Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

BE - SEMESTER–VII (NEW) EXAMINATION – WINTER 2021

Subject Code:3171608 Date:10/12/2021

Subject Name: Wireless Communication

Time: 10:30 AM TO 01:00 PM Total Marks: 70

Instructions:

1. **Attempt all questions.**
2. **Make suitable assumptions wherever necessary.**
3. **Figures to the right indicate full marks.**
4. **Simple and non-programmable scientific calculators are allowed.**

MARKS

Q.1 (a) What is Wireless Communication? Also Explain the Types of Wireless Communication. **03**

Wireless communication refers to the exchange of data or information between devices or machines without the use of physical connections such as cables or wires. Instead, wireless communication relies on electromagnetic waves or signals to transmit data over the air.

There are several types of wireless communication technologies, including:

1. Radio frequency (RF) communication
2. Infrared (IR) communication
3. Bluetooth
4. Wi-Fi
5. Satellite communication
6. Cellular communication
7. Near field communication (NFC)

(b) Explain the Difference between Wired and Wireless Communication. **04**

	Wired Communication	**Wireless Communication**
Physical connection	Requires a physical connection such as a cable or wire	Does not require a physical connection
Range	Limited by the length of the physical connection	Can transmit data over longer distances using electromagnetic waves or signals
Speed	Generally faster than wireless communication	May be slower than wired communication, depending on the technology used
Security	Generally more secure as data is transmitted over a physical connection	May be less secure as data is transmitted over the air and can potentially be intercepted
Flexibility	Limited in terms of placement and movement of devices	Allows for greater flexibility in terms of placement and movement of devices
Interference	Less likely to be affected	May be more prone to

	by interference from other devices or sources	interference from other devices or sources
Cost	May be cheaper to install and maintain	May be more expensive to install and maintain

(c) Explain the Evolution of Mobile Communication. **07**

The evolution of mobile communication has occurred in several stages over the past several decades:

1. First generation (1G): The first generation of mobile communication, also known as analog cellular, was introduced in the 1980s. 1G networks used analog signals to transmit voice and basic data services such as text messaging.
2. Second generation (2G): The second generation of mobile communication, also known as digital cellular, was introduced in the 1990s. 2G networks used digital signals to transmit voice and data services, including the ability to send and receive text messages, access the Internet, and make phone calls over the Internet (VoIP).
3. Third generation (3G): The third generation of mobile communication, also known as broadband cellular, was introduced in the early 2000s. 3G networks provided faster data speeds and the ability to access more advanced data services such as streaming video and audio.
4. Fourth generation (4G): The fourth generation of mobile communication, also known as LTE (Long-Term Evolution), was introduced in the late 2000s. 4G networks provided even faster data speeds and the ability to access high-definition video and other advanced data services.
5. Fifth generation (5G): The fifth generation of mobile communication, also known as 5G, was introduced in the 2010s. 5G networks provide ultra-high data speeds and low latency, making it possible to access even more advanced data services such as virtual and augmented reality.

Each new generation of mobile communication has brought significant improvements in terms of data speeds and the types of services that can be accessed, enabling the proliferation of mobile devices and the widespread use of mobile communication for both personal and business purposes.

Q.2 **(a)** What is Wi-Fi? **03**

Wi-Fi (Wireless Fidelity) is a wireless networking technology that allows devices to connect to the Internet or to other devices through a wireless network. It operates in the 2.4 GHz and 5 GHz frequency bands and uses radio waves to transmit data over short distances. Wi-Fi enables devices such as computers, smartphones, and tablets to connect to the Internet and exchange data without the need for physical cables or wires. Wi-Fi is commonly used in home and office networks, as well as in public places such as cafes, airports, and hotels. It has become an essential part of modern communication and has greatly facilitated the use of the Internet and other online services.

(b) Explain the CSMA Protocols in Detail. **04**

CSMA (Carrier Sense Multiple Access) is a type of protocol used in wireless and Ethernet networks to enable multiple devices to share the same

communication channel and access the network efficiently. CSMA protocols allow devices to detect when the channel is in use and to avoid transmitting data at the same time, reducing the risk of data collision and improving the overall performance of the network.

There are several different types of CSMA protocols, including:

1. CSMA/CD (Collision Detection): This is the most common type of CSMA protocol and is used in Ethernet networks. When a device wants to transmit data, it first listens to the channel to see if it is in use. If the channel is free, the device begins transmitting. If another device starts transmitting at the same time, a collision occurs and both devices stop transmitting. The devices then wait a random amount of time before trying to transmit again.
2. CSMA/CA (Collision Avoidance): This type of CSMA protocol is used in wireless networks. Like CSMA/CD, CSMA/CA allows devices to listen to the channel before transmitting. However, instead of simply waiting a random amount of time before retrying, the device sends a request to transmit (RTS) message to the receiving device, which responds with a clear to send (CTS) message. This allows the devices to coordinate their transmissions and avoid collisions.
3. CSMA/CA with ACK (Acknowledgment): This is a variant of CSMA/CA that includes an additional step to ensure that the data was received successfully. After transmitting the data, the transmitting device waits for an acknowledgement (ACK) message from the receiving device before ending the transmission. If the ACK message is not received, the transmitting device assumes that the transmission was not successful and retries the transmission.

CSMA protocols help to improve the efficiency and reliability of wireless and Ethernet networks by enabling multiple devices to share the same communication channel without interfering with each other.

(c) Write a Short notes.1) TDMA 2) CDMA **07**

TDMA (Time Division Multiple Access) is a multiplexing technique used in digital communication systems to allow multiple devices to share the same frequency spectrum. It works by dividing the channel into different time slots and assigning each device a specific time slot in which it can transmit data. This allows multiple devices to transmit simultaneously without interfering with each other. TDMA is commonly used in 2G and 3G mobile communication systems. It is an efficient way to increase the capacity of a communication system by allowing multiple devices to share the same frequency band. TDMA works by dividing the channel into time slots, with each device assigned a specific time slot in which it can transmit data. This allows multiple devices to transmit simultaneously without interfering with each other. TDMA is a popular choice for mobile communication systems because it is relatively simple to implement and can provide good performance in a variety of environments.

CDMA (Code Division Multiple Access) is a multiplexing technique used in digital communication systems to allow multiple devices to share the same frequency spectrum. It works by assigning each device a unique code that is used to spread the data signal over a wide frequency band. This allows multiple devices to transmit simultaneously without interfering with each other. CDMA is commonly used in 3G and 4G mobile communication systems, as well as in some types of wireless networking. It is an efficient way to increase the capacity of a communication system by allowing multiple devices to share the same frequency band. CDMA works by assigning each device a unique code that is used to spread the data signal

over a wide frequency band. This allows multiple devices to transmit simultaneously without interfering with each other. CDMA is a popular choice for mobile communication systems because it can provide good performance in a variety of environments and has the ability to support a large number of users in a single frequency band.

OR

(c) Write a Short notes.1) FDMA 2) OFDM **07**

1. FDMA (Frequency Division Multiple Access): FDMA is a multiplexing technique used in digital communication systems to allow multiple devices to share the same frequency spectrum by dividing the frequency band into different channels and assigning each device a specific channel. This allows multiple devices to transmit simultaneously without interfering with each other. FDMA is commonly used in analog communication systems, such as AM and FM radio, as well as in some types of digital communication systems.
2. OFDM (Orthogonal Frequency Division Multiplexing): OFDM is a multiplexing technique used in digital communication systems to allow multiple devices to share the same frequency spectrum by dividing the frequency band into multiple subcarriers and assigning each device a specific subcarrier. OFDM is commonly used in wireless networking and broadband communication systems, such as Wi-Fi and digital TV. It is an efficient way to increase the capacity of a communication system by allowing multiple devices to transmit simultaneously without interfering with each other. OFDM is particularly useful in environments with high levels of interference, as it is less susceptible to interference than other multiplexing techniques.

Q.3 **(a)** Explain the Wireless Protocol. **03**

A wireless protocol is a set of rules and standards that govern how devices communicate with each other over a wireless network. Wireless protocols specify the technical details of how devices transmit and receive data, including the type of wireless technology used, the frequency bands and channels used for communication, and the data rates and transmission ranges supported.

There are several different types of wireless protocols, including:

1. IEEE 802.11: This is a family of wireless networking protocols that is commonly used for Wi-Fi networks. It includes several different versions, such as 802.11b, 802.11g, and 802.11n, which define the technical details of how the Wi-Fi network operates and the features and capabilities of the network.
2. Bluetooth: This is a wireless protocol that is commonly used for short-range communication between devices such as headphones, speakers, and personal devices. Bluetooth uses a low-power radio frequency to transmit data over short distances and can be used to connect devices without the need for physical cables or wires.
3. Zigbee: This is a wireless protocol that is commonly used for low-power, low-data-rate communication between devices such as sensors, smart home devices, and industrial automation systems. Zigbee uses a low-power radio frequency to transmit data over short distances and is designed to be energy-efficient.
4. Cellular: This is a wireless protocol that is used for mobile communication and data transfer over long distances. Cellular communication uses a network of cell towers and antennas to transmit

data and is commonly used for mobile phone communication and mobile data transfer.

(b) What is Soft Handoff in Wireless Systems? **04**

Soft handoff is a process used in wireless communication systems to improve the continuity of service and the quality of communication when a mobile device moves between cells or coverage areas. In a soft handoff, the mobile device maintains a connection to multiple cells or base stations at the same time, allowing it to seamlessly switch between them as it moves around.

The process of soft handoff involves several steps:

1. The mobile device establishes a connection with a base station or cell and begins transmitting and receiving data.
2. As the mobile device moves out of the coverage area of the initial cell, it begins to establish a connection with a new base station or cell.
3. The mobile device maintains both connections simultaneously, allowing it to continue transmitting and receiving data without interruption.
4. As the mobile device moves closer to the new cell, the connection with the initial cell is gradually phased out, and the connection with the new cell becomes stronger.
5. When the connection with the initial cell is completely terminated, the mobile device is fully connected to the new cell and continues to transmit and receive data.

Soft handoff helps to improve the continuity of service and the quality of communication for mobile devices, as it allows them to maintain a connection even when they are moving between cells or coverage areas. It is an important feature of modern wireless communication systems and is used to provide reliable and seamless communication for users.

Explain the GSM Architecture.

GSM (Global System for Mobile Communications) is a widely-used mobile communication system that provides voice and data services to mobile devices. The GSM architecture consists of several different components, including:

1. Mobile station (MS): This is the mobile device that is used by the user to access the GSM network. It includes a SIM (Subscriber Identity Module) card, which stores the user's subscription information and enables the device to connect to the GSM network.
2. Base station subsystem (BSS): This includes the base transceiver stations (BTS) and the base station controllers (BSC) that are used to transmit and receive signals between the mobile devices and the network. The BTS is

(c) Explain the GSM Architecture. **07**

GSM (Global System for Mobile Communications) is a widely-used mobile communication system that provides voice and data services to mobile devices. The GSM architecture consists of several different components, including:

1. Mobile station (MS): This is the mobile device that is used by the user to access the GSM network. It includes a SIM (Subscriber Identity Module) card, which stores the user's subscription information and enables the device to connect to the GSM network.
2. Base station subsystem (BSS): This includes the base transceiver stations (BTS) and the base station controllers (BSC) that are used to transmit and receive signals between the mobile devices and the network. The BTS is responsible for transmitting and receiving signals to and from the mobile devices within its coverage area, while the BSC is responsible for managing the BTS and coordinating communication between the mobile devices and the network.
3. Network and Switching Subsystem (NSS): This includes the mobile switching center (MSC) and the home location register (HLR), which are responsible for switching calls and providing services to the mobile devices. The MSC is responsible for routing calls and messages between the mobile devices and the rest of the network, while the HLR stores the subscription and location information for each mobile device.
4. Operation and Support Subsystem (OSS): This includes the various systems and processes that are used to support and maintain the GSM network, including the authentication center (AUC), the equipment identity register (EIR), and the billing systems. The AUC is responsible for verifying the authenticity of the SIM card and the mobile device, while the EIR is used to track and manage the equipment used in the network. The billing systems are used to track and charge for the use of the network and the services provided by the network.

Overall, the GSM architecture is designed to provide reliable and efficient communication services to mobile devices and to support the various functions and processes required to operate the network. It has become the dominant mobile communication system in many parts of the world and has been the foundation for the development of many other mobile communication systems.

OR

Q.3 **(a)** Explain the Difference LAN and WLAN. **03**

Feature	LAN	WLAN
Definition	A network that connects devices in a local area, such as an office or home	A wireless version of a LAN, which connects devices in a local area using wireless technology
Connection type	Physical cables	Wireless
Coverage area	Limited to the local area	Limited to the local area
Maximum distance	Typically up to 100 meters	Typically up to 100 meters
Data transfer rate	Faster than WLAN	Slower than LAN
Security	Generally more secure than WLAN	Generally, less secure than LAN
Cost	Generally cheaper than WLAN	Generally, more expensive than LAN
Examples of devices	Computers, printers, routers,	Computers, smartphones, tablets,
	switches, hubs	printers, routers, switches, hubs

(b) Explain the Indoor and outdoor propagation models. **04**

Propagation models are mathematical models that are used to predict the behavior of electromagnetic waves as they propagate through different environments. They are used to understand how the signal strength and quality of a wireless communication system may be affected by the characteristics of the environment, including the type of materials and objects present, the distance between the transmitter and receiver, and the presence of any obstacles or reflections.

There are two main types of propagation models: indoor and outdoor.

Indoor propagation models are used to predict the behavior of electromagnetic waves as they propagate through indoor environments, such as buildings and homes. These models take into account the characteristics of the materials and objects present in the indoor environment, such as walls, floors, and furniture, as well as the presence of any obstacles or reflections. Indoor propagation models are useful for understanding how the signal strength and quality of a wireless communication system may be affected by the layout and materials of the indoor environment.

Outdoor propagation models are used to predict the behavior of electromagnetic waves as they propagate through outdoor environments, such as streets, fields, and forests. These models take into account the characteristics of the terrain and the atmosphere, as well as the presence of any obstacles or reflections. Outdoor propagation models are useful for understanding how the signal strength and quality of a wireless communication system may be affected by the terrain and atmospheric conditions of the outdoor environment.

(c) Explain the GPRS Architecture. **07**

GPRS (General Packet Radio Service) is a wireless communication system that provides data transfer and internet access for mobile devices. It is an evolution of the GSM (Global System for Mobile Communications) system

and is designed to support higher data rates and more efficient data transfer.

The GPRS architecture consists of several different components, including:

1. Mobile station (MS): This is the mobile device that is used by the user to access the GPRS network. It includes a SIM (Subscriber Identity Module) card, which stores the user's subscription information and enables the device to connect to the GPRS network.
2. Base station subsystem (BSS): This includes the base transceiver stations (BTS) and the base station controllers (BSC) that are used to transmit and receive signals between the mobile devices and the network. The BTS is responsible for transmitting and receiving signals to and from the mobile devices within its coverage area, while the BSC is responsible for managing the BTS and coordinating communication between the mobile devices and the network.
3. Network and Switching Subsystem (NSS): This includes the mobile switching center (MSC) and the home location register (HLR), which are responsible for switching calls and providing services to the mobile devices. The MSC is responsible for routing calls and messages between the mobile devices and the rest of the network, while the HLR stores the subscription and location information for each mobile device.
4. Gateway GPRS Support Node (GGSN): This is a network element that connects the GPRS network to other networks, such as the internet. It is responsible for routing data packets between the GPRS network and the other networks and for translating between different protocols.
5. Serving GPRS Support Node (SGSN): This is a network element that is responsible for managing the connection between the mobile devices and the GPRS network. It is responsible for tracking the location of the mobile devices, maintaining the connection with the mobile devices, and routing data packets between the mobile devices and the GPRS network.

Q.4 (a) Explain the CDMA features. (Any Four) **03**

1. Multiple Access: CDMA (Code Division Multiple Access) is a multiple access technique that allows multiple devices to share the same frequency spectrum by assigning each device a unique code. This allows multiple devices to transmit simultaneously without interfering with each other.
2. Spread Spectrum: CDMA uses spread spectrum technology to spread the data signal over a wide frequency band. This helps to reduce interference and improve the capacity of the communication system.
3. Interference Rejection: CDMA uses advanced algorithms to reject interference and noise, which helps to improve the quality and reliability of the communication system.
4. Multiple User Detection: CDMA is able to detect and separate multiple users transmitting on the same frequency, allowing them to communicate simultaneously without interference.
5. Power Control: CDMA uses power control algorithms to adjust the power of the transmitted signal in order to optimize the use of the available frequency spectrum and reduce interference.
6. Handoff: CDMA supports seamless handoff between cells, allowing mobile devices to move between coverage areas without interrupting their communication.

(b) Write Short Note: ZigBee Networks **04**

ZigBee is a wireless communication protocol that is designed for low-power, low-data-rate communication between devices such as sensors, smart home devices, and industrial automation systems. It uses a low-power radio frequency to transmit data over short distances and is designed to be energy-efficient.

ZigBee networks are self-organizing and self-healing, which means that they can automatically adjust to changes in the network environment and recover from disruptions. They are also highly scalable, allowing them to support a large number of devices on a single network.

ZigBee supports a variety of networking topologies, including star, tree, and mesh, which allows it to be used in a variety of different applications and environments. It is also interoperable with other wireless technologies, such as Wi-Fi and Bluetooth, which allows it to be used in conjunction with these technologies in a variety of different applications.

Overall, ZigBee is a widely-used wireless communication protocol that is known for its low power consumption, low data rates, and reliability. It is an important technology in the Internet of Things (IoT) and is used in a variety of applications, including smart home systems, industrial automation, and environmental monitoring.

(c) Explain the Authentication and security in GSM **07**

Authentication and security are important aspects of the GSM (Global System for Mobile Communications) mobile communication system. GSM uses several different mechanisms to authenticate users and protect the confidentiality and integrity of communication over the network.

Authentication:

1. SIM (Subscriber Identity Module) card: The SIM card is a small smart card that is inserted into the mobile device and stores the user's subscription information. It is used to authenticate the user and authorize access to the network.
2. Authentication center (AUC): The AUC is a network element that is responsible for verifying the authenticity of the SIM card and the mobile device. It uses a secret key that is stored on the SIM card and shared between the mobile device and the AUC to authenticate the user.

Security:

1. Encryption: GSM uses encryption to protect the confidentiality of communication over the network. It uses a variety of encryption algorithms, such as A5/1 and A5/3, to encode the data transmitted over the network.
2. Integrity protection: GSM uses integrity protection mechanisms to ensure the integrity of the data transmitted over the network. It uses a variety of techniques, such as message authentication codes (MACs) and cyclic redundancy checks (CRCs), to detect and prevent the tampering of data.
3. Access control: GSM uses access control mechanisms to restrict access to the network and to prevent unauthorized use. It uses a variety of techniques, such as subscription-based access and network-based access control, to ensure that only authorized users can access

the network.

OR

Q.4 (a) Write Short Note: Hand Over **03**

Handover, also known as handoff, is a process that is used in wireless communication systems to transfer a connection from one cell or base station to another as a mobile device moves around. It is an important feature of modern wireless communication systems, as it allows mobile devices to maintain a connection even when they are moving between cells or coverage areas.

There are two main types of handover:

1. Hard handover: This is a process in which the connection with the current cell or base station is terminated before a connection is established with a new cell or base station. Hard handover is generally used in systems with low mobility, as it requires a strong and stable connection to be established with the new cell before the connection with the old cell is terminated.
2. Soft handover: This is a process in which the connection with the current cell or base station is maintained while a connection is established with a new cell or base station. Soft handover allows the mobile device to maintain a connection with both cells or base stations simultaneously, allowing it to seamlessly switch between them as it moves around. Soft handover is generally used in systems with high mobility, as it allows the mobile device to maintain a connection even when it is moving between cells or coverage areas.

(b) Explain the Security issues and challenges in a Wireless network. **04**

Wireless networks present a number of security issues and challenges that must be addressed in order to protect against unauthorized access and ensure the confidentiality and integrity of the communication. Some of the main security issues and challenges in a wireless network include:

1. Unauthorized access: Wireless networks are vulnerable to unauthorized access, as they use wireless signals that can be intercepted and accessed by anyone with a wireless device within range. This can lead to unauthorized users gaining access to the network and potentially compromising its security.
2. Eavesdropping: Wireless networks are vulnerable to eavesdropping, as the wireless signals can be intercepted and monitored by anyone with the right equipment. This can lead to the confidentiality of communication being compromised, as the intercepted data may be sensitive or confidential.
3. Man-in-the-middle attacks: Wireless networks are vulnerable to man-in-the-middle attacks, in which an attacker intercepts and alters the communication between two parties. This can lead to the integrity of the communication being compromised and the parties being misled or deceived.
4. Denial-of-service attacks: Wireless networks are vulnerable to denial-of-service attacks, in which an attacker floods the network with traffic in an attempt to overwhelm it and prevent legitimate users from accessing it.
5. Weak encryption: Wireless networks may use weak encryption algorithms or keys, which can make them vulnerable to being hacked and the data transmitted over the network being compromised.

Overall, wireless networks present a number of security issues and challenges that must be addressed in order to protect against unauthorized access and ensure the confidentiality and integrity of the communication. It is important for organizations to implement robust security measures and to regularly update and maintain them in order to protect against these threats.

(c) What is UWB Radio? Explain in Detail. **07**

UWB (Ultra-Wideband) radio is a wireless communication technology that uses very low-power, high-frequency signals to transmit data over short distances. It is characterized by its wide bandwidth, which allows it to transmit large amounts of data with low power consumption and low interference.

UWB radio operates in the unlicensed frequency bands, typically between 3.1 GHz and 10.6 GHz, and uses a pulse-based modulation scheme to transmit data. The pulse-based modulation allows UWB radio to transmit data at a very high rate, with data rates of up to several gigabits per second being possible.

UWB radio is well-suited for a variety of applications, including short-range wireless data transfer, location tracking, and high-precision ranging. It is used in a variety of different industries, including consumer electronics, healthcare, and industrial automation.

UWB radio has several advantages over other wireless communication technologies, including:

1. High data rates: UWB radio is capable of transmitting data at very high rates, making it suitable for applications that require fast data transfer.
2. Low power consumption: UWB radio uses very low-power signals, making it an energy-efficient choice for applications that require long battery life.
3. Low interference: UWB radio uses a wide bandwidth and a pulse-based modulation scheme, which helps to reduce interference with other wireless systems.
4. High-precision ranging: UWB radio is capable of providing high-precision ranging and location information, making it suitable for applications such as indoor positioning and asset tracking.

Q.5 (a) Write a short Note : Bluetooth **03**

Bluetooth is a wireless communication technology that is used to connect devices over short distances. It uses a low-power radio frequency to transmit data and is designed to be energy-efficient. Bluetooth is widely used in a variety of devices, including smartphones, tablets, laptops, and smart home devices, and is known for its ease of use and compatibility with a wide range of devices.

Bluetooth is based on the IEEE 802.15.1 standard and operates in the unlicensed 2.4 GHz frequency band. It uses a variety of protocols and techniques to transmit data, including frequency-hopping spread spectrum and time-division multiplexing.

Bluetooth supports a variety of networking topologies, including point-to-

point, point-to-multipoint, and mesh, and is able to support a large number of devices on a single network. It is also interoperable with other wireless technologies, such as Wi-Fi and ZigBee, which allows it to be used in conjunction with these technologies in a variety of different applications.

(b) Write a short Note : Personal Area Network **04**

A personal area network (PAN) is a type of computer network that is used to connect devices in close proximity to each other, typically within a range of a few meters. PANs are used to connect devices such as laptops, smartphones, tablets, and smart home devices, and are often used to exchange data and enable device control.

There are several technologies that can be used to create a PAN, including Bluetooth, infrared, and NFC (Near Field Communication). These technologies use a variety of protocols and techniques to transmit data and enable device communication.

PANs are often used to connect devices that are used by a single person, such as a laptop and a smartphone, and are designed to be easy to set up and use. They are an important part of the Internet of Things (IoT) and are used in a variety of applications, including wireless audio, data transfer, and device control.

(c) Explain the Wireless Ad Hoc Network and Mobile Portability. **07**

A wireless ad hoc network is a type of wireless network that is formed spontaneously and does not require a central infrastructure or access point. In an ad hoc network, the devices communicate directly with each other and form a network on the fly, without the need for a central coordinating device or access point.

Ad hoc networks are often used in situations where a traditional network infrastructure is not available, such as in disaster recovery situations or in remote or rural areas. They are also used in applications where mobility is a requirement, such as in military operations or in emergency response situations.

Mobile portability, also known as mobility management, is the ability of a wireless communication system to support the movement of mobile devices within and between cells or coverage areas. Mobile portability allows mobile devices to maintain a connection and access services as they move around, even if they are outside of the coverage area of their home network.

There are several different techniques that can be used to support mobile portability, including:

1. Handover: This is a process in which the connection with the current cell or base station is transferred to a new cell or base station as the mobile device moves around. Handover allows the mobile device to maintain a connection and access services as it moves between cells or coverage areas.
2. Roaming: This is the ability of a mobile device to access services and communicate with other devices outside of its home network. Roaming allows mobile devices to access services and communicate with other devices in other countries or regions.

OR

Q.5 (a) Explain the Small scale multipath propagation. **03**

Small-scale multipath propagation refers to the phenomenon of a wireless signal being reflected, refracted, and scattered as it travels through a wireless communication environment. This can result in multiple copies of the signal arriving at the receiver at different times and with different amplitudes, which can cause interference and degradation of the signal.

Small-scale multipath propagation is a common problem in wireless communication systems and is caused by a variety of factors, including reflections from objects and surfaces, refraction through layers of different materials, and scattering from small irregularities in the environment.

Small-scale multipath propagation can have a significant impact on the performance of a wireless communication system, as it can cause interference, fading, and reduced signal-to-noise ratio. It can also make it difficult to accurately determine the location of a device, as the multipath signals can cause errors in the position estimate.

There are several techniques that can be used to mitigate the effects of small-scale multipath propagation, including:

1. Diversity techniques: These techniques use multiple antennas or multiple paths to transmit and receive the signal, which can help to reduce the impact of fading and interference caused by multipath propagation.
2. Channel estimation: This involves using algorithms to estimate the characteristics of the channel, such as the delay, phase, and amplitude of the multipath signals. This information can be used to cancel or mitigate the effects of the multipath signals.
3. Multipath fading compensation: This involves using algorithms to estimate the multipath fading and compensate for it, which can help to improve the performance of the communication system.

(b) Explain the cell Splitting and cell sectorization. **04**

ell splitting and cell sectorization are techniques that are used to improve the coverage and capacity of a wireless communication system. They are used to divide a cell or coverage area into smaller areas, which can help to reduce interference, increase capacity, and improve the quality of service for users.

Cell splitting involves dividing a single cell into two or more smaller cells, each with its own base station. This can help to reduce interference and increase capacity, as more users can be served by the network.

Cell sectorization involves dividing a cell into smaller sectors, each with its own base station and antenna. This can help to reduce interference and increase capacity, as the base station can transmit and receive signals from different directions and serve multiple users simultaneously.

Both cell splitting and cell sectorization can help to improve the performance and capacity of a wireless communication system, but they also have some drawbacks. They can be expensive to implement and may require the deployment of additional base stations and antennas. They may also require the allocation of additional frequency bands, which can be a limited resource.

(c) Explain Hexagonal geometry cell and concept of frequency reuse, **07**

Hexagonal geometry cells are a common arrangement used in cellular wireless communication systems to divide a coverage area into smaller cells or sectors. In this arrangement, the coverage area is divided into a grid of hexagonal cells, each with its own base station. The base stations are typically located at the center of the cells and use antennas to transmit and receive signals within the cell.

The concept of frequency reuse refers to the use of the same frequency band in multiple cells or sectors within a wireless communication system. In order to increase capacity and improve the performance of the system, the same frequency band can be used in multiple cells or sectors, provided that the cells are spaced far enough apart to avoid interference.

The hexagonal geometry of the cells and the concept of frequency reuse are closely related, as the hexagonal shape of the cells allows for a more efficient use of the available frequencies. By using a hexagonal cell arrangement and carefully controlling the spacing between cells, it is possible to reuse the same frequency band in multiple cells while minimizing interference.

To optimize the use of the available frequencies and minimize interference, the spacing between cells is carefully controlled in a cellular wireless communication system. This is typically done using a frequency reuse factor, which determines how many cells can reuse the same frequency band. A frequency reuse factor of 1 means that the same frequency band is used in every cell, while a higher frequency reuse factor means that the same frequency band is used in fewer cells.

Overall, the hexagonal geometry of the cells and the concept of frequency reuse are important considerations in the design and operation of a cellular wireless communication system. They are used to optimize the use of the available frequencies and improve the performance and capacity of the system.

****

Seat No.: XXXXXXX Enrolment No. XXXXXXX

GUJARAT TECHNOLOGICAL UNIVERSITY

BE - SEMESTER–VII (NEW) EXAMINATION – SUMMER 2022

Subject Code:3171608 Date:01/06/2022

Subject Name: Wireless Communication

Time: 02:30 PM TO 05:00 PM Total Marks: 70

Instructions:

1. **Attempt all questions.**
2. **Make suitable assumptions wherever necessary.**
3. **Figures to the right indicate full marks.**
4. **Simple and non-programmable scientific calculators are allowed.**

Q.1 **(a)** Why hexagonal cell shape is preferred in cellular architecture? **03**

There are several reasons why hexagonal cell shapes are often preferred in cellular architecture:

1. Efficiency: Hexagonal cell shapes provide a more efficient use of space compared to other shapes like square or triangular cells. This is because hexagons can pack together more tightly without any gaps, resulting in a higher density of cells in a given area.
2. Symmetry: Hexagonal cells have rotational symmetry, which means that they look the same no matter how they are rotated. This property makes it easier to design and build networks using hexagonal cells.
3. Strength: Hexagonal cells are also stronger and more stable than other shapes because their sides are evenly distributed around a central point. This makes them less prone to deformation or collapse under load.
4. Communication: In cellular communication networks, hexagonal cell shapes are often used to create a regular pattern of coverage that can be easily predicted and planned for. This allows for more efficient use of resources and better overall coverage.

(b) Explain the concept of frequency reuse in cellular system **04**

Frequency Reuse is the scheme in which allocation and reuse of channels throughout a coverage region is done. Each cellular base station is allocated a group of radio channels or Frequency sub-bands to be used within a small geographic area known as a cell. The shape of the cell is Hexagonal. The process of selecting and allocating the frequency sub-bands for all of the cellular base station within a system is called **Frequency reuse** or **Frequency Planning**.

Salient features of using Frequency Reuse:

- Frequency reuse improve the spectral efficiency and signal Quality (QoS).
- Frequency reuse classical scheme proposed for GSM systems offers a protection against interference.
- The number of times a frequency can be reused is depend on the tolerance capacity of the radio channel from the nearby transmitter that is using the same frequencies.
- In Frequency Reuse scheme, total bandwidth is divided into

different sub-bands that are used by cells.
- Frequency reuse scheme allow WiMax system operators to reuse the same frequencies at different cell sites.

(c) Draw and Explain GSM system architecture. **07**

The Global System for Mobile Communications (GSM) is a standard for mobile telephony that was developed to replace the analog cellular networks that were in use in the 1980s. The GSM system architecture is made up of several different components, including the following:

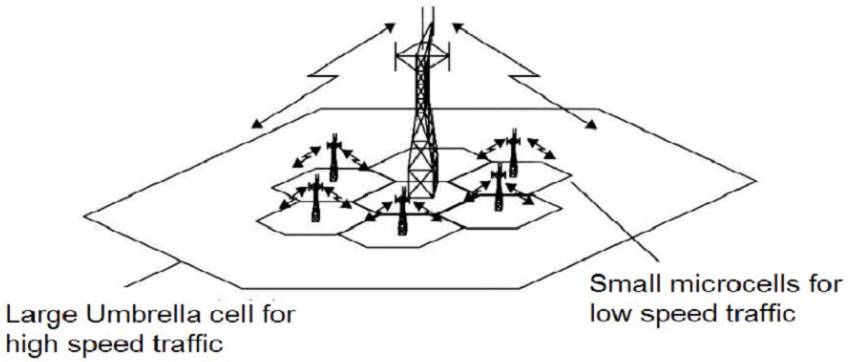
1. Mobile Station (MS): This is the device that the user carries, such as a mobile phone or a wireless device. The MS is responsible for transmitting and receiving voice and data signals over the network.
2. Base Station Subsystem (BSS): This is the infrastructure that connects the MS to the network. It consists of two main components: the Base Transceiver Station (BTS) and the Base Station Controller (BSC). The BTS is responsible for managing the radio frequency (RF) communication between the MS and the network, while the BSC is responsible for managing the communication between the BTS and the network core.
3. Network Switching Subsystem (NSS): This is the central component of the GSM network, responsible for switching and routing calls and data between different MSs and other networks. It consists of a Mobile Switching Center (MSC) and a Home Location Register (HLR). The MSC is responsible for switching calls and data between the BSS and other networks, while the HLR is a database that stores information about each MS, including its location and capabilities.
4. Operation Support Subsystem (OSS): This component of the GSM network is responsible for maintaining and managing the network, including tasks such as provisioning, billing, and fault management. It consists of various subsystems, such as the Equipment Identity Register (EIR), the Authentication Center (AuC), and the Visitor Location Register (VLR).

In summary, the GSM system architecture consists of the following components: mobile stations (MSs), base station subsystems (BSSs) that include base transceiver stations (BTSs) and base station controllers (BSCs), a network switching subsystem (NSS) that includes a mobile switching center (MSC) and a home location register (HLR), and an operation support subsystem (OSS) that includes various subsystems such as the equipment identity register (EIR), the authentication center (AuC), and the visitor location register (VLR). These components work together to provide mobile telephony services to users.

Q.2 **(a)** Explain the concept of umbrella cell. **03**

An umbrella cell is a type of cell in a mobile communication network that covers a large geographic area and provides coverage to a large number of mobile devices. It is called an "umbrella" cell because it is typically used to provide coverage over a wide area, like an umbrella providing shelter from the rain.

In a cellular network, the coverage area of each cell is determined by the location and power of the base station that serves the cell. Umbrella cells are typically used in areas where the demand for mobile services is high, such as in urban areas or along major transportation corridors. They are also used to provide coverage in areas where it is not practical or cost-effective to install a large number of smaller cells, such as in rural or remote areas.

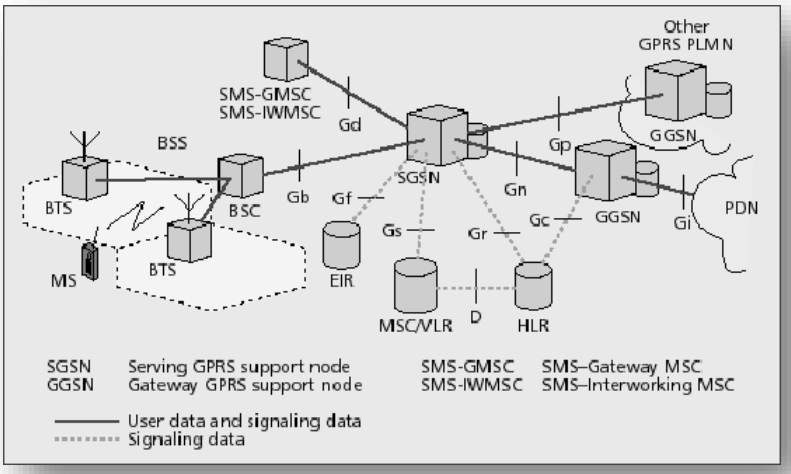


(b) Compare Wi-Fi and Wi-max technology. **04**

Here is a comparison of Wi-Fi and WiMAX technology in table form:

Feature	**Wi-Fi**	**WiMAX**
Definition	A wireless networking technology that uses radio waves to provide Internet access to devices within a limited range	A wireless networking technology that uses radio waves to provide high-speed Internet access over a wide area, such as a city or a region
Range	Typically covers a range of about 100 meters (328 feet)	Can cover a range of up to 50 kilometers (31 miles)
Bandwidth	Typically provides bandwidth of up to 54 megabits per second (Mbps)	Can provide bandwidth of up to 75 Mbps
Frequency	Operates at a frequency of 2.4 GHz or 5 GHz	Operates at a frequency of 2.5 GHz, 3.5 GHz, or 5.8 GHz
Mobility	Provides limited mobility, as devices must remain within range of the Wi-Fi access point	Provides high mobility, as devices can move freely within the coverage area
Security	Provides security through the use of encryption protocols such as WPA2	Provides security through the use of encryption protocols such as WPA2 and IEEE 802.16e

(c) With the help of a neat sketch, describe GPRS architecture. **07**



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.

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 charging for the use of the air interface.

OR

(c) Briefly explain knife-edge diffraction model. **07**

The knife-edge diffraction model is a mathematical model used to predict the behavior of electromagnetic waves as they pass through or around obstacles. It is based on the principle of diffraction, which describes how waves bend and spread as they pass through small openings or around obstacles.

The knife-edge diffraction model is often used to predict the strength and pattern of the electromagnetic field at a point on the far side of an obstacle, such as a building or a hill. The model assumes that the obstacle is a sharp edge or a thin strip, and it calculates the diffraction of the wave as it passes over or around the obstacle.

The knife-edge diffraction model is useful for predicting the behavior of radio waves in urban environments, where there are many obstacles that can affect the strength and coverage of the signal. It is also used in the design of wireless communication systems, such as cellular networks, to ensure that the signal can reach all areas of the coverage area.

Q.3 **(a)** Define: (1) Control Channel **03**
(2) Dwell time
(3) Full Duplex Systems

(1) Control Channel: In a communication system, a control channel is a dedicated channel that is used for transmitting control signals and information. It is separate from the channels that are used for transmitting data or voice signals. Control channels are used to establish and maintain communication between devices, and they can be used for tasks such as signaling, handshaking, and synchronization.

(2) Dwell time: In a communication system, the dwell time is the amount of time that a device spends receiving or transmitting on a particular frequency or channel. In a mobile communication system, the dwell time is an important factor that can affect the performance and efficiency of the system. For example, a device with a long dwell time may be less efficient at transmitting and receiving data, as it spends more time on a single frequency or channel.

(3) Full Duplex Systems: A full duplex system is a communication system that allows devices to transmit and receive signals simultaneously over the same channel. This means that the devices can communicate with each other at the same time, in both directions. Full duplex systems are often used in telephony and other two-way communication systems, as they allow for real-time, interactive communication between devices.

In summary:

- A control channel is a dedicated channel used for transmitting control signals and information in a communication system.
- The dwell time is the amount of time that a device spends receiving or transmitting on a particular frequency or channel.
- A full duplex system is a communication system that allows devices to transmit and receive signals simultaneously over the same channel.

(b) Write short note on: Bluetooth. **04**

Bluetooth is a wireless technology that allows devices to communicate with each other over short distances using radio waves. It was developed in the late 1990s as a way for devices to communicate with each other without the need for cables or other physical connections.

Bluetooth operates in the 2.4 GHz frequency band and uses a technique called frequency-hopping spread spectrum to transmit data. It is designed to be low-power and low-cost, and it is commonly used in devices such as mobile phones, laptops, and headsets.

Bluetooth devices communicate with each other using a wireless connection called a piconet, which consists of a master device and up to seven slave devices. The master device controls the connection and determines which slave devices are allowed to transmit data.

Bluetooth has a number of different applications, including file transfer, wireless networking, and wireless audio. It is also used in a variety of consumer and industrial products, such as smart watches, fitness trackers, and industrial automation systems.

In summary, Bluetooth is a wireless technology that allows devices to communicate with each other over short distances using radio waves. It is low-power, low-cost, and commonly used in a wide range of consumer and industrial products.

(c) Discuss the fixed channel allocation, Channel borrowing and dynamic channel allocation techniques in cellular systems. **07**

In a cellular communication system, the available frequency spectrum is divided into a number of channels, which are used to transmit data and voice signals between the mobile devices and the network. There are several different techniques that can be used to allocate these channels to the cells in the network. These techniques include fixed channel allocation, channel borrowing, and dynamic channel allocation.

1. Fixed channel allocation: In fixed channel allocation, each cell in the network is assigned a fixed set of channels that it can use to communicate with mobile devices. These channels are typically chosen based on the expected traffic demand in the cell and the available frequency spectrum. The advantage of fixed channel allocation is that it is simple and easy to implement, as the channels are assigned to the cells in advance and do not need to be reallocated. However, it can be

inflexible and may not be able to adapt to changing traffic conditions.

2. Channel borrowing: In channel borrowing, cells can borrow channels from neighboring cells when they need additional capacity. This allows cells with low traffic demand to share their unused channels with cells that are experiencing high traffic demand. The advantage of channel borrowing is that it can increase the overall capacity of the network and make better use of the available frequency spectrum. However, it can also lead to interference between cells and may require additional signaling between cells to coordinate the borrowing of channels.
3. Dynamic channel allocation: In dynamic channel allocation, the channels are assigned to the cells on an as-needed basis, based on the current traffic demand in each cell. This allows the network to adjust to changing traffic conditions and allocate resources more efficiently. The advantage of dynamic channel allocation is that it can improve the capacity and efficiency of the network, but it can also be more complex and require more sophisticated signaling and control mechanisms.

OR

Q.3 **(a)** Briefly describe Hand-off strategies in cellular system. **03**

In cellular telecommunications, the terms **handover** or **handoff** refers to the process of transferring ongoing call or data connectivity from one Base Station to other Base Station. When a mobile moves into the different cell while the conversation is in progress then the MSC (Mobile Switching Center) transfer the call to a new channel belonging to the new Base Station.

When a mobile user A moves from one cell to another cell then BSC 1 signal strength loses for the mobile User A and the signal strength of BSC 2 increases and thus ongoing calls or data connectivity for mobile user goes on without interrupting.

Types of Handoffs:

Hard Handoff:
When there is an actual break in the connectivity while switching from one Base Station to another Base Station. There is no burden on the Base Station and MSC because the switching takes place so quickly that it can hardly be noticed by the users. The connection quality is not that good. Hard Handoff adopted the ‘break before make’ policy.

Soft Handoff:
In Soft Handoff, at least one of the links is kept when radio signals are added or removed to the Base Station. Soft Handoff adopted the ‘make before break’ policy. Soft Handoff is more costly than Hard Handoff.

(b) Compare TDMA, FDMA and CDMA techniques. **04**

FDMA	TDMA	CDMA
FDMA stands for Frequency Division Multiple Access.	TDMA stands for Time Division Multiple Access.	CDMA stands for Code Division Multiple Access.
In this, sharing of bandwidth among different stations takes place.	In this, only the sharing of time of satellite transponder takes place.	In this, there is sharing of both i.e. bandwidth and time among different stations takes place.
There is no need of any codeword.	There is no need of any codeword.	Codeword is necessary.
In this, there is only need of guard bands between the adjacent channels are necessary.	In this, guard time of the adjacent slots are necessary.	In this, both guard bands and guard time are necessary.
Synchronization is not required.	Synchronization is required.	Synchronization is not required.
The rate of data is low.	The rate of data is medium.	The rate of data is high.
Mode of data transfer is continuous signal.	Mode of data transfer is signal in bursts.	Mode of data transfer is digital signal.
It is little flexible.	It is moderate flexible.	It is highly flexible.

(c) Explain the hidden-node problem and exposed-node problem in context of mobile ad-hoc networks. **07**

In a mobile ad-hoc network (MANET), a hidden-node problem occurs when two nodes are able to communicate with a third node, but they are unable to communicate directly with each other because they are out of range or obstructed by an obstacle. This can cause problems in the network because the two nodes may transmit data simultaneously, resulting in a collision that can cause errors and reduce the efficiency of the network.

The hidden-node problem can be particularly challenging in a MANET because the nodes are constantly moving and changing their positions, which can make it difficult to predict and avoid collisions. One solution to the hidden-node problem is to use a protocol that allows nodes to coordinate their transmissions and avoid colliding with each other, such as the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol.

The exposed-node problem is a related issue that occurs when a node is able to communicate with another node, but it is not able to communicate with the rest of the network because it is too far away or obstructed by an obstacle. This can create a "black hole" in the network, as the node is able to receive data but is not able to transmit it to other nodes.

The exposed-node problem can be solved by using relay nodes or mesh routing protocols that allow data to be forwarded from one node to another. These techniques can help to extend the range and coverage of the network and ensure that all nodes are able to communicate with each other.

Q.4 **(a)** Explain channel assignment strategies. **03**

Channel Allocation means to allocate the available channels to the cells in a cellular system. When a user wants to make a call request then by using channel allocation strategies their requests are fulfilled. Channel Allocation Strategies are designed in such a way that there is efficient use of frequencies, time slots and bandwidth.

Types of Channel Allocation Strategies:

These are Fixed, Dynamic, and Hybrid Channel Allocation as explained as following below.

- **Fixed Channel Allocation (FCA):**
  Fixed Channel Allocation is a strategy in which fixed number of channels or voice channels are allocated to the cells. Once the channels are allocated to the specific cells then they cannot be changed. In FCA channels are allocated in a manner that maximize *Frequency reuse*.
- **Dynamic Channel Allocation (DCA):**
  Dynamic Channel allocation is a strategy in which channels are not permanently allocated to the cells. When a User makes a call request then Base Station (BS) send that request to the Mobile Station Center (MSC) for the allocation of channels or voice channels. This way the likelihood of blocking calls is reduced. As traffic increases more channels are assigned and vice-versa.
- **Hybrid Channel Allocation (HCA):**
  Hybrid Channel Allocation is a combination of both Fixed Channel Allocation (FCA) and Dynamic Channel Allocation (DCA). The total number of channels or voice channels are divided into fixed and dynamic set.

(b) Discuss the concept of spread spectrum. **04**

Spread spectrum is a technique used to transmit data over a communication channel in a way that spreads the data over a wider frequency band. It is used in a variety of communication systems, including wireless networks, satellite systems, and radar systems.

There are several different types of spread spectrum, including frequency-hopping spread spectrum (FHSS), direct-sequence spread spectrum (DSSS), and chirp spread spectrum (CSS). In FHSS, the data is transmitted by rapidly switching between different frequencies within the frequency band. In DSSS, the data is transmitted by modulating it with a spread spectrum code, which is a sequence of pseudorandom binary digits (bits). In CSS, the data is transmitted by modulating the frequency of the signal over a wide range.

Spread spectrum has several advantages over other techniques, including the following:

1. Resistance to interference: Because the data is spread over a wide frequency band, it is less vulnerable to interference from other sources.
2. Security: Spread spectrum techniques can be used to encode the data, which makes it more difficult for unauthorized users to intercept and decode the transmission.
3. Capacity: Spread spectrum techniques can increase the capacity of a communication system by allowing multiple

users or devices to share the same frequency band.
4. Robustness: Spread spectrum techniques can improve the robustness of a communication system by allowing it to recover from errors or interference.

(c) Explain the working of UWB radio. Discuss the features, advantages and disadvantages of UWB technology. **07**

Ultra-wideband (UWB) radio is a type of wireless communication technology that uses very short pulses of radio frequency (RF) energy to transmit data over a wide frequency band. UWB technology is characterized by its very wide bandwidth, which can be hundreds of megahertz or even gigahertz in some cases.

UWB radio works by transmitting extremely short pulses of RF energy, which can be as short as a few nanoseconds in duration. These pulses are spread over a very wide frequency band, which allows them to carry a large amount of data. UWB radio is able to transmit data over a wide frequency range because it uses a special type of modulation called pulse-position modulation (PPM), which encodes the data by varying the timing of the pulses rather than their amplitude or frequency.

UWB technology has several features and characteristics that distinguish it from other wireless communication technologies:

- Very wide bandwidth: UWB technology uses a very wide bandwidth, which allows it to transmit a large amount of data in a short period of time.
- Low power: UWB technology uses very low power levels, which makes it suitable for use in devices with limited battery life.
- Short range: UWB technology has a relatively short range, typically a few meters or less, which makes it suitable for use in close proximity applications.
- High resolution: UWB technology can provide high spatial and temporal resolution, which makes it useful for applications such as radar and location tracking.

Some advantages of UWB technology include:

- High data rates: UWB technology can achieve very high data rates, making it suitable for applications that require a lot of bandwidth.
- Low interference: Because UWB signals have such a wide bandwidth, they are less likely to interfere with other signals in the same frequency band.
- High security: UWB signals are difficult to detect and intercept, which makes them suitable for use in secure communication systems.

Some disadvantages of UWB technology include:

- Short range: The short range of UWB signals limits their use to applications that require communication over a small area.
- Complexity: UWB technology can be complex to implement, as it requires specialized hardware and software.
- Limited availability: UWB technology is not as widely available as other wireless technologies, and it may not be supported by all devices.

OR

Q.4 **(a)** Explain: I-persistent CSMA, non-persistent CSMA, P-persistent CSMA. **03**

1. I-persistent CSMA: In I-persistent CSMA, a node waits for a fixed interval of time before attempting to transmit data. If the channel is still idle after the interval has elapsed, the node transmits its data. If the channel is busy, the node continues to wait until it becomes idle.
2. Non-persistent CSMA: In non-persistent CSMA, a node waits for a random interval of time before attempting to transmit data. If the channel is still idle after the interval has elapsed, the node transmits its data. If the channel is busy, the node defers its transmission and tries again later.
3. P-persistent CSMA: In P-persistent CSMA, a node waits for a random interval of time before attempting to transmit data. If the channel is idle, the node transmits its data with a probability of p. If the channel is busy, the node defers its transmission and tries again later.

(b) Explain wireless Ad-Hoc network. **04**

A wireless ad-hoc network (WANET) is a type of wireless network that does not require a fixed infrastructure or central coordinating device. Instead, the nodes in the network communicate directly with each other and form a temporary network on the fly.

WANETs are self-organizing and self-configuring, which means that they can automatically detect and connect to nearby nodes and form a network without the need for any central control. This makes them highly flexible and resilient, as they can adapt to changing conditions and continue to operate even if some of the nodes fail or are removed from the network.

WANETs have several characteristics that distinguish them from other types of wireless networks:

- Decentralized: WANETs do not have a central coordinating device or fixed infrastructure, which makes them decentralized and self-organizing.
- Dynamic: WANETs are dynamic, as the nodes can move freely and the network can change in size and configuration.
- Ad-hoc: WANETs are ad-hoc, as they are formed on the fly and do not require any pre-planning or coordination.
- Peer-to-peer: WANETs are peer-to-peer, as the nodes communicate directly with each other and do not rely on a central server or hub.

WANETs have several advantages, including:

- Flexibility: WANETs are highly flexible, as they can be deployed quickly and easily in any location.
- Resilience: WANETs are resilient, as they can continue to operate even if some of the nodes fail or are removed from

(c) Describe the various outdoor propagation models. **07**

Outdoor propagation models are mathematical models that are used to predict the behavior of electromagnetic waves as they propagate through the environment. These models are used to design and analyze communication systems, such as wireless networks and satellite systems, and to understand the impact of the environment on the performance of the system.

There are several different outdoor propagation models that are used to predict the behavior of electromagnetic waves in different situations, including:

1. Free-space propagation model: The free-space propagation model assumes that the electromagnetic waves propagate through a vacuum or a homogeneous medium with no obstacles or reflections. It is often used to predict the behavior of electromagnetic waves over long distances or in situations where the environment is relatively simple.
2. Two-ray ground reflection model: The two-ray ground reflection model assumes that the electromagnetic waves propagate through the air and are reflected off the ground. It is often used to predict the behavior of electromagnetic waves at low frequencies or over short distances, where the ground reflection is significant.
3. Log-distance path loss model: The log-distance path loss model assumes that the power of the electromagnetic waves decreases with distance according to a logarithmic function. It is often used to predict the behavior of electromagnetic waves over moderate distances, where the environment is relatively homogeneous.
4. Okumura-Hata model: The Okumura-Hata model is a more complex model that takes into account the effect of obstacles and reflections on the propagation of electromagnetic waves. It is often used to predict the behavior of electromagnetic waves in urban or suburban environments, where there are many buildings and other obstacles.
5. Longley-Rice model: The Longley-Rice model is a highly detailed model that takes into account the effect of the environment, including terrain, vegetation, and weather, on the propagation of electromagnetic waves. It is often used to predict the behavior of electromagnetic waves over long distances or in complex environments.

Q.5 **(a)** Explain briefly how a RAKE receiver improves the received signal strength. **03**

A RAKE receiver is a type of receiver that is used in communication systems to improve the performance of the system in the presence of multipath interference. A RAKE receiver works by combining multiple copies of the same signal that have arrived at the receiver

via different paths, in order to improve the signal-to-noise ratio (SNR) and increase the received signal strength.

In a communication system, the signal can arrive at the receiver via multiple paths due to reflections, scattering, and other effects. This can result in multipath interference, which can cause errors and reduce the quality of the received signal.

A RAKE receiver addresses this problem by using multiple "fingers" to independently receive and demodulate the different copies of the signal. The fingers are then combined using a RAKE combiner, which combines the signals based on their relative timing and amplitudes. This process can improve the SNR and increase the received signal strength by effectively canceling out the multipath interference.

RAKE receivers are used in a variety of communication systems, including mobile phones, satellite systems, and wireless networks. They are particularly useful in environments where there is a high level of multipath interference, such as in urban or suburban areas or in the presence of moving objects.

(b) Mention the techniques to improve the capacity in cellular system and explain any one. **04**

There are several techniques that can be used to improve the capacity of a cellular system, which refers to the ability of the system to handle more users or devices simultaneously. These techniques include:

1. Frequency reuse: Frequency reuse is a technique that allows the same set of frequencies to be used by multiple cells in the system. By carefully arranging the cells in a pattern known as a reuse pattern, the system can ensure that the frequencies are used efficiently and avoid interference between cells.
2. Cell splitting: Cell splitting is a technique that involves dividing a large cell into smaller cells, which increases the number of cells in the system and allows more users or devices to be served.
3. Sectorization: Sectorization is a technique that involves dividing a cell into sectors, which are smaller areas that are served by separate antennas. This allows the system to increase capacity by serving more users or devices within a given frequency band.
4. Cell breathing: Cell breathing is a technique that involves adjusting the size of the cells in a cellular system based on the traffic demand. By dynamically adjusting the cell size, the system can increase capacity in areas with high traffic demand and reduce capacity in areas with low traffic demand.
5. Coordinated multipoint (CoMP): Coordinated multipoint (CoMP) is a technique that involves using multiple base stations to serve a single user or device. By using multiple base stations, the system can increase capacity and improve coverage.

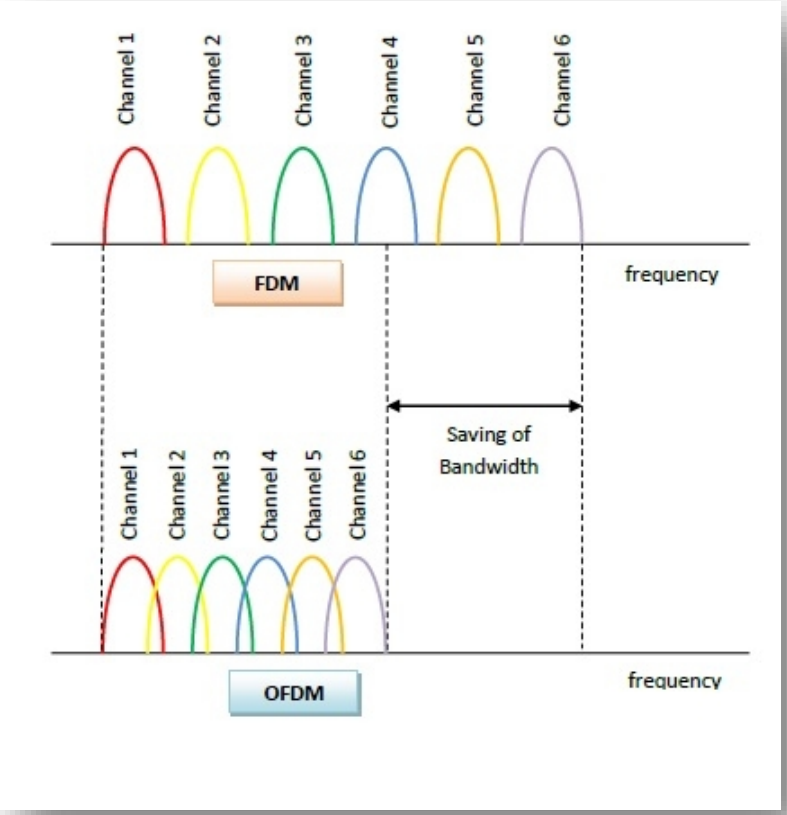
One example of a technique to improve capacity in a cellular system is frequency reuse. Frequency reuse involves using the same set of frequencies in multiple cells in the system, but arranging the cells in

a pattern to avoid interference between cells. This allows the system to increase capacity by efficiently using the available frequencies and avoiding interference.

(c) Write a short note on OFDM. **07**

Orthogonal Frequency Division Multiplexing (OFDM) is a type of digital modulation technique that is used to transmit data over a communication channel. It works by dividing the available frequency band into a number of narrow subcarriers, and modulating each subcarrier with a different data stream.

The following diagram illustrates the basic structure of an OFDM system:



In the transmitter, the data is divided into a number of parallel data streams and encoded using a forward error correction (FEC) code. Each data stream is then modulated onto a different subcarrier using a technique such as quadrature amplitude modulation (QAM). The modulated subcarriers are then combined using an inverse fast Fourier transform (IFFT) to create the OFDM symbol, which is transmitted over the communication channel.

In the receiver, the OFDM symbol is demodulated using a fast Fourier transform (FFT) to separate the subcarriers. The data streams are then decoded using the FEC code and recovered.

OFDM has several advantages, including:

- High spectral efficiency: OFDM allows a large amount of data to be transmitted in a narrow frequency band, making it highly spectrally efficient.

- Robustness to frequency-selective fading: OFDM is robust to frequency-selective fading, which is a type of interference that affects only certain frequencies. This makes it suitable for use in environments where the channel conditions are variable.
- Low complexity: OFDM requires relatively simple hardware and algorithms, which makes it suitable for use in low-cost devices.

OFDM is used in the following area −

- Wi-Fi
- DSL internet access
- 4G wireless communications
- digital television
- radio broadcast services

OR

Q.5 **(a)** List the security issues of wireless networks. **03**

Wireless networks are vulnerable to a number of security threats and issues, which can compromise the confidentiality, integrity, and availability of the data transmitted over the network. Some of the security issues of wireless networks include:

1. Unauthorized access: Wireless networks are vulnerable to unauthorized access, as attackers can potentially gain access to the network by intercepting the wireless signals or cracking the encryption used to secure the network.
2. Eavesdropping: Wireless networks are vulnerable to eavesdropping, as attackers can potentially intercept and listen to the data transmitted over the network.
3. Man-in-the-middle attacks: Wireless networks are vulnerable to man-in-the-middle attacks, in which an attacker intercepts and modifies the data transmitted between two parties.
4. Denial of service (DoS) attacks: Wireless networks are vulnerable to DoS attacks, in which an attacker overloads the network with traffic or sends malicious data to disrupt the network's operation.
5. Rogue access points: Wireless networks are vulnerable to rogue access points, which are unauthorized access points that are set up by attackers to gain access to the network.
6. Unsecured data: Wireless networks are vulnerable to unsecured data, as data transmitted over the network may not be encrypted or may be encrypted using weak or outdated algorithms.

(b) Write a short note on software defined radio. **04**

Software defined radio (SDR) is a type of radio system that uses software to define the radio's function and characteristics. SDRs are flexible and programmable, as the software can be easily modified to support different communication standards, protocols, and frequencies.

In an SDR system, the radio functions are implemented in software rather than in hardware. This allows the radio to be reconfigured and reprogrammed easily, without the need to replace any hardware

components. SDRs are often implemented using general-purpose processors and digital signal processing (DSP) algorithms, which allows them to be highly flexible and adaptable.

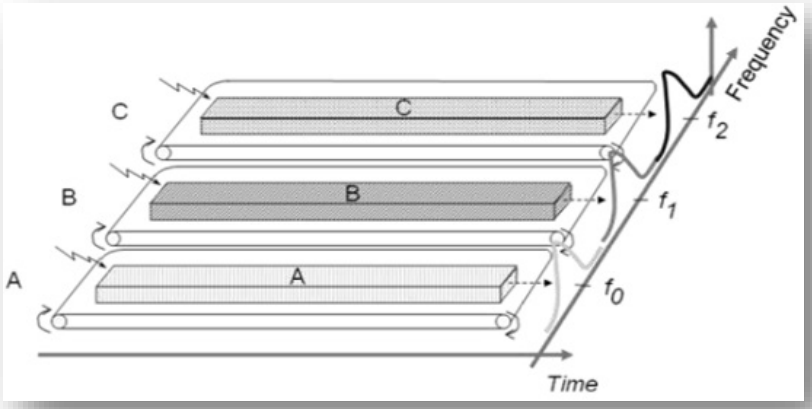
SDRs have several advantages, including:

- Flexibility: SDRs are highly flexible, as they can be easily reconfigured and reprogrammed to support different communication standards, protocols, and frequencies.
- Cost-effectiveness: SDRs can be implemented using low-cost, general-purpose hardware and software, which makes them cost-effective compared to traditional radio systems that require specialized hardware.
- Scalability: SDRs are scalable, as they can be easily modified and expanded to support new features and capabilities.

SDRs are used in a variety of applications, including wireless communication, military systems, and emergency response systems. They are also used in research and development, as they provide a platform for testing and evaluating new communication technologies.

(c) Explain Frequency Division Multiple Access (FDMA) in wireless communication with figure. **07**

Frequency Division Multiple Access (FDMA) is one of the most common analogue multiple access methods. The frequency band is divided into channels of equal bandwidth so that each conversation is carried on a different frequency (*as shown in the figure below*).



In FDMA method, guard bands are used between the adjacent signal spectra to minimize crosstalk between the channels. A specific frequency band is given to one person, and it will received by identifying each of the frequency on the receiving end. It is often used in the first generation of analog mobile phone.

Advantages of FDMA

As FDMA systems use low bit rates (large symbol time) compared to average delay spread, it offers the following advantages −

- Reduces the bit rate information and the use of efficient numerical codes increases the capacity.
- It reduces the cost and lowers the inter symbol interference (ISI)
- Equalization is not necessary.

- An FDMA system can be easily implemented. A system can be configured so that the improvements in terms of speech encoder and bit rate reduction may be easily incorporated.
- Since the transmission is continuous, less number of bits are required for synchronization and framing.

Disadvantages of FDMA

Although FDMA offers several advantages, it has a few drawbacks as well, which are listed below −

- It does not differ significantly from analog systems; improving the capacity depends on the signal-to-interference reduction, or a signal-to-noise ratio (SNR).
- The maximum flow rate per channel is fixed and small.
- Guard bands lead to a waste of capacity.
- Hardware implies narrowband filters, which cannot be realized in VLSI and therefore increases the cost.

****