# UNIT - 3 IOT Notes - R1

**UNIT 3: Wireless Medium Access Issues and MAC Protocols**

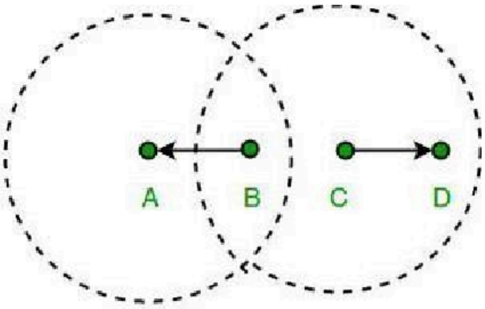
**1. Introduction to Wireless Medium Access in IoT**

- **Definition:** Refers to the methods and protocols used to manage how multiple IoT devices communicate over shared wireless communication channels. (Notes Page 1)
- **Importance of Efficient MAC:** Critical in IoT networks for:
  - Ensuring reliable data transmission.
  - Minimizing collisions and interference.
  - Optimizing the use of limited wireless spectrum. (Notes Page 1)
- **Challenges:**
  - Dense and heterogeneous nature of IoT environments.
  - Interference from other present wireless communication technologies. (Notes Page 1)
- **Wireless Communication:** Involves message transfer without physical medium (wires). (Notes Page 1)

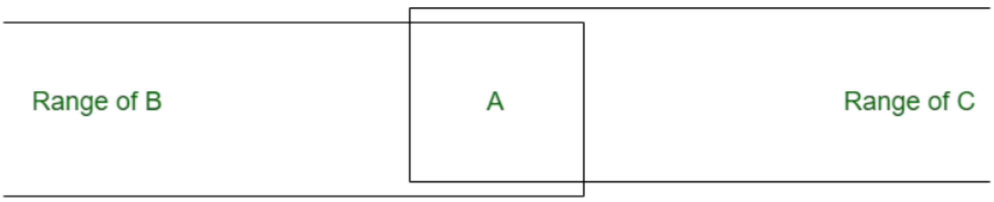
**2. Issues in MAC Design for Wireless Networks**

- Compared to wired networks, MAC design for wireless is more difficult due to unique challenges. (Notes Page 1)
  - **a. Half Duplex Operation:** (Notes Page 1)
    - Sender and receiver can share data, but only one at a time.
    - Difficult to receive data when the transmitter is sending due to significant signal energy leakage during broadcasting.
    - Magnitude of transferred and received signal differs greatly.
    - Collision detection by the sender is often not possible because the intensity of the transferred signal is much larger than the received one (if any).
    - Leads to collision problems; prime focus is to minimize collisions.
  - **b. Time-Varying Channel:** (Notes Page 2)
    - Radio signal propagation is affected by three mechanisms:
      - **Reflection:** Occurs when a propagating wave (carrying information) intrudes on an object with dimensions much larger than the wave's wavelength.
      - **Diffraction:** Occurs when the radio path between transmitter and receiver is obstructed by a surface with sharp edges, causing the wave to bend around the obstacle.

        - **Scattering:** Occurs when the medium through which the wave travels contains objects with dimensions smaller than the wave's wavelength.
- **c. Exposed Terminal Problem:** (Notes Page 2)
    - **Definition:** A wireless node is prevented from transmitting data because another node (outside its communication range) is sending data to a third node that *is* within the first node's communication range.
    - **Scenario:**




        - Four stations: A, B, C, D.
        - B transmits to A. C wants to transmit to D.
        - B and C can hear each other. A and D cannot hear each other.
        - C hears B's transmission and mistakenly assumes its own transmission to D would interfere, so C refrains from sending.
        - However, C's transmission to D would not have interfered with B's reception at A (as A is out of C's range, and D is out of B's range for interference).
    - **Consequence:** Reduced throughput and network performance.
- **d. Hidden Station Problem (HSP) / Hidden Terminal Problem:** (Notes Page 3)
    - **Definition:** Two stations are "hidden" from each other (not in each other's range) but are both in the range of a third station. If they transmit simultaneously to the third station, a collision occurs at that third station.
    - **Scenario:**

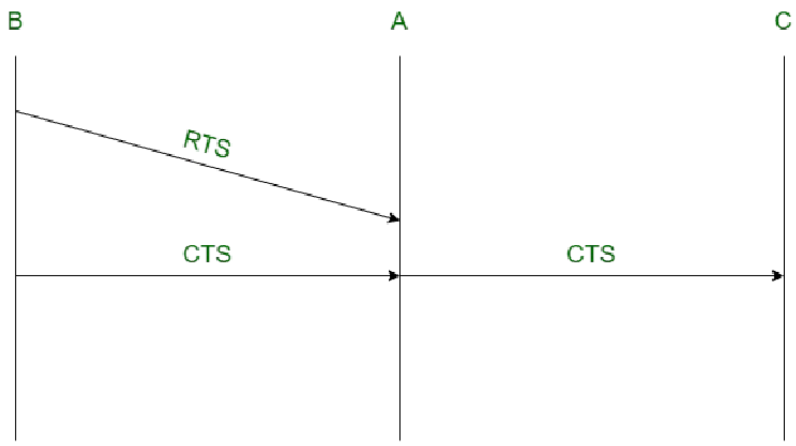



Hidden Station Problem

        - Stations B and C are hidden from each other.
        - Station A is within range of both B and C.
    - **How HSP is created:** (Notes Page 4)
        - B sends data to A.

- C, unaware of B's transmission (because B is out of C's range), also decides to send data to A, assuming A is free.
- Collision occurs at station A.

- **Consequence:** Reduces network capacity due to collisions.
- **How to prevent HSP:** (Notes Page 4)
  - Using handshake frames like RTS (Request to Send) and CTS (Clear to Send).

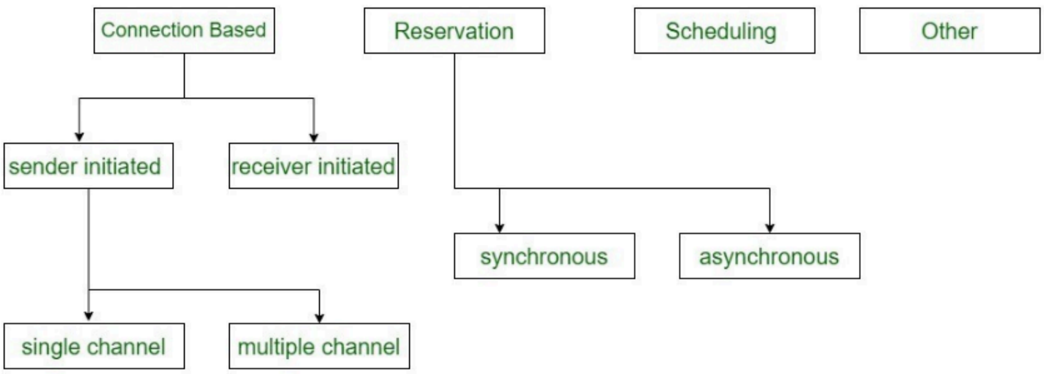



Use of handshaking to prevent hidden station problem

  - **Mechanism:**
    - Node B sends RTS to A.
    - Node A replies with CTS. This CTS is heard by C.
    - CTS message contains the duration of B's upcoming data transmission.
    - Node C, upon hearing the CTS, knows the medium will be busy for that duration and refrains from transmitting, thus avoiding collision.

**3. Classification of MAC Protocols** (Notes Page 4)

- MAC protocols can be broadly classified based on how nodes access the medium.




- [FIG] (Diagram on Notes Page 4 showing main categories: Connection Based, Reservation, Scheduling, Other. Further breakdown on Notes Page 5: sender/receiver initiated, synchronous/asynchronous, single/multiple channel).

**4. MAC (Medium Access Control) Layer** [PYQ Q7a (Dec 2024), PYQ Q5a (June 2024 - Data-link layer protocols)] (Notes Page 5)

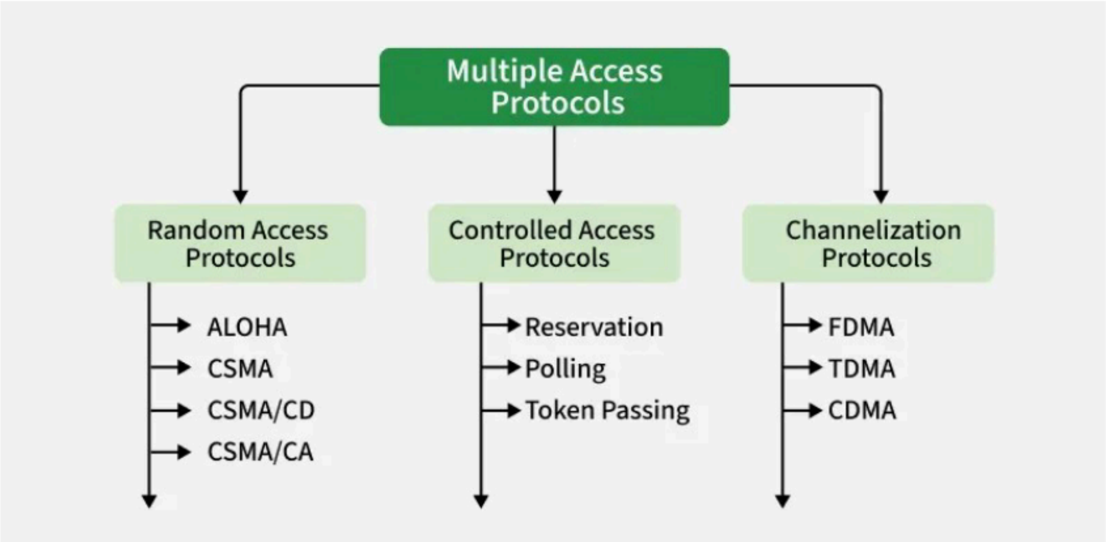
- **Definition:** A sublayer of the Data Link Layer (Layer 2) in the OSI reference model.
- **Responsibilities:**
    - Flow control.
    - Multiplexing for the transmission medium.
    - Controls transmission of data packets via remotely shared channels.
    - Controlling how devices on a shared network gain access to and utilize the communication medium.
    - Coordinating access to the shared medium.
    - Preventing collisions to enable multiple devices to share network bandwidth effectively.

**5. Contention-Based Protocols**

- **a. Contention-Based Protocols Without Reservation/Scheduling:** (Notes Page 5)
- **Mechanism:** Multiple devices attempt to access the channel simultaneously without explicit coordination.
    - When collisions occur, devices back off and try again.
    - Devices transmit when they have data, relying on techniques like carrier sensing or random backoffs to reduce collisions.
    - **Characteristics:**
        - Simple to implement.
        - Adaptive to changing network conditions.
    - **Key Points:**
        - Bandwidth is not reserved.
        - No guarantees of successful transmission on first attempt.
    - **Sub-types:** (Notes Page 6)
        - **Sender-initiated protocols:** Transmission of packets is initiated by the sender node.
        - **Single-channel sender initiated.**
        - **Multiple-channel sender initiated protocols.**
        - **Receiver-initiated protocols:** The connection is initiated by the receiver node.
- **b. Contention-Based Protocols With Reservation Mechanisms:** (Notes Page 6)
- **Mechanism:** A central controller periodically polls devices to grant them exclusive access to the channel, ensuring each gets a turn. A master/base station queries each device, and only the polled device is allowed to transmit.
    - **Key Points:**

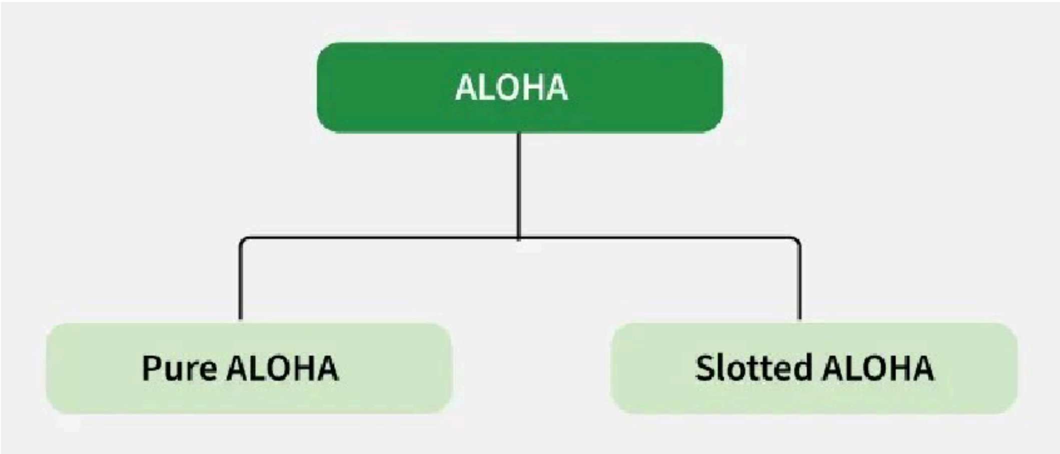
        - Bandwidth is reserved for transmission.
        - Guarantees (e.g., for timely delivery) can be given.
    - **Types based on timing:**
        - **Synchronous protocols:** Data is sent in continuous streams or blocks without start/stop bits for each character. Sender and receiver must be synchronized with a common clock signal. More complex to implement.
        - **Asynchronous protocols:** Data is sent character-by-character, with start and stop bits added for synchronization. Easier and less expensive to implement. Less efficient due to overhead of start/stop bits. Relative time information is used for effective reservations.
- **c. Contention-Based Protocols with Scheduling Mechanisms:** (Notes Page 7)
- **Mechanism:** The network allocates specific time/frequency/code resources to each device, so transmissions do not overlap. Each station is assigned a unique time slot, frequency band, or spreading code.
    - **Characteristics:**
        - Ensures non-interfering transmissions.
        - Provides deterministic access.
        - Predictable Quality of Service (QoS).
        - Efficient utilization under steady traffic conditions.
    - **Examples:**
        - Polling schemes in Bluetooth piconets (master polls slaves).
        - Industrial networks using a central controller.
    - **Ideal for:** Networks needing strict timing guarantees (e.g., industrial control systems, sensor networks requiring reliable data collection).
    - **Also used in:** Cellular networks, satellite communications where guaranteed bandwidth and predictable latency are critical.
- **d. Other Hybrid Protocols:** (Notes Page 7)
- **Mechanism:** Combine features of contention-based and scheduled approaches (or other methods) to balance flexibility, efficiency, and reliability.
    - Part of the bandwidth or time is allocated deterministically (scheduled slots), while the remainder is accessed using contention or polling.
    - **Characteristics:**
        - Adaptable to varying traffic conditions.
        - Can provide QoS guarantees.
        - Can handle heavy traffic efficiently.

**6. Subdivisions of Multiple Access Protocols** (Notes Page 7)

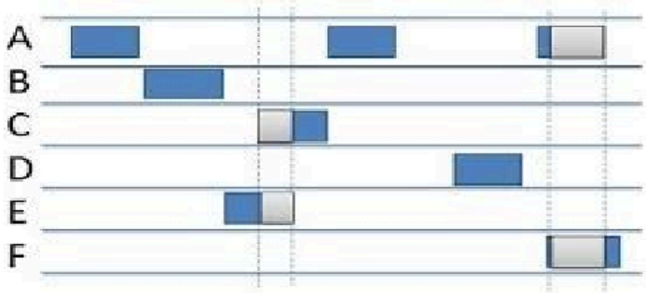



* **1. Random Access Protocols**
* **2. Controlled Access Protocols**
* **3. Channelization Protocols**

- **6.1. Random Access Protocols:** [PYQ Q5a (June 2024 - Data-link layer protocols)] (Notes Page 8)
- **Principle:** All stations have the same priority. Any station can send data depending on the medium's state (idle or busy).
  - **Features:**
    - No fixed time for sending data.
    - No fixed sequence of stations sending data.
  - **Types:**
    - **A. ALOHA:** (Notes Page 8)
      - Originally designed for wireless LANs, also applicable for shared medium.
      - Multiple stations can transmit data at the same time, leading to collisions and garbled data.



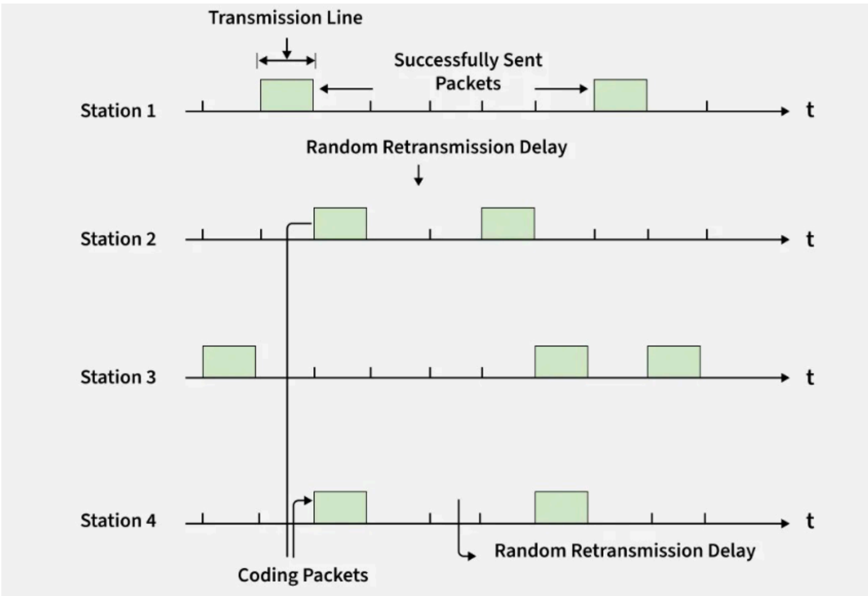
- **Pure ALOHA:**




Pure ALOHA

  - Station sends data and waits for an acknowledgement.
  - If no ACK within allotted time, station waits for a random back-off time (Tb) and re-sends.
  - Different back-off times for different stations reduce probability of further collision.

- **Slotted ALOHA:** (Notes Page 9)
  - Time is divided into discrete slots.
  - Data transmission is allowed only at the beginning of a time slot.
  - If a station misses the allowed time, it must wait for the next slot.
  - Reduces the probability of collision compared to Pure ALOHA (vulnerable period is halved).

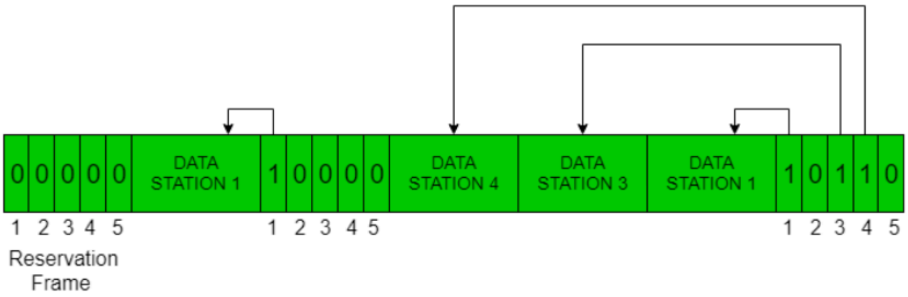



- **B. CSMA (Carrier Sense Multiple Access):** (Notes Page 10)
  - **Principle:** Station first senses the medium (carrier) before transmitting.
  - If idle, sends data. If busy, waits until the channel becomes idle.
  - **Collision Possibility:** Collisions can still occur due to propagation delay.
    - Example: Station A senses medium as idle and starts sending. Before A's signal reaches B, B might also sense the medium as idle and start sending, leading to a collision.
- **C. CSMA/CD (Carrier Sense Multiple Access with Collision Detection):** (Notes Page 10)

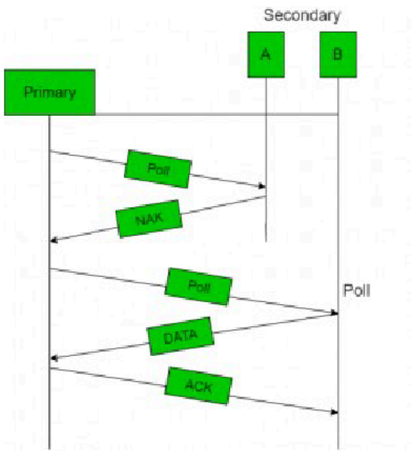
        - **Principle:** Stations can detect collisions while transmitting.
        - If a collision is detected, stations terminate their transmission, wait a random back-off period, and try again.
        - Commonly used in wired Ethernet (e.g., IEEE 802.3).
      - **D. CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance):** (Notes Page 11)
        - **Principle:** Used in networks where collision detection is difficult or unreliable (e.g., wireless networks like IEEE 802.11).
        - Aims to *avoid* collisions rather than just detect them.
        - Collision detection in wireless involves sender receiving acknowledgement signals. One signal (its own reflected) might imply success if strong enough, but if two signals (its own + another's) are mixed, it means collision. Collision must have a significant impact on received signal to be detectable, which is not always true in wireless.
        - **Mechanisms to Avoid Collision:**
          - **Interframe Space (IFS):** Station waits for a specific period (IFS) after the medium becomes idle before attempting to transmit. IFS duration can depend on the priority of the station/traffic.
          - **Contention Window:** An amount of time divided into slots. If ready to send, sender chooses a random number of slots as a wait time. This window size (number of slots) typically doubles each time the medium is found busy or a collision occurs (Exponential Backoff). The timer pauses if the medium becomes busy and resumes when idle again.
          - **Acknowledgement (ACK):** The sender re-transmits data if an ACK is not received from the receiver before a timeout.
- **6.2. Controlled Access Protocols:** [PYQ Q5a (June 2024 - Data-link layer protocols)] (Notes Page 11)
- **Principle:** Stations seek permission or are granted turns to send data. Only one node is typically allowed to send at a time on a shared medium, avoiding collisions.
  - **Methods:**
    - **A. Reservation:** (Notes Page 12)
      - **Mechanism:** A station needs to make a reservation before sending data.
      - **Timeline:** Consists of:
        - Reservation interval: Fixed time length, divided into mini-slots (e.g., M mini-slots for M stations). Each station has one mini-slot to signal its intent to send.
        - Data transmission period: Variable length, where stations that made reservations transmit their data in order.
      - **Process:**

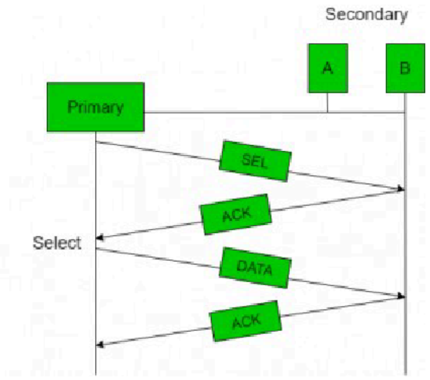
- During its mini-slot in the reservation interval, a station with data transmits a bit.
- After all mini-slots, every station knows which stations wish to transmit.
- Stations transmit their frames in the agreed-upon order.
- A new reservation interval begins after the data transmission period.

- **Advantage:** No collisions during data transmission as the order is pre-determined.

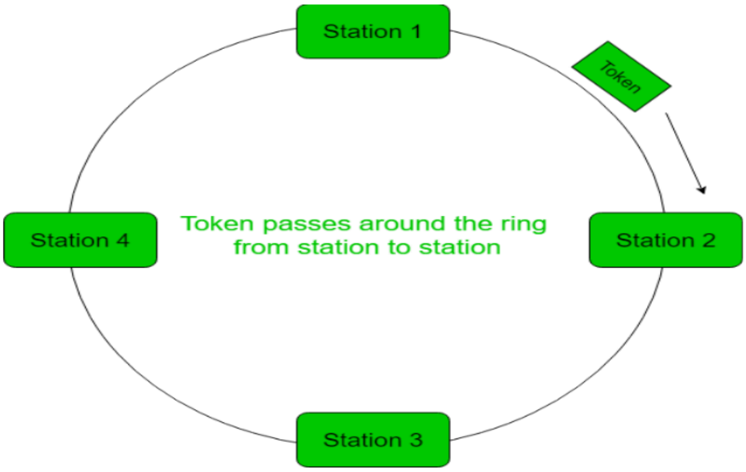



- **B. Polling:** (Notes Page 13)
  - **Mechanism:** A central controller (primary station) polls each secondary station in turn, granting them permission to transmit.
  - **Process:**
    - Primary station sends a poll message to a secondary station (message contains the address of the selected node).
    - All data exchanges must go through or be authorized by the controller.
    - The addressed secondary station responds by sending its data (if any) or a negative acknowledgment (NAK/poll reject) if it has no data.
  - **Problems:**
    - High overhead due to polling messages.
    - High dependence on the reliability of the controller.






    - [FIG] (Diagrams illustrating polling with NAK and polling with data transmission on Notes Page 14)
- **C. Token Passing:** (Notes Page 14)
    - **Mechanism:** Stations are connected logically (e.g., in a ring or bus topology). A special control frame called a "token" circulates among the stations in a predefined order.
    - **Token:** Represents permission to send. A special bit pattern or small message.
    - **Process:**
        - A station wanting to transmit must wait until it receives the token.
        - Upon receiving the token, if the station has data, it seizes the token, sends its data frame(s), and then releases/passes the token to the next station in the logical sequence.
        - If a station receives the token but has no data, it passes the token immediately. (Notes Page 15)
        - After sending a frame, a station must wait for the token to circulate through all N stations (including itself) and potentially for other N-1 stations to send a frame before it can send again.
    - **Topologies:**
        - **Token Ring:** Token passed to the adjacent station in a physical or logical ring.
        - **Token Bus:** Token passed to the next station in a logical sequence over a shared bus.
    - **Problems:** Token duplication, token loss, insertion/removal of new stations require careful management.




- **6.3. Channelization Protocols (Channel Partitioning):** [PYQ Q5a (June 2024 - Data-link layer protocols)] (Notes Page 15)
- **Principle:** The available bandwidth of the link is shared in time, frequency, or code among multiple stations to allow simultaneous access.
  - **Types:**
    - **A. Frequency Division Multiple Access (FDMA):** (Notes Page 16)
      - Available bandwidth is divided into equal, non-overlapping frequency bands.
      - Each station is allocated its own band.
      - Guard bands (unused frequency strips) are used between allocated bands to prevent crosstalk and noise.
    - **B. Time Division Multiple Access (TDMA):** (Notes Page 16)
      - Bandwidth is shared by dividing access time into slots.
      - Each station is allotted specific time slots to transmit data.
      - **Overhead:** Synchronization bits are needed in each slot so stations know their turn.
      - **Issue:** Propagation delay; resolved by adding guard times between slots.
    - **C. Code Division Multiple Access (CDMA):** (Mentioned in diagram on Notes Page 8, but not detailed in text)
      - Allows multiple users to share the entire frequency spectrum at the same time.
      - Users are separated by unique codes.

**7. Wireless Sensor Network (WSN)** [PYQ Q5a (June 2024), PYQ Q5b (June 2024)] (Notes Page 16)

- **Definition:** An infrastructure-less wireless network deployed with a large number of wireless sensors in an ad-hoc manner. Used to monitor the system, physical, or environmental conditions.
- **Sensor Nodes:**
  - Equipped with an onboard processor.
  - Manage and monitor the environment in a particular area.
  - Connected to a Base Station, which acts as a processing unit.

- **Base Station:** Connected through the Internet to share data.

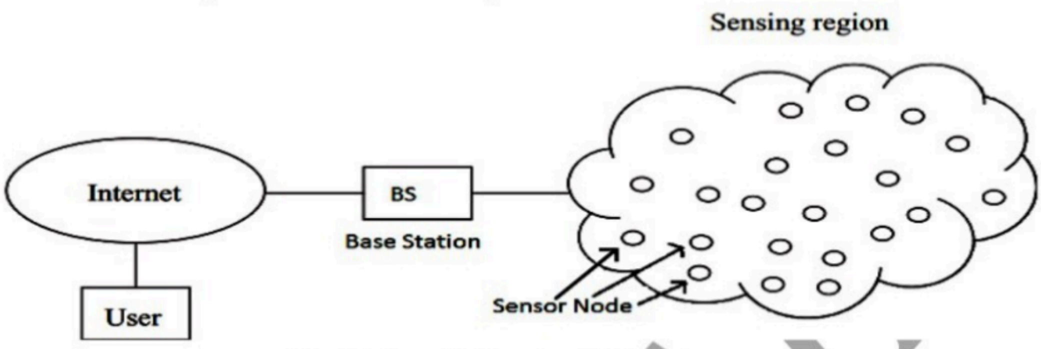



Fig. 3.1 Base Station in a WSN System

- **7.1. Components of WSN:** (Notes Page 17)
    - **1. Sensors:** Capture environmental variables for data acquisition; convert sensor signals into electrical signals.
    - **2. Radio Nodes:** Receive data produced by sensors and send it to the WLAN access point. Consist of a microcontroller, transceiver, external memory, and power source.
    - **3. WLAN Access Point:** Receives data sent by Radio nodes wirelessly, generally through the internet.
    - **4. Evaluation Software:** Processes data received by the WLAN Access Point. Presents reports to users for further processing, analysis, storage, and mining of data.
- **7.2. Applications of WSN:** (Notes Page 17)
    - Internet of Things (IoT)
    - Surveillance and Monitoring (for security, threat detection)
    - Environmental monitoring (temperature, humidity, air pressure)
    - Noise Level monitoring of surroundings
    - Medical applications (e.g., patient monitoring)
    - Agriculture
    - Landslide Detection
- **7.3. Modern Wireless Sensor Network (WSN) Challenges:** [PYQ Q5a (June 2024 - security aspects), PYQ Q5b (June 2024 - node behaviours influenced by these)] (Notes Page 17-18)
    - **a) Limited power and energy:** Typically battery-powered sensors with finite energy. Challenging to ensure long network lifetime without frequent battery replacements.
    - **b) Limited processing and storage capabilities:** Sensor nodes are usually small, restricting complex tasks or large data storage.
    - **c) Heterogeneity:** Networks often consist of various sensor types and nodes with different capabilities. Ensuring effective and efficient network function is a challenge.
    - **d) Security:** [PYQ Q5a (June 2024)] WSNs are vulnerable to attacks like eavesdropping, jamming, and spoofing. Ensuring network and data security is crucial.
    - **e) Scalability:** Often need to support a large number of sensor nodes and handle large data volumes. Scaling to meet demands is a significant challenge.

        - **f) Interference:** Often deployed in environments with interference from other wireless devices, making reliable communication difficult.
        - **g) Reliability:** Used in critical applications (e.g., environmental monitoring, industrial processes). Ensuring reliable function in all conditions is a major challenge.
    - **7.4. Advantages of Wireless Sensor Networks (WSN):** (Notes Page 18)
        - **a) Low cost:** Small, low-cost sensors are easy to deploy, making WSNs cost-effective.
        - **b) Wireless communication:** Eliminates need for wired connections (costly, difficult to install). Enables flexible deployment and reconfiguration.
        - **c) Energy efficiency:** Use low-power devices and protocols to conserve energy, enabling long-term operation.
        - **d) Scalability:** Can be easily scaled up or down by adding/removing sensors, suitable for various applications/environments.
        - **e) Real-time monitoring:** Enable real-time monitoring of physical phenomena, providing timely information for decision-making and control.
    - **7.5. Disadvantages of Wireless Sensor Networks (WSN):** (Notes Page 19)
        - **a) Limited range:** Wireless communication range is limited, a challenge for large-scale deployments or obstructed environments.
        - **b) Limited processing power:** Low-power devices may have limited processing/memory, hindering complex computations or advanced applications.
        - **c) Data security:** Vulnerable to security threats, compromising data confidentiality, integrity, and availability.
        - **d) Interference:** Susceptible to interference from other wireless devices/signals, degrading data transmission quality.
        - **e) Deployment challenges:** Proper sensor placement, power management, and network configuration can be complex and require significant time/resources.

**8. Routing in WSNs** [PYQ Q5a (June 2024 - Network layer protocols)]

- **Survey routing protocols:** (Notes Page 19)
  * **Definition:** Process to select a suitable path for data to travel from source to destination.
  * **Influencing factors:** Network type, channel characteristics, performance metrics.
  * **Data flow in WSN:** Sensed data -> Base Station -> Other networks (e.g., Internet) for collection, analysis, action.
- **8.1. Routing challenges in WSNs:** (Notes Page 19)
  * **Universal Identifiers:** Difficult to allocate for a large quantity of sensor nodes; thus, WSN motes often cannot use classical IP-based protocols.
  * **Data Flow Pattern:** Predominantly from multiple sources (sensor nodes) to a specific base station (sink).
  * **Data Redundancy:** Multiple sensing nodes may generate similar data. Routing protocols should exploit this redundancy for bandwidth and energy efficiency. (Notes Page 20)

- **8.2. Classification of routing protocols (based on information update mechanism for Ad hoc):** (Notes Page 20)
  - **A. Proactive or Table-Driven Routing Protocols:**
    - Each node maintains network topology information (routing tables).
    - Routing information is exchanged periodically and typically flooded throughout the network.
    - When a path is needed, node runs a pathfinding algorithm on its stored topology information.
  - **B. Reactive or On-Demand Routing Protocols:**
    - Nodes do not maintain network topology information continuously.
    - A path is discovered only when it is required, typically by initiating a connection establishment process (route discovery).
  - **C. Hybrid Routing Protocols:**
    - Combine features of proactive and reactive protocols.
    - Nodes within a certain distance or "routing zone" use a table-driven approach.
    - For nodes beyond this zone, an on-demand approach is used.
- **8.3. Specific Types of WSN Routing Protocols:** [PYQ Q5a (June 2024)]
  - **A. Hierarchical Routing Protocols:** (Notes Page 21)
    - **Description:** Nodes are organized into groups (clusters) or hierarchies. Some nodes (e.g., cluster heads, gateways) perform more complex routing tasks, while others act as simple sensors.
    - **Purpose:** Facilitates efficient data aggregation and routing.
    - **Example: LEACH (Low Energy Adaptive Clustering Hierarchy):**
      - Nodes are divided into clusters.
      - Cluster heads aggregate data from nodes in their cluster.
      - Cluster heads communicate with the sink or base station.
  - **B. Geographical Routing Protocols:** (Notes Page 21)
    - **Description:** Use the physical location of nodes (often from GPS) to make routing decisions.
    - **Purpose:** Reduces overhead associated with maintaining a global network topology.
    - **Example: Greedy Routing:**
      - Nodes forward data packets to the neighbor that is geographically closest to the destination.
  - **C. Dynamic Routing:** (Notes Page 21)

        - **Description:** Adapts routing paths based on real-time network conditions like traffic load or topology changes.
        - **Example:** Protocols that dynamically adjust routes to avoid congested or unreliable links.
    - **D. Flat Routing Protocols:** (Notes Page 22)
        - **Description:** All nodes are treated equally, and each node may participate in routing decisions.
        - **Example: Flooding:**
            - A simple technique where each node broadcasts a received packet to all its neighbors.
            - Can cause redundancy and network congestion.
    - **E. Other Notable Protocols (often from ad-hoc networks, applicable to WSNs):** (Notes Page 22)
        - **AODV (Ad-hoc On-Demand Distance Vector):** Reactive routing protocol used in mobile ad-hoc networks.
        - **DSR (Dynamic Source Routing):** Another reactive protocol that uses source routing to find paths in mobile ad-hoc networks.
        - **EPR (Energy-Aware Peering Routing):** Designed to reduce network traffic and energy consumption in wireless body sensor networks.

**9. Sensor Deployment & Node Discovery in WSN**

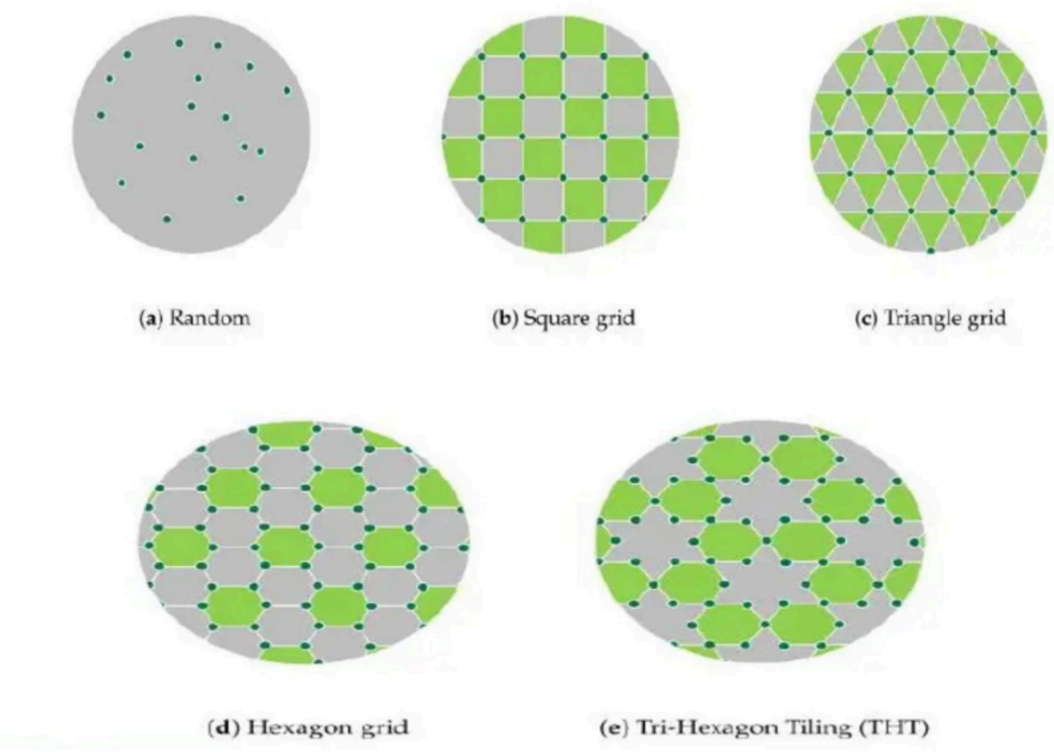
### 9.1. Sensor Deployment in WSN:

Sensor deployment methods vary based on application requirements and environmental conditions. Deployment can be broadly categorized into two main methods:

**1. Deterministic Deployment:**

- **Characteristics:**
    - Suitable when the environment's conditions are well-understood.
    - Sensor nodes are fixed in pre-selected areas following a defined pattern.

- **Examples of Deployment Patterns:**




  - **Square Grid:**
    - Area is divided into small squares.
    - Nodes are positioned at the grid intersections.
    - **Reference:** Fig (b) on Notes Page 25.
  - **Triangle Grid:**
    - Area is divided into small triangles.
    - Sensors are placed at the vertices of the triangles.
    - **Reference:** Fig (c) on Notes Page 25.
  - **Hexagon Grid:**
    - Area is divided into hexagonal cells.
    - Sensors are positioned at the vertices of the hexagons.
    - **Reference:** Fig (d) on Notes Page 25.
  - **Tri-Hexagon Tiling (THT):**
    - Combines triangles and hexagons for coverage.
    - Sensors are placed in a star-like pattern, maximizing area coverage without gaps or overlap.
    - **Reference:** Fig (e) on Notes Page 25.
- **Advantages:**
  - Geometric structures, such as hexagons, ensure high coverage, low energy consumption, and a minimum number of sensors.
  - THT offers good energy performance by combining triangle and hexagon benefits.

- **Use Case:** Non-harsh and small-to-moderate scale regions.

**2. Random Deployment:**

- **Characteristics:**
  - Sensors are scattered randomly across the region of interest.
  - Typically used in environments where precise placement is challenging.
- **Examples of Deployment Patterns:**
  - **Uniform Random Deployment:**
    - Sensors are deployed randomly without known exact positions.
    - Often dropped using UAVs or aircraft.
    - **Reference:** Fig (a) on Notes Page 25.
- **Advantages:**
  - Simple and economical, especially for harsh environments like disaster zones or battlefields.
- **Challenges:**
  - Coverage may be uneven, leading to weak connectivity.
  - Networks are less robust to sensor failures.
  - Requires additional nodes for full coverage in large-scale deployments.

### 9.2. IoT Sensor Deployment Challenges:

**Challenge #1: Variety of Sensors and Chipsets**

- IoT applications require diverse cellular technologies (e.g., NB-IoT, Cat-M1, LoRa).
- No single chipset offers a cost-effective solution for all scenarios.

**Challenge #2: Optimal Sensor Location**

- Difficulties in identifying suitable deployment spots due to varying environmental factors and connectivity.
- Operators rely on statistical models, which can result in sub-optimal placement.

**Challenge #3: Remediating Sensor Performance Issues**

- Sensors are often deployed in hard-to-access locations.
- Network performance issues can lack real-time visibility, requiring costly remediation efforts.

**Challenge #4: Network SLA Validation**

- Ensuring service level agreements is challenging without post-deployment network health data.
- Deployment assumptions based on RF/RAN models can fail under real-world conditions.

### 9.3. Node Discovery in WSN:

**Definition:**

The process of identifying and integrating new devices into an IoT network.

**Importance:**

- Ensures seamless addition of new devices.
- Maintains network scalability and flexibility.

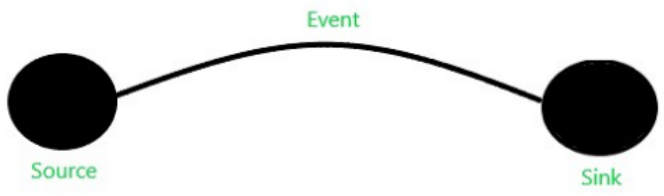
**Sensor Node Functionality Related to Discovery/Operation:**

- **Sensing Unit:** Monitors environmental conditions such as temperature and pressure.
- **Processing Unit:** Processes data gathered by the sensing unit.
- **Communication Unit:** Facilitates the exchange of processed information among neighboring nodes.

This document outlines the foundational concepts and challenges of sensor deployment and node discovery, providing references and diagrams for further study.

**10. Data Dissemination in WSNs** [PYQ Q5b (June 2024 - node behaviours)]

- **Definition:** Procedure where a server (or source node) initiates and manages the transfer of data as well as updates. Helps in maintaining data consistency and cache management. (Notes Page 27)
- Can be thought of as "Pushing data to mobile devices from a server or some other computer."
- **Traffic Models in WSN (vs. Ad-hoc's peer-to-peer):** (Notes Page 27)
    - **Data Collection Model:** Source sends data to a collection point periodically or on demand.
    - **Data Diffusion Model:** A sensor node generates data based on its sensing mechanism's observation and diffuses it.
- **Entities in Data Dissemination:** (Notes Page 27-28)
    - **Source:** Node generating data.
    - **Event:** Something that needs to be reported (e.g., abnormal activity in target detection).
    - **Sink:** A node (often a base station or gateway) randomly located in the field, interested in events, and seeks such information.
- **Process Overview:**




    - Information (event) needs to be reported.
    - Sink expresses interest; source receives interest; event (data) is transferred from source to sink.
    - **Two-step process:**

- 
    1. Interested node (sink) broadcasts its interests periodically to neighbors. Interests propagate through the network.
- 
    2. Nodes that have requested data (or possess relevant data) send it back after receiving/matching an interest. Intermediate nodes can cache received interests and data to satisfy future requests or aggregate data. (Notes Page 28)

- **10.1. Data Dissemination Methods:**
    - **A. Flooding:** (Notes Page 28)
        - Simplest design.
        - Each node receiving data repeats it by broadcasting the data to every neighbor (unless a maximum hop lifetime for the data has been reached).
        - Can lead to "implosion" (many copies of same data) and "overlap" (nodes receive redundant data).
    - **B. Gossiping:** (Notes Page 29)
        - Enhancement of Flooding.
        - When a node receives data, it randomly chooses one neighbor and sends the data to it.
        - Reduces duplicate packets compared to flooding.
        - Can contribute to network latency.
        - **Advantages:**
            - Easily scalable.
            - Eliminates some shortcomings of Flooding.
            - Sends data in an autonomous and decentralized manner.
        - **Disadvantages:**
            - Random destination selection might lead to starvation for some nodes (not selected to receive data) or longer paths.
    - **C. SPIN (Sensor Protocols for Information via Negotiation):** (Notes Page 29)
        - Aims to overcome shortcomings of flooding (like implosion and overlap) by using negotiation.
        - Nodes advertise data availability before sending. Data is sent only if requested.
        - **SPIN Messages (3 types):**
            - **ADV (Advertise):** Used by a sensor to signal it has data to send and describes the data (metadata).
            - **REQ (Request):** Used by a node when it is ready (and interested) to receive data advertised by a neighbor.
            - **DATA:** The actual information/data to be sent.

            - **Advantages:**
                - More efficient than flooding because negotiation reduces implosion (unnecessary data copies) and overlap (redundant data).

**11. Data Aggregation in WSNs/IoT** [PYQ Q5b (June 2024 - node behaviours, e.g. cluster head)]

- **Definition:** The process of collecting and aggregating useful data. (Notes Page 30)
- **In WSNs:**
    - Technique to solve implosion and overlap problems in data-centric routing.
    - Data coming from multiple sensor nodes regarding the same phenomenon attribute can be aggregated (e.g., averaged, min/max found) at an intermediate routing node on the way to the sink.
    - Widely used technique.
    - **Security Issues:** Data confidentiality and integrity in aggregation become vital if the WSN is deployed in a hostile environment.
    - **Process:** Sensor data is aggregated using approaches/algorithms like centralized approach, LEACH (cluster-based aggregation), TAG (Tiny Aggregation). Aggregated data is then transferred to the sink via an efficient path.
- **In IoT (General):** (Notes Page 30)
    - Involves combining and summarizing data from multiple sensors or devices into a more concise and meaningful form.
    - **Primary Goals:**
        - Reduce the volume of transmitted data.
        - Minimize communication overhead.
        - Improve the efficiency of data transfer within an IoT network.
    - Aggregated data is often more manageable for storage, analysis, and transmission compared to raw data from individual sensors.

---