Unit 1

What are Wireless Sensor Networks? What are the different participants and their roles in WSN?

WSNs are distributed networks of miniature sensor nodes that cooperatively monitor physical or environmental conditions. These conditions can include temperature, sound, pressure, vibration, and more. Here's a breakdown of key aspects of WSNs:

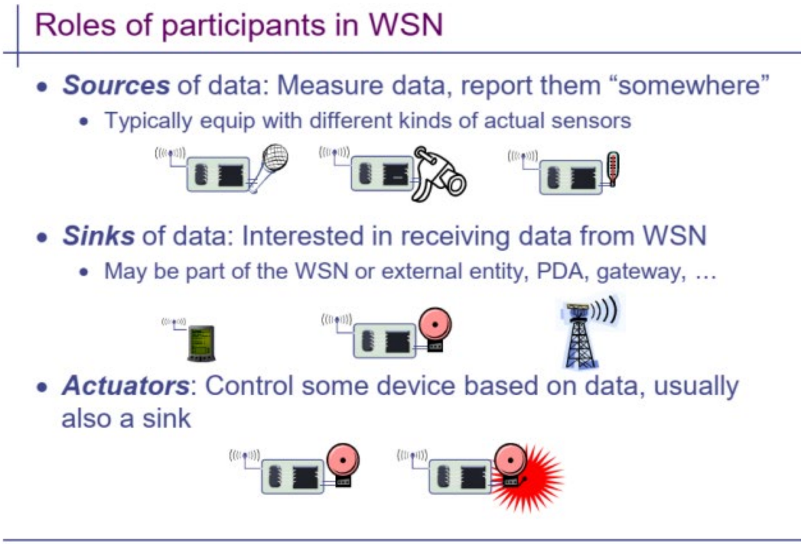
- Wireless Communication: Sensor nodes communicate using radio waves, eliminating the need for cables and simplifying deployment.
- Collaborative Data Routing: Sensor nodes work together to route collected data towards a central location, often called a base station.
- Sensor Nodes: These tiny computers are equipped with built-in sensors and have limited processing power to conserve battery life. They gather specific data and may perform basic processing or self-calibration tasks.
- Base Station: The central hub of the network, the base station collects data from sensor nodes. It may perform initial processing and filtering before transmitting data to other networks for further analysis or storage. The base station can also manage network configuration and communicate with sensor nodes.
- Self-Organization: WSNs are adaptable. They can automatically reconfigure when nodes fail or network conditions change.
- Scalability: WSNs can be deployed with a varying number of sensor nodes, making them suitable for a wide range of monitoring applications, from small-scale to large-scale.
- Long-Term Monitoring: WSNs are ideal for continuous monitoring in remote or hard-to-reach areas due to their wireless nature and low power consumption.

Applications: WSNs have diverse applications in various fields, including:

- Precision agriculture (monitoring soil moisture, crop health)
- Environmental monitoring (air quality, pollution levels)
- Industrial automation (machine health, process control)
- Smart buildings (energy management, security)
- Healthcare (patient monitoring, remote diagnostics)

Advantages:

- Easy deployment
- Cost-effective
- Adaptable to various environments
- Enables real-time data collection for informed decision-making



Roles of participants in WSN

- ***Sources*** of data: Measure data, report them "somewhere"
  - Typically equip with different kinds of actual sensors
- ***Sinks*** of data: Interested in receiving data from WSN
  - May be part of the WSN or external entity, PDA, gateway, …
- ***Actuators***: Control some device based on data, usually also a sink

What are the different Deployment options for WSNs?

There are two main deployment strategies for sensor nodes in WSNs:

Regular Deployment:

- Planned and organised placement of sensor nodes.
- Often involves geometric patterns for optimal coverage and connectivity.
- Advantages:
    - Better sensing coverage: Ensures all areas of interest are monitored effectively.
    - Higher degree of connectivity: Nodes are strategically placed to facilitate communication and data transfer.
    - Easier network management: Known node locations simplify network configuration and troubleshooting.
- Disadvantages:
    - More time-consuming and labour-intensive to plan and deploy, especially for large areas.
    - May not be suitable for harsh or inaccessible environments.

Random Deployment:

- Sensor nodes are scattered randomly throughout the target area.
- Often used for large-scale deployments where precise control is difficult.
- Deployment methods:
- Dropping from aeroplanes or UAVs (unmanned aerial vehicles).
- Scattering by hand in accessible areas.
- Advantages:
    - Easy to implement and scalable for large areas.
    - Suitable for hostile environments where precise positioning might be risky.
- Disadvantages:
    - Lower sensing coverage: May leave some areas unmonitored due to random distribution.
    - Unpredictable connectivity: Nodes may be too far apart or have obstacles hindering communication.
    - Increased network management complexity: Difficulty in locating and managing individual nodes.

Mobile Sensor Nodes:

- This approach introduces mobility to sensor nodes, offering additional flexibility:
- Passive Mobility: Nodes are moved by external forces like wind or water currents.
- Useful for monitoring dynamic environments like rivers or studying air quality patterns.
- Active Mobility: Nodes can move on their own to optimise data collection.
- Can adjust their positions to:
- Fill coverage gaps in the network.
- Investigate areas with detected anomalies or events.
- Extend network lifespan by moving away from depleted energy sources.

Choosing a Deployment Strategy:

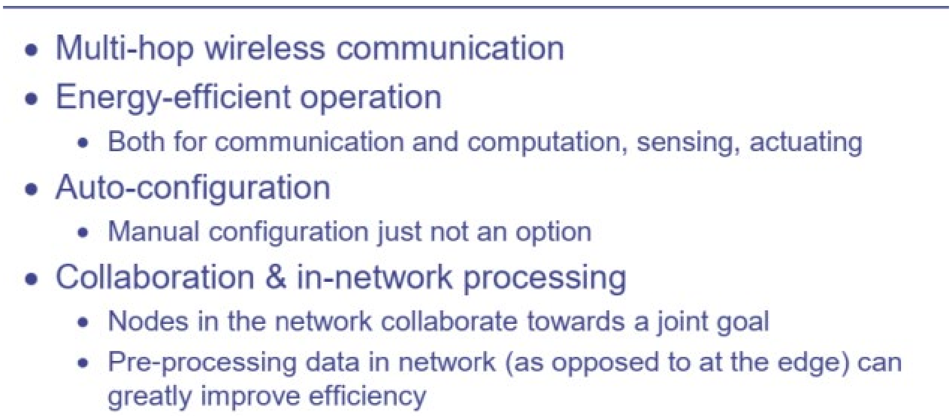
- The optimal deployment strategy depends on various factors:
    - Application requirements: Coverage area, data fidelity, network lifetime.
    - Deployment environment: Accessibility, terrain, potential hazards.
    - Cost and resources: Time, manpower, budget constraints.

Characteristics of WSN

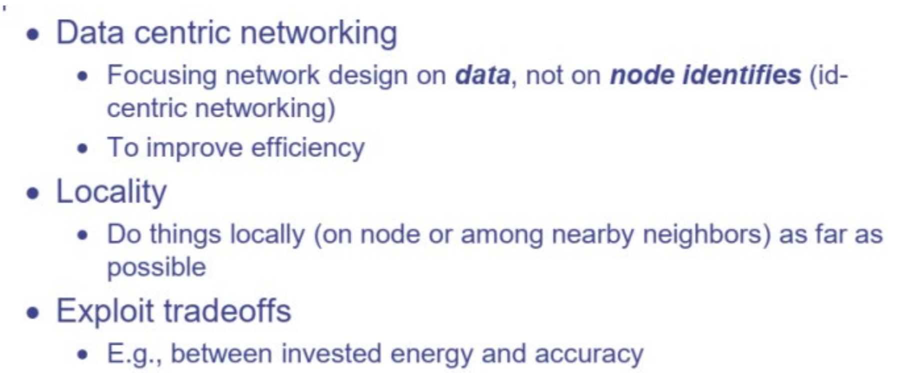
WSNs differ from traditional networks in several key aspects. Here's a breakdown of some crucial requirements for WSNs:

1. Type of Service:
    - Beyond data transfer: Unlike regular networks that focus on moving data packets, WSNs need to provide meaningful information and potentially take actions based on the data collected.
    - Geographic Scoping: WSNs often deal with data specific to a particular location or region. Understanding the geographic context is essential.
    - Time-Sensitive: Data needs to be delivered within a specific timeframe to be useful (e.g., real-time temperature monitoring).
2. Quality of Service (QoS):
    - Traditional QoS metrics like bandwidth or delay may not be the main concern.
    - Focus on right answers: WSNs need to deliver accurate and timely information relevant to the specific application.
    - Adapted QoS concepts:
    - Reliable detection of events (e.g., smoke alarm triggering).
    - Approximation quality (e.g., acceptable accuracy for a temperature map instead of exact readings from every point).
3. Fault Tolerance:
    - WSNs must be robust against failures of individual sensor nodes. This can be due to:
    - Exhausted batteries
    - Physical damage
    - Environmental factors
4. Lifetime:
    - The network should function for as long as possible, depending on the application.
    - Lifetime of individual nodes is less critical compared to the overall network lifespan. However, they are often mistakenly treated as equivalent.
5. Scalability:
    - WSNs can involve a large number of sensor nodes deployed across an area.
    - The network architecture and communication protocols need to handle this efficiently.
6. Wide Range of Densities:
    - The number of nodes per unit area can vary greatly depending on the application:
    - Dense deployments might be used for precise monitoring in a small area.
    - Sparse deployments might cover a vast area with fewer nodes.
    - The density can also change over time due to node failures or movement.
7. Programmability:
    - The ability to reprogram sensor nodes remotely can be crucial.
    - This allows for:
    - Adapting to changing conditions or requirements.
    - Fixing bugs or implementing new functionalities.
    - Improving the overall flexibility and future-proofing of the WSN.
    - Increase the flexibility by ensuring the re-programmability of nodes in the field to react to new situations.
8. Maintainability
    - WSN has to adapt to changes, self-monitoring, adapt operation.
    - Incorporate possible additional resources, e.g., newly deployed nodes
    - Environment and WSN itself are changing.
    - Self-monitoring and adaptation of the system.

What are the required mechanisms to meet characteristic requirements for WSNs?



- Multi-hop wireless communication
- Energy-efficient operation
  - Both for communication and computation, sensing, actuating
- Auto-configuration
  - Manual configuration just not an option
- Collaboration & in-network processing
  - Nodes in the network collaborate towards a joint goal
  - Pre-processing data in network (as opposed to at the edge) can greatly improve efficiency



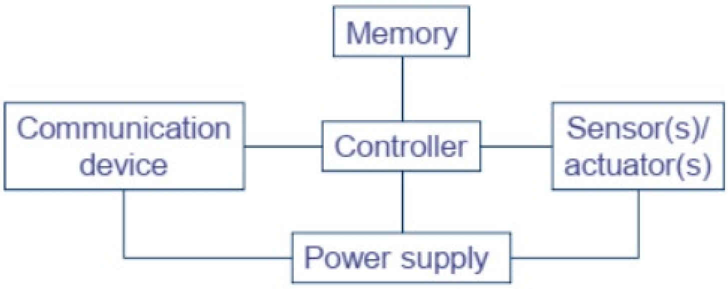
- Data centric networking
  - Focusing network design on ***data***, not on ***node identifies*** (id-centric networking)
  - To improve efficiency
- Locality
  - Do things locally (on node or among nearby neighbors) as far as possible
- Exploit tradeoffs
  - E.g., between invested energy and accuracy

Compare MANET and WSN.

Feature	Wireless Sensor Network (WSN)	Mobile Ad-hoc Network (MANET)
Purpose	Monitor physical or environmental conditions	Provide network connectivity for mobile devices
Node Type	Specialised sensor nodes with limited processing power	General-purpose devices like laptops, smartphones, etc.

Node Mobility	Usually static	Mobile and dynamic
Network Structure	Pre-defined or self-organizing	Self-organizing and dynamic
Scalability	Designed for large-scale deployments (hundreds to thousands of nodes)	Smaller scale deployments (tens to hundreds of nodes)
Data Traffic	Periodic and low-bandwidth (sensor readings)	Variable and potentially high-bandwidth (voice, video, data)
Security	More focused on data integrity and preventing unauthorized access to sensor data	Needs robust security measures for authentication and access control due to open network nature
Applications	Precision agriculture, environmental monitoring, industrial automation	File sharing, collaborative work, temporary network access
QoS Requirements	Focus on reliable event detection and data accuracy	Focus on connectivity, bandwidth, and low latency for real-time applications
Deployment	Planned or random deployment depending on application	Spontaneous deployment as needed

Explain Sensor node architecture with a diagram



Controller:

- Type: Microcontrollers are the preferred choice due to their low power consumption and processing capabilities optimised for embedded applications.
- Functionality: Acts as the central processing unit, processing sensor data, controlling communication, and managing other components within the node.
- Considerations: Limited processing power compared to general-purpose processors, but sufficient for sensor network tasks.

Power Source:

- Challenges: Remote deployments make battery replacements difficult and expensive. Energy efficiency is crucial for long-term operation.
- Options: Rechargeable or non-rechargeable batteries are the main source, but energy harvesting techniques like solar panels are being explored.
- Energy Consumption: Data transmission is the most energy-consuming task. Careful design and protocols are needed to minimise power usage.

Sensors/Actuators:

- Sensing Types: Sensors can be passive (self-powered, detecting changes in the environment) or active (requiring continuous power for probing the environment like radar).
- Selection: Choice depends on the application (e.g., temperature, pressure, motion). Sensors should be small, low-power, and have appropriate accuracy and sensitivity.
- Capabilities: Some nodes integrate actuators allowing them to take physical actions based on sensor data (e.g., adjusting a valve based on temperature readings).

Communication Devices:

- Technology: Radio transceivers are used for wireless communication, converting digital data into radio waves for transmission and receiving radio waves and converting them back to data.
- Range and Frequency: Transmission range and radio frequency depend on application needs and regulations.
- Protocols: Communication protocols define data formatting and transmission procedures for efficient and reliable data exchange within the network.

Memory:

- Types: Flash memory is commonly used for program and data storage due to its low power consumption and high storage capacity.
- Capacity: Memory requirements depend on the application's complexity and data storage needs.
- Trade-offs: Balancing memory capacity with cost and power consumption is crucial.

Explain the different Transceiver states of a Sensor node

A wireless transceiver is a key component that enables wireless communication. Here's a breakdown of its operation:

Functionality:
Combines a transmitter and a receiver in a single unit.
Transmitter:

- Converts digital data (1s and 0s) from a computer into an analog signal (radio waves or light). This process is called modulation.
- Amplifiers boost the strength of the signal before transmission via an antenna.

Receiver:

- Picks up the weak transmitted signal from the antenna.
- Demodulates the signal back into digital data that the receiving computer can understand.

Operational States:

- Transmit: Actively sending data.
- Receive: Actively listening for and receiving incoming data.
- Idle: Ready to receive data but not currently doing so.
    - In this state, some hardware components can be powered down to conserve energy. However, leakage current still consumes some power.
- Sleep: Most transceiver components are powered down, significantly reducing power consumption.
    - The device cannot receive data immediately upon entering sleep mode.
    - Waking up from sleep requires some time and energy.

Key Points:

- Transceivers are often integrated into wireless network interface cards (NICs).
- Selecting the appropriate operational state (idle vs. sleep) depends on factors like data traffic and power conservation needs.

What are the Operating system challenges in WSN

Traditional OS Goals:

- Resource Virtualization: Provide an abstraction layer hiding hardware complexities and allowing applications to access resources uniformly.
- Resource Protection: Prevent concurrent access conflicts and ensure data integrity through mechanisms like memory management and protected CPU modes.

Challenges in WSNs:

- Limited Resources: Microcontrollers lack features like memory management units (MMUs) and protected CPU modes common in traditional operating systems.
- Cost and Power Constraints: Implementing a full-fledged OS would increase complexity, cost, and power consumption, negating the benefits for resource-constrained WSNs.

Approaches for WSNs:

- Lightweight OS Approach:
    - Develop a lightweight OS that provides:
    - A programming interface for application development.
    - Process support (with limitations due to lack of memory protection).
    - Trade-off: Simplified OS offers some abstraction but may not fully isolate processes, potentially impacting reliability.
- Bare-Metal Approach:
    - Eliminate the OS entirely.
    - Applications have direct hardware control, maximizing efficiency.

    - Drawback: Complex programming model with low-level hardware details and potential for errors due to lack of protection mechanisms.
- Current Trend:
    - Simple Runtime Environment: Popular choice for WSNs.
    - Provides basic abstractions to simplify hardware interaction for application development.
    - Focuses on efficiency and avoids full OS overhead.
    - Impact: Requires a unique programming model compared to traditional OS-based development.

Write a note on TinyOS.

Traditional operating systems are not well-suited for resource-constrained sensor networks due to

- Limited resources: Sensor nodes have limited processing power, memory, and battery life.
- Concurrency needs: Sensor nodes handle multiple tasks simultaneously (e.g., sensor readings, communication).
- Diversity in design: Sensor networks are application-specific, requiring modular and adaptable software.

TinyOS: A Tailored Solution

Developed at UC Berkeley, TinyOS is a popular lightweight operating system designed specifically for sensor networks. It addresses the challenges mentioned above with the following features:

- Event-driven Architecture: Responds to events triggered by sensors, timers, or network communication. This conserves power by focusing on tasks when needed instead of continuous operation.
- Software Modularity: Applications are built as a combination of components. Each component includes:
- Commands: Represent requests for services (e.g., start sensor reading).
- Event Handlers: Define how to react to specific events.
- Internal Storage: Stores component-specific data.
- Static Memory Allocation: Memory allocation happens during compilation, improving efficiency and reducing runtime overhead.
- Focus on Efficiency: The goal is to perform tasks quickly and then enter a low-power sleep state.

Key Concepts in TinyOS:

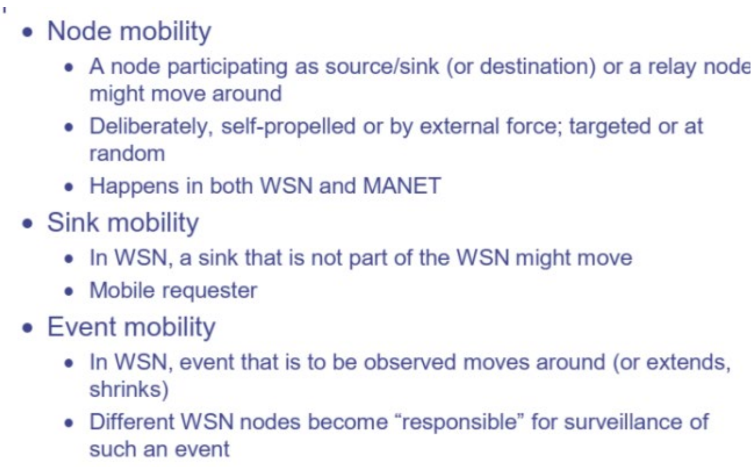
Commands:

- Non-blocking requests for services from components.
- Can be used to trigger sensor readings, communication, or other actions.
- Can be chained together to form complex workflows.

Events:

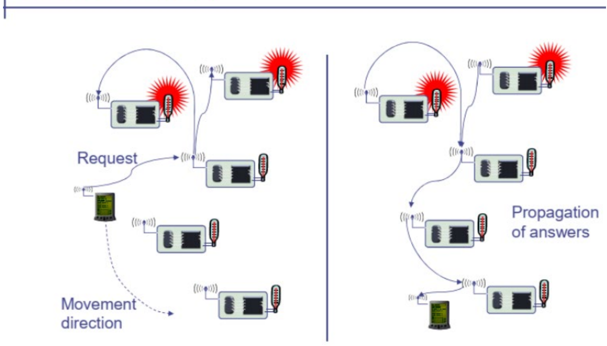
- Time-critical occurrences triggered by hardware interrupts (timers, sensors, etc.).
- Short in duration to minimise processing overhead.
- Can trigger tasks, signal higher-level events, or call lower-level commands.

What are the different sources of mobility in WSNs?

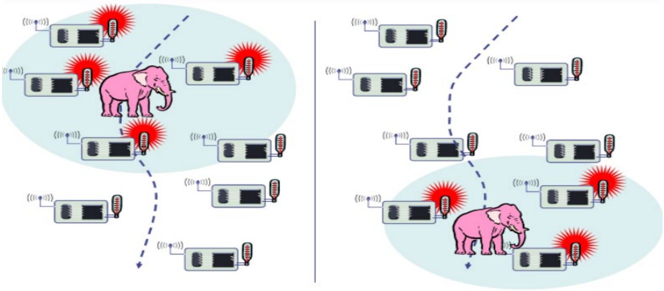


- Node mobility
  - A node participating as source/sink (or destination) or a relay node might move around
  - Deliberately, self-propelled or by external force; targeted or at random
  - Happens in both WSN and MANET
- Sink mobility
  - In WSN, a sink that is not part of the WSN might move
  - Mobile requester
- Event mobility
  - In WSN, event that is to be observed moves around (or extends, shrinks)
  - Different WSN nodes become “responsible” for surveillance of such an event

WSN sink mobility



WSN event mobility: Track the pink elephant



Here: Frisbee model as example

Explain the quality of service parameters of WSN

- 1. Event Detection/Reporting Probability:
  - Measures the likelihood of an actual event going undetected or unreported to the designated information sink.
  - Balancing factors:
    - Overhead associated with setting up network structures for event reporting (e.g., routing tables).
  - Runtime overhead related to factors like sampling frequencies.
- 2. Event Classification Error:
  - When events need to be not only detected but also categorised, this attribute measures the accuracy of that classification.
- 3. Event Detection Delay:
  - Represents the time difference between detecting an event and reporting it to the interested parties.
- 4. Missing Reports:
  - In applications requiring periodic reporting, this attribute focuses on minimising the probability of undelivered reports.
- 5. Approximation Accuracy:
  - Relevant for applications that approximate a function (e.g., temperature distribution in an area). It measures the deviation (absolute or relative) between the approximated function and the actual one.
- 6. Tracking Accuracy:
  - Crucial for tracking applications. It encompasses various aspects:
  - Minimising missed detections of the tracked object.
  - Ensuring reported positions are close to the actual location (low positional error).
  - Maintaining accuracy even with temporary sensing gaps (areas without sensor coverage).

Write a note on in-networking processing in WSNs

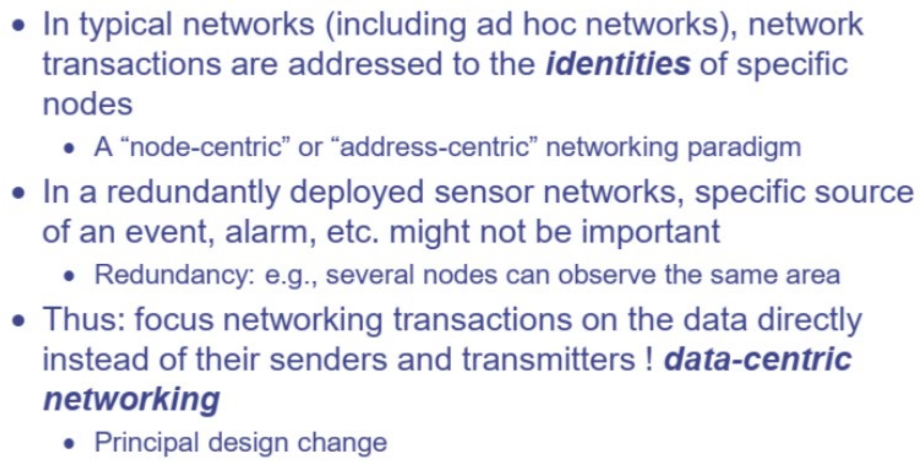
In-Network Processing: Boosting Efficiency in Wireless Sensor Networks (WSNs)
In-network processing is a powerful technique for WSNs that involves processing sensor data within the network itself, rather than sending it all to a central location for processing. Here's a breakdown of its key benefits and challenges:
Advantages:

- Energy Efficiency: Reduces the amount of data transmitted, saving battery life on sensor nodes. This is crucial since sensor nodes are often battery-powered and difficult to replace.
- Scalability: Improves network performance in large deployments by processing data closer to the source, reducing overall network traffic.
- Reduced Redundancy: Eliminates unnecessary transmission of redundant information collected by multiple sensors.
- Advanced Functionality: Enables WSNs to provide more complex services beyond simple data collection, allowing for real-time processing and analysis.

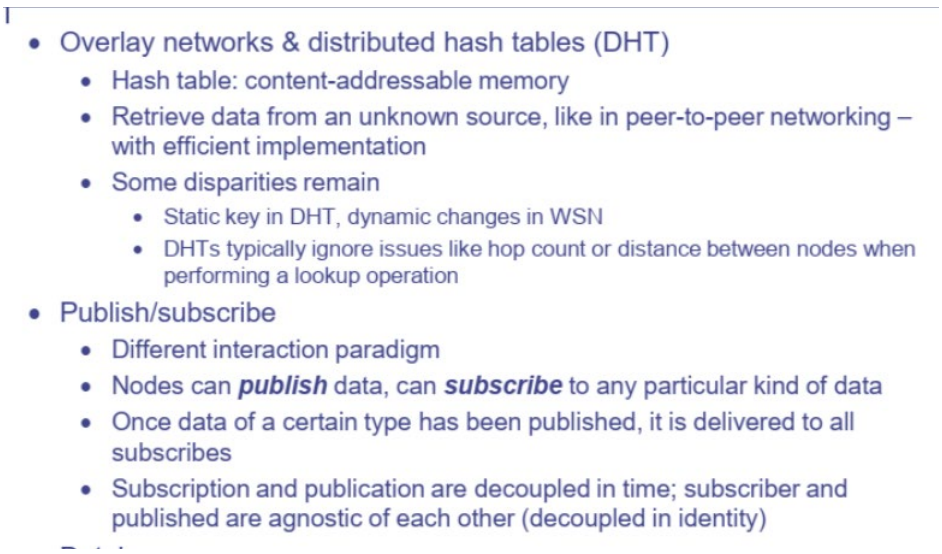
Challenges:

- Balancing Act: Finding the right balance between:
- Computational Overhead: The energy consumed by processing data on sensor nodes (limited processing power).
- Delay: The time it takes to process data within the network can introduce delays in data delivery.
- Data Resolution: Processing might reduce the detail or accuracy of the data collected.
- Data Trustworthiness: Ensuring data integrity and security becomes more complex when processing happens within the network.

What is Data centric networking and its implementation options in WSNs?



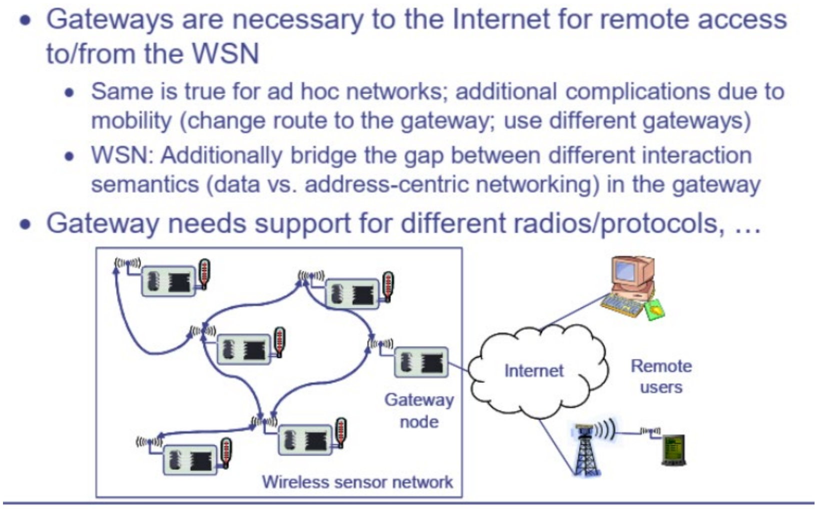
- In typical networks (including ad hoc networks), network transactions are addressed to the ***identities*** of specific nodes
  - A "node-centric" or "address-centric" networking paradigm
- In a redundantly deployed sensor networks, specific source of an event, alarm, etc. might not be important
  - Redundancy: e.g., several nodes can observe the same area
- Thus: focus networking transactions on the data directly instead of their senders and transmitters ! ***data-centric networking***
  - Principal design change



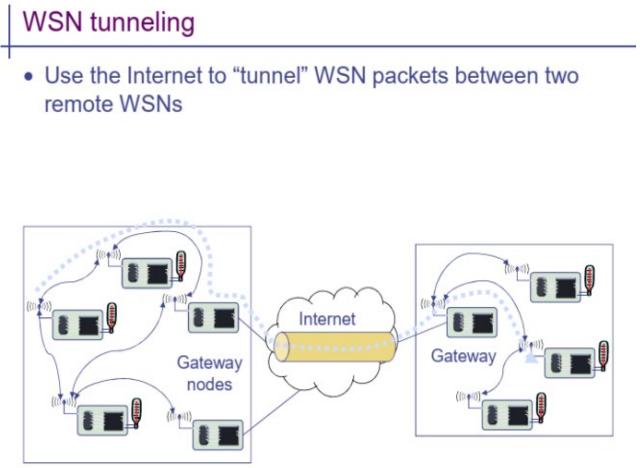
- Overlay networks & distributed hash tables (DHT)
  - Hash table: content-addressable memory
  - Retrieve data from an unknown source, like in peer-to-peer networking – with efficient implementation
  - Some disparities remain
    - Static key in DHT, dynamic changes in WSN
    - DHTs typically ignore issues like hop count or distance between nodes when performing a lookup operation
- Publish/subscribe
  - Different interaction paradigm
  - Nodes can ***publish*** data, can ***subscribe*** to any particular kind of data
  - Once data of a certain type has been published, it is delivered to all subscribes
  - Subscription and publication are decoupled in time; subscriber and published are agnostic of each other (decoupled in identity)

. How does gateway play role in WSNs?

- A gateway is a network node that connects two networks using different protocols
- together.
- A gateway is used to join two dissimilar networks.
- A gateway is a data communication device that provides a remote network with connectivity to a host network.
- A gateway device provides communication to a remote network or an autonomous system that is out of bounds for the host network nodes.
- Gateways serve as the entry and exit point of a network; all data routed inward or outward must first pass through and communicate with the gateway in order to use routing paths.
- Generally, a router is configured to work as a gateway device in computer networks.



- Gateways are necessary to the Internet for remote access to/from the WSN
  - Same is true for ad hoc networks; additional complications due to mobility (change route to the gateway; use different gateways)
  - WSN: Additionally bridge the gap between different interaction semantics (data vs. address-centric networking) in the gateway
- Gateway needs support for different radios/protocols, …

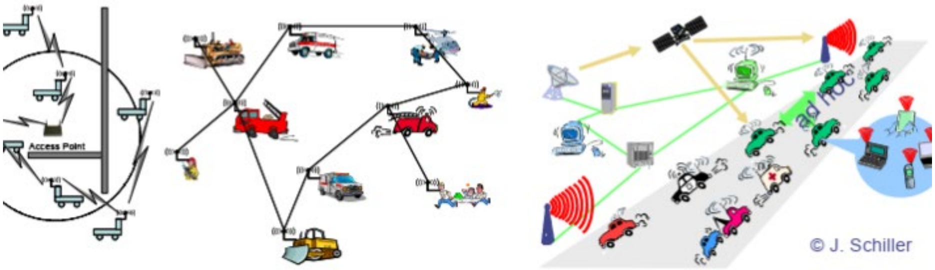


WSN tunneling

- Use the Internet to "tunnel" WSN packets between two remote WSNs

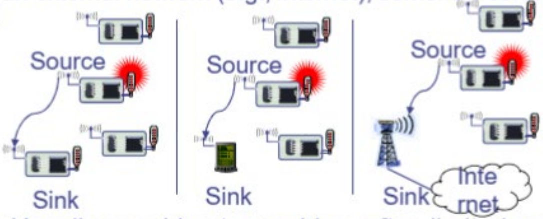
What are basic network scenarios in Ad hoc networks and WSNs?

- (Mobile) ad hoc scenarios
  - Nodes talking to each other
  - Nodes talking to “some” node in another network (Web server on the Internet, e.g.)
    - Typically requires some connection to the fixed network
  - Applications: Traditional data (http, ftp, collaborative apps, …) & multimedia (voice, video) ! humans in the loop



© J. Schiller

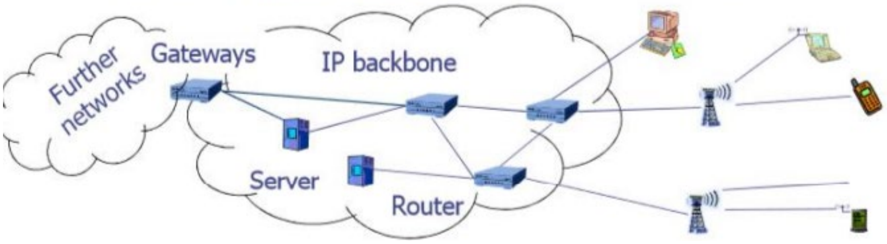
- Sensor network scenarios
  - ***Sources***: Any entity that provides data/measurements
  - ***Sinks***: Nodes where information is required
    - Belongs to the sensor network as such
    - Is an external entity, e.g., a PDA, but directly connected to the WSN
      - Main difference: comes and goes, often moves around, …
    - Is part of an external network (e.g., internet), somehow connected to the WSN



  - Applications: Usually, machine to machine, often limited amounts of data, different notions of importance

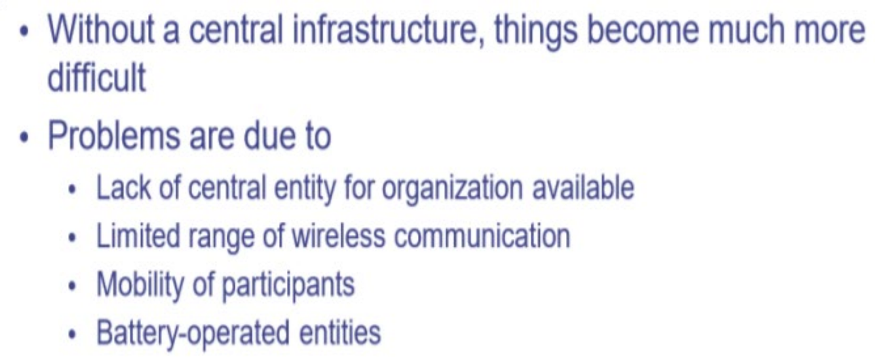
Write a note on Infrastructure-based wireless networks

- Typical wireless network: Based on infrastructure
  - E.g., GSM, UMTS, …
  - Base stations connected to a wired backbone network
  - Mobile entities communicate wirelessly to these base stations
  - Traffic between different mobile entities is relayed by base stations and wired backbone
  - Mobility is supported by switching from one base station to another
  - Backbone infrastructure required for administrative tasks



What are ad hoc networks and what are their challenges?

An ad hoc network is a type of temporary computer-to-computer connection. In ad hoc mode, you can set up a wireless connection directly to another computer without having to connect to a Wi-Fi access point or router. The network is ad hoc because it does not rely on a pre-existing infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. Instead, each node participates in routing by forwarding data for other nodes, so the determination of which nodes forward data is made dynamically on the basis of network connectivity and the routing algorithm in use



- Without a central infrastructure, things become much more difficult
- Problems are due to
  - Lack of central entity for organization available
  - Limited range of wireless communication
  - Mobility of participants
  - Battery-operated entities

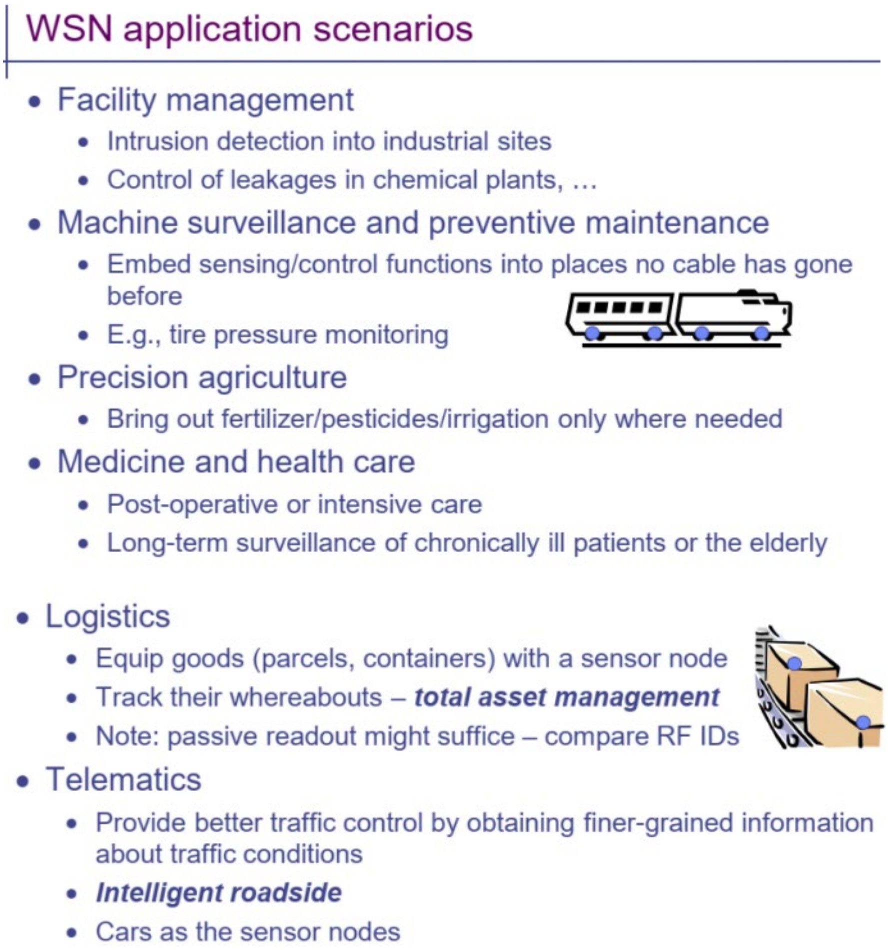
What are MANETs and what are their design challenges? (same as 17)

- A type of wireless network where devices connect directly with each other, without a central access point.
- Nodes can be mobile and change locations, requiring the network to self-configure on the fly.
- Connections can be established using various wireless technologies like Wi-Fi, cellular, or satellite.
- Applications range from small local networks (e.g., laptops sharing files) to large-scale deployments like emergency response or environmental monitoring.

Challenges of MANETs:

- Limited Bandwidth: Wireless connections generally offer less bandwidth compared to wired networks. Factors like fading, interference, and multiple access methods can further limit effective data transfer rates.
- Dynamic Topology: Nodes move around, constantly changing the network layout. This makes maintaining routing tables and connections a challenge. Trust between nodes can also be difficult to establish in such a dynamic environment.
- High Routing Overhead: Due to the ever-changing network topology, routing protocols need to constantly update routes to maintain connectivity. This can consume significant resources on mobile devices.
- Hidden Terminal Problem: A node outside the sender's range but within the receiver's range can attempt to transmit simultaneously, causing collisions and data loss.
- Transmission Errors and Packet Loss: Collisions, interference, hidden terminals, and frequent path breaks due to mobility can lead to high packet loss in MANETs.
- Security Threats: The open nature of wireless communication makes MANETs susceptible to security attacks. Trust management between nodes is crucial to prevent unauthorised access or data manipulation.

What are different applications scenarios of WSN?



WSN application scenarios

- Facility management
  - Intrusion detection into industrial sites
  - Control of leakages in chemical plants, …
- Machine surveillance and preventive maintenance
  - Embed sensing/control functions into places no cable has gone before
  - E.g., tire pressure monitoring
- Precision agriculture
  - Bring out fertilizer/pesticides/irrigation only where needed
- Medicine and health care
  - Post-operative or intensive care
  - Long-term surveillance of chronically ill patients or the elderly

- Logistics
  - Equip goods (parcels, containers) with a sensor node
  - Track their whereabouts – ***total asset management***
  - Note: passive readout might suffice – compare RF IDs
- Telematics
  - Provide better traffic control by obtaining finer-grained information about traffic conditions
  - ***Intelligent roadside***
  - Cars as the sensor nodes

How can the applications of WSN be classified based on interaction patterns between sources and sinks?

- 1. Event Detection:
  - Simple Events: Detected by a single sensor (e.g., temperature exceeding a threshold).
  - Complex Events: Collaboration among multiple sensors needed (e.g., detecting a steep temperature gradient).
  - Event Classification: May be required if multiple event types are possible (e.g., distinguishing fire from engine heat).
- 2. Periodic Measurements:
  - Triggered by Events: Measurements reported upon detecting an event (e.g., increased temperature readings after a fire alarm).
  - Application-Dependent Frequency: Reporting frequency varies based on the application's needs (e.g., more frequent readings for critical events).
- 3. Function Approximation and Edge Detection:
  - Approximating a Function: Estimating how a physical value (e.g., temperature) changes spatially based on sensor data.
  - Balancing Accuracy and Energy: Trade-off between achieving a desired accuracy and minimising energy consumption by sensors.
  - Edge Detection: Identifying boundaries or areas with specific values (e.g., finding the fire perimeter by locating points with the same high temperature).
- 4. Tracking:
  - Mobile Event Sources: Tracking the movement of objects like intruders in a surveillance scenario.
  - Sensor Collaboration: Sensors work together to provide updates on the object's position.

    - Positional Estimates: May include speed and direction estimations along with location updates.

Unit 3

What are Transport Control Protocols and what are its features?

Transmission control protocol (TCP) is a network communication protocol designed to send data packets over the Internet. TCP is a transport layer protocol in the OSI layer and is used to create a connection between remote computers by transporting and ensuring the delivery of messages over supporting networks and the Internet.
Transmission Control Protocol is one of the most used protocols in digital network communications and is part of the Internet protocol suite, commonly known as the TCP/IP suite. Primarily, TCP ensures end-to-end delivery of data between distinct nodes. TCP works in collaboration with Internet Protocol, which defines the logical location of the remote node, whereas TCP transports and ensures that the data is delivered to the correct destination. Before transmitting data, TCP creates a connection between the source and destination node and keeps it live until the communication is active. TCP breaks large data into smaller packets and also ensures that the data integrity is intact once it is reassembled at the destination node.

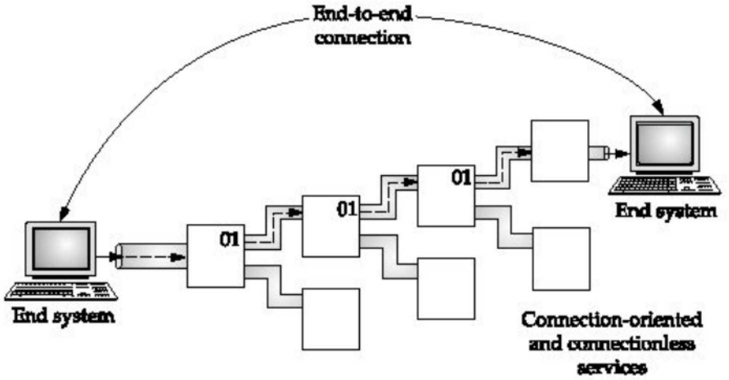
1. Connection oriented: An application requests a “connection” to destination and uses connection to transfer data
2. Stream Data transfer:- It is the duty of TCP to pack this byte stream to packets, known as TCP segments, which are passed to the IP layer for transmission to the destination device.
3. Reliable:- It recovers data from Network layer if data is damaged, duplicated or corrupted.
4. Point to Point:- TCP connection provides end to end delivery.
5. Interoperability:- It eliminates the cross-platform boundaries.
6. Error and flow control:- error-checking, flow-control, and acknowledgement functions.
7. Name resolution:- It helps in solving human readable name into IP address.
8. Routability:- TCP/IP is a routable protocol,
9. It helps in resolving logical address.
10. Full Duplex:- It provides connection in both the directions.

What are the phases of connection in connection oriented and connectionless TCPs?

Two distinct techniques are used in data communications to transfer data.
Each has its own advantages and disadvantages. They are the connection-oriented method and the connectionless method:

- **Connection-oriented** Requires a session connection (analogous to a phone call) be established before any data can be sent. This method is often called a "reliable" network service. It can guarantee that data will arrive in the same order. Connection-oriented services set up virtual links between end systems through a network, as shown in Figure 1. Note that the packet on the left is assigned the virtual circuit number 01. As it moves through the network, routers quickly send it through virtual circuit 01.
- **Connectionless** Does not require a session connection between sender and receiver. The sender simply starts sending packets (called datagrams) to the

destination. This service does not have the reliability of the connection-oriented method, but it is useful for periodic burst transfers. Neither system must maintain state information for the systems that they send transmission to or receive transmission from. A connectionless network provides minimal services.



- Connection-Oriented (CO): Establishes a connection before data transfer. Ensures reliable delivery and order of data. Examples: TCP (Transport layer), X.25 (Data Link layer).
- Connectionless (CL): No prior connection setup. Faster but doesn't guarantee delivery or order. Examples: UDP (Transport layer), LANs (Data Link layer), Internet (Network layer).

Examples:

- LANs: Operate connectionlessly, but transport protocols like TCP can establish CO sessions.
- Internet: Uses connectionless IP at the network layer, with TCP providing CO services on top.
- MPLS: A newer CO scheme for IP that creates label-switched paths for faster routing.
- WAN Services: Frame Relay (PVCs) and ATM (virtual circuits) are examples of CO WAN services.

Key Takeaways:

The choice between CO and CL depends on the trade-off between reliability and speed. Modern networks often combine CO services (like TCP) built on top of CL layers (like IP) for optimal performance.

What are the objectives of WSN MAC Design?

Wireless Sensor Networks (WSNs) have unique challenges due to their battery-powered nature and often large-scale deployments. Here's a breakdown of the key objectives for designing effective Medium Access Control (MAC) protocols in WSNs:

1. Energy Efficiency (Top Priority):

- Duty Cycling: Nodes spend most of their time in low-power sleep mode, waking up periodically to transmit or receive data. This minimises idle listening, where nodes waste energy waiting for packets that may not be for them.
- Overhearing Avoidance: Protocols prevent nodes from receiving irrelevant transmissions, further conserving energy.
- Collision Reduction: Efficient collision avoidance mechanisms minimise wasted energy from retransmitting packets that collide with other transmissions.

2. Scalability:

- Distributed Operation: Large WSNs benefit from distributed MAC protocols that don't rely on a central coordinator, reducing overhead and improving scalability.

- Adaptability to Network Density: Protocols should adjust their behaviour based on the number of nodes in the network to maintain efficiency.

3. Latency (for Time-Sensitive Applications):
    - Prioritisation: Protocols can treat critical data (e.g., intrusion detection) with higher priority for faster delivery.
    - Low Latency Mechanisms: The protocol design should aim for efficient data forwarding and minimise delays in delivering critical packets.
4. Fairness:
    - Channel Access Mechanisms: Techniques like Time Division Multiple Access (TDMA) or Carrier Sense Multiple Access (CSMA) allocate channel access fairly to ensure all nodes have a chance to transmit.
5. Adaptability to Network Conditions:
    - Power Control: Adjusting transmission power can improve link quality and reduce interference between nodes.
    - Adaptive Channel Selection: Protocols that can sense channel conditions and switch to less congested channels can maintain performance in dynamic environments.
6. Reliability:
    - Error Detection and Correction: Techniques like using error-correcting codes help ensure data integrity despite potential noise or interference in the wireless channel.
    - Retransmission Mechanisms: Protocols may employ mechanisms to resend lost packets if necessary.

Additional Considerations:

- Throughput: While energy efficiency is paramount, some applications might also require high data rates. Protocols might consider optimising throughput when possible without compromising energy efficiency.
- Security: MAC protocols should consider security measures to protect against eavesdropping or malicious attacks on the network.
- Support for Mobility: If sensor nodes are mobile, the MAC protocol needs to handle handovers (switching from one access point to another) and node association (adding new nodes to the network) seamlessly.

Explain the sources of energy waste in WSN.

- Collisions:
    - Occurs when multiple nodes transmit simultaneously, causing data corruption.
    - The destination node receives useless data, wasting energy.
    - Retransmissions of collided packets further increase energy consumption and delays.
    - Solutions:
        - Collision Avoidance Protocols: Techniques like TDMA (Time Division Multiple Access) or careful CSMA (Carrier Sense Multiple Access) with hidden terminal detection can prevent collisions.
        - Fixed Assignment Schemes: Pre-assigning transmission slots to nodes eliminates collisions.
- Overhearing:
    - Occurs when a node receives packets not intended for it.
    - This wastes energy, especially with high network traffic and node density.
    - Solutions:
        - Spatial Reuse: Techniques that exploit the limited transmission range of nodes to reduce overlap and overhearing.

    - Directed Transmission: Sending data only to specific nodes that need it.
- Idle Listening:
  - Occurs when a node is in a listening state but doesn't receive any data.
  - This can consume a significant portion of energy (reportedly 50-100% of receive energy).
  - Solutions:
    - Duty Cycling: Nodes alternate between sleep and active states, reducing idle listening time.
    - Low-Power Listening Mechanisms: Techniques that allow nodes to listen for transmissions with minimal energy consumption.
- Control/Protocol Overhead:
  - Energy is consumed for sending, receiving, and processing control packets used by MAC protocols.
  - While necessary, minimising overhead is crucial.
  - Solutions:
    - Lightweight Protocols: Designing MAC protocols that use minimal control messages.
    - Adaptive Protocols: Protocols that adjust control overhead based on network conditions.

Schedule-Based vs. Contention-Based MAC Protocols in WSNs

Feature	Schedule-Based MAC	Contention-Based MAC
Access Mechanism	Nodes are assigned specific time slots for transmission.	Nodes compete for access to the shared medium.
Scheduling	Done by a central coordinator or distributed algorithm.	No central coordination, nodes decide who transmits.
Deterministic Access	Guaranteed access within assigned time slots.	No guarantee of access, collisions can occur.
Latency	Generally lower due to planned transmissions.	Can be variable depending on channel contention.

Fairness	Requires careful scheduling to ensure fair access.	May not be inherently fair, some nodes might be starved.
Scalability	May face challenges with large, dynamic networks.	Generally more scalable for large networks.
Complexity	More complex to implement scheduling and coordination.	Simpler to implement, less overhead for basic protocols.
Energy Efficiency	Can be energy-efficient if duty cycling is used.	May require more energy due to retransmissions from collisions.
Examples	TDMA (Time Division Multiple Access),	CSMA (Carrier Sense Multiple Access),

Additional Notes:
Schedule-Based MACs:

- Well-suited for applications with predictable traffic patterns and real-time requirements.
- Can be less efficient with bursty or unpredictable traffic.

Contention-Based MACs:

- More flexible and adaptable to changing network conditions.
- Can suffer from performance degradation in high-traffic scenarios due to collisions.

How to shut up senders in WSN

In WSNs, the goal is to control and optimize transmissions, not completely silence them. Idle listening consumes significant energy, so techniques focus on reducing unnecessary transmissions.
Managing Sender Behavior:

Duty Cycling and Sleep Scheduling:

- Concept: Nodes alternate between active (transmit/receive) and sleep states.
- Benefits: Significantly reduces energy waste.
- Techniques:
    - Synchronised Sleep: Nodes coordinate sleep/wake periods for organised data collection.

  - Asynchronous Sleep: Nodes have independent cycles for increased fault tolerance.

TDMA-based MAC Protocols:

- Concept: Time Division Multiple Access (TDMA) assigns specific time slots to nodes for transmission.
- Benefits: Eliminates collisions, minimises idle listening.
- Control: Nodes only transmit in their designated slots, conserving power during sleep periods.

Contention-based MAC Protocols with Suppression:

- Concept: Protocols (like CSMA/CA) use carrier sensing to avoid transmitting on a busy channel.
- Suppression Mechanisms:
  - Backoff Periods: Nodes wait randomly before retrying a transmission after sensing a busy channel, reducing collisions.
  - RTS/CTS: Request-to-Send/Clear-to-Send signalling allows nodes to reserve the channel for transmission, preventing collisions.

Query-based Systems:

- Concept: Centralised or designated nodes issue queries to trigger data transmissions from specific sensors, instead of continuous pushing of data.
- Control: Sensors only transmit when explicitly requested, minimising unnecessary traffic.

Geographic Routing and Data Aggregation:

- Geographic Routing: Data is forwarded based on node location, sometimes requiring fewer nodes to participate.
- Data Aggregation: Nodes can combine data (e.g., compute averages) before transmission, reducing the number of messages.

Important Considerations:

- Criticality: In applications like fire detection, rapid and continuous data transmission is crucial.
- Adaptive Approaches: WSNs should dynamically adjust sender behaviour based on network conditions. For example, increasing wake periods during high-traffic phases.

Write a note on Sensor MAC.

S-MAC is a Medium Access Control (MAC) protocol specifically designed for Wireless Sensor Networks (WSNs).

Network Model:

- Peer-to-Peer communication: Unlike some protocols that focus on communication with a central base station, S-MAC assumes communication occurs between sensor nodes themselves.

Application Focus:

- Tolerates latency: Applications involving S-MAC typically have long periods where nodes are idle and can tolerate some delay in data transmission.

Design Goals:

- Energy Efficiency: S-MAC prioritises minimising energy consumption by addressing major energy drains:
- Periodic Listen and Sleep: Nodes sleep most of the time, waking up only for transmissions or to receive specific messages.
- Collision Avoidance: Techniques are employed to prevent collisions that waste energy due to retransmissions.

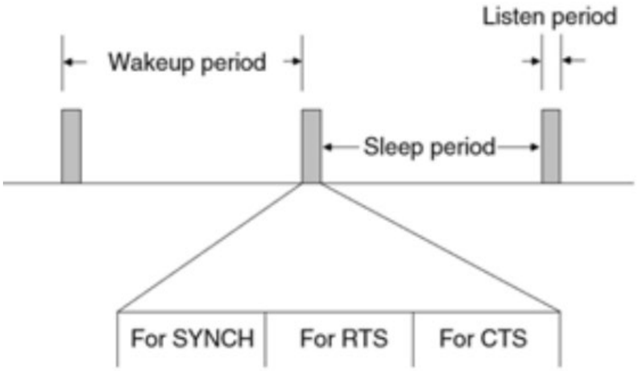
- Coordinated Synchronisation: Nodes synchronise sleep and wake schedules for organised communication with minimal wasted listening.
- Message Passing: Data aggregation and other techniques reduce the number of transmissions required.
- Scalability: S-MAC is designed to work efficiently in sensor networks with a large number of nodes.
- Collision Avoidance: S-MAC aims to minimise collisions during data transmission.

Trade-offs:

- Fairness: To achieve energy efficiency, S-MAC may allow some performance degradation in terms of fairness (equal access to the channel) and latency (transmission delays) compared to other protocols.

Implementation:

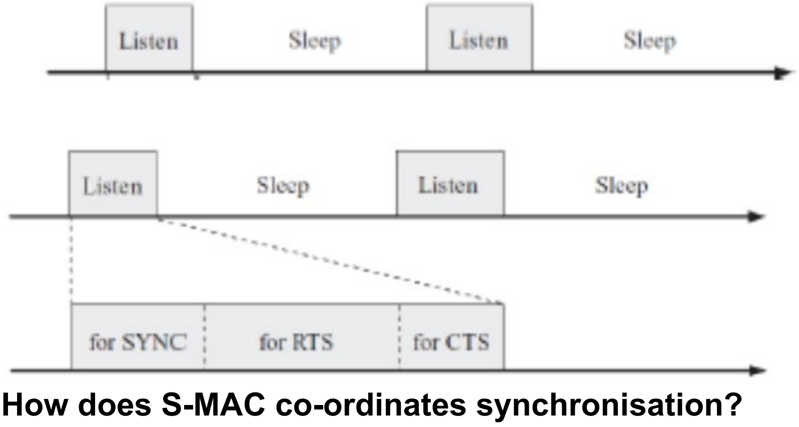
S-MAC builds upon the IEEE 802.11 standard, a common wireless networking protocol, but with additional control mechanisms optimised for sensor networks.



RTS - request to send and CTS - clear to send

How to S-MAC Periodic Listen and Sleep Mechanism works and how does S-MAC passes messages?

To reduce idle listening
Establish a low-duty-cycle operation on each node
Ratio of listen time to whole frame time
A complete cycle of listen and sleep periods is called a frame.
The listen period is further divided into smaller intervals for sending or receiving SYNC, RTS, and CTS packets.
The duration of the listen period is normally fixed depending on physical - and MAC - layer parameters, e.g.the radio bandwidth and the contention window size.



How does S-MAC co-ordinates synchronisation?

To establish coordinated or synchronised sleep schedules, each node exchanges its schedule with other nodes by periodically (in SYNC)
S - MAC allows a node to adopt multiple schedules to enable multihop operation in the network.
S - MAC uses relative timestamps instead of absolute ones to avoid clock drifts
Nodes try to pick up schedule synchronisation from neighbouring nodes
If no neighbour found, nodes pick some schedule to start If additional nodes join, some node might leam about two different schedules from different nodes
'Synchronised islands' To bridge this gap, it has to follow both schemes

What are the routing challenges and design issues in WSN?

WSN Distinctions:

- Limited Resources: Sensor nodes have low processing power, memory, and communication capabilities due to cost and size constraints.
- Energy Constraints: Battery life is critical, as frequent recharging might be impractical.
- Scalability: WSNs can range in size from very few nodes to large deployments with thousands of nodes.
- Dynamic Environments: Sensor nodes might be deployed in unpredictable environments with changing conditions.
- Data Traffic Models: WSNs can have diverse data collection patterns – periodic, event-driven, or bidirectional communication with the sink.

Challenges Arising from these Distinctions:
Network Scale and Time-Varying Characteristics:

- Large-scale deployments with limited node capabilities require efficient routing protocols.
- Sensor behavior needs to adapt to changing network conditions and unreliable wireless connections.

Resource Constraints:

- Energy efficiency is paramount. Techniques like duty cycling (sleeping most of the time) are crucial.
- Routing protocols need to optimize data flow while minimizing energy consumption.
- Scalable and efficient routing algorithms are essential.

Sensor Applications Data Models:

- Different applications have varying data gathering needs (periodic, event-driven, bidirectional).
- Routing protocols need to adapt to support diverse data models.

What are the classes of WSN routing techniques? Explain in detail.

Routing Strategies:
Flat Routing Protocols:

- All nodes are considered peers with no hierarchy.
- Advantages:
  - Low overhead for maintaining network structure.
  - Potential for multiple paths for fault tolerance.
- Disadvantages:
  - Can be inefficient for large networks due to increased routing overhead.
  - May not scale well with growing network size.

Hierarchical Routing Protocols (Clustering):

- Nodes are organized into clusters with a cluster head (CH) managing each cluster.
- CHs:
  - Coordinate activities within the cluster.
  - Forward information between clusters.
- Advantages:
  - Improves energy efficiency by reducing data transmissions within clusters.
  - More scalable than flat routing for large networks.
- Disadvantages:
  - Requires additional overhead for cluster formation and maintenance.
  - CH selection and fault tolerance can be complex.

Data-Centric Routing Protocols:

- Focuses on data attributes rather than specific sensor nodes.
- Source node broadcasts an "interest" message specifying the desired data attributes.
- Sensor nodes with relevant data respond to the interest.
- Advantages:
  - Efficient for event-driven data collection.
  - Reduces unnecessary communication overhead.
- Disadvantages:
  - Can be complex to implement and manage.
  - May not be suitable for all applications.

Location-Based Routing Protocols:

- Leverages sensor location information for routing decisions.
- Useful for queries that specify geographical areas of interest.
- Advantages:
  - Efficient for location-aware data collection.
  - Reduces unnecessary transmissions outside the relevant area.
- Disadvantages:
  - Requires additional hardware or configuration for location awareness.
  - May not be applicable for all deployment scenarios.

How does the Flooding technique routes in WSN?

- Used for path discovery and information dissemination in wired and wireless ad hoc networks
- Uses a reactive approach whereby each node receiving a data or control packet sends the packet to all its neighbours
- After transmission, a packet follows all possible paths
- Unless the network is disconnected, the packet will eventually reach its destination
- To prevent a packet from circulating indefinitely in the network, a hop count field is usually included in the packet.
- Initially, the hop count is set to approximately the diameter of the network.
- As the packet travels across the network, the hop count is decremented by one for each hop that it traverses.
- When the hop count reaches zero, the packet is simply discarded.
- A similar effect can be achieved using a time-to-live field, which records the number of time units that a packet is allowed to live within the network.
- Flooding can be further enhanced by identifying data packets uniquely, forcing each network node to drop all the packets that it has already forwarded.
- Flooding suffers several deficiencies when used in WSNs.
- susceptibility to traffic implosion: duplicate control or data packets being sent repeatedly to the same node

- overlap problem: Overlapping occurs when two nodes covering the same region send packets containing similar information to the same node.
- resource blindness: Energy constraint are ignored

How sensor Protocols For Information Via Negotiation technique routes in WSN?

SPIN (Sensor Protocols for Information via Negotiation) is a communication protocol for Wireless Sensor Networks (WSNs) that focuses on efficient data delivery.

Data-Centric and Negotiation-Based:

- SPIN prioritises data content over specific destinations.
- Nodes negotiate data exchange based on metadata descriptions.

Reduces Redundant Transmissions:

- Nodes advertise data using metadata (descriptions) in ADV messages.
- Only interested nodes request data (REQ messages), minimising unnecessary transmissions.

Eliminates Traffic Implosion:

- Unlike flooding protocols, data is only sent to requesting nodes, preventing overwhelming downstream nodes.

Reduces Overlap:

- Metadata descriptions prevent sending the same data to nodes that already have it.

Three Message Types:

- ADV (Advertisement): Announces new data with metadata.
- REQ (Request): Sent by nodes interested in specific advertised data.
- DATA: Carries the actual sensor data along with metadata.

Benefits:

- Efficient data dissemination.
- Reduced energy consumption due to fewer transmissions.
- Improved network scalability.

How does Low-Energy Adaptive Clustering Hierarchy technique routes in WSN?

LEACH (Low-Energy Adaptive Clustering Hierarchy) is a hierarchical routing protocol designed for Wireless Sensor Networks (WSNs) to improve energy efficiency. Here's a breakdown of its key features:

Hierarchical Approach:

LEACH organises the network into clusters, each with a designated cluster head (CH).

Cluster Head Responsibilities:

- Collects data from member nodes within the cluster.
- Aggregates data (combines similar data) to reduce redundancy.
- Transmits aggregated data directly to the base station (single hop).
- Creates a schedule (TDMA) assigning time slots to nodes for data transmission within the cluster.

LEACH Phases:

Setup Phase:

- Cluster-Head Selection: Nodes become CHs based on a probabilistic algorithm, ensuring fair distribution of the CH role and energy consumption.
- Cluster Formation: Non-CH nodes join the closest CH, forming clusters.

Steady-State Phase:

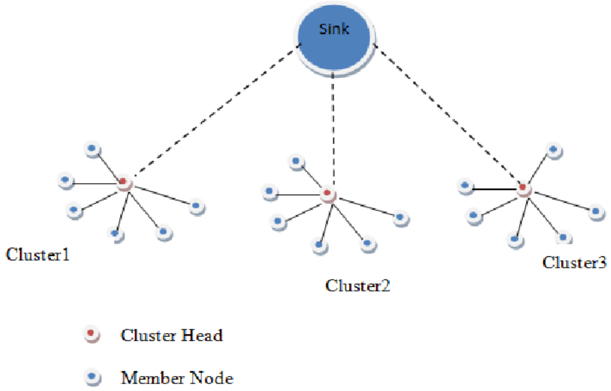
- Data Collection: Nodes transmit data to their CH during their assigned time slots.
- Data Aggregation: CHs aggregate data to remove redundancy.
- Data Transmission: CHs transmit aggregated data to the base station.

Benefits:

- Reduces energy consumption by:
  - Minimising transmissions from non-CH nodes (single-hop to CH).
  - Eliminating collisions with TDMA scheduling.
- Reducing data redundancy through aggregation.
- Improves network scalability.

Limitations:

- CHs might deplete their energy faster due to receiving and processing data from other nodes.
- Requires periodic re-clustering to balance energy consumption.



How does Power-Efficient Gathering in Sensor Information Systems technique routes in WSN?

PEGASIS (Power-Efficient Gathering in Sensor Information Systems) Protocol
The passage describes PEGASIS, a chain-based routing protocol for Wireless Sensor Networks (WSNs) designed to improve energy efficiency. Here's a breakdown of its key points:

Network Assumptions:

- Homogeneous nodes (similar capabilities) deployed across an area.
- Global knowledge of node positions (may not be realistic in all scenarios).
- Adjustable transmission power for controlled range.
- CDMA-capable radios for potentially reducing interference.

Goal:

- Gather and deliver data from sensor nodes to a central sink (base station).

Chain Structure:

- Nodes form a single chain where each node communicates with its closest neighbours.
- Nodes are added progressively, starting from the closest neighbour to the farthest (greedy approach).
- Signal strength is used to measure distance and adjust transmission range for communication with the closest neighbour only.

Chain Leader:

- One node in the chain is chosen as the leader, responsible for transmitting aggregated data to the base station.
- Leadership rotates periodically to distribute energy consumption evenly among nodes.

Data Aggregation:

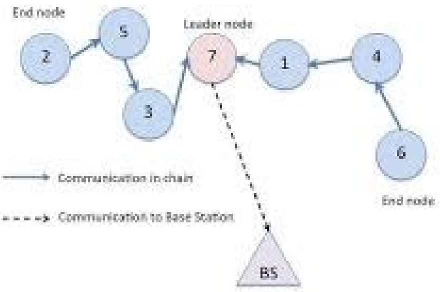
- Data is aggregated (combined) as it travels along the chain towards the leader.
- Two aggregation approaches are mentioned:
- Sequential aggregation: Token-based process where data is aggregated one hop at a time, moving towards the leader from both ends of the chain.
- Parallel aggregation: Simultaneous aggregation along the chain, potentially reducing delay.

Benefits:

- Reduces energy consumption by:
- Minimising transmissions from individual nodes (data travels along the chain).
- Utilising aggregation to reduce data volume.

Limitations:

- Relies on unrealistic assumptions like global knowledge of node positions.
- Might not be suitable for highly dynamic networks.



How does Directed Diffusion technique routes in WSN?

Directed Diffusion, a data-centric routing protocol designed for energy-efficient data collection in Wireless Sensor Networks (WSNs). Here's a breakdown of the key points:

Main Goal:

- Achieve significant energy savings to extend network lifetime.

Communication Approach:

- Focuses on localized communication, minimizing message exchanges beyond a limited network area.

Key Elements:

- Interests: Queries specifying desired data attributes (e.g., temperature > 80°C).
- Data Messages: Sensor data sent in response to matching interests.
- Gradients: Values indicating data relevance and direction to the source.
- Reinforcements: Mechanisms to adjust data delivery rates.

Data Request with Interests:

- The sink broadcasts an "interest message" containing data attributes.
- Nodes maintain an "interest cache" to track received interests.
- Nodes forward interest messages to neighbors if relevant data might exist.

Data Response with Matching:

- Sensor nodes check their cache for matching interests upon receiving data.
- If a match is found, the data is sent to interested neighbors.

Gradient Setup:

- Gradients are set during the initial interest propagation.
- Gradients indicate data relevance (event rate) and direction towards the source.

Path Reinforcement:

- Sink can reinforce specific paths to increase data delivery rate from valuable sources.
- Reinforcement involves resending interest messages at a higher rate along those paths.

Negative Reinforcement:

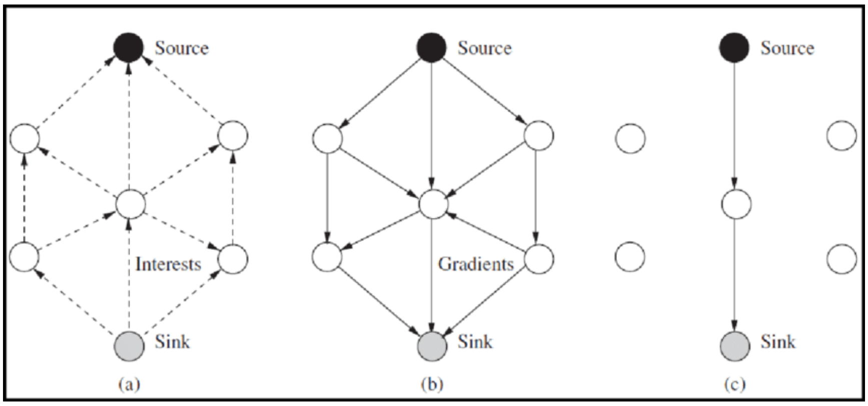
- Paths not explicitly reinforced are negatively reinforced by letting their gradients expire.

Benefits:

- Efficient data collection focused on specific needs.
- Reduced network traffic by forwarding only relevant data.
- Improved energy efficiency by minimising unnecessary transmissions.

Limitations:

- More complex to implement compared to simpler protocols.
- May require additional processing power on sensor nodes.



A- propagating interest B - Making Gradients C- Reinforcing path

How do Geographical Routing strategies routes in WSN?

Focus:

Utilise location data to establish efficient routes for data transmission.

Benefits:

- Reduces control overhead by eliminating unnecessary route discovery messages.
- Minimises energy consumption by focusing transmissions towards the destination.

1. Geocasting:

- Delivers data packets to a designated geographic region.
- Only nodes within the predefined area forward the packet.
- Forwarding zone can be:
- Static: Defined by the source node.
- Dynamic: Adjusted by intermediate nodes to exclude unnecessary detours.

Efficiency of Geocasting:

- Depends on how the forwarding zone is defined and updated during data travel.
- Relies on good network connectivity within the designated zone.

2. Position-Based Routing:

- Nodes only require location information of their immediate neighbors.
- Uses a greedy forwarding mechanism:
- Each node forwards data to the neighbor closest to the destination.
- "Closeness" can be measured by:
  - Euclidean distance
  - Projected distance along a straight line
  - Deviation from a straight line towards the destination

Advantages of Position-Based Routing:

- Lowers control overhead compared to flooding-based protocols.
- Potentially reduces energy consumption by limiting route discovery to single hops.

How do Geographical Routing forwarding approaches work in WSN?

Geographical Routing:

- Leverages location information for efficient route creation.
- Well-suited for WSNs due to data aggregation techniques that reduce redundancy.
- Attractive for large, dynamic networks with unreliable nodes.
- Requires minimal routing table maintenance due to its localised approach.
- Avoids flooding for route discovery.

Greedy Forwarding:

- Nodes forward packets to neighbours closest to the destination (locally optimal choice).
- Nodes only need location data of immediate neighbours, minimising routing table size.

Perimeter Forwarding:

- Activated when greedy forwarding fails due to a void (empty area) between the node and destination.

Explain the phases of flow and congestion control process of TCP?

Slow Start (Exploration Phase):

- Default starting point for all transmissions.
- Congestion window (cwnd): This value limits the number of outstanding data packets (unacknowledged) the sender can transmit.
- Strategy:
- cwnd increases by 1 for each received ACK (acknowledgment) for a data segment.
- This allows the sender to gradually increase transmission rate and probe for available network capacity.
- Example:
  - Start with congestion window (cwnd) = 20 (representing 1 Maximum Segment Size or MSS).
  - After receiving the first ACK, cwnd increases to 21 (2 MSS).
  - If all segments are acknowledged, cwnd becomes 23 (8 MSS).
- Its 2^n per ACK received

2. Congestion Avoidance (Controlled Growth Phase):

Activated when cwnd reaches a threshold value.

Strategy:

- cwnd is incremented by a smaller value (typically 1/cwnd) after each ACK.
- This allows for slower growth, preventing network overload.
- A timer is set for each transmitted segment.

Timeout:

- If the timer expires before an ACK arrives (segment loss), TCP enters slow start again.
- Threshold is halved, and the timer is doubled (penalising for congestion).
- this phase slows down the growth from slow start to prevent congestion.
- Example:
  - Start with cwnd = 1.
  - After each ACK, cwnd increases by 1 (additive increase).
  - So, cwnd becomes 2, then 3, and so on.

3. Fast Recovery and Fast Retransmission (FRFT):
Triggered when TCP detects segment loss based on ACK patterns.
Strategy:

- cwnd is halved (similar to timeout in congestion avoidance).
- The lost segment is immediately retransmitted (fast retransmission).
- FRFT avoids unnecessary slow start if the loss is isolated and not due to congestion.

Overall Benefits:

- Flexible flow control: Allows efficient data transfer based on network capacity.
- Congestion control: Prevents network overload by adjusting transmission rate.
- Reliable data delivery: Ensures data arrives at the receiver through retransmissions.

Explain TCP Connection establishment with three way handshaking and flow control

TCP Characteristics:

- Connection-oriented: Establishes a dedicated connection between two processes (applications) before data transfer.
- Process-to-Process: Delivers data reliably between specific applications on different devices.
- Flow control: Regulates data flow to prevent overwhelming the receiver.
- Error control: Ensures data arrives correctly through error detection and retransmission.
- Full-duplex communication: Allows data transmission in both directions simultaneously.
- Connection Establishment: Three-Way Handshake

This handshake ensures both sides are ready to communicate before data exchange begins.

Client SYN (Synchronise):

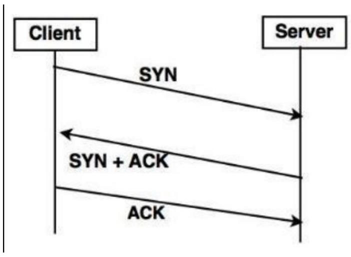
- The client initiates by sending a SYN packet to the server.
- This packet indicates the client's desire to establish a connection and carries a sequence number for data synchronisation.
- Server SYN/ACK (Synchronise/Acknowledge):

Upon receiving the SYN, the server:
Acknowledges the connection request (ACK).

- Sends a SYN packet back (indicating its readiness).
- Includes its own sequence number.
- Client ACK (Acknowledge):

The client acknowledges the server's SYN/ACK packet.
Handshake Outcome:

- After the successful exchange of these three packets, a TCP connection is established, and data transfer can begin.



What is Mobile IP and how does it works?

Mobile IP is a networking technology that allows mobile devices to maintain a constant IP address while roaming across different networks. This ensures uninterrupted communication for applications like remote access and file transfers. Here's a breakdown of the key points:
Benefits:

- Uninterrupted Connectivity: Users keep the same IP address even when switching networks, preventing session disruptions.
- Scalability: Works across various network types (wired, wireless) due to its reliance on IP.
- Simplified Application Use: Applications don't need to adapt to changing IP addresses, maintaining functionality.
- Security: IP-based network services (licenses, access control) remain functional because the IP address stays the same.

Components:

- Mobile Node (MN): The mobile device (phone, laptop) with roaming capability.
- Home Agent (HA): A router on the user's home network that acts as a communication anchor.
- Foreign Agent (FA): A router on a visited network that provides a connection point for the MN.
- Care-of Address (CoA): The temporary IP address assigned to the MN on the visited network.

How it Works:

- Home Network:
  - The MN operates normally with its permanent IP address assigned by the home network.
- Roaming to a Foreign Network:
  - The MN acquires a CoA on the new network (via DHCP, PPP, or other methods).
  - The MN registers its CoA with its HA using a special registration message.
- Communication While Roaming:
  - Data packets addressed to the MN's home IP are intercepted by the HA.
  - The HA encapsulates these packets with a new header containing the MN's CoA.
  - The encapsulated packets are tunneled to the FA on the visited network.
  - The FA decapsulates the packets and delivers them to the MN using its CoA.

Additional Points:

- The MN can discover available FAs through "agent advertisement" messages.
- The MN can deregister with the HA when returning to its home network.
- CoA can be provided by the FA or obtained by the MN dynamically.

What problems may make TCP or UDP unsuitable for implementation in WSNs?

While TCP and UDP dominate internet communication, they fall short in WSNs due to several limitations:
TCP Issues:

- Overhead:
  - The three-way handshake for connection establishment is excessive for small data packets.
- Inefficient Congestion Control:

    - TCP's window-based system reacts poorly to packet loss caused by errors (not congestion). This leads to unnecessary retransmissions and reduced throughput.
- Slow Response:
    - End-to-end congestion control in TCP results in slow response times and higher packet loss, wasting energy on retransmissions.
- Unfairness:
    - Nodes closer to the sink receive more transmission opportunities, depleting their energy faster and potentially disconnecting distant nodes.
- Long RTT Impact:
    - TCP's reliance on end-to-end ACKs leads to lower throughput and longer transmission times with high round-trip times (RTT) common in WSNs.

UDP Issues:

- No Congestion Control:
    - UDP lacks flow and congestion control mechanisms, potentially leading to network congestion and wasted energy due to datagram loss.
- No Reliability:
    - UDP doesn't guarantee delivery, leaving lost datagram recovery to lower or upper layers, increasing processing overhead.

Write notes on any two examples of TCPs

CODA (Congestion Detection and Avoidance):

- Focuses on upstream congestion control (sensor nodes to sink).
- Uses three mechanisms:
    - Congestion Detection: Monitors buffer occupancy and channel load.
    - Open-Loop Backpressure: Congested node notifies upstream neighbor to reduce rate (e.g., using AIMD).
    - Closed-Loop Multisource Regulation:
        - Sensor sets "regulation" bit in packet if exceeding theoretical rate.
        - Sink sends ACK to all sensors to reduce rate if congestion detected.
        - Sink sends ACK to increase rate when congestion clears.
- Disadvantages:
    - Unidirectional control (no sink-to-sensor feedback).
    - No reliability considerations (lost ACKs during congestion).
    - Slower response time under heavy congestion.

PSFQ (Pump Slowly, Fetch Quickly):

- Manages downstream reliability (sink to sensors).
- Goal: Balance slow data delivery with efficient loss recovery.
- Uses three operations:
    - Pump: Sink broadcasts data fragments slowly (every T units).
    - Fetch: Sensor requests missing fragments (NACK) from neighbors upon detection of gaps.
    - NACKs are not relayed by neighbors unless exceeding a threshold.
    - Report: Sink gathers data delivery status from sensors.
- Disadvantages:
    - Can't detect single packet loss.
    - Slow data delivery due to "pumping" approach.
    - Requires larger buffer sizes for hop-by-hop recovery with caching.

Unit 2

What are the fundamental principles of naming and addressing in wireless sensor networks (WSNs)?

Four Pillars of Naming and Addressing in WSNs:

1. Scalability:
   - WSNs can have many nodes, potentially growing over time.
   - Addressing schemes must efficiently assign unique identifiers to a large and dynamic number of nodes.
   - Each node needs to be recognizable and addressable within the expanding network.
2. Energy Efficiency:
   - Sensor nodes typically run on batteries with limited power.
   - Addressing schemes should minimise communication overhead for address management.
   - This includes reducing control messages for address assignment/updates and optimising address size/format for lower energy consumption during transmission.
3. Local Manageability:
   - WSNs are dynamic environments with nodes joining, leaving, or moving.
   - Ideally, addressing schemes allow nodes to manage their own addresses or those of nearby nodes.
   - This distributed approach fosters adaptability and resilience: nodes adjust addressing strategies without global coordination when network changes occur.
4. Fault Tolerance:
   - Harsh conditions and node failures are realities in WSN deployments.
   - Addressing schemes need to be fault-tolerant, adapting to missing or malfunctioning nodes.
   - The overall network addressing system should remain functional even with node disruptions, preventing cascading failures and maintaining network stability.

How are addresses and names managed in WSNs?

Here's a breakdown of different approaches for managing addresses and names in Wireless Sensor Networks (WSNs):

1. Centralised Assignment:
   - Function: A central server or gateway assigns unique addresses to all nodes.
   - Suitability: Good for small, static networks with few nodes and stable topology. Easy to manage and ensures uniqueness.
   - Limitations: Not scalable for large networks. Becomes a single point of failure and struggles with frequent node changes.
2. Hierarchical Addressing:
   - Function: Network has a hierarchical structure (like an inverted tree). Addresses reflect a node's location within the hierarchy.
   - Suitability: Good for medium-sized, geographically dispersed networks. Offers scalability and efficient routing based on hierarchy.
   - Limitations: Maintaining hierarchy and efficient routing paths can be complex in dynamic networks. Requires careful design based on network size and geography.
3. Distributed Assignment:
   - Function: Nodes collaborate with neighbours to discover and assign unique addresses locally. No central authority.

- Suitability: Good for large-scale, dynamic networks. Adapts to topology changes and eliminates single point of failure.
- Limitations: Requires robust algorithms for address assignment and conflict resolution to avoid duplicate addresses. Monitoring can be challenging.

4. Content-Based Addressing:
    - Function: Nodes identified based on the data they collect (type of information or service offered). Focuses on "what" rather than "who".
    - Suitability: Good for applications where specific data types are of interest. Enables efficient querying and data retrieval.
    - Limitations: Not suitable for all applications where node identification or tracking individual data is crucial. Defining a standardised scheme can be challenging.
5. Geographic Addressing:
    - Function: Nodes assigned addresses based on their physical location within the network. Leverages location information.
    - Suitability: Ideal for location-aware applications where knowing sensor node positions is essential (routing, data visualisation).
    - Limitations: Requires mechanisms for acquiring and maintaining location information, which can add overhead. Not feasible for all deployments. Ensuring accurate location data is crucial.

How are MAC addresses assigned in WSNs?

MAC addresses are essential for identifying devices on a network. There are two main approaches for assigning these unique identifiers:

1. Centralised Assignment:
    - Function: A central entity, like a server or router, acts as the sole authority.
    - Process: The central entity assigns unique MAC addresses to each device before deployment or upon connection to the network.
    - Advantages:
        - Simplicity: Easy to implement and manage, especially for small networks.
        - Guaranteed Uniqueness: Central authority ensures no duplicate addresses exist.
    - Disadvantages:
        - Scalability Issues: Managing a central server becomes cumbersome for large networks.
        - Single Point of Failure: If the central entity fails, address assignment is disrupted.
        - Limited Flexibility: Doesn't adapt well to dynamic networks with frequent node changes.
2. Distributed Address Assignment:
    - Function: Devices collaborate with their neighbours to discover and assign unique addresses within their local area.
    - Process: Algorithms are used for devices to find unused addresses and avoid conflicts with neighbours.
    - Advantages:
        - Scalability: No central server needed, allowing for easier network expansion.
        - Flexibility: Adapts to dynamic network changes (nodes joining/leaving/moving) through local address discovery.
        - Fault Tolerance: Network remains operational even with node failures as other nodes can still manage local addressing.
    - Disadvantages:

    - Increased Complexity: Requires implementing algorithms for distributed communication and conflict resolution among nodes.
    - Potential for Address Conflicts: Risk of assigning the same address to different nodes in separate network regions. Mechanisms for global uniqueness are crucial.

How does content-based addressing differ from traditional addressing schemes?

Traditional addressing in WSNs assigns unique IDs to each sensor node. This method has limitations:

- Limited Expressiveness: IDs don't tell you what data a node collects (e.g., temperature, humidity).
- Inefficient Routing: Data packets might be sent to unnecessary nodes before reaching the target.

CBA offers a new approach that focuses on data content, not node identity.

How CBA Works:

- Data packets are tagged with descriptive labels specifying the data type (e.g., "temperature reading").
- Users query the network based on data content (e.g., "find temperatures above 30 degrees Celsius").

Benefits of CBA:

- Enhanced Expressiveness: Users can ask for specific data types, making queries more precise and efficient.
- Efficient Routing: Packets are directed to relevant nodes based on data content, reducing unnecessary traffic.

Unlocking the Potential of CBA:

- Simplifies data acquisition: Users don't need to know node IDs, just the data they want.
- Supports dynamic networks: Data retrieval works even if nodes join/leave.
- Reduces network congestion: Data goes only to relevant nodes, saving energy and bandwidth.

What is the significance of time synchronisation in WSNs?

Imagine a WSN without time synchronisation - it would be like an orchestra without a conductor, resulting in chaos. Time synchronisation ensures all nodes agree on the current time, critical for:

- Data Correlation: Accurate analysis of data from different nodes requires them to be referenced to the same time frame. Imagine comparing temperatures from thermometers with different times - it's meaningless. synchronisation ensures data collected at different times can be compared and interpreted correctly.
- Collaborative Tasks: Many applications involve coordinated actions among nodes, like tracking objects or triggering alarms. Precise timing is crucial. Without synchronisation, nodes might initiate actions at different times, leading to:
    - Missed detections
    - Inaccurate results
    - Network disruptions
- Power Management: WSNs rely on batteries, so energy efficiency is key. synchronisation allows for scheduling sleep/wake cycles effectively. Nodes wake up

and collect data at synchronised intervals, minimising active time and saving energy, extending network life.

What are the different categories of time synchronisation protocols based on synchronisation source ?

In WSNs, time synchronisation keeps all nodes on the same beat. The source of the reference time plays a key role, leading to two main categories of protocols:
1. Sender-Receiver Synchronisation:
- Source: A designated sender node broadcasts its current timestamp periodically.
- Process:
- Receivers estimate the propagation delay (signal travel time) from sender to receiver.
- Receivers adjust their clocks by adding the estimated delay to the received timestamp, aligning with the sender's time.

Advantages:
- Simple and easy to implement.
- Potentially scalable for large networks with a powerful sender.

Limitations:
- Accuracy relies on estimating propagation delay, which can be affected by:
- Environment
- Distance variations
- Single point of failure - sender malfunction disrupts everyone's synchronisation.

Examples: Lightweight Time synchronisation (LTS)
2. Receiver-Receiver Synchronisation:
- Source: No single sender, nodes synchronise directly with neighbours.
- Process:
- Nodes broadcast their timestamps to nearby nodes.
- Each node calculates the time offset between itself and its neighbours:
- Uses received timestamps and estimated propagation delays (based on signal strength).
- Nodes adjust their clocks to minimise the overall time difference with neighbours, achieving local cluster synchronisation.

Advantages:
- Distributed - no single point of failure, more resilient to node failures.
- Potentially more accurate - uses information from multiple neighbours to reduce individual estimation errors.

Limitations:
- Increased communication overhead - frequent timestamp exchange consumes energy and creates network congestion.
- More complex - requires algorithms for efficient offset calculation and clock adjustment.

Examples: Receiver-Receiver Broadcast synchronisation (RBS)

Explain the principle behind the Lightweight Time Synchronisation (LTS) protocol.

LTS is a practical time synchronisation protocol for WSNs, balancing simplicity, efficiency, and moderate accuracy. Here's how it works:
LTS Operation:
- Sender-Receiver Approach: A designated sender node broadcasts beacon messages with timestamps at regular intervals.

- Receiving and Delay Estimation: Receivers within range:
- Receive the beacon message.
- Estimate the propagation delay (signal travel time) from sender to receiver (using factors like signal strength or distance).
- Clock Adjustment: Receivers adjust their clocks based on:
    - Received timestamp from sender.
    - Estimated propagation delay. (Essentially aligning their clocks with the sender's time, accounting for travel time.)

Advantages of LTS:

- Lightweight: Low communication overhead. Sender transmits infrequently, receivers calculate delays locally. Saves energy and bandwidth, ideal for resource-constrained WSNs.
- Simplicity: Easy to implement and integrate due to the straightforward concept. Works well with limited processing power in sensor nodes.

Limitations of LTS:

- Accuracy: Can be affected by:
    - Varying propagation delays (due to environment or obstacles) leading to clock synchronisation inaccuracies.
- Limited Scalability: In large networks, the sender's signal might not reach all nodes effectively, creating areas with different synchronisation levels.

What are the advantages and limitations of the RBS (Receiver-Receiver Broadcast Synchronisation) protocol?

Process:

- Nodes broadcast their timestamps periodically.
- Each node receives timestamps from neighbours and estimates propagation delays.
- Nodes calculate clock offsets based on received timestamps and delays.
- Nodes adjust their clocks to minimise the overall time difference with neighbours.

Advantages:

- Scalability and Distributed Nature:
    - No single leader - all nodes participate by broadcasting timestamps.
    - Eliminates single point of failure and scales well for large networks.
- Fault Tolerance:
    - Distributed nature allows remaining nodes to function even with some failures.
    - Mitigates impact of individual node malfunctions on overall timing.

Limitations:

- Increased Message Overhead:
    - Frequent timestamp broadcasts lead to higher communication overhead.
    - Can drain battery life and strain bandwidth in resource-constrained WSNs.
- Vulnerability to Byzantine Failures:
    - RBS relies on "majority vote" of timestamps to estimate clock skews.
    - Malicious nodes can disrupt synchronisation by broadcasting inaccurate timestamps.
    - This can lead to inaccurate timing information throughout the network and compromise applications relying on synchronised data.
- Accuracy:
- RBS offers scalability and fault tolerance, but accuracy can be affected by:
- Varying message propagation delays.
- Presence of malicious nodes.

How do clock skews and drifts affect time synchronisation in WSNs?

Time synchronisation is crucial for WSNs, but achieving it perfectly is difficult due to inherent timing variations in sensor nodes. Here's a breakdown of these challenges:

1. The Imprecision:

- Clock Skew: The initial difference between the rates of two clocks. Imagine two clocks starting together, but one runs slightly faster/slower. This initial difference is the skew.
- Clock Drift: The gradual change in a clock's rate over time. Even if initially synchronised, clocks might drift apart due to factors like temperature, ageing, or power fluctuations.

2. Synchronisation Challenges:

These timing discrepancies can significantly impact WSNs:

- Inaccurate Time Estimates: Nodes with different times due to skews/drifts might collect data at misaligned moments, leading to inaccurate overall network insights.
- Disrupted Communication: Some synchronisation protocols rely on precise timing for communication. Skews/drifts can disrupt these interactions, causing data loss or communication failures.
- Reduced Network Efficiency: Ineffective synchronisation due to clock discrepancies can waste resources. Nodes might spend extra time clarifying timestamps or retransmitting lost data.

3. Mitigating the Impact:

- Time synchronisation protocols address these challenges:
- Offset Calculation: Protocols estimate the clock skew and drift between nodes during synchronisation. This information is used to adjust timestamps, accounting for individual timing discrepancies.
- Periodic Resynchronization: Since drifts are continuous, protocols often employ periodic resynchronization to readjust timestamps and minimise the cumulative effect of drifts over time.
- Error Correction Mechanisms: Advanced protocols might incorporate error correction algorithms to further refine synchronisation and compensate for inaccuracies caused by skews and drifts.

What are some advanced techniques for time synchronisation in WSNs?

- Clustering:
  - Challenge: Flooding messages in large WSNs wastes energy.
  - Solution: Group nodes into clusters with cluster heads managing synchronization within each cluster, reducing message overhead and improving scalability.
- Adaptive Algorithms:
  - Challenge: Static protocols might not adapt well to changing network conditions, leading to inaccuracies.
  - Solution: Algorithms adjust behavior based on real-time network conditions (density, environment) to optimize synchronization (e.g., message frequency, message size, partner selection).
- Message Aggregation:
  - Challenge: Balancing accuracy (frequent messages) and energy efficiency (fewer messages). Separate data and synchronization messages add to traffic.
  - Solution: Combine synchronization information with sensor data packets, reducing overall messages and improving efficiency.

How can security vulnerabilities be addressed in time synchronization protocols?

1. Authentication and Encryption:

- Authentication (e.g., message codes or digital signatures):
- Verify message origin and legitimacy.
- Prevent unauthorised entities from injecting false timing information or impersonating nodes.
- Encryption:
- Protects confidentiality of timing information.
- Even if attackers intercept messages, they cannot decipher the actual timing data.

2. Byzantine Fault Tolerance (BFT):

- Traditional protocols are vulnerable to malicious nodes providing inaccurate timing.
- BFT protocols tolerate such behaviour:
- Ensure accurate synchronisation even with a limited number of Byzantine faults (nodes exhibiting arbitrary behaviour).
- Trade-off: Increased complexity and communication overhead.

3. Reputation Systems:

- Identify and isolate potentially malicious nodes:
- Monitor node behaviour over time.
- Assign reputation scores based on adherence to protocols and communication patterns.
- Flag nodes with suspicious behaviour and exclude them from synchronisation.

4. Secure Key Management:

- Crucial for authentication and encryption effectiveness:
- Secure communication channels for key distribution.
- Robust key generation algorithms.
- Secure key storage mechanisms.

What are the trade-offs between accuracy, energy consumption, and scalability in time synchronization protocols?

Accuracy vs. Energy Consumption:

- High Accuracy: More frequent communication for faster drift correction, but drains battery life.
- Low Energy Consumption: Less communication saves energy, but reduces accuracy due to slower drift response.

Scalability vs. Accuracy:

- Centralized Approach: Excellent scalability for large networks, but accuracy might suffer due to delays from the central server.
- Distributed Approach: More accurate (avoids delays), but scalability challenges in very large networks due to communication overhead.

Trade-off Considerations:

- Application Sensitivity: Accuracy might be crucial for timing-critical applications, even if it costs more energy.
- Network Size: Scalability matters for large deployments; choose protocols that handle many nodes efficiently.

How does time synchronisation in WSNs differ from traditional synchronisation in wired networks?

Factor	Wired Networks	WSNs
Resource Constraints	Reliable power, complex algorithms, more communication for synchronisation	Battery-powered, lightweight protocols, minimal communication to conserve energy
Network Topology	Fixed, well-defined topology, easy to establish hierarchies and propagate timing information	Dynamic topologies (failures, mobility, environment changes), adaptive protocols needed for accurate timing
Clock Skew	Smaller, predictable clock skews due to controlled environment and well-maintained connections	Larger, unpredictable clock skews due to temperature, humidity, and hardware limitations. Protocols need to handle these effectively.
Centralization	Network Time Protocol (NTP) - centralised server approach	Centralised approach less feasible due to resource constraints and dynamic topologies. Distributed protocols (nodes collaborate) are more common.
Security	Security addressed through centralised management and access control	More vulnerable due to remote deployments. Protocols need security measures to prevent unauthorised access or manipulation of time information.

What future trends are expected in time synchronisation for WSNs?

- Leveraging Emerging Technologies:

    - RFID tags for synchronisation without extra messages.
    - Visible Light Communication (VLC) for potentially faster and more reliable synchronisation.
- Enhanced Security Mechanisms:
    - Lightweight cryptography for secure synchronisation without compromising energy efficiency.
    - Post-quantum cryptography for long-term security against evolving threats.
- Self-Healing and Self-Organising Protocols:
    - Adaptive synchronisation for maintaining accuracy despite network changes.
    - Distributed fault tolerance for improved network robustness.
- Machine Learning and Artificial Intelligence Integration:
    - Machine learning for proactive anomaly detection in synchronisation.
    - AI for optimising synchronisation parameters based on real-time network conditions.
- Focus on Energy Efficiency:
    - Low-power communication protocols for extended network lifespan.
    - Duty-cycling and sleep modes for reduced energy consumption while maintaining synchronisation accuracy.

What are the key properties of effective localization and positioning procedures in WSNs?

- Accuracy:
    - Provide precise location estimates.
    - Minimise errors from noise, environment, and hardware.
- Scalability:
    - Handle large networks efficiently.
    - Minimise communication overhead for managing large deployments.
- Energy-Efficiency:
    - Conserve battery life by:
    - Reducing message transmissions.
    - Leveraging localised processing.
    - Utilising duty cycling (sleep modes).
- Robustness:
    - Function reliably in various environments:
    - Resist noise and interference.
    - Adapt to environmental changes.
- Security:
    - Protect sensitive location information:
    - Use secure communication protocols.
    - Implement access control mechanisms.

What are the different approaches for localization and positioning in WSNs?

Various approaches are used for localization and positioning:

- Range-based: Measures distances between nodes using techniques like Received Signal Strength (RSSI) or Time of Arrival (TOA).
- Range-free: Estimates location based on connectivity information or hop count from reference nodes.
- Angle-based: Uses directional information from antennas to estimate the direction of arrival of signals.
- Collaborative: Nodes share location information with each other to improve individual estimates.

Explain the principle behind single-hop localization.

- Core Principles:
- Anchor Deployment:

    - Place reference nodes (anchors) with known locations strategically throughout the area.
    - Number and placement impact accuracy and coverage.
    - Ideally: Even distribution, minimise blind spots.
- Distance/Direction Measurement:
    - Measure distance or direction between target node and anchors.
    - Techniques:
        - Received Signal Strength (RSSI) - Signal strength weakens with distance (affected by environment).
        - Time of Arrival (TOA) - Requires precise time synchronisation (challenging).
        - Angle of Arrival (AOA) - Uses directional antennas for improved accuracy (requires specialised hardware).
- Position Estimation:
    - Estimate target node position based on measurements from anchors.
    - Methods:
        - Trilateration (3+ non-collinear anchors, distance measurements).
        - Triangulation (2+ anchors with known locations, angle measurements).
- Advantages:
    - Simplicity: Direct communication simplifies calculations.
    - Accuracy: High accuracy with reliable communication and minimal interference.
    - Computational Efficiency: Less processing power required compared to multi-hop.
- Limitations:
    - Limited Scalability: Deploying and maintaining anchors can be challenging and costly in large/complex environments.
    - Line of Sight Dependency: Techniques like TOA and AOA require clear line of sight (obstacles can affect accuracy).
    - Vulnerability to Anchor Failures: Failure or compromise of a reference point disrupts localization for nearby nodes (creates blind spots).

Multi Hop localisation

- Core Principles:
- Collaborative Ranging:
    - Unlike single-hop, nodes estimate distances to unknown locations by relaying signals through neighbouring nodes.
    - Nodes rely on messages containing distance estimates or signal hop counts to build a network-wide map of relative positions.
- Multi-hop Communication:
    - Information exchange occurs through multiple hops between nodes, eventually reaching nodes without a direct line of sight to reference points.
    - Routing protocols are crucial for efficient message forwarding and minimizing communication overhead.
- Position Calculation:
    - Various algorithms process the collected distance estimates or hop counts to compute the location of unknown nodes.
    - Common techniques include:
        - DV-Hop: Estimates actual distances based on the number of hops a signal traverses.
        - Centroid: Calculates the average position of neighboring nodes with known locations.
        - Multilateration: Uses distance estimates from multiple neighbors (like single-hop, but leverages relayed information).
- Advantages:
    - Scalability: Well-suited for large deployments as it doesn't require extensive

    anchor placement.
    - Coverage: Can provide location information for nodes even in areas without direct access to reference points.
    - Flexibility: Less reliant on precise anchor locations compared to single-hop.
- Limitations:
    - Lower Accuracy: Position estimates are based on accumulated errors from multiple hops, potentially leading to less precise results compared to single-hop.
    - Communication Overhead: Multi-hop communication can generate more message traffic compared to single-hop, impacting energy consumption.
    - Computational Complexity: Processing hop count data or distance estimates from multiple neighbours can require more processing power on nodes.

Feature	Single-Hop Localization	Multi-Hop Localization
Reference Points	Requires anchor deployment	Leverages existing network
Scalability	Limited	Well-suited for large deployments
Coverage	Limited (line of sight)	Provides coverage in blind spots
Accuracy	Potentially higher	Lower due to accumulated errors
Communication	Lower overhead	Higher overhead due to multi-hop
Processing	Less demanding	More demanding algorithms

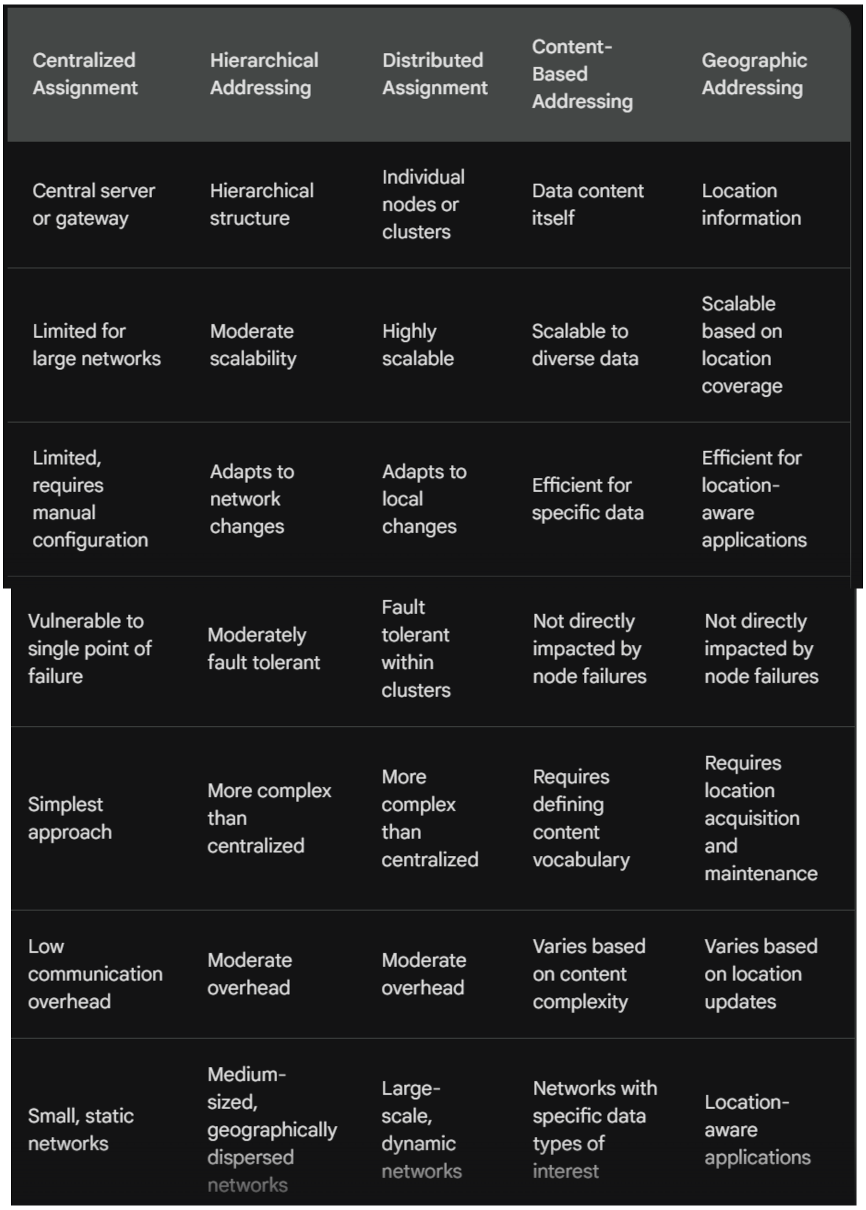
Line of Sight	Often critical	Less reliant
Anchor Failure	Disruptive to nearby nodes	Network can reroute

What are the challenges and limitations of localization and positioning in WSNs?

- Hardware Limitations:
    - Limited range restricts area for accurate positioning.
    - Inaccuracy due to imperfect hardware, signal limitations, and noise.
- Environmental Factors:
    - Obstacles disrupt signal propagation, causing positioning errors.
    - Signal fading due to multipath and atmospheric effects reduces accuracy.
    - Background noise interferes with signals, affecting precision.
- Computational Complexity:
    - Resource constraints limit use of complex algorithms.
    - High energy consumption reduces network lifespan.
    - Increased latency can impact real-time applications.
- Security Concerns:
    - Vulnerable to attacks like spoofing or jamming, disrupting operations.
    - Privacy concerns necessitate robust security mechanisms.
- Scalability Challenges:
    - Network size increases complexity of managing accurate localization.
    - Heterogeneity requires adaptable algorithms for diverse node capabilities.

Discuss the potential challenges associated with implementing content-based

- Standardisation:
    - Defining a universal vocabulary for diverse data is difficult.
    - Maintaining consistency with evolving data types and features is complex.
    - Handling dynamic content characteristics requires flexible mechanisms.
- Scalability:
    - Managing CBA schemes in large networks can be resource-intensive.
    - Efficient routing for content-based queries becomes complex in large/dynamic networks.
    - A vast vocabulary size can lead to search inefficiencies.
- Security:
    - Exposing content in addressing raises privacy concerns (needs anonymization/encryption).
    - Malicious manipulation of content descriptions can disrupt operations (needs integrity/authenticity checks).
    - Security measures can add overhead impacting resource-constrained nodes.



Centralized Assignment	Hierarchical Addressing	Distributed Assignment	Content-Based Addressing	Geographic Addressing
Central server or gateway	Hierarchical structure	Individual nodes or clusters	Data content itself	Location information
Limited for large networks	Moderate scalability	Highly scalable	Scalable to diverse data	Scalable based on location coverage
Limited, requires manual configuration	Adapts to network changes	Adapts to local changes	Efficient for specific data	Efficient for location-aware applications
Vulnerable to single point of failure	Moderately fault tolerant	Fault tolerant within clusters	Not directly impacted by node failures	Not directly impacted by node failures
Simplest approach	More complex than centralized	More complex than centralized	Requires defining content vocabulary	Requires location acquisition and maintenance
Low communication overhead	Moderate overhead	Moderate overhead	Varies based on content complexity	Varies based on location updates
Small, static networks	Medium-sized, geographically dispersed networks	Large-scale, dynamic networks	Networks with specific data types of interest	Location-aware applications

Unit 4

Write a note on signal propagation.

Signal Propagation Basics:
Imagine throwing a pebble into a still pond. The ripples emanating outwards represent how signals propagate – they travel outward from a source (transmitter) through a medium (like air or water) until they reach a receiver. In ideal conditions (like free space), radio waves travel in straight lines similar to light.

The Impact of Distance:

The strength of a received signal weakens as the distance (d) between the transmitter and receiver increases. This can be understood by the $1/d^2$ rule: The received power is inversely proportional to the square of the distance. Simply put, doubling the distance reduces the received power by a factor of four.

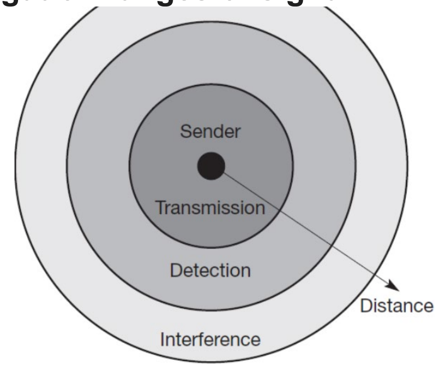
Real-World Effects:

Unlike the perfect scenario, radio waves in real environments encounter various obstacles and conditions that influence their propagation:

- Fading: Signal strength can fluctuate due to factors like frequency and multipath propagation (where the signal travels along multiple paths). This can lead to an uneven signal strength at the receiver.

- Shadowing: Large objects like buildings can block the signal path entirely, creating areas with no signal reception (shadow zones).
- Reflection: Signals can bounce off large surfaces like walls or mountains. While reflection can sometimes be helpful to extend coverage, it can also cause unwanted signal delays or create multiple versions of the signal arriving at the receiver (multipath).
- Refraction: When a signal travels through mediums with different densities (like air and water), it can bend slightly. This phenomenon is similar to how light bends when it enters water.
- Scattering: Small objects can scatter the signal in various directions, weakening its overall strength but still allowing some signal to reach the receiver.
- Diffraction: Radio waves can bend slightly around edges of objects, allowing some signal to reach areas that would otherwise be in a shadow zone.

What are different propagation ranges of signal?

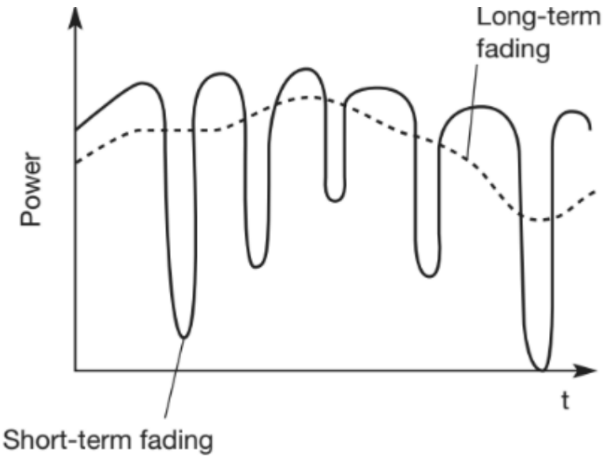


- Transmission range: Within a certain radius of the sender transmission is possible i.e A receiver receives the signals with an error rate low enough to be able to communicate and can also act as sender.
- Detection range: Within a second radius, detection of the transmission is possible, i.eThe transmitted power is large enough to differ from background noise. However, the error rate is too high to establish communication.
- Interference range: Within a third even larger radius, the sender may interfere with other transmission by adding to the background noise. A receiver will not be able to detect the signals, but the signals may disturb other signals

What is multipath propagation and how does it affect mobility?

Multipath Mayhem:

- Signal travels along multiple paths (reflection, refraction, scattering).
- Paths have different lengths, causing signals to arrive at the receiver at slightly different times (delay spread).
- This smears out short pulses and overlaps data symbols (ISI), leading to errors.
- Faster data rates suffer more from ISI due to closer symbols.
- Multipath also causes fading, variations in received signal strength:
- Short-term fading due to movement (rapid power changes).
- Long-term fading due to distance or obstacles (slower power variations).
- Techniques like equalisation and diversity can reduce ISI and fading effects.
- Error correction coding helps recover from errors caused by these issues.



Write a note on Code Division Multiplexing

Code Division Multiplexing (CDM) Explained:

- Relatively new for commercial use: Originally developed for military applications due to its security benefits.
- Sharing the Same Frequency: Unlike other methods, all channels transmit on the same frequency simultaneously.
- Separation by Codes: Each channel has a unique code for identification (like assigned languages in a conversation).
- Security Advantage: Unknown codes appear as background noise, making it difficult to eavesdrop without the "secret code".
- Benefits:
  - Good protection against interference and jamming.
  - Efficient use of code space compared to limited frequency space.
- Drawbacks:
  - Increased receiver complexity due to code separation requirements.
  - Precise power control is necessary for proper operation.

What is spread spectrum technology? What are its advantages and disadvantages?

What is Spread Spectrum?
A transmission technique that spreads the data signal across a wider frequency band than the minimum required.
Advantages:

- Reduced Interference:
- Resists narrowband interference – strong signals on a specific frequency band have less impact.
- Lowers susceptibility to multipath fading – signal variations due to reflections are less disruptive.
- Improved Quality and Security:
- Reduces crosstalk – unwanted signal mixing from nearby transmissions.
- Improves voice quality or data integrity – less static noise and errors.
- Makes the signal appear like background noise, enhancing security as it's difficult to detect without the "key" (spreading code).
- Efficient Sharing:
- Allows multiple users to share the same frequency band without coordination (as long as they use different spreading codes).

Disadvantages:

- Complexity: Requires more complex receivers to "despread" the signal and extract the data.
- Bandwidth Usage: Spreads the signal, potentially interfering with other transmissions if not managed properly.

Write a note on Direct Sequence Spread Spectrum

(**encoding it to 0 and 1 that go faster through a signal then og message/data**)

A transmission technology used in wireless networks.

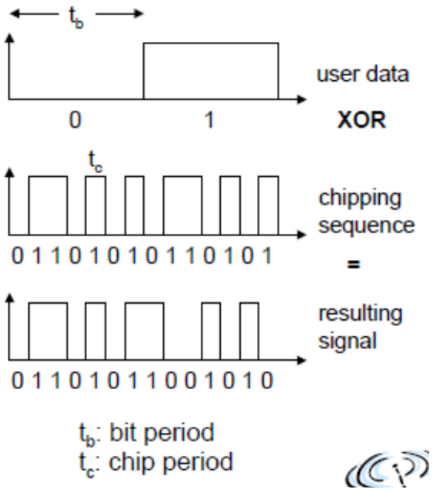
Spreads the data signal over a wider frequency band using a high-speed code (chipping code).

Benefits of DSSS:

- Resists jamming: Makes it harder to disrupt communication by jamming signals.
- Shared channels: Allows multiple users to share the same channel without interference (like using different languages in a conversation).
- Reduced noise: Improves signal quality by reducing background noise.
- Synchronisation: Helps maintain timing between transmitter and receivers.

How Does DSSS Work?

- Data Splitting: The data is divided into small pieces.
- Spreading with a Code: Each data piece is multiplied by a high-speed chipping code, like a secret key.
- Wider Bandwidth: This creates a wider signal spread across the frequency spectrum.
- Transmission: The spread signal is transmitted.
- Despreading at Receiver: The receiver uses the same chipping code to recover the original data.
- Security Aspect:
    - Someone without the chipping code (like not knowing the secret language) would see the signal as noise, making it more secure.



Write a note on Frequency Hopping Spread Spectrum

The FHSS Solution:

- Rapid Frequency Changes: FHSS is like having a walkie-talkie that constantly jumps between different channels according to a secret plan (a pseudo-random sequence) that only you and your teammate know.
- Wide Frequency Band: This "hopping" happens across a wide range of frequencies, making it harder for enemies to jam the signal entirely.

Benefits of FHSS:

- Resistance to Interference: Even if one channel is jammed, the signal simply hops to another, keeping the communication going.
- Security: Since the hopping pattern is secret, it's difficult for eavesdroppers to listen in without knowing the sequence – it's like trying to listen to a conversation that keeps rapidly changing channels!
- Multiple Users: With different hopping sequences, multiple users can share the same frequency band without interfering with each other (like having multiple spy conversations happening at once on different "channels").

How FHSS Works:

- Frequency Channels: A large area is divided into smaller radio channels, like lanes on a highway.

- Hopping Sequence: You and your teammate agree on a secret sequence that determines the order in which you hop between channels (like a pre-arranged list of channels to switch to).
- Dwell Time: You spend a short time (dwell time) on each channel before hopping to the next one, like briefly stopping on each lane on the highway.
- Synchronization: It's crucial for you and your teammate to be perfectly in sync with the hopping sequence, ensuring you're both on the same channel at the right time to receive messages (like both needing to be on the same lane at the same time to talk).

Types of FHSS:

- Slow Hopping: Changes channels less frequently than the data rate (like taking longer stops on each lane).
- Fast Hopping: Changes channels very quickly, even within a single message (like constantly switching lanes).

Applications of FHSS:

- Military: Used for its anti-jamming and secure communication features.
- Wireless Networks: Used in some early Wi-Fi systems.
- Bluetooth: Older versions of Bluetooth employed FHSS.

Explain the concept of cell structure in mobile communication

Cell structure is the backbone of mobile communication networks, allowing for widespread and efficient coverage. Here's a breakdown:

- Cells and Base Stations:
- The service area is divided into smaller geographic areas called cells.
- Each cell has a base station (like a mini-tower) that acts as a communication hub for mobile devices within its range.
- The base station transmits and receives radio signals with these devices.
- Signal Coverage and Reuse:
- Each base station uses specific radio frequencies, but these frequencies are limited.
- A key concept is frequency reuse. Different, non-adjacent cells can reuse the same frequencies to avoid user interference within close proximity.
- Hexagonal Cells (Idealised Model):
- While cells can be various shapes, the ideal model is a hexagon.
- Hexagons efficiently "tile" an area, minimising wasted space and maximising coverage.

Types of Cells:

- Macrocells: Large cells (several kilometres) for rural or less populated areas.
- Microcells: Smaller cells (hundreds of metres) for urban areas, increasing capacity and signal quality in high-traffic zones.
- Picocells: Even smaller cells (tens of metres) for indoor coverage in buildings.
- Femtocells: Tiny cells (up to 10 metres) for home or office use, often boosting signal within a small area.

Benefits of Cell Structure:

- Scalability: Easy network expansion by adding more base stations.
- Increased Capacity: More users can be accommodated within a given area compared to a single large cell.
- Efficient Spectrum Use: Frequency reuse allows multiple users to share the same radio spectrum without excessive interference.
- Handoff: As a mobile user moves between cells, the call is seamlessly handed off to the new base station, ensuring uninterrupted communication.

What is frequency planning in mobile communication?

Frequency reuse is a crucial concept in mobile communication that allows for efficient use of limited radio spectrum resources. Here's a breakdown of its key aspects:

The Idea:

It's the concept of using the same radio frequencies in different areas (cells) within a network, but with a sufficient distance between those areas to minimise interference.
Benefits:

- Multiple Conversations: Allows for multiple conversations to happen simultaneously within a given service area using the same frequency band.
- Limited Frequencies: Makes efficient use of the limited available radio frequencies.
- Power Control: Limits the power of transmitted signals to minimise interference with neighbouring cells using the same frequency.
- Frequency Reuse Factor: The number of times a frequency can be reused depends on the distance between cells and the acceptable level of interference (typically 10 to 50 frequencies per cell).

Frequency Assignment Strategies:

Fixed Assignment:

- A traditional approach where specific frequencies are permanently assigned to each cell.
- Problem: Doesn't adapt well to varying traffic loads in different cells, potentially leading to wasted capacity if a cell is underused.

Dynamic Assignment:

- A more flexible approach where base stations choose frequencies based on:
- Real-time usage: Frequencies already in use by neighboring cells.
- Traffic load: Assigning more frequencies to cells with higher traffic for increased capacity.
- Interference measurements: Considering actual interference levels to optimize frequency selection.
- Dynamic assignment allows for a more efficient allocation of frequencies, especially in situations with varying traffic loads across different cells.

What are the Performance characteristics of GSM?

Boosting Capacity:

- Frequency Reuse: GSM allows the same frequencies to be used in non-adjacent cells, increasing overall network capacity.
- Time Division Multiple Access (TDMA): This divides frequency channels into timeslots, enabling up to 8 users to share a single channel without interference.

Spectrum Efficiency (Packing More Users):

- GMSK Modulation: This technique offers a reasonable balance, allowing for more users within the limited radio spectrum.
- Limited Bandwidth: Compared to newer technologies using wider bands, GSM's traditional narrow bands limit overall efficiency.

Security Considerations:

- Encryption (A5/1 & A5/2): These ciphers provide some protection against eavesdropping, but have vulnerabilities.
- SIM Authentication: Subscriber Identity Modules (SIM) help prevent unauthorised network access.

Voice Quality:

- Codecs: Original codecs prioritised efficiency (low bitrate) over top audio quality (Full-Rate: 13kbps, Half-Rate: 6.5 kbps).
- Improvements: Enhanced Full Rate (EFR) and Adaptive Multi-Rate (AMR) codecs have enhanced call quality.

Data Rate Limitations:

- Original Design: Primarily focused on voice calls, resulting in limited data speeds (up to 9.6 kbps).
- Enhancements: GPRS and EDGE improved data speeds, but are still significantly

slower than later technologies.

Roaming Advantage:

- International Standard: GSM's widespread adoption allows seamless roaming between compatible networks in many countries.

Limitations to Remember:

- Capacity: Can struggle in high-traffic areas due to limitations.
- Data Rates: Significantly slower than newer technologies (3G, 4G, 5G).
- Security: Encryption vulnerabilities exist.

What are Geostationary satellites?

Geostationary satellites orbit Earth above the equator at an altitude of about 36,000 kilometres (22,369 miles).

Their speed and direction match Earth's rotation, making them appear stationary from our perspective.

Why this special orbit?

- This specific altitude is called the **Clarke Belt.**
- It allows the satellite to stay fixed in the sky, providing continuous coverage of a specific Earth region.

Benefits:

- Broad Coverage: Three geostationary satellites spaced 120 degrees apart can cover nearly the entire Earth's surface (except the poles).
- Simple Antennas: Since the satellite appears fixed, inexpensive directional antennas can be used to communicate with it.
- Long Lifespan: Geostationary satellites typically last 10-15 years.
- Applications: Ideal for telecommunications, television broadcasting, weather monitoring, and more.

Drawbacks:

- Signal Delay: Radio signals take about a quarter-second for a round trip, causing a slight delay in interactive communication like phone calls.
- Limited Polar Coverage: The poles are not covered by geostationary satellites.
- High Cost: Launching and maintaining these satellites can be expensive.
- Large Antennas for Some Areas: Larger antennas may be needed in the northern and southern regions.
- Not ideal for mobile phones: These satellites are not suitable for small mobile devices due to the signal delay.

Comparison with Geosynchronous Orbits:

- Geosynchronous satellites have the same orbital period as Earth's rotation but may not be directly over the equator. They can appear to move slightly in the sky.

What are LEO systems?

Low Earth Orbit (LEO) Satellites Explained:

What are they?

LEO satellites orbit Earth at a relatively low altitude, between 400 and 1,200 miles (644 and 1,931 kilometers) above the surface.

Applications:

Primarily used for data communication like email, video conferencing, and paging.

LEO systems can provide telecommunication services to remote or underdeveloped regions where laying cables is impractical.

Key Features:

- High Speed: LEO satellites move very fast and are not stationary in the sky.
- Shorter Signal Path: Due to the lower altitude, data transmission experiences less delay compared to higher orbits.
- Handoff Required: As LEO satellites move out of range, data needs to be "handed off" to other satellites in the network.
- Lower Power Transmission: Ground stations require less power to transmit signals to

LEO satellites compared to those in higher orbits.

Advantages:

- Low Transmission Power: Requires less powerful antennas at ground stations.
- Low Latency: Offers lower signal delay compared to higher orbits.
- Smaller Coverage: Useful for providing services to specific regions.

Disadvantages:

- Large Constellation Needed: Requires a large number of satellites (50-200) for global coverage.
- Complex Handoff: Necessary to seamlessly transfer data between moving satellites.
- Shorter Lifespan: LEO satellites typically have a lifespan of 5-8 years, requiring frequent replacements.
- Packet Routing: Data packets need to be routed between satellites within the network.

What are MEO systems?

MEO satellites orbit Earth at an altitude between LEO (Low Earth Orbit) and GEO (Geostationary Orbit), ranging from a few hundred to a few thousand miles (up to 12,000 kilometers) above the surface.

Orbital Characteristics:

Orbital Period: 2 to 12 hours, depending on altitude.

Orbit Shapes:

- Circular: Constant altitude and speed.
- Elliptical: Varies in altitude (perigee - lowest, apogee - highest) and speed.
- Elliptical Orbits: Easier to access near apogee (higher point) due to longer visibility and less frequent antenna adjustments.

Advantages:

- Fewer Satellites Needed: Compared to LEO, a dozen MEO satellites can provide global coverage.
- Simpler Design: MEO systems are generally less complex than LEO systems.
- Fewer Handovers: Data transfer between satellites is less frequent than in LEO constellations.

Disadvantages:

- Higher Transmission Power: Requires more powerful ground stations compared to LEO.
- Special Antennas: MEO systems might require specialized antennas for communication.

Applications:

- MEO satellites are used for various applications including:
- Global navigation systems (GPS, GLONASS)
- Mobile communication
- Satellite internet

What are different types of handover in satellite systems?

Satellite networks, especially those with Low Earth Orbit (LEO) satellites, face unique challenges due to the constant movement of satellites. Handovers are crucial to maintain seamless communication during these changes. Here's a breakdown of the different types:

Link-Layer Handover (Focusing on LEO Systems):

- Deals with changing connections due to satellite movement.
- Subtypes based on the connection being switched:
- Spotbeam Handover (Intra-satellite): User moves between coverage areas (spotbeams) within a single satellite (frequent, every 1-2 minutes).
- Satellite Handover (Intersatellite): User moves out of one satellite's coverage zone and connects to another (less frequent).
- ISL Handover: Connection reroutes due to temporary unavailability of links between neighboring satellites (ISL = Inter-Satellite Link).

Network-Layer Handover (Maintaining Connections):

- Handles changes in IP addresses due to user or satellite movement.
- Ensures higher-level protocols (TCP, UDP) maintain connections during handover.
- Three handover schemes:
- Hard Handover: Releases the current connection before establishing a new one (brief service interruption).
- Soft Handover: Maintains both old and new connections until the new one is stable (smoother transition).
- Signaling-Diversity: Similar to soft handover, but user data continues through the old link while signaling uses both links.

Additional Handover Situations in Satellite Networks (Compared to Terrestrial):

- Intra-Satellite Handover: Switching between spotbeams within a single satellite.
- Inter-Satellite Handover: Moving from one satellite's coverage zone to another's.
- Gateway Handover: Switching to a different gateway station while remaining connected to the same satellite.
- Inter-System Handover: Transitioning from the satellite network to a terrestrial cellular network (when available, potentially cheaper or lower latency).

Explain Hard handover in Mobile communication

Hard handover, also known as break-before-make handover, is a technique for transferring a call or data session between base stations in mobile networks when a user moves between coverage areas.

How it works:

- Signal Degradation: As a user moves away from a base station, the signal weakens, affecting call quality.
- Monitoring: The user's phone (mobile station) constantly checks signal strength from nearby base stations.
- Handover Decision: When the current signal falls below a threshold and a stronger signal from another base station is available, a handover is initiated.
- Channel Release: The phone disconnects from the current channel on the serving base station.
- New Channel Acquisition: The phone establishes a new connection with the target base station on a new channel.
- Resumption of Communication: Once connected to the target station, communication resumes.

Key characteristics:

- Break-before-Make: The connection with the old base station is broken before a new one is established, causing a brief interruption (milliseconds).
- Suitable Technologies: Commonly used with TDMA and FDMA networks where users have dedicated channels.
- Simplicity: Relatively easy to implement from a network management perspective.
- Drawback: The interruption can be noticeable, especially for voice calls.

Explain Soft handover in Mobile Communication

Process:

- Similar to hard handover, signal weakens from serving station.
- Network initiates handover upon finding a stronger neighbouring signal. Key Difference: Mobile station connects to the target station WHILE maintaining the connection with the serving station (dual connectivity).
- Network combines data from both stations (if compatible) or selects the stronger signal.
- Connection with serving station gradually weakens.
- Mobile station relies solely on the target station.

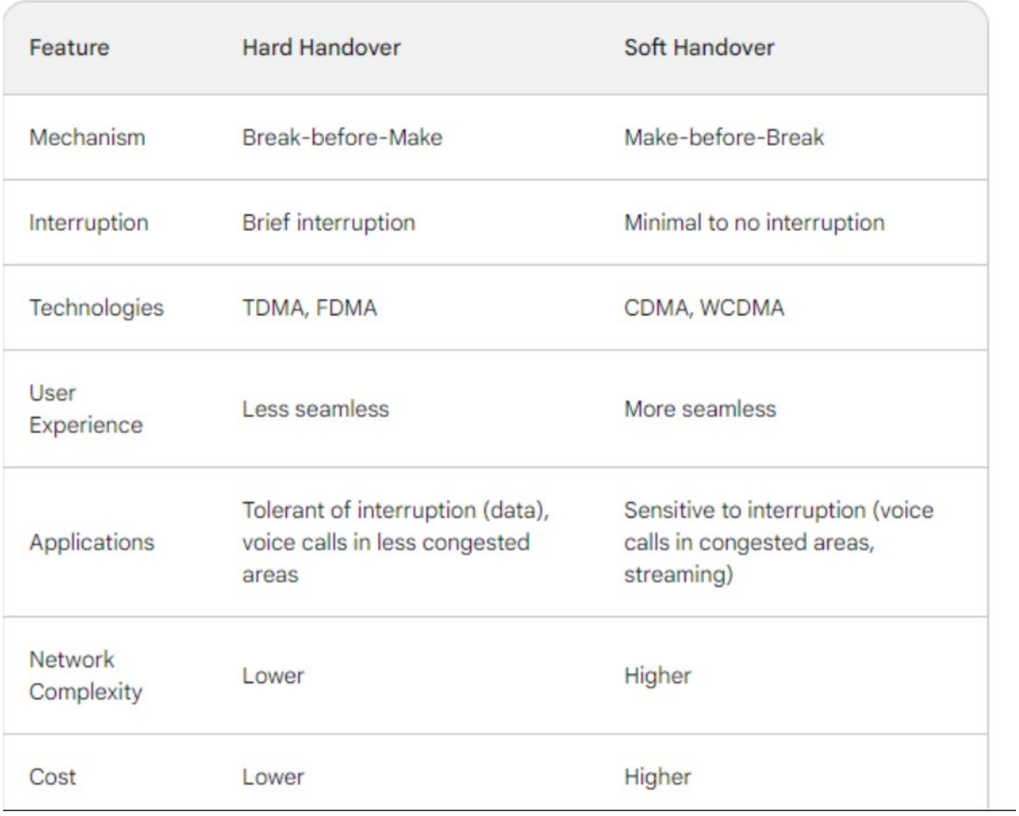
Pros:

- Minimises or eliminates communication interruptions.
- Improved performance for delay-sensitive applications (voice calls, streaming).
- Suitable for CDMA/WCDMA networks without dedicated channels.
- Potentially better network resource utilisation (combining signals).

- Enhanced user experience (seamless connection).

Cons:

- Increased network complexity (infrastructure, handover management).
- Higher cost to implement and maintain.



Feature	Hard Handover	Soft Handover
Mechanism	Break-before-Make	Make-before-Break
Interruption	Brief interruption	Minimal to no interruption
Technologies	TDMA, FDMA	CDMA, WCDMA
User Experience	Less seamless	More seamless
Applications	Tolerant of interruption (data), voice calls in less congested areas	Sensitive to interruption (voice calls in congested areas, streaming)
Network Complexity	Lower	Higher
Cost	Lower	Higher

GEO vs. LEO vs. MEO Satellite Systems

Feature	GEO (Geostationary Orbit)	MEO (Medium Earth Orbit)	LEO (Low Earth Orbit)
Orbit	36,000 km above equator	Few hundred to few thousand km above Earth	400-1,200 km above Earth's surface
Position	Fixed relative to Earth (appears stationary)	Varies (circular or elliptical)	Moves across the sky

Coverage	Large (can cover nearly entire Earth with 3 satellites)	Moderate (requires fewer than LEO for global coverage)	Smaller (requires more satellites for global coverage)
Signal Delay	Higher (round trip signal takes about 0.25 seconds)	Moderate (between GEO and LEO)	Lower (faster signal travel time)
Complexity	Less complex (simpler antenna requirements)	Moderate (may require special antennas)	More complex (need for handover between satellites)
Applications	Broadcasting, television, weather monitoring	Navigation (GPS), mobile communication, satellite internet	Data communication (email, internet access)
Number of Satellites	Fewer satellites needed for global coverage	Dozen or so satellites for global coverage	More satellites needed for global coverage
Cost	Generally higher launch and maintenance costs	Moderate launch and maintenance costs	Lower launch costs, but may require more frequent satellite replacements

Latency	Higher latency (less ideal for real-time applications)	Moderate latency (better than GEO for real-time)	Lower latency (better for real-time communication)