VIT Vidyalankar Institute of Technology

End Semester Examination (MU)

Evaluation of University Question Paper Solution Prepared by Faculty

Subject (Write in full) : Wireless Technology (Regular / KT)

Exam : May 20 18 / Nov. 20 _____ Exam Date : 29/05/2018 Q. Paper Code : 23491

Department : INFT Year : FE/SE/TE/BE/ME/MMS Semester : VII Scheme : CBSGS/CBGS

Handwritten Solution Prepared by : Prof. Neha Kudu

Name of the Subject Cluster : _____

Name of the Cluster Mentor / Assessor : Prof. Ranjana Gite.

1st Assessment :

Question No.	Marks Obtained						Total
1	(a) 08	(b) 10	(c)	(d)	(e)	(f)	18
2	(a) 10	(b) 10	(c)	(d)	(e)	(f)	20
3	(a) 07	(b) 10	(c)	(d)	(e)	(f)	17
4	(a) 5/5	(b) 5/5	(c) 10/10	(d)	(e)	(f)	20
5	(a) 10	(b) 10	(c)	(d)	(e)	(f)	20
6	(a) 10	(b) 08	(c) 08	(d) 10	(e)	(f)	36
Total (Out of marks)							131/140

Signature of Assessor / Cluster Mentor : R.R. Gite

2nd Assessment :

Question No.	Marks Obtained						Total
1	(a)	(b)	(c)	(d)	(e)	(f)	
2	(a)	(b)	(c)	(d)	(e)	(f)	
3	(a)	(b)	(c)	(d)	(e)	(f)	
4	(a)	(b)	(c)	(d)	(e)	(f)	
5	(a)	(b)	(c)	(d)	(e)	(f)	
6	(a)	(b)	(c)	(d)	(e)	(f)	
Total (Out of marks)							

Signature of Assessor / Cluster Mentor : _____

Scanned with CamScanner

Re-Assessor

Space for Marks	Question No.	START WRITING HERE

Q 1. Explain the concept of frequency reuse. Assume a cellular system of 32 cells with a cell radius of 1.6 km, a total spectrum allocation that supports 336 traffic channels and a reuse pattern of 7. Calculate the total service area covered with this configuration, the number of channels per cell. and total system capacity. Assume regular hexagonal topology.

- A group of radio channels are allocated a separate circular base station to be used within a small geographic area called as cell.
- The base stations in adjacent cells are assigned channel groups that contains completely different channels than the neighbouring
- The antennas located at base stations are designed to obtain the required coverage for specific cell.
- If the coverage area is limited to within the boundary of the cell then the same group of channels can cover different cells that are separated from each other by large distance
- The design method of selecting and allocating channel groups for all cellular base stations within a system is called as frequency reuse

diag

Scanned with CamScanner

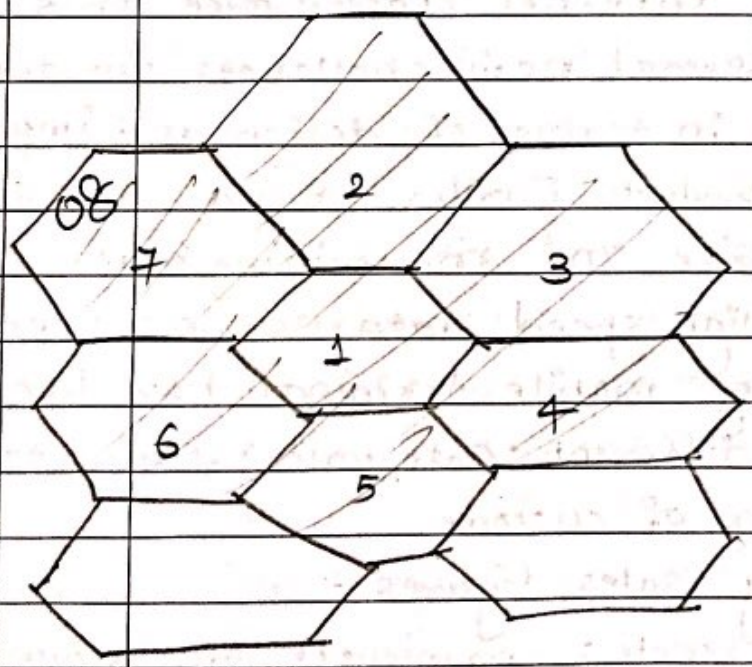
Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

- Total No of cells in cellular system = 32.
Radius of cell = 1.6 km.
No of traffic channels = 336.
Reuse pattern = 7

1) Total service area covered is
$\therefore 32 \times 1.6 = 51.2 km$

2) Calculate the number of channels per cell
$\therefore$ for N = 7, the available channels are
$\frac{336}{7} = 48$
$\therefore$ Total channels = 32×48
= 1536 channels.



cellular pattern for reuse factor

Scanned with CamScanner

Question No.

START WRITING HERE

Q1 (b) Detail the main factors of change in economics of wireless Technology.

- The integration of the internet and wireless networks for data transmission have led to developements in the wireless market for generation of large revenues.
- Wireless market refers to companies covering complete layers to provide services to users using vertical integration.
- The data oriented wireless networks will modify the economics of the wireless industry
- The main factors affected by the modification are :-

1. Terminal manufacturers :

i) Movement towards internet devices :

Earlier wireless Terminals have been currently substituted by internet enabled once. This change has brought several new challanges for terminal manufacturers in terms of design and implementation of its product. Earlier it was only focused for reducing size and minimizing battery power consumption. High speed data services needs to be corporated. Every mobile terminal have been categorize for different categories. which targets different section of customer

ii) Maximizing sales figures :-

The sales of mobile terminals will always increase as people will change their devices

Scanned with CamScanner

rks of n no.		Examiner	
		Moderator	
		Re-Assessor	

Question No.	START WRITING HERE

every few years or so to keep a pace with new services provided by mobile carriers. The best example is the upgrade of a general packet radio service (GPRS) phone from a global system for mobile communication (GSM) phone so that one can enjoy high data rates provided by GPRS. such an evolution towards mobile terminals having higher capabilities was a challangeing task because of the additional complications involved due to extra functionality offered.

2) Role played by government Agency :-

i) There are some regulatory bodies that play an important role in the economics of wireless industry and governs the telecommunication system in different countries. TRAI is the regulatory body setup to govern the telecom and broadcasting sectors in INDIA. This act enables TRAI to specify the conditions for the entry of new telecom service providers and terms and conditioning for license. The act also provides the standards for qualing of service and specifies the tariff policy

TRAI performs following Roles.

1) Protecting customer interests.
2) Monitoring the QoS.
3) Regulating Retail and wholesale Tarrifs.
4) Ensuring Transparency in service provision
5) Combating spam
6) Offering number portability

Scanned with CamScanner

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

- Governments get alot of money through spectrum licensing. They made profit by auctioning the 3G spectrum which created huge revenue. The high prices of 3G spectrum indicate the competition amongst the different mobile carriers.
- The spectrum licenses the carriers by limiting them with the type of service they can use over the spectrum. and time period for which spectrum can be used
- By increasing the number of competing mobile carriers in the spectrum the market growth rate will increase.

8) Infrastructure Manufactures :-

Increased market opportunities : with time new generations of wireless networks with some advancement is deployed. It is quite obvious that the infrastructure of the mobile market will also increase rapidly in size.

Increased Entry Barriers :- The next generations of wireless networks consists of increased complexity of infrastructure equipment. The companies that are already enjoying a major market share are benefitted by increasing demand for such equipment. Further with each new generation of wireless network, manufacturers of equipments for data networks are also likely to enter this market

Scanned with CamScanner

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

Mobile carriers :- Reducing prices in mobile carriers led to the competition between different mobile carriers and the reduced prices of fixed line services. mobile carriers had to adapt to the shift towards the wireless internet and explore different ways to gain profits out of it. This also meant spending too much money on procuring 3G licenses and setting up new infrastructure and equipment with the hope that investing in wireless internet will bring more money and popularity in subscribers Adopting wireless internet meant that mobile carriers would then have to play different roles to stay competitive

Portal Role :- Mobile subscribers have to create their portals for providing wireless Internet. Therefore mobile carriers having successful portals of the wired Internet had a major advantage In such a case mobile carriers had more chances of making profits from the knowledge and customer base of the fixed internet portal.

10/ Application service provider Role : with developement of new generations carriers have to create their ~~own portals~~ different new services. carriers are potential provider to these services. which contains revenue.

Content provider Role :- Imitating the world of the fixed internet, carriers have to create own content for portals.

Scanned with CamScanner

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

Bundled product:- customers preferred bundled product. Telecom operators such as those related to data service had a relative advantage.

Changing Traffic patterns:- The increase in the intra country mobility that too within the european union, has increased the traffic associated with roaming between countries. In small countries, traffic resulting from roaming constituted more than half of traffic exchanged.

Different situation to every country:

It was difficult to comment on successful carriers as the factors such as large distance, Lack of spectrum, high competition, huge subscriber base, Internet popularity, Divergence of standard influenced telecommunications scenario and society in every country is different.

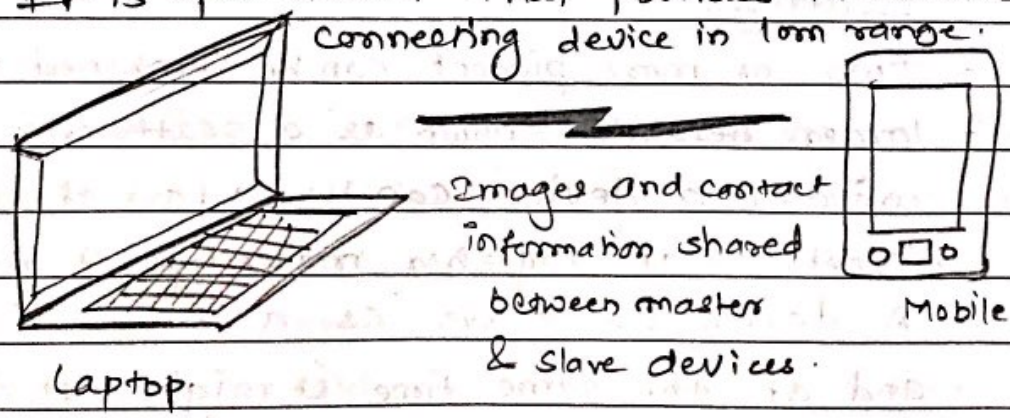
Scanned with CamScanner

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

Q 2 (a) Define Piconet and scatternet. Explain Bluetooth protocol stack structure.

- In WPAN, Piconet consists of one master and at least one or more slave devices. The only master device in the piconet control the transmis and the maximum number of slave devices that can be present in one piconet are seven.
- When devices come in each other's proximity a master device is elected with which the slave devices can communicate.
- Spread spectrum techniques such as FHSS are used within a piconet for efficiency and scheduling algorithm such as round robin is used for switching between the slaves.
- Moreover it is not necessary that if a device is once elected as a master, then it will always remain a master device. Different devices in a piconet can adopt the role of a master at different point of time. Figure shows basic piconet that consists of one master and one slave device
- It is open started that provides an ad-hoc way for connecting device in low range.



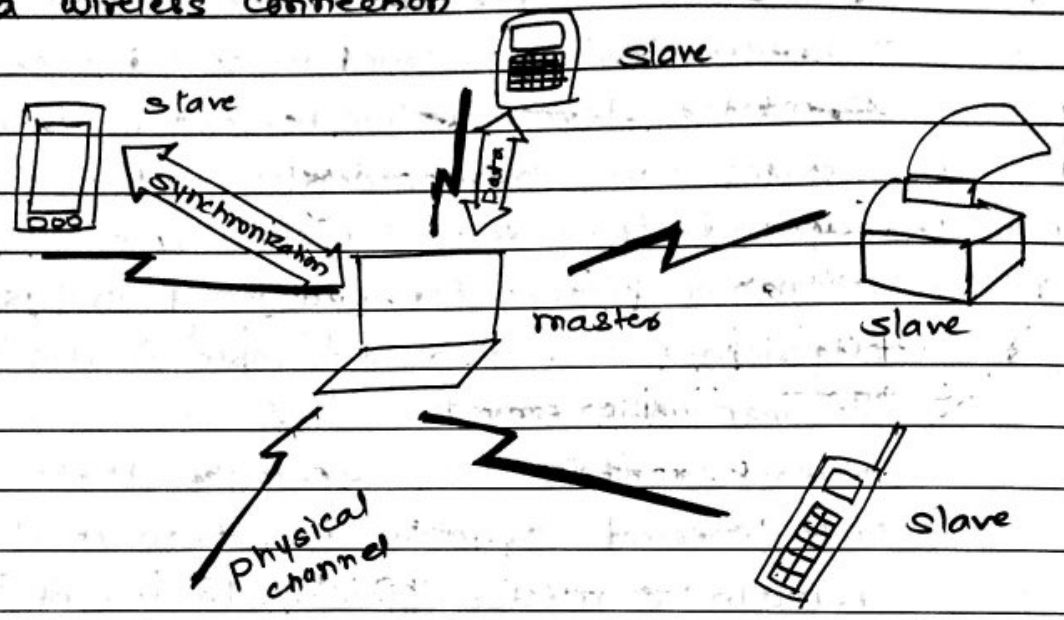
piconet (Basic structure).

Scanned with CamScanner

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

In the example shown in figure, when the master (laptop) and slave (mobile phones) devices come in each other's proximity, the application software operating in a laptop establishes a connection with the mobile phones. Data such as image, music files, contact information can be exchanged using such a wireless connection.



Master device and numbers of slaves controlled by master

Scatternet

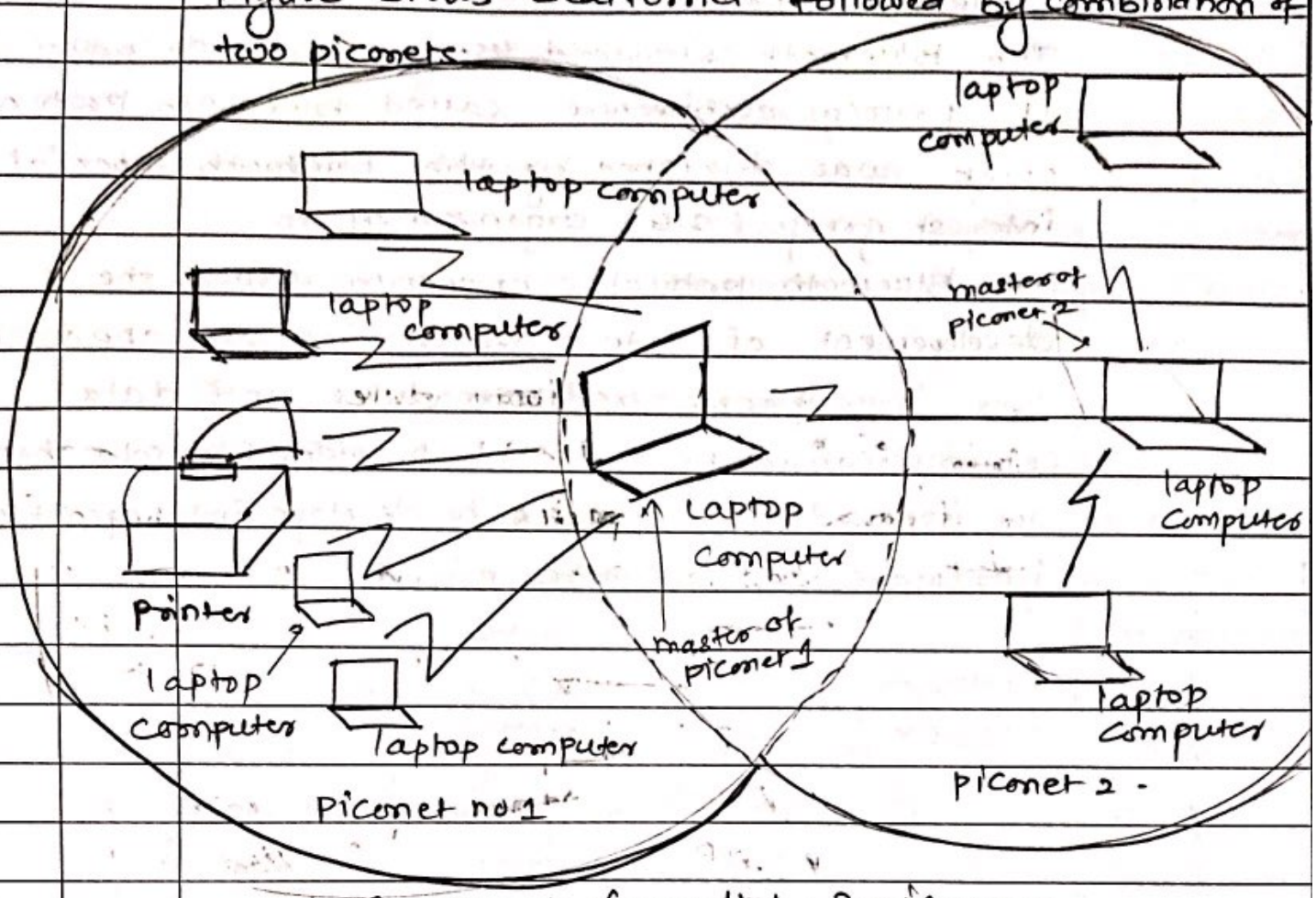
- Two or more piconet can be combined to form a larger network known as a scatternet. In other words, a device can be a part of two or more piconets that together make up a scatternet
- A device can serve as a master in one piconet and at the same time it might act as a master device in more than one piconet at the same time.

Scanned with CamScanner

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

Figure shows scatternet followed by combination of two piconets.



Scatternet formed by 2 piconets

- In addition to 7 slaves, there can be upto 255 parked nodes in the net that can only respond to a becon signal from the master.
- Slaves are dumb devices to do the task and master tells them to do.
- It is a TDM system with the master controlling the clock and determining which slave gets to communicate in which time slot.
- All the communication is between the master and slave and not between the slaves.

Scanned with CamScanner

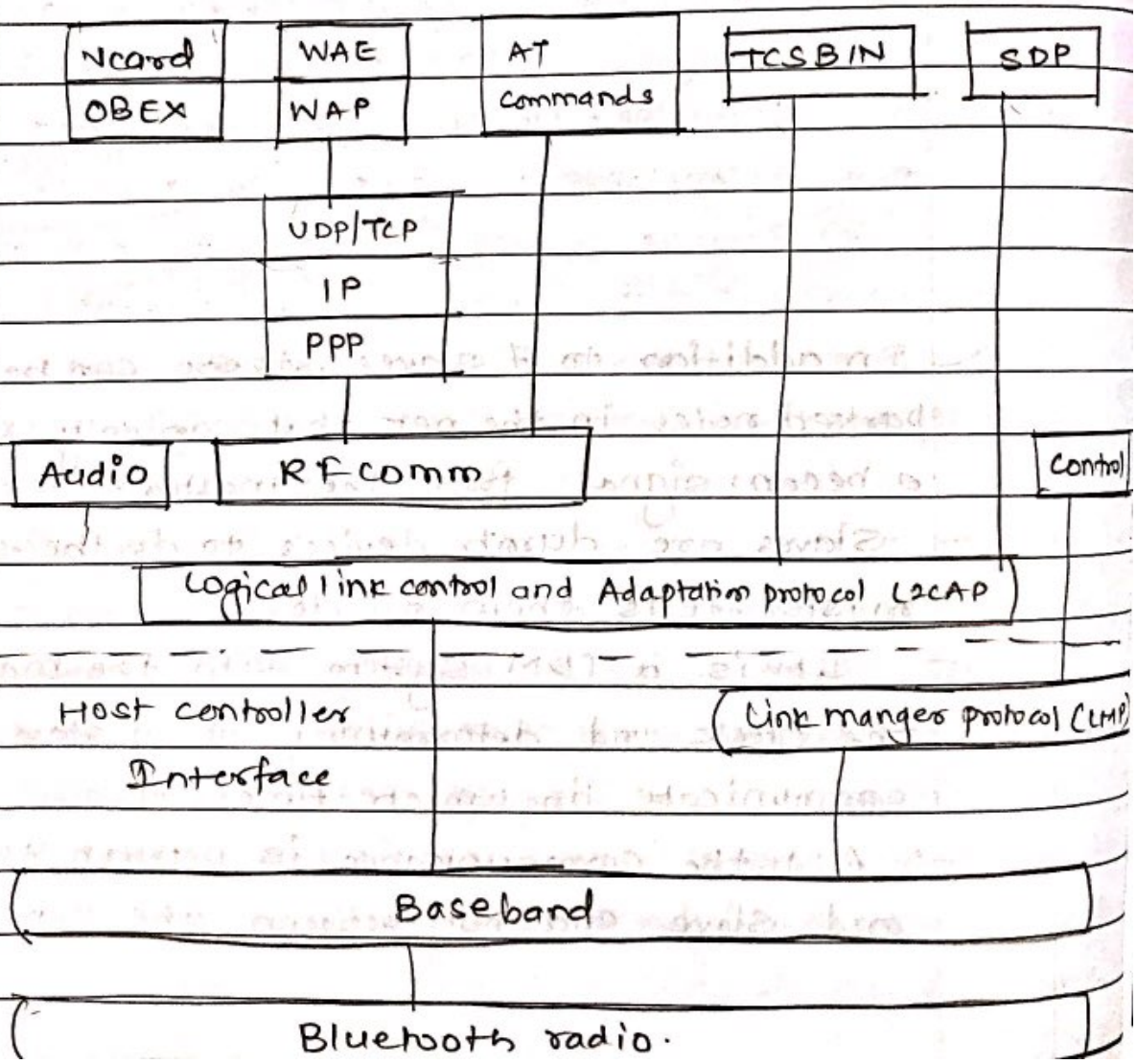
Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

Bluetooth Protocol stack :-

The Bluetooth standard uses a variety of protocols. Its protocol architecture, called bluetooth protocol stack. was developed by the bluetooth special interest group (SIG) organization.

The Bluetooth protocol architecture allows the developement of interactive services and applications over interoperable radio modules and data communications protocol. It provides protocols that are followed by companies to develope interoperable hardware and software



Scanned with CamScanner

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

1) Bluetooth core protocols layer : This layer is always needed by bluetooth devices while the rest of the layers are required only when needed. It consists of following protocols.

- Baseband (BB) : BB and link layer control creates a physical radio frequency link between different bluetooth devices thereby creating a piconet. In Bluetooth core protocols, the baseband layer handles the lower level operations at the bit and packet levels. Some examples of such operations are forward Error correction (FEC), operations, encryption, cyclic redundancy check (CRC) calculations and Automatic repeat Request (ARQ) protocol. The bluetooth radio frequency system is a frequency hopping spread spectrum system and therefore packets are sent in specific time slots. It facilitates two types of physical links : synchronous Connection oriented and Asynchronous connection less (ACL). synchronous Connection oriented packets are used for the transmission of audio only or a combination of audio and data whereas ACL packets are used for transmitting data only

- Link manager protocol (LMP) : This protocol is responsible for configuring a link between bluetooth devices. It handles connection establishment and release, authentication, traffic scheduling and power management link tasks.

Scanned with CamScanner

Space for Marks	Question No.	START WRITING HERE

• Logic link control and Adaptation layer (L2CAP):
This protocol adjusts upper layer protocols over the baseband. It works in parallel with LMP. (L2CAP) offers various services to the upper layer if the payload data is not transmitted to the LMP messages.
This protocol offers both connection oriented and connectionless data services to the upper layer protocols. It also offers protocol multiplexing, segmentation and so on. It allows protocols and applications to send and receive L2CAP data packets upto 64 kilobytes in length. It also handles the tasks of mixing higher layer protocols with the baseband layer protocols and segmentation and Reassembly (SAR) of large data packets.

• service discovery protocol (SDP):
SDP offers discovery services to bluetooth devices. These services act as the basis for all the usage models. with the help of this protocol, information relating to the device and services can be queried. It also helps in establishing connection between multiple bluetooth devices.

2) Cable Replacement protocol layer
This layer specifies call control signalling and establishes data calls between bluetooth devices. It consists of the following protocols.

Scanned with CamScanner

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

• Radio frequency communication (RFCOMM) : This protocol is an emulation protocol, which is based on European Telecommunication standardization Institute (ETSI) 0.7.10 specification. It emulates RS-232 control and offers transport capabilities to upper layer services

3) Telephony controls protocol layer : It contains the following protocol.

• Telephony control specification Binary (TCS BIN) This protocol specifies the call control signalling for configuring speech and data calls between different bluetooth devices. It also provides information on different procedures to be undertaken for managing mobility to handle TCS device.

• Attention sequence (AT) : TCS BIN defines some AT commands. These commands specify the procedure to control a mobile phone or modem

4) Adopted Protocols layer : The protocols provided in this layer are reused for various purposes. This layer consists of following protocols

• Point to point protocol (PPP) : This protocol is used to establish point to point connection. with the help of this protocol, IP Packets are sent or received from the PPP layer and placed on the LAN.

• User datagram protocol (UDP) / Transmit control Protocol (TCP) / Internet Protocol (IP) : TCP/IP is used as a communication Protocol across the internet

Scanned with CamScanner

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

The use of TCP/IP stack can be found in several devices, such as mobile handsets, printers and so on. UDP/IP is also used as WAP transport protocol. TCP refers to a connection oriented reliable protocol. TCP sends data in the form of packets of data or IP datagrams. TCP specifies the procedure to convert data streams into data packets, assemble them in a proper sequence and sends requests to replace damaged packets. As the packets travel through different paths to reach the destination using the internet they reach the destination at different times and not in a specific order. Therefore all these packets are maintained temporarily till the arrival of the last packet. later they are arran in proper sequence. If a packet is damaged, it is discarded. IP delivers datagrams from one network to another with the help of routers. A distinct IP address is given to each device in the autonomous system (AS). TCP guarantees the delivery of data packets whereas UDP simply transfers messages to IP. As IP is not reliable, there is no guarantee that the data packets will be delivered. UDP is useful in a case of quick database lookups.

- Object Exchange Protocol (OBEX): Infrared Data association (IrDA) developed a session protocol called OBEX to exchange objects. A client server model is used by OBEX and helps a reliable data transfer. OBEX offers a model to represent objects and applications

Scanned with CamScanner

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

• Wireless Application protocol (WAP): Using WAP in Bluetooth helps in creating application gateways. These gateways can act as a intermediary between WAP servers and other PC applications WAP helps in facilitating remote control and data retrieval functions from PC to headset. WAP is used to reuse the upper layer software application.

• Vcard and V calender: VCard and V calender are specifications created by the versit consortium and managed by the internet mail. Consortium. These specifications helps in specifying formats for electronic business card and calendar. Both these specifications define the format using which data is sent. with the help of the Vcard and Vcalendar supported formats, the SIG will help in exchanging personal information. Internet mail consortium makes these specifications available. They are further developed by the internet Engineering Task force (IETF).

• wireless Application Environment (WAE): WAE follows the web content delivery model. All the WAP applications reside within WAE.

Scanned with CamScanner

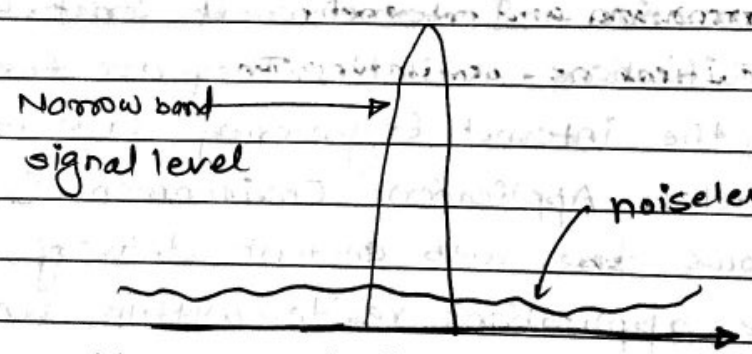
Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

Q 2 (b) Why is the concept of spread spectrum is important? Briefly explain FHSS and DSSS concept.

Importance of spread spectrum

In a wireless system, communicating devices are designed a bandwidth for communication. Bandwidth is a range of electromagnetic frequencies used for transmitting message. However the medium of transmission is used by wireless devices is air or free space. Therefore securing becomes a major concern in a wireless system. The data released in free space in the form of electromagnetic radiation can be easily intercepted and jammed. Such a signal represents a narrow band signal. Figure shows a narrow band signal



Narrow band signal that can be easily intercepted

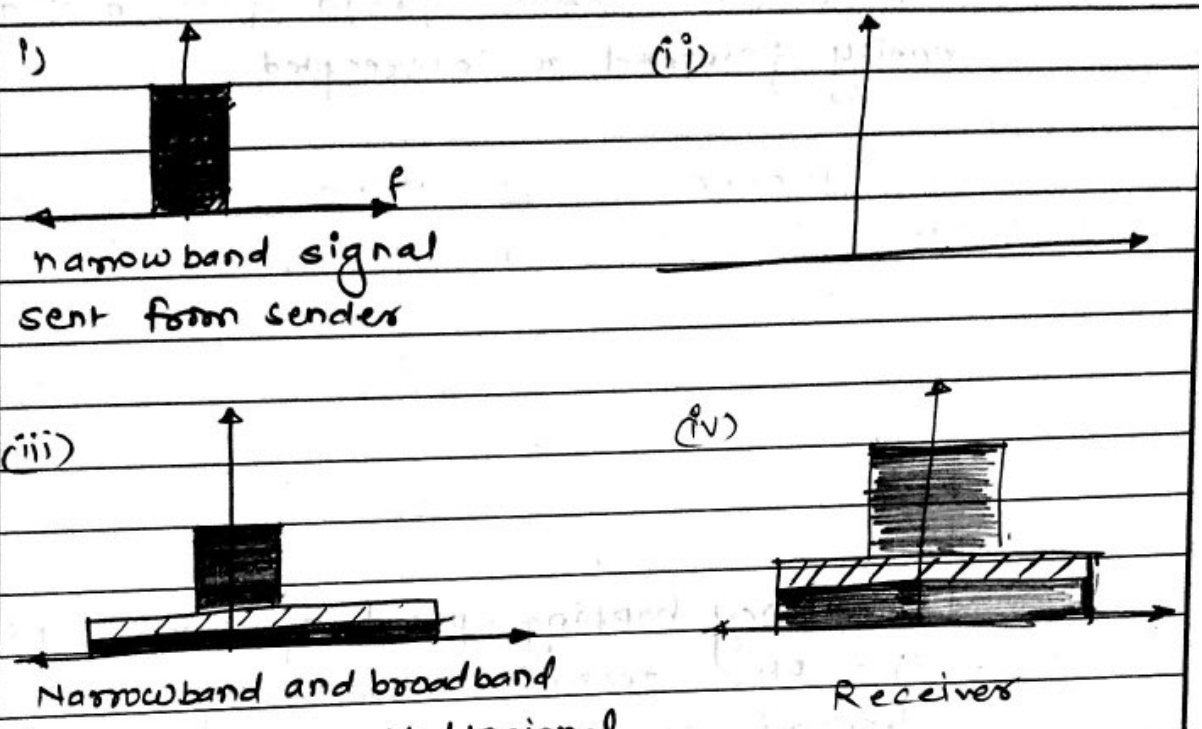
To solve these issues, a technique known as spread spectrum is used. This technique works by allocating a bandwidth that is larger in comparison to the actual bandwidth that is required by a source to transmit a message and at the same time it also retains the same signal power. The

Scanned with CamScanner

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

benefit of using spread spectrum is that it eliminates the problem of narrowband interference. Fig shows the concept of spread spectrum spreading and despreading

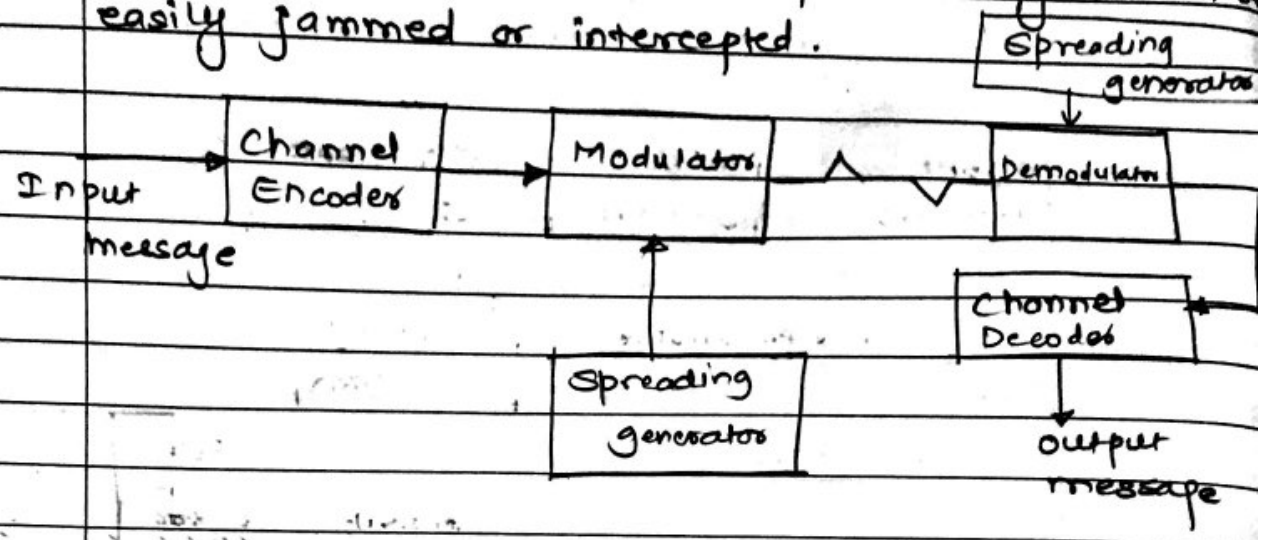


Scanned with CamScanner

Question no.		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

A Coding technique is used to spread the bandwidth of message signal. The message is spreaded over a larger bandwidth appears more like a noise as its actual pattern remains hidden during transmission. Due to this reason, spread spectrum signal cant be easily jammed or intercepted.



- Frequency hopping spread spectrum (FHSS):
- The FHSS technique works by changing the transmission frequency at a very high rate. The frequent change in carrier frequency is termed as hopping.
- In this method, the bandwidth is divided into several paths known as frequency channels while a message is transmitted from source to destination, several hope are made from one frequency channel to another.
- Although the hopping patterns appears to be random; it is actually generated by the following certain Encryption algorithm to which the transmitter and receiver have agreed. Such a pattern that

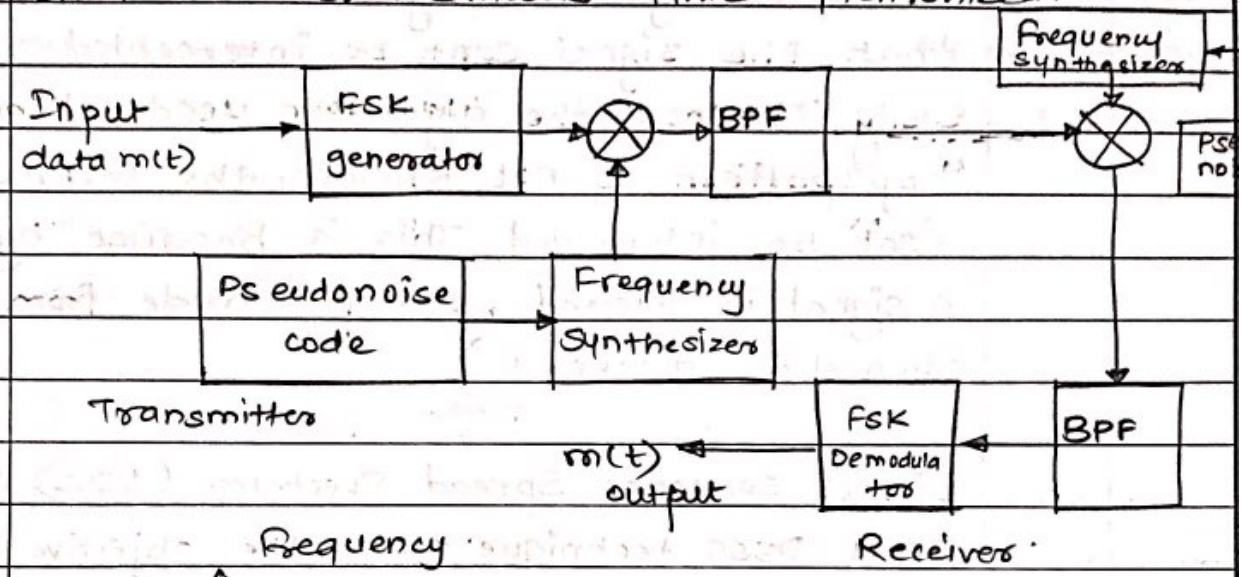
Scanned with CamScanner

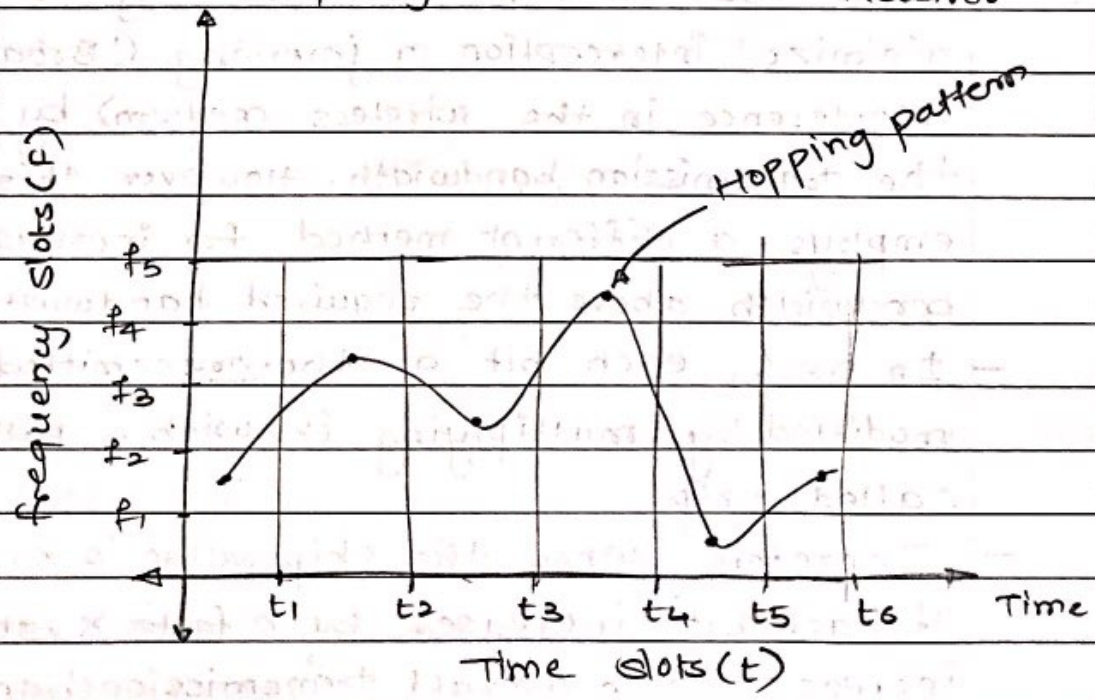
Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

appears to be random but is generated using some mathematical or logical construct is known as pseudo-random pattern.

- Following an agreed upon algorithm to generate a hop pattern is essential so that the transmitter and receiver remains time synchronized.





FHSS Frequency Hopping

Scanned with CamScanner

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

In the preceding figure, it can be seen that a frequency band splits into five frequency channels namely F1, F2, F3, F4 and F5. A message jump to different frequency channels at the time inte t1, t2, t3 and so on till the time interval t6. The advantage of using the FHSS technique is that the signal cant be intercepted or jammed easily. Unless the algorithm used for generating hop pattern is not known, the communication can't be intercepted. This is because by the tim a signal is detected, a hop is made from one frequ channel to another.

Direct sequence Spread Spectrum (DSSS):

- In a DSSS technique also, the objective is to minimize interception or jamming (Broadcasting interference in the wireless medium) by increasin the transmission bandwidth. However this technique employs a different method for increasing the bandwidth above the required bandwidth
- In DSSS, each bit of the transmitted signal modified by multiplying it with a pattern of val called chip.
- Therefore, when the chip value is x, the band of each bit increases by a factor x, thereby increasing the overall transmission bandwidth b a multiple of x.
- A mathematical algorithm (spread code) is app

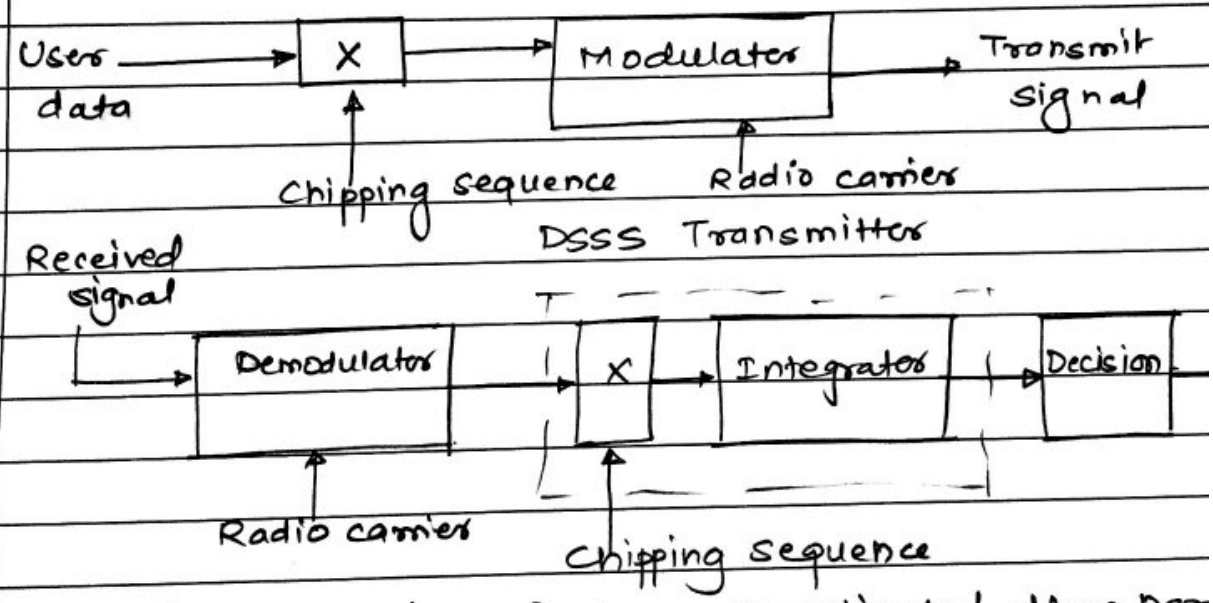
Scanned with CamScanner

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

to generate a pseudo random chip pattern consisting of a number of chip values. The generated pattern is large enough to spread the signal in such a way that it appears like noise signal, which becomes difficult to detect while transmission.

- In DSSS transmitter, the first step is to spread the user data with the help of chipping sequence. The spread signal is later modulated using radio carrier. The signal is then transferred to the carrier frequency by the radio carrier. Finally the signal is transmitted further.



The DSSS receiver is more complicated than DSSS transmitter. The receiver simply does the inverse function of two transmitter modulation steps. However additional methods are required to rebuild the original data in case of noise and multipath propagation. The first step in case of receiver involved demodulation of the signal received. This is done by

Scanned with CamScanner

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE
		using the same carrier as the transmitter. that reverses the modulation. This leads to a signal having the same bandwidth as compared to the original spread spectrum signal. The next step is difficult for DSSS receivers as they must know in advance the original chipping sequence

Scanned with CamScanner

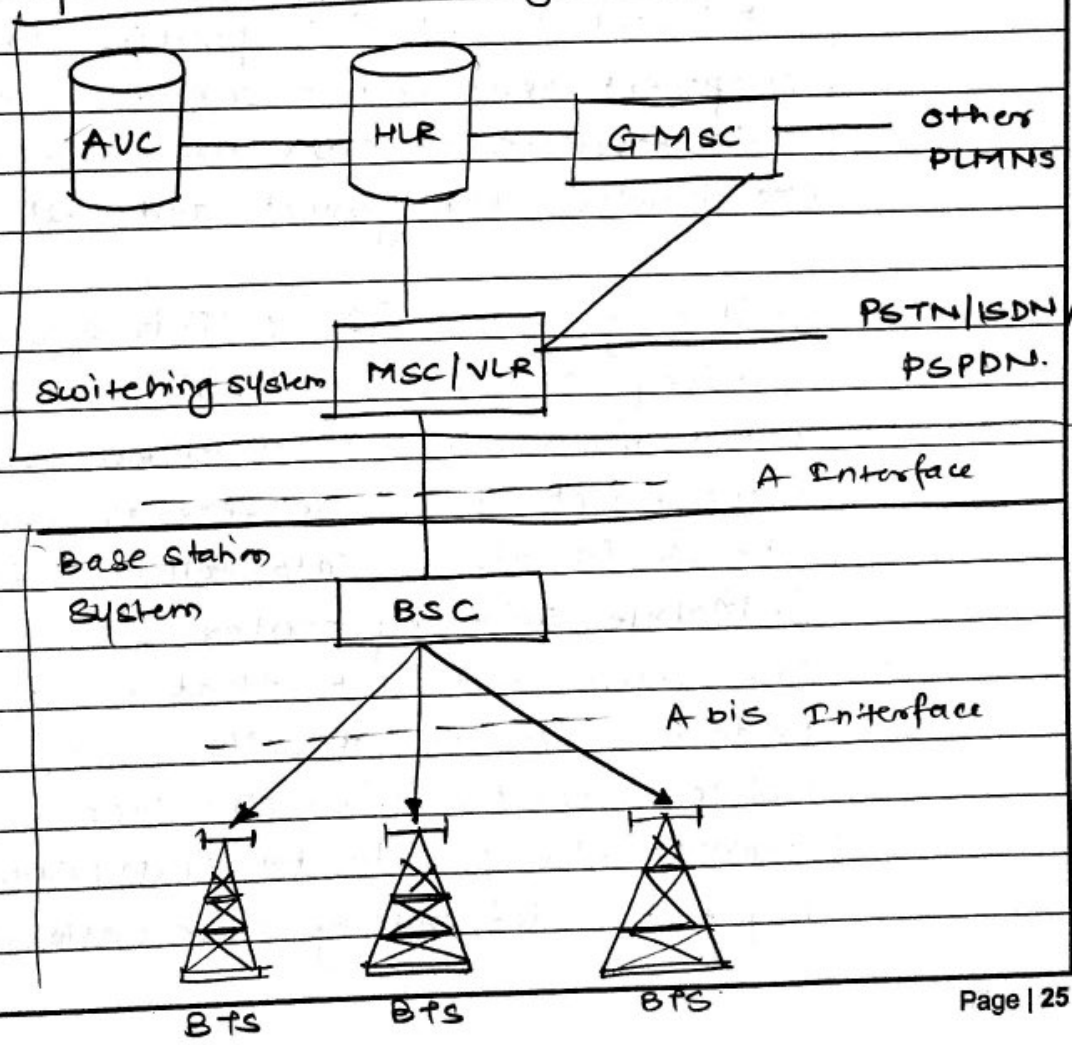
Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

Q3 (a) Explain GSM architecture. and Explain how authentication and Encryption is provided in GSM?

- The GSM network consists of various functional entities, whose functions and interfaces are specified
- The GSM architecture consists of three major subsystem that interact between themselves with the users through some network interfaces. The subsystems are:

① Base station subsystem (BSS)
② Network and switching subsystem (NSS)
③ Operation support subsystem (OSS).



Scanned with CamScanner

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

BS system (BS): The role of a BSS is to handle traffic between a mobile phone and the network switching system. It consists of the following functional units:

1) Base Transceivor station (BTS): Specifies the radio equipment that facilitates wireless communication between a mobile and a network. It handles and serves one mobile at a time. This radio equipment has various parts, which includes Transceiver (TRX), Power amplifier (PA), combiner, duplexer, antenna alarm extension system, control function, Baseband receiver Unit (BBXX)

2) BS controller (BSC): Specifies a mobile network component that controls a number of BTs. The main functions of a BSC are radio network management BTS handover management and call setup.

Switching system (SS): This system performs the switching of calls between a mobile and other fixed or mobile network users as well as the management of mobile services such as authentication. The SS is divided into following functional units

① Mobile switching center (MSC): specifies the main component that is actually used to perform switching of calls among different mobile network users. The MSC is the primary service delivery node for GSM/CDMA that is responsible for routing voice calls and SMS as

Scanned with CamScanner

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

well as other services such as conference calls, fax, circuit switched data. It is identified with the help of an assigned unique ID. An MSC also manages mobile services such as registration, authentication, location updating, handovers, call routing to a roaming subscriber.

(2) Visitor location register (VLR): specifies a database that temporarily stores information about subscribers needed by the MSC for handling visited subscribers. A VLR is always associated with an MSC. It also stores data about a mobile station from the Home location register (HLR) in case the mobile station is roaming in a new MSC area.

(3) HLR: Specifies a database that stores subscribers information specific to a particular public land mobile network (PLMN). The subscriber information can include a subscriber service profile, location information and services assigned to the subscriber.

(4) Authentication center (AUC): Includes a database containing a secret key that is maintained in each user's SIM card. This secret key is used for the authentication and encoding of radio channel. AUC safeguards network operators from different types of mobile network's fraudlent activities.

(5) Equipment Identity Register (EIR): Refers to a database that stores a record of mobile station equipment on the network, while its international

Scanned with CamScanner

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

Mobile equipment identity (IMEI) identifies each mobile station. (MS)

MS: ~~Each~~ This unit contains physical equipment used by subscribers to access a network. It is composed of the following two functional entities.

- Mobile Equipment (ME): Specifies a device containing three functional blocks: Terminal equipment (TE), Mobile terminal (MT), Termin Adapter (TA). Service oriented functions such as a fax machine are performed by the TE. however functions concerned with the operation of the GSM systems are not hacked by it. The transmission and reception of information through the GSM radio interface are done by the MT.
- Subscriber Identity Module (SIM): Specifies a small sized card, such as credit card by a subscriber to personalize the ME. If a valid SIM is inserted in a mobile phone, the user would be able to receive or make calls using the phone. A SIM card gives freedom to subscriber to switch between different network operators. It also allows its subscriber to change ME without changing the number or subscription details.
- operation and maintainance center (OMC): This entity monitors and maintains the performance of all other entities such as BS, MS, MSC and BSC, involved in the network. It also manages

Scanned with CamScanner

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

telecommunications hardware, network operations, charges and billing procedures. and all mobile equipment in GSM systems.

Public Land Mobile Network : It is a complete network that is operated by an administration and Recognized operating Agency (ROA) for providing mobile telecommunications services to public. A PLMN is identified by a combination of the mobile country code (MCC) and Mobile network code (MNC). Each operator that provides mobile services must have its own PLMN within a country however the country can have multiple PLMNs.

Gateway Mobile switching center (GMSC) :- It is a gateway that interconnects the GSM and other networks. It is implemented in an MSC therefore it is referred as GMSC. When a call is made to a subscriber in the GSM network, the call is routed to GMSC first. Then, the GMSC finds out in which part of the GSM network the required HLR exists and routes the call there.

Authentication in GSM :

To prevent fraudulent use of the mobile identities and the subscriber, the GSM uses two techniques. They are :

(i) GSM uses a 4 digit PIN (personal identity number) stored in the SIM. A user that wishes to make a call enters the PIN that is checked by SIM

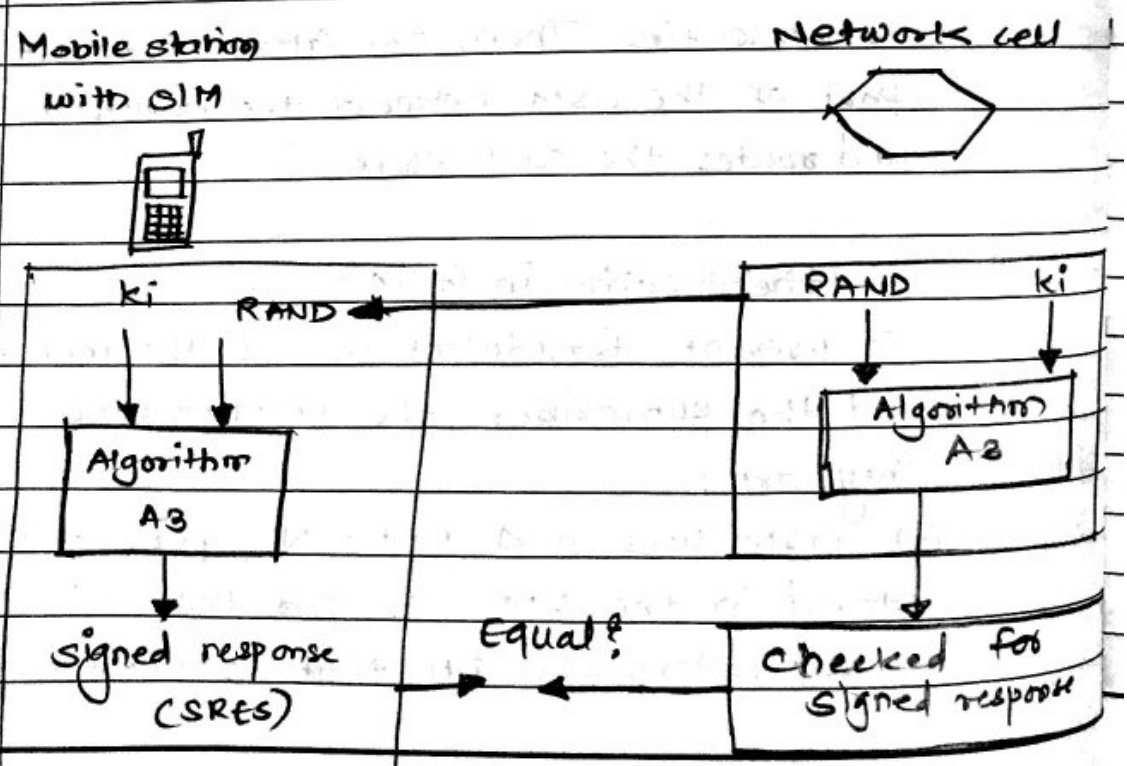
Scanned with CamScanner

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

(ii) GSM interrogates with the units. It is controlled from the MSC/VLR. Authentication can be done at call setup, localization, handover etc.

- once a mobile user has done an access and service request, the network checks the identity of the user by sending a random number (RAND) of 128 bits to the mobile.
- The mobile uses the RAND, Ki and A3 Algorithm to produce a 32 bit signed response (SRES) that is checked by against the response from the mobile. Access continues only if the two responses match. Fig. shows the authentication
- In order to maintain desired ~~response~~ security level, A3 is derived so that computation of signed response (SRES) from RAND and Ki is simple. The computation of Ki from RAND and SRES is complex.



GSM Authentication

Scanned with CamScanner

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

- The RAND and SRES and secret key 'Kc' are sent to the Home location register (HLR). The visitor location register (VLR) sends random number RAND to the SIM where the subscriber and network does the same type of functions. When both match, the VLR will accept the subscriber or will reject it. Hence, higher user authentication is made possible in the GSM users.
- Also authentication of GSM mobile users can be carried out on mobile originated call and mobile terminated call setup and on activation of supplementary services.

Encryption -

Scanned with CamScanner

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

Q 3(b) Describe the system that uses 802.16 stand and also compare 802.16 standards.

IEEE 802.16 refers a set of wireless broadband standards offered by the institute of electrical and electronics engineer (IEEE). The IEEE standard been formed a working group of broadband wireless acc standards in 1999 to improve the standards in WMA The workgroup is an entity of the IEEE 802LA and MAN standards committee.

The IEEE 802.16 set of standards is officially known as wireless MAN in IEEE but now it is commercialized by WiMax forum industry alliance. and is called WiMax. which stands for worldwide interoperability for microwave access. Various produ that are based on various standards of IEEE 802.1 are promoted and certified by compatibility and interoperability by the WiMax Forum industry alliance.

Another standard known as HIPERACCESS was developed in Europe by broadband radio access network (BRAN) committee in 2002. The European standard band offers 40.5 - 43.5 GHz.

WiMax :-

Wimax provides wireless transmission of data using a variety of transmission modes from point to multipoint links to portable and fully mobile internet access.

Scanned with CamScanner

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

Wimax standards.

- Wimax is associated to IEEE 802.16a/REVd/e standards. These standards were issued by IEEE 802.16 subgroup that originally covered the wireless local loop (WLL) technologies with radio spectrum from 10 to 66 GHz. Recently these specifications were extended below 10 GHz.
- In january 2003, the IEEE approved 802.16a as an amendment to IEEE 802.16 defining line of site ~~p~~ capability
- In July 2004, The IEEE 802.16 REVd was introduced to support indoor customer Premises Equipment (CPE) (NLOS) through additional radio capabilities like antenna beam forming and OFDM sub-channeling.
- In 2005, an 802.16a variant was developed for supporting mobility

WiMax

802.16a	802.16revd	802.16a
Fixed outdoor	Fixed outdoor	Limited mobility
(i) services for enterprises	Indoor broadband access for residential users (high speed Internet, VoIP ...)	(i) Portable broad band access for customers
(ii) Backhaul for Hotspots		(ii) Always best connected
(iii) Limited residential broadband access		
CPE	CPE	CPE
(i) External box connected to PC with outside antenna	(i) External box connected to PC with built in antenna	PC card.

Scanned with CamScanner

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

Wimax standards

	Parameter	802.16	802.16a	802.16e
1)	Spectrum	10-66 GHz	2-11 GHz	< 6 GHz
2)	configuration	Line of sight (LOS)	Non-line of sight (NLOS)	Non line of sight (NLOS)
3)	Modulation	QPSK-16 QAM 64 QAM	256 subcarrier OFDM using QPSK 16 QAM, 64 QAM, 256-QAM	256 sub carrier OFDM using QPSK, 16-QAM, 64 QAM, 256-QAM
4)	Mobility	Fixed	Fixed	< 75 mph
5)	channel Bandwidth	20,25 MHz 28 MHz	selectable 1.25-20 MHz	3 MHz Planned
6)	Typical cell Radius	1-3 miles	3-5 miles	1-3 miles
7)	Completion	Dec 2001	Jan 2003	2nd Half of 2004

Wi-max forum:-

- Wi-Max forum is an industry led non-profit organi Corporation formed to promote and certify compatability and interoperability of broadband wireless products.
- The function of wi-max forum is to harmonize standards and certify interoperability between equip from different vendors. standardized interoperable solutions will result in mass volume and bring down its function is to promote and establish a brand for the technology.

Scanned with CamScanner

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

- Wimax forum has more than 400 members from equipment manufacturers, semiconductor suppliers and service providers. Some of its members are Alcatel, AT&T, Fujitsu, Intel, Motorola, SBC, Siemens and Nortel.

Comparison between 802.16 standards

	Feature	Wimax (802.16a)	Wi-Fi (802.11b)	Wi-Fi (802.11a/g)
1)	Primary Application	Broadband wireless Access	Wireless LAN	Wireless LAN
2)	Frequency Band	Licensed/ Unlicensed 2G to 11 GHz	2.4 GHz ISM	2.4 GHz ISM (g) 5 GHz U-NII (a)
3)	Channel Bandwidth	Adjustable 1.25 M to 20 MHz	25 MHz	20 MHz
4)	Half/Full Duplex	Full	Half	Half
5)	Radio Technology	OFDM (256 channels)	Direct sequence spread spectrum	OFDM (64 channels)
6)	Bandwidth Efficiency	≤ 6 bps/Hz	≤ 0.44 bps/Hz	≤ 2.7 bps/Hz
7)	Modulation	BPSK, QPSK, 16-, 256-, 64-QAM	QPSK	BPSK, QPSK, 16-64, QAM

Scanned with CamScanner

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE			
	8)	FEC	Convolutional code Reed-Solomon	None	Convolutional code
	9)	Encryption	Mandatory - SDES Optional - AES	optional - RC4 (AES in 802.11i)	Optional - RC4 (AES in 802.11
	10)	Mobility	Mobile Wi-Max (802.16e)	In development	In development
	11)	Mesh	Yes	Vendor Proprietary	Vendor Proprietary
	12)	Access Protocol	Request/Grant	CSMA/CA	CSMA/CA

Scanned with CamScanner

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

Q5(a) Define the threats and challanges in wireless systems. Explain the different types of device security issues.

- Data related with banking operations, Income Tax, trading, military data, credit card records are stored in computer. If there is any attack on the network, this data can be leaked. and users can misuse the data or modify it.
- Two types of attacks are there ① passive attack where attacker tries to access the data that has transmitted over the network
- Active Attacks: where user data is modified or fraud data is created.

Challanges in security system:

① M's managed different types of wireless devices

② These devices can be easily stolen.

② Information exposure or compromise due to some unauthorized access to devices containing sensitive information

③ challanges for the security of information transferred through wireless networks or transmitted over the air between wireless devices and base stations and networks

④ Device security: Issues for security of wireless devices and information stored in them.

⑤ Different types of wireless networks which has its own merits and demerits.

Scanned with CamScanner

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

Device security Issues :-

In addition to the network-specific security issues, wireless communication and computing is associated with some device-specific issues also. Wireless devices, such as mobiles, which provide computational and communicational facilities in small space as compared to usual desktop computers, are owned by a specific individual and provide easy operability and convenient portability to the users. We can store and process confidential information on these devices without being bounded at a single location (environment), such as office or home. This convenience of performing usual office activities at home without bothering about the distance, traffic etc. however, is not risk free, and it accompanies a number of security threats faced only when we use mobile devices or resources for communication and computing

The most threatening concern in wireless device security is its theft. Laptops, PDAs, cellular handsets etc can be easily stolen. An even bigger threat about a device being stolen is that some of the crucial data can be lost. The primary goal of stealing a wireless device is to gain access to the information stored on it.

Today, almost all the manufacturers of wireless device employ specific security measures, including the use of longer code for unlocking wireless device

Scanned with CamScanner

Total Marks of question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

and extended support for encryption in data storage devices or systems. Wireless devices, however still need implementation of stringent security measures because new types of security threats and attacks which have increased the vulnerability of devices are growing

1) Pull Attacks: The device may be controlled by attackers to gain access to some propriety data and control information. An attacker can use the device as a source to extract data from other pepple or places or he/she may use it to provide data itself through data export interfaces, synchronized desktops, applications running on the device or intranet servers.

2) Push Attacks: Push attacks is a way through which attackers plant malicious code on wireless mobile devices so that the code can be spread all over the network, infecting various network elements. Attackers may use a device to attack several other devices/systems if they become capable of compromising the security on one device in a secure network.

3) Forced de-authentication: In order to maintain continuous connectivity with the network while moving from one place to another, mobile wireless devices have to access different networks. At times, an attacker may convince a mobile device user by sending packets to drop its current network connection and acquire a new signal. In case the user agrees, the attacker inserts a device of his/her own between the user's device and the genuine network in order to steal crucial data.

Scanned with CamScanner

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

4) Multi-Protocol communication : Many wireless mobile devices that can operate on several protocols are manufactured today. This feature itself, at times, becomes an issue for the security of the mobile device. An example of multiprotocol communication is the use of 802.11 family protocol. Also a cellular service provider's network protocol and some other protocols can involve well-known flaws, which are associated with the security of mobile devices. These protocols are not used actively nowadays, but the interface in a number of devices for these protocols is in active status by default. This vulnerability may be exploited by attackers who could connect to the device and take advantage by getting permission to access some of the information from the device or to use its services.

5) Mobility and Roaming :- The location related security issues are the results of movement of users and the data carried with them. In addition certain secrecy and authenticity issues for the exchanged data and privacy issues for user profiles may also creep in because of the need for a continuous change in the location of the user and/or data. A user on a move requires all the significant information to be available to him/her all the time because users are mostly unable to afford any degradation and latency in accessing a service and/or a resource therefore to allow proper

Scanned with CamScanner

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

roaming facilities to users and prevent any kind of access disruption or degradation in service/resource replication of certain parameters and user profiles at different locations would be important. This is, however, a sensitive data and replicating it across various sites. increases the number of points of attack which makes security management difficult and increases the risk for device security at the same time

Disconnection: Wireless mobile devices face frequent disconnections due to handoffs that are performed when a device crosses the region of one connectivity point and enters into the reach of another. Meanwhile an intruder may sense an opportunity to masquerade either as a mobile device or as a mobile support station. This creates issues regarding the security and integrity of the device

Delegation:- Delegation is the process that may open ways for attackers to hijack mobile sessions during which the access control of mobile devices is decided in a flexible and dynamic manner. A delegation mechanism is a temporary permit that the delegator issues to the delegate who, for a limited period, is authorized on behalf of the delegator. Different network access points require some kind of delegation to tackle the switching of wireless mobile devices at various connectivity locations between different types of networks during their movements. The networking

Scanned with CamScanner

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

system may require frequent delegation due to the continuous detachment and reattachment of mobile devices to different access points. This may lead to the problem of potential masquerading and access control loss, which is a huge threat for wireless mobile device and data security.

Q5 (b) Neatly explain WLL architecture. Explain the two local loop techniques with diagram.

WLL refers to a system that is used to link subscribers to the PSTN with the help of radio signals. WLL architecture contains following major components.

Wireless Access network Unit (WANU):

contains BS transceivers or radio ports (RPs), an access manager (AM), a radio port controller Unit (RPCU), and a Home location register (HLR). Its main responsibility is to provide authentication, privacy of air interface and management of radio resource. Further it is must provide operations, administration and maintainance (OAM), billing routing and switching functions. It also provides the facility of converting protocols and encrypting voice and data.

2) Wireless access subscriber Unit (WASU)

- offers two air interfaces - UWLL and TWLL
- UWLL is an air interface towards a network

Scanned with CamScanner

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

and TWU is traditional air interface towards the subscriber

- WASU facilitates services such as protocol conversion and transponding, OAM, authentication functions and signalling functions and provides the power supply locally
- OWU, if required, can used proprietary protocols or standard air interfaces such as advanced mobile phone systems (AMPS), Global systems for mobile communications (GSM), Digital enhanced cordless telecommunications (DECT) or personal access comm. system (PACS) for radio based communication link. TWU can be RJ-11, RJ-45 and so forth. OWU is an air interface that aimed at facilitating OAM to the WLL system. RJ-11 and RJ-45 are registered Jacks that are physical network interfaces used for the purpose of connecting telecommunication devices to a service provider.

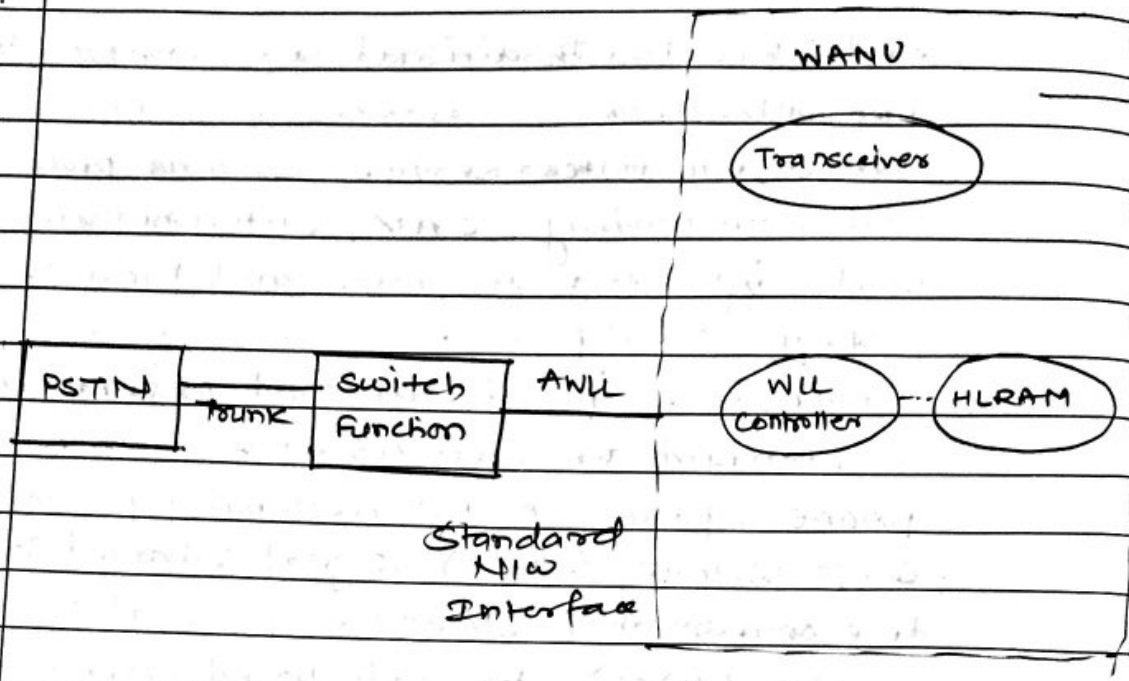
2) Switch Function (SF) :-

Refers to a switch which can be a digital switch that may or may not have advanced intelligent network (AIN) capability, an integrated services digital network (ISDN) switch or a mobile switching center. figure shows WLL Reference model.

Scanned with CamScanner

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE



WLL Reference model.

A leased line, cable or microwave link can be used as transmission back haul between WANU and SF. AWLL is an air interface between WANU and SF and it might be ISDN - BRI or some other

Multichannel multipoint Distribution Service
This is WLL based telecommunication technology that operates in the frequency range of 2.15 GHz to 2.68 GHz. Although MMDS - based transmission system was initially used for transmitting data for business firms, it is now mainly used for wide broadcast of television signals. Therefore it is also

Scanned with CamScanner

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

Known as broadband radio service or wireless cable. However, it is not restricted to television signal; therefore, it is also known as broadband radio service or wireless cable. However it is not restricted to television signal transmission and can be used for wireless transmission of facsimile, telephone and other data signal. You can say that MMDS uses multipoint to point transmission because a single transmission station serves several subscribers. It is a fixed wireless access system, which means that the signal receivers are stationary with respect to the broadcasting station. In most of the countries, MMDS is used primarily to broadcast television signals in remote locations where installation and setting up of wired broadcast network can be a costly affair. It is increasingly becoming a replacement for wired cable connections and some countries are researching and trying to use higher frequencies for transmission.

MMDS Architecture and Its Working

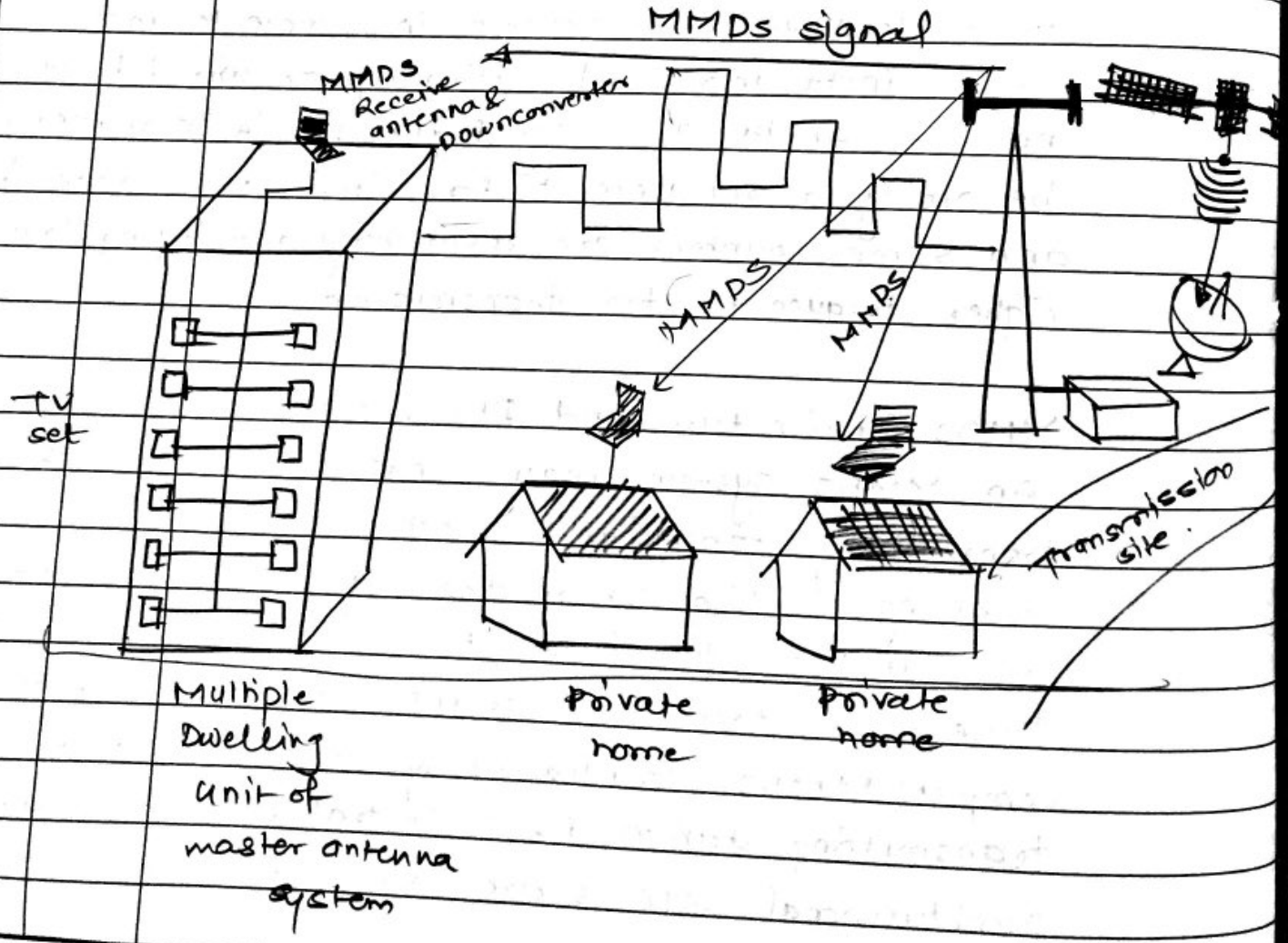
An MMDS system mainly has two components: a transmitting station (or base station) and a subscriber's receiving station where the signals are received and routed to television set. These two components have some other subcomponents that make up the complete MMDS broadcasting system. Head end or transmitting station is a central point from which omnidirectional signals are transmitted, which are then

Scanned with CamScanner

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

received by the antennas installed at subscriber's end. Antennas are installed for both signal broadcast at the head end and signal reception at each subscriber location. At the head end, an up converter that is usually a component of antenna converts the signal to the higher frequency. A set top Box (works as a down converter) is required at the receiving station to convert high frequency signal to appropriate for viewing in television. Figure depicts the working of an MMDS system.



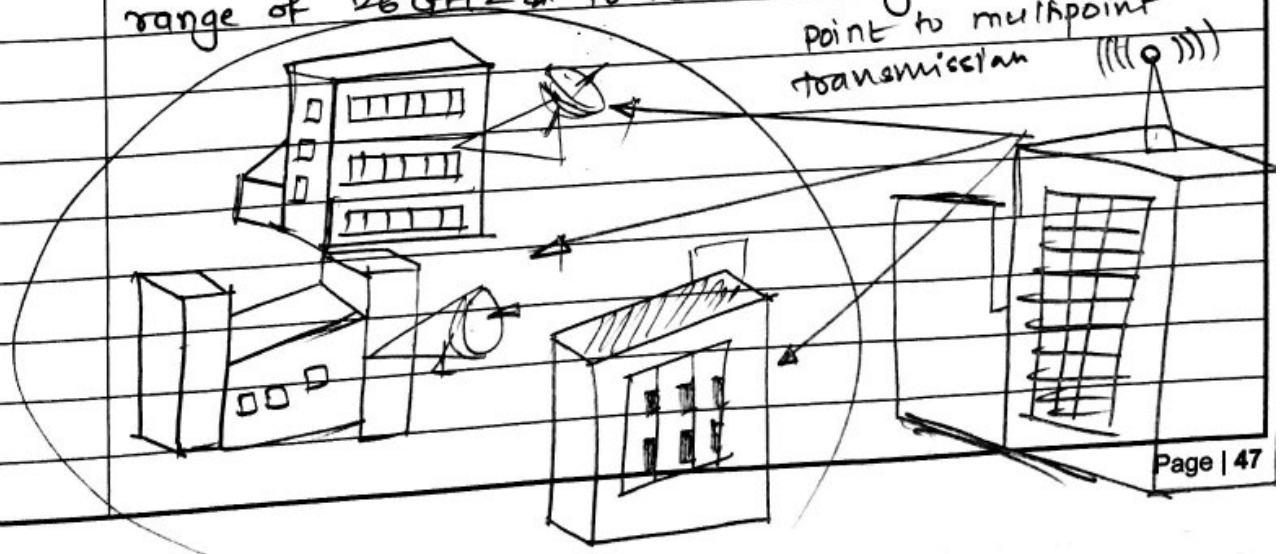
Scanned with CamScanner

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

Generally, a satellite system is used to deliver data at the head end. However, it is not necessary to have a satellite system for the delivery of data. The data might be available in some storage device such as a tape or might be generated locally. It is then converted and modulated to appropriate form and directed to the transmitting antenna through a cable. Transmitting station antennas radiate the signal in an omnidirectional manner. The antennas installed at the subscriber station catch these ~~stations~~ signals, and through a converter (such as set top Box). These signals are fed to the intended device such as a television.

Local multipoint Distribution service (LMDS)
There is no much difference in the architecture of local multipoint distribution service (LMDS) and MMDS. LMDS is a fixed wireless access technology that operates on high frequencies (much higher compared to MMDS) that lie within the approximate range of 28 GHz to 43 GHz. Fig. shows LMDS.



Scanned with CamScanner

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

because of the propagation characteristics of frequencies used in LMDS, the cellular network architecture is used. It provides high speed data transmission and is widely used for providing internet connections that have high data rates. It can operate in duplex mode and serve subscribers within the range of 8 to 5 miles. In the US, LMDS is assigned 1.3 MHz of frequency band for transmitting signals to residential as well as business organizations. Compared to MMDS system LMDS has faster data transmission but lesser range.

Scanned with CamScanner

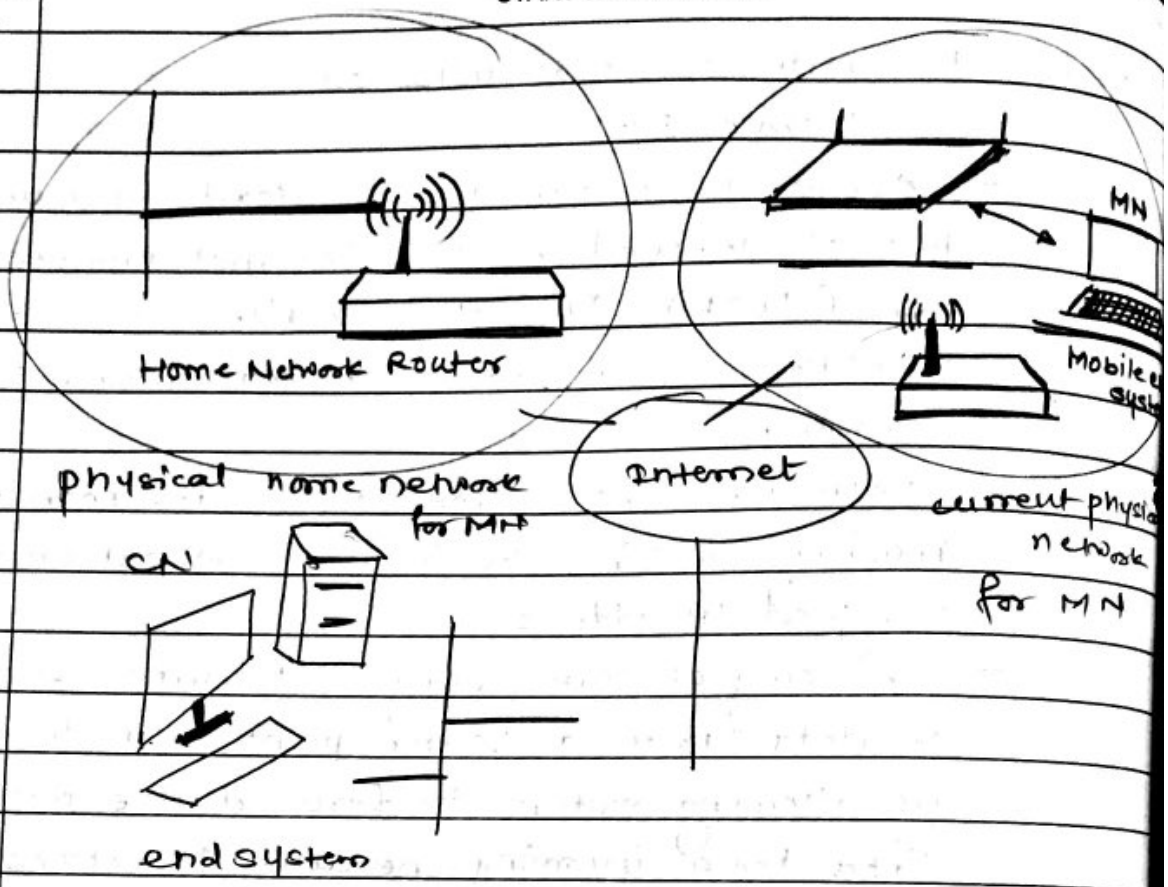
Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE
	Q6	(a) Write a short notes on.
		(a) Mobile IP.
		- Mobile IP is an open standard communication protocol defined by the internet engineering Task force (IETF). It allows mobile users to have same IP address and stay connected in case of network roaming.
		- MIP provides a mechanism for mobile node (MN) mobility within the internet without changing its assigned IP address.
		- Working of MIP routing :- IP routes send packets of data from a source point to a destination point by allowing routers to forward the packets of data from incoming network interfaces to outbound network interfaces on the basis of routing tables. These routing tables store and maintains the information of ~~to~~ outbound interface for destination IP addresses connected in the network.
		- Data packets that have to be sent to a destination point have to be routed to a home network. Home network means a network identified on the basis of home address of an MN. Now the Home Agent (HA) of the MN receives these data packets and moves them towards the MN, which has recently reported care of address (COA) Finally the packets are decapsul and delivered to the destinat MN.
		- Consider the example of mobile network shown in figure.

Scanned with CamScanner

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE



1) MN : specifies a mobile device or a system that can change its connection point on a network without changing its IP address.

2) Home network (HN) : Specifies the network of mobile devices that have their own unique and individual IP addresses or home addresses

3) Home addresses :- Specifies the IP address of a mobile device that is assigned to it within a home network.

4) Foregin network (FN) : specifies the network of mobile devices, but these mobile devices are operating far from their home network.

Scanned with CamScanner

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

5) CoA: Specifies the network-native IP address of a mobile device that operates in a foreign network

6) HA: Specifies a router of mobile devices (or node on a home network. This router sends datagrams to mobile devices when these devices are away from the home network. An HA also maintains the current locations of mobile devices on the basis of identifying their IP addresses. Moreover, HAs are generally used with one or more foreign agents.

7) Foreign Agents (FA): Specifies a router that stores information about mobile devices that are visiting its network. FAs also promote CoAs that are used by MIP.

8) Binding: Specifies the association of a home address with a CoA of a mobile device

9) correspondant node: Specifies a communication partner

MIP was basically developed to allow mobile computers to have internet connection even while moving from one internet access point to another. Here, the term mobile means the subscriber is connected to either one or multiple applications over the internet and the access point changes with each movement. This is completely different from a user who uses his or her internet service provider (ISP) account to use the internet from various locations while travelling.

MIP enables the client to transmit datagrams irrespective of where it is connected to the network.

Scanned with CamScanner

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

The only security issue with such a technique is the redirection attack. Such an attack takes place when a malicious client provides false data to the HA in the MIP network. The HA is notified that the client contains a new care of address. Therefore all the IP datagrams sent to the actual clients are redirected to the malicious client.

MIP resists the following two types of attacks.

1) A malicious agent that might ~~apply~~ reply to past registration messages and cut the node form its network

2) A node that might act as a foreign agent and send a request for registration to a HA to divert traffic that is intended for a mobile node to itself

Usually, such types of attacks on MIPs can be averted by following message authentication process and making appropriate use of the identification field of the registration request and reply message. Every registration request and reply consists of an authentication extension. having following ~~test~~ fields.

1) Type :- 8 bit field. Describes the type of authentication extension.

2) Length : 8 bit field. Recognizes the number of bytes in authenticator

3) Security parameter Index :- 4 byte field. Used for finding out the security context in a pair of nodes. The security context is set up in such a manner that the two nodes share the same secret key and parameters appropriate for authentication scheme.

Scanned with CamScanner

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

Authenticator : Refers to a field that contains a code that is added by the sender into the message with the help of shared secret key. The receiver then uses the same code to ensure that the message that has not been tampered. The default authentic scheme is the keyed - MD5 which generates a 128 bit message digest.

2) Wireless Sensor Network.

WSNs are used to monitor or gathered enviornmental data such as pressure, temprature, smoke or any unusual change in the existing environment. The method used for collecting data related to enviornment or processes is known as sensing. A sensor is a device that converts the physical parameters to a form that can be stored or transmitted for computation and analysis. Electronic sensors are similar to human organs such as eyes, ears and nose. similar to the way these organs collect enviornment data (such as temp, smell and Images) and provide it to our brain, electronic sensors also collect enviornmental data for further analysis.

WSN is widely used and popular because of utilization and advantages it offers. some of the advantages of WSN are as follows.

① Robust :- it can withstand with rough and harsh weather condition. WSNs can be installed

Scanned with CamScanner

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

START WRITING HERE

Space for Marks	Question No.

in remote locations where monitoring is needed.

(3) wider area coverage Even in dangerous enviornment.

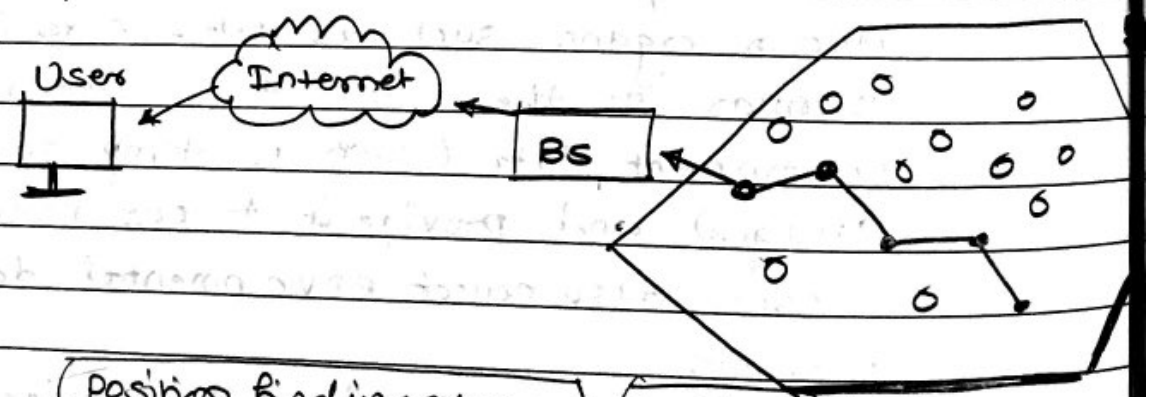
(4) capability to cope up with node failures:

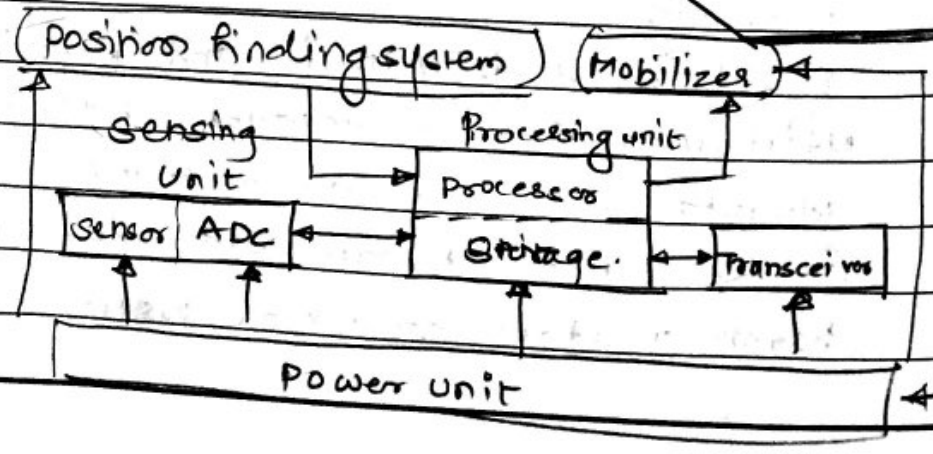
In case some nodes are damaged or not working WSN can coped up with such node failure issues because it can be assigned to different routing path to the data is being sensed. This is not the case in wired networks. and the failure of single node can crash entire network

Network model:

A WSN is made up of several sensor nodes scattered in an area that can be left unattended. It consists of 4 components

1. Sensing unit 2. processing unit
3. power unit 4. Transceiver.





Scanned with CamScanner

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

WSN can have other components also such as a unit for location detection, power generator, mobilizer.

A sensing unit can have further subcomponents such as analog to digital converter (ADC) that is used for converting the analog signals generated by sensors to digital form. These digital signals are generated by ADC are sent to the processing unit. Usually, a processing unit has a small memory storage that stores procedures for processing and communicating with other sensors. A transceiver unit is used for sending and receiving signals from one sensor node to another and also for transmitting sensed data to the base station receiver. The processing unit has a several functions some of these are as follows:

1) Managing the data collected by sensor
2) power management
3) Managing network operations according to wireless network protocols.

Power management is an important task performed by a microprocessor. Managing power is essential so that the WSN can work for a long period of time without changing the power supply. Each sensor node follows certain procedures and does not transmit signals unnecessarily. It transmits signal only under some required situation and when certain environmental changes are sensed.

Scanned with CamScanner

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

(5) Handoff strategies:

The process of reallocating a different voice channel to the mobile cellular phone as the user moves between cells during a call is known as handoff.

The handoff process (for first generation analog cellular systems) involves the following basic operations.

1) During a call, the serving base station monitors the signal strength [RSSI] from the mobile on reverse voice channel.

2) If the signal strength falls below a pre-designated threshold, the base station sends a request to the MTSO for a hand off of the call.

3) The MTSO then requests the location receivers of neighbouring base stations to measure the signal

Scanned with CamScanner

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

strength (RSSI) from the mobile.

4) If another base stations from the neighbouring cells indicates better signal strength then the serving base station, then under instructions from the MTSO the serving base station sends a signalling message to the mobile on the speech channel. asking the mobile to retune to a free channel in the neighbouring cell.

5) The mobile retunes to the new channel (in new cell) and simultaneously the MTSO switches the call to the new base station. signal quality measurement and new cell selection generally take several seconds. but the change of speech channels that is the actual hand off takes a fraction of a second (200ms) and it is completely unnoticeable to the user.

During the process of mobile conversation, when a mobile user moves from one cell to another cell, the MSC must transfer the call from the current base station BS to the next base station. when the user leaves the border of the current cell, the strength of the signal decreases, and the moment user enters another cell, BS2 looks after the call progress, and the signal strength starts increasing as per BS2

This process where a proper call progress is maintained even when the mobile user is moving

Scanned with CamScanner

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

from one cell to another is called handoff.. Accuracy should be maintained at all the times to prevent any termination of call when two users are converseing with each other

However if the MSC excessively delays the assigning of handoff, the signal will automatic get down to the minimum acceptable level. this will result in an appropriate handoff. such a minimum acceptable level is referred as acceptable audio quality level at the BS receiver side

A strong signal, which is considered to be slight stronger than the acceptable audio level, is then used as threshold. Handoff is made at this threshold level, which is represented by Δ. and is considered as optimum. This threshold level must not be either large or small from the required level. Threshold level is calculated as follows

$$\Delta = P_{RH} - P_{RM}$$

Where

P_{RH} = handoff signal power that is received

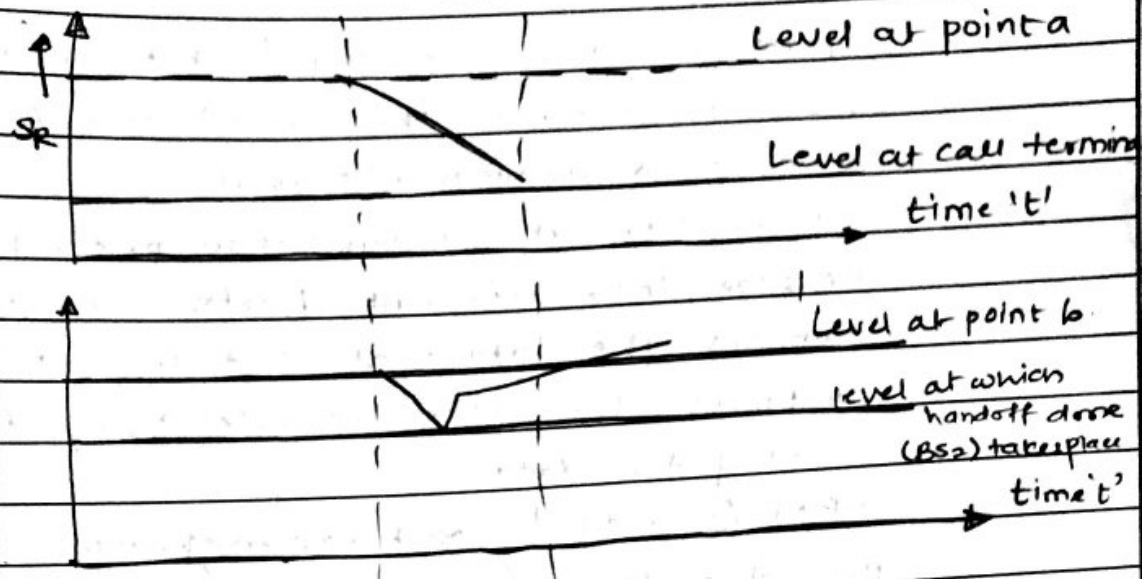
P_{RM} = minimum usable signal power.

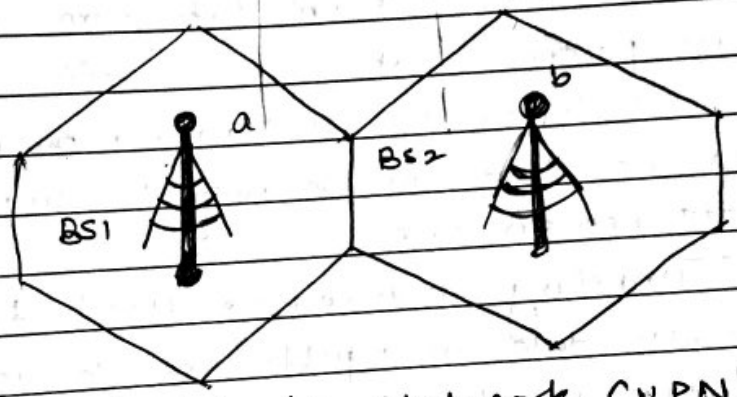
When the MSC excessively delays the assigning of the desired handoffs, the signal drops below the optimum level.

Scanned with CamScanner

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

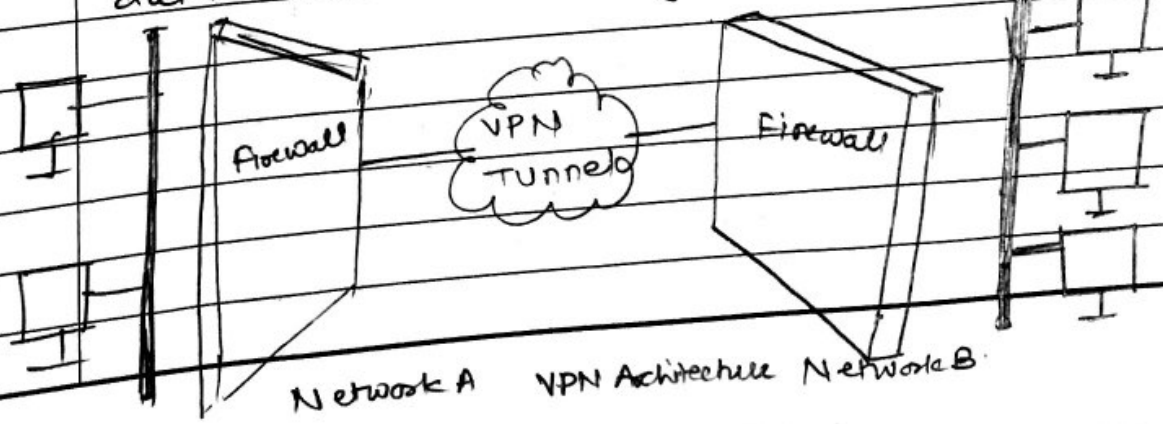




④ Virtual private Network (VPN)

i) A VPN is used for connecting networks and resources of a network over another network that are located over different places.

2) VPN uses a public network (Internet) in order to connect to the computer networks making data communications very easy and cheap.



Network A VPN Architecture Network B

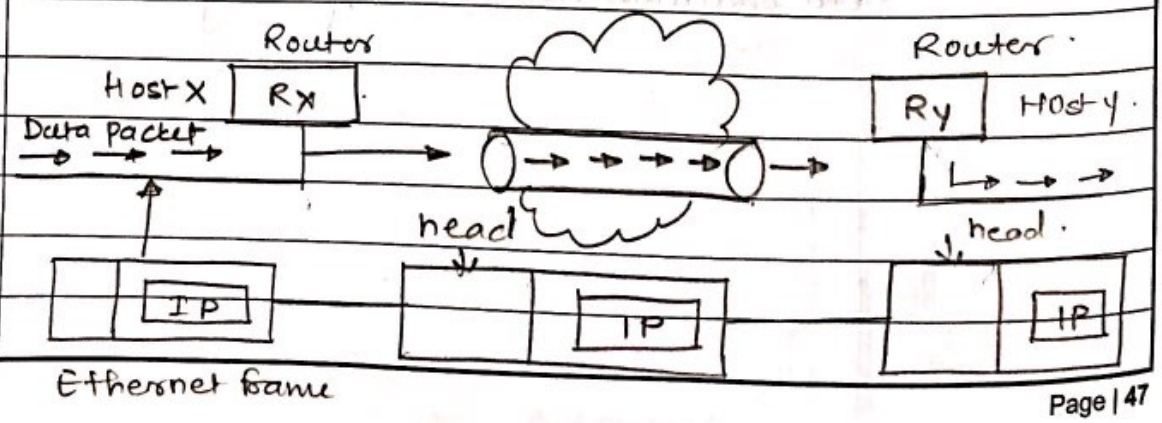
Scanned with CamScanner

Total Marks of Question no.		Examiner	
		Moderator	
		Re-Assessor	

Space for Marks	Question No.	START WRITING HERE

Whenever data is exchanged between two devices over the internet they must transfer it in regard to some communication protocol

- These different communication protocol split the message into different parts such that one part comprises the data that is to be sent and another comprises the different rules to be followed for sending the data.
- VPN is based on tunneling protocol. A tunneling protocol encloses in its datagram another complete data packets that uses a different communication protocol. It creates a tunnel between 2 points of a network that can securely transmit any kind of data between them.
- Tunneling protocols are used for transmitting private data on a public network usually in developing virtual private network. (VPN)
- Tunneling protocols when transmitted over a public network provide security to the transmitted data. today for secure data transmission we use various tunneling protocols like PPTP (point to point tunneling), SSH (secure socket) IPsec, L2TP.



Scanned with CamScanner

Total Marks of Question no.	Examiner	
	Moderator	
	Re-Assessor	

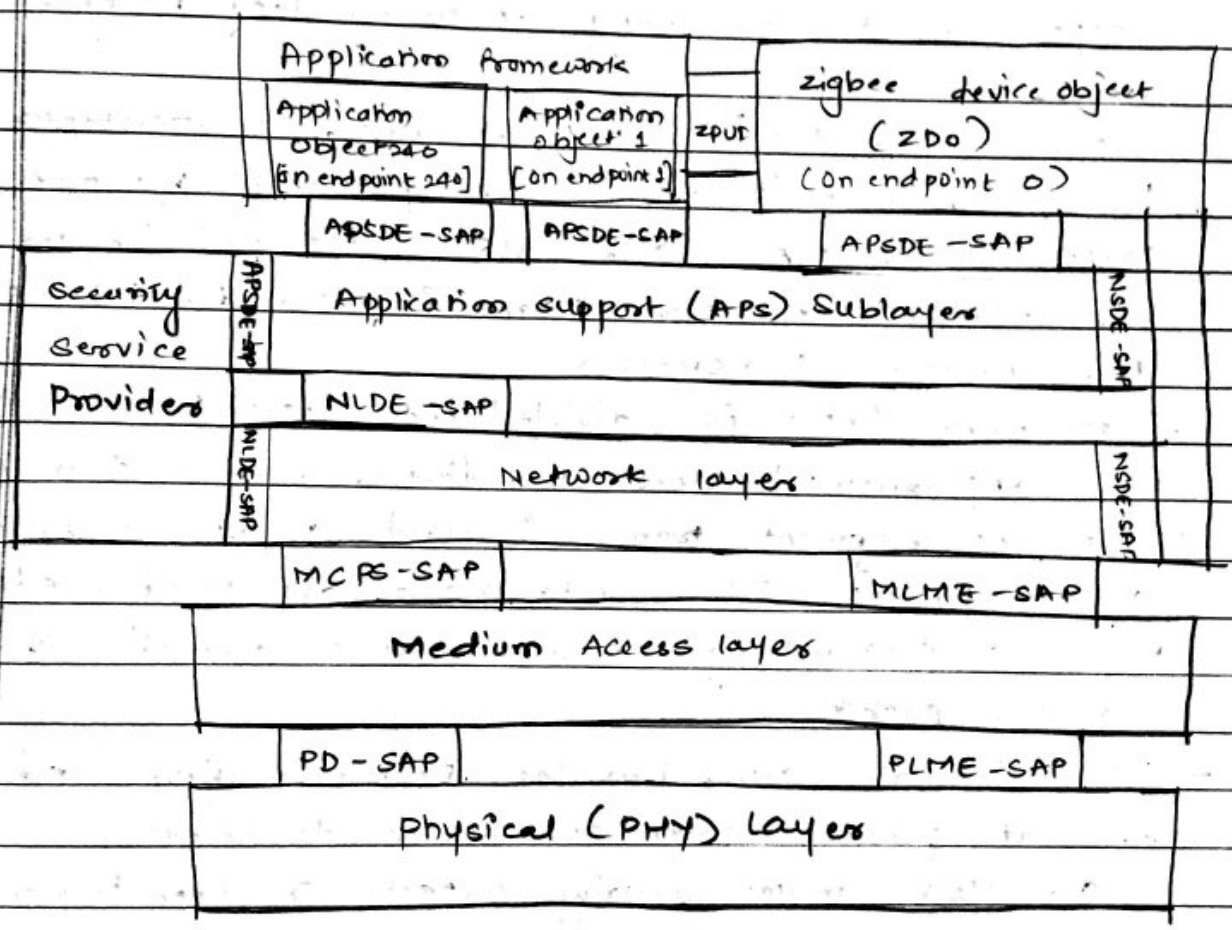
Space for Marks	Question No.	START WRITING HERE

- Host X wishes to send a data packet to Host Y. The data packet at host A has the IP address of Host Y.
- Host A transmits the data packet. When the data packet receives Router Rx, the IP packet is removed. The router inserts the payload field and sends it to router Ry.
- On receiving the packet router Ry removes the IP packet and sends it to the hostY in the ithernet frame.
- VPN is a group of two or more computer systems that is connected to a private network that is maintained by an institution or company for its own use with public access
- For secure transmission following tunneling protocols are used as a result of developements in VPN. PPTP, SSH, L2TP, IPsec
- VPN is already deployed in various organizations to enable remote workers to access the organization network data through the internet securing
- Traffic control, security, enterprise management are three parameters needed for VPN Technology.

Scanned with CamScanner

Q4 (a) zigbee architecture

- Each layer in the zigbee stack is independent of every other layer although lower layers provide services to higher layers. In other words, we can say that a higher layer acts as a ~~member~~ master, whereas lower layer behaves as a slave providing services to the master layer.
- Fig shows Zigbee stack Architecture



- Zigbee architecture has layered structure similar to that of the OSI model, consisting of physical, network and link (MAC) layer. Moreover the APS and ZDO layers of the zigbee architecture provide similar functionality as provided by the transport, presentation, session and application layers of OSI model taken together.

Scanned with CamScanner

- There exists service access points (SAPs) between al
In the architecture. These SAPs separate each layer f
another layer and enable it to function independently
- The lowest layer i.e. physical layer is responsible
for converting data packets into a form which is suita
for transmission over a wireless channel. It is also
responsible for receiving incoming data packets from
other devices.
- Networking facilities such as network identifier and
beacon request / responce are provided by the MAC
layer. The MAC layer uses different types of fra
for example: a beacon frame is used by the co-ordina
for beacon transmission.
- Further data is divided into data frames and ac
with appropriate headers and footers before transmissio
- Acknowledgement frame is used when a device recei
a data packet. It sends back an acknowledgement
frame to transmitting device as a confirmation of proper
delivery packet.
- The network layer handles proper routing and delivery
of data packets from one device to another
- It also handles security aspects of data transmission
It is a duty of APs layer to capture and remove dupli
data packets transmitted by network layer in an attemp
to send all the data frames whose acknowledgement is
not received on the time. It also maintains a table
for node called binding table that holds the informa
of other nodes that wish to connect with it

Scanned with CamScanner

Q4 (b) Explain Hidden and exposed node terminal problem

Hidden Terminal:-

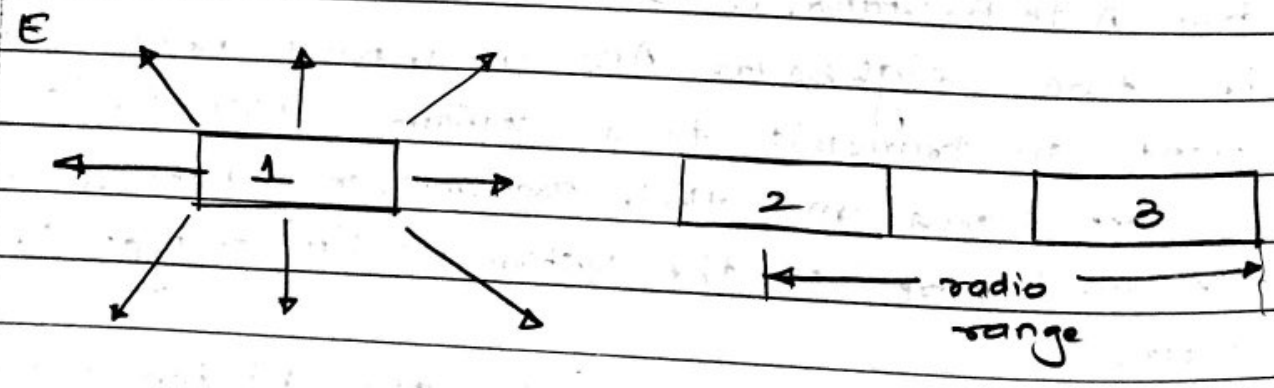
To understand the problem of hidden terminal in wireless network, let's consider an example of an ad hoc wireless network in which the stations A, B and C exists. station B exists between two stations A and C, the distance between stations A and C is quite large. Now assume that stations A and C start sending data packets to station B simultaneously without knowing the state of each other. In such a situation a collision occurs. Both stations A and C transmit to station B till the end of their packets without realizing that their packets can not be received correctly. In such situation two types of wastage occurs.

- First a collision occurs due to simultaneous sending of packets. second the time duration of a whole packet has been wasted.
- In fact, station C is behind station B during the transmission from A to B. Station C is hidden for station A. similarly if two neighbours APs in infrastructure based WLANs want to transmit to a station. which is located in the overlapped area and their transmission is not co-ordinated by the wired part of the system. a similar type of collision occurs.

one of the solutions to solve the hidden station problem is to partially avoid it. For this, it should be ensured that the channel sensing range is greater than the receiving range. Generally, this method is applied in high performance radio local area network

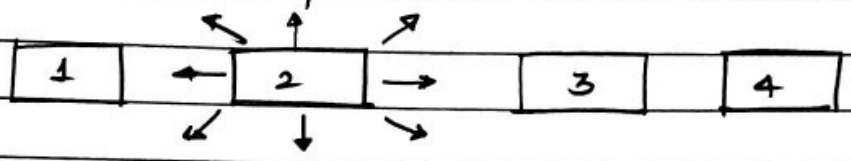
Scanned with CamScanner

- Another solution of hidden station problem is the appl of a multiple access with collision avoidance (MACA) In MACA scheme, you can start transmission fro station A to station B. station A sends a request fo sending request-to-send (RTS) packet. This RTS packet contains address of address of transmittin and receiving stations. and duration of future transmi The station B sends answer to station A with the clear to send (CTS) packet. which is also heard by station C. This CTS packet stores the addresses of the sender and reciplent and duration of transmission. Throug this information, station C realized that the medium will be occupied for a particular time period which is already specified. therefore, the specified time period will not be given to othe transmission. Collision will ~~occur~~ occurs if stations A and C send the R packets concurrently. but the collision is for a short time.



Exposed Terminal :-

- To understand the problem of exposed terminal, lets take the same stations A, B and C. In this case, consider that station B sends some data to station A and station C requires to send data to different mobile phones which is outside the interference range of station A and B. station C finds that the carrier that is B's signal is busy hence it postpones that transmission of data till it finds the medium to be idle. However as station A is outside the interference of station C, waiting is not required. A collision at B does not matter as the collision is considered very weak to propagate to A. hence C is considered to be exposed to B.



Exposed terminal

RTS - CTS mechanism

- Sender sends a request to send RTS packet to the receiver. This short frame 30 bytes size contains the length of that data frame that will be transmitted. RTS is received by all the stations that can hear the sender
- Every station that receives RTS packet will send network allocation vector (NAV). This NAV of a station specifies the earliest time at which station is allowed to attempt transmission
- Intended receiver waits for SIFS and sends CTS packet showing that it is ready to receive data. CTS has the data length copied from RTS frame. All station receiving CTS will set their NAVs.
- These stations are within the range of receiver

Scanned with CamScanner

- station receiving CTS are different from those wh receives RTS
- RTS packet has been sent and CTS has been rec all nodes near sender and receiver understands tha medium is reserved for one sender
- The sender waits for SIFS and starts data packet transmission. The receiver receives data packet, wai for another SIFS and send ACK. ~~as~~
- As soon as Tx is completed NAV in each node wil mark medium as free and process is repeated.
- When RTS and CTS are being sent collision occu
- nodes will listen RTS and CTS will refrain from Transmissions and avoid collisions.

Scanned with CamScanner

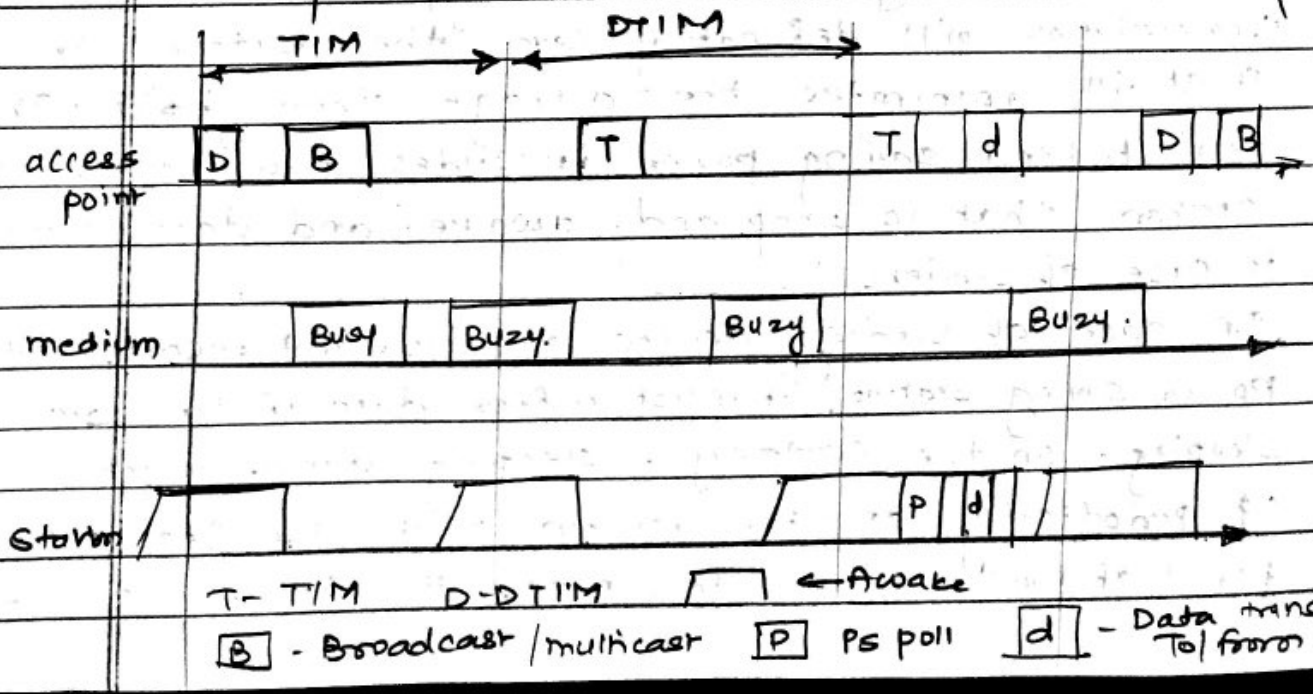
Q4(C) List 802.11 MAC management functions. Explain in detail power management function with neat diagram

— Typically all wireless devices run on battery unless a solar panel is used. Thus it is important to use different power saving methods to ensure that the commercial success of such devices. LAN protocols have this notion that stations are always available to receive data. In case of lightly loaded networks, receivers are usually found idle most of the time. However such a readiness should always be there in the receiving module. This is essential for the battery life as receiver current may be upto 100mA. The main goal of IEEE 802.11 power management is to keep the transceivers off when it is not needed. In case of sending device, it is simple task as the transmission is prompted by the device itself. However in case of receiving device, the power management does not know when to keep the transceivers active for a particular packet hence it has to wake up the transceiver periodically. The process of switching off transceivers should be transparent enough to the existing protocols. switching of transceivers will definately save the battery life but it will minimize the average throughput. The goal behind saving power includes two states for a station that is sleep and awake. and data buffering in case of senders.

In case of sending device requires interacting with power saving station, it must buffer data if the station is sleeping. on the contrary, sleeping station must wake up periodically and the remain awake for the specific period of time. During this time, all the sending devices

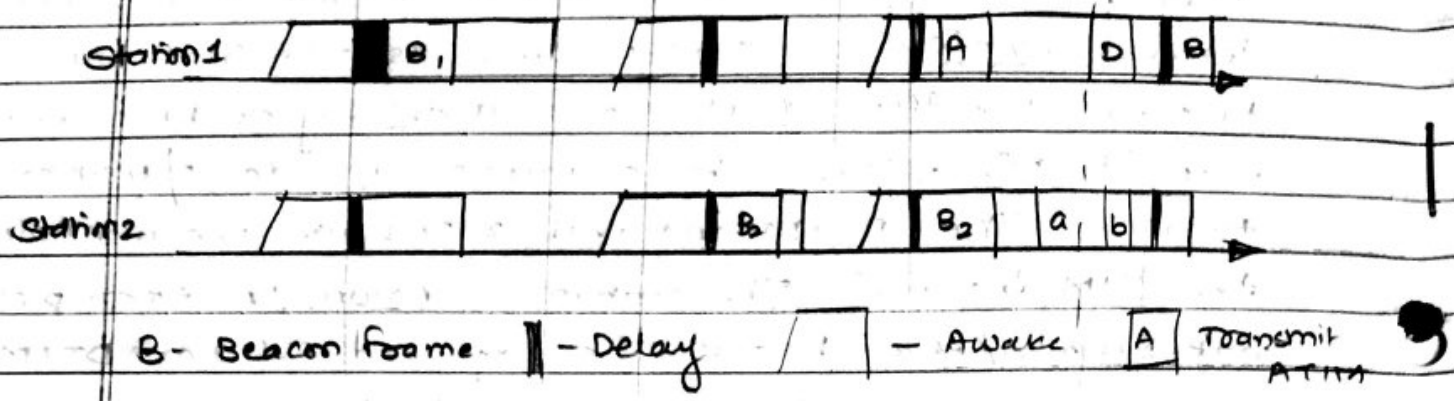
can broadcast the destinations for their buffered d
frames, once the station is found to be a destination
buffered packet. then it has to remain awake till th
transfer occurs. In order to wake up at the right tim
it is essential to use TSF. All stations must be awake
must wake up at that time.

It is quite easier to manage power in infrastructure b
networks in comparison to ad hoc networks. All the f
that are to be transmitted to stations working in powe
save mode are buffered by the access point along
with a beacon, a traffic indication Map (TIM)
also sent by access point. The TIM maintains the rec
of all stations for which the access point buffers un
data frames. The sleeping station must wake up peri
and start listening to the beacon and TIM. Inc
the TIM contains a unicast frame buffered for
station, then the station must remain awake specia
for multicast and broadcast transmission. Another rea
for which the station must remain awake is a fra
which needs to be transferred from station to the
access points. The TSP timer runs on a sleeping st



In the preceeding scenario, there is a single access point and single station used in the infrastructure network. The transmission state of medium is shown to be busy. The access points transfers the beacon frame at a beacon interval, which is almost same as the TIM interval. Further, the access point stores a delivery traffic indication map (DTIM) interval to transmit broadcast/multicast the frames. The DTIM interval represents the multiple of the TIM interval. The station, shown in examples, wakes up ~~after~~ before the expected TIM or DTIM. In first scenario, the access point transmits a broadcast frame, it gets back to the sleeping mode. The station ~~gets~~ then wakes up just prior to the next TIM transmission. At this point, the TIM gets delayed because of a busy medium; hence station has to remain awake. where the sleeping period is too short. In this method, it is illustrated how battery power is saved but there are short delays in accessing stations. The more short the TIM, the more short delay and power saving is low.

In case of ad hoc networks, it becomes more complicated to manage power as compared to Infrastructure network. In ad hoc networks, no access point is used to buffer a data at a single location but every station could require to buffer data in order to interact with a station that saves power. When all stations are awake they broadcast a list of buffered frames and the destinations ~~for~~ for the data are broadcasted with the help of ad hoc traffic indication map (ATIMS) hence announcement period is ATIM window



B - Beacon frame ▌ - Delay / ▏ - Awake [A] Transmit ATIM

a - Acknowledgement d - Acknowledge Data D - Transmit data

In proceeding figure, two stations are used. The beacon interval in this case is ascertained with the help of a distributed function. Multiple stations send beacon at the same time and because of this synchronizations all the stations have to awake at the same time. As depicted in the first two steps in the preceding figure, all stations will remain awake for the ATIM interval and then go to sleep mode if no frame is buffered. After that station 1 buffers data for station 2. This is shown in ATIM transferred by station 1. When station 2 receives the buffered data, It acknowledges this ATIM and remains awake. After the ATIM window station 1 is now ready to send the data frame and station 2 after receiving the data frame acknowledges it Both stations will be awake to receive new beacon.

Scanned with CamScanner