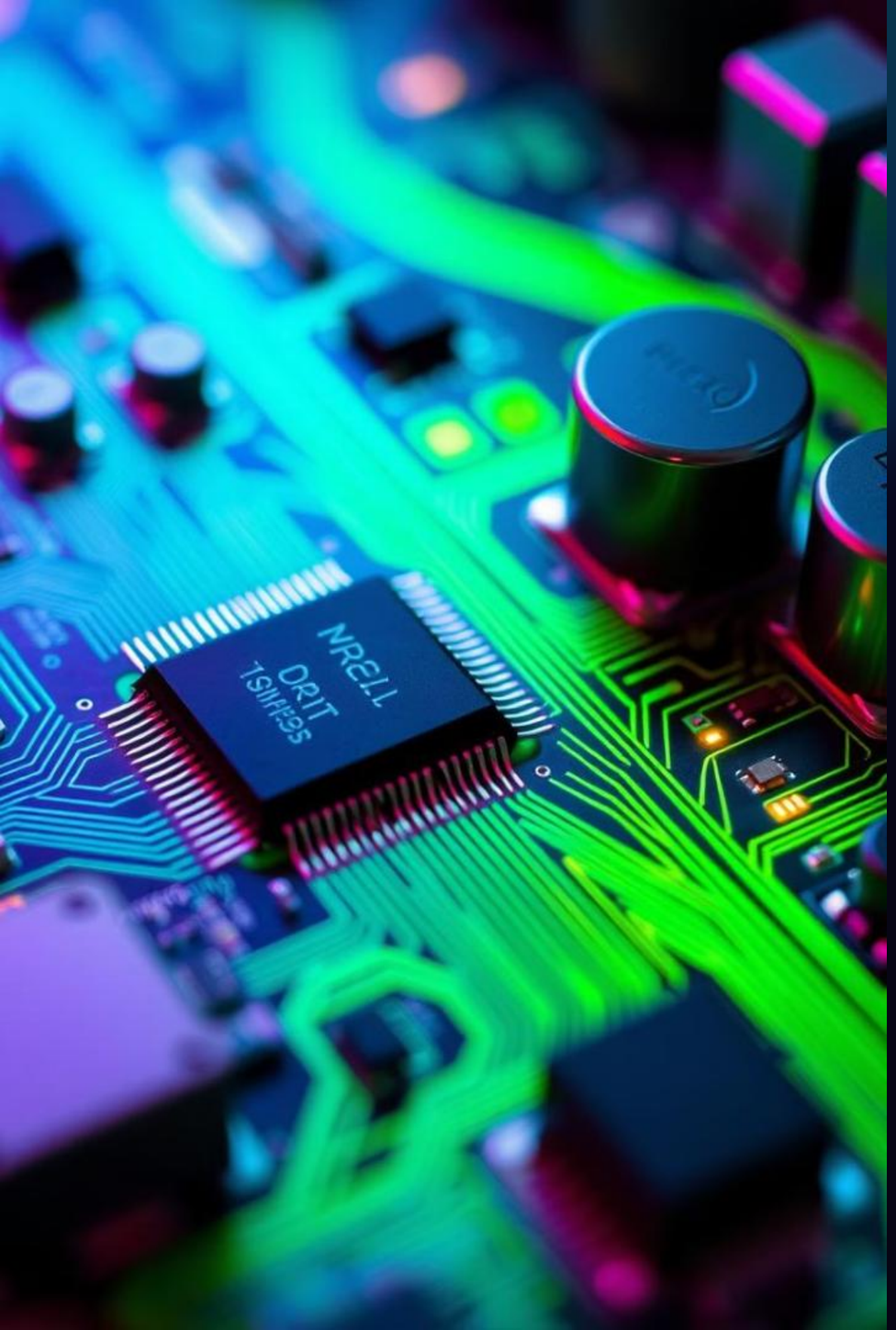


UNIT III

Network & Communication Aspects in IoT

Wireless Medium Access Issues

When it comes to communication using a wireless medium there is always a concern about the interference due to other present wireless communication technologies. Wireless means communication and message transfer without the use of physical medium i.e., wires.

The very important issues which are observed are:

- Half Duplex operation
- Time-varying channel
- Burst channel errors.

Wireless Medium Access Issues

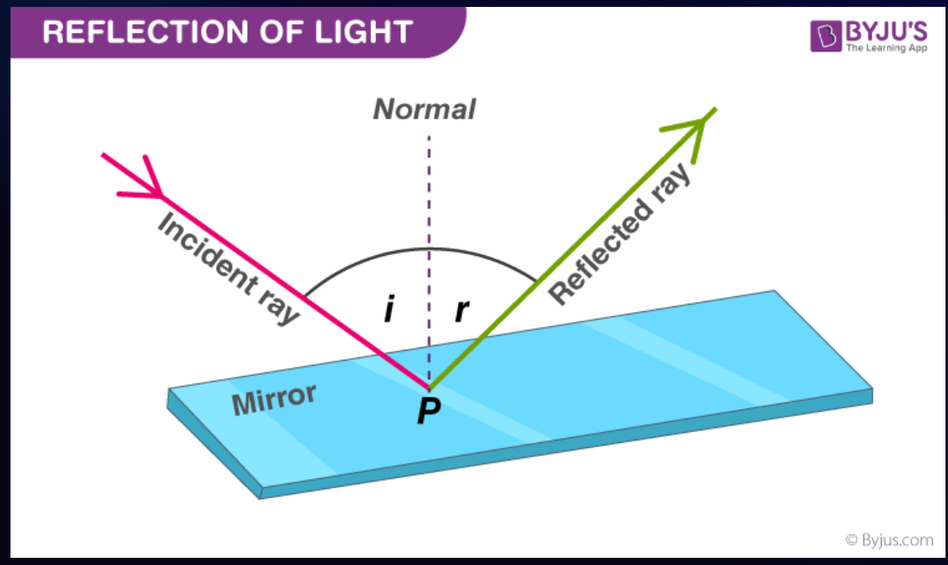
1. Half Duplex Operation

- Half-duplex transmission means when the sender and receiver both are capable of sharing data but one at a time.
- In wireless transmission, it is difficult to receive data when the transmitter is sending the data because during transmission a large amount or a large fraction of signal energy is leaked while broadcasting.
- The magnitude of the transferred signal and received signal differs a lot.
- Due to which collision detection is even not possible by the sender as the intensity of the transferred signal is large than the received one. Hence this causes the problem of collision and the prime focus should be to minimize the collision.

Wireless Medium Access Issues

2. Time-varying channel

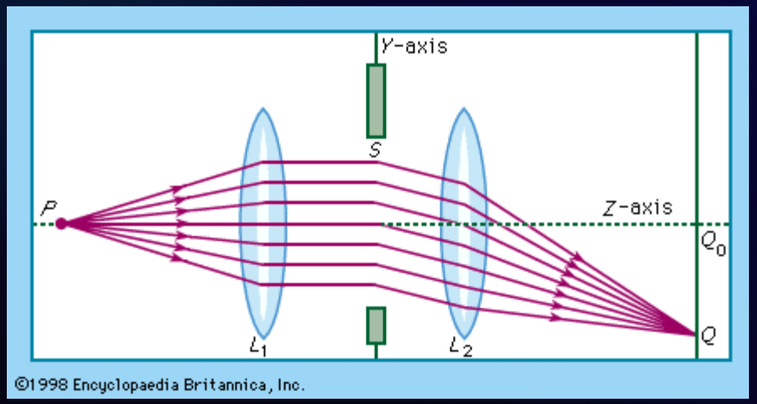
- Time-varying channels include the three mechanisms for radio signal propagations they are Reflection, Diffraction, and Scattering.
- **Reflection –**
  - In communication, when a signal encounters a large object, like a building or a mountain, it can bounce off that object and travel back in the direction it came from. This is reflection.
  - Reflection can cause signals to bounce around and reach the receiver from multiple paths, which can sometimes strengthen or weaken the signal.



Wireless Medium Access Issues

2. Time-varying channel

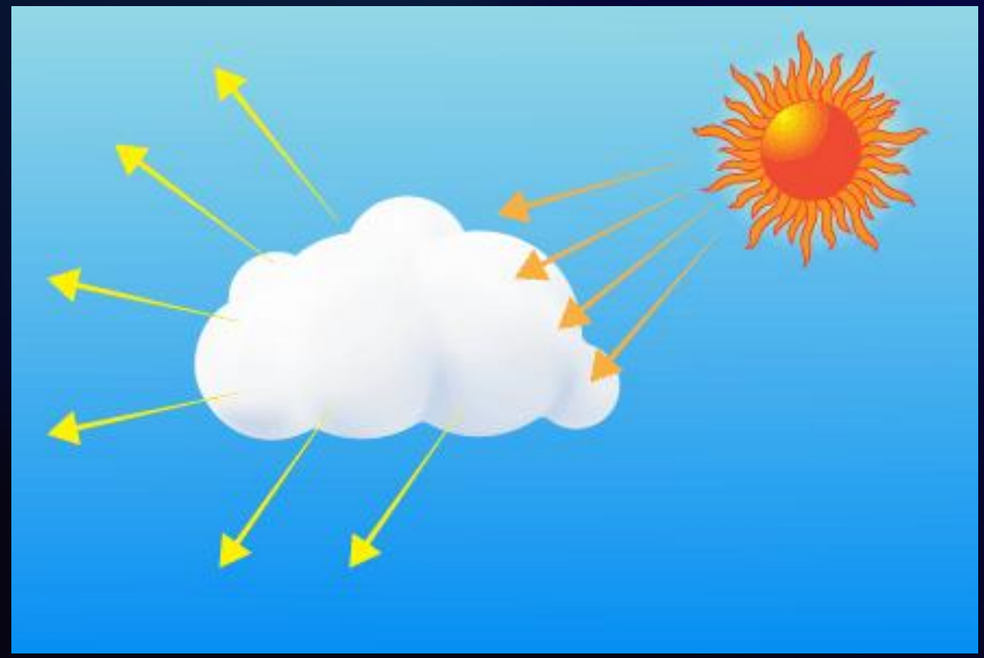
- Diffraction –
  - Diffraction is the deviation of waves from straight-line propagation without any change in their energy due to an obstacle or through an aperture.
  - When a signal encounters an obstacle with sharp edges, like a building or a hill, it can bend around that obstacle and spread out. This bending and spreading of the signal is diffraction.
  - Diffraction can cause the signal to reach areas that are not directly in the line of sight of the transmitter.



Wireless Medium Access Issues

2. Time-varying channel

- Scattering –
  - This occurs when the medium through from the wave is traveling consists of some objects which have dimensions smaller than the wavelength of the wave.
  - In communication, when a signal encounters objects smaller than its wavelength, like trees or buildings, the signal can bounce off or get scattered in various directions. This scattering of the signal is called scattering.



Wireless Medium Access Issues

2. Time-varying channel

While transmitting the signal by the node these are time shifted and this is called multipath propagation. While when this node signals intensity is dropped below a threshold value, then this is termed as fade.

Wireless Medium Access Issues

3. Burst channel errors

- Burst channel errors occur when multiple data packets are lost or corrupted in a short time due to interference, weak signals, or obstacles like walls or weather conditions. This causes delays, as the system needs to resend data, reducing communication efficiency.
- To manage this, techniques like error correction, retransmission, and using multiple channels help minimize disruptions and maintain smooth communication.

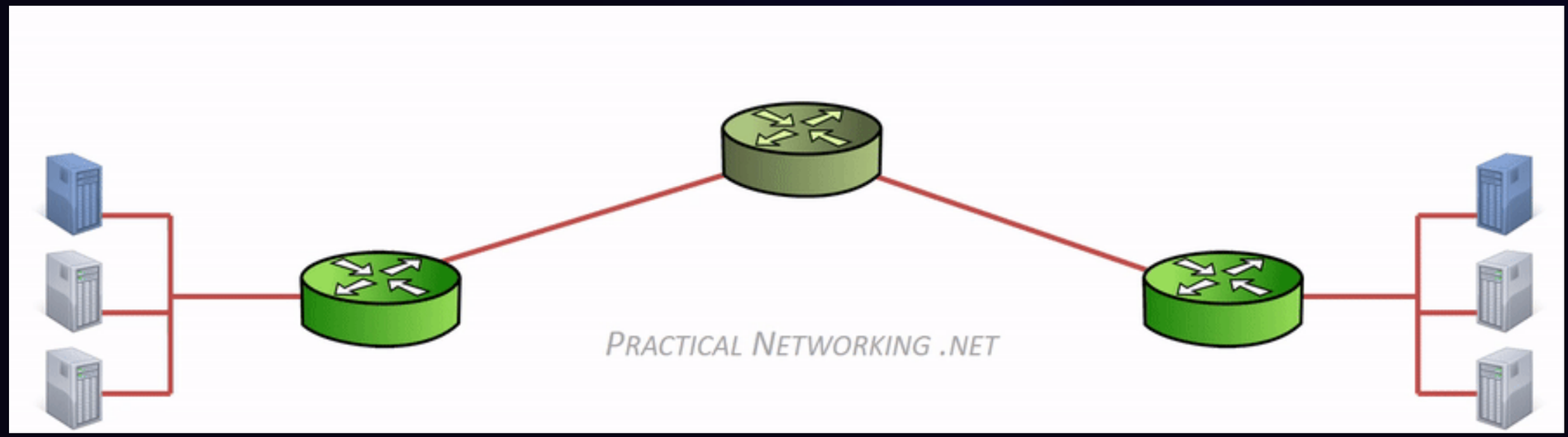
MAC Protocol Survey

- A MAC (Medium Access Control) protocol survey refers to a comprehensive study and analysis of various MAC protocols used in wireless networks. It involves examining and evaluating multiple protocols to understand their characteristics, performance, and suitability for different network scenarios.
- The goal of a MAC protocol survey is to provide insights into the strengths and weaknesses of different protocols, compare their features, and identify the most suitable protocol for specific applications or requirements.

MAC Protocol Survey

Categories of MAC Protocols

a. Contention-Based MAC Protocols
b. Time-Slotted MAC Protocols
c. Aloha-Based MAC Protocols



MAC Protocol Survey

Categories of MAC Protocols

a. Contention-Based MAC Protocols

   Contention-based MAC protocols are prevalent in IoT environments where devices contend for access to the communication channel. Protocols like Carrier Sense Multiple Access (CSMA) and its variants are widely used, balancing efficiency and simplicity.

MAC Protocol Survey

Categories of MAC Protocols

b. Time-Slotted MAC Protocols

Time-synchronized MAC protocols allocate specific time slots to devices, enabling efficient communication by avoiding collisions. Zigbee and IEEE 802.15.4 are notable examples of time-slotted protocols, suitable for applications requiring low-latency and predictable communication.

MAC Protocol Survey

Categories of MAC Protocols

c. Aloha-Based MAC Protocols

Aloha-based MAC protocols, such as the Low-Power Wide Area Network (LPWAN) technologies, leverage random access without synchronization. These protocols are well-suited for scenarios where energy efficiency is paramount, enabling long-range communication with minimal energy consumption.

MAC Protocol Survey

Key Considerations in IoT MAC Protocols

When designing and selecting Medium Access Control (MAC) protocols for Internet of Things (IoT) devices, several key considerations come into play. These considerations are essential for ensuring efficient and reliable communication within IoT networks.

1. Energy Efficiency

IoT devices often operate on limited battery power. MAC protocols in IoT must prioritize energy efficiency to extend device lifetimes and minimize the need for frequent battery replacements.

MAC Protocol Survey

Key Considerations in IoT MAC Protocols

2. Scalability

   IoT networks vary significantly in size and complexity, ranging from small-scale home automation systems with a few connected devices to large-scale industrial and smart city deployments with thousands or even millions of devices. A MAC protocol designed for IoT must be scalable, meaning it should efficiently handle both small and large numbers of devices without performance degradation.

3. Synchronization

   Achieving synchronization among devices is challenging due to heterogeneity and intermittent connectivity. MAC protocols must address synchronization issues to ensure reliable communication.

MAC Protocol Survey

Key Considerations in IoT MAC Protocols

4. Data Rate and Throughput

Different IoT applications may require varying data rates and throughput. MAC protocols should be adaptable to support a range of communication requirements.

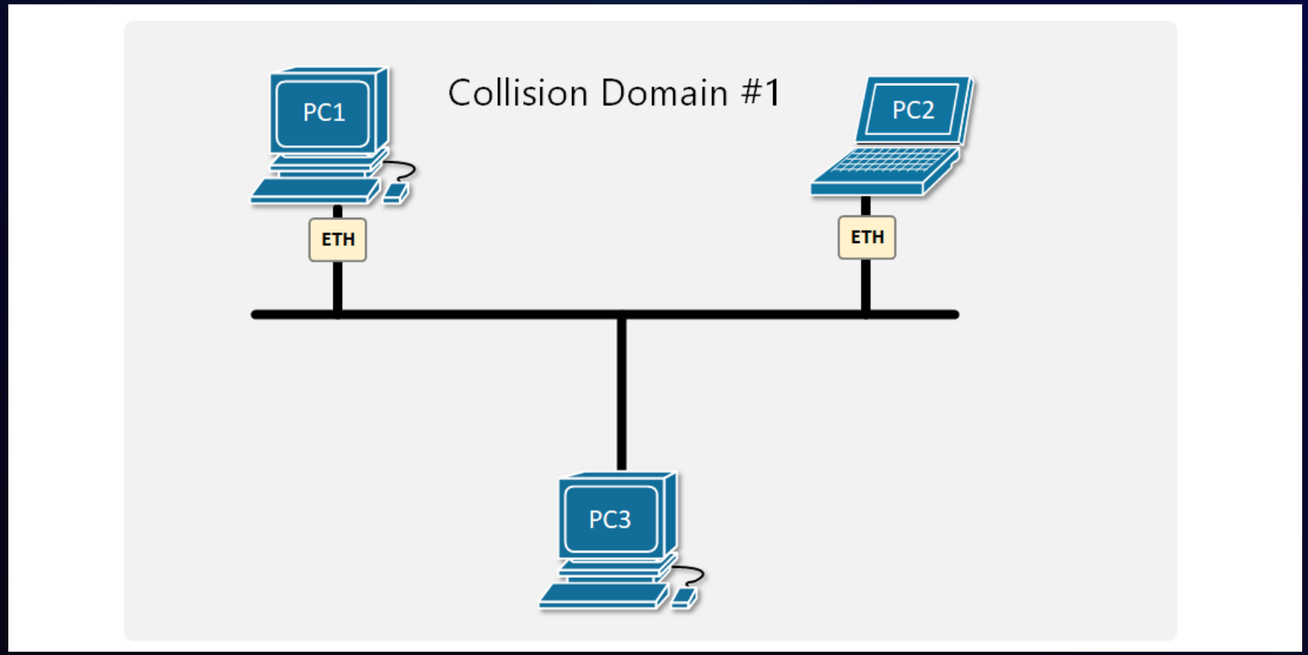
5. Collision Avoidance and Resolution

In crowded IoT networks, collisions can significantly degrade performance. MAC protocols need to implement effective collision avoidance and resolution mechanisms.

MAC Protocol Survey

CSMA

- **Carrier-sense multiple access (CSMA)** is a medium access control (MAC) protocol that can be used in the Internet of Things (IoT) to manage how devices share a communication channel.
- CSMA is a method that helps reduce collisions by ensuring that devices wait until the channel is free before transmitting data. This helps to ensure smoother communication across the network.



MAC Protocol Survey

CSMA

- **How it works:** A device uses a carrier-sense mechanism to check if another transmission is in progress before attempting to transmit. If a carrier is detected, the device waits for the transmission to end before transmitting its own data.
- **When it's used:** CSMA is commonly used in technologies like Ethernet and Wi-Fi.
- **Variations:** Carrier-sense multiple access with collision detection (CSMA/CD) is a variation of CSMA that uses collision detection to improve performance. In CSMA/CD, a transmitting station stops transmitting if it detects a collision, transmits a jam signal, and then waits before trying again.

MAC Protocol Survey

TDMA

TDMA (Time Division Multiple Access) is a Medium Access Control (MAC) protocol widely used in IoT (Internet of Things) networks. These devices transmit in specific time slots. Here's how it works and why it is suitable for IoT:

How TDMA works?

Time Slots:

- The communication channel is divided into fixed time slots.
- Each device in the network gets a specific time slot to send its data.

Scheduled Access:

- Devices transmit data only during their allocated slot, avoiding collisions.
- This scheduling ensures efficient use of the shared communication medium.

MAC Protocol Survey

TDMA

Why it is used?

Energy Efficiency:

IoT devices are often battery-powered. TDMA allows devices to sleep when it's not their time to transmit, saving energy.

Collision-Free:

Since each device has a dedicated time slot, data collisions are avoided, improving reliability.

Scalability:

TDMA can support many devices by dynamically assigning time slots based on the network's needs.

Predictable Latency:

With fixed time slots, the delay in communication is predictable, which is important for time-sensitive IoT applications.

MAC Protocol Survey

FDMA

FDMA (Frequency Division Multiple Access) is a medium access control (MAC) protocol that divides the available frequency spectrum into separate channels, each assigned to a specific device or node. In the context of IoT (Internet of Things).

How FDMA works?

- Each IoT device communicates using its assigned frequency channel, ensuring no overlap or interference.
- Devices transmit data simultaneously, but on different frequencies.

Where It’s Used in IoT?

- Smart grids and metering systems where devices periodically send data.
- Industrial IoT setups with pre-determined device roles.
- Environments requiring minimal interference, such as medical monitoring systems.

MAC Protocol Survey

Aloha

The Aloha MAC protocol is a simple method for managing communication in shared networks, including the Internet of Things (IoT). It works by allowing devices to send data whenever they have information to transmit, without waiting for permission or checking if the channel is free.

Key Features:

Simplicity:

Aloha is lightweight and easy to implement, making it suitable for IoT devices with limited processing power.

Collisions:

Since devices transmit freely, data packets can collide if multiple devices send at the same time. This leads to retransmissions and reduced efficiency.

Survey Routing Protocols

- A survey on routing protocols examines and analyzes the design, functionality, and performance of multiple routing protocols to provide an overview of their strengths, weaknesses, and applicability to specific network environments.
- Routing protocols in the context of wireless sensor networks (WSNs) refer to sets of rules and algorithms governing how data packets are forwarded from source nodes to destination nodes within the network.
- These protocols are specifically designed to address the unique characteristics and constraints of WSNs, such as limited energy, computation, and memory resources, as well as dynamic network topologies and potentially unreliable wireless communication channels.
- Routing protocols in WSNs typically determine the optimal paths for data transmission based on various metrics, including energy efficiency, latency, reliability, and network lifetime. They play a crucial role in ensuring efficient and reliable communication while prolonging the network's operational lifespan.

Survey Routing Protocols

The routing protocols can be broadly categorized into three main types:

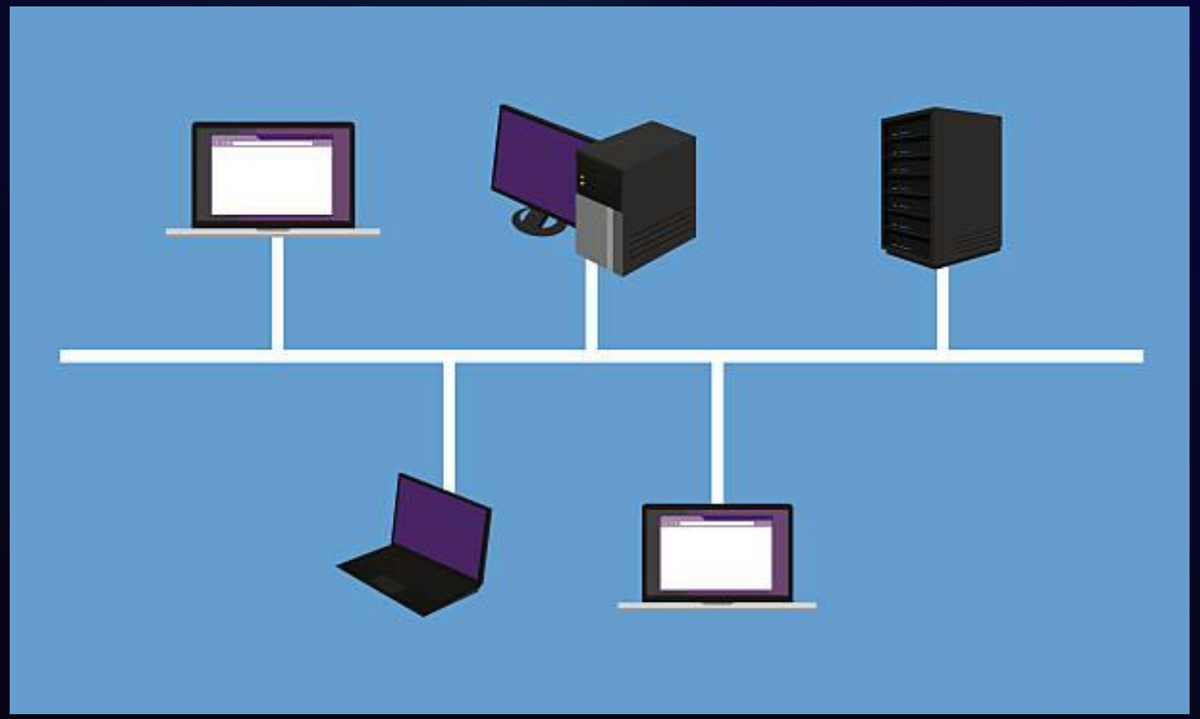
- Flat Routing Protocols
- Hierarchical Routing Protocols
- Location-Based Routing Protocols

Survey Routing Protocols

The routing protocols can be broadly categorized into three main types:

Flat Routing Protocols

In flat routing protocols, all nodes in the network are considered peers, and there is no hierarchical structure. Each node may act as a source, destination, or intermediate relay node. Examples include Ad-hoc On-demand Distance Vector (AODV) and Dynamic Source Routing (DSR).

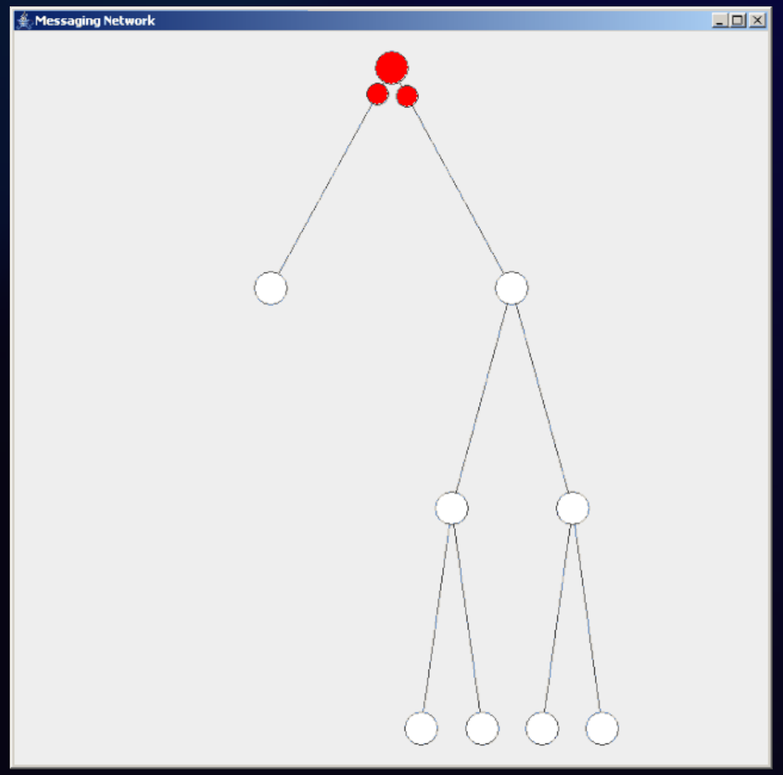


Survey Routing Protocols

The routing protocols can be broadly categorized into three main types:

Hierarchical Routing Protocols

Hierarchical routing protocols organize nodes into a hierarchical structure, typically consisting of multiple levels of nodes, such as cluster heads and ordinary nodes. This hierarchical organization helps in reducing energy consumption, managing network scalability, and improving data aggregation and dissemination. Examples include Low-Energy Adaptive Clustering Hierarchy (LEACH) and Threshold-sensitive Energy Efficient Sensor Network Protocol (TEEN).

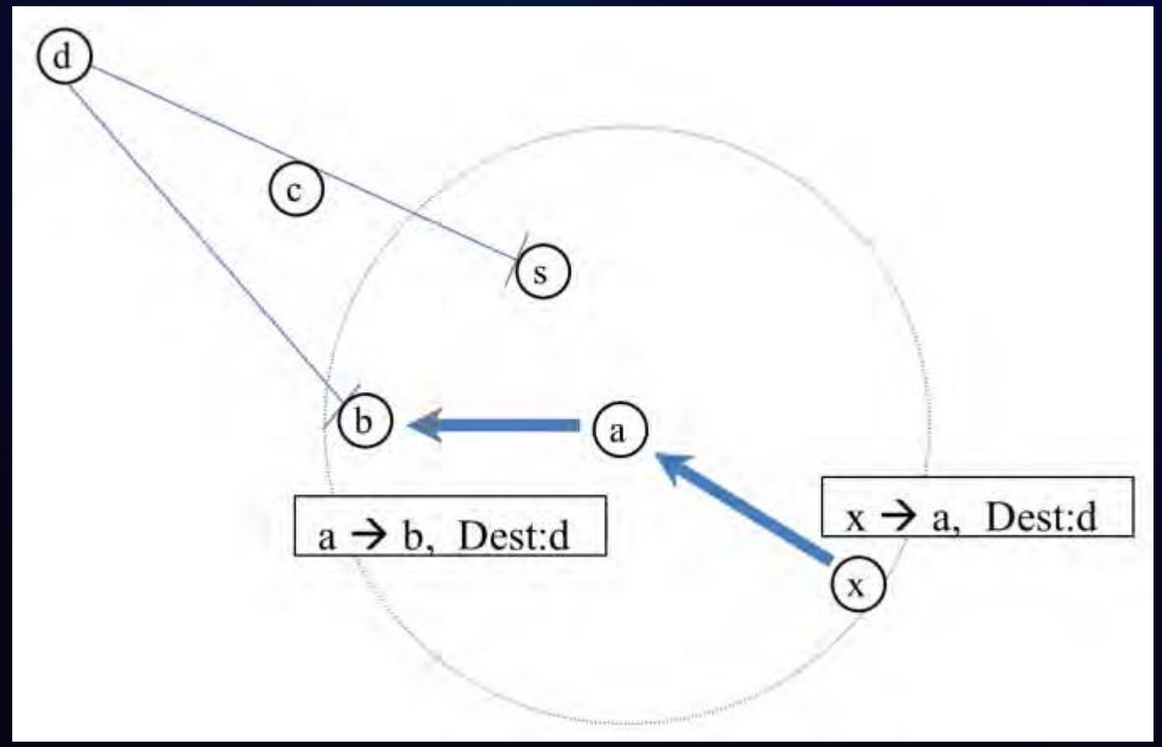


Survey Routing Protocols

The routing protocols can be broadly categorized into three main types:

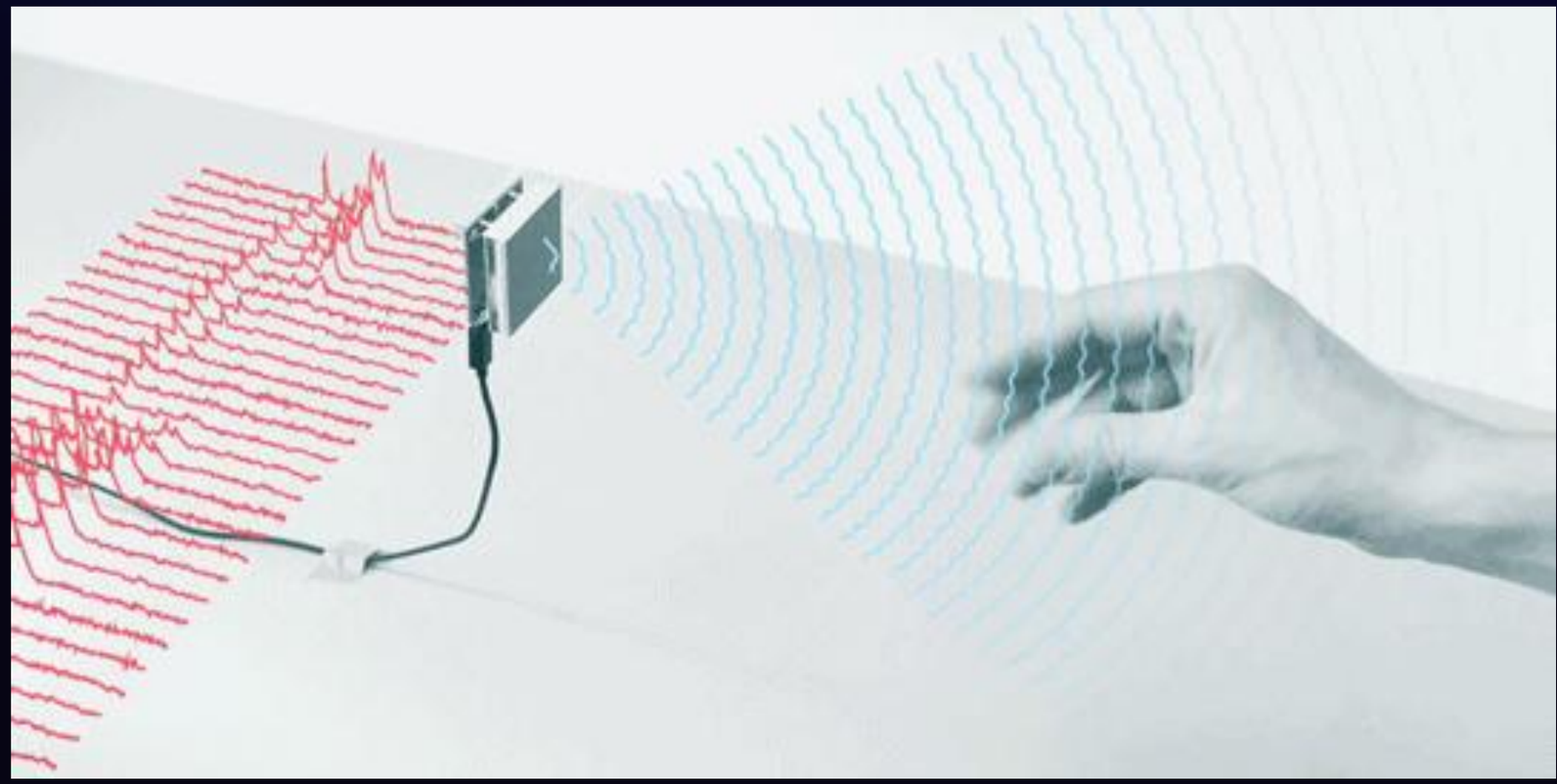
Location-Based Routing Protocols

Location-based routing protocols utilize the geographic locations of nodes to determine optimal routing paths. These protocols leverage information about node positions to make routing decisions, which can result in more efficient routing paths and reduced overhead. Examples include Geographic Routing Protocol (GRP) and Greedy Perimeter Stateless Routing (GPSR).



Sensor deployment & Node discovery

In the context of Wireless Sensor Networks (WSNs), sensor deployment and node discovery are critical processes that ensure the network operates efficiently and effectively.



Sensor deployment & Node discovery

Sensor deployment

This refers to the placement of sensor nodes in the network area to monitor the environment and collect data.

Types of Deployment:

Manual Deployment:

Sensors are placed manually in specific locations, often for smaller or controlled environments.

Example: Deploying sensors in a greenhouse.

Random Deployment:

Sensors are distributed randomly, usually by dropping them over a wide area (e.g., using drones or planes). This is common in large, inaccessible terrains.

Example: Sensors scattered in a forest for wildlife monitoring.

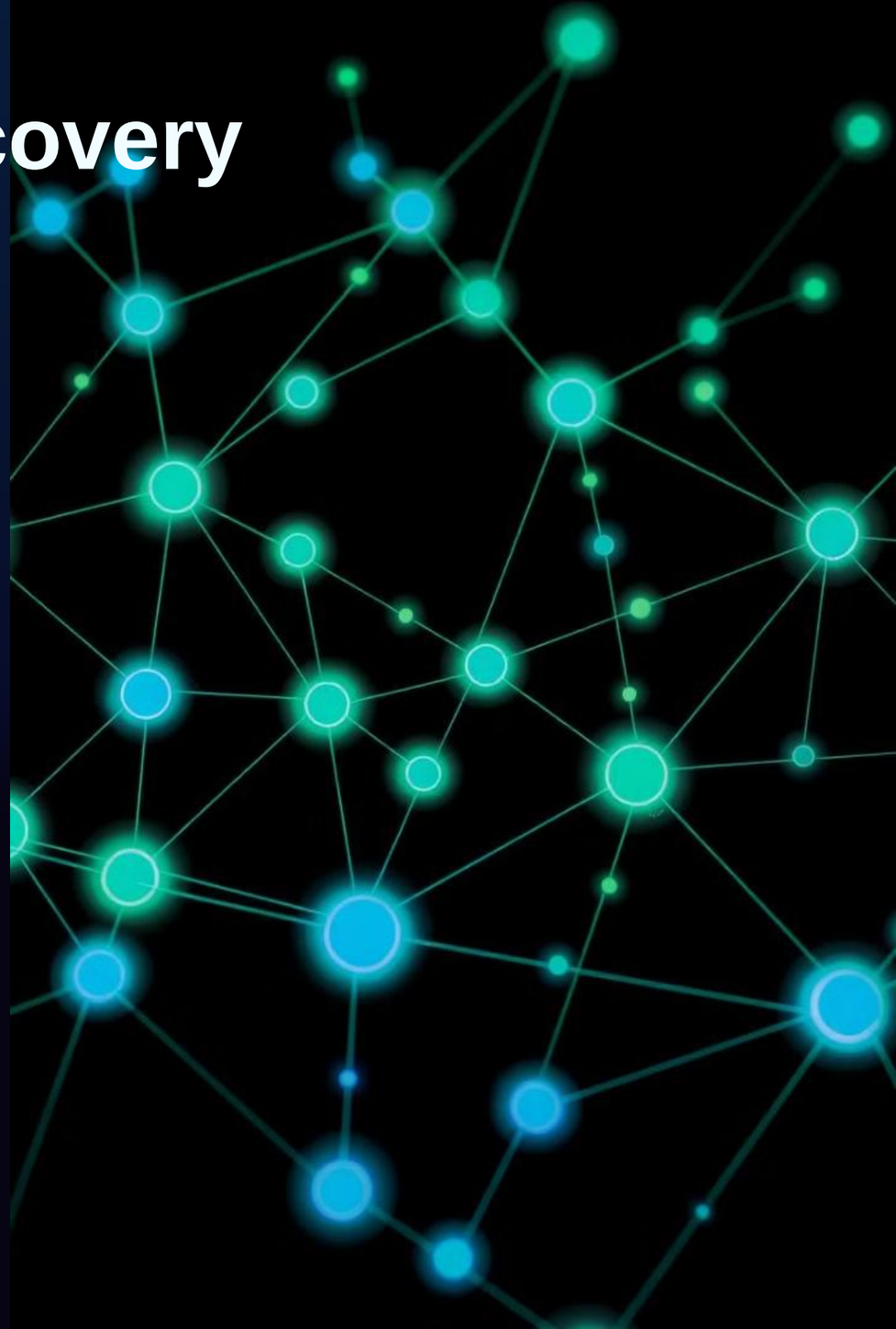
Sensor deployment & Node discovery

Node discovery

Once sensors are deployed, they must identify and connect to other nodes in the network. This process is called node discovery.

Purpose:

- Establish communication links between nodes.
- Form a topology for efficient data routing.
- Detect and manage newly added or lost nodes.



Sensor deployment & Node discovery

Node discovery

Process:

1. **Broadcasting Signals:**

   Nodes send out signals to announce their presence.

2. **Neighbor Discovery:**

   Nodes detect other nodes within their communication range and exchange information (e.g., location, ID).

3. **Network Formation:**

   Based on discovered neighbors, nodes form a communication topology (e.g., star, mesh, or tree structure).

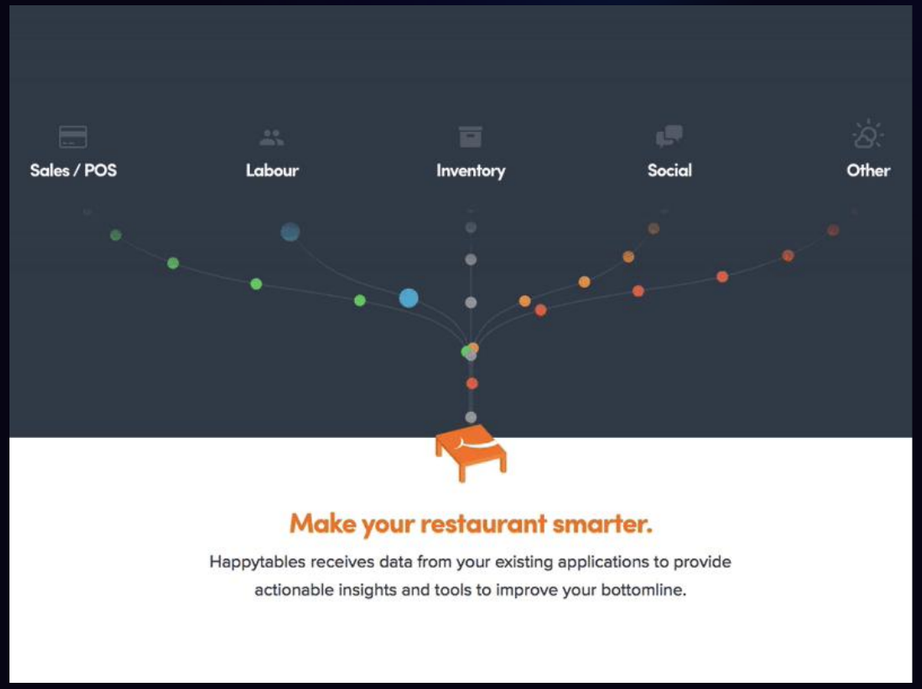
Sensor deployment & Node discovery

Relation Between Sensor Deployment and Node Discovery

- Deployment determines how well the network covers the area and how easy it is for nodes to discover each other.
- Node Discovery ensures connectivity and communication between nodes after deployment.

Data Aggregation & Dissemination

In Wireless Sensor Networks (WSNs), data aggregation and data dissemination are essential mechanisms for efficient data collection and distribution.



Aggregation

Dissemination

Data Aggregation & Dissemination

Data Aggregation

Data aggregation is the process of gathering and combining data from multiple sensor nodes to reduce redundancy, minimize energy consumption, and improve efficiency.

Purpose:

- To reduce the amount of data transmitted to the base station or sink, saving energy and bandwidth.
- To eliminate duplicate or redundant data collected by neighboring sensors.

Data Aggregation & Dissemination

Data Aggregation

How It Works:

- Sensor nodes collect raw data from the environment.
- Data is sent to a central node (aggregator) or processed collaboratively to combine it into a smaller, meaningful summary.

  Example: In a temperature monitoring system, instead of sending every node's temperature reading, the average temperature of the area is calculated and transmitted.

Challenges:

- Aggregators may become bottlenecks or fail due to excessive workload.
- Ensuring data accuracy during aggregation.

Data Aggregation & Dissemination

Data Dissemination

Data dissemination refers to the process of distributing data (or queries) from the base station or sink to the sensor nodes and vice versa.

Purpose:

- To share queries or control messages from the base station to the nodes.
- To transmit sensor-collected data to the sink.

How It Works:

- The sink sends a query (e.g., "What is the temperature in Zone A?") to the relevant nodes.
- Nodes respond with the requested data.

Data Aggregation & Dissemination

Data Dissemination

Dissemination Methods:

Flooding: The sink broadcasts the query to all nodes in the network.

Gossiping: Nodes share the query with a random neighbor until all relevant nodes receive it.

Hierarchical Dissemination: The network is divided into clusters or layers to distribute data more efficiently.

Challenges:

- High energy consumption in flooding and gossiping.
- Delay in data delivery due to multiple hops.