IOT Module 1

1.What is Single Node Architecture in IoT?

->

Single Node Architecture in the Internet of Things (IoT) refers to a system design where a single IoT device operates independently, functioning as the sole unit in the network. Unlike more complex IoT architectures that involve multiple interconnected devices communicating with one another and with a centralized system or cloud, a single-node IoT architecture focuses on standalone operations.

Key Features of Single Node Architecture in IoT:

1. **Standalone Functionality:**
   - The single node (device) operates independently, performing its tasks without relying on other devices or a network.
   - It may still communicate with a user or a local interface, but it doesn't depend on external IoT nodes.
2. **Sensors and Actuators:**
   - The node typically contains sensors to collect data and may also include actuators to perform actions based on that data.
3. **Processing Capability:**
   - The device often has onboard processing capabilities, such as a microcontroller or microprocessor, to analyze data and make decisions.
4. **Limited or No Connectivity:**
   - Connectivity may be limited to occasional data transmission or could be entirely absent, depending on the use case.
   - In some cases, the device might store data locally or allow a user to extract data manually.
5. **Low Complexity:**
   - The architecture is simple and suitable for applications that do not require real-time communication with other devices or a cloud infrastructure.
6. **Energy Efficiency:**
   - These devices are often designed for low power consumption, making them suitable for battery-operated or energy-constrained environments.

Use Cases of Single Node Architecture:

- **Wearable Devices:** Fitness trackers that record steps, heart rate, and other metrics without requiring constant internet connectivity.
- **Standalone Sensors:** Environmental monitors, such as temperature or humidity sensors, that store data locally for periodic manual retrieval.
- **Appliances:** Smart appliances, like programmable coffee makers, which work independently without connecting to a network.
- **Remote or Isolated Systems:** Devices in areas with limited connectivity, where the primary requirement is to function autonomously.

2. Write hardware and software components of a sensor node

->

Hardware Components:

1. **Sensor**: Detects and measures physical parameters such as temperature, humidity, or motion.
2. **Microcontroller**: Processes data collected by the sensor and manages node operations.
3. **Transceiver**: Facilitates wireless communication with other nodes or the base station.
4. **Power Source**: Provides energy, typically through batteries or energy harvesting methods.
5. **Memory**: Stores data temporarily or permanently for processing and transmission.

Software Components:

1. **Operating System**: Manages the node's resources and provides a platform for applications. Examples include TinyOS or Contiki.
2. **Communication Protocols**: Ensures data is transmitted efficiently and reliably. Common protocols include Zigbee and Bluetooth.
3. **Application Software**: Executes specific tasks such as data aggregation, signal processing, or alert generation.
4. **Middleware**: Simplifies the development and deployment of applications by providing a set of services and APIs.

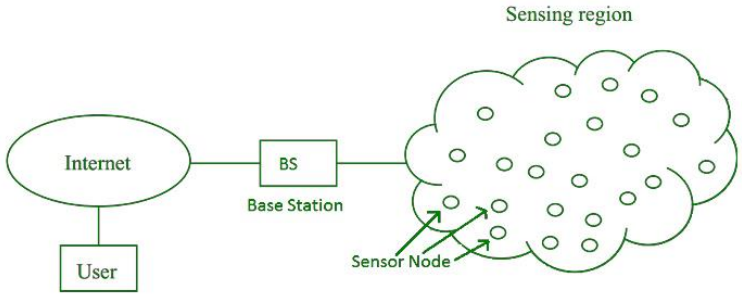
Security Mechanisms: Protects data integrity and confidentiality through encryption and authentication techniques.

3.What do you mean by WSN network architecture?

->

Wireless Sensor Network (WSN), is an infrastructure-less wireless network that is deployed in a large number of wireless sensors in an ad-hoc manner that is used to monitor the system, physical, or environmental conditions.

Sensor nodes are used in WSN with the onboard processor that manages and monitors the environment in a particular area. They are connected to the Base Station which acts as a processing unit in the WSN System. The base Station in a WSN System is connected through the Internet to share data. WSN can be used for processing, analysis, storage, and mining of the data.



Wireless Sensor Network Architecture

A Wireless Sensor Network (WSN) architecture is structured into three main layers:

- **Physical Layer**: This layer connects sensor nodes to the base station using technologies like radio waves, infrared, or Bluetooth. It ensures the physical communication between nodes and the base station.
- **Data Link Layer**: Responsible for establishing a reliable connection between sensor nodes and the base station. It uses protocols such as IEEE 802.15.4 to manage data transmission and ensure efficient communication within the network.
- **Application Layer**: Enables sensor nodes to communicate specific data to the base station. It uses protocols like ZigBee to define how data is formatted, transmitted, and received, supporting various applications such as environmental monitoring or industrial control.

4.Write about Data relaying and aggregation strategies.

->

Data Relaying and Aggregation Strategies in IoT are crucial for efficiently managing the vast amounts of data generated by IoT devices. These strategies aim to ensure reliable data transmission, minimize communication overhead, conserve energy, and provide meaningful insights from raw data.

Data Relaying in IoT

Data relaying involves transmitting data from IoT devices (nodes) to a central processing unit, such as a cloud server, edge server, or gateway, often using intermediate nodes.

Key Techniques in Data Relaying:

1. **Single-Hop Communication:**
   - Each node directly sends data to a centralized server or gateway.
   - Used in small-scale IoT networks with nodes in close proximity to the receiver.
   - **Advantages:** Simplicity and low latency.
   - **Limitations:** Energy-intensive for distant nodes.
2. **Multi-Hop Communication:**
   - Data passes through intermediate nodes before reaching the destination.
   - Reduces energy consumption of far-away nodes and improves coverage in large networks.
   - **Challenges:** Requires efficient routing protocols to prevent bottlenecks and ensure reliability.
3. **Opportunistic Relaying:**
   - Nodes opportunistically forward data when conditions (e.g., available energy, signal quality) are optimal.
   - Helps adapt to dynamic network conditions.
4. **Relay Selection Strategies:**
   - Nodes with higher energy or better connectivity are prioritized as relays.
   - Balances network load and conserves energy.
5. **Wireless Sensor Networks (WSNs):**
   - Relaying often uses mesh topologies, where each node acts as both a sensor and a relay.

- Effective for large-scale deployments like smart agriculture or industrial monitoring.

Data Aggregation in IoT

Data aggregation refers to the process of combining and summarizing data from multiple IoT nodes before transmitting it to reduce redundancy and communication overhead.

Key Techniques in Data Aggregation:

1. **Centralized Aggregation:**
   - All raw data is sent to a central node or server for aggregation.
   - Simplifies node operations but increases network traffic and energy consumption.
2. **Distributed Aggregation:**
   - Data is aggregated at intermediate nodes (e.g., gateways or edge devices) before being forwarded.
   - Reduces data transmission costs and delays.
3. **Hierarchical Aggregation:**
   - IoT nodes are organized into clusters, each with a cluster head responsible for aggregating data within the cluster.
   - Cluster heads forward the aggregated data to the central server.
   - Common in wireless sensor networks.
4. **In-Network Aggregation:**
   - Data is aggregated progressively as it moves through the network.
   - E.g., nodes may compute the average, sum, or other statistical measures before forwarding data.
5. **Temporal Aggregation:**
   - Data is aggregated over time to detect trends or patterns (e.g., hourly averages).
   - Reduces data frequency while preserving useful information.
6. **Compression-Based Aggregation:**
   - Compresses data using techniques like delta encoding or data deduplication to minimize transmission size.

Strategies for Efficient Relaying and Aggregation:

1. **Energy-Efficient Protocols:**
   - Routing and aggregation strategies that minimize energy use extend the lifetime of battery-powered nodes.

2. **Data Prioritization:**
    - Prioritize critical or time-sensitive data for immediate relay and aggregation, while less critical data can be delayed or summarized.
3. **AI and Machine Learning:**
    - Use AI models to predict traffic patterns, optimize routing, and identify redundant data for aggregation.
4. **Edge Computing:**
    - Aggregation at edge nodes reduces latency and bandwidth usage by processing data close to the source.
5. **Security and Privacy Measures:**
    - Ensure encryption and secure data transmission during relaying.
    - Use differential privacy techniques during aggregation to protect sensitive information.
6. **Adaptive Strategies:**
    - Dynamically adjust relaying and aggregation based on network conditions, data volumes, and energy availability.

Benefits of Data Relaying and Aggregation in IoT:

- **Reduced Communication Overhead:** Minimizes redundant data transmission.
- **Energy Conservation:** Extends the life of battery-powered IoT devices.
- **Improved Scalability:** Handles large-scale networks with thousands of devices.
- **Enhanced Data Insights:** Aggregation simplifies raw data into meaningful summaries.

Challenges:

- **Node Failures:** Relay and aggregation strategies must handle node failures to ensure reliable data delivery.
- **Latency:** Aggregation and relaying may introduce delays.
- **Data Accuracy:** Over-aggregation can lead to loss of important details.
- **Security Risks:** Relay nodes or aggregation points can be targets for attacks

5. Write about MAC layer protocol?

->

In Wireless Sensor Networks (WSNs), the Medium Access Control (MAC) protocol is a set of guidelines that dictate how each node should transmit data over the shared wireless medium. The primary objective of the MAC protocol is to minimize the occurrence of idle listening, over-hearing, and collisions of data packets. By efficiently managing access to the wireless medium, the MAC protocol helps to reduce energy consumption and optimize the use of network resources.

MAC Protocol Categories

- Contention based MAC
- Scheduled based MAC
- Hybrid MAC
- Cross-Layer MAC

Contention-based MAC

Contention-based MAC protocol is also known as a random access MAC protocol. It allows all nodes to transmit data on the shared medium, but they have to compete with each other to access the medium. One example of contention-based MAC is CSMA/CA.

In CSMA/CA, each node senses the medium before transmitting the data. If the medium is idle, the node can transmit data immediately. However, if the channel is busy the node has to wait for a random time also known as back-off time. This back-off time reduces the chances of collisions.

Scheduled-based MAC

Scheduled-based MAC is also known as a deterministic MAC protocol. Where each node follows a predetermined schedule and transmits the data according to its given time slot. The data collision is completely nullified in scheduled-based MAC. An example of Scheduled based MAC is TDMA(Time Division Multiple Access).

In TDMA the time is divided into fixed slots and each node is allocated a specific time frame in which they can transmit the data. During this time slot, other nodes remain silent.

Hybrid MAC

Hybrid MAC is a combination of different protocols such as contention-based MAC and scheduled-based MAC to optimize the performance of wireless sensor networks. For example, contention-based MAC protocols, such as CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), allow nodes to access the medium based on a random backoff interval, which reduces collisions but may result in inefficient utilization of the medium. On the other hand, scheduled-based MAC protocols, such as TDMA (Time Division Multiple Access), divide the medium into time slots and assign them to different nodes, which can achieve high utilization but may not be flexible enough to adapt to changing network conditions. Hybrid MAC solved the issue by using other MAC protocols, During transmission of data if the channel is idle or the channel has low traffic then Hybrid MAC switches to contention-based MAC. If the traffic in the channel increases then it is switched to scheduled-based MAC such as TDMA

Cross-Layer MAC

Cross-layer MAC allows the different layers in the protocol stack, typically including physical, MAC, and network layers, to interact and share information with one another. Firstly MAC layers gather information about the state of the channel whether the channel is busy or not. This information will be further used to control the other parameters such as data transmission rate, packet loss rate, and delay.

Once the parameters have been determined, the MAC layer sends the data packets to the PHY layer for transmission over the wireless channel. After the data transmission, the PHY layer sends feedback to the MAC layer about the success or failure of the transmission. If the transmission was unsuccessful. Based on the feedback MAC layer repeats the transmission

7. Write short note on Hybrid TDMA/FDMA

->

In communication systems, FDMA, TDMA, and CDMA are three different methods used to share a single communication channel among multiple users. Understanding these methods helps us see how multiple users can efficiently share communication channels without interference.

FDMA (Frequency Division Multiple Access) divides the channel into separate frequency bands for each user. TDMA (Time Division Multiple Access) assigns different time slots to each user on the same frequency. CDMA (Code Division

Multiple Access) uses unique codes to differentiate users sharing the same frequency band at the same time. In this article, we are going to discuss the differences between these communication channels in detail.

What is FDMA?

Frequency Division Multiple Access (FDMA): FDMA is a type of channelization protocol. This bandwidth is divided into various frequency bands. Each station is allocated a band to send data and that band is reserved for the particular station for all the time which is as follows.

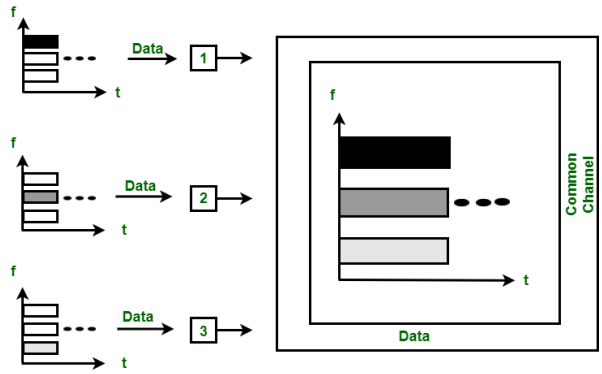
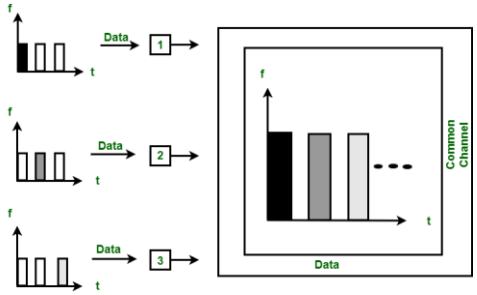


Figure – FDMA

The frequency bands of different stations are separated by small bands of unused frequency and unused frequency bands are called as guard bands that prevent the interference of stations. It is like the access method in the data link layer in which the data link layer at each station tells its physical layer to make a bandpass signal from the data passed to it. The signal is created in the allocated band and there is no physical multiplexer at the physical layer.

What is TDMA?

Time Division Multiple Access (TDMA) : TDMA is the channelization protocol in which bandwidth of channel is divided into various stations on the time basis. There is a time slot given to each station, the station can transmit data during that time slot only which is as follows.



Each station must aware of its beginning of time slot and the location of the time slot. TDMA requires synchronization between different stations. It is type of access method in the data link layer. At each station data link layer tells the station to use the allocated time slot.

8. Write and explain about CSMA based MAC

->

Carrier Sense Multiple Access (CSMA) is a method used in computer networks to manage how devices share a communication channel to transfer the data between two devices. In this protocol, each device first sense the channel before sending the data. If the channel is busy, the device waits until it is free. This helps reduce collisions, where two devices send data at the same time, ensuring smoother communication across the network. CSMA is commonly used in technologies like Ethernet and Wi-Fi.

This method was developed to decrease the chances of collisions when two or more stations start sending their signals over the data link layer. Carrier Sense multiple access requires that each station **first check the state of the medium** before sending.

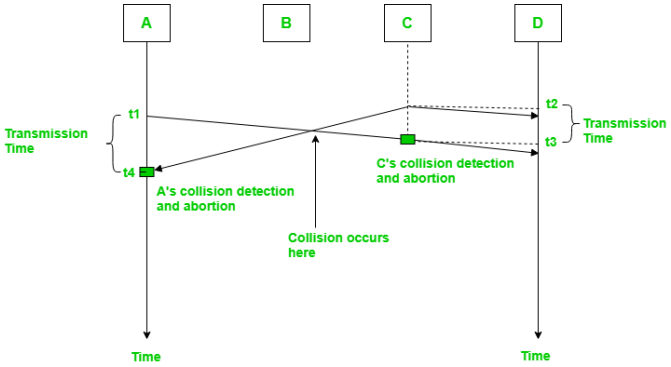
Types of CSMA Protocol

There are two main types of **Carrier Sense Multiple Access (CSMA)** protocols, each designed to handle how devices manage potential data collisions on a shared communication channel. These types differ based on how they respond to the detection of a busy network:

1. CSMA/CD
2. CSMA/CA

Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

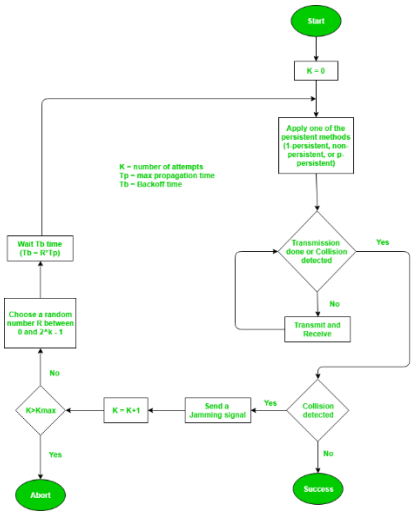
In this method, a station monitors the medium after it sends a frame to see if the transmission was successful. If successful, the transmission is finished, if not, the frame is sent again.



In the diagram, *starts* sending the first bit of its frame at t1 and since C sees the channel idle at t2, starts sending its frame at t2. C detects A's frame at t3 and aborts transmission. A detects C's frame at t4 and aborts its transmission. Transmission time for C's frame is, therefore, t3-t2 and for A's frame is t4-t1

So, the **frame transmission time (Tfr) should be at least twice the maximum propagation time (Tp)**. This can be deduced when the two stations involved in a collision are a maximum distance apart.

Process: The entire process of collision detection can be explained as follows:



Throughput and Efficiency: The throughput of CSMA/CD is much greater than pure or slotted ALOHA.

- For the 1-persistent method, throughput is 50% when G=1.
- For the non-persistent method, throughput can go up to 90%.

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

The basic idea behind CSMA/CA is that the station should be able to receive while transmitting to detect a collision from different stations. In wired networks, if a collision has occurred then the energy of the received signal almost doubles, and the station can sense the possibility of collision. In the case of wireless networks, most of the energy is used for transmission, and the energy of the received signal increases by only 5-10% if a collision occurs. It can't be used by the station to sense collision. Therefore **CSMA/CA has been specially designed for wireless networks**.

These are three types of strategies:

1. **InterFrame Space (IFS):** When a station finds the channel busy it senses the channel again, when the station finds a channel to be idle it waits for a period of time called **IFS time**. IFS can also be used to define the priority of a station or a frame. Higher the IFS lower is the priority.

2. **Contention Window:** It is the amount of time divided into slots. A station that is ready to send frames chooses a random number of slots as **wait time**.

3. **Acknowledgments:** The positive acknowledgments and time-out timer can help guarantee a successful transmission of the frame.

9.What is scheduled based protocol?

-> [not found]

10. Advantages and Disadvantages of Single Node Architecture

->

Advantages:

- **Simplicity:** Easier to design, deploy, and maintain compared to multi-node systems.
- **Cost-Effective:** Lower hardware and infrastructure costs since it doesn't rely on a network.
- **Robustness:** Fewer points of failure because the system operates independently.

Limitations:

- **Limited Scalability:** Cannot accommodate complex IoT systems with multiple devices or nodes.
- **Restricted Functionality:** Lack of inter-device communication and centralized control limits broader use cases.
- **Data Access Challenges:** Retrieving data might require manual intervention if the device lacks connectivity.

11. Write about WSN network topologies

->

Wireless Sensor Networks (WSNs) can be organized into different network topologies based on their application and network type. Here are the most common types:

- **Bus Topology**: In a Bus Topology, multiple nodes are connected to a single line or bus. Data travels along this bus from one node to the next. It's a simple layout often used in smaller networks.

- **StarTopology**: Star Topology have a central node, called the master node, which connects directly to multiple other nodes. Data flows from the master node to the connected nodes. This topology is efficient for centralized control.

- **Tree Topology**: Tree Topology arrange nodes in a hierarchical structure resembling a tree. Data is transmitted from one node to another along the branches of the tree structure. It's useful for expanding coverage in hierarchical deployments.

- **Mesh Topology**: Mesh Topology feature nodes interconnected with one another, forming a mesh-like structure. Data can travel through multiple paths from one node to another until it reaches its destination. This topology offers robust coverage and redundancy.

12. Types of WSN

->

Terrestrial Wireless Sensor Networks

- Used for efficient communication between base stations.
- Consist of thousands of nodes placed in an ad hoc (random) or structured (planned) manner.
- Nodes may use solar cells for energy efficiency.
- Focus on low energy use and optimal routing for efficiency.

Underground Wireless Sensor Networks

- Nodes are buried underground to monitor underground conditions.
- Require additional sink nodes above ground for data transmission.
- Face challenges like high installation and maintenance costs.
- Limited battery life and difficulty in recharging due to underground setup.

Underwater Wireless Sensor Networks

- Deployed in water environments using sensor nodes and autonomous underwater vehicles.
- Face challenges like slow data transmission, bandwidth limitations, and signal attenuation.
- Nodes have restricted and non-rechargeable power sources.

Multimedia Wireless Sensor Networks

- Used to monitor multimedia events such as video, audio, and images.
- Nodes equipped with microphones and cameras for data capture.
- Challenges include high power consumption, large bandwidth requirements, and complex data processing.
- Designed for efficient wireless data compression and transmission.

Mobile Wireless Sensor Networks (MWSNs)

- Composed of mobile sensor nodes capable of independent movement.
- Offer advantages like increased coverage area, energy efficiency, and channel capacity compared to static networks.
- Nodes can sense, compute, and communicate while moving in the environment.

13.Advantages and Disadvantages of WSN

->

Advantages

- **Low cost:** WSNs consist of small, low-cost sensors that are easy to deploy, making them a cost-effective solution for many applications.
- **Wireless communication:** WSNs eliminate the need for wired connections, which can be costly and difficult to install. Wireless communication also enables flexible deployment and reconfiguration of the network.
- **Energy efficiency:** WSNs use low-power devices and protocols to conserve energy, enabling long-term operation without the need for frequent battery replacements.
- **Scalability:** WSNs can be scaled up or down easily by adding or removing sensors, making them suitable for a range of applications and environments.
- **Real-time monitoring:** WSNs enable real-time monitoring of physical phenomena in the environment, providing timely information for decision making and control.

Disadvantages

- **Limited range:** The range of wireless communication in WSNs is limited, which can be a challenge for large-scale deployments or in environments with obstacles that obstruct radio signals.
- **Limited processing power:** WSNs use low-power devices, which may have limited processing power and memory, making it difficult to perform complex computations or support advanced applications.

- **Data security:** WSNs are vulnerable to security threats, such as eavesdropping, tampering, and denial of service attacks, which can compromise the confidentiality, integrity, and availability of data.

- **Interference:** Wireless communication in WSNs can be susceptible to interference from other wireless devices or radio signals, which can degrade the quality of data transmission.

- **Deployment challenges:** Deploying WSNs can be challenging due to the need for proper sensor placement, power management, and network configuration, which can require significant time and resources.

- while WSNs offer many benefits, they also have limitations and challenges that must be considered when deploying and using them in real-world applications

14.What is CDMA?

->

What is CDMA?

Code Division Multiple Access (CDMA) : In CDMA, all the stations can transmit data simultaneously. It allows each station to transmit data over the entire frequency all the time. Multiple simultaneous transmissions are separated by unique code sequence. Each user is assigned with a unique code sequence.

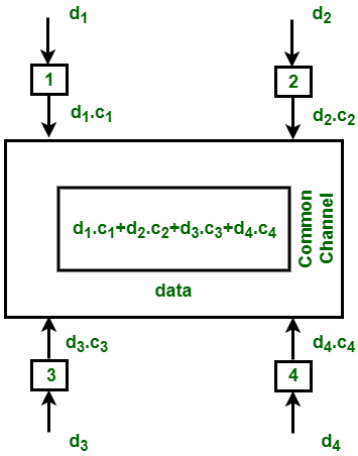


Figure – CDMA

In the above figure, there are 4 stations marked as 1, 2, 3 and 4. Data assigned with respective stations as d1, d2, d3 and d4 and the code assigned with respective stations as c1, c2, c3 and c4.

15. Write advantages and disadvantages of TDMA

->

Advantages of TDMA

- As cell sizes decrease, TDMA requires substantial investment in space, support, and base-station hardware.
- It can transmit data at speeds ranging from 64 kbps to 120 Mbps.
- TDMA separates users based on time, ensuring no interference from simultaneous transmissions.
- It supports services like fax, voiceband data, SMS, multimedia applications, and video conferencing.
- TDMA extends battery life by allowing devices to transmit only part of the time during conversations.
- It effectively handles both data transmission and voice communication needs.

Disadvantages of TDMA

- If all time slots in the current cell and the next cell are occupied, users allocated specific slots may not connect to a call.
- Frequency/slot allocation in TDMA can be complex.
- High data rates in TDMA require equalization.
- TDMA focuses on organization and range planning.

16. State advantages and disadvantages of FDMA

->

Advantages of FDMA

- FDMA uses simple hardware resources and is easy to set up.
- It efficiently handles smaller groups of users.

- The system isn't overly complicated.
- All stations can transmit continuously without waiting their turn.
- It lowers the amount of data transmitted, which can increase capacity.
- It reduces interference between symbols, improving communication quality.

Disadvantages of FDMA

- FDMA works only with analog signals.
- It lacks flexibility, so existing traffic patterns must change gradually.
- Transponders need extensive bandwidth.
- It doesn't support high traffic capacity.

17. Write advantages and disadvantages of CDMA

->

Advantages of CDMA

- CDMA has a very high spectral capacity, supporting many users within a wide bandwidth.
- It doesn't require synchronization between users.
- CDMA channels are hard to decode, improving cellular communication security.
- It provides better secure transmission capabilities.
- Dropouts only occur when the user is twice the distance from the base station.

Disadvantages of CDMA

- CDMA faces channel pollution when a user's phone connects to multiple cell sites, but only one has strong signal.
- CDMA isn't as mature as GSM, since it's newer.

- CDMA requires time synchronization.
- Performance of the CDMA system decreases as the number of users increases.
- CDMA equipment tends to be more expensive due to its complexity.

18. Explain the differences of TDMA, FDMA, CDMA

->

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.

FDMA	TDMA	CDMA
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

19. Write advantages of CSMA Access Mode

->

There are 4 types of access modes available in CSMA. It is also referred as 4 different types of CSMA protocols which decide the time to start sending data across shared media.

1. **1-Persistent:** It senses the shared channel first and delivers the data right away if the channel is idle. If not, it must wait and ***continuously*** track for the channel to become idle and then broadcast the frame without condition as soon as it does. It is an aggressive transmission algorithm.

2. **Non-Persistent:** It first assesses the channel before transmitting data; if the channel is idle, the node transmits data right away. If not, the station must wait for an arbitrary amount of time (***not continuously***), and when it discovers the channel is empty, it sends the frames.

3. **P-Persistent:** It consists of the 1-Persistent and Non-Persistent modes combined. Each node observes the channel in the 1Persistent mode, and if the channel is idle, it sends a frame with a P probability. If the data is not transferred, the frame restarts with the following time slot after waiting for a (q = 1-p probability) random period.

4. **O-Persistent:** A supervisory node gives each node a transmission order. Nodes wait for their time slot according to their allocated transmission sequence when the transmission medium is idle.

20.Advantgaes and Disadvantages of CSMA

->

Advantages of CSMA

- **Increased Efficiency:** CSMA ensures that only one device communicates on the network at a time, reducing collisions and improving network efficiency.
- **Simplicity:** CSMA is a simple protocol that is easy to implement and does not require complex hardware or software.
- **Flexibility:** CSMA is a flexible protocol that can be used in a wide range of network environments, including wired and wireless networks.
- **Low cost:** CSMA does not require expensive hardware or software, making it a cost-effective solution for network communication.

Disadvantages of CSMA

- **Limited Scalability:** CSMA is not a scalable protocol and can become inefficient as the number of devices on the network increases.
- **Delay:** In busy networks, the requirement to sense the medium and wait for an available channel can result in delays and increased latency.
- **Limited Reliability:** CSMA can be affected by interference, noise, and other factors, resulting in unreliable communication.
- **Vulnerability to Attacks:** CSMA can be vulnerable to certain types of attacks, such as jamming and denial-of-service attacks, which can disrupt network communication.

21.Short note on LEACH

->

LEACH (Low-Energy Adaptive Clustering Hierarchy) is a popular protocol designed for energy-efficient communication in wireless sensor networks (WSNs), which are integral to IoT systems. It organizes the network into clusters to optimize energy usage, extend the lifetime of battery-powered devices, and ensure reliable data transmission.

In LEACH, nodes are grouped into clusters, each with a designated **Cluster Head (CH)**. The CH is responsible for aggregating data from member nodes within its cluster and transmitting it to the base station (or sink). This reduces the number of direct transmissions to the base station, conserving energy. CHs are rotated periodically among nodes to distribute energy consumption evenly and prevent individual nodes from draining their power too quickly.

LEACH operates in two phases: the **setup phase**, where clusters are formed and CHs are elected, and the **steady-state phase**, where data is transmitted within clusters and aggregated at the CHs. By balancing the workload and employing techniques like data aggregation, LEACH minimizes redundant transmissions, making it highly suitable for IoT applications like smart agriculture, environmental monitoring, and industrial automation.

22. Short note on SMACS

->

SMACS (Self-Organizing Medium Access Control for Sensor Networks) is a protocol designed for wireless sensor networks, commonly used in IoT applications. It focuses on autonomous organization and medium access in a distributed manner, enabling nodes to establish communication links without a central controller. SMACS allows nodes to discover their neighbors and set up communication schedules during an initial setup phase, facilitating efficient data transfer.

One of its key features is its ability to coordinate medium access while ensuring energy efficiency by allowing nodes to alternate between active and sleep states. This reduces power consumption, which is crucial for battery-operated IoT devices. SMACS also supports dynamic network configurations, where nodes can join or leave the network without disrupting overall operations, making it robust for scalable IoT systems. Its decentralized approach and adaptability make it suitable for applications like environmental monitoring and industrial IoT.

23. Short note on TRAMA

->

TRAMA (Traffic-Adaptive Medium Access Protocol) is an energy-efficient MAC protocol designed for wireless sensor networks and IoT systems. It aims to reduce energy consumption by minimizing idle listening and avoiding collisions through a traffic-aware scheduling mechanism. Nodes share

information about their intended transmissions, and a schedule is dynamically generated based on traffic demands, ensuring that only one node transmits at a time.

TRAMA operates in two phases: a **contention-based signaling phase**, where nodes exchange schedules, and a **contention-free data transmission phase**, where data is transmitted according to the schedule. Nodes that are not involved in communication enter a sleep mode, conserving energy. This makes TRAMA particularly suitable for IoT applications requiring efficient power usage and reliable communication, such as smart grids and environmental monitoring. Its adaptability to changing traffic patterns enhances performance in dynamic IoT environments.

24. Address and name management on WSN

->

Address Management:

1. **Distributed Address Assignment**: Nodes autonomously assign addresses to avoid conflicts.
2. **Hierarchical Addressing**: Uses structured addresses to simplify routing and management.
3. **Locally Unique Addresses**: Each node has a unique address within its local cluster to prevent conflicts.

Name Management:

1. **Mapping Names to Addresses**: Services like DNS map user-friendly names to IP addresses.
2. **Content-Based Naming**: Names are derived from the data or context, making them meaningful and easier to manage.
3. **Geographic Naming**: Names are based on the physical location of nodes, aiding in location-based services.

25. How to assign Mac address on WSN

->

1. Manufacturer-Based Assignment

- **Global Unique MAC Addresses**: Each device is pre-assigned a globally unique MAC address by the manufacturer.
- **IEEE Standards**: Follow IEEE standards where each manufacturer is assigned a unique Organizationally Unique Identifier (OUI).

2. Dynamic Assignment

- **Self-Organizing Networks**: Devices dynamically generate unique MAC addresses based on network conditions.
- **Conflict Resolution**: Use algorithms to detect and resolve address conflicts within the network.

3. Hierarchical Assignment

- **Cluster-Based Networks**: Cluster heads manage MAC address assignment for their cluster members.
- **Address Pool Management**: Cluster heads maintain a pool of available MAC addresses for efficient assignment.

4. Energy-Efficient Assignment

- **Low-Energy Protocols**: Use energy-efficient protocols to minimize the overhead of address assignment.

Sleep and Wake Cycles: Consider the sleep and wake cycles of devices to avoid address conflicts.