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

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

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

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

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

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

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

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

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

Handover scenarios in GSM systems

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

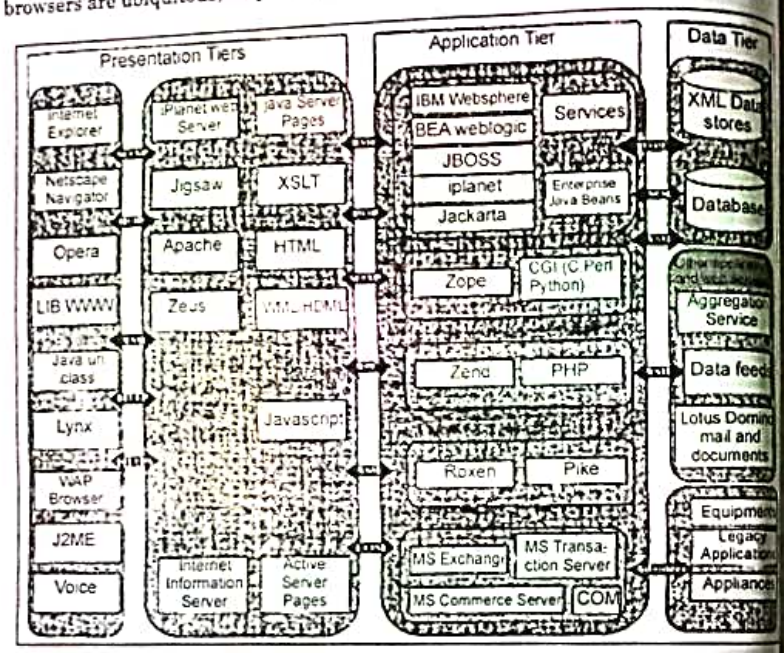


Fig. The mobile Computing Architecture

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 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.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 extraction, 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. (1

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.

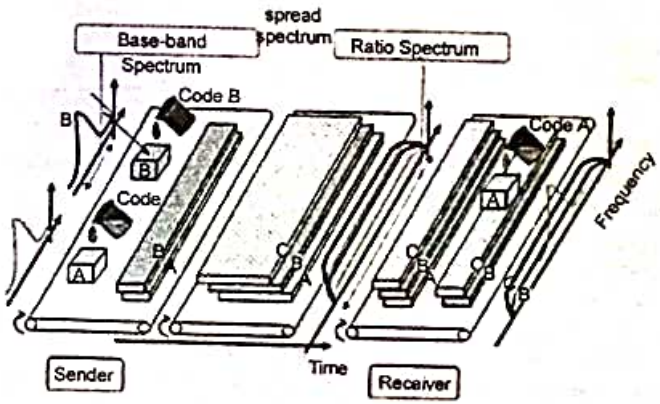
CDMA Overview: Code Division Multiple Access system is very different from time and frequency multiplexing. In this system, a user has access to the whole bandwidth for the entire duration. The basic principle is that different CDMA codes are used to distinguish among the different users.

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

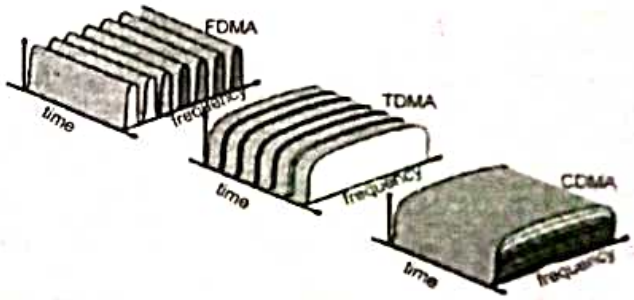
CDMA has a soft capacity. The greater the number of codes, the more the number of users. It has the following advantages

- 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 the (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.

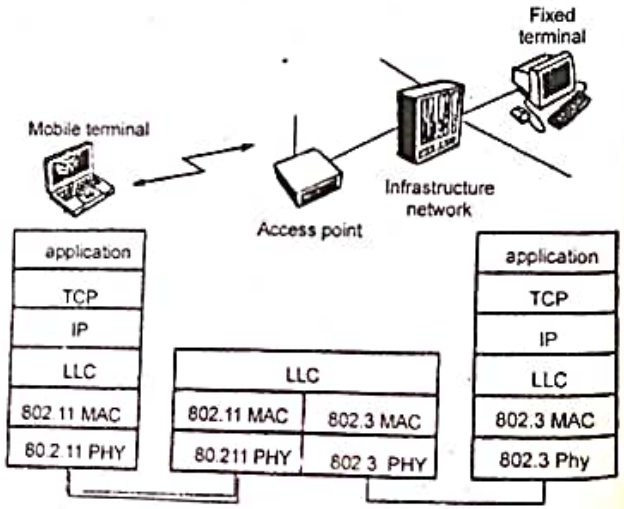


Fig. IEEE 802.11 protocol architecture and bridging

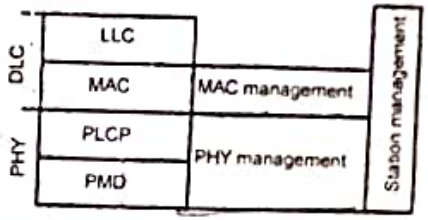


Fig. Detailed IEEE 802.11 protocol architecture and management

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.

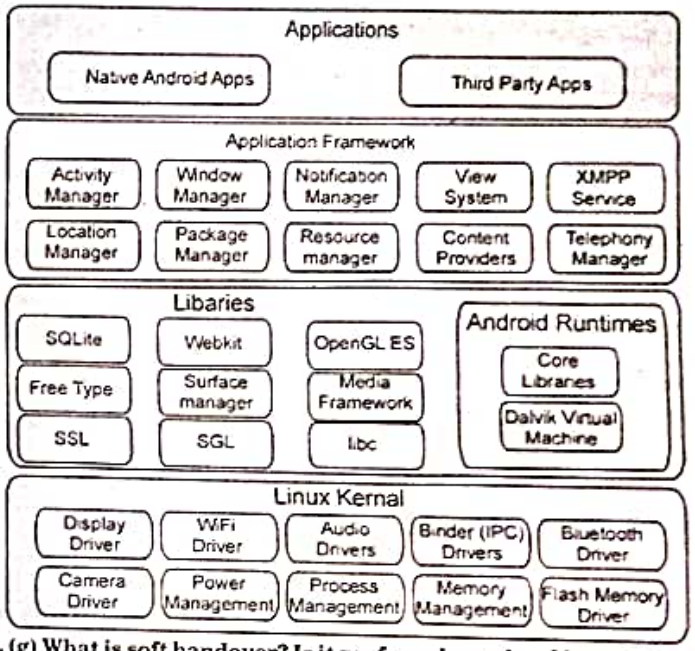
Like modern desktop operating systems, iOS uses a graphical user interface, or GUI. However, since it is a mobile operating system, iOS is designed around touchscreen input, rather than a keyboard and mouse.

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.

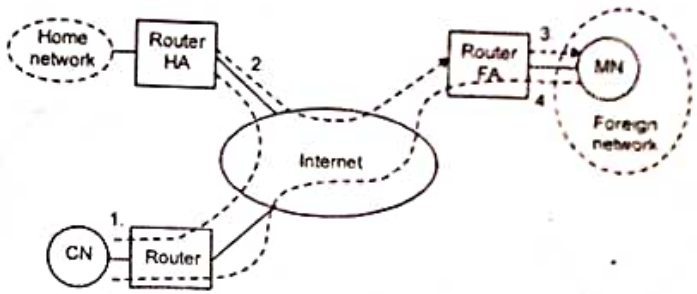
Challenges in ADHOC Networks:

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.

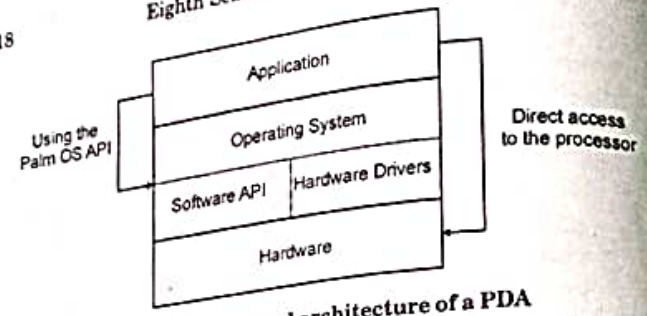
Finally the MN Receives the packet with the Source address as CN and Destination address as MN.

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.

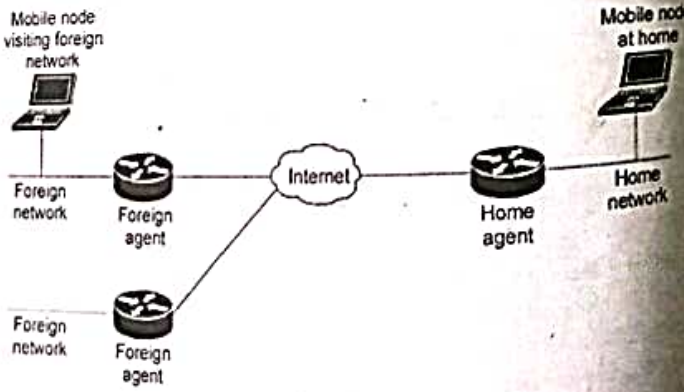


Typical layered architecture of a PDA

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. (8.5)

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.

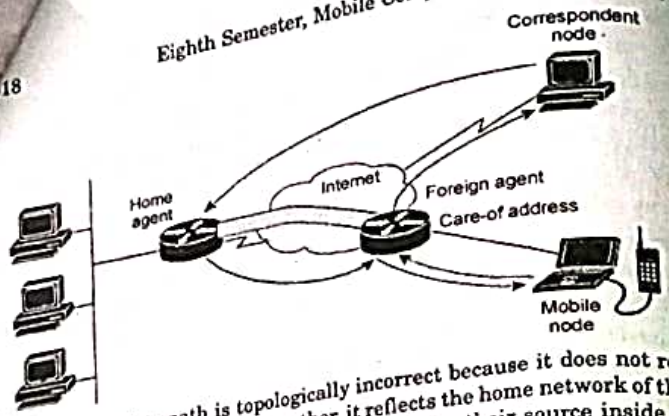
A foreign agent can be too busy to serve additional mobile nodes. However, a foreign agent must continue to send agent advertisements. This way, mobile nodes that are already registered with it will know that they have not moved out of range of the foreign agent and that the foreign agent has not failed.

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

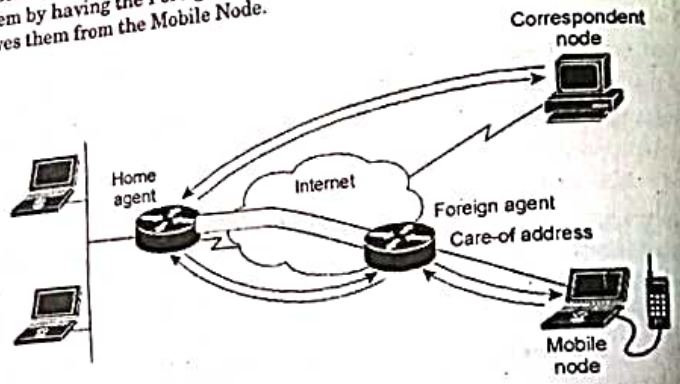
Ans. The Mobile Node sends packets using its home IP address, effectively maintaining the appearance that it is always on its home network. Even while the Mobile Node is roaming on foreign networks, its movements are transparent to correspondent nodes.

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 ,ig. where the bottom most layer interacts with the underlying hardware/hardw ire abstaction layer as the case maybe. This layer includes the kernel, memory, dev.ce, 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.

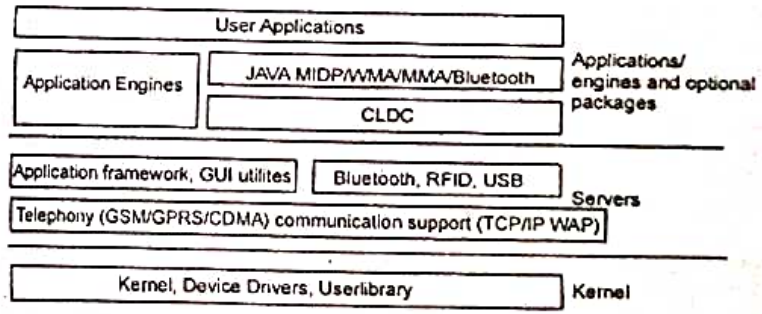


Fig. Symbian OS Architecture

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 mode switch. This mechanism is conceptually similar to that in UNIX/WindowsNT. The kernel 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 program Symbian OS.

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

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. wireless personal area networks. It has similar goals to Bluetooth in that it looks address wireless networking of portable and mobile computing devices such as 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 Network Standards Committee of the IEEE.

At the time of establishment, the 802.15 WPAN Working Group was aware of 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 the 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 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 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 specification takes into consideration coexistence requirements with 802.11 wireless local area network (WLAN) devices.

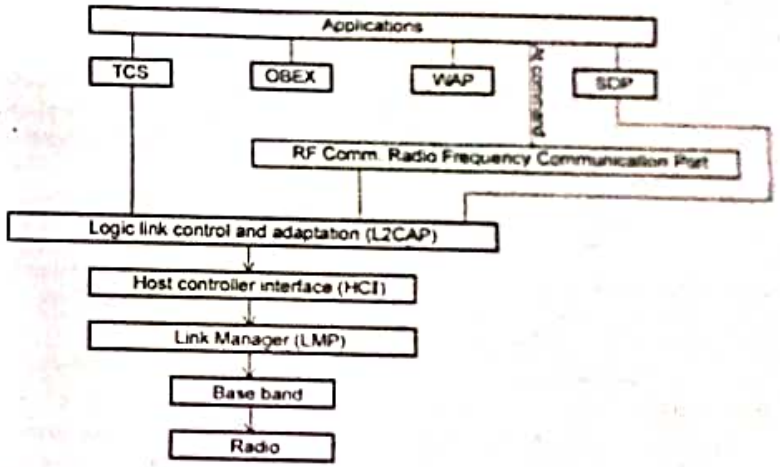
- **802.15 WPAN Task Group 2: Coexistence Mechanisms.** The 802.15 WPAN Task Group 2 (TG2) is developing the recommended practices to facilitate the coexistence of WPAN (802.15) and WLAN (802.11) technologies. Part of this task involves developing a coexistence model to quantify the mutual interference of a WPAN and a WLAN. If 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) WPAN. In addition to high data rates, 802.15.3 also has to provide a means for low-power, 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) hand'es 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.

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 the 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.

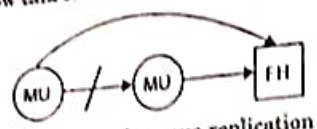
Q.6. (a) How the data replication in mobile computing is handled? Explain asynchronous replication. Differentiate between online data replication and offline data replication.

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

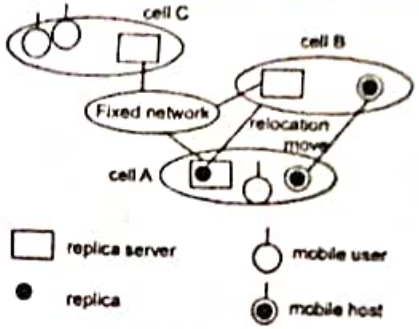
- Copy is closer to the writer than the reader

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

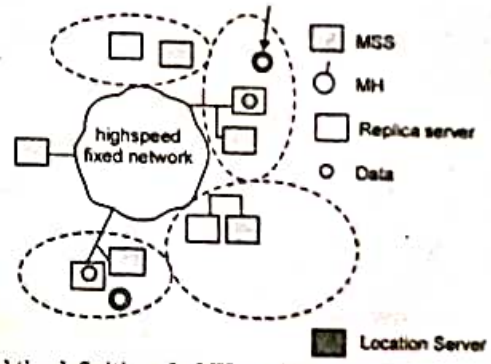
• Replica relocation is done as the MH moves from cell to cell

• 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)

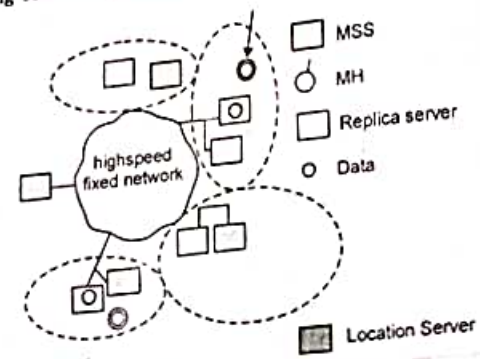
• Each MH has a replica of its data on FH called a replica server

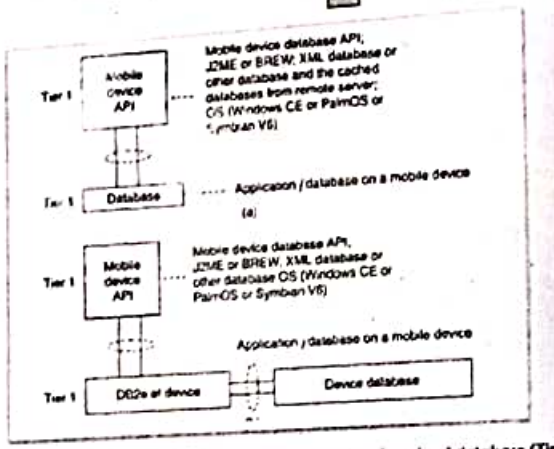
• Eacg MSS has a coordinator which receives transactions operations from MH or coordinators of other MSSs, and monitors their execution in the local replica server if the corresponding replicas exist

• 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)

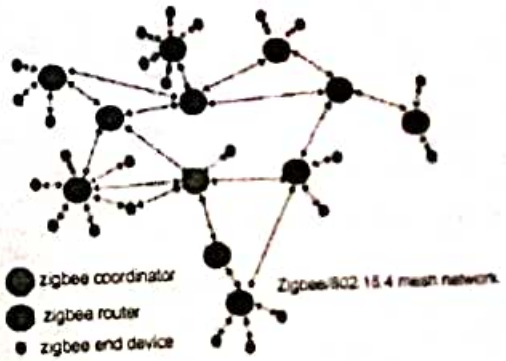
Ans. ZigBee is an open global standard for wireless technology designed to use low-power digital radio signals for personal area networks. ZigBee operates on the IEEE 802.15.4 specification and is used to create networks that require a low data transfer rate, energy efficiency and secure networking. 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.

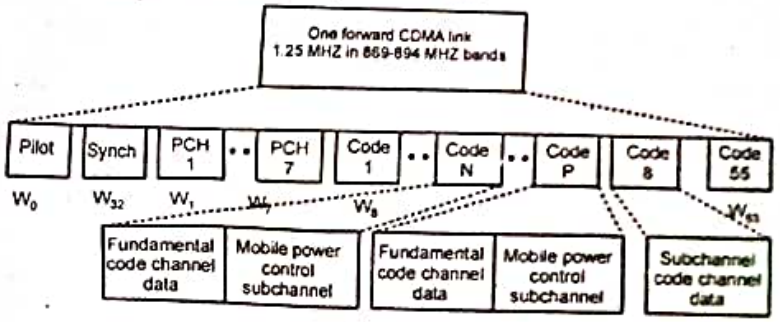


Fig. IS-95 Forward Channel

• 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:

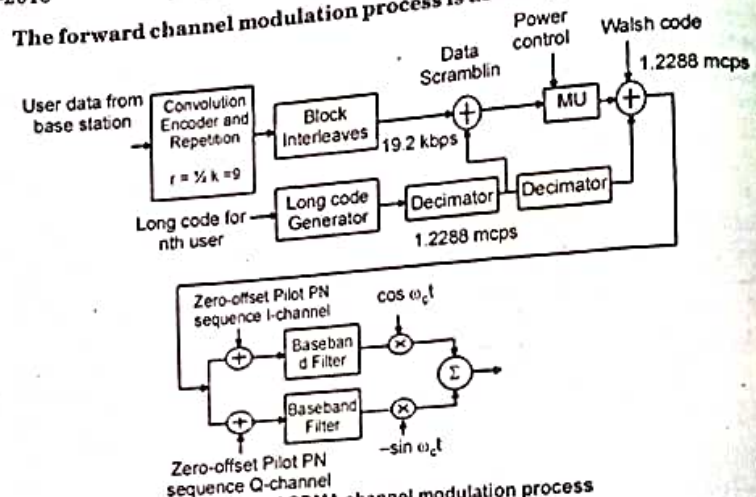


Fig. Forward CDMA channel modulation process

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 transmicsion 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.

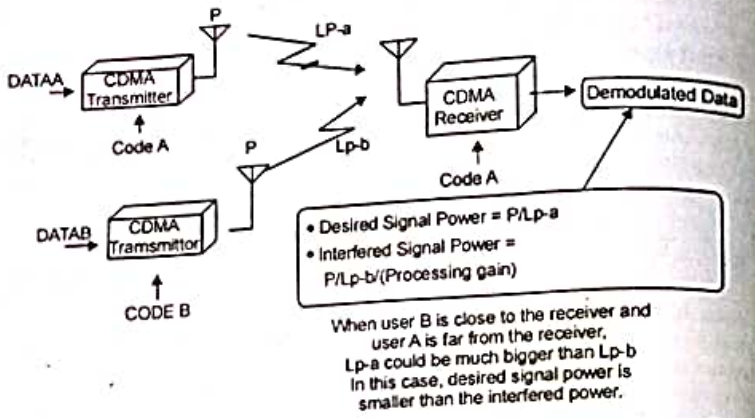
In general it is defined as ratio of signal to noise ratio (SNR) at output to the SNR at the input.

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

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.

FIRST TERM EXAMINATION [FEB. 2019]
EIGHTH SEMESTER [B.TECH]
MOBILE COMPUTING [ETIT–402]

Time : 1.5 hrs. **M.M. : 30**

Note: Q. 1. is compulsory. Attempt any two more questions from the rest.

Q.1. Explain the architecture of GPRS. **(10)**

Ans. GPRS architecture works on the same procedure like GSM network, but, has additional entities that allow packet data transmission. This data network overlaps a second-generation GSM network providing packet data transport at the rates from 9.6 to 171 kbps. Along with the packet data transport the GSM network accommodates multiple users to share the same air interface resources concurrently. Following is the GPRS Architecture diagram:

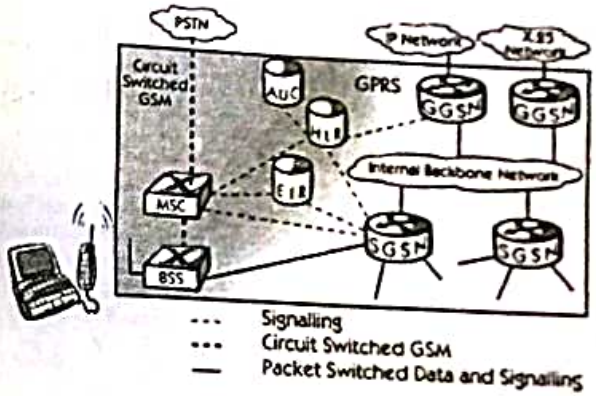


Fig. GPRS Architecture

GPRS attempts to reuse the existing GSM network elements as much as possible, but to effectively build a packet-based mobile cellular network, some new network elements, interfaces, and protocols for handling packet traffic are required.

GPRS Mobile Stations

New Mobile Stations (MS) are required to use GPRS services because existing GSM phones do not handle the enhanced air interface or packet data. A variety of MS can exist, including a high-speed version of current phones to support high-speed data access, a new PDA device with an embedded GSM phone, and PC cards for laptop computers. These mobile stations are backward compatible for making voice calls using GSM.

GPRS Base Station Subsystem

Each BSC requires the installation of one or more Packet Control Units (PCUs) and a software upgrade. The PCU provides a physical and logical data interface to the Base Station Subsystem (BSS) for packet data traffic. The BTS can also require a software upgrade but typically does not require hardware enhancements.

When either voice or data traffic is originated at the subscriber mobile, it is transported over the air interface to the BTS, and from the BTS to the BSC in the same way as a standard GSM call. However, at the output of the BSC, the traffic is separated,