1.Introduction

1. What is Mobile Computing

- Mobile computing refers to the ability to use computing devices (such as smartphones, tablets, laptops, or wearable devices) while being mobile, without the need for a fixed location.

- Mobile computing means using computers or devices (like smartphones, tablets, laptops) **anytime and anywhere without being fixed in one place**.

- It works using **wireless networks** (Wi-Fi, mobile data, Bluetooth, etc.).

- It allows you to:
  - **Send and receive data** (messages, emails, files).
  - **Access the internet and apps** from anywhere.
  - **Work or communicate on the move.**

Functions of Mobile Computing

1. **Data Communication**
   - Enables the transmission of data between devices using wireless technologies (e.g., 4G, 5G, Wi-Fi, Bluetooth).
   - Ensures seamless connectivity for accessing the internet, emails, or cloud-based services.
2. **Remote Access**
   - Provides access to applications, files, and systems stored in remote servers or cloud platforms.
   - Allows real-time data sharing and collaboration from any location.
3. **Mobility**
   - Ensures that users are not restricted to a single physical location.
   - Supports location-based services (LBS) such as GPS navigation.
4. **Data Synchronization**
   - Keeps data updated across multiple devices automatically.
   - For example, contacts, emails, or documents remain consistent on both smartphones and laptops.
5. **Real-Time Communication**
   - Facilitates instant communication via voice calls, video conferencing, messaging apps, or collaboration tools (Zoom, WhatsApp, Teams).
6. **Security Management**
   - Ensures data privacy and protection through encryption, authentication, VPNs, and secure access protocols.

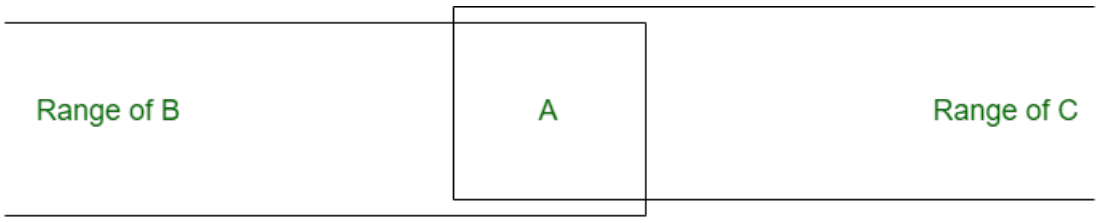
Applications of Mobile Computing

1. **Healthcare**
   - Remote patient monitoring, telemedicine, and mobile health apps.
2. **Education**
   - E-learning platforms, virtual classrooms, and access to digital resources.
3. **Business and Commerce**
   - Mobile banking, e-commerce platforms, and digital payment solutions.
4. **Transportation and Logistics**
   - GPS-based vehicle tracking, fleet management, and ride-hailing services (Uber, Ola).
5. **Entertainment**
   - Streaming services (Netflix, Spotify), online gaming, and social media.
6. **Government and Public Services**
   - Mobile apps for tax filing, e-governance, and public safety alerts.
7. **Travel and Tourism**
   - Online ticket booking, hotel reservations, and travel guides.

2.Explain the following term

I.Hidden terminal Problem:-

- When two stations hidden from each other i.e., not in range of each other send signals to third station at the same considering third station is free.
- It causes collision at third station and is known as Hidden Station Problem. It reduces capacity of network due to possibility of collision.
- Following is diagrammatically representation of Hidden Station Problem (HSP) in wireless LAN.



Hidden Station Problem

In a wireless network:

- Devices (stations) communicate with each other through a central access point (AP).
- However, not all devices are always within each other's radio range.

Imagine this scenario:

- Station A and Station C are both connected to the same access point (AP).
- A and C cannot hear each other's signals because they are physically far apart or obstructed (they are "hidden" from each other).
- Both try to transmit data to the AP at the same time, thinking the channel is free.
- This causes a collision at the AP, because both signals overlap.

Creation of HSP
In the above shown diagram, station B and C both covers station A in their own range. Each station B and C can send data to station A separately. Both stations B and C are outside of range of each other. Suppose station B is sending data to station A and in middle of transmission station C also has to send data to station A. Since station B and station C are out of each other range therefore station C thinks that station A is free. Station C send data to station A and collision occurs at station A.

Prevention of HSP

Hidden Station Problem (HSP) can be prevented by using handshake frames.

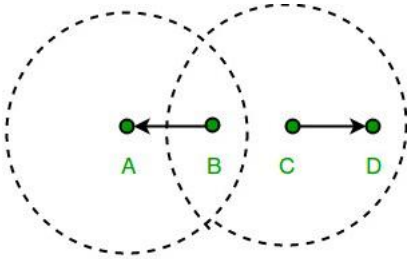
RTS : Request To Send
CTS : Clear To Send

II. Exposed Terminal Problem:-

The exposed terminal problem occurs in wireless networks when **a node (device) unnecessarily stops transmitting data because it senses another nearby transmission**, even though its own transmission would not create interference.

This leads to **wasted network capacity** and **reduced throughput** because multiple transmissions that could have happened at the same time are avoided unnecessarily.

Example Scenario



Imagine four stations: **A, B, C, and D**

- **B is transmitting data to A.**
- **C wants to send data to D.**
- **B and C are within each other's range**, so C can sense B's transmission.
- **A and D are out of each other's range**, so their communications would not interfere.

However, **C stops sending data to D** because it thinks its transmission will interfere with B → A communication, even though it would not.

This is called the **Exposed Terminal Problem**, as C becomes an "exposed terminal" unnecessarily.

Impact of Exposed Terminal Problem

1. **Wasted bandwidth** – Because transmissions are halted even when they could occur.
2. **Reduced throughput** – Less data is sent overall.
3. **Increased delay** – Nodes wait unnecessarily to transmit.

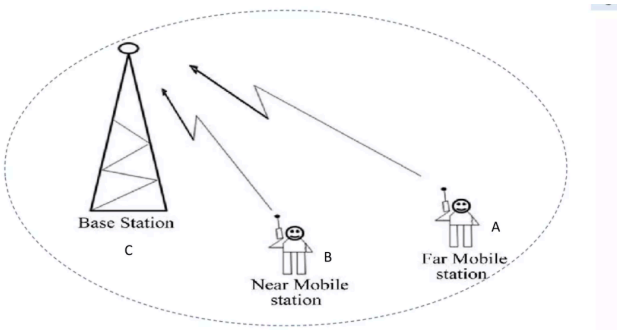
How to Prevent Exposed Terminal Problem?

The most common solution is using **RTS/CTS (Request to Send / Clear to Send) mechanism**, which is part of the IEEE 802.11 protocol.

III.Near-Far Problem (Simple Explanation)

The **near-far problem** happens in **CDMA (Code Division Multiple Access)** when two mobile devices—one close to the base station and one far away—**send signals at the same time**.

- The **near device** sends a strong signal.
- The **far device** sends a weak signal (because signal strength becomes weaker as distance increases).
- The strong signal **overpowers (drowns out)** the weak one, so the base station cannot hear the far device properly.



Example (Simple)

- Stations: **A, B, C**
- **A and B are sending to C (receiver/ base station)**
- B is close to C → Strong signal
- A is far from C → Weak signal
- **Result:** B's strong signal covers A's weak signal → C cannot receive A's data.

Why does it happen?

- Because in open space, signal strength becomes weaker as distance increases.
- The further a device is, the weaker its signal.

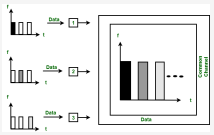
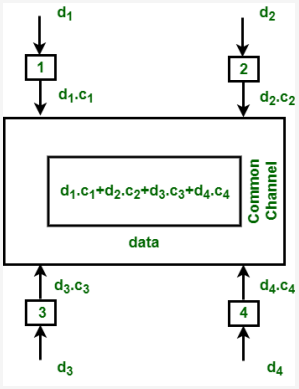
Effects of Near-Far Problem

1. **Far device loses connection or data gets lost.**
2. **Network bandwidth reduces.**
3. **Poor coverage for far devices.**

How to Solve It?

1. **Power control:** Adjusts the power of near devices to match far ones.
2. **Proper scheduling:** Gives time slots to far devices to avoid interference.
3. **Advanced CDMA techniques:** Help reduce signal interference.

FDMA	TDMA	CDMA	SDMA
FDMA stands for Frequency Division Multiple Access.	TDMA stands for Time Division Multiple Access.	CDMA stands for Code Division Multiple Access.	Space 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.	Divides users based on their physical location (space/area).
There is no need of any codeword.	There is no need of any codeword.	Codeword is necessary.	No codeword is needed.
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.	Guard sectors/angles between beams may be required.
Synchronization is not required.	Synchronizatio n is required.	Synchronization is not required.	Minimal synchronization needed (mainly antenna alignment).
The rate of data is low.	The rate of data is medium.	The rate of data is high.	Depends on the spatial design; generally **high** in dense setups.
Mode of data transfer is continuous signal.	Mode of data transfer is signal in bursts.	Mode of data transfer is digital signal.	Data transfer based on spatial beams/sectors.
It is little flexible.	It is moderate flexible.	It is highly flexible.	Highly flexible in dense environments using smart antennas.

3. Explain:-

i) Classical ALOHA

Classical ALOHA is an early network protocol used for data communication where users send data whenever they want **without checking if the channel is free**.

How it Works?

1. A station sends data whenever it has information to send.
2. If two or more stations send data at the same time → **collision occurs** → data is lost.
3. If no collision → data is received successfully.
4. After a collision, the station waits for a random time and retransmits.

Efficiency

- Very low: Maximum throughput is about **18.4% (1/2e)** because collisions happen frequently.

Key Points

- No synchronization required.
- Simple but inefficient.
- Suitable for low traffic.

ii) Slotted ALOHA

An improved version of ALOHA that **divides time into equal slots** and allows transmission **only at the start of each time slot**.

How it Works?

1. Time is divided into fixed slots.
2. A station waits for the beginning of a slot to send data.
3. If two or more stations send in the same slot → collision occurs.
4. If only one station sends → data is received successfully.
5. After a collision, the station waits for a random slot and retransmits.

Efficiency

- Higher than classical ALOHA: Maximum throughput is about **36.8% (1/e)**.

Key Points

- Requires synchronization of time slots.
- Reduces collisions compared to classical ALOHA.
- Better for moderate traffic.

4.Write a short note of CSMA/CD and CSMA/CA.

I. What is CSMA/CA

CSMA/CA stands for **Carrier Sense Multiple Access / Collision Avoidance** is a network protocol for carrier transmission.

Like CSMA/CD it is also operated in the medium access control layer. Unlike CSMA/CD(that is effective after a collision) CSMA / CA is effective before a collision.

Advantages of CSMA/CA

- Collision Reduction
- Better for Wireless Networks
- Efficient Channel Use
- Energy Efficient

Disadvantages of CSMA/CA

- Lower Throughput
- Delay and Latency
- Complex Implementation
- Inefficiency in High Traffic

II. What is CSMA/CD

CSMA/CD stands for **Carrier Sense Multiple Access / Collision Detection** is a network protocol for carrier transmission.

It is operated in the medium access control layer. It senses that the shared channel is busy broadcasting and interrupts the broadcast until the channel is free.

In CSMA/CD collision is detected by broadcast sensing from the other stations. Upon collision detection in CSMA/CD, the transmission is stopped, and a jam signal is sent by the stations and then the station waits for a random time context before retransmission.

Advantages of CSMA/CD

- Efficient for Wired Networks
- Reduces Collisions
- Balances Network Traffic
- Simple to Implement

Disadvantages of CSMA/CD

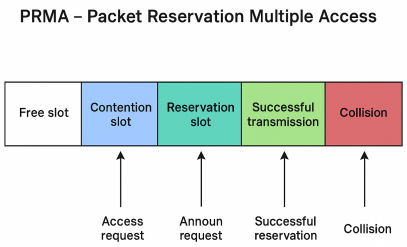
- **Not Suitable for Wireless Networks**
- **Adds Latency**
- **Lower Efficiency in Busy Networks**
- **Less Common in Today's Era**

CSMA/CA	CSMA/CD
CSMA / CA is effective before a collision.	CSMA / CD is effective after a collision.
CSMA / CA is commonly used in wireless networks.	CSMA / CD is used in wired networks.
CSMA/ CA minimizes the possibility of collision.	It only reduces the recovery time.
CSMA / CA will first transmit the intent to send for data transmission.	CSMA / CD resends the data frame whenever a conflict occurs.
CSMA / CA is used in 802.11 standard.	CSMA / CD is used in 802.3 standard.
It is similar to simple CSMA(Carrier Sense Multiple Access).	It is more efficient than simple CSMA(Carrier Sense Multiple Access).
It is the type of CSMA to avoid collision on a shared channel.	It is the type of CSMA to detect the collision on a shared channel.
It is work in MAC layer.	It also work in MAC layer.

5.PRMA – Packet Reservation Multiple Access

PRMA (Packet Reservation Multiple Access) is a **channel access method** used in wireless and satellite communication systems to efficiently transmit packet-based data and voice over shared channels.

It is a combination of **TDMA (Time Division Multiple Access)** and **reservation-based access**.



What is PRMA?

- PRMA allows multiple users to share a communication channel using **time slots**, but it also includes a **reservation mechanism** so users can reserve slots for future transmissions.
- It is mainly used in **packet-switched networks** where users transmit data intermittently (bursty traffic).

How PRMA Works?

1. **Channel Division:**
    - The available bandwidth is divided into **time frames**, and each frame has multiple time slots.
2. **Contention Phase (Access Request):**
    - When a user wants to transmit, it sends a packet in the next free time slot.
    - Multiple users may try to send at the same time → this can cause **collisions**.
3. **Reservation Phase:**
    - If the packet is received successfully, the base station reserves the slot for that user for future packets.
    - If collision occurs, users retry after a random backoff time.
4. **Data Transmission:**
    - Once reserved, the user transmits subsequent packets in its allocated slot without contention.
5. **Release:**
    - When the user finishes transmitting, the slot is released for others.

Key Features of PRMA

- **Reservation-based**: Reduces collisions after the first successful attempt.
- **Supports bursty traffic**: Ideal for voice packets and intermittent data.
- **Improved efficiency** over pure ALOHA or slotted ALOHA.

Advantages

- High channel efficiency.
- Reduces delay for continuous transmissions.
- Fair allocation for active users.

Disadvantages

- Initial collisions during access requests.
- Requires **synchronization** (like TDMA).
- Slight delay for reservation setup.

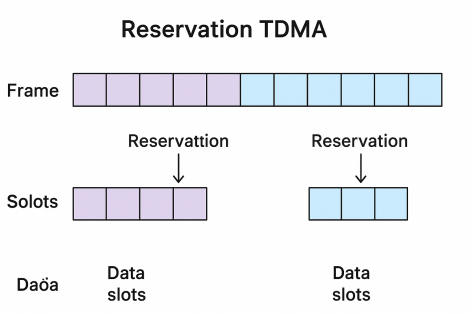
Applications

- Wireless networks with voice/data integration.
- Satellite communication.
- Mobile cellular systems (early GSM-like networks).

6.Reservation TDMA (Time Division Multiple Access)

Reservation TDMA is an enhanced form of TDMA where time slots are **reserved in advance** for users who want to transmit data.

Unlike pure TDMA, where each user has a fixed slot, Reservation TDMA allows **dynamic allocation of slots** based on demand.



How Reservation TDMA Works

1. **Frame Division:**
   - The communication channel is divided into frames, and each frame contains multiple time slots.
2. **Reservation Phase:**
   - Users send a **reservation request** in special reservation slots within a frame.
3. **Slot Allocation:**
   - The base station (or central controller) assigns slots to users based on their requests.
4. **Data Transmission:**
   - After slots are reserved, users send their data in the assigned slots.
5. **Release:**
   - Once data is transmitted, the reserved slot is freed for other users.

Key Features

- **Efficient for bursty traffic**, as slots are used only when needed.
- **Centralized control** manages reservations.
- **Reduces collisions** compared to ALOHA and other contention-based protocols.

Advantages

- Higher efficiency compared to fixed TDMA.
- Fair allocation of resources.
- Reduces idle slots.

Disadvantages

- **Overhead for reservation process.**
- Requires synchronization and central control.
- May cause slight delay before transmission.

Applications

- Satellite communication systems.
- Wireless LANs.
- Cellular networks with variable data transmission.

7.ISMA – Inhibit Sense Multiple Access

ISMA (Inhibit Sense Multiple Access) is a **medium access control (MAC) protocol** used in wireless and satellite communication to manage how multiple devices share a communication channel.

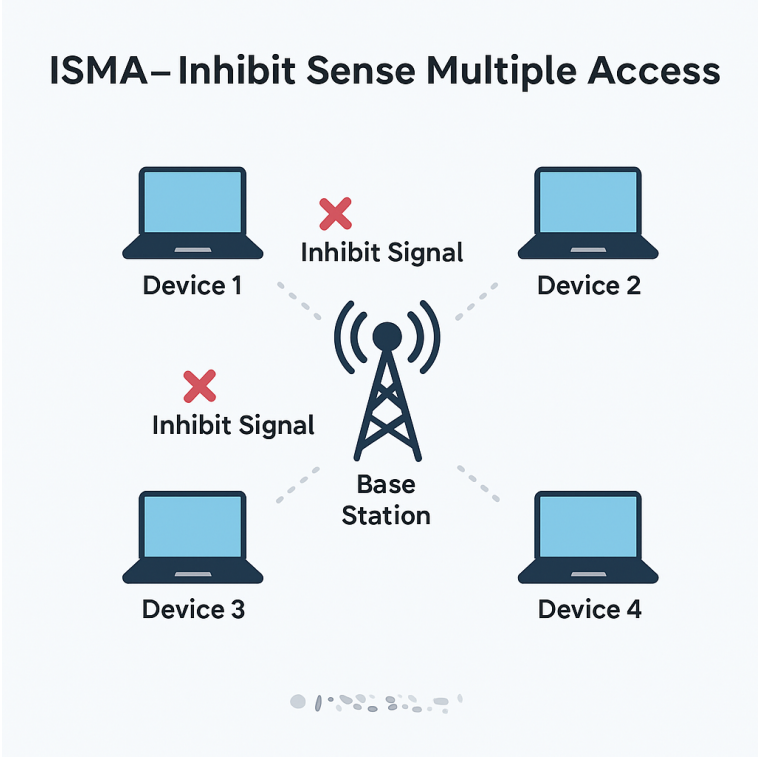
It helps in avoiding collisions and ensuring efficient channel utilization.

How ISMA Works

- ISMA is based on **Carrier Sense Multiple Access (CSMA)** principles.
- Instead of just listening to the channel, ISMA uses **control signals from a central station (base station)**.
- Devices can transmit only when they get an **"inhibit" signal cleared** from the central station.
- If the central station sends an **inhibit signal**, other stations must wait to avoid collisions.

Importance of ISMA

1. **Collision Avoidance:** Prevents multiple devices from sending data at the same time, reducing interference.
2. **Efficient Channel Utilization:** Ensures the communication medium is used effectively.
3. **Better Control:** The base station manages transmissions, leading to more stable communication.
4. **Improved Performance in Satellite and Wireless Networks:** Suitable for networks where propagation delay is high.
5. **Reduces Retransmissions:** Minimizes data loss and the need for retransmission.
6. **Energy Saving:** Devices transmit only when allowed, saving power.
7. **Supports Multiple Users:** Enables multiple stations to share the same channel without chaos.



8.Short Note on Pure ALOHA

Pure ALOHA is one of the simplest and earliest channel access protocols used for wireless and satellite communication.

It allows users to transmit data **whenever they have data to send**, without checking if the channel is free.

Pure ALOHA is a basic method to send data over a shared network channel.

- Any device can send data **whenever it wants** without checking if someone else is sending.
- If two devices send data at the same time, their signals **collide**, and both messages are lost.

How Does It Work?

1. A device sends a data packet.
2. It waits for an **acknowledgment (ACK)** from the receiver.
3. If the ACK comes → the transmission was successful.
4. If no ACK → a **collision happened**, and the data was lost.
5. The device waits for a **random time (back-off time)** and then tries again.

Vulnerable Time (Collision Zone)

- Each packet takes a certain time to send (let's call it *tp*).
- A collision can happen if another packet starts sending **during the packet's time OR within one more packet time after it started (2 × tp)**.
- So, the **vulnerable period is 2 × tp**.

Problems with Pure ALOHA

- **Collisions are very common**, especially when many users are sending data.
- **Efficiency is low** — only about 18% of the channel is used effectively.
- **No check before sending**, so many packets get wasted.

Example in Real Life

Imagine a group of people talking on a walkie-talkie without saying "over" before speaking.

- If two people talk at the same time, **both messages are lost**.
- They wait randomly before speaking again to avoid another clash.