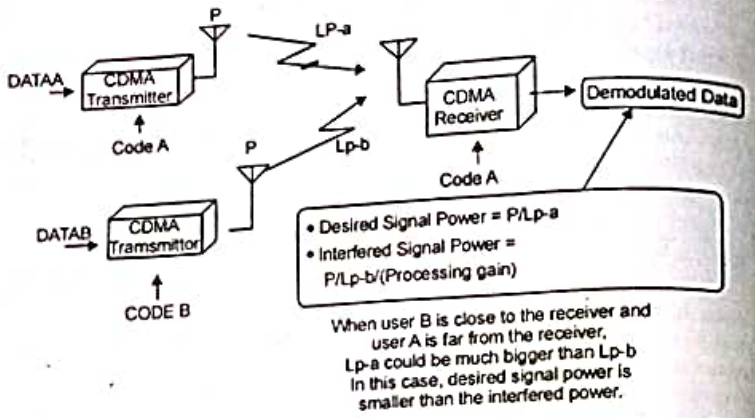


As shown in the illustration, user A is far away from the receiver and user B is close to the receiver, there will be big difference between desired signal power and interfered signal power. Desired signal power will be much higher than the interfered signal power and hence SN ratio of user A will be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

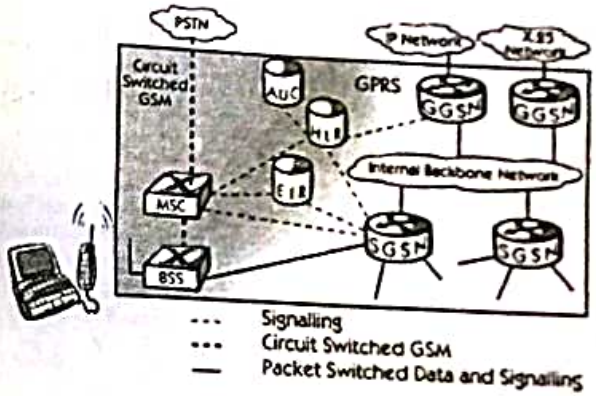


Fig. GPRS Architecture

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,

voice is sent to the Mobile Switching Center (MSC) per standard GSM, and data is sent to a new device called the SGSN via the PCU over a Frame Relay interface.

GPRS Support Nodes

Following two new components, called Gateway GPRS Support Nodes (GSNs) and, Serving GPRS Support Node (SGSN) are added:

Gateway GPRS Support Node (GGSN)

The Gateway GPRS Support Node acts as an interface and a router to external networks. It contains routing information for GPRS mobiles, which is used to tunnel packets through the IP based internal backbone to the correct Serving GPRS Support Node. The GGSN also collects charging information connected to the use of the external data networks and can act as a packet filter for incoming traffic.

Serving GPRS Support Node (SGSN)

The Serving GPRS Support Node is responsible for authentication of GPRS mobiles, registration of mobiles in the network, mobility management, and collecting information on chWTLS Primitivesarging for the use of the air interface.

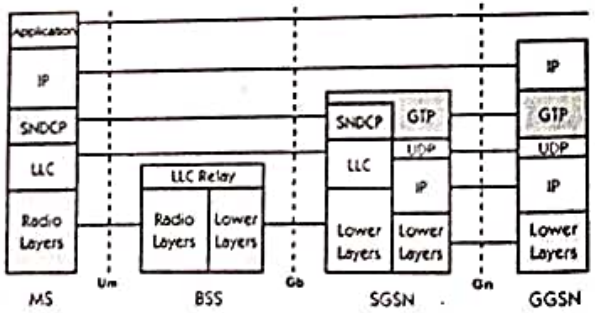
Internal Backbone

The internal backbone is an IP based network used to carry packets between different GSNs. Tunnelling is used between SGSNs and GGSNs, so the internal backbone does not need any information about domains outside the GPRS network. Signalling from a GSN to a MSC, HLR or EIR is done using SS7.

Routing Area

GPRS introduces the concept of a Routing Area. This concept is similar to Location Area in GSM, except that it generally contains fewer cells. Because routing areas are smaller than location areas, less radio resources are used While broadcasting a page message.

The flow of GPRS protocol stack and end-to-end message from MS to the GGSN is displayed in the below diagram. GTP is the protocol used between the SGSN and GGSN using the Gn interface. This is a Layer 3 tunneling protocol.



The process that takes place in the application looks like a normal IP sub-network for the users both inside and outside the network. The vital thing that needs attention is, the application communicates via standard IP, that is carried through the GPRS network and out through the gateway GPRS. The packets that are mobile between the GGSN and the SGSN use the GPRS tunneling protocol, this way the IP addresses located on the external side of the GPRS network do not have deal with the internal backbone. UDP and IP are run by GTP.

SubNetwork Dependent Convergence Protocol (SNDCP) and Logical Link Control (LLC) combination used in between the SGSN and the MS. The SNDCP flattens data to reduce the load on the radio channel. A safe logical link by encrypting packets is provided by LLC and the same LLC link is used as long as a mobile is under a single SGSN.

In case, the mobile moves to a new routing area that lies under a different SGSN, then, the old LLC link is removed and a new link is established with the new Serving GSN X.25. Services are provided by running X.25 on top of TCP/IP in the internal backbone.

Quality of Service (QoS) requirements of conventional mobile packet data applications are in assorted forms. The QoS is a vital feature of GPRS services as there are different QoS support requirements for assorted GPRS applications like realtime multimedia, web browsing, and e-mail transfer.

GPRS allows defining QoS profiles using the following parameters :

1. Service Precedence
2. Reliability
3. Delay and
4. Throughput

Q.2. What is handover? Why is it required? What are the handover scenarios in GSM? How the handover decisions take place depending on receiver signal strength? (10)

Ans. Refer to Q.1. First Term Examination 2018. (Page No. 1-2018)

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. Refer to Q.3. First Term Examination 2018. (Page No. 5-2018)

Q.4. Explain the terms: (10)

(i) ZigBee

Ans. ZigBee is a low-cast, low-power, wireless mesh network standard targeted at the wide development of long battery life devices in wireless control and monitoring applications. Zigbee devices have low latency, which further reduces average current.

ZigBee chips are typically integrated with radios and with microcontrollers that have between 60-256 KB of flash memory. ZigBee operates in the industrial, scientific and medical (ISM) radio bands: 2.4 GHz in most jurisdictions worldwide; 784 MHz in China, 868 MHz in Europe and 915 MHz in the USA and Australia. Data rates vary 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.

(ii) IrDA

Ans. 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.

(iii) WiMax

Ans. 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.

(iv) RFID

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

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

(ii) Mechanism to filter some of the data.

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

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

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

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

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

Q.1. Answer the following in brief :

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

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

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

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

$$K = q^2/3$$

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

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

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

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

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

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

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

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

Ans.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

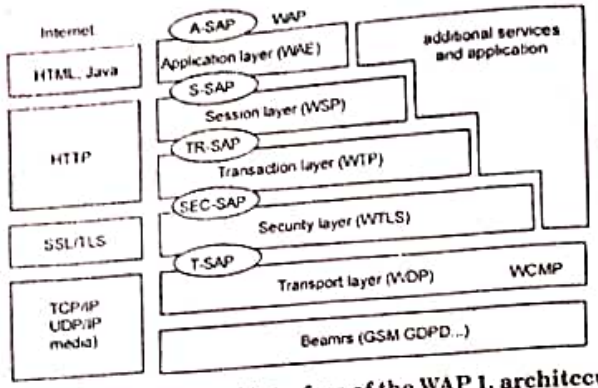


Fig.1. Components and interface of the WAP 1. architecure

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

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

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

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

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

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

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

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

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

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

Advantages of TDMA:

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

Disadvantages of TDMA

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

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

Advantages of CDMA

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

Disadvantages of CDMA

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

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

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

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

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

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

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

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

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

This results in wasting power on transmissions when there are no mobile units to reach, in addition to causing interference for adjacent cells using the same frequency, 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.

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

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

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

Key features (technology) of 1G system

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

Key features of 2G system

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

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

Key features of 3G system

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

Key features of 4G system

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

Key features of 5G technology

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

UNIT - I

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

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

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

Ans. Problems of data forwarding

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

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

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

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

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

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

OR

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

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

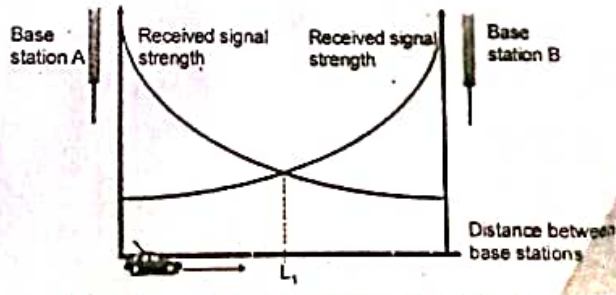
Q.3. (b) Consider the handoff procedure in GSM systems that is based on relative signal strength with threshold; that is, a mobile switches from one cell to another if? **(6)**

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

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

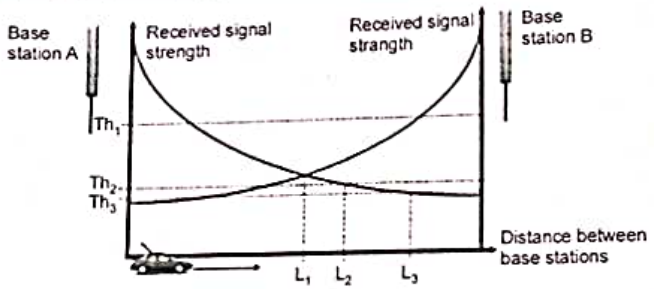
Ans. Relative Signal Strength (RSS)

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



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

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



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

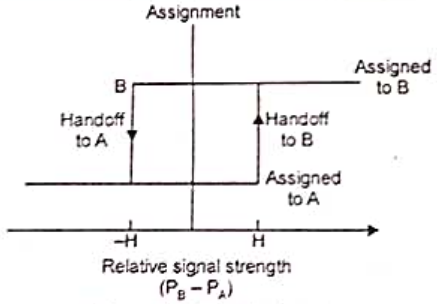
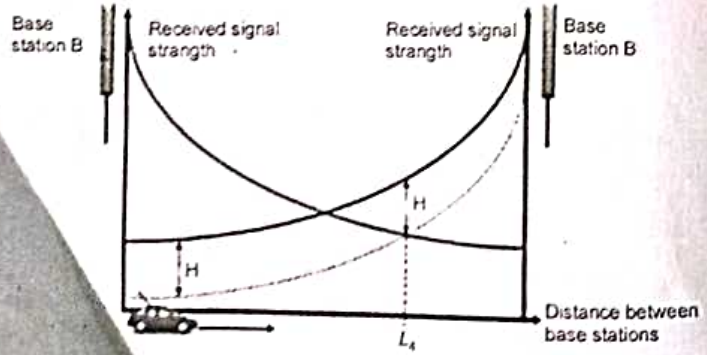
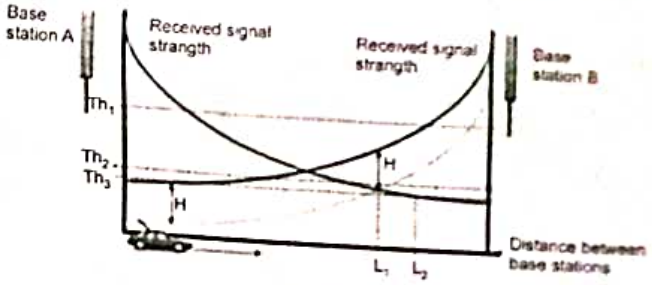


Fig. Hysteresis Mechanism



Relative Signal Strength with Threshold and Hysteresis (RSS-TH) Handover occurs only if the current signal level drops below a threshold, and the target base station is stronger than the current one by a hysteresis margin H. Handover occurs at L_1 if the threshold is either Th_1 or Th_2. Handover occurs at L_3, if the threshold is at Th_3. Scheme avoids the ping-pong effect and execution of handover if signal from the serving base station is still strong enough. Decreasing threshold in the RSS-HT new cause increase the probability of handoff and therefore the number of handoffs and the number of wrong handoff increase.



UNIT - II

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

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

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

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

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

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

(ii) Mechanism to filter some of the data

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

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

IrDA, ZigBee, RFID, WiMax

Refer of Q 4. First Term Examination 2019.

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

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

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

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

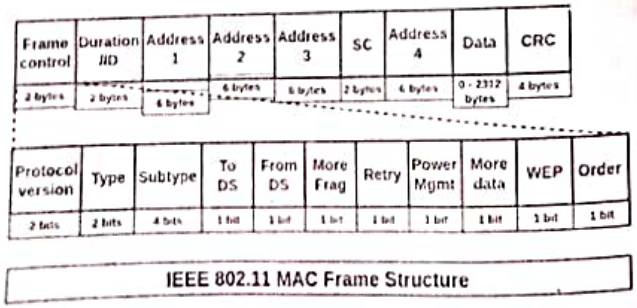
Fairness problem: In HiperLAN2 and Bluetooth medium access is controlled by an access point or master, respectively. Fairness then depends on these special nodes, which also decide upon the waiting time of a packet when it will be transmitted. In 802.11 the waiting time directly influences the chances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

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

OR

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

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



IEEE 802.11 MAC Frame Structure

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1. Spread Spectrum Radio:

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

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

Two types Spread Spectrum techniques,

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

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

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

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

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

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

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

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

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

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

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

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

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

UNIT-III

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

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

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

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

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

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

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

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

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

→ The send buffer size on the sending system

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

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

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

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

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

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

OR

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Basic TCP methodology:

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

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

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

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

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

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

UNIT-IV

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

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

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

Ans. Mobile application languages:

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

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

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

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

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

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

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

Mobile application toolkits

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

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

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

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

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

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

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

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

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

OR

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

Ans. Features of data replication:

Mobile environment

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

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

1. Every node has a unique ID and knows the IDS of its 1-hop neighbors.

2. A message sent by a node is received correctly within a finite time by all its 1-hop neighbors.

3. Network topology does not change during the execution.

Q.9. (b) Attempt any two parts: **(4 × 2 = 8)**

(i) User agent profile and Caching.

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

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

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

(ii) Data synchronization.

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

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

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

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

(iii) Mobility management.

Ans. Mobility management:

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