UNIT-1

MAC & ROUTING IN AD HOC NETWORKS

1 a) Define Wireless Network. Explain the different Types of Wireless Communication. [L2, CO1] [6M]

What is a Wireless Network?

A wireless network is a type of network that does not use wires to connect devices. Instead, it uses radio waves or infrared signals to send data. This makes it easy to connect phones, computers, and other devices without cables.

Types of Wireless Communication:

1. **Satellite Communication**
    - Uses satellites in space to send signals.
    - Used for TV broadcasting, GPS, and global communication.
2. **Infrared (IR) Communication**
    - Uses infrared light for short distances.
    - Example: TV remotes, security systems.
3. **Broadcast Radio**
    - Oldest wireless method using radio waves.
    - Example: AM/FM radio, walkie-talkies.
4. **Microwave Communication**
    - Uses high-frequency radio waves to send data.
    - Used for long-distance telephone calls and satellite internet.

5. **Wi-Fi**
    - Wireless internet using routers.
    - Used in mobile phones, laptops, smart devices.
6. **Cellular & Mobile Communication**
    - Uses cell towers for mobile calls and internet.
    - **Generations:**
        - 1G – Old, slow (analog).
        - 2G – Digital (better calls & SMS).
        - 3G, 4G, 5G – Faster internet and calls.
7. **Bluetooth**
    - Wireless connection for short distances (10m – 100m).
    - Example: Wireless headphones, file sharing.
8. **ZigBee**
    - Low-power wireless technology.
    - Used in smart homes and sensor networks.
9. **WiMAX**
    - High-speed wireless internet for big areas.
    - Used in places where Wi-Fi or cables are not available.

b) List and explain about various operating modes in wireless networks [L2,CO1] [6M]

1. **Infrastructure Mode**
    - Centralized network architecture
    - **Components:**
        - Access Point (Router)

        - Client Devices
    - **Characteristics:**
        - Controlled communication
        - Managed by central device
    - Real-world example: Home/Office Wi-Fi

2. **Ad-Hoc Mode**
    - Peer-to-peer communication
    - No central infrastructure
    - Direct device-to-device connection
    - **Use cases:**
        - Emergency communications
        - Quick file sharing
        - Limited area networking

3. **Mesh Mode**
    - Multiple interconnected devices
    - Self-healing network
    - Features:
        - Multiple communication paths
        - Redundant connections
        - Improved reliability
    - Example: Smart home networks

2 a) Describe the classifications in Wireless Network. [L2,CO1] [6M]

1. **By Network Size:**
    - Personal Area Network (PAN)

        - Range: Up to 10 meters
        - Devices: Bluetooth, Wireless USB
        - Example: Connecting smartphone to smartwatch
    - Local Area Network (LAN)
        - Range: Single building
        - Typical Speed: 10-100 Mbps
        - Example: Office computer network
    - Metropolitan Area Network (MAN)
        - Range: City-wide
        - Technology: Fiber optic
        - Example: City-wide internet infrastructure
    - Wide Area Network (WAN)
        - Range: Country/Global
        - Technology: Satellite, Leased lines
        - Example: Internet itself

2. **By Communication Technology:**
    - Cellular Networks
        - Generations: 1G, 2G, 3G, 4G, 5G
        - Coverage: Nationwide
        - Use: Mobile communication
    - Wireless LAN (Wi-Fi)
        - Standard: IEEE 802.11
        - Frequency: 2.4 GHz, 5 GHz
        - Range: 50-100 meters

- Bluetooth
    - Short-range communication
    - Personal devices
    - Low power consumption

2 b)Difference Between Wired and Wireless Communication (Very Simple Answer)

Feature	**Wired Communication (With Wires)**	**Wireless Communication (Without Wires)**
How it works?	Uses cables to send data.	Uses air (radio waves) to send data.
Speed	Faster and stable.	Can be slower and affected by interference.
Reliability	Very reliable, no signal loss.	Less reliable, signal can be weak.
Mobility	Cannot move freely (limited by wires).	Can move freely (no wires needed).
Installation	Harder to set up (needs cables).	Easy to set up (no cables needed).
Security	More secure (data stays in wires).	Less secure (data can be hacked).
Examples	Ethernet, telephone cables.	Wi-Fi, Bluetooth, mobile networks.

Easy Trick to Remember:

- Wired = Uses cables (like TV cable or phone line).
- Wireless = No cables, uses air (like Wi-Fi or mobile network).

✅ For best speed and security → Use wired.
✅ For easy movement and convenience → Use wireless.

3 a) Explain in detail about Issues in ad hoc wireless networks. [L2,CO1] [6M]

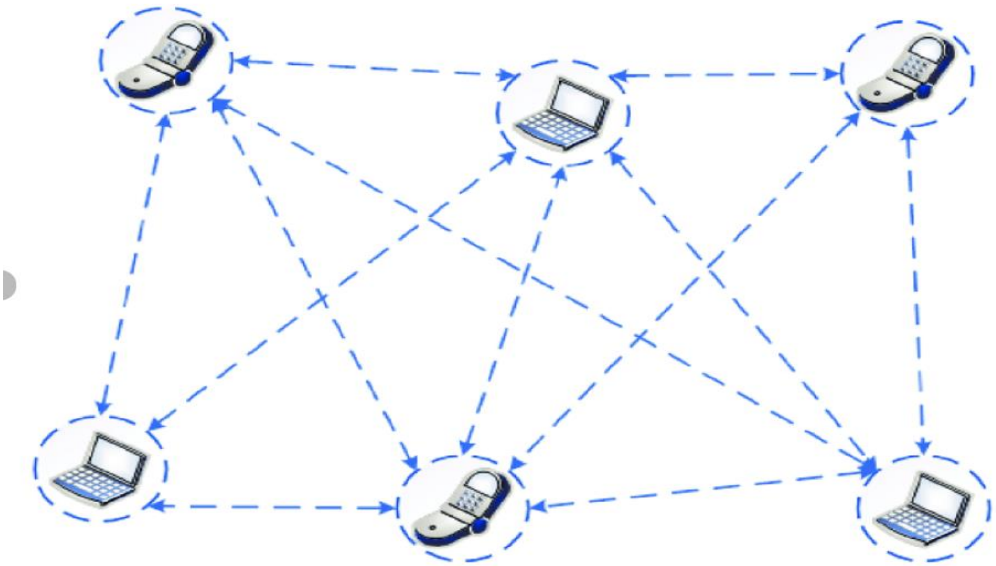
Ad hoc wireless networks are temporary networks where devices communicate without a central system. These networks face many challenges:

1. Limited Bandwidth – Wireless networks have less speed compared to wired networks, making data transfer slower.
2. Variable Link Capacity – The connection strength keeps changing due to obstacles and interference.
3. Dynamic Topology – Devices move frequently, changing the network structure and breaking connections.
4. Multicast Routing – Sending data to multiple devices is difficult because they keep moving.
5. Routing Overhead – Routes change frequently, so extra data is needed to update paths, wasting bandwidth.
6. Mobility – Devices move, breaking connections and causing delays in communication.
7. Hidden Terminal Problem – Some devices send data at the same time, causing collisions and errors.
8. Packet Loss – Data gets lost due to weak signals, movement, or interference.
9. Frequent Network Partitions – Some devices may move too far, breaking the network into smaller parts.
10. Power Constraints – Devices use batteries, so energy-saving techniques are important.

11. Diffusion Hole Problem – Some devices near network gaps use too much power, making the problem worse.
12. Quality of Service (QoS) – The network keeps changing, making it hard to provide smooth communication.
13. Inter-networking – Connecting ad hoc networks with normal networks is difficult due to different rules.
14. Security Challenges – Hackers can attack because there is no central security system.
    - External Threats – Unauthorized users can enter the network and steal data.
    - Reliability Issues – Wireless networks are weaker and have more errors.
15. Passive Attacks – Hackers can secretly listen to data without being detected.

b) Explain the ad hoc network architecture. [L2,CO1] [6M]

An **Ad hoc network** is a type of network where devices (like phones or laptops) connect to each other directly without using a central server or access point. It is often used in emergency situations, like during natural disasters, where it is hard to set up a normal network.



Key Points:

1. **No central control**: There is no main server or access point. All devices communicate directly with each other.
2. **Temporary**: This type of network is set up only for a short time, especially during emergencies.
3. **Moving devices**: The devices in the network can move around and still stay connected.
4. **Message forwarding**: If two devices are far from each other, other devices can help pass the message.

Categories of Ad hoc Networks:

1. **Enabling technologies**: These are the technologies used to make the network work. There are different types like **Personal Area Networks (PAN)** or **Wide Area Networks (WAN)**.
2. **Networking**: Since devices can move, special methods are needed to send messages correctly.
3. **Applications**: Ad hoc networks are used in areas like **emergency services**, **disaster recovery**, and **environmental monitoring**.

In simple terms, an ad hoc network is a temporary, decentralized network where devices connect directly and communicate without a central server. It's very useful when normal networks are not available.

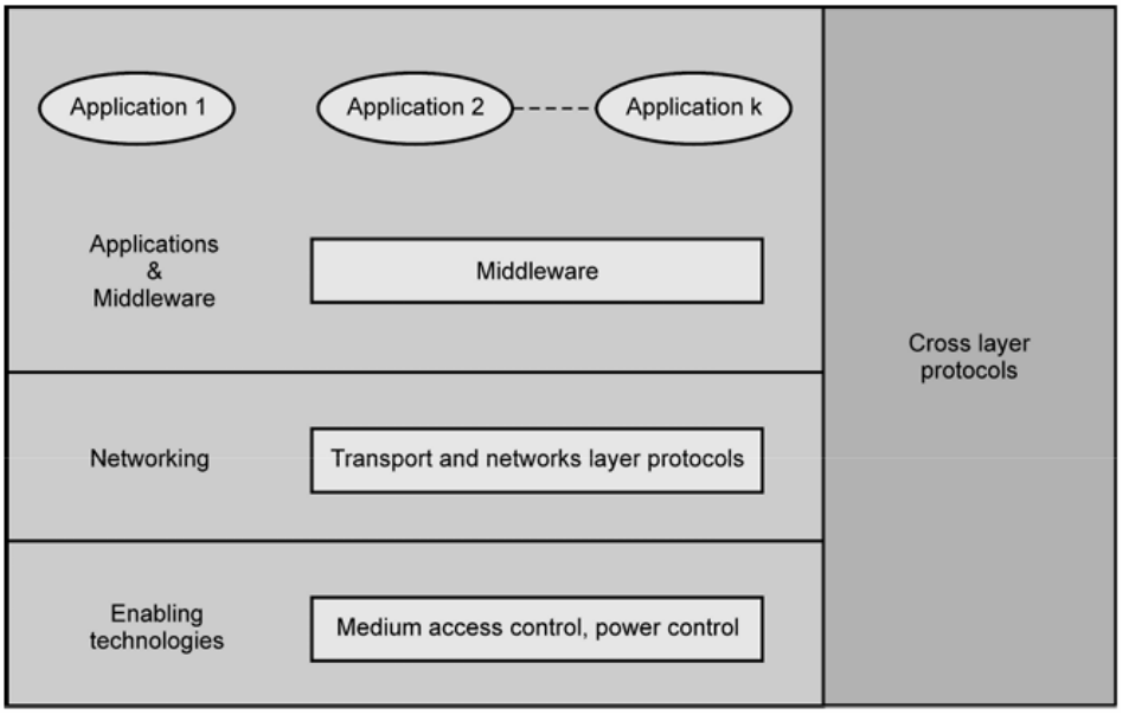
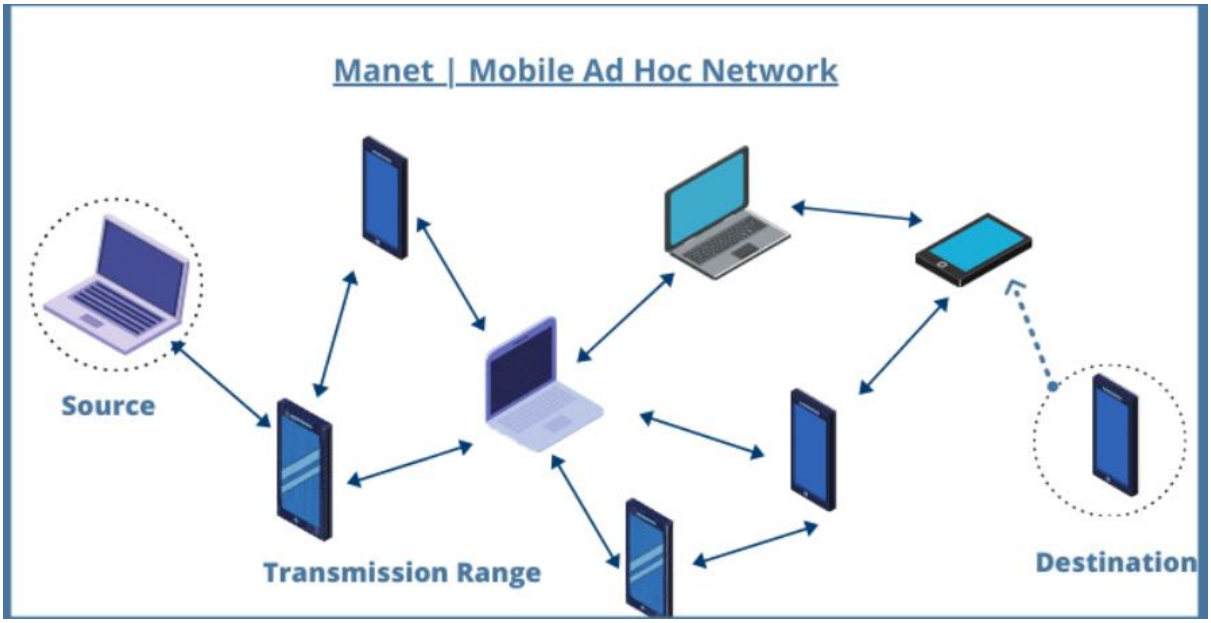


Fig. 1.2.3 Adhoc Network Architecture

4 a) Demonstrate the different types of Wireless Adhoc Networks. [L2,CO1] [6M]

- **Mobile Ad hoc Network (MANET):**
  - A network of mobile devices that can connect with each other without any fixed infrastructure, like Wi-Fi between phones.



- **Vehicular Ad hoc Network (VANET):**

- A network where vehicles communicate with each other and roadside devices to share information, like traffic updates or accident alerts.

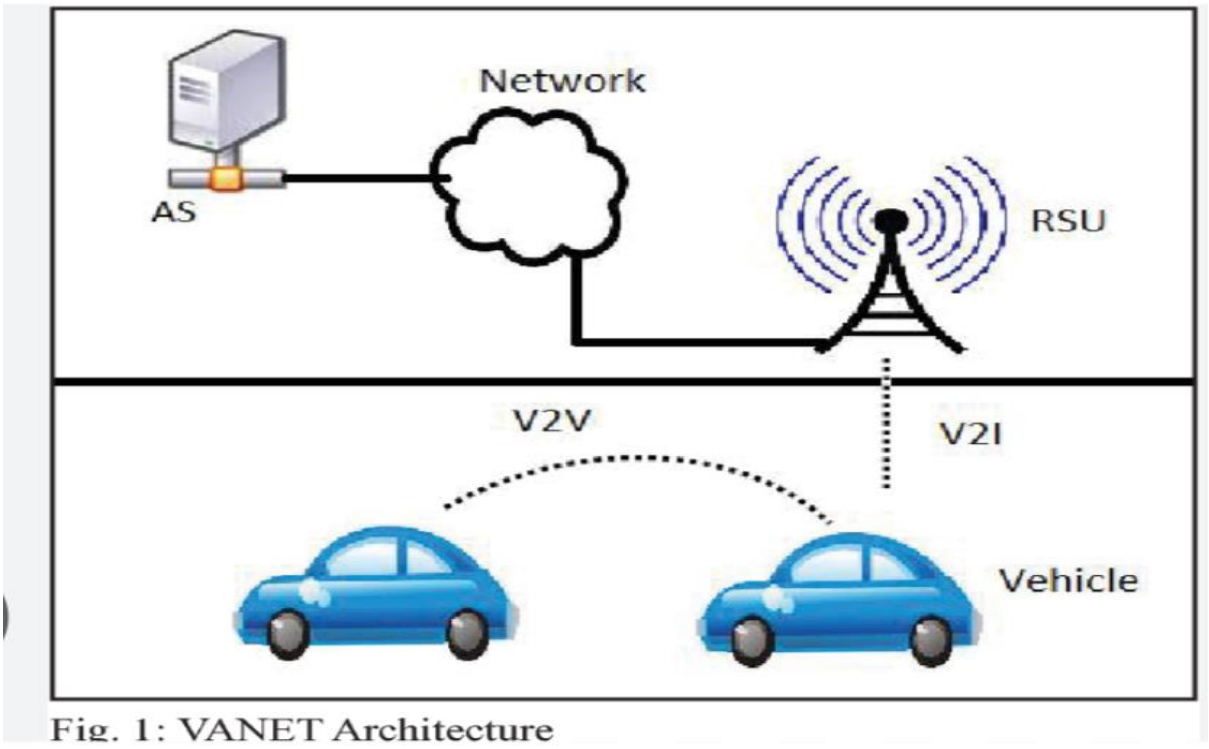
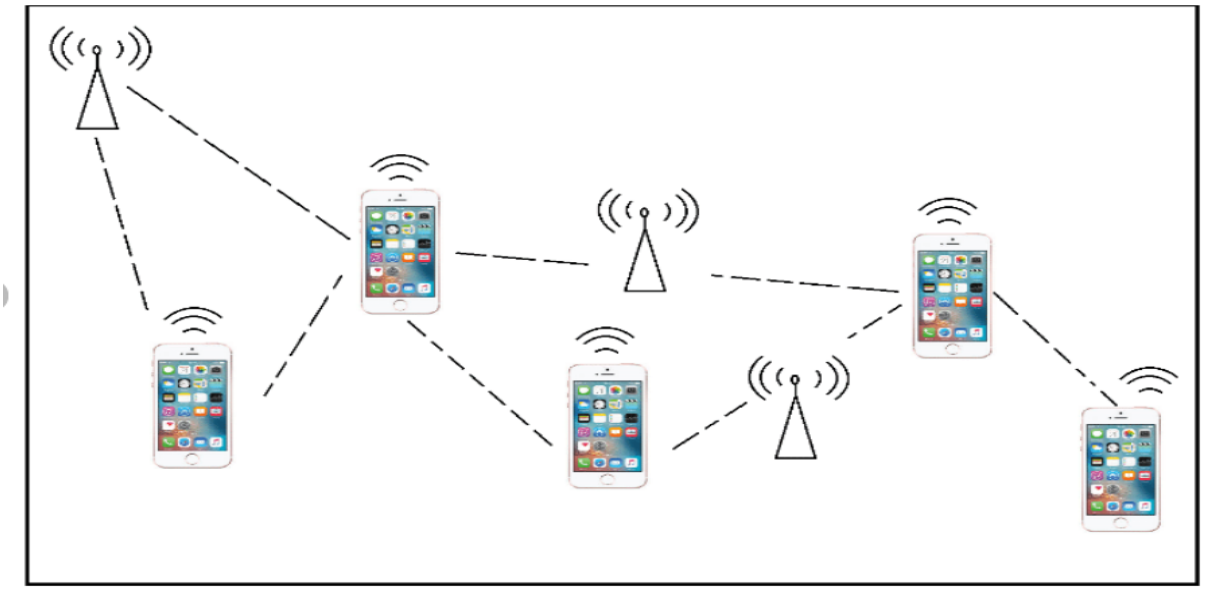


Fig. 1: VANET Architecture

Smartphone Ad hoc Network (SPAN):

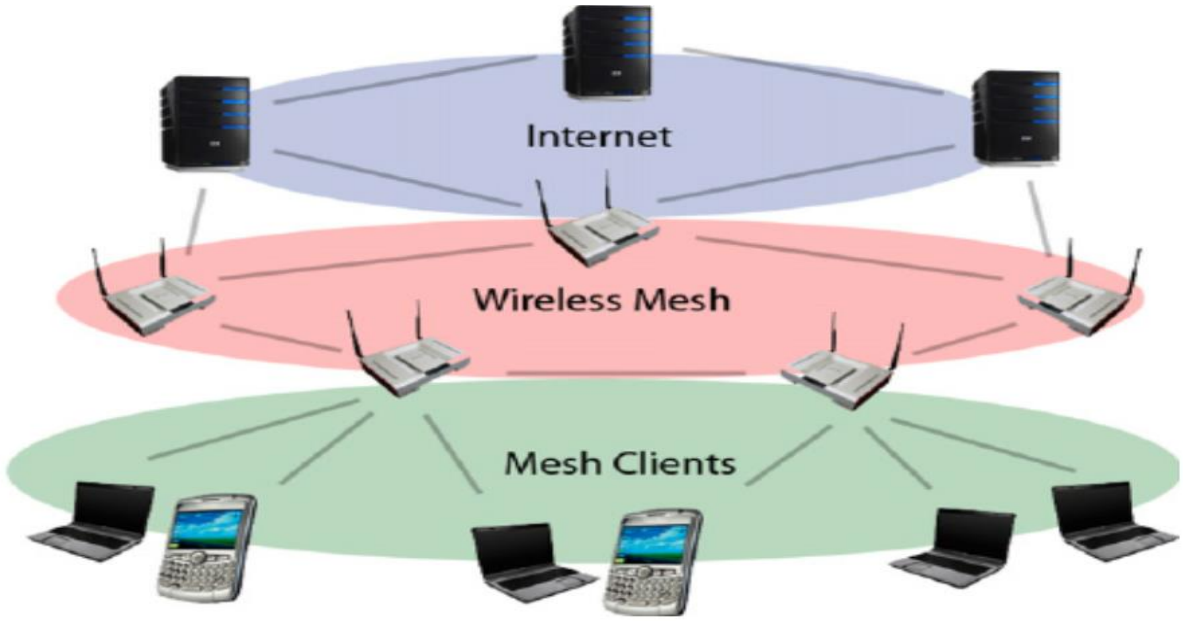
- A network formed between smartphones using Wi-Fi or Bluetooth without needing a cell tower or internet.



A Mobile Ad Hoc Network (An example of SPAN)

🔹 Wireless Mesh Network (WMN):

- A network where devices are connected in a way that they can communicate with each other and relay information, like a web of connected devices.



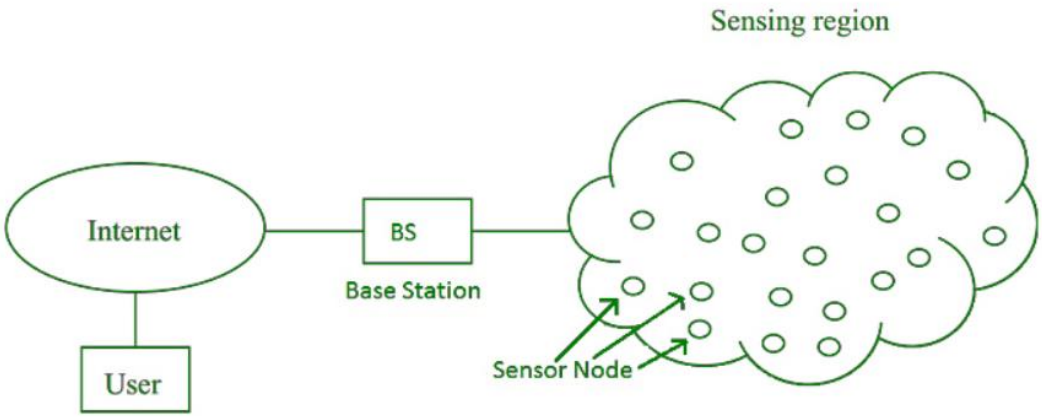
Wireless mesh network (WMN).

🔹 Army Tactical MANET:

- A mobile network used by the army for communication when they are on the move and need quick setup.

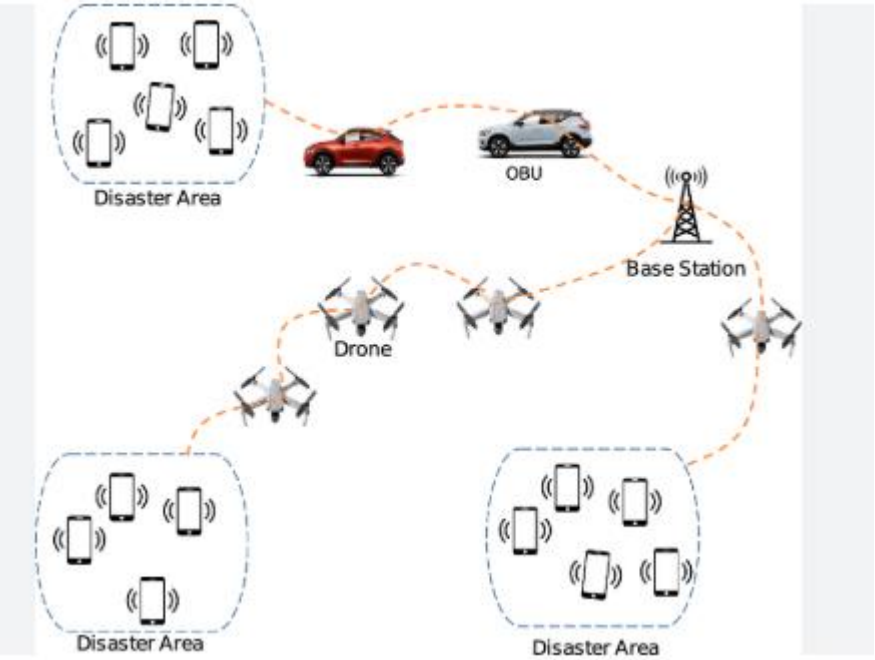
🔹 Wireless Sensor Network:

- A network of sensors that collect data (like temperature or traffic) and send it to a central system.



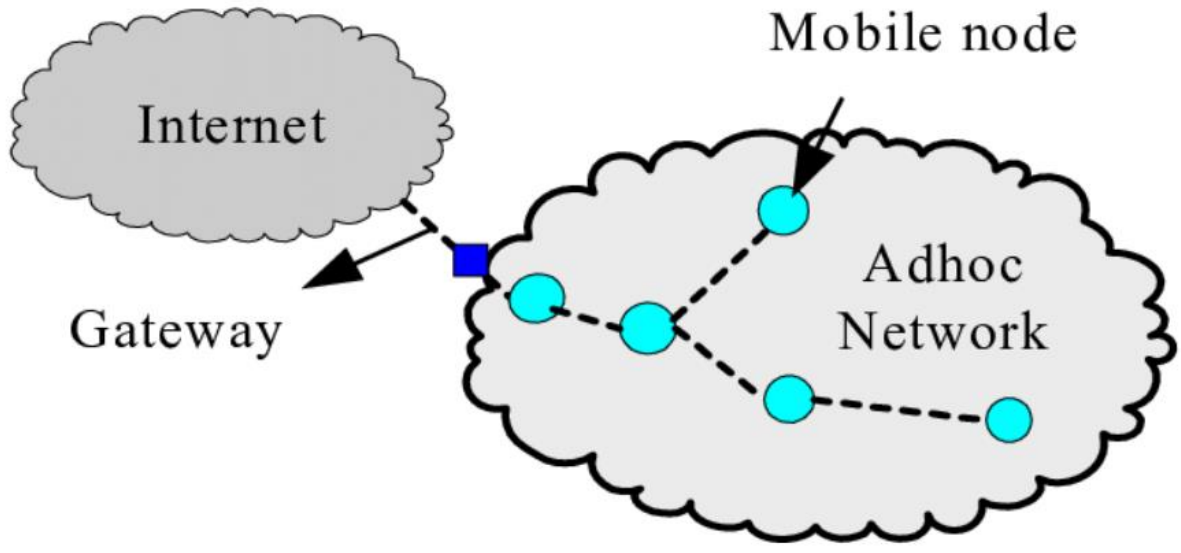
🔹 Disaster Rescue Adhoc Network:

- A network used during disasters when normal communication systems fail, to help rescuers communicate.



⍰ Intelligent Mobile Ad hoc Network (iMANET):

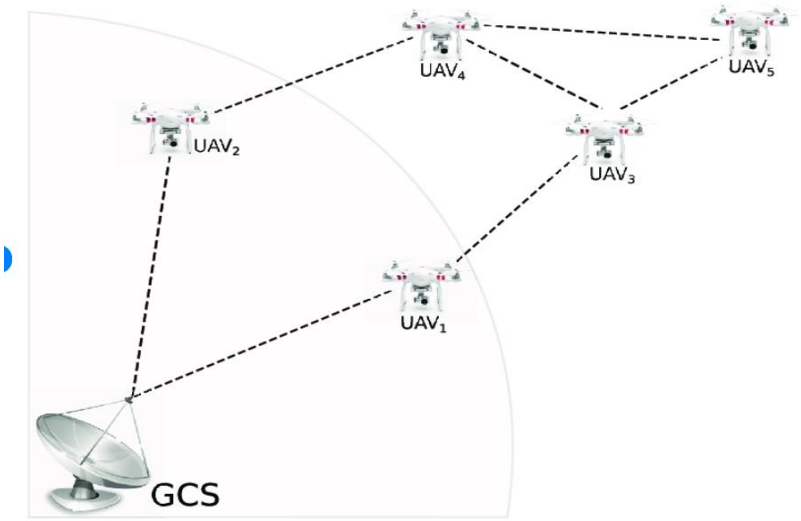
- A smart network that connects moving devices and fixed ones automatically using intelligent routing.



Mobile Ad Hoc network connected with Internet

⍰ Flying Ad hoc Network (FANET):

- A network where flying drones (unmanned aerial vehicles) communicate with each other or ground stations.



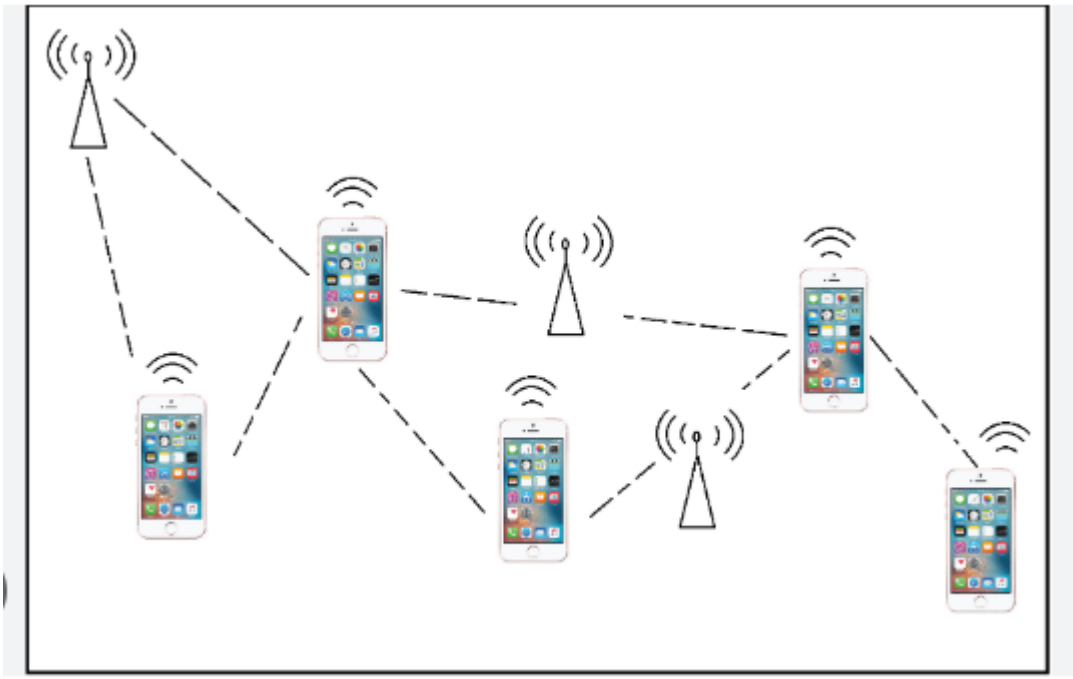
Simple example of a FANET (Flying ad hoc network).

4 b) Differentiate between Mobile Adhoc Network and Vehicular Adhoc Network

Feature	MANET (Mobile Adhoc Network)	VANET (Vehicular Adhoc Network)
Definition	A network of mobile devices (like phones or laptops) that connect without wires or a fixed setup.	A type of network for communication between vehicles and road systems.
Mobility	Mobile devices move at a normal speed.	Vehicles move fast at high speeds.
Topology	The network changes slowly because devices don't move very fast.	The network changes quickly because vehicles move fast.
Communication Range	Short range (like between phones or laptops).	Long range (between vehicles and road systems).
Energy Use	Devices use battery power, so energy is important.	Vehicles have enough power, so energy isn't a big issue.
Routing Protocols	Uses protocols like AODV and DSR to send data.	Uses special protocols like GPSR for vehicle communication.
Applications	Used in places like the military, remote areas, or disasters.	Used for traffic control, car safety, and smart transportation.
Challenges	Problems like slow connections and security issues.	Problems with fast-moving cars and needing real-time data.

5 a) Illustrate in detail about Smartphone Adhoc Network with an example. [L3,CO1] [6M]

Smartphone Adhoc Network (SPAN)



SPAN is a network where phones connect directly to each other without using cell towers or Wi-Fi routers. It doesn't need a central server, and phones connect automatically using Bluetooth or Wi-Fi Direct.

Example: After an Earthquake

If there's an earthquake and the regular phone network is down, people can still talk:

1. **Making the Network**:
    - Phones of rescue workers and civilians connect automatically using Bluetooth or Wi-Fi.
    - The network updates as people move.
2. **Sending Messages**:
    - If someone is stuck, their message can go through other phones to reach help.
    - For example, Phone A → Phone B → Phone C → Rescue Worker's Phone.

3. **Sharing Information**:
    - People can send their location or pictures to help rescuers.
4. **Sending Alerts**:
    - Emergency officials can send messages to everyone in the network, like instructions to stay safe.
5. **Working Without All Phones**:
    - If some phones stop working, the network still keeps going using other phones.

Key Features:

- No need for cell towers or Wi-Fi.
- Phones connect automatically.
- Saves battery with Bluetooth Low Energy (BLE).
- More phones can join the network at any time.

Where It's Used:

- In disasters, military areas, events, and remote schools.

b) Discuss various design issues of Medium Access Control (MAC) layer. [L2, CO1] [6M]

Design Issues of MAC Layer in Ad Hoc Wireless Networks

The **MAC layer** helps control how nodes (devices) share the communication channel in a network. In **ad hoc wireless networks**, there are some problems that the MAC layer needs to solve. Here are the main issues:

1. **Mobility of Nodes**

- **Problem**: Nodes move around, so the network keeps changing.
- **Solution**: The MAC protocol should adjust to these changes and keep the network working smoothly.

2. **Distributed Operation**
   - **Problem**: There is no central control, so all nodes need to manage the channel on their own.
   - **Solution**: The MAC protocol should make sure that nodes don’t waste too much bandwidth with extra control messages.
3. **Bandwidth Efficiency**
   - **Problem**: Bandwidth (the network's capacity) is limited.
   - **Solution**: The MAC protocol should make the best use of the available bandwidth.
4. **Signal Propagation Delay**
   - **Problem**: Signals take time to travel, which can cause collisions if nodes don’t know when others are sending data.
   - **Solution**: The MAC protocol should help nodes synchronize and avoid these delays.
5. **Hidden Terminal and Exposed Terminal Problems**
   - **Problem**: Hidden terminals cause data collisions, and exposed terminals are blocked from sending data unnecessarily.
   - **Solution**: The MAC protocol should use methods like **RTS/CTS** to avoid these problems.

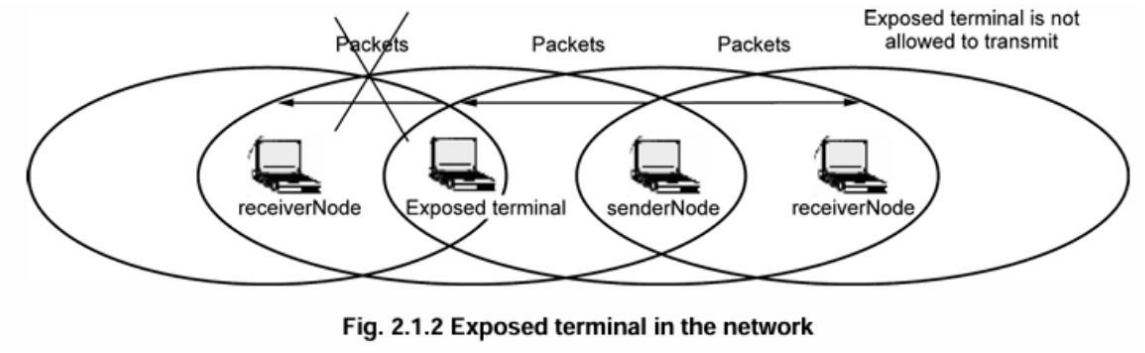


Fig. 2.1.2 Exposed terminal in the network

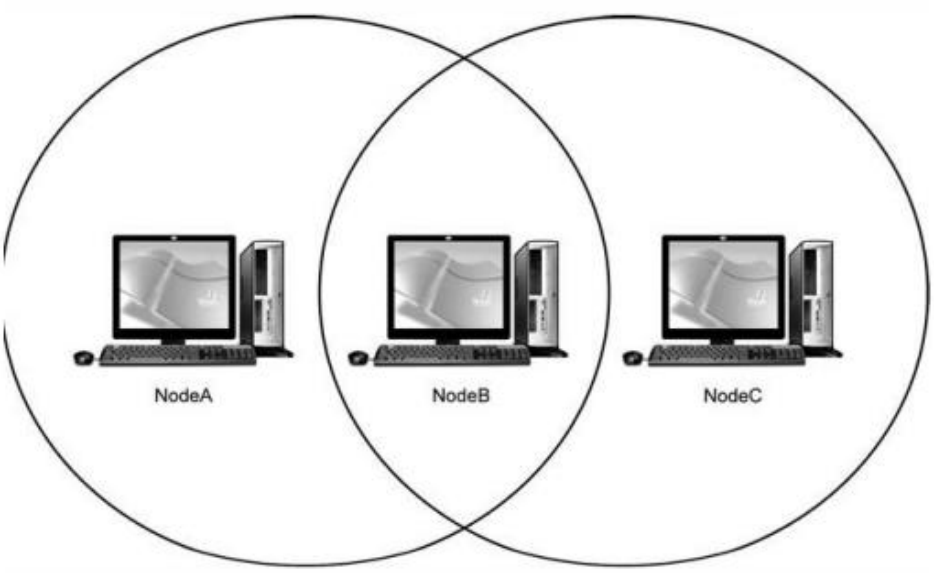


Fig. 2.1.1 Hidden terminal in the network

6. **Support for Real-Time Traffic**
    - **Problem**: Real-time data (like video or voice) needs to be sent quickly without delays.
    - **Solution**: The MAC protocol should ensure that real-time data is transmitted on time.

6 a) Classify MAC protocols for ad hoc networks

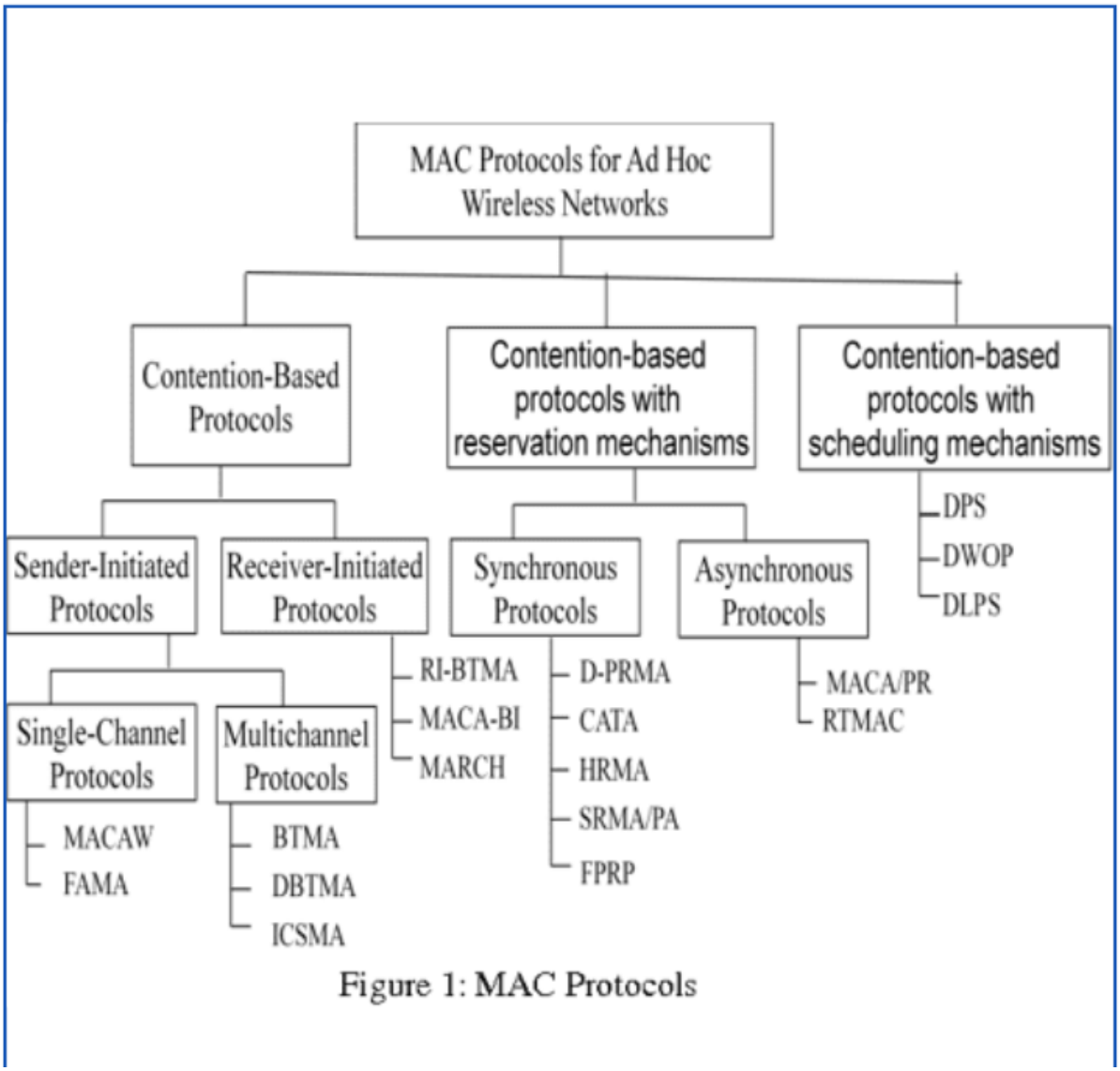


Figure 1: MAC Protocols

MAC Protocols for Adhoc Networks

MAC Protocols help devices in an ad hoc network share the communication channel. There are different types of MAC protocols based on how devices access the channel.

Three Main Types of MAC Protocols:

1. **Contention-based Protocols**:
    - Devices **compete** to access the channel.
    - No special order. They just try when they can.
    - Example: **CSMA/CA** (Devices check if the channel is free before sending data).

2. **Contention-based with Reservation**:
    - Devices **reserve** time slots to send data, reducing the chance of competition.
    - Example: **RTS/CTS** (Devices request permission before sending).
3. **Contention-based with Scheduling**:
    - A **schedule** is created for devices, telling them when to send data, so there's no competition.
    - Example: **TDMA** (Each device gets a specific time to send).

Key Point:

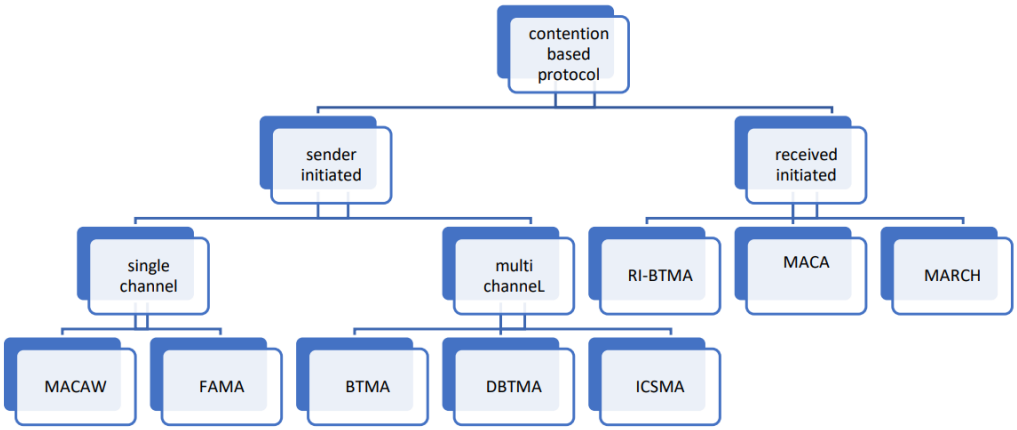
- **Contention-based** = Competing to send data.
- **Reservation** = Reserving time to send data.
- **Scheduling** = Scheduled times to send data.

6 b) Explain about Contention based MAC Layer Protocols

Contention-Based MAC Layer Protocols:

Contention-based protocols are used when multiple devices want to use the same communication channel. These devices don't reserve the channel in advance; they compete for it when they need to send

data. The device that wins the competition gets to send the data.



Two Types of Contention-Based Protocols:

1. **Sender-Initiated Protocols**:
    - Here, the sender starts the process of sending data.
    - **Single-Channel Sender-Initiated Protocols**: Only one device can send at a time. Examples:
        - **MACAW**: Helps wireless devices avoid collisions while sending data.

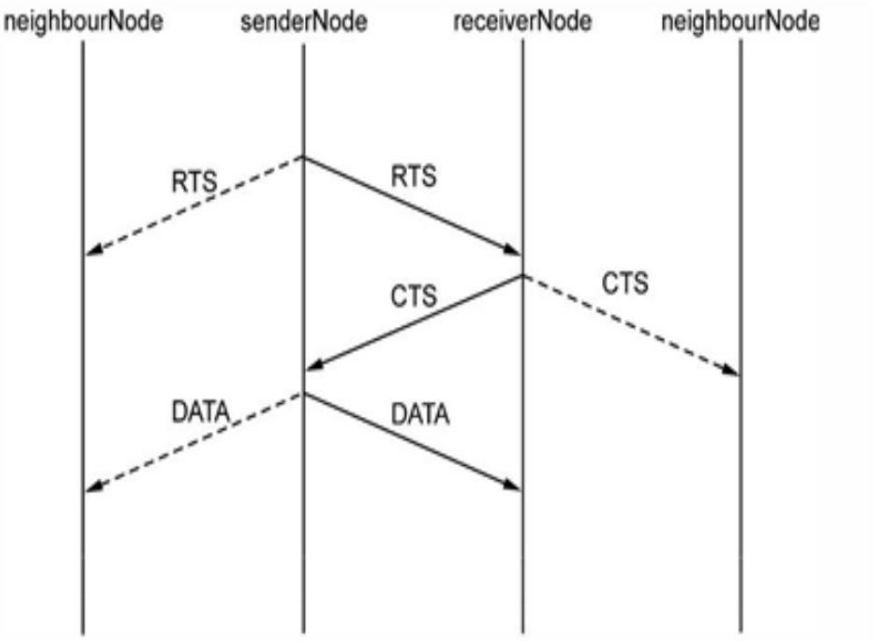


Fig. 2.2.2 MACA protocol initial signal / control message packet transfer

        - **FAMA**: Devices use a method to avoid collisions by controlling when they can send data.
    - **Multi-Channel Sender-Initiated Protocols**: The available bandwidth is split into multiple channels, so many devices can send data at the same time. Examples:
        - **BTMA**: The channel is split into two parts: one for sending data and one for control signals.
        - **DBTMA**: Similar to BTMA, but with two signals to help devices know when others are sending or receiving data.
2. **Receiver-Initiated Protocols**:
    - Here, the receiver controls when data can be sent.
    - **RI-BTMA**: The receiver controls the channel and signals when the sender can send data.
    - **MACA-BI**: The receiver tells the sender when to start sending data using a simple message.
    - **MARCH**: It reduces the number of messages needed before sending data.

In simple terms, **contention-based protocols** let devices take turns using the channel, either by the sender or receiver controlling when data can be sent.