are self-forming, self-maintaining,

- Self-healing architecture.
- No fixed access point
- Dynamic network topology
- Contrary environment
- Irregular connectivity.
- Ad hoc network
- Immediately forms and accommodate the modification and limited power.
- Finally, ad hoc have no trusted centralized authority

Q.2. (b)Explain the process of IP packet delivery. (6.5)

Ans. The mobile i.e. movement of Mobile Node (MN) from one location to another has to be hidden as per the requirement of mobile IP. Correspondent Node (CN) may not know the exact location of MN.



STEP 1: CN sends the packet as usual to the IP address of MN. With Source address as CN and Destination address as MN .The internet, that does not have any information of 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.

STEP 2: The HA now diverts 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 tunneled 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 (FA) now decapsulates the packet, i.e., removes the additional header (newly added as COA as destination and HA as source), and forwards the original packet with CN as source and MN as destination to the MN. Again, for the MN mobility is not visible.

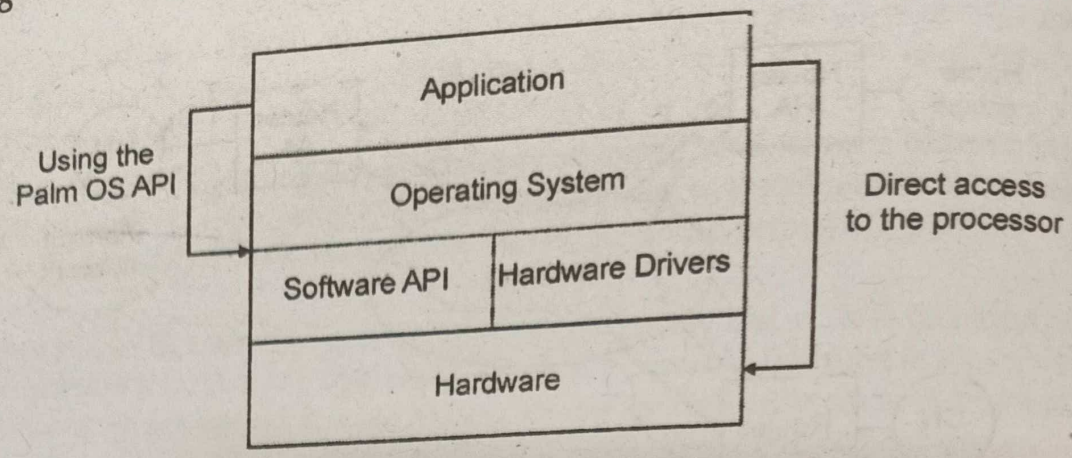
Finally the MN Receives the packet with the Source address as CN and Destination address as MN.

STEP 4: The MN sends the packet MN as Source Address and CN as Destination Address. 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. Simple mechanism works if CN is fixed at a location if it has got mobility then the above Steps 1 to 3 are to be followed to deliver the packet from MN to CN.

Q.3. (a) Elaborate the architecture of Palm OS and explain in brief. (6)

Ans. At the highest level, the architecture of the Palm OS device, and most other PDAs, can be broken down into three layers: Application, Operating System, and Hardware.

Use of the Palm OS Application Programming Interface (API) provides the application developer with a notion of hardware independence and provides a layer of abstraction. If the API is used properly, recompiling of the application is all that is necessary in order to run on Palm OS devices based on different hardware. Therefore, it is important to examine weaknesses and attack vectors that can be found at the programming interface to the operating system.

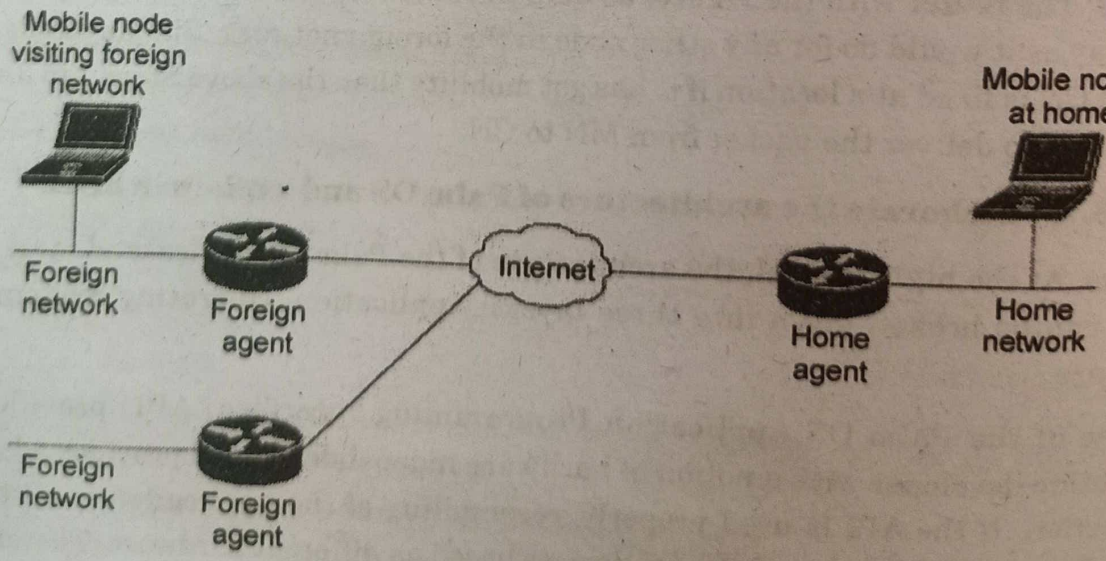


Typical layered architecture of a PDA

Directly accessing the processor by avoiding the interface put forward by the operating system allows the developer to have more control of the processor and its functionality. A risk of legitimate use of direct processor access is the loss of compatibility for future models. For example, older Palm OS devices did not support a grayscale LCD palette through the Palm OS API, even though the underlying hardware possessed this capability. Bypassing this interface and tapping into the functionality of the processor directly will remedy this. Ideally, to provide some semblance of access control and security, only the operating system should have access to the underlying hardware. Allowing applications to directly access hardware provides an avenue for malicious attack.

Q.3. (b)Explain the process of agent discovery. How the agent advertisement messages are transferred? Explain. **(6.5)**

Ans. When a mobile node is first turned on, it cannot assume that it is still "at home" the way normal IP devices do. It must first determine where it is, and if it is not at home, begin the process of setting up datagram forwarding from its home network. This process is accomplished by communicating with a local router serving as an agent, through the process called agent discovery.



Mobile IP components

Agent Discovery Process

The main goals of agent discovery include the following:

1. Agent/Node Communication: Agent discovery is the method by which a mobile node first establishes contact with an agent on the local network to which it is attached. Messages are sent from the agent to the node containing important information about the agent; a message can also be sent from the node to the agent asking for this information to be sent.

2. Orientation: The node uses the agent discovery process to determine where it is. Specifically, it learns whether it is on its home network or a foreign network by identifying the agent that sends it messages.

3. Care-Of Address Assignment: The agent discovery process is the method used to tell a mobile node the care-of address it should use, when foreign agent care-of addressing is used.

Mobile IP agents are routers that have been given additional programming to make them "Mobile IP aware". The communication between a mobile node and the agent on its local network is basically the same as the normal communication required between a device on an IP network and its local router, except more information needs to be sent when the router is an agent.

Agent Advertisement

Mobile nodes use agent advertisements to determine their current point of attachment to the Internet or to an organization's network. An agent advertisement is an Internet Control Message Protocol (ICMP) router advertisement that has been extended to also carry a mobility agent advertisement extension.

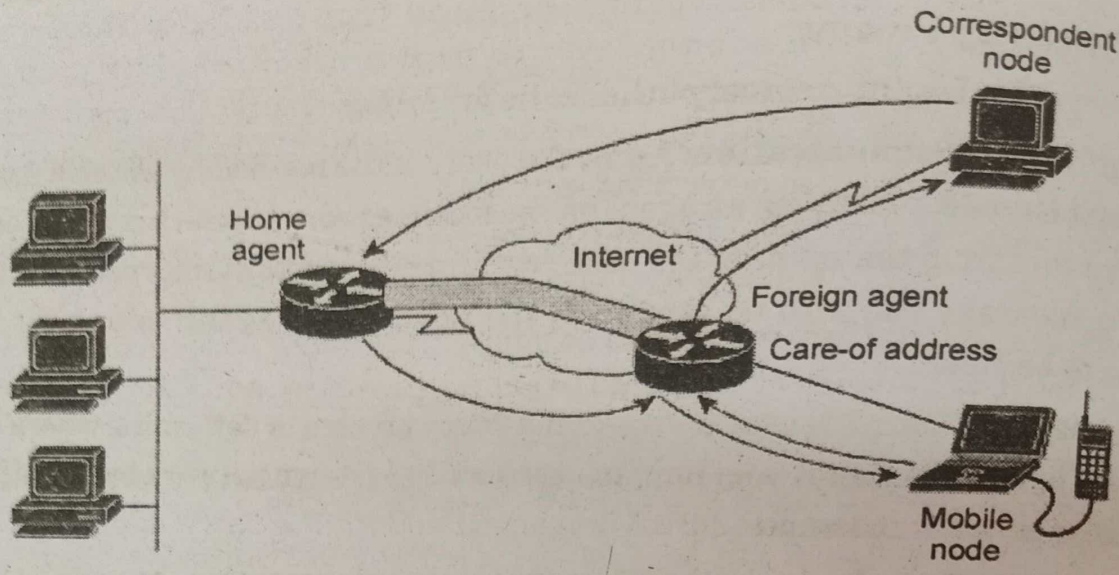
A foreign agent can be too busy to serve additional mobile nodes. However, a foreign agent must continue to send agent advertisements. This way, mobile nodes that are already registered with it will know that they have not moved out of range of the foreign agent and that the foreign agent has not failed.

Q.4. (a) Differentiate between tunneling, reverse tunneling, and encapsulation. **(6)**

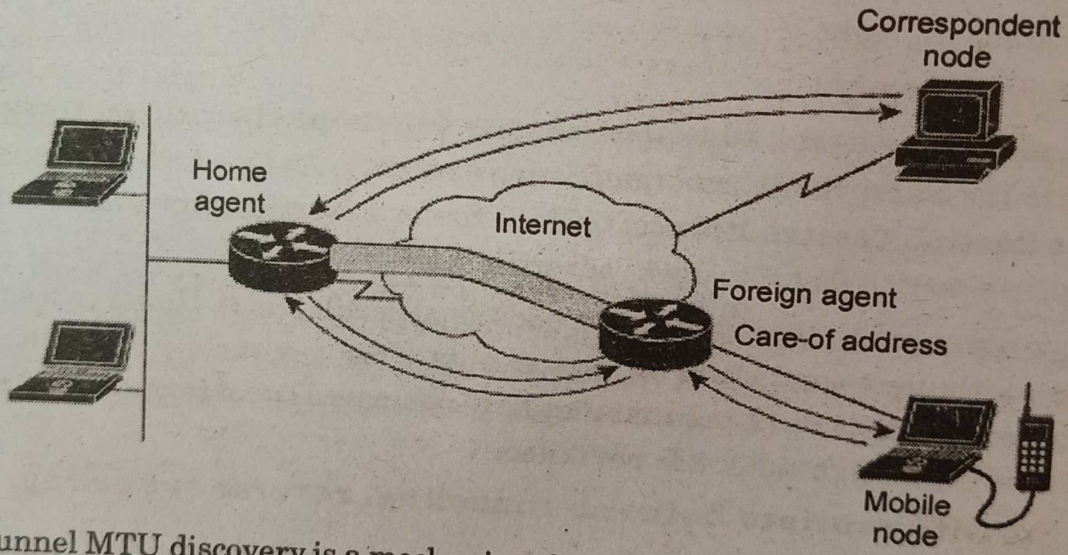
Ans. The Mobile Node sends packets using its home IP address, effectively maintaining the appearance that it is always on its home network. Even while the Mobile Node is roaming on foreign networks, its movements are transparent to correspondent nodes.

Data packets addressed to the Mobile Node are routed to its home network, where the Home Agent now intercepts and tunnels them to the care-of address toward the Mobile Node. Tunneling has two primary functions: encapsulation of the data packet to reach the tunnel endpoint, and decapsulation when the packet is delivered at that endpoint. The default tunnel mode is IP Encapsulation within IP Encapsulation. Optionally, GRE and minimal encapsulation within IP may be used.

Typically, the Mobile Node sends packets to the Foreign Agent, which routes them to their final destination, the Correspondent Node



However, this data path is topologically incorrect because it does not reflect the true IP network source for the data—rather, it reflects the home network of the Mobile Node. Because the packets show the home network as their source inside a foreign network, an access control list on routers in the network called ingress filtering drops the packets instead of forwarding them. A feature called reverse tunneling solves this problem by having the Foreign Agent tunnel packets back to the Home Agent when it receives them from the Mobile Node.



Tunnel MTU discovery is a mechanism for a tunnel encapsulator such as the Home Agent to participate in path MTU discovery to avoid any packet fragmentation in the routing path between a Correspondent Node and Mobile Node. For packets destined to the Mobile Node, the Home Agent maintains the MTU of the tunnel to the care-of address and informs the Correspondent Node of the reduced packet size. This improves routing efficiency by avoiding fragmentation and reassembly at the tunnel endpoints to ensure that packets reach the Mobile Node.

A tunnel establishes a virtual pipe for data packets between a tunnel entry and a tunnel endpoint. Packets entering a tunnel are forwarded inside the tunnel and leave the tunnel unchanged. Tunneling, i.e., sending a packet through a tunnel is achieved by using encapsulation

Encapsulation is the mechanism of taking a packet consisting of packet header and data and putting it into the data part of a new packet. The reverse operation, taking a packet out of the data part of another packet, is called de-capsulation. Encapsulation

and de-capsulation are the operations typically performed when a packet is transferred from a higher protocol layer to a lower layer or from a lower to a higher layer respectively.The HA takes the original packet with the MN as destination, puts it into the data part of a new packet and sets the new IP header so that the packet is routed to the COA.The new header is called outer header.

Types of Encapsulation Three types of encapsulation protocols are specified for Mobile IP:

1. IP-in-IP encapsulation: required to be supported. Full IP header added to the original IP packet. The new header contains HA address as source and Care of Address as destination.

2. Minimal encapsulation: optional. Requires less overhead but requires changes to the original header. Destination address is changed to Care of Address and Source IP address is maintained as is.

3. Generic Routing Encapsulation (GRE): optional. Allows packets of a different protocol suite to be encapsulated by another protocol suite.

Q.4. (b) Explain the architecture of Symbion OS in brief. **(6.5)**

Ans. Symbian OS Architecture

The strength of Symbian OS lies in its small foothprint (the kernal is less than 200 Kb,) adaptability to limited memory devices, a powerful power management model, a robust software layer conforming to industry standards, and support for integration with a. plethora of peripheral hardware. The foundation for this is a fast, low power, low cost CPU core. The Symbian OS works a top the ARM architecture RISC processors (with V4 instruction set or higher). Supported processors including ARMv4T, ARMvST, ARMvSTJ and Intel x86 (for the emulator). The CPU is expected to be equipped with an integrated memory management unit (MMU) and a cache.

As in any other OS, the main objective of the OS is to provide hardware abstraction and manage system resources. A Symbian system can be divided into three layers Fig. where the bottom most layer interacts with the underlying hardware/hardware abstaction layer as the case maybe. This layer includes the kernel, memory, device, drivers and file services. On top of this are the network and security support components. Also included are multimedia and communication protocol implimentations. The third layer is the application framework and applications support mechanism for PC synchronization, Bluetooth and USB support. The topmost layer of course is the development environment and the applications themselves.

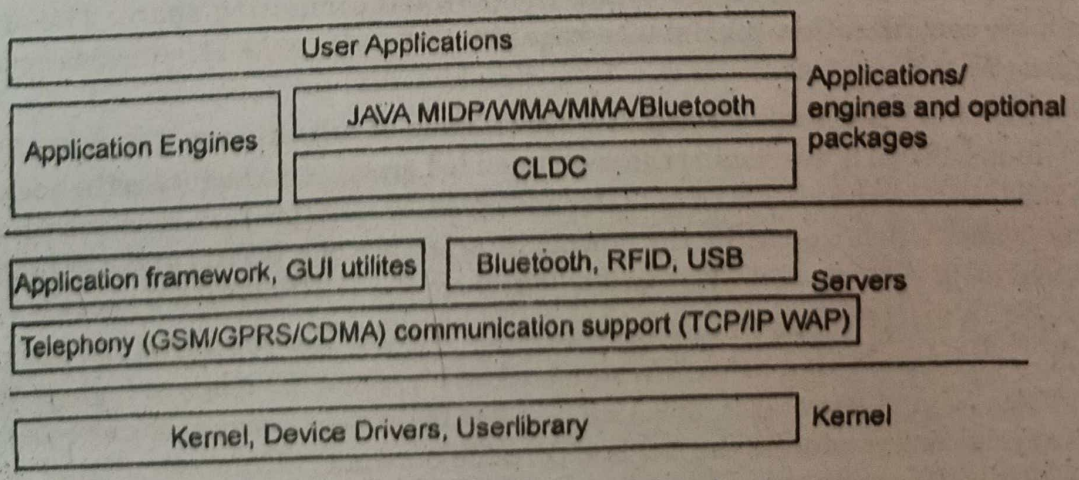


Fig. Symbian OS Architecture

Symbian OS supports pre-emptive multitasking. All system services run in privileged mode, while user applications run in a user context. When an application requests a system service it is temporarily given privileged access through a context switch. This mechanism is conceptually similar to that in UNIX/WindowsNT. The MMU is designed for interrupt handling and privileged access modes. The CPU, MMU and cache along with timers and hardware drivers, all reside on the chip.

The kernel encapsulates the system services like multitasking, file services, power management, memory management and the various device drivers. It includes support for the telephony services for GSM, GPRS, CEMA and the security features. Version 8.0 boasts of powerful/kernel architecture with hard real-time capabilities. It provides the programming framework in the form of an abstraction making it easier to port Symbian OS.

Q.5. (a) Explain the architecture of IEEE 802.15 and discuss its characteristic in brief. Elaborate the security issues in IEEE 802.15. **(6.5)**

Ans. 802.15 is a specification driven by the Institute of Electrical and Electronics Engineers (IEEE) to develop consensus standards for short-range wireless networks or wireless personal area networks. It has similar goals to Bluetooth in that it looks to address wireless networking of portable and mobile computing devices such as PCs, PDAs, mobile phones, peripherals, and consumer electronics. The 802.15 WPAN Working Group was established in 1999 as part of the Local and Metropolitan Area Networks Standards Committee of the IEEE.

At the time of establishment, the 802.15 WPAN Working Group was aware of the Bluetooth specification and used parts of it as the foundation for the 802.15 standard. The 802.15 WPAN specifications is aimed at standardizing the Media Access Control (MAC) and Physical (PHY) layers of Bluetooth, in the attempt to accommodate wider adoption of short-range wireless technology. 802.15 also deal with issues such as coexistence and interoperability within the networks. To accomplish this goal, four task groups have been established, each working on specific components of the 802.15 specifications. They are:

- **802.15 WPAN Task Group 1: WPAN/Bluetooth.** The WPAN Task Group 1 (TG1) has created the WPAN 802.15.1 standard based on the Bluetooth v1.1 specification. To accomplish this, the IEEE licensed technology from the Bluetooth SIG. Specifically; 802.15.1 defines the MAC and PHY specifications for wireless connectivity of devices that are either fixed or portable within the personal computing space. The spec also takes into consideration coexistence requirements with 802.11 wireless local area network (WLAN) devices.

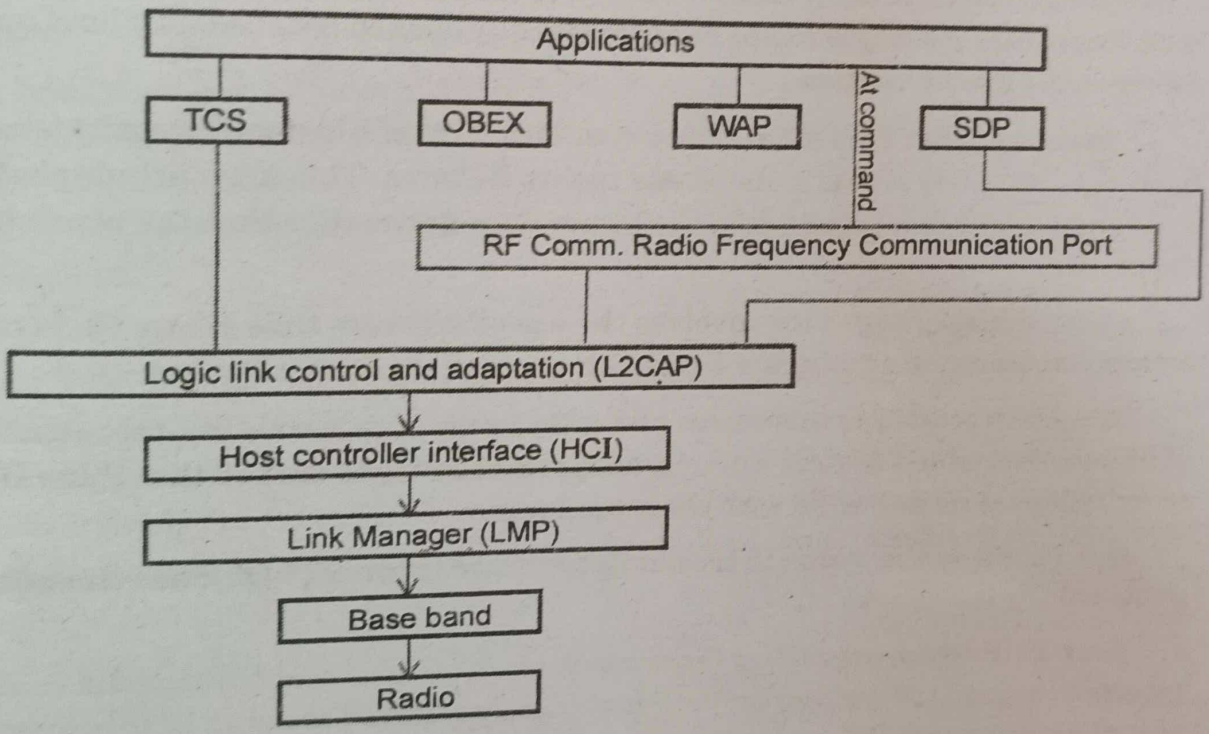
- **802.15 WPAN Task Group 2: Coexistence Mechanisms.** The 802.15 WPAN Task Group 2 (TG2) is developing the recommended practices to facilitate the coexistence of WPAN (802.15) and WLAN (802.11) technologies. Part of this task involves developing a coexistence model to quantify the mutual interference of a WPAN and a WLAN. Once approved, this outcome of TG2's work will become the IEEE 802.15.2 specification.

- **802.15 WPAN Task Group 3: High Rate WPAN.** The 802.15 WPAN Task Group 3 (TG3) is chartered to publish a new standard for high-rate (20 Mbps or higher) WPANs. In addition to high data rates, 802.15.3 also has to provide a means for low-power and low-cost solutions to address the needs of portable consumer electronics, digital imaging, and multimedia applications.

• **802.15 WPAN Task Group 4: Low Rate-Long Battery Life.** The 802.15 WPAN Task Group 4 (TG4) is chartered to establish a low-data-rate (200 Kbps maximum) solution with long battery life (many months to many years) and low complexity. It is intended to operate in an unlicensed international frequency band and is targeted at sensors, interactive toys, smart badges, home automation, and remote controls.

The 802.15 specification is still a work in progress as each of the task groups is at different stages in the specification process. TG1 has completed the 802.15.1 specification and has gotten approval from the IEEE Standards Association (IEEE-SA), while the other groups are still working toward that level. Once completed, the 802.15 WPAN specification will cover all of the current issues surrounding WPAN technology, including Bluetooth compatibility, coexistence with 802.11, high-data transfer rates, and low-power consumption solutions. The combination of all of these will make the IEEE 802.15 specification very attractive for WPAN infrastructure providers.

The protocol architecture of Bluetooth is given below:



The radio layer is responsible for:

* Modulation/Demodulation of data for transmitting (OR) receiving over air.

The base band layer is responsible for:

* Controlling the physical links via radio
* Assembling the packets
* Controlling frequency hopping.

The link manager protocol controls and configures links to other devices.

The host controller interface(HCI) handles communication between the host and the module. For this purpose, it uses several HCI command packets such as the even packets and data packets. The L2CAP layer converts the data obtained from higher layers into packets of different sizes.

The RF COMM provides a serial interface with wireless application protocol (WAP) and object exchange(OBEX).

WAP and OBEX provide interface to other communications protocols.

The TCS(Telephone control protocol specification) provide telephony service.

The SDP(Service discovery protocol) allows the devices to discover the services available on another Bluetooth enabled device.

The applications present in the application layer can extract the services of the lower layers by using one of the many profiles available.

Common Bluetooth security issues

There are a number of ways in which Bluetooth security can be penetrated, often because there is little security in place. The major forms of Bluetooth security problems fall into the following categories:

- ***Bluejacking:*** Bluejacking is often not a major malicious security problem, although there can be issues with it, especially as it enables someone to get their data onto another person's phone, etc. Bluejacking involves the sending of a vCard message via Bluetooth to other Bluetooth users within the locality - typically 10 metres. The aim is that the recipient will not realise what the message is and allow it into their address book. Thereafter messages might be automatically opened because they have come from a supposedly known contact.

- ***Bluebugging:*** This more of an issue. This form of Bluetooth security issue allows hackers to remotely access a phone and use its features. This may include placing calls and sending text messages while the owner does not realise that the phone has been taken over.

- ***Car Whispering:*** This involves the use of software that allows hackers to send and receive audio to and from a Bluetooth enabled car stereo system

In order to protect against these and other forms of vulnerability, the manufacturers of Bluetooth enabled devices are upgrading he security to ensure that these Bluetooth security lapses do not arise with their products.

Q.5. (b) How the voice is transmitted over internet? Discuss the concerned protocol for it. (6)

Ans. VoIP (voice over IP) is the transmission of voice and multimedia content over Internet Protocol (IP) networks. VoIP historically referred to using IP to connect private branch exchanges (PBXs), but the term is now used interchangeably with IP telephony.

VoIP is enabled by a group of technologies and methodologies used to deliver voice communications over the internet, enterprise local area networks or wide area networks. VoIP endpoints include dedicated desktop VoIP phones, softphone applications running on PCs and mobile devices, and WebRTC-enabled browsers.

How does VoIP work?

VoIP uses codecs to encapsulate audio into data packets, transmit the packets across an IP network and unencapsulate the packets back into audio at the other end of the connection. By eliminating the use of circuit-switched networks for voice, VoIP reduces network infrastructure costs, enables providers to deliver voice services over their broadband and private networks, and allows enterprises to operate a single voice and data network.

VoIP also piggybacks on the resiliency of IP-based networks by enabling fast failover following outages and redundant communications between endpoints and networks.

VoIP protocols and standards

VoIP endpoints typically use International Telecommunication Union (ITU) standard codecs, such as G.711, which is the standard for transmitting uncompressed packets, or G.729, which is the standard for compressed packets.

Many equipment vendors also use their own proprietary codecs. Voice quality may suffer when compression is used, but compression reduces bandwidth requirements. VoIP typically supports non-voice communications via the ITU T.38 protocol to send faxes over a VoIP or IP network in real time.

Once voice is encapsulated onto IP, it is typically transmitted with the Real-Time Transport Protocol (RTP) or through its encrypted variant, the Secure Real-Time Transport protocol. The Session Initiation Protocol (SIP) is most often used to signal that it is necessary to create, maintain and end calls.

Within enterprise or private networks, quality of service (QoS) is typically used to prioritize voice traffic over non-latency-sensitive applications to ensure acceptable voice quality.

Additional components of a typical VoIP system include the following: an IP PBX to manage user telephone numbers; devices; features and clients; gateways to connect networks and provide failover or local survivability in the event of a network outage; and session border controllers to provide security, call policy management and network connections.

A VoIP system can also include location-tracking databases for E911 — enhanced 911 — call routing and management platforms to collect call performance statistics for reactive, and proactive voice-quality management.

VoIP telephones: The two main types of VoIP telephones are hardware-based and software-based.

A hardware-based VoIP phone looks like a traditional hard-wired or cordless telephone and includes similar features, such as a speaker or microphone, a touchpad, and a caller ID display. VoIP phones can also provide voicemail, call conferencing and call transfer.

Software-based IP phones, also known as softphones, are software clients installed on a computer or mobile device. The softphone user interface often looks like a telephone handset with a touchpad and caller ID display. A headset equipped with a microphone connects to the computer or mobile device to make calls. Users can also make calls via their computer or mobile device if they have a built-in microphone and speaker.

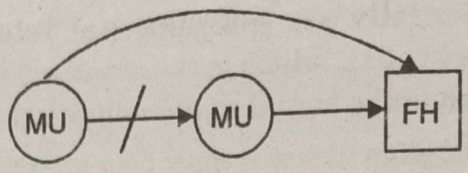
Q.6. (a) How the data replication in mobile computing is handled? Explain asynchronous replication. Differentiate between online data replication and offline data replication.

Q.6. (b) How the movements of user affect data replication? Explain. (6)

Ans. Data replication.

- Allocate replicas of mobile user's data on fixed sites in the network.
- Now it becomes possible to handle access requests from other users locally on the fixed sites, without accessing the owner MH
- So now instead of MU (or a FH) talking to a MH

• AMU (or a FH) can now talk to a FH.



Asynchronous replication: Asynchronous replication is a store and forward approach to data backup or data protection.

Asynchronous replication writes data to the primary storage array first and then, depending on the implementation approach, commits data to be replicated to memory or a disk-based journal. It then copies the data in real-time or at scheduled intervals to replication targets.

The benefits of asynchronous replication

There are two main benefits to asynchronous replication:

• **It tends to cost significantly less than synchronous replication.** Synchronous replication requires more bandwidth than asynchronous replication and may also require specialized hardware (depending on the implementation).

• **It is designed to work over long distances.** Since the replication process does not have to occur in real time, asynchronous replication can tolerate some degradation in connectivity.

Synchronous replication is typically used to provide high availability of critical applications. In this scenario, failover from the primary to secondary array is nearly instantaneous, to ensure little to no application downtime. As noted above, it is also expensive.

Data Replication Strategies

• Static replica allocation (SRA): locations of replicas are fixed, regardless of movements of MU

Dynamic strategies:

• Primary-copy tracking replication allocation (PTRA)

• User majority replication allocation (UMRA)

SRA Strategy

• We assume MH do not move too far from their location server.

Server replicates the copy of data at the mobile client

• On each write, the server needs to write to the copy on the mobile client

• Reading is from a loial copy on the mobile client

• The replicated copy resides at the location server of the client

• Client reads from its own location server

• Reads and writes are on the same copies

- Copy is closer to the reader than the writer

The server has a copy of data at its home location server

- Client reads from the home location server

- Reads and writes are on the same copies

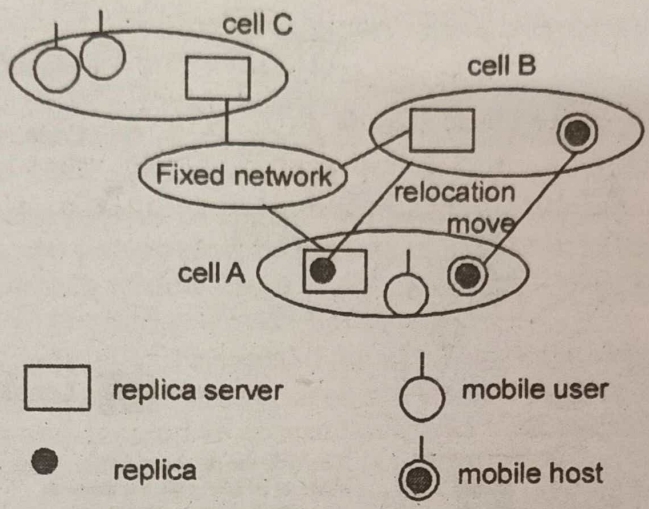
- Copy is closer to the writer than the reader

• Replica is always allocated at the replica server in the cell where its owner MH exists

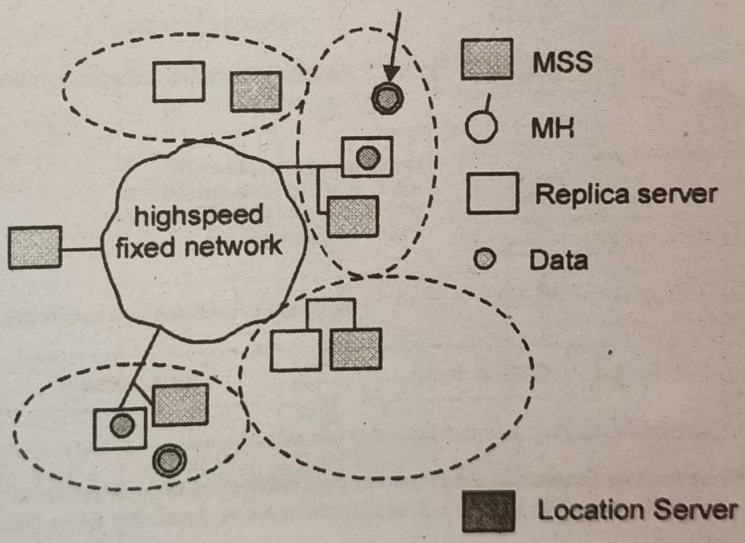
• Replica relocation is done as the MH moves from cell to cell

• When a MH enters a cell, it registers itself to the new cell by notifying the location server

• The location server will query the previous location of the MH and will issue a replication relocation request to the coordinator of the previous location



Architecture



We shall extend the definition of a MU to a MH

• MH can act as a data client and a data server at the same time

– MH, as a data server, is to support transaction operations such as read, write prepare, and abort

• MH, as a data client, must submit transaction operations to the coordinator laid on the MSS of its current cell (if request cannot be satisfied locally)

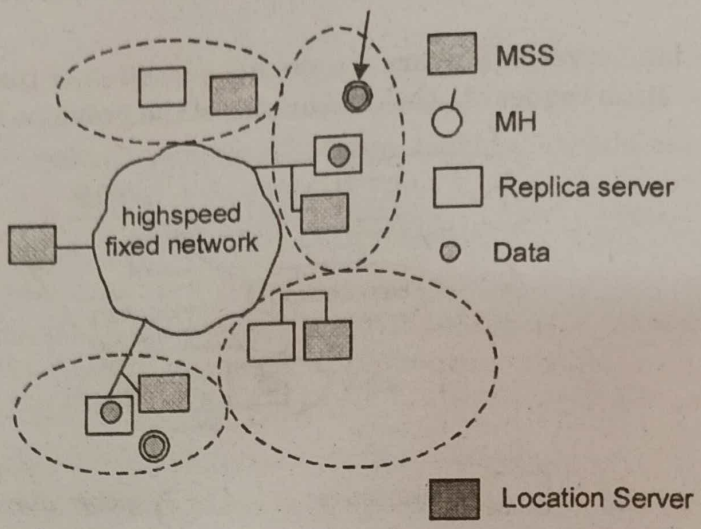
• Each MH has a replica of its data on FH called a replica server

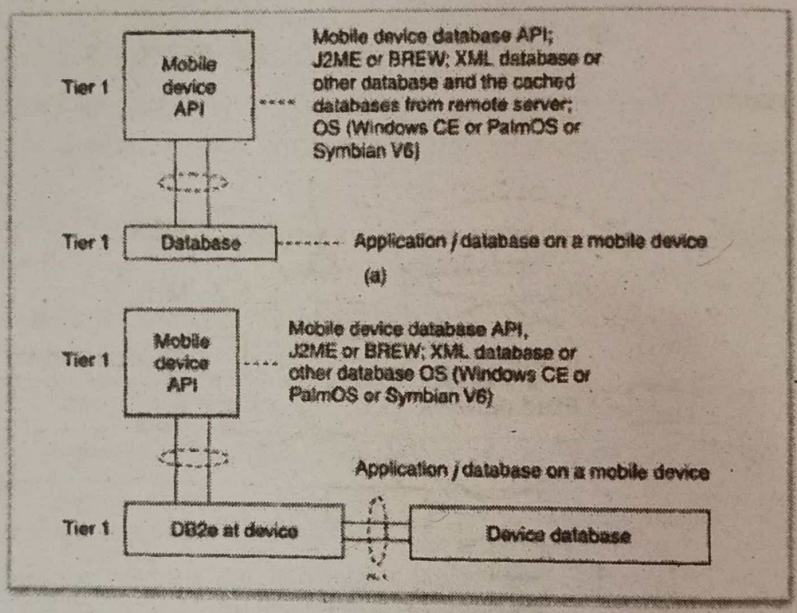
• Eacg MSS has a coordinator which receives transactions operations from MH or coordinators of other MSSs, and monitors their execution in the local replica server if the corresponding replicas exist

• If the corresponding data replicas do not exist, the coordinator contacts the location server to get information on their locations.

• On receiving location info on replicas, the coordinator submits transaction operations to coordinator of MSS where each replica exists.

• The receiving coordinator will send the request to the local replica server for executions.





(a) API at mobile device sending queries and retrieving data from local database (Tier 1)
(b) API at mobile device retrieving data from database using DB2e (Tier 1)

There are two channel assignment strategies in cellular system.

A. Fixed channel assignment:

1. In fixed channel assignment each cell is permanently allocated predetermined group of channels. Any call attempt within cell can only be served by unused channels in that particular cell.

2. If all channels are occupied, the call is blocked and subscriber does not receive service.

3. Borrowing technique where a cell is allowed to borrow channels from a neighbouring cell if all channels are already occupied is always used with this type of strategy. Mobile Base station (MSC) monitors the function of base station including borrowing ensuring that borrowing does not interfere with any call in progress in donor cell.

B. Dynamic channel assignment:

1. In dynamic channel assignment strategy, voice channels are not allocated permanently.

2. Entire pool of frequency channels lies with MSC and each time a call request is made, the serving base station requests a channel from the MSC. Switch then allocates a channel to the requested cell following a algorithm.

3. MSC allocates frequency channels on dynamic basis if that frequency channel is not presently in use in the cell or any other cell which falls within the minimum restricted distance of frequency reuse to avoid co-channel interference.

4. It reduces chances of blocking which increases trunking capacity of system as all available channels are accessible to all cells.

5. In this MSC has to collect real time data on channel occupancy, traffic distribution, radio signal strength indication of all channels on continuous basis, thus increasing the computational load on MSC.

Q.7. (a) Explain the basics of Zigbee technology. Mention clearly how many frequency channels are supported in Zigbee in different PHY versions. Explain the different components which form Zigbee network of system. What is Zigbee RF4CE version and Zigbee 6LoWPAN version? (6)

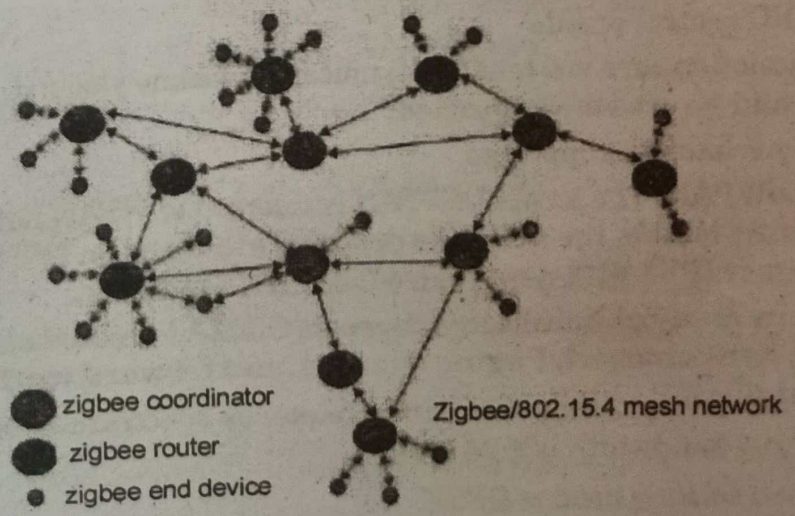
Ans. ZigBee is an open global standard for wireless technology designed to use low-power digital radio signals for personal area networks. ZigBee operates on the IEEE 802.15.4 specification and is used to create networks that require a low data transfer rate, energy efficiency and secure networking. It is employed in a number of applications such as building automation systems, heating and cooling control and in medical devices.

ZigBee is designed to be simpler and less expensive than other personal are network technologies such as Bluetooth.

Frequency channels in Zigbee:

PHY (MHz)	Frequency band (MHz)	Spreading parameters		Data parameters		
		Chip rate (kchip/s)	Modulation	Bit rate (kb/s)	Symbol rate (ksymbol/s)	Symbols
868/915	868–868.6	300	BPSK	20	20	Binary
	902–928	600	BPSK	40	40	Binary
868/915 (optional)	868–868.6	400	ASK	250	12.5	20-bit PSSS
	902–928	1600	ASK	250	50	5-bit PSSS
868/915 (optional)	868–868.6	400	O-QPSK	100	25	16-ary Orthogonal
	902–928	1000	O-QPSK	250	62.5	16-ary Orthogonal
2450	2400–2483.5	2000	O-QPSK	250	62.5	16-ary Orthogonal

Zigbee network:



As mentioned in the network diagram, zigbee network is comprised of coordinator(C), router(R) and end devices (E). Zigbee supports mesh-routing. For detailed information on routing protocol employed in zigbee, one may refer Ad-hoc on-demand Distance Vector Routing protocol (AODV protocol), RFC 3561

Coordinator: Always first coordinator need to be installed for establishing zigbee network service, it starts a new PAN (Personal Area Network), once started other zigbee components viz. router(R) and End devices(E) can join the network(PAN).

It is responsible for selecting the channel and PAN ID.

It can assist in routing the data through the mesh network and allows join request from R and E.

It is mains powered (AC) and support child devices.

It will not go to sleep mode.

Router: First router needs to join the network then it can allow other R & E to join the PAN.

It is mains powered (AC) and support child devices.

It will not go to sleep mode.

End Devices: It cannot allow other devices to join the PAN nor can it assist in routing the data through the network.

It is battery powered and do not support any child devices. This may sleep hence battery consumption can be minimized to great extent. There are two topologies, star and mesh, as mentioned Zigbee supports mesh routing. PAN ID is used to communicate between zigbee devices, it is 16 bit number. Coordinator will have PAN ID set to zero always and all other devices will receive a 16 bit address when they join PAN.

There are two main steps in completing Zigbee Network Installation. Forming the network by Coordinator and joining the network by Routers and End devices.

Zigbee RF4CE: RF4CE referred as Radio Frequency for Consumer Electronics. This consortium has been formed in 2009. RF4CE consortium and Zigbee alliance agreed to work for a standard to take care of radio frequency remote control of various consumer devices such as TVs, Audio devices, set-top boxes and so on.

Silent features of ZigBee RF4CE:

- 2.4GHz frequency of operation over three channels
- Compliant to IEEE 802.15.4
- Power saving feature
- Multi star topology with Inter-PAN communication
- Utilizes AES-128 security standard
- Simple RC control profile
- Transmission options viz. broadcast, unicast, unacknowledged, acknowledged, unsecured and secured are supported.
- Pairing mechanism supported

Zigbee 6LoWPAN: The term 6LoWPAN is referred to WPAN network having IPV6 based protocols. As most of the networks deployed are based on IPV4 there is a need to interoperate legacy IPV4 with newly introduced IPV6 network.

Q.7. (b) How many channels are there in CDMA forward channels? Explain Pilot channel, Sync channel, Paging channel, and forward traffic channel. *(6.5)*

Ans. • CDMA forward link uses same frequency spectrum as AMPS i.e. 869-894 MHz. One channel bandwidth is 1.25 MHz

• Modulation scheme used is QPSK.

• Orthogonal Walsh codes are used. Walsh codes are called Hadamard codes and they are used in all CDMA techniques.

• Forward channels are separated from each other using different spreading codes. 64 Walsh codes are used to identify each channel.

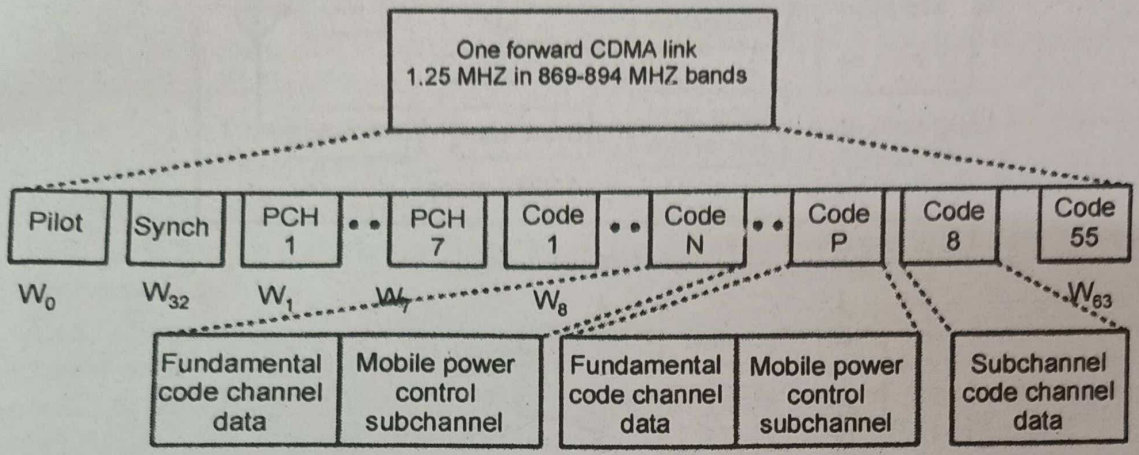


Fig. IS-95 Forward Channel

• Type of forward channel:

A. Pilot channel:

- It provides phase for coherent demodulation, time, signal strength, comparison with reference signal for determining when to hand off for all mobile stations.
- It is used to uniquely identify sectors or cells.
- It is 4-6 db stronger than all other channels. It is used to lock onto other channel.
- It is obtained using all zero Walsh code i.e. it contains no information except the RF carrier.

B. Synch channel:

- It is used to acquire initial time synchronization.
- Synch messages include System ID (SID), Network ID (NID), the offset of the PN short code and the paging channel data rate.
- It broadcasts synch messages to the mobile station and operates at 1200 bps.
- It uses Walsh code 32 for spreading.

C. Paging channel:

- There are 7 paging channels used to page the mobile station in case of an incoming call, or to carry the control messages for call set up.
- It uses Walsh code 1-7. There is no power control.
- It is additionally scrambled by PN long code, which is generated by LFSR of length 42.
- It operates at the rate of 4.8 kbps or 9.6 kbps.

D. Traffic channel:

- There are 55 traffic channels used to carry actual information.
- It supports variable data rates-RS1={9.6. 4.8, 2.4, 1.2 kbps} and RS2={14.4, 7.2, 3.6, 1.8 kbps}
- RS1 is mandatory for IS-95. But support for RS2 is optional.
- It also carries power control bits for the reverse channel.

The forward channel modulation process is as follows:

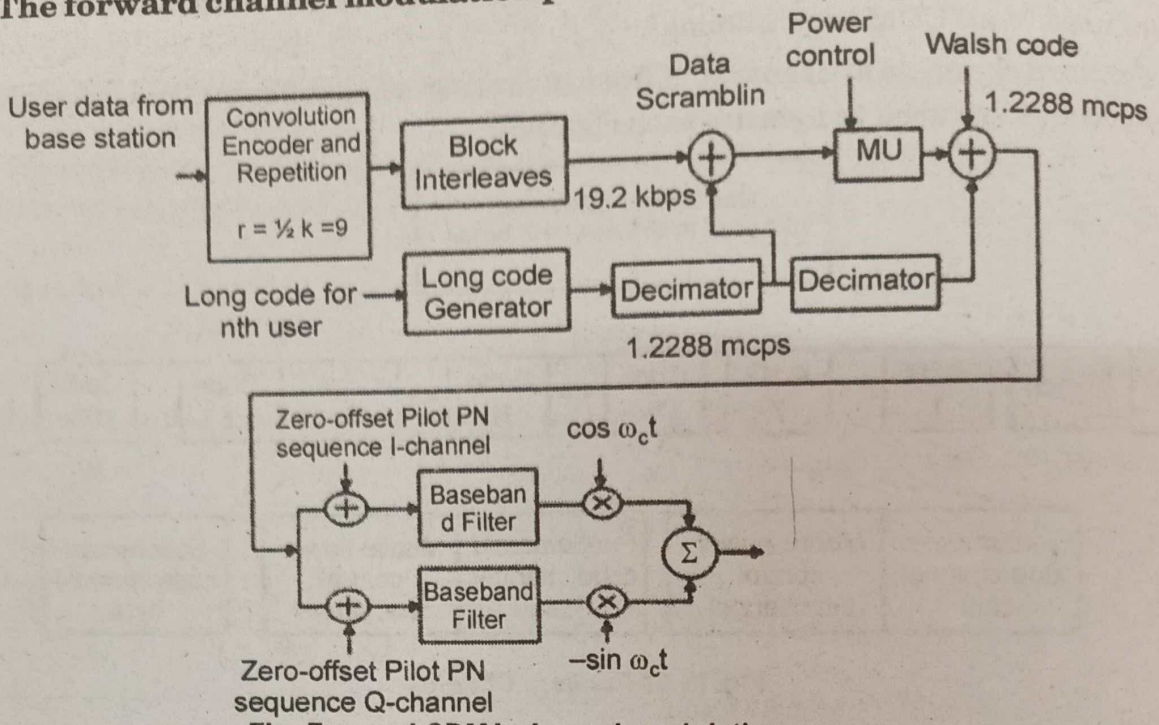


Fig. Forward CDMA channel modulation process

A. Convolution encoder and repetition:

- Speech coded voice or user data is encoded using ½ rate convolution encoder with constraint length 9.
- The speech coder exploits gaps and pauses in speech and reduces its output from 9600 bps to 1200 bps during silent period.
- Whenever the user data rate is less than 9600 bps each bit is repeated to maintain a constant symbol rate of 19.2 kbps.

B. Block interleaver:

- It makes data block of 20 ms in a random way i.e. consecutive bits are not in a same block.
- It maps the data bits in a 24 by 16 matrix and then transmit it column wise.
- This procedure is helpful in recovering the data back if a block is lost during channel transmission.

C. Long PN sequence:

- In forward CDMA channel Direct Sequence is used for data scrambling.
- Long PN sequence is user specific code of period 242"1242"1 chips.
- PN sequence is generated from a 42 bit code also called as the public mask.
- Public mask is specified as- M41 through M32 is set to 1100011000 and M31 through M0 is set to mobile station ESN bits. ESN= (E31, E30, E29, E28, ... , E1, E0), permuted ESN= (E0, E31, E22, E13, E14, E26, E17, E8, ... , E18, E9)

D. Data scrambler:

- It is performed after block interleaver. The 1.2288 MHz PN sequence is applied to decimator which keeps only the first chip out of every 64 consecutive PN chips.
- The data rate from the decimator is 19.2 ksps. The data scrambling is performed by modulo-2 addition of the interleaver output with the decimator output symbol.

E. Power control subchannel:

- Power control measures are sent by base station every 1.25ms. Power control commands are sent to raise or lower its transmission power in 1 db steps.

• If the received signal is low 0 is sent over power control subchannel instructing the mobile station to increase its mean output power level. If mobile's power level is high 1 is sent to indicate that the mobile station should decrease the power level.

F. Orthogonal covering:

• Orthogonal scrambling is performed following the data scrambling on the forward link.

• Each traffic channel is transmitted on the forward CDMA channel is spread with a Walsh function at fixed rate of 1.2288 Mcps.

• The Walsh functions consist of 64 binary sequences each of length 64 which are completely orthogonal to each other and provide orthogonal channelization.

• After orthogonal covering Quadrature modulation is performed.

Q.8. (a)What is data hoarding? How the channel allocation takes place in cellular systems? **(6)**

Ans. A database is a collection of systematically stored records or information. Databases store data in a particular logical manner. A mobile device is not always connected to the server or network; neither does the device retrieve data from a server or a network for each computation. Rather, the device caches some specific data, which may be required for future computations, during the interval in which the device is connected to the server or network. Caching entails saving a copy of select data or a part of a database from a connected system with a large database. The cached data is hoarded in the mobile device database. Hoarding of the cached data in the database ensures that even when the device is not connected to the network, the data required from the database is available for computing.

Database hoarding may be done at the application tier itself. The following figure shows a simple architecture in which a mobile device API directly retrieves the data from a database. it also shows another simple architecture in which a mobile device API directly retrieves the data from a database through a program, for ex: IBM DB2 Everyplace (DB2e)

Q.8. (b) Explain processing gain in CDMA. "In a CDMA system, mutual interference will determine the majority of SN ration of each user". Do you agree? Justify this statement. **(6.5)**

Ans. Processing Gain

For DSSS, bits are known as chips after spreading, Tb is one bit period and Tc is one chip period. 1/Tc is the chip rate which characterise this spread spectrum transmission system.

The ratio of information bit duration to chip duration is known as processing gain(PG).

Processing gain = Tb/Tc

It is also known as **spreading factor**.

In other words it represents number of chips in one data bit period.

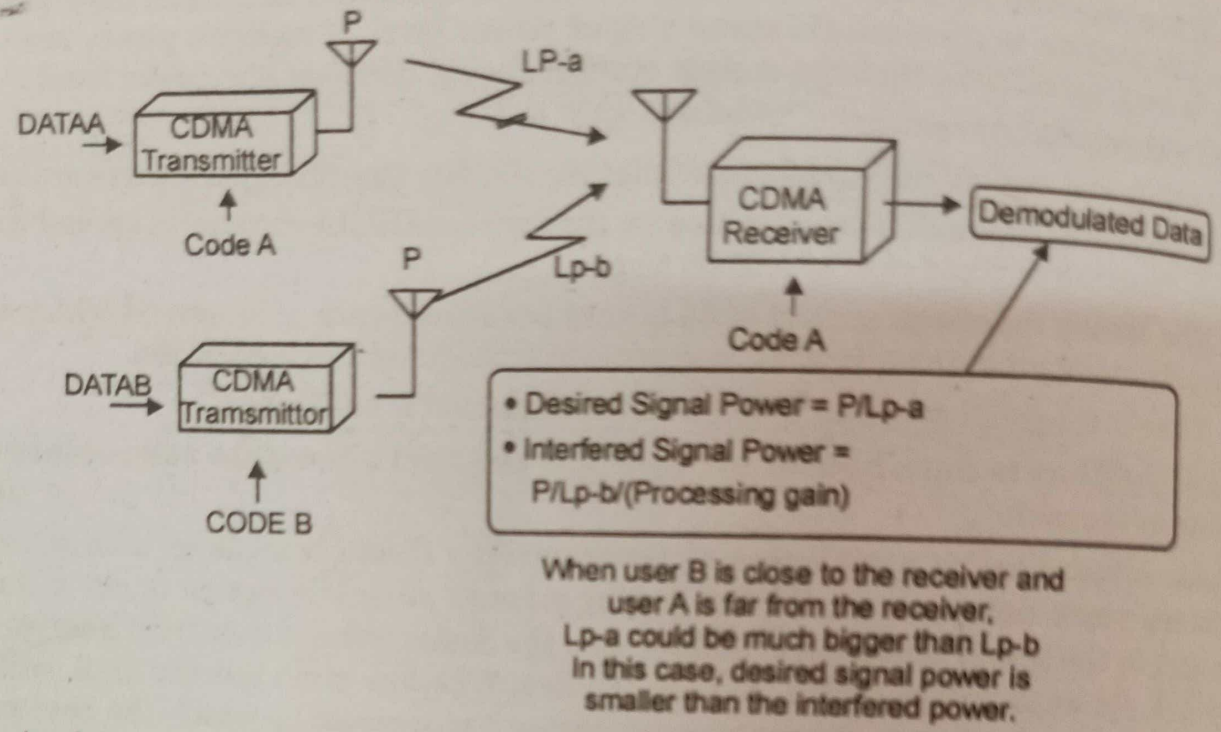
In general it is defined as ratio of signal to noise ratio (SNR) at output to the SNR at the input.

$$PG\,(dB) = SNR_{OUT}\,(dB) - SNR_{IN}\,(dB)$$

Near-far problem is one of the major problems that hurts mobile communications badly. In a CDMA system, mutual interference will determine the majority of SN ratio of each user.

How Near-Far Problem Affects Communication?

The following illustration shows how near-far problem affects communication.



As shown in the illustration, user A is far away from the receiver and user B is close to the receiver, there will be big difference between desired signal power and interfered signal power. Desired signal power will be much higher than the interfered signal power and hence SN ratio of user A will be smaller and communication quality of user A will be severely degraded.

END TERM EXAMINATION [MAY 2019]
EIGHTH SEMESTER [B.TECH]
MOBILE COMPUTING [ETIT–402]

Time : 3 hrs. **M.M. : 75**

Note: *Attempt five questions in alll including question no.1 which is compulsory. Select one question from each unit.*

Q.1. Answer the following in brief :

Q.1. (a) If BT/BC is total number of voice channels, C/I is carrier to interference ration of system. Give the relation (m) among voice quality, dropped call rate and capacity. **(3)**

Ans. The cellular radio capacity, m, of TDMA can be determined by the relationship

$$m = \frac{B_t}{B_c} / K$$

where B_t is the total allocated spectrum for the system, B_c is the channel bandwidth, and K is the number of cells in a frequency reuse pattern and can be obtained by,

$$K = q^2/3$$

where q is the co-channel interference reduction factor (CIRF). In mobile radio environment, we may assume a fourth power rule, i.e. $\gamma = 4$,

$$m = \frac{B_t}{B_c\sqrt{(2/3)(C/I)}}$$

$$= \frac{M}{K} \text{ number of channels/cell}$$

Where M is the total number of equivalent channels and (C/I) is the minimum received carrier-to interference ratio per channel or per time slot.

The C/I ratio of CDMA and TDMA system is related to E_b/N_o through

$$\frac{C}{I} = \frac{E_b}{N_o} = \frac{R_b}{B_c}$$

Where R_b is the transmission data rate, B_c is the transmission bandwidth, E_b is the energy per bit and N_o is the interference power per hertz. **(3)**

Q.1. (b) Compare 2G and 3G cellular standards.

Ans.

Name	1st Generation Mobile Network	2nd Generation Mobile Network
Introduced in year	1980s	1993
Location of first commercialization	USA	Finland
Technology	AMPS (Advanced Mobile Phone System), NMT, TACS	IS-95, GSM

Multiple Address/ Access system	FDMA	TDMA, CDMA
Switching type	Circuit switching	Circuit switching for Voice and Packet switching for Data
Speed (data rates)	2.4 Kbps to 14.4 kbps	14.4 Kbps
Special Characteristic	First wireless communication	Digital version of IG technology
Features	Voice only	Multiple users on single channel
Supports	Voice only	Voice and Data
Internet service	No Internet	Narrowband
Bandwidth	Analog	25 MHz
Operating frequencies	800 MHz	GSM: 900MHz, 1800MHz CDMA: 800MHz
Band (Frequency) type	Narrow band	Narrow band
Carrier frequency	30 KHz	200 KHz
Advantage	Simpler (less complex) network elements	Multimedia features (SMS, MMS), Internet access and SIM introduced
Disadvantages	Limited capacity, not secure, poor battery life, large phone size, background interference	Low network range, slow data rates
Applications	Voice Calls	Voice calls, Short messages, browsing (partial)

Q.1. (c) Define handoffs? What are the types of handoffs? **(3)**

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

When a mobile user travels from one area of coverage or cell to another cell within a call's duration the call should be transferred to the new cell's base station. Otherwise, the call will be dropped because the link with the current base station becomes too weak as the mobile recedes. Indeed, this ability for transference is a design matter in mobile cellular system design and is call *handoff*.

With hard handoff, the link to the prior base station is terminated before or as the user is transferred to the new cell's base station. That is to say that the mobile is linked to no more than one base station at a given time. Initiation of the handoff may begin when the signal strength at the mobile received from base station 2 is greater than that of base station 1. The signal strength measures are really signal levels averaged over a chosen amount of time.

In cellular telephone communication, soft handoff refers to the overlapping of repeater coverage zones, so that every cell phone set is always well within range of at least one repeater (also called a base station). In some cases, mobile sets transmit signals to, and receive signals from, more than one repeater at a time.

Soft handoff technology is used by code-division multiple access (CDMA) systems. Older networks use frequency division multiplex (FDM) or time division multiplex (TDM). In CDMA, all repeaters use the same frequency channel for each mobile phone set, no matter where the set is located. Each set has an identity based on a code, rather than on a frequency (as in FDM) or sequence of time slots (as in TDM). Because no change in frequency or timing occurs as a mobile set passes from one base station to another, there are practically no dead zones. As a result, connections are almost never interrupted or dropped.

Q.1. (d) Why is routing in multi hop ad-hoc network complicated? What are the special challenges? (3)

Ans. Wireless ad-hoc network is becoming one of the most animated and dynamic field of communication and networks because of fame of movable device and wireless networks that has increased significantly in recent years. A mobile ad-hoc network is formed by collecting portable devices like laptops, smart phones, sensors, etc. that communicate through wireless links with one another. These devices collaborate with each other to offer the essential network functions in the nonappearance of immovable organization in a distributed manner. This type of network creates the way for various innovative and stimulating applications by functioning as an independent network or with multiple points of connection to cellular networks or the Internet.

Routing of packets to destination is done by the cooperation of nodes of a MANET. The sending and receiving devices may be situated at a much higher distance as compared to transmission radius R, however, each network node can communicate only with nodes placed within its broadcast radius R. All the nodes in a multi- hop wireless ad-hoc network collaborate with one another to create a network in the absence of infrastructure such as access point or base station.

In order to permit transmission among devices beyond the transmission range in MANET, the mobile devices require advancing data-packets for one another. The network devices can move freely and autonomously in any route. The nodes can detach and attach to the network haphazardly. Thus variations in link states of the node with other nodes are experienced by a node regularly. Challenges for routing protocols operating in MANET are eventually increased the movement in the ad-hoc network, changes in link states and other characteristics of wireless transmission such as attenuation, multipath propagation, interference etc. The challenges are boosted by the numerous sorts of nodes of restricted processing power and competences that may join the network

Q.1. (e) Explain the WAP architecture in brief. (4)

Ans. Fig. (1) gives an overview of the WAP architecture, its protocols and components, and compares this architecture with the typical internet architecture when using the world wide web.

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

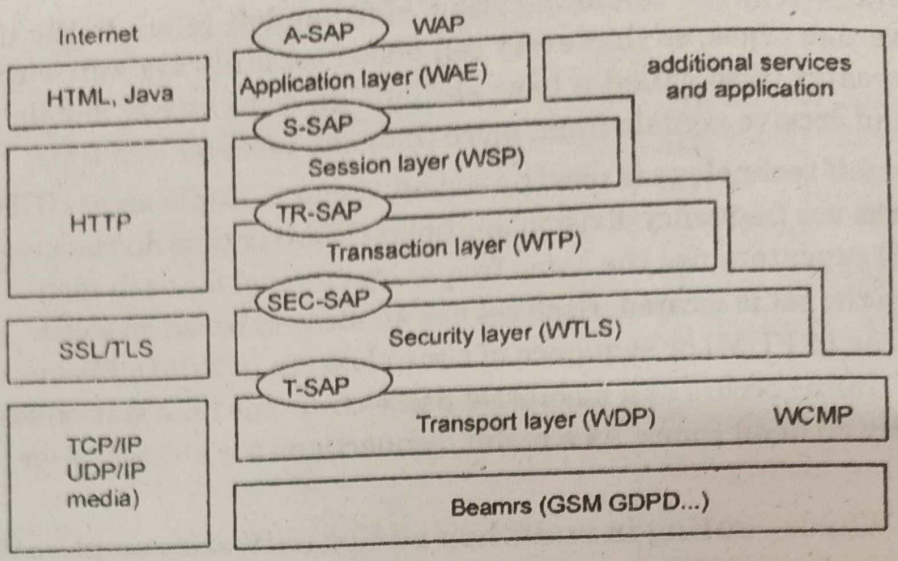


Fig.l. Components and interface of the WAP 1. architccure

The transport layer service access point (T-SAP) is the common interface to be used by higher layers independent of the underlying network.

The next higher layer, the security layer with its wireless transport layer security protocol WTLS offers its service at the security SAP (SEC-SAP). WTLS is based on the transport layer security (TLS, formerly SSL, secure sockets layer) already known from the www. WTLS has been optimized for use in wireless net-works with narrow-band channels.

The WAP **transaction layer** with its **wireless transaction protocol** (WTP) offers a lightweight transaction service at the transaction SAP (TR-SAP). This service efficiently provides reliable or unreliable requests and asynchronous transactions. The **session layer** with the **wireless session protocol** (WSP) currently offers two services at the **session-SAP** (S-SAP), one connection-oriented and one connectionless if used directly on top of WDP. A special service for browsing the web (WSP/B) has been defined that offers HTTP/1.1 functionality, long-lived session state, session suspend and resume, session migration and other features needed for wireless mobile access to the web.

Finally the **application layer** with the wireless **application environment** (WAE) offers a framework for the integration of different www and mobile telephony applications.The main issues here are scripting languages, special markup languages, interfaces to telephony applications, and many content formats adapted to the special requirements of small, handheld, wireless devices.

Q.1. (f) Compare IEEE 802.11, HiperLAN2 and Bluetooth with regard to their ad-hoc capabilities. Where is the focus of these technologies? (3)

Ans. All three standards offer ad-hoc functionality, although only Bluetooth was designed with the focus on ad-hoc networking. 802.11 heavily relies on an access point for many functions (e.g., power control, frequency selection, QoS in polling mode, access control etc.). Bluetooth on the other hand implements all functions in all nodes enabling all devices to set up a network. Main focus of HiperLAN2 is the infrastructure mode, too. Roughly, it can be said that 802.11 covers all standard office applications, Bluetooth focuses on inter-device connectivity, while HiperLAN2 was designed for QoS support (no products yet).

Parameters	BLUETOOTH	HIPERLAN-2	802.11WLAN
Application	Wireless network	Access to ATM fixed network	Wireless networks
Frequency, Band	2.45GHz	5 GHz	2.4 GHz
Maximum Data rate	1Mbps	54 Mbps	2 Mbps
Topology	Ad-hoc	Cellular, centralized	Can be adhoc or infra-based
Error control	Arq/fec mac layer	Arq/fec phy layer	ARQ
Range	Upto 10m	50-100m	100m
Interface	low	high	medium
Medium Access methods	Master is responsible for medium	AP centralized	CSMA/CA
Connectivity	Connection less and Oriented	Connection oriented	Connectionless
QoS (Quality of Service)	Statistical	ATM/802.1p/RSVP	PCF (optional)
Frequency Selection	Frequency hopping	Dynamic frequency selection (DSS)	Frequency hopping or DSSS
Tvpical Outdoor Range	100 metres	–	–
Encryption	DES, 3DES	DES, 3DES	40 bit RC4
Authentication	No	X.509	No

Q.1. (g) Explain three types of multiple access techniques. Why CDMA technique is more secure? **(3)**

Ans. TDMA: Time Division Multiple Access (TDMA) is a digital wireless telephony transmission technique. TDMA allocates each user a different time slot on a given frequency. TDMA divides each cellular channel into three time slots in order to increase the amount of data that can be carried.

TDMA technology was more popular in Europe, Japan and Asian countries, where as CDMA is widely used in North and South America. But now a days both technologies are very popular through out of the world.

Advantages of TDMA:

- TDMA can easily adapt to transmission of data as well as voice communication.
- TDMA has an ability to carry 64 kbps to 120 Mbps of data rates.
- TDMA allows the operator to do services like fax, voice band data, and SMS as well as bandwidth-intensive application such as multimedia and video conferencing.
- Since TDMA technology separates users according to time, it ensures that there will be no interference from simultaneous transmissions.
- TDMA provides users with an extended battery life, since it transmits only portion of the time during conversations.
- TDMA is the most cost effective technology to convert an analog system to digital.

Disadvantages of TDMA

- Disadvantage using TDMA technology is that the users has a predefined time slot. When moving from one cell site to other, if all the time slots in this cell are full the user might be disconnected.
- Another problem in TDMA is that it is subjected to multipath distortion. To overcome this distortion, a time limit can be used on the system. Once the time limit is expired the signal is ignored.

CDMA: Code Division Multiple Access (CDMA) is a digital wireless technology that uses spread-spectrum techniques. CDMA does not assign a specific frequency to each user. Instead, every channel uses the full available spectrum. Individual conversations are encoded with a pseudo-random digital sequence. CDMA consistently provides better capacity for voice and data communications than other commercial mobile technologies, allowing more subscribers to connect at any given time, and it is the common platform on which 3G technologies are built.

Advantages of CDMA

- One of the main advantages of CDMA is that dropouts occur only when the phone is at least twice as far from the base station. Thus, it is used in the rural areas where GSM cannot cover.
- Another advantage is its capacity; it has a very high spectral capacity that it can accommodate more users per MHz of bandwidth.

Disadvantages of CDMA

- Channel pollution, where signals from too many cell sites are present in the subscriber. s phone but none of them is dominant. When this situation arises, the quality of the audio degrades.
- When compared to GSM is the lack of international roaming capabilities.
- The ability to upgrade or change to another handset is not easy with this technology because the network service information for the phone is put in the actual phone unlike GSM which uses SIM card for this.
- Limited variety of the handset, because at present the major mobile companies use GSM technology.
- **FDMA:** FDMA is the process of dividing one channel or bandwidth into multiple individual bands, each for use by a single user. Each individual band or channel is wide enough to accommodate the signal spectra of the transmissions to be propagated. The data to be transmitted is modulated on to each subcarrier, and all of them are linearly mixed together.

FDMA divides the shared medium bandwidth into individual channels. Subcarriers modulated by the information to be transmitted occupy each sub channel.

The best example of this is the cable television system. The medium is a single coax cable that is used to broadcast hundreds of channels of video/audio programming to homes. The coax cable has a useful bandwidth from about 4 MHz to 1 GHz. This bandwidth is divided up into 6-MHz wide channels. Initially, one TV station or channel used a single 6-MHz band. But with digital techniques, multiple TV channels may share a single band today thanks to compression and multiplexing techniques used in each channel.

This technique is also used in fibre optic communications systems. A single fibre optic cable has enormous bandwidth that can be subdivided to provide FDMA. Different data or information sources are each assigned a different light frequency for transmission. Light generally isn't referred to by frequency but by its wavelength (ë). As a result, fiber optic

FDMA is called wavelength division multiple access (WDMA) or just wavelength division multiplexing (WDM).

One of the older FDMA systems is the original analog telephone system, which used a hierarchy of frequency multiplex techniques to put multiple telephone calls on single line. The analog 300-Hz to 3400-Hz voice signals were used to modulate subcarriers in

12 channels from 60 kHz to 108 kHz. Modulator/mixers created single sideband (SSB) signals, both upper and lower sidebands. These subcarriers were then further frequency multiplexed on subcarriers in the 312-kHz to 552-kHz range using the same modulation methods. At the receiving end of the system, the signals were sorted out and recovered with filters and demodulators.

SDMA: Space-division multiple access (SDMA) is a channel access method based on creating parallel spatial pipes next to higher capacity pipes through spatial multiplexing and/or diversity, by which it is able to offer superior performance in radio multiple access communication systems. In traditional mobile cellular network systems, the base station has no information on the position of the mobile units within the cell and radiates the signal in all directions within the cell in order to provide radio coverage.

This results in wasting power on transmissions when there are no mobile units to reach, in addition to causing interference for adjacent cells using the same frequency, sc called co-channel cells. Likewise, in reception, the antenna receives signals coming from all directions including noise and interference signals. By using smart antenna technology and differing spatial locations of mobile units within the cell, space-division multiple access techniques offer attractive performance enhancements.

The radiation pattern of the base station, both in transmission and reception, is adapted to each user to obtain highest gain in the direction of that user. This is often done using phased array techniques. In GSM cellular networks, the base station is aware of the distance (but not direction) of a mobile phone by use of a technique called "timing advance" (TA). The base transceiver station (BTS) can determine how distant the mobile station (MS) is by interpreting the reported TA.

- In CDMA technology, More security is provided as compared with the GSM technology because encryption is inbuilt in the CDMA.
- A unique code is provided to each and every user and all the conversation between two users are encoded ensuring a greater level of security for CDMA users.
- The signal cannot be traced easily in CDMA as compared to the signals of GSM, which are concentrated in the narrow bandwidth.
- Therefore, the CDMA phone calls are more secure than the GSM calls. In terms of encryption, the GSM technology has to be upgraded so as to make it operate more securely.

Q.1. (h) Give overview of evolution of wireless mobile communication. (3)

Ans. Mobile wireless communication system has gone through several evolution stages in the past few decades after the introduction of the first generation mobile network in early 1980s. Due to huge demand for more connections worldwide, mobile communication standards advanced rapidly to support more users.

Key features (technology) of 1G system

- Frequency 800 MHz and 900 MHz
- Bandwidth: 10 MHz (666 duplex channels with bandwidth of 30 KHz)
- Technology: Analogue switching
- Modulation: Frequency Modulation (FM)
- Mode of service: voice only
- Access technique: Frequency Division Multiple Access (FDMA)

Key features of 2G system

- Digital system (switching)
- SMS services is possible
- Roaming is possible

12–2019

- Enhanced security
- Encrypted voice transmission
- First internet at lower data rate
- Disadvantages of 2G system
- Low data rate
- Limited mobility
- Less features on mobile devices
- Limited number of users and hardware capability

Key features of 3G system

- Higher data rate
- Video calling
- Enhanced security, more number of users and coverage
- Mobile app support
- Multimedia message support
- Location tracking and maps
- Better web browsing
- TV streaming
- High quality 3D games

Key features of 4G system

- Much higher data rate up to 1Gbps
- Enhanced security and mobility
- Reduced latency for mission critical applications
- High definition video streaming and gaming
- Voice over LTE network VoLTE (use IP packets for voice)

Key features of 5G technology

- Ultra fast mobile internet up to 10Gbps
- Low latency in milliseconds (significant for mission critical applications)
- Total cost deduction for data
- Higher security and reliable network
- Uses technologies like small cells, beam forming to improve efficiency
- Forward compatibility network offers further enhancements in future
- Cloud based infrastructure offers power efficiency, easy maintenance and upgrade of hardware

UNIT - I

Q.2. (a) Explain the architecture of GSM. **(6.5)**

Ans. Refer to Q.3. (a) End Term Examination 2017. (Page No. 16-2017)

Q.2.(b) What are the advantages and problems of forwording mechanisms in Bluetooth networks regarding security and power saving? **(6)**

Ans. Problems of data forwarding

Security is a problem – Devices of different connected piconets are not authenticated to each other which would be a risk in communication.

Power saving is also a problem – The forwarding device is more loaded than others and it would be best to choose another device from time to time.

This goes on **stability** as well – as the problem that the forwarding device has to keep synchronization between two networks.Also stability is a problem when devices move.

Advantages of data forwarding: By connecting using scatternets, the devices can keep low transmit power to transmit only in their piconets. Thus only connecting devices are highly loaded, the others in piconet are less loaded.

Also having piconets, stability is higher: if a master breaks down, only its piconet is down, the other piconets of scatternet can go on working.

Forwarding data in Bluetooth between piconets require a node jumping back and forth between these piconets. This also requires authentication in both networks, nodes that are (almost) always active and synchronous clocks if the master jumps into another piconet. If the master jumps away all network traffic in the piconet stops, all slaves have to wait until the master returns. All hopping sequences must stay synchronous during that time. Up to now not many devices are capable of forming scatternets with nodes jumping back and forth.

OR

Q.3. (a) What is WAP? Discuss in detail about the components and interface of the WAP architecture. **(6.5)**

Ans. Refer to Q.1. (e) End Term Examination 2019. (Page No. 7-2019)

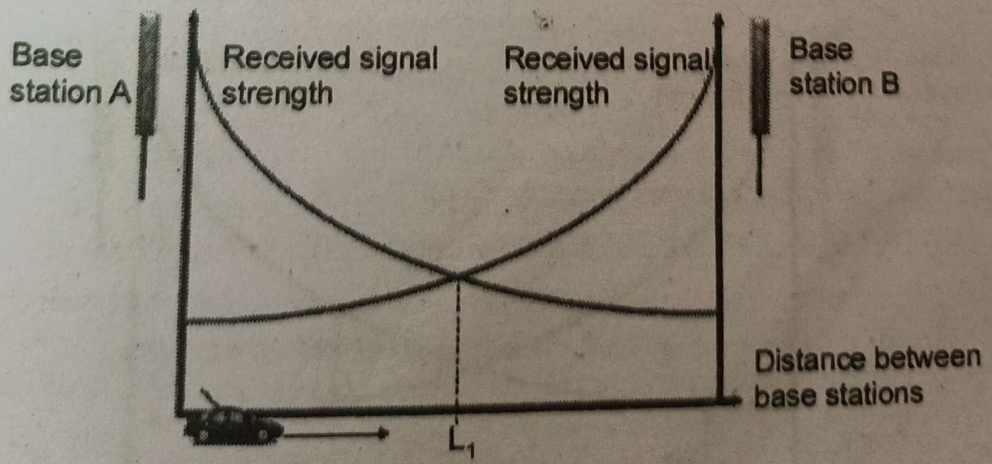
Q.3. (b) Consider the handoff procedure in GSM systems that is based on relative signal strength with threshold; that is, a mobile switches from one cell to another if? **(6)**

(i) The signal at the current BS(base station) is sufficiently weak (less than a predefined threshold) and

(ii) The other signal is stronger than the two. What are the drawbacks of this scheme, when the threshold is too low or too high ?

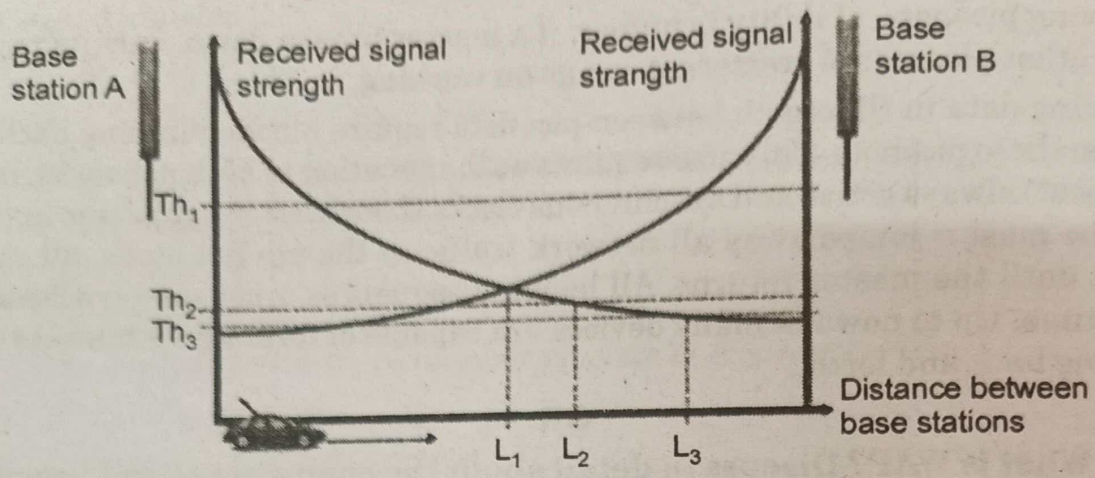
Ans. Relative Signal Strength (RSS)

Mobile terminal is handed off from BS A to BS B when the signal strength at B first exceeds that at A. If the signal strength at B first exceeds that at A, the mobile unit is handed back to A. In figure- handover occurs at point L_1. Because signal strength fluctuates due to multipath propagation effects, several handoffs may be occurred while BS1's RSS is still sufficient to serve the MS. These unnecessary handoffs are known as the ping-pong effect. As the number of handoffs increase, forced termination probability and network load also increases. But, handoff techniques should avoid such unnecessary handoffs.



Relative Signal Strength with Threshold (RSS-T) Relative signal strength with threshold introduces a threshold value to overcome the ping-pong effect. Handover only occurs if the signal at the current BS is less than a predefined threshold and the signal

from a neighboring base station is stronger. For a high threshold (e.g., Th_1), this scheme performs the same as the relative signal strength scheme. On the other hand, if the threshold is set quite low (e.g., Th_3), the mobile may move far into the new cell. Threshold should not be used alone because its effectiveness depends on prior knowledge of the crossover signal strength between the current and the candidate base stations.



Relative Signal Strength with Hysteresis (RSS-H) Handover occurs only if the new base station is sufficiently stronger (by a margin H) than the current one. While the mobile is assigned to base station A, the scheme will generate a handover when the relative signal strength reaches or exceeds H. Once the mobile is assigned to B, it remains so until the relative signal strength falls below –H, at which point it is handed back to A. This scheme prevents the ping-pong effect but the first handover may still be unnecessary if base station A still has sufficient signal strength.

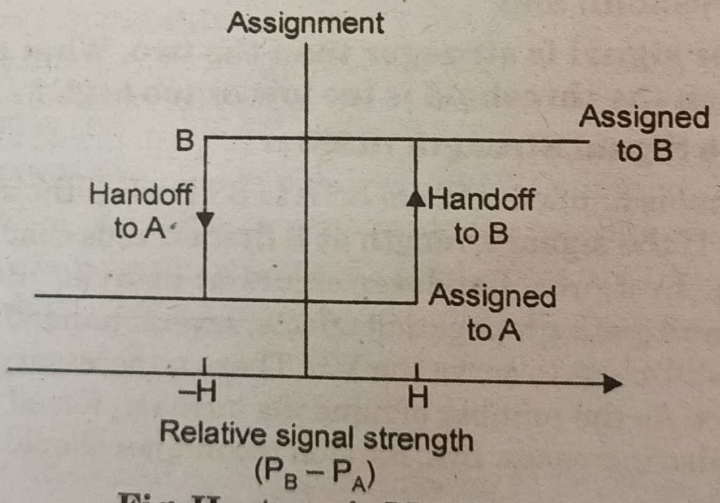
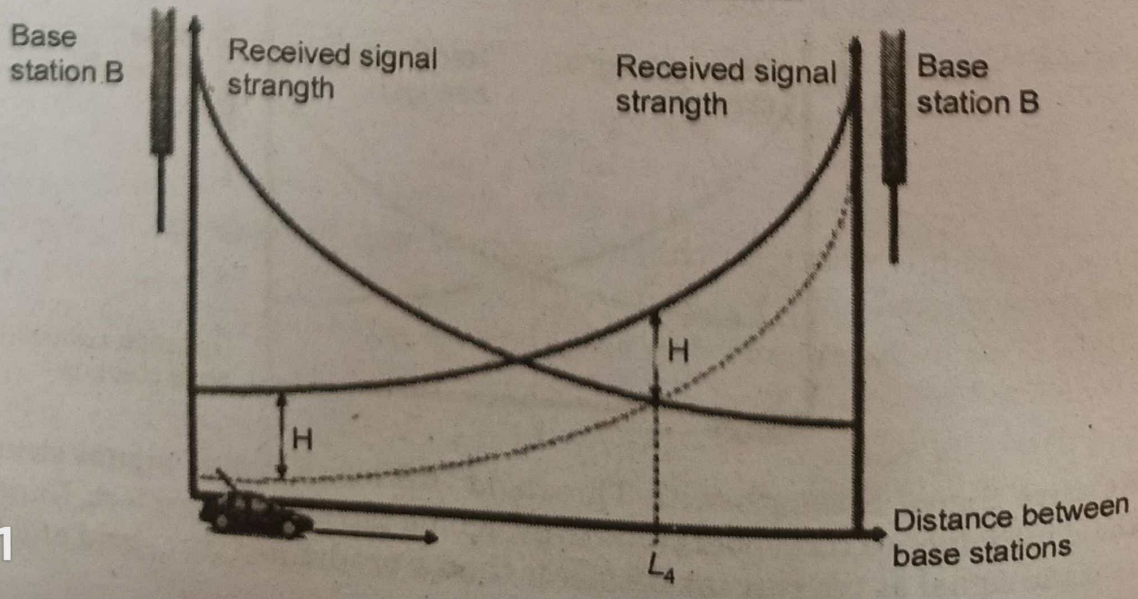
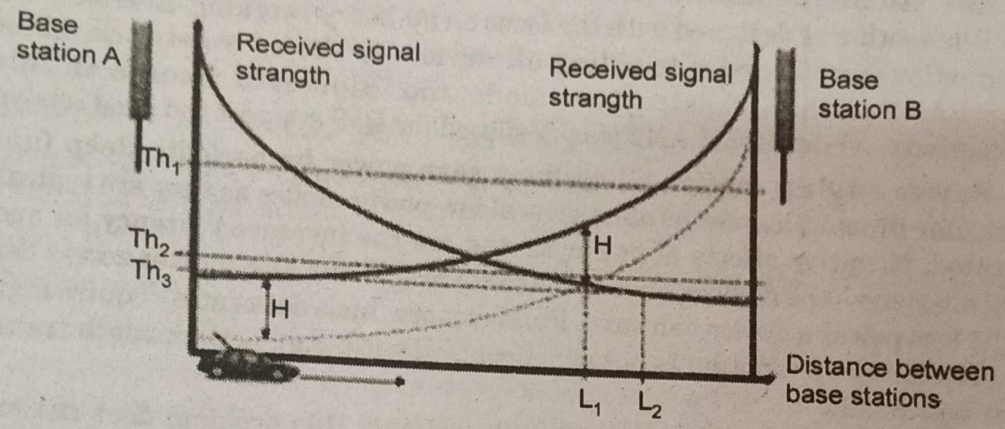


Fig. Hysteresis Mechanism



Relative Signal Strength with Threshold and Hysteresis (RSS-TH) Handover occurs only if the current signal level drops below a threshold, and the target base station is stronger than the current one by a hysteresis margin H. Handover occurs at L_4, if the threshold is either Th_1 or Th_2. Handover occurs at L_3, if the threshold is at Th_3. Scheme avoids the ping-pong effect and execution of handover if signal from the serving base station is still strong enough. Decreasing threshold in the RSS-HT new cause increase the probability of handoff and therefore the number of handoffs and the number of wrong handoff increase.



UNIT - II

Q.4. (a) Define WPABX, IrDA, ZigBee, RFID, WiMax. **(6.5)**

Ans. WPBX: WPBX systems integrate wireless telephones with a PBX switching system. Wireless PBX telephones (handsets) communicate through wired base stations (fixed radio transmitters) to the WPBX switching system. Most WPBX systems have automatic switching call transfer that allows wireless handsets to transfer their calls to other base stations as the move through the WPBX radio coverage areas. Base stations are strategically located around the served area (both inside and/or outside) to provide contiguous radio coverage. WPBX systems can be completely, or partially, wireless between the system and the telephone instruments.

WPBX systems fill a need where all, or part, of the work force is highly mobile in a relatively small area such as a building/plant or a small commercial campus. Hospitals and manufacturing plants tend to have several types of personnel that tend to be constantly on the move: medical emergency personnel, maintenance personnel, and production-line supervisors to name a few. Such people are frequently away from their desk or other fixed telephone station set location; however, it is often quite important that they be contacted quickly.

There are several different types of WPBX systems industry standard systems and proprietary systems. Some of the standard WPBX systems include digital enhanced cordless telephone (DECT) and cordless telephony second generation (CT2). A WPBX radio system allows for voice or data communications on either an analog (typically FM) or digital radio channel. The radio channel typically allows multiple mobile telephones to communicate on the same frequency at the same time by special coding of their radio signals.

RFID (Radio Frequency Identification) is a radio transponder carrying an ID that can be read through radio frequency interfaces. These transponders are commonly known as RFID tags or simply tags. A RFID system comprises different functions are

(i) Means of reading or interrogating the data in the tag.

(ii) Mechanism to filter some of the data.

(iii) Means to communicate the data in the tag with a host computer..

(iv) Means for updating or entering customized data into the tag.

IrDA, ZigBee, RFID, WiMax

Refer of Q.4. First Term Examination 2019.

Q.4. (b) Compare HiperLAN, and Bluetooth in terms of ad-hoc capabilities, power saving mode, solving hidden terminal problem, providing reliability fairness problem regarding channel access. (6)

Ans. Ad hoc capabilities: Both the standards offer ad-hoc functionality, although only Bluetooth was designed with the focus on ad-hoc networking. Bluetooth implements all functions in all nodes enabling all devices to set up a network. Main focus of HiperLAN2 is the infrastructure mode, too. Bluetooth focuses on inter-device connectivity, while HiperLAN2 was designed for QoS support (no products yet).

Power saving mode: All systems save power by periodic sleep functions. In particular Bluetooth systems offer several low power modes as they are typically battery operated. Negative effects of power saving are the increased latency for spontaneous transmissions – the devices have to wake-up first. Thus, the shorter access delay should be the less power a device can save. Furthermore, high data rates require high power. If the periodic sleep function is not synchronised with, e.g., periodic data transfer heavy jitter will result.

Hidden terminal problem: For HiperLAN2 this problem does not exist as the access point controls all medium access. If a terminal is hidden it cannot communicate at all and, thus, does not interfere. In Bluetooth, too, are no hidden terminals as the master controls all visible slaves. If a terminal does not see the master it cannot participate in communication. If this terminal sends anyway it will not interfere as this terminal then acts as master with a different hopping sequence.

Fairness problem: In HiperLAN2 and Bluetooth medium access is controlled by an access point or master, respectively. Fairness then depends on these special nodes, which also decide upon the waiting time of a packet when it will be transmitted. In 802.11 the waiting time directly influences the chances for transmission in the next contention cycle.

Reliability: Bluetooth implements different ARQ and FEC schemes, as well as while HiperLAN2 does.

OR

Q.5. (a) Draw the MAC frame of 802.11 and list the use of various fields. (6)

Ans. The MAC layer frame consists of 9 fields. The following figure shows the basic structure of an IEEE 802.11 MAC data frame along with the content of the frame control field.

Frame control	Duration /ID	Address 1	Address 2	Address 3	SC	Address 4	Data	CRC
2 bytes	2 bytes	6 bytes	6 bytes	6 bytes	2 bytes	6 bytes	0 - 2312 bytes	4 bytes

Protocol version	Type	Subtype	To DS	From DS	More Frag	Retry	Power Mgmt	More data	WEP	Order
2 bits	2 bits	4 bits	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit

IEEE 802.11 MAC Frame Structure

• **Frame Control (FC)** – It is 2 bytes long field which defines type of frame and some control information. Various fields present in FC are:

1.Version: It is a 2 bit long field which indicates the current protocol version which is fixed to be 0 for now.

2.Type: It is a 2 bit long field which determines the function of frame i.e management (00), control(01) or data(10). The value 11 is reserved.

3.Subtype: It is a 4 bit long field which indicates sub-type of the frame like 0000 for association request, 1000 for beacon.

4.To DS: It is a 1 bit long field which when set indicates that destination frame is for DS (distribution system).

5.From DS: It is a 1 bit long field which when set indicates frame coming from DS.

6.More frag (More fragments): It is 1 bit long field which when set to 1 means frame is followed by other fragments.

7.Retry: It is 1 bit long field, if the current frame is a retransmission of an earlier frame, this bit is set to 1.

8.Power Mgmt (Power management): It is 1 bit long field which indicates the mode of a station after successful transmission of a frame. Set to 1 the field indicates that the station goes into power-save mode. If the field is set to 0, the station stays active.

9.More data: It is 1 bit long field which is used to indicates a receiver that a sender has more data to send than the current frame. This can be used by an access point to indicate to a station in power-save mode that more packets are buffered or it can be used by a station to indicate to an access point after being polled that more polling is necessary as the station has more data ready to transmit.

10.WEP: It is 1 bit long field which indicates that the standard security mechanism of 802.11 is applied.

11.Order: It is 1 bit long field, if this bit is set to 1 the received frames must be processed in strict order.

• **Duration/ID** – It is 4 bytes long field which contains the value indicating the period of time in which the medium is occupied(in μs).

• **Address 1 to 4** – These are 6 bytes long fields which contain standard IEEE 802 MAC addresses (48 bit each). The meaning of each address depends on the DS bits in the frame control field.

• **SC (Sequence control)** – It is 16 bits long field which consists of 2 sub-fields, i.e., Sequence number (12 bits) and Fragment number (4 bits). Since acknowledgement mechanism frames may be duplicated hence, a sequence number is used to filter duplicate frames.

• **Data** – It is a variable length field which contain information specific to individual frames which is transferred transparently from a sender to the receiver(s).

• **CRC (Cyclic redundancy check)** – It is 4 bytes long field which contains a 32 bit CRC error detection sequence to ensure error free frame.

Q.5. (b) Explain the two different basic transmission technologies used to set up WLANs? **(6.5)**

Ans. Two different basic transmission technologies that can be used to set up wireless LAN is,

1. Spread Spectrum Radio:

The Spread Spectrum technique was developed initially for military and intelligence requirements. The essential idea is to spread the information signal over a wider bandwidth. The first type of spread spectrum developed is known as frequency hopping. And the recent version is direct sequence spread spectrum. Both of these techniques are used in various wireless data network products. They also find use in other communications, applications, such as cordless telephones.

These techniques are used for a variety of reasons, including the establishment of secure communications, increasing resistance to natural interference and jamming and to prevent detection.

Two types Spread Spectrum techniques,

(i) Frequency Hopping: Frequency hopping spread spectrum is a method of transmitting radio signals by rapidly switching a carrier among many frequency channels. Its transmission offers three main advantages over a fixed frequency transmission:

Spread-spectrum signals are highly resistant to narrowband interference. The process of re-collecting a spread signal spreads out the interfering signal, causing it to recede into the background.

Spread-spectrum signals are difficult to intercept. An Frequency hopping signal simply appears as an increase in the background noise to a narrowband receiver.

Spread-spectrum transmissions can share a frequency band with many types of conventional transmissions with minimal interference. Bandwidth can be utilized more efficiently.

(ii) Direct Sequence: Direct Sequence Spread Spectrum is one of two types of spread spectrum radio. It is a transmission technology used in Local Area Wireless Network transmissions where a data signal at the sending station is combined with a higher data rate bit sequence, or chipping code, that divides the user data according to a spreading ratio.

The chipping code is redundant bit pattern for each bit that is transmitted, which increases the signal's resistance to interference. If one or more bits in the pattern are damaged during transmission, the original data can be recovered due to the redundancy of the transmission.

The original signal's every bit is represented by multiple bits in the transmitted signal, known as a chipping code. The chipping code spreads the signal across a wider frequency band in direct proportion to the number of bits used. Therefore, a 10-bit chipping code spreads the signal across a frequency band that is 10 times greater than a 1-bit chipping code.

One technique with direct-sequence spread spectrum is to combine the digital information stream with the pseudorandom bit stream using an exclusive-OR.

2. Diffused Infrared: Diffused Infrared(DIR) technology is known as a physical phenomenon for years.

It enables the use of infrared optical emissions without the need for line-of-sight between the transmit and receive communication entities.

The diffused infrared technique has limited usage, inside the buildings only. The transmission is diffused, meaning that the sender and receiver do not have to be aimed at each other.

It can create communication links at distances of over 10meters (30 feet) or more,depending on the emitted optical power. Unlike a direct infrared signal, which emits light in a narrow beam, creating a line-of-sight, narrow angle communication link, a diffuse infrared device floods the room with an infrared signal, and then utilizes the reflections from the ceiling, walls, floors, and other natural surfaces to maintain robust optical communications.

Fully diffused infrared is defined as infrared(IR) communications that is simultaneously non-line-of sight and non-directional. The diffused IR signal, which is emitted from the transmitter at a typically wide emission angel (± 50 degree), fills an enclosed area like the light emanating from a bulb. There is no need to emit in the general direction of the receiver device, because the IR light emitted from the transmitter naturally scatters within the enclosure and reaches the receiver.

UNIT-III

Q.6. (a) As a transport layer protocol, TCP uses a window mechanism to exercise the flow control over the best effort IP in the internet. Flow control is exercised by the edge router based on congestion status encountered in the core routers between the TCP sender and the TCP, receiver. Describe the operation of the window flow control mechanism. **(6.5)**

Ans. The TCP sliding window determines the number of unacknowledged bytes, x, that one system can send to another. Two factors determine the value of x:

- The size of the send buffer on the sending system.
- The size and available space in the receive buffer on the receiving system.

The sending system cannot send more bytes than space that is available in the receive buffer on the receiving system. TCP on the sending system must wait to send more data until all bytes in the current send buffer are acknowledged by TCP on the receiving system.

On the receiving system, TCP stores received data in a receive buffer. TCP acknowledges receipt of the data, and advertises (communicates) a new receive window to the sending system. The receive window represents the number of bytes that are available in the receive buffer. If the receive buffer is full, the receiving system advertises a receive window size of zero, and the sending system must wait to send more data. After the receiving application retrieves data from the receive buffer, the receiving system can then advertise a receive window size that is equal to the amount of data that was read. Then, TCP on the sending system can resume sending data.

The available space in the receive buffer depends on how quickly data is read from the buffer by the receiving application. TCP keeps the data in its receive buffer until the receiving application reads it from that buffer. After the receiving application reads the data, that space in the buffer is available for new data. The amount of free space in the buffer is advertised to the sending system.

Ensure that you understand the TCP window size when you use sliding window for flow control. The window size is the amount of data that can be managed. You might need to adjust the window size if the receive buffer receives more data than it can communicate.

How the send and receive buffers interact has the following consequences:

- The maximum number of unacknowledged bytes that a system can send is the smaller of two numbers:
  - The send buffer size on the sending system

→ The receive window size that the receiving system advertises to the sending system

• When the receiving application reads data as fast as the sending system can send it, the receive window stays at or near the size of the receive buffer. The result is that data flows smoothly across the network. If the receiving application can read the data fast enough, a larger receive window can improve performance.

• When the receive buffer is full, the receiving system advertises a receive window size of zero. The sending system must pause and temporarily cannot send any more data.

• In general, more frequent occurrences of zero size for the receive window results in overall slower data transmission across the network. Every time the receive window is zero, the sending system must wait before sending more data.

Q.6. (b) With a suitable example compare the behaviour or DSDV and DSR algorithms with their routing table and cache contents. (6)

Ans. Refer to Q.4. (b) End Term Examination 2017. (Page No. 22-2017)

OR

Q.7. (a) With an example explain the process of the dynamic source routing of the ad-hoc network. (6)

Ans. Dynamic Source Routing Protocol: The dynamic source routing (DSR) protocol deploys *source routing*. Each node *caches* the specified route to destination during source routing of a packet through that node. This enables a node to provide route specification when a packet source routes from that node. Each node *deletes* the specified route to destination. The deletion is done during routing of error packet in reverse path to the source. The error packet is sent by reverse path in case it is observed by a router that there is a disconnection during forward path to destination. The process of deletion of link shown by the routing table or route-cache is called as link reversal.

DSR ensures that each data packet includes the routing-node addresses also. It is a reactive protocol. It means the router node reacts to the changes and dynamically maintains only the routing addresses from source to destination. The routing addresses at the packets are the active paths to a destination at a given instant.

The router does unicast routing. It means packets are routed to a single destined address.

Let us first understand the two phases, Phase 1 and 2, of the protocol in order to understand the header for source routing, caching of specific route addresses, and the reversal processes of route address specifications.

Phase 1 in DSR Protocol Source node initiates a route discovery process. It broadcasts the packets, each with a header. It then expects a return of acknowledgement from each destination. The packets are called route request (RREQ) packets. DSR uses flooding (sends multiple RREQs).

A header for each RREQ packet has the (*i*) unique request number and (*ii*) source and destination addresses. This enables identification of the (*i*) RREQ at each intermediate node in the request and (*ii*) acknowledged packet(s).

Initially only the source address is given in the header when the routing process starts. When the packet reaches a neighbour, that is, any intermediate node, the node adds its own address in the header if it is able to successfully send the packet to its next

neighbour. When the packet reaches the destined address, its header therefore has all addresses of the nodes in the path.

Q.7. (b) Mention certain situations where Ad-hoc networks are the only choice. **(3)**

Ans. With the increased number of lightweight devices as well as evolution in wireless communication, the ad hoc networking technology is gaining effort with the increasing number of widespread applications. Ad hoc networking can be used anytime, anywhere with limited or no communication infrastructure. The preceding infrastructure is fancy or annoying to use. The ad hoc network architecture can be used in real time business applications, corporate companies to increase the productivity and profit. The ad hoc networks can be classified according to their application as Mobile Ad hoc NETwork (MANET) which is a self-arranging infrastructureless network of mobile devices communicated through wireless link. Vehicular Ad hoc NETwork (VANET) uses travelling cars as nodes in a network to create a mobile network. Wireless Sensor Network (WSN) consists of autonomous sensors to control the environmental actions. The importance of ad hoc network has been highlighted in many fields which are described below:

Military arena: An ad hoc networking will allow the military battleground to maintain an information network among the soldiers, vehicles and headquarters.

Provincial level: Ad hoc networks can build instant link between multimedia network using notebook computers or palmtop computers to spread and share information among participants (e.g. Conferences).

Personal area network: A personal area network is a short range, localized network where nodes are usually associated with a given range. Industry sector: Ad hoc network is widely used for commercial applications. Ad hoc network can also be used in emergency situation such as disaster relief. The rapid development of non-existing infrastructure makes the ad hoc network easily to be used in emergency situation.

Bluetooth: Bluetooth can provide short range communication between the nodes such as a laptop and mobile phone

Q.7 (c) Explain mobile TCP. **(3.5)**

Ans. With the advent of WLANs, a lot of research went into increasing the performance of TCP in wireless and mobile environments, some of its outcome are I-TCP and SNOOP-TCP, Mobile-TCP etc.

• M-TCP (mobile TCP) has the same goals as similar to its variants i.e. I-TCP and Snoop-TCP. It too wants to improve overall throughput, to lower the delay, to main end-to-end semantics of TCP.

• But, it is mainly enhanced to address problems related to lengthy or frequent disconnections.

Basic TCP methodology:

1. When a node does not receive an acknowledgement back form the host, it carries out retransmission.

2. A TCP sender tries to retransmit data controlled by retransmission timer which doubles up with each unsuccessful attempt. (upto a maximum of one minute)

3. A sender tries to retransmit an unacknowledged packet every one minute and gives up after 12 minutes.

4. If in I-TCP, the mobile host is disconnected, then in such a situation, the FA will keep of buffering more and more data packets.

5. In case of a handover following this disconnection, we have more data to be transmitted to new FA.

6. Snoop-TCP also suffers from similar such problems.

UNIT-IV

Q.8. (a) Explain wireless device with palm OS architecture. (6)

Ans. Refer to Q.5. (b) End Term Examination 2017. (Page No. 25-2017)

Q.8. (b) Explain in detail about mobile application languages and tool kits. (3)

Ans. Mobile application languages:

1. Java: Java has always been the undisputed leader of being the most prominent and highly employed mobile app coding language since its birth. Java is mainly utilized for developing desktop applications, back-end web frameworks and Android applications, which makes it the best mobile platform for developers in 2019.

2. Python: In recent years, Python has become a language employed by substantial users including enterprises and best business organizations. They were widely popular due to their ability to give better results, agility and user experience to the customers.

3. PHP: It is a server-side scripting language, designed by Zend Technologies in 1995. It is used for general purpose development today but originally, was developed for websites.

4. js: Buildfire.js uses the BuildFire SDK and Javascript to allow developers to build mobile apps with the support of BuildFire backend at an unprecedented rate.

5. C++: C++ features low-level memory manipulation with a general purpose object-oriented programming language.

6. JavaScript: It is a high-level expound programming language. JavaScript is a multi-patterned language supporting object-oriented and functional programming.

7. C#: C# is also known as C Sharp. It is component and object-oriented, multi-paradigm programming language. This general-purpose programming language is developed Microsoft.

Mobile application toolkits

1. BuildFire.js: BuildFire.js is a cross platform library used to build custom functionality in BuildFire's platform. It allows unlimited customization with nothing but JavaScript, making it one of the simplest to implement frameworks.

2. Framework 7: Framework 7 used to be iOS only, but now offers Android support as well. If you want to develop an app that looks and feels like a clean iOS app even on Android, Framework 7 is for you.

3. Ionic: The Ionic Framework is based on the Sass CSS language. It's also cross-platform, meaning it can run on multiple operating systems. It's pretty easy to use and can also be integrated with AngularJS to build more advanced apps.

4. jQuery Mobile: Over half of all mobile websites are currently using jQuery mobile. It's one of the oldest app dev tools out there, and has more functionality than most. It's been called the "swiss army knife of mobile app dev tools".

Q.8. (c) Explain the features of SyncML. **(3.5)**

Ans. SynchML is a data synchronization language based on XML. SynchML-based software synchronized data for PIM (email, calender, tasks-to-do list, or contacts list) databases and files for data.

SynchML is an open stanard based on XML. Use of a common and standard language enables interoperability. It also provides specifications for the protocols for sending message from one node to another and representation of the messages.

SynchML has revolutionized mobile application–development, services, and devices. The SynchML data engine performs the following tasks:

- SynchML code generation
- parsing of received synchML data
- validation of DTA in WBXML and XML formats of data
- base-64 encoding/dedcoding
- notification message passing
- credential checks.
- security operations and
- HMAC data integrity check.

OR

Q.9. (a) Explain the features of data replication and adaptive clustering for mobile wireless network. **(4.5)**

Ans. Features of data replication:

Mobile environment

- Limited memory space
- Disk Space
- Battery Power
- Processor capacity
- Device flexibility
- Mobility of users
- Multiterminal accesses
- Nature of wireless n/w
- Security and other aspects

Adaptive clustering: The objective of clustering is to partition the network into several clusters, within each cluster, nodes can communicate with each other in at most two hops. The clusters can be constructed based on node ID. The following algorithm partitions the multihop network into some non overlapping clusters.

1. Every node has a unique ID and knows the IDS of its 1-hop negihbors.
2. A message sent by a node is received correctly within a finite time by all its 1-hop neighbors.
3. Network topology does not change during the execution.

(4 × 2 = 8)

Q.9. (b) Attempt any two parts:

(i) User agent profile and Caching.

Ans. The user Agent profile (UA Prof) specification allows WAP to notify the content server about the device capability.

UA Profile is also referred to as capability and preference information (CPI). CPI is passed from the WAP client to the origin server through intermediate network points. It is compatible with composite capability/preferance profile of the W3C.

Devices that support UAProf architecture provide a URL in the WAP or HTTP session header. This URL points to a XML file that describes the profile of that device. Many vendors have their own public HTTP-servers whare service providers can download device profiles as standardized XML documents. In case of MMS (Multimedia message service), the MMSC (MMS controller) is able to pick the profile address from the protocol header and fetch the respective device profiile. Device profile information is used by the MMSC to format the content to best suit the terminals capabilities.

(ii) Data synchronization.

Ans. SynchML is a data synchronization language based on XML. SynchML-based software synchronized data for PIM (email, calender, tasks-to-do list, or contacts list) databases and files for data.

SynchML is an open stanard based on XML. Use of a common and standard language enables interoperability. It also provides specifications for the protocols for sending message from one node to another and representation of the messages.

SynchML has revolutionized mobile application–development, services, and devices. The SynchML data engine performs the following tasks:

- SynchML code generation
- parsing of received synchML data
- validation of DTA in WBXML and XML formats of data
- base-64 encoding/dedcoding
- notification message passing
- credential checks.
- security operations and
- HMAC data integrity check.

(iii) Mobility management.

Ans. Mobility management:

Location management on mobile devices will become increasingly important in the new future, considering the increasing number of location-enabled mobile devices and location-based services on the technical side, location-enabled devices and location-based services have been deployed and used for a number of years already. However, there are two issues, one is, how to make location information openly available on the Web, and the second is, how to provide users with privacy control in such an environment. Location management is a two -stage process that enables the network to discover the current attachment point of the mobile user for call delivery. The first stage is location registration (or location update). In this stage, the mobile terminal periodically notifies the network of its new access point, allowing the network to authenticate the user and revise the user's location file. The second stage is call delivery. Here, the network is queried for the user location profile and the current position of the mobile host is found.

MID TERM EXAMINATION [MAY, 2023]
EIGHTH SEMESTER [B.TECH]
MOBILE COMPUTING [ETIT-402]

Time: 1.5 Hrs. **Max. Marks: 30**

Note: Q. No. 1 is compulsory. Attempt any two more Questions from the rest.

Q.1. (a) Explain the shape of the cell in a cellular system with reason. (3)

Q.1. (b) Compare the features of 2G, 3G and 4G. (3)

Q.1. (c) What is frequency re-use. (2)

Q.1. (d) What changes done in GSM network to support GPRS services. (2)

Q.2. (a) Explain GSM operations with its architecture. (5)

Ans. Refer to Q.3 (a) End Term Examination 2017 (Pg. No. 16-2017).

Q.2. (b) What is handoff. What are its type. (5)

Ans. Refer to Q.1 (c) End Term Examination 2019 (Pg. No. 6-2019).

Q.3. (a) What are multiple access techniques. Explain in detail. (5)

Q.3. (b) Write a short note on (a) WAP (b) Zigbee

Ans. Refer to Q.1 (b) End Term Examination 2017 (Pg. No. 8-2017). & Refer to Q.4 (i) First Term Examination 2019 (Pg. No. 3-2019).

Q.4. (a) Explain WiMax. (5)

Ans. Refer to Q.4 (iii) First Term Examination 2019 (Pg. No. 4-2019).

Q.4. (b) Explain Bluetooth with its types. (5)

END TERM EXAMINATION [JULY 2023]
EIGHTH SEMESTER [B.TECH]
MOBILE COMPUTING [ETIT-402]

Time: 3 Hrs. **Max. Marks: 75**

Note: Attempt five questions in all including Q. No. 1 which is compulsory. Select one question from each unit.

Q.1. Answer the following briefly.

Q.1. (a) Extending the functions of a foreign agent with a 'snooping' TCP proves to be advantages. Justify. (2.5)

Q.1. (b) What advantages does the use of IPv6 offer for mobility? (2.5)

Ans. Refer to Q.1 (b) Second Term M.P.

Q.1. (c) Explain RTS and CTS frames with respect to WLANs. (2.5)

Q.1. (d) Explain the concept of near & far terminals in wireless networks? (2.5)

Q.1. (e) List the significant advantages of HIPERLAN 2 networks. (2.5)

Q.1. (f) Draw the Three tier architecture of mobile computing. (2.5)

Ans. Refer to Q.2 First Term Examination 2018 (Pg. No. 4-2018).

Q.1. (g) Explain data hoarding and data dissemination with respect to mobile computing. (2.5)

Q.1. (h) Justify the importance of Routing in Ad-Hoc networks and give examples of routing protocols used in wireless networks. (2.5)

Q.1. (i) State the main differences between UDP and TCP. (2.5)

Q.1. (j) Explain the need for specialized MAC in mobile networks. (2.5)

UNIT - I

Q.2. (a) Justify: In mobile cellular networks the uplink frequencies are of lower range as compared to the downlink frequencies but in satellite communication systems the uplink frequencies are of higher frequency range as compared to downlink frequency range. Mention the Uplink and Downlink frequency range for GSM and CDMA systems. (4)

Q.2. (b) Draw neatly the WAP protocol stack. (2.5)

Ans. Refer to Q.1 (b) End Term Examination MTP.

Q.2. (c) A FDD Cellular telephone system has a total bandwidth of 33 MHz. Two 25 KHz simplex channels is are used to provide a full duplex voice and control channels, compute the number of channels available per cell if a system uses, (6)

(1) 4-cell reuse (2) 7-cell reuse (3) 12-cell reuse.

Determine an equitable distribution of control channels and voice channels in each cell for each of the three systems if control channels are allocated a total bandwidth of 1MHz.

Q.3. (a) In reference to file systems, discuss the problems and solutions regarding consistency in mobile networks. (6)

Q.3. (b) Explain the logical channels of GSM along with the classification chart and state where that channel is uplink channel or downlink channel. (6.5)

UNIT - II

Q.4. (a) In context with wireless systems, explain how multiple access with collision avoidance scheme solves the problem of hidden terminal. (6)

Q.4. (b) With help of a neat diagram explain the Major baseband states of a Bluetooth device? (6.5)

Q.5. (a) In context to MAC schemes, explain the polling scheme and the Inhibit sense multiple access scheme, with relevant diagrams? (6)

Q.5. (b) With help of a neat diagram show the formation of piconet and scatternet in bluetooth networks. Discuss the 6 main differences between Bluetooth technology and Zigbee technology. (6.5)

UNIT - III

Q.6. (a) Justify with an example that least interference routing proves to be an efficient method as compared to the routing methods based on number of hops. (6.5)

Q.6. (b) In reference to mobile IP networks explain-Tunneling, Encapsulation and Registration. (6)

Q.7. (a) How and why does I-TCP isolate problems on the wireless link? What are the main drawbacks of this solution? (6.5)

Q.7. (b) In mobile IP networks explain the triangular routing problem and what is the solution to this problem? (6)

UNIT IV

Q.8. Discuss the different Operating Systems in wireless devices. (12.5)

Q.9. How does caching improve access time and reduce bandwidth requirements? What are locations for a cache and their specific advantages? (12.5)