FIRST TERM EXAMINATION [FEB. 2017]
EIGHTH SEMESTER [B.TECH]
MOBILE COMPUTING [ETIT–402]

Time : 1.5 Hrs. **M.M. : 30**

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

Q.1. (a) What are the applications of Bluetooth. **(2)**

Ans. (i) Internet Bridge: Providing dial-up networking and fax capabilities without need for physical connection to the PC.

(ii) File transfer: Ability to transfer data objects from one device to another.

(iii) LAN Access: In this usage model multiple data terminals use a LAN access point as a wireless coneection to an Ethernet LAN.

(iv) Synchronization: Provides a device-to-device synchronization of data.

(v) Headset: It can be wirelessly connected for the purpose of acting as a remote device's audio input and output interface.

Q.1. (b) What do you mean by handoff in GSM? **(2)**

Ans. Refer Q.1. (d) of First Term 2016.

Q.1. (c) Describe the functions of MAC in mobile data link layer. **(2)**

Ans. Functions of MAC (Medium Access control) are:

(i) Paging

(ii) Network control, error control and correction

(iii)Setup, maintain, and releasing channels for higher layers.

(iv) Activating/deactivating physical channels.

(v) Broadcasting

(vi) Segmentation

(vii) Re-assembly

(viii) Packet formatting.

Q.1. (d) What are the applications of GPRS? **(2)**

Ans. Applications of GPRS

(i) Chat: It is a very popular services in Internet and GSM.

(ii) Multimedia services: Multimedia objects like photographs, pictures, post cards, greeting cards and presentations, static web pages can be sent and received over the mobile network.

(iii) Virtual private network: GPRS network can be used to offer VPN services. Many Bank ATM machines use VSAT to connect the ATM system with the banks server.

(iv) Personal Information Management: Personal diary, address book, appointments, engagements etc. are very useful for a mobile individual. Some of these are kept in the phone, some in the organizer and some in the Intranet.

(v) Job Sheet Dispatch: GPRS can be used to assign and communicate job sheets from office-based staff to mobile field staff. Customers typically telephone a call center whose staff takes the call and categorize it. Those calls requiring a visit by field sales or service representative can then be escalated to those mobile workers.

(vi) Unified Messaging: Unified messaging uses a single mailbox for all messages, including voice mail, fax, e-mail, SMS, MMS, and pager messages. With the various mailboxes in one place, unified messaging systems then allow for a variety of access methods to recover message of different types. Some will use text-to-voice systems to read e-mail and, less commonly, faxes over a normal, phone line, while most will allow the interrogation of the contents of the various mailboxes through data access, such as the Internet.

(vii) Vehicle Positioning: This application integrates GPS (Global Positioning System) that tell people where they are. GPS is a free-to-use global network of 24 satellites run by the US Department of Defense. Anyone with a GPS receiver can receive their satellite position and thereby find out where they are. Vehicle-positioning applications can be used to deliver several services including remote vehicle diagnostics, ad hoc stolen vehicle tracking and new rental car fleet tariffs.

(viii) Location-based Services and Telematics: Location-based services provide the ability to link push or pull information services with a user's location. Examples include hotel and restaurant finders, roadside assistance, and city-specific news and information.

Q.1. (e) What are the applications of mobile computing? **(2)**

Ans. (i) Smartphones: A smartphone is a mobile phone with additional computing functions so as to enable multiple applications.

(ii) Enterprise solutions: Enterprises or large business networks have huge database and documentation requiremeats

(iii) Music, video, and e-books.

(iv) Mobile cheque: It is a mobile-based payment system employed during a purchase.

(vi) Mobile-based supply chain management.

Q.2. (a) Draw and explain the architecture of WAP.

Ans. Refer Q.1. (b) of End Term 2017.

Q.2. (b) Explain the design considerations for Mobile Computing. **(5)**

Ans. Design Considerations for Mobile Computing

The mobile computing environment needs to be context-independent as well as context-sensitive. Context information is the information related to the surrounding environment of an actor in that environment. The term "context" means, all the information that helps determine the state of an object (or actor). This object can be a person, a device, a place, a physical or computational object, the surrounding environment or any other entity being tracked by the system. There are many ways in which content and behaviour can be adapted. Following are some examples:

1. Content with context awareness: Build each application with context awareness. There are different services for different client context (devices). For example, a bank decides to offer mobile banking application through Internet, PDA and mobile phone using WAP These services are different and are http://www.mybank.com/inet.html, http://www.mybank.com/ palm.html and http://www.mybank.com/wap.wml, respectively The service http://www. mybank.com/inet.html assumes that the user will use computer to access this service. Therefore it is safe to offer big pages with text boxes and drop down menus. We know that http:// www.mybank.com/palm.html is a service for a PalmOS PDA. As the display size is small, we design the screen to be compact for the PDA and do not offer the same product animation.

2. Content switch on context: Another way is to provide intelligence for the adaptation of content within the service. This adaptation happens transparent to the ient. In this case the service is the same for Internet, PDA and WAP. All access the nk's service through http://www.mybank.com/. An intelligent piece of code identifies e agent to decide what type of device or context it is.

3. Content transcoding on context: Another way is to provide an underlying iddleware platform that performs the adaptation of the content based on the context nd behaviour of the device. This adaptation happens transparent to the client and the pplication. The middleware platform is intelligent enough to identify the context either m the HTTP or additional customized parameters. In this case the service may be in ml or XML, the middleware platform transcodes the code from html (or XML) to html, nd wml on the fly. It can also do the transcoding based on policy so that the html nerated for a computer is different from a PDA

Q.3. (a) Explain wireless session protocol. **(5)**

Ans. The wireless transaction protocol (WTP) is on top of either WDP or, if security required, WTLS. WTP has been designed to run on very thin clients, such as mobile ones.

WTP offers many features to the higher layers. The basis is formed from three classes transaction service as explained in the following paragraphs. Class 0 provides reliable message transfer without any result message. Classes 1 and 2 provide reliable essage transfer, class 1 without, class 2 with, exactly one reliable result message (the pical request/response case). WTP achieves reliability using duplicate removal, transmission, acknowledgements and unique transaction identifiers. No WTP-class quires any connection set-up or tear-down phase. This avoids unnecessary overhead the communication link. WTP allows for asynchronous transactions abort of nsactions, concatenation of messages, and can report success or failure of reliable essages (e.g., a server cannot handle the request).

WTP class 0

Class 0 offers an unreliable transaction service without a result message. The nsaction is stateless and cannot be aborted. The service is requested with the R-Invoke.req primitive as shown in Figure(1). Parameters are the source address (SA), urce port (SP), destination address (DA), destination port (DP) Additionally, with, e A flag the user of this service can determine, if the responder "WTP entity should nerate an acknowledgement or if a user acknowledgement should be used. The WTP yer will transmit the **user data** (UD) transparently to its destination The class type indicates here class 0. Finally, the transaction handle H provides a simple index to niquely identify the transaction and is an alias for the tuple (SA, SP, DA, DP), i.e., a cket pair, with only local significance.

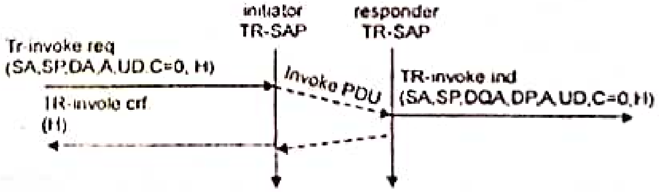


Fig. 1. Basic transaction

WTP Class 1.

Class 1 offers a reliable transaction service but without a result message. Again, e initiator sends an invoke PDU after a TR-Invoke.req from a higher layer. This time, class equals '1', and no user acknowledgement has been selected as shown in Fig. The responder signals the incoming invoke PDU via the. TR-Invoke.ind primitive higher layer and acknowledges automatically without user intervention specification also allows the user on the responder's side to acknowledge, but th

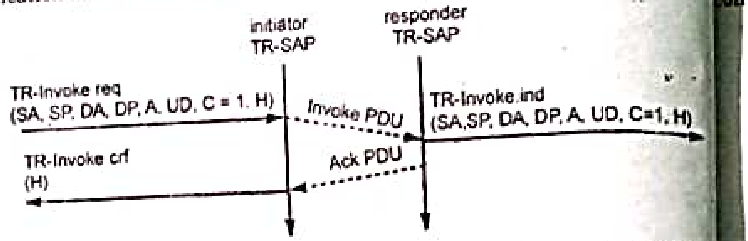

initiator TR-SAP
responder TR-SAP
TR-Invoke req (SA, SP, DA, DP, A, UD, C = 1, H)
Invoke PDU
TR-Invoke.ind (SA,SP, DA, DP, A, UD, C=1, H)
TR-Invoke crf (H)
Ack PDU

Fig. 2. Basic transaction, WTP class 1, no user acknowledgment

acknowledgement is not required. For the initiator the transaction ends wi reception of the acknowledgement. The responder keeps the transaction state for time to be able to retransmit the acknowledgement if it receives the same invoke again indicating a loss of the acknowledgement.

WTPClass2.

Finally, class 2 transaction service provides the classic reliable request/re transaction known from many client/server scenarios. Depending on user require many different scenarios are possible for initiator/responder inter-action.

Fig. (3) shows the basic transaction of class 2 .without-user acknowledgement a user on the initiator's side requests the service and the WTP entity sends the PDU to the responder. The WTP entity on the responder's side indicates the r with the TR-Invoke.ind primitive to a user.

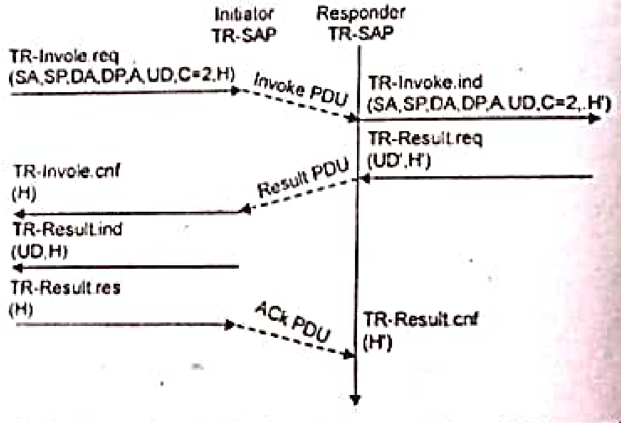


Fig. (3) Basic transaction WTP class 2, no user acknowledgement

Q.3. (b) Explain multiple access with collision avoidance.

Ans. Multiple access with collision avoidance (MACA) presents a simple that solves the hidden terminal problem, does not need a base station, and i random access Aloha scheme - but, with dynamic reservation. Figure(1) shows th

minals. Remember, A and C both want to send to B. A has already started the nsmission, but is hidden for C, C also starts with its transmission, thereby causing ollision at B.

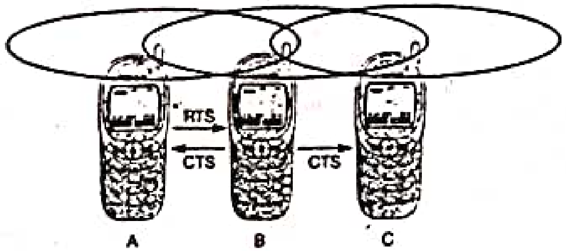


Fig. 1. MACA can avoid hidden terminals

With MACA, A does not start its transmission at once, but sends a request **to send** TS) first. B receives the RTS that contains the name of sender and receiver, as well as length of the future transmission. This RTS is not heard by C, but triggers an owledgement from B, called clear to send (CTS). This CTS is now heard by C and medium for future use by A is now reserved for the duration of the transmission. r receiving a CTS, C is not allowed to send anything for the duration indicated in CTS toward B. A collision cannot occur at B during data transmission, and the hidden inal problem is solved-provided that the transmission conditions remain the same.

Still, collisions can occur during the sending of an RTS, Both A and C could send an that collides at B. RTS is very small compared to the data transmision, so the bability of a collision is much lower. B resolves this contention and acknowledges y one-station in the CTS (if it was able to recover the RTS at all). No transmission is owed without an appropriate CTS.

Figure (2) shows simplified state machines for a sender and receiver. The sender is until a user requests the transmission of a data packet. The sender then issues an S and waits for the right to send. If the receiver gets an RTS and is in an idle state, ends back a CTS and waits for data. The sender receives the CTS and sends the a. Otherwise, the sender would send an RTS again after a time-out (e.g., the RTS

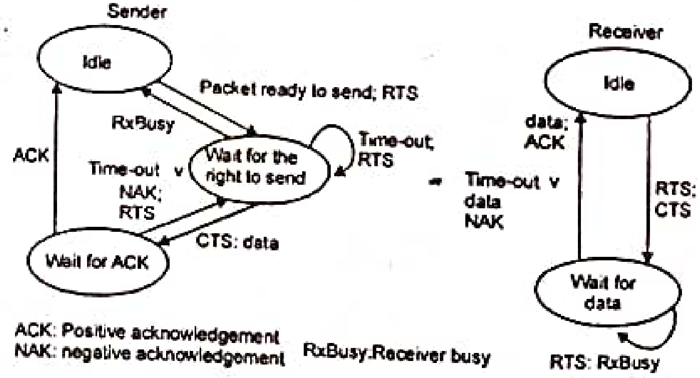


Fig. 2. Protocol machines for multiple access with collision avoidance

could be lost or collided). After transmission of the data, the sender waits for a posi acknowledgement to return into an idle state. The receiver sends back a posi acknowledgement if the received data was correct. If not, or if the waiting time for d is too long, the receiver returns into idle state. If the sender does not receive acknowledgement or a negative acknowledgement, it sends an RTS and again wait the right to send. Alternatively, a receiver could indicate that it is currently busy v separate RxBusy.

Q.4. (a) Explain ISMA (Inhibit Sense Multiple Access) and polling scheme medium access control.

Ans. Polling

Where one station is to be heard by all others (e.g., the base station of a mob phone network or any other dedicated station), **polling** schemes (known from mainframe/terminal world) can be applied. Polling is a strictly centralized scheme one master station and several slave stations. The master can poll the slaves accord to many schemes: round robin (only efficient if traffic patterns are similar over stations), randomly, according to reservations (the classroom example with po students) etc. The master could also establish a list of stations wishing to trans during a contention phase. After this phase, the station polls each station on the Similar schemes are used, e.g., in the Bluetooth wireless LAN and as one possible ac function in IEEE 802.11 systems.

Inhibit sense multiple access (ISMA)

Another combination of different schemes is represented by inhibit sense mult access (ISMA). This scheme, which is used for the packet data transmission ser Cellular Digital Packet Data (CDPD) in the AMPS mobile phone system, is also kn as **digital sense multiple access** (DSMA). Here, the base station only signals a b medium via a busy tone (called BUSY/IDLE; indicator) on the downlink Figure (1). A the busy tone-stops, accessing the uplink is not coordinated any further. The base sta acknowledges successful transmissions, a mobile station detects a collision only the missing positive acknowledgement. In case of collisions, additional back-off retransmission mechanisms are implemented.

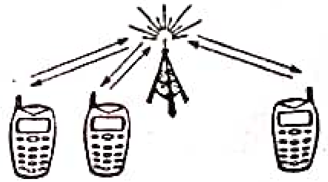


Fig.1. Inhibit sense multiple access using a busy tone.

Q.4. (b) Write short notes on any two of the following.

Ans. (b) ZigBee is a low-cast, low-power, wireless mesh network standard targ at the wide development of long battery life devices in wireless control and monito applications. Zigbee devices have low latency, which further reduces average curre

ZigBee chips are typically integrated with radios and with microcontrollers have between 60-256 KB of flash memory. *ZigBee* operates in the industrial, scie and medical (ISM) radio bands: 2.4 GHz in most jurisdictions worldwide; 784 MH *China*, 868 MHz in Europe and 915 MHz in the USA and Australia. Data rates *from* 20 kbit/s (868 MHz band) to 250 kbit/s (2.4 GHz band).

The ZigBee network layer natively supports both star and tree networks, and generic mesh networking. Every network must have one coordinator device, tasked with its creation, the control of its parameters and basic maintenance. Within star networks, the coordinator must be the central node. Both trees and meshes allow the use of ZigBee routers to extend communication at the network level.

ZigBee builds on the physical layer and media access control defined in IEEE standard 802.15.4 for low-rate WPANs. The specification includes four additional key components: network layer, application layer, ZigBee device objects (ZDOs) and manufacturer-defined application objects which allow for customization and favor total integration. ZDOs are responsible for some tasks, including keeping track of device roles, managing requests to join a network, as well as device discovery and security.

ZigBee is one of the global standards of communication protocol formulated by the significant task force under the IEEE 802.15 working group. The fourth in the series, WPAN Low Rate/ZigBee is the newest and provides specifications for devices that have low data rates, consume very low power and are thus characterized by long battery life. Other standards like Bluetooth and IrDA address high data rate applications such as voice, video and LAN communications.

Q.4. (b) (*ii*) WiMAX (Worldwide Interoperability for Microwave Access) is a family of wireless communication standards based on the IEEE 802.16 set of standards, which provide multiple physical layer (PHY) and Media Access Control (MAC) options.

The name "WiMAX" was created by the WiMAX Forum, which was formed in June 2001 to promote conformity and interoperability of the standard, including the definition of predefined system profiles for commercial vendors. The forum describes WiMAX as "a standards-based technology enabling the delivery of last mile wireless broadband access as an alternative to cable and DSL".

WiMAX was initially designed to provide 30 to 40 megabit-per-second data rates.with the 2011 update providing up to 1 Gbit/ss for fixed stations.

Q.4. (b) (*iii*) IrDA- IrDA (Infrared Data Association) is an industry-sponsored organization set up in 1993 to create international standards for the hardware and software used in infrared communication links. In this special form of radio transmission, a focused ray of light in the infrared frequency spectrum, measured in terahertz, or trillions of hertz (cycles per second), is modulated with information and sent from a transmitter to a receiver over a relatively short distance. Infrared radiation (IR) is the same technology used to control a TV set with a remote control.

Infrared data communication is playing an important role in wireless data communication due to the popularity of laptop computers, personal digital assistants (PDAs), digital cameras, mobile telephones, pagers, and other devices. Among existing uses or likely possibilities are:

- Sending a document from your notebook computer to a printer
- Exchanging business cards between handheld PCs
- Coordinating schedules and telephone books between your desktop and notebook computers.

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 ar.d 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 n[illegible]equired 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.

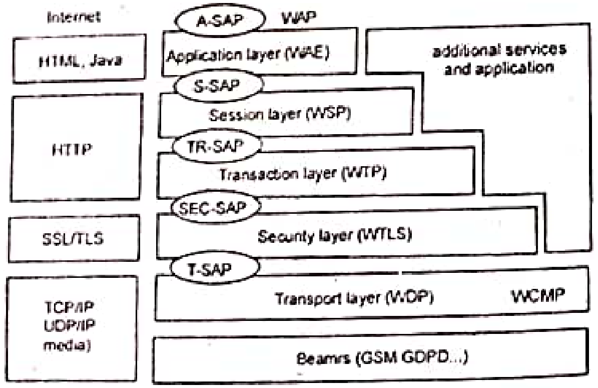


Fig.l. Components and interface of the WAP 1. architccure

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 schem doubles the congestion window every time the acknowledgements come back, which tak one round trip time (RTT). This is called the exponential growth of the congestion windo in the slow start mechanism.

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

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

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

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

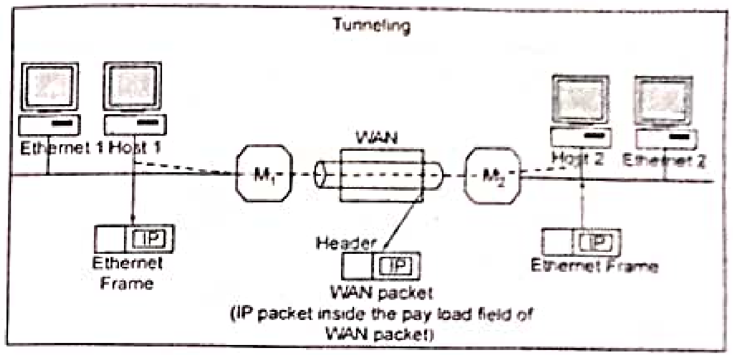
Ans. Tunneling

Tunneling is an internetworking strategy that is used when source and destina 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 v different kind pf network that interconnects them.

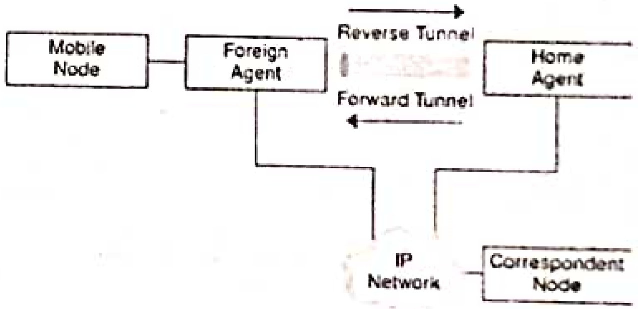
To understand tunneling, let an Ethernet is to be connected to another Ethernet v a WAN.

- The IP packets are to be sent from host 1 of Ethernet 1 to host 2 of Ethernet 2 v a WAN.
- To send an IP packet to host 2, host 1 constructs the packet containing the I address of host 2.
- It then inserts this packet into an Ethernet frame. This frame is addressed the multi-protocol router M_1 and is placed on Ethernet.
- When this packet reaches, multiprotocol router M_1, it removes the IP packet a 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
- When this packet reaches M_2, it removes the IP packet and inserts it into t Ethernet frame and sends it to host 2.
- In the above process, IP packets do not have to deal with WAN, they just tra from one end of the tunnel to the other end. The host 1 and host 2 on two Ethernet a 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.

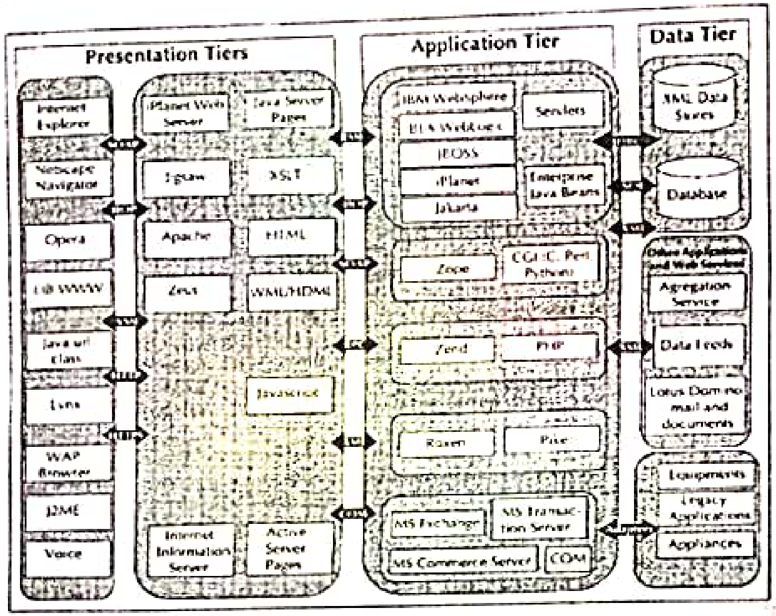


Fig.1. The mobile Computing Architecture

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 deviceis 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 cal! 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:

(a) Group one includes methods based on network architecture and algorithms, mainly on processing capabilities of the system.

(b) Group two includes methods based on learning processes (i.e. which require the collection of statistics on subscribers' mobility behavior). This method emphasizes the information capabilities of the network.

For LM purposes, a wireless network usually consists of Location Areas (LAs) and Paging Areas (PAs). While LAs are a set of areas over which location updates take place, PAs are a set of areas over which paging updates take place. Usually, LAs and PAs are contiguous, but that is not the case always. In addition, a LA usually contains several PAs.

As the size of the LA increases, the cost of paging will also increase as more PAs are to be paged to find a called mobile host. On the other hand, reducing the size of a LA will increase the number of crossings per unit time. Hence, the cost of location update or registration will rise. Both paging and location updates consume scarce resources like wireless network bandwidth and power of mobile hosts. Each has a significant cost associated with it. So, LA planning is to be based on a criterion that guarantees the total signaling load, which comprises paging and registration, is kept under tolerable limits. Therefore, it is characterized by the trade-off between the number of location updates and the amount of paging signaling that the wireless network has to deal with.

Q.2. (b) What is TCP/IP? Explain the architecture of TCP/IP with a schematic diagram. (6.5)

Ans. Transmission Control Protocol/Internet Protocol (TCP/IP) is the language a computer uses to access the Internet. It consists of a suite of protocols designed to establish a network of networks to provide a host with access to the Internet.

TCP/IP is responsible for full-fledged data connectivity and transmitting the data end-to-end by providing other functions, including addressing, mapping and acknowledgment. TCP/IP contains four layers, which differ slightly from the OSI model.

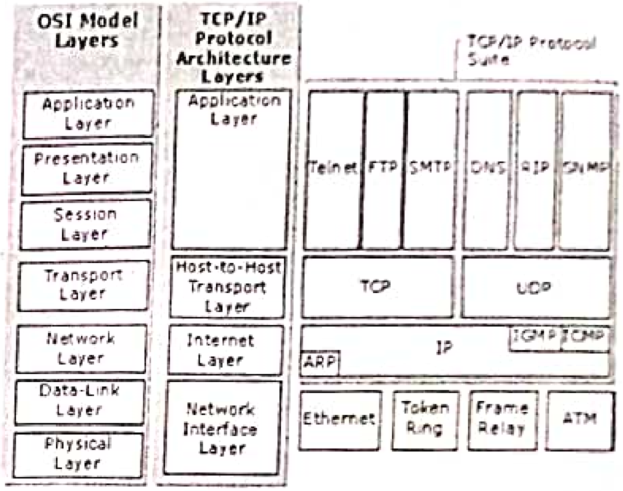
As with any form of communication, two things are needed: a message to transmit and the means to reliably transmit the message. The TCP layer handles the message part. The message is broken down into smaller units, called packets, which are then transmitted over the network. The packets are received by the corresponding TCP layer in the receiver and reassembled into the original message.

The IP layer is primarily concerned with the transmission portion. This is done by means of a unique IP address assigned to each and every active recipient on the network.

TCP/IP is considered a stateless protocol suite because each client connection is newly made without regard to whether a previous connection had been established.

TCP/IP Protocol Architecture

TCP/IP protocols map to a four-layer conceptual model known as the *DARPA model*, named after the U.S. government agency that initially developed TCP/IP. The four layers of the DARPA model are: Application, Transport, Internet, and Network Interface. Each layer in the DARPA model corresponds to one or more layers of the seven-layer Open Systems Interconnection (OSI) model.



Network Interface Layer

The *Network Interface layer* (also called the Network Access layer) is responsible for placing TCP/IP packets on the network medium and receiving TCP/IP packets off the network medium. TCP/IP was designed to be independent of the network access method, frame format, and medium. In this way, TCP/IP can be used to connect differing network types. These include LAN technologies such as Ethernet and Token Ring and WAN technologies such as X.25 and Frame Relay. Independence from any specific network technology gives TCP/IP the ability to be adapted to new technologies such as Asynchronous Transfer Mode (ATM).

The Network Interface layer encompasses the Data Link and Physical layers of the OSI model. Note that the Internet layer does not take advantage of sequencing and acknowledgment services that might be present in the Data-Link layer. An unreliable Network Interface layer is assumed, and reliable communications through session establishment and the sequencing and acknowledgment of packets is the responsibility of the Transport layer.

Internet Layer

The *Internet layer* is responsible for addressing, packaging, and routing functions. The core protocols of the Internet layer are IP, ARP, ICMP, and IGMP.

- The *Internet Protocol* (IP) is a routable protocol responsible for IP addressing, routing, and the fragmentation and reassembly of packets.
- The *Address Resolution Protocol* (ARP) is responsible for the resolution of the Internet layer address to the Network Interface layer address such as a hardware address.
- The *Internet Control Message Protocol* (ICMP) is responsible for providing diagnostic functions and reporting errors due to the unsuccessful delivery of IP packets.
- The *Internet Group Management Protocol* (IGMP) is responsible for the management of IP multicast groups.

The Internet layer is analogous to the Network layer of the OSI model.

Transport Layer

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

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

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

Application Layer

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

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

- The Hypertext Transfer Protocol (HTTP) is used to transfer files that mak 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 m messages and attachments.
- Telnet, a terminal emulation protocol, is used for logging on remotely to netwo hosts.

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

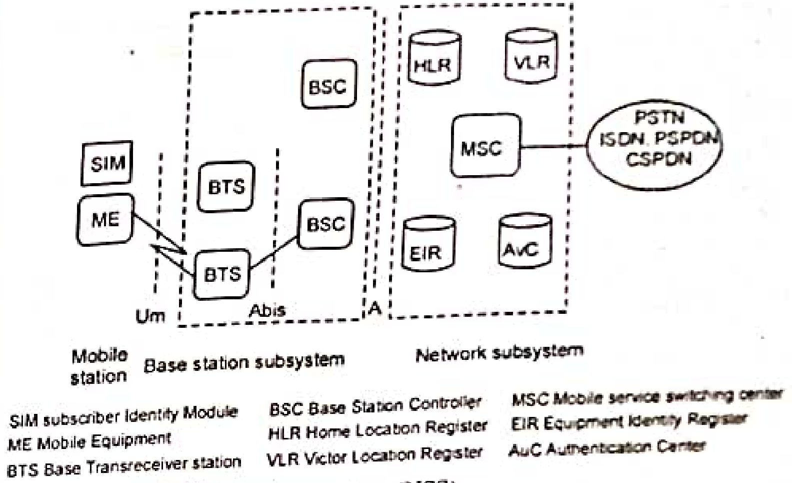
- The Domain Name System (DNS) is used to resolve a host name to an IP addre
- The Routing Information Protocol (RIP) is a routing protocol that routers use exchange routing information on an IP internetwork.
- The Simple Network Management Protocol (SNMP) is used between a netw management console and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

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

Q.3. (a) Explain the architecture of GSM and discuss GSM services a security in brief. (6

Ans.

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


SIM
ME
BTS
BTS
BSC
BSC
HLR
VLR
MSC
EIR
AuC
PSTN
ISDN, PSPDN
CSPDN
Um
Abis
A
Mobile station
Base station subsystem
Network subsystem
SIM subscriber Identity Module
ME Mobile Equipment
BTS Base Transreceiver station
BSC Base Station Controller
HLR Home Location Register
VLR Victor Location Register
MSC Mobile service switching center
EIR Equipment Identity 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), Authentication 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 location, forwarding address, authentication/ciphering keys, and billings information. In addition to the ISDN telephone number for the terminal, the SIM card is identified with a 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 MSC's 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

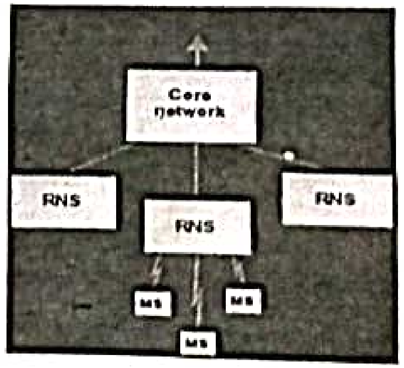
The UMTS network architecture can be divided into three main elements:

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 mecha

Ans. DSDV- Destination sequence distance vector

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

DSDV now adds two things to the distance vector algorithm:

• **Sequence numbers:** Each routing advertisement comes with a sequence num Within ad-hoc networks, advertisements may propagate along many paths. Seq numbers help to apply the advertisements in correct order. This avoids the loops are likely with the unchanged distance vector algorithm.

• **Damping:** Transient changes in topology that are of short duration should destabilize the routing mechanisms. Advertisements containing changes in the top currently stored are therefore not disseminated further. Anode waits with dissemi if these changes are probably unstableWaiting time depends on the time betwee first and the best annoucement of a path to a certain destination.

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

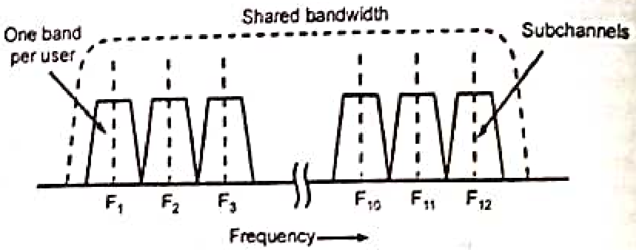
Time Division Multiple Access (TDMA) is a digital wireless telephony transmission technique. TDMA allocates each user a different time slot on a given frequency. TDMA divides each cellular channel into three time slots in order to increase the amount of data that can be carried.

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 indivi bands, each for use by a single user. Each individual band or channel is wide enough accommodate the signal spectra of the transmissions to be propagated. The data t transmitted is modulated on to each subcarrier, and all of them are linearly mi together.



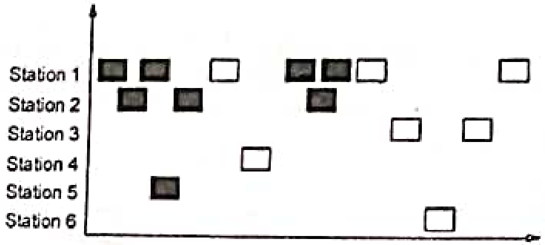
SDMA

Space-division multiple access (SDMA) is a channel access method based on creati parallel spatial pipes next to higher capacity pipes through spatial multiplexing and diversity, by which it is able to offer superior performance in radio multiple acce communication systems. In traditional mobile cellular network systems, the base stati has no information on the position of the mobile units within the cell and radiates t 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 ha data to transmit. Because the threat of data collision exists, each station must eith monitor its transmission on the rebroadcast or await an acknowledgment from t destination station. By comparing the transmitted packet with the received packet by the lack of an acknowledgement, the transmitting station can determine the succe of the transmitted packet. If the transmission was unsuccessful it is resent after random amount of time to reduce the probability of re-collision.

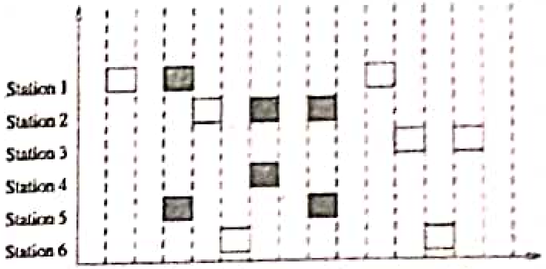


Time (shaded slots indicate collisions)

.Slotted Aloha

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

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.



Time (shaded slots indicate collisions)

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 access 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.

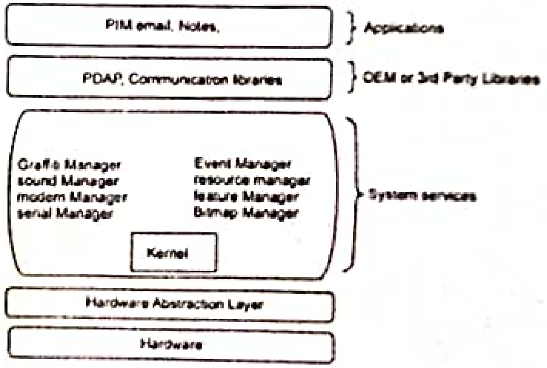


Fig. Architecture of Palm OS

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.

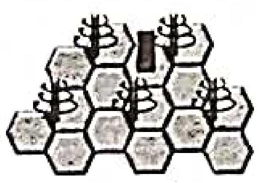
Time slicing and scheduling: This essentially allows the execution of several tasks according to their priority thereby supporting timers and time procedure. There are three types of triggers for task switching:

- 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.

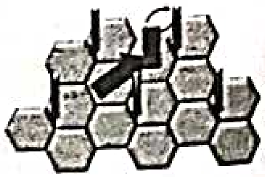
Differences between paging and Location Update

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



UNIT-III

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 well as bandwidth-intensive application such as multimedia and video conferencing
- Since TDMA technology separates users according to time, it ensures that the will be no interference from simultaneous transmissions.
- TDMA provides users with an extended battery life, since it transmits portion of the time during conversations.
- TDMA is the most cost effective technology to convert an analog system to dig

Disadvantages of TDMA

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

CDMA

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

Advantages of CDMA

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

Disadvantages of CDMA

- Channel pollution, where signals from too many cell sites are present in subscriber. s phone but none of them is dominant. When this situation arises, the q 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 technology because the network service information for the phone is put in the phone unlike GSM which uses SIM card for this.
- Limited variety of the handset, because at present the major mobile comp use GSM technology.

FDMA

FDMA is the process of dividing one channel or bandwidth into multiple indiv bands, each for use by a single user. Each individual band or channel is wide enou accommodate the signal spectra of the transmissions to be propagated. The data transmitted is modulated on to each subcarrier, and all of them are linearly 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 (e). 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 o base stations as the move through the WPBX radio coverage areas. Base stations a strategically located around the served area (both inside and/or outside) to prov contiguous radio coverage. WPBX systems can be completely, or partially, wirele between the system and the telephone instruments.

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

There are several different types of WPBX systems industry standard systems a proprietary systems. Some of the standard WPBX systems include digital enhan cordless telephone (DECT) and cordless telephony second generation (CT2). A WP radio system allows for voice or data communications on either an analog (typic FM) or digital radio channel. The radio channel typically allows multiple mo telephones to communicate on the same frequency at the same time by special codin 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 a that can be read through radio frequency interfaces. These transponders are comm known as RFID tags or simply tags. A RFID system comprises different functiona

(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 betwe~~n~~ Hidden and Exposed Terminal, Near and F Terminals.

Ans.A significant difference between wired and wireless LANs is the fact tha general a fully connected topology between the WLAN nodes cannot b assumed T 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 n Similarly, the range of C reaches B but not A. Also the range of B reaches both A a
- Now, the node A starts to send something to B and C doesn't receiv transmission.
- Now C also wants to send data to B and senses the carrier. As it senses i 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 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.

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