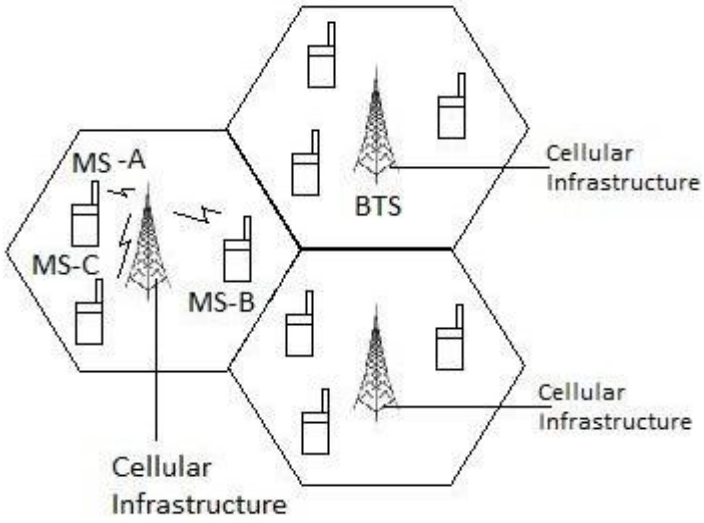
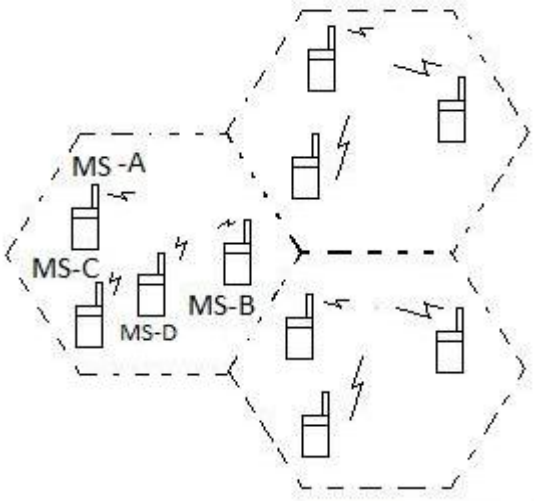
**What is Cellular and Ad Hoc wireless networks?**




Cellular Network




Ad Hoc Network

**1. Cellular Wireless Network:** A Cellular Network is an infrastructure-based wireless communication system where mobile devices (Mobile Stations or MS) communicate through Base Transceiver Stations (BTS). The network is divided into multiple hexagonal cells, and each cell is served by a BTS •All communication goes through the BTS, even if the devices are close to each other. **Key Features:** •Requires a fixed infrastructure (BTS, switching centres). •Centralized control and resource management. •Supports wide coverage, mobility, and handoffs between cells. •Suitable for large-scale communication like mobile telephony and mobile internet. •**Example:** GSM, CDMA, LTE, and 5G networks. **2. Ad Hoc Wireless Network:** An Ad Hoc Network is a decentralized wireless network where mobile devices communicate directly with each other without any pre-existing infrastructure. Each device in the network acts as both a host and a router, forwarding data for other devices. •**Key Features:** •No need for infrastructure like BTS or access points. •Each node is responsible for routing and network configuration. •Highly flexible and can be deployed quickly. •Best suited for temporary, emergency, or military communications. •**Example:** MANETs (Mobile Ad Hoc Networks), VANETs (Vehicular Ad Hoc Networks), and sensor networks.

---

**What are MAC protocols in Ad Hoc wireless networks?**

Medium Access Control (MAC) protocols in ad hoc wireless networks are responsible for coordinating access to the shared communication medium. Unlike traditional networks with centralized infrastructure (like base stations), ad hoc networks rely on distributed and self-organizing mechanisms for communication, making MAC protocols crucial for performance, reliability, and efficiency. **Key Functions of MAC Protocols:** 1. **Channel Access Coordination**: Ensure that multiple nodes can transmit data without collisions. **2. Collision Avoidance**: Implement strategies to minimize packet collisions. **3. Efficient Bandwidth Utilization**: Share the wireless channel effectively among all nodes. **4. Energy Efficiency**: Minimize energy consumption to extend the lifetime of battery-powered nodes. **5. Scalability**: Handle dynamic changes in the network topology. **Types of MAC Protocols: 1. Contention-Based MAC Protocols:** •Nodes compete for the channel. •**Example**: IEEE 802.11 (Wi-Fi) with CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). **2. Contention-Free MAC Protocols:** •Use mechanisms like Time Division Multiple Access (TDMA) or Frequency Division. •Nodes are scheduled to transmit in assigned time slots or frequencies. **3. Hybrid MAC Protocols:** •Combine contention and contention-free techniques. •**Example**: Z-MAC (Zebra MAC) switches between CSMA and TDMA based on traffic. **Examples of MAC Protocols in Ad Hoc Networks: 1. MACA (Multiple Access with Collision Avoidance):** Uses RTS/CTS handshake to avoid collisions. **2. MACAW (MACA for Wireless):** Enhances MACA with ACK, DS, and RRTS messages for improved performance. **3. IEEE 802.11 DCF (Distributed Coordination Function):** Implements CSMA/CA and is widely used in ad hoc modes. **Challenges in Ad Hoc MAC Design:** •Hidden Terminal Problem •Exposed Terminal Problem •Dynamic Topology •Lack of Centralized Control.

**Describe Design goals of MAC protocol.**

MAC (Medium Access Control) protocols in ad hoc wireless networks must be designed to handle the unique challenges of decentralized and infrastructure-less communication. The following are the key design goals: **1. Fair and Equitable Medium Access:** •Ensure all nodes have equal opportunity to access the shared channel. •Prevent scenarios where some nodes monopolize the medium or others get starved. •Promotes balanced communication among all network participants. **2. Efficient Bandwidth Utilization:** •Maximize the use of available bandwidth by reducing idle time and collisions. •Minimize control overhead and optimize data transmission. •Ensures high throughput and better performance. **3. Low Latency and Delay Sensitivity** •Reduce the time taken for data to be transmitted after a node requests access. •Important for real-time applications like video calls or emergency alerts. •Helps maintain quality of service in time-sensitive communications. **4. Energy Efficiency:** •Conserve battery power by minimizing unnecessary transmissions and idle listening. •Use sleep modes and efficient scheduling to extend node and network lifetime. •Critical for battery-powered devices in mobile ad hoc networks. **5. Scalability:** •Perform efficiently regardless of the number of nodes in the network. •Handle increased traffic and node density without degrading performance. •Supports both small and large-scale ad hoc deployments. **6. Adaptability to Changing Topology:** •Quickly respond to changes caused by node mobility or failure. •Maintain stable communication even with dynamic and unpredictable topology. •Essential for mobile and fast-changing network environments. **7. Collision Avoidance and Reliable Transmission:** •Minimize data collisions using techniques like RTS/CTS and backoff algorithms. •Ensure data is transmitted and received correctly through acknowledgments and retransmissions. •Improves reliability and reduces retransmission overhead.

| Cellular Wireless Network | Ad Hoc Wireless Network |
|---|---|
| Requires fixed infrastructure like base stations and towers. | Does not require any fixed infrastructure; nodes communicate directly. |
| Centralized control is used to manage communication. | Distributed control; each node acts as both a host and a router. |
| Nodes (users) connect through base stations or access points. | Nodes communicate directly or through multi-hop routing. |
| Designed for large-scale, wide-area coverage. | Typically used for smaller, localized or temporary networks. |
| Better scalability and support for high mobility with seamless handoffs. | Limited scalability and more affected by mobility due to frequent topology changes. |
| Power consumption is less of a concern for base stations. | Energy efficiency is critical since nodes are usually battery-powered. |
| Examples: GSM, LTE, 5G networks. | Examples: Military networks, disaster recovery, sensor networks. |
| Setup and maintenance cost is high due to infrastructure. | Setup cost is low as no fixed infrastructure is required. |
| More secure and controlled due to centralized management. | More vulnerable to security threats due to decentralized nature. |

**Issues in Ad Hoc wireless networks.**

Ad hoc wireless networks, while flexible and infrastructure-less, face several critical issues due to their decentralized and dynamic nature. **Issues in Ad Hoc Wireless Networks: 1. Dynamic Topology**: •Nodes in ad hoc networks are mobile and frequently change their positions, causing the network topology to change rapidly and unpredictably. •Such frequent changes cause link breakages, requiring constant route rediscovery and updates to maintain communication paths. **2. Limited Bandwidth:** •Wireless communication channels inherently provide less bandwidth compared to wired networks,

restricting the amount of data that can be transmitted simultaneously. •Since the wireless medium is shared by all nodes, multiple simultaneous transmissions can cause congestion and collisions, further reducing effective bandwidth. **3. Energy Constraints:** •Nodes in ad hoc networks are typically battery-operated devices, which means energy is a scarce resource. •Frequent transmissions, receptions, and protocol overhead like routing updates consume significant energy, leading to faster depletion of battery power. **4. Security Vulnerabilities** •Due to the absence of centralized infrastructure, ad hoc networks are more exposed to security threats such as eavesdropping, data tampering, spoofing, and denial-of-service (DoS) attacks. •The open wireless medium allows attackers to easily intercept or disrupt communication, posing a risk to data confidentiality and network integrity. **5. Scalability Challenges:** •As the number of nodes in an ad hoc network increase, the complexity of managing routes and communication rises exponentially. •High node density results in increased collisions and interference, causing network performance to degrade. **6. Hidden and Exposed Terminal Problems**: •The hidden terminal problem occurs when two nodes, which are out of each other's transmission range, attempt to send data to a common receiver simultaneously, causing collisions. •The exposed terminal problem arises when a node refrains from transmitting because it senses the channel busy, even though its transmission would not cause interference. **7. Quality of Service (QoS) Maintenance:** •Maintaining consistent QoS in ad hoc networks is difficult due to variable link quality, node mobility, and fluctuating network loads. •Delay-sensitive applications like video streaming and VoIP require guarantees on bandwidth, delay, and jitter, which are hard to ensure.

---

**Which are the types of different Ad Hoc wireless networks?**

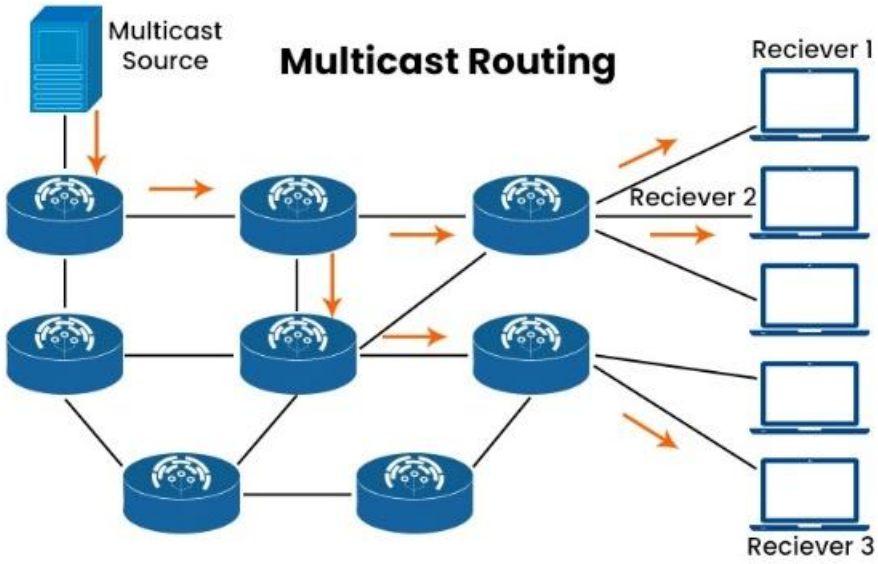
Ad Hoc wireless networks are self-configuring, infrastructure-less networks where nodes communicate directly without relying on any centralized access point or fixed infrastructure. These networks are highly flexible and suitable for scenarios were setting up infrastructure is difficult or impossible. **Types of Different Ad Hoc Wireless Networks: 1. Mobile Ad Hoc Networks (MANETs):** •Consist of mobile nodes that communicate without fixed infrastructure. •Each node acts as both a host and a router. •Used in military, emergency, and temporary event communications. **2. Wireless Sensor Networks (WSNs):** •Made up of small, low-power sensor nodes that monitor environmental data like temperature or humidity. •Nodes send data to a central base station for analysis. •Used in agriculture, health monitoring, and industrial applications. **3. Vehicular Ad Hoc Networks (VANETs):** •Vehicles equipped with communication devices form a network on the move. •Enable vehicle-to-vehicle and vehicle-to-infrastructure communication. •Improve road safety, traffic management, and navigation. **4. Wireless Mesh Networks (WMNs):** •Consist of fixed or mobile nodes connected in a mesh topology. •Nodes forward data for others, creating reliable, extended coverage. •Used for community internet access and smart cities. **5. Internet-based Ad Hoc Networks:** •Connect ad hoc nodes to the internet via gateways. •Allow mobile devices to access global internet services without fixed infrastructure. •Important for IoT and smart device communication. **6. Body Area Networks (BANs):** •Wireless networks formed by sensors placed on or around the human body. •Used for health monitoring and medical data collection. •Nodes communicate vital signs to a local or remote monitoring system. **7. Underwater Wireless Ad Hoc Networks:** •Networks where nodes communicate underwater using acoustic signals. •Used for oceanographic data collection, underwater surveillance, and environmental monitoring. •Face challenges like high latency and limited bandwidth.

---

**What is Operation of multicast routing protocols?**

(((((((((DIAGRAM))))))))) **Operation of Multicast Routing Protocols:** Multicast routing protocols enable efficient data transmission from one or multiple sources to multiple receivers in a network by sending a single copy of data that is distributed to all members of a multicast group. Their operation involves the following key steps: **1. Group Membership Management:** •Nodes interested in receiving multicast data join a multicast group by sending join requests to their local routers. •Protocols like IGMP (Internet Group Management Protocol) help manage group membership at the host-router level. **2. Multicast Tree Construction:** •Routers create a multicast distribution tree that defines the path from the source(s) to all group members. •The tree ensures efficient data forwarding, avoiding duplication of

packets on any link. **3. Types of Multicast Trees: a) Source-based Trees:** A separate tree is built rooted at each source, such as in DVMRP (Distance Vector Multicast Routing Protocol). **b) Shared Trees:** A single shared tree is built for the group with a designated router called the Rendezvous Point (RP), as in Protocol Independent Multicast - Sparse Mode (PIM-SM). **4. Data Forwarding:** •Once the multicast tree is established, the source sends one copy of data to the router. •Routers replicate and forward the data only along the branches where group members exist, conserving bandwidth. **5. Pruning and Grafting:** •Routers prune branches of the tree with no group members to stop unnecessary data transmission. •If a new receiver joins, routers graft branches back to the tree to include the new member. **6. Handling Multiple Sources:** •Protocols support multiple sources by either building separate trees for each or using shared trees that handle multiple senders efficiently. **7. Reliability and Maintenance:** •Multicast routing protocols maintain the tree dynamically as members join or leave. •They handle topology changes by updating routing information to ensure continuous delivery.




**What are issues in design a multicast routing protocol?**

Designing an efficient multicast routing protocol involves addressing several challenges to ensure reliable, scalable, and efficient data delivery. The main issues include **Issues in Designing a Multicast Routing Protocol: 1. Efficient Tree Construction:** •The multicast routing protocol must construct a distribution tree that efficiently connects all group members. •It should minimize redundant transmissions to save bandwidth and reduce network congestion. •Choosing between source-based trees and shared trees impacts complexity and scalability. **2. Scalability:** •The protocol must handle large numbers of multicast groups and receivers without overwhelming routers. •Maintaining routing information for many groups increases memory and processing overhead. •Protocol design should allow growth without performance degradation. **3. Dynamic Membership Management:** •Group members frequently join and leave multicast groups, requiring constant updates. •The protocol must quickly propagate join and leave messages to maintain accurate membership. •Delays or failures in updates can cause data loss or unnecessary data transmission. **4. Loop Prevention:** •Multicast packets must not circulate endlessly in the network, which wastes resources. •Protocols need mechanisms to detect and prevent routing loops in the multicast tree. •Loop prevention helps reduce duplicate packets and avoids network congestion. **5. Robustness to Network Changes:** •Networks can experience node mobility, link failures, or topology changes at any time. •The multicast routing protocol must adapt dynamically to maintain connectivity. •Fast recovery and rerouting mechanisms are necessary to prevent data loss. **6. Support for Multiple Sources** •Many multicast groups have multiple active senders that require data distribution. •The protocol must efficiently manage routing paths for all sources to the group members. •Handling multiple sources should not cause excessive overhead or complexity. **7. Security Concerns:** •Protecting multicast data from unauthorized access is critical, especially for sensitive applications. •The protocol must ensure authentication of group members and data sources.

**Explain classification of routing protocols.**

**Classification of Routing Protocols:** Routing protocols are essential for determining the best path for data packets to travel across a network. They are classified based on various criteria like network structure, routing updates, and route discovery methods. The main classifications are: **1. Based on Network Architecture: •Interior Gateway Protocols (IGPs):** • Used within a single autonomous system (AS), such as a corporate network or ISP domain. Examples include RIP, OSPF, and EIGRP. • IGPs focus on routing efficiency and quick convergence within the AS. • They handle routing between routers that belong to the same administrative domain. **•Exterior Gateway Protocols (EGPs): •** Operate between different autonomous systems, primarily for routing on the internet. • The most common EGP is BGP (Border Gateway Protocol). • EGPs manage policy-based routing and inter-domain connectivity. **2. Based on Routing Update Mechanism: •Distance Vector Routing Protocols: •** Routers share routing tables with neighbors periodically. • Decisions are made based on the number of hops or distance to the destination. • Example: RIP (Routing Information Protocol). They are simple but slower to converge and prone to routing loops. **•Link State Routing Protocols: •** Routers have complete knowledge of the network topology by exchanging link state advertisements. • Each router independently calculates the best path using algorithms like Dijkstra's. • Examples include OSPF and IS-IS, known for faster convergence and scalability. **3. Based on Routing Path: •Static Routing: •** Routes are manually configured and do not change unless manually updated. • Simple to implement but not suitable for large or dynamic networks. • Provides high security and predictability but lacks flexibility. **•Dynamic Routing: •** Routes are automatically discovered and updated based on network topology changes. • Protocols adapt to failures and congestion for better reliability. • Common in large, complex, or frequently changing networks. **•Based on Network Topology Awareness: •Flat Routing Protocols: •** Treat all routers equally without hierarchy. • Suitable for small or medium networks. May suffer scalability issues as network size grows. **•Hierarchical Routing Protocols: •** Divide the network into multiple levels or areas. • Reduces routing table size and controls update traffic. • OSPF and IS-IS use hierarchical routing structures.

---

**Draw and explain architecture reference model for multicast routing protocol.**

((((((((((SAME DIAGRAM)))))))))) **Architecture Reference Model for Multicast Routing Protocol:**

Multicast routing enables efficient delivery of data from one source to multiple receivers without sending multiple copies. The architecture of multicast routing includes several key components that work together to build and maintain a multicast distribution tree.

**Components in the Architecture: 1. Multicast Source:** •The sender of the multicast data (e.g., a server broadcasting a video stream). •Sends a single copy of data to the network. **2. Multicast Routers:** •Special routers capable of forwarding multicast packets. •They use multicast routing protocols like PIM (Protocol Independent Multicast) to construct multicast trees. •They replicate packets only where needed to reach multiple receivers. **3. Distribution Tree:** •A logical tree structure connecting the source to all multicast receivers. •Two types: **Source-Based Tree (SBT):** One tree per source. **Shared Tree:** One common tree for all sources in a group. **4. Receivers (Receiver 1, 2, 3):** •End devices (e.g., computers or TVs) that join a multicast group to receive data. •Use Internet Group Management Protocol (IGMP) to inform routers of their interest. **5. Forwarding Paths:** •Indicated by the arrows in the diagram. •Show the flow of multicast packets from source to receivers through routers. **6. Group Management (via IGMP):** •Hosts send IGMP messages to join or leave a multicast group. •Routers maintain group membership lists based on IGMP. **7. Routing Protocol Support:** •Protocols like PIM-SM (Sparse Mode), DVMRP, and MOSPF build and maintain multicast routing paths. •These protocols help update the multicast forwarding table as receivers join/leave.

**Working:** •When a multicast source starts sending data, it is forwarded by multicast-enabled routers. •Routers use multicast routing protocols to determine the best paths and replicate packets only when necessary. •Receivers express interest in joining a multicast group using IGMP. •The multicast tree dynamically adapts as receivers join or leave the group.

**Explain Sequential Consistency Model.**

Sequential Consistency is a memory consistency model that ensures the execution of a multiprocessor program appears as if all operations from all processors are executed in some sequential order, while preserving the program order of each individual processor. **Key Characteristics: •Preservation of Program Order:** The operations of each processor must appear in the order specified by its program. **•Global Sequential Order:** All operations across all processors must appear to execute in a single total order that is consistent with each processor's program order.

**•For a system to be sequentially consistent:** •The result of any execution must be the same as if all operations were executed in some sequential order. •The order of operations in this sequence must respect the program order of each individual processor.

**Example Scenario-** Consider two processors P1 and P2: •P1 executes: A = 1; print(B) •P2 executes: B = 1; print(A) •Under Sequential Consistency, possible outputs are: • (A=1, B=1) • (A=0, B=1) • (A=1, B=0) •But not (A=0, B=0) because at least one write must appear before the reads.

**Advantages: 1. Simple to Understand:** Easier to reason about program behavior compared to weaker models. **2. Deterministic Execution:** Ensures a consistent view of memory operations across all processors. **Disadvantages: 1. Performance Overhead:** Requires strict ordering, limiting optimizations like out-of-order execution. **2. Not Always Necessary:** Some applications do not need such strong guarantees, making it inefficient. **Applications:** •Used in systems where correctness depends on a predictable order of memory operations. •Common in early multiprocessor systems and some programming languages for concurrent execution. **Challenges in Implementation:** •Requires synchronization mechanisms (e.g., barriers, locks) to maintain order. •Hardware and compiler optimizations must be restricted to preserve sequential consistency.

---

**What are the Issues and challenges in Quality of service?**

Quality of Service (QoS) refers to the ability of a network to provide better service to selected network traffic over various technologies such as the Internet, WAN, or LAN. It ensures reliable performance for critical applications such as voice, video, and real-time data. However, implementing and maintaining QoS faces several issues and challenges, which are outlined below: **1. Bandwidth Limitations:** Network resources are finite. High traffic volume or inadequate bandwidth can cause congestion, leading to packet loss, delays, and jitter—significantly affecting QoS-sensitive applications like VoIP and video conferencing. **2. Latency and Jitter:** Latency is the time taken for data to travel from source to destination, while jitter is the variation in packet arrival times. Both are crucial in real-time communications. Maintaining low and consistent latency is a major QoS challenge. **3. Packet Loss:** When network congestion occurs, routers may drop packets. Lost packets in video or voice applications can result in poor user experience, requiring retransmission and buffering, which further increases delay. **4. Scalability:** As networks grow, maintaining consistent QoS becomes difficult. Large-scale networks need complex traffic management mechanisms, which may not scale efficiently. **5. Heterogeneous Networks:** QoS implementation across diverse network types (wired, wireless, satellite, etc.) with different protocols and standards complicates end-to-end QoS assurance. **6. Security vs. QoS Trade-off:** Security mechanisms like encryption add overhead and processing delay, which can conflict with QoS goals, especially in time-sensitive applications. **7. Lack of Standardization:** Different vendors use proprietary QoS mechanisms, making interoperability difficult. Standardized QoS models like IntServ and DiffServ are not uniformly adopted. **8. Dynamic Traffic Patterns:** Network traffic can be unpredictable. QoS mechanisms must adapt in real-time to varying loads, which is technically challenging and resource intensive.

---

**What is key management process?**

Key management is a fundamental component of cryptographic systems that involves the creation, distribution, storage, updating, and destruction of cryptographic keys used to protect data. •Key management is the process of handling cryptographic keys throughout their lifecycle to ensure data confidentiality, integrity, and authenticity in a secure manner. **Steps in Key Management Process: 1. Key Generation:** •Cryptographic keys (symmetric/asymmetric) are created using secure algorithms

and random number generators. •Must ensure high entropy and unpredictability. **2. Key Distribution:** •Securely transmitting keys between parties. •Techniques include key exchange protocols (e.g., Diffie-Hellman), digital envelopes, or using trusted third parties like Key Distribution Centers (KDCs). **3. Key Storage:** •Storing keys in secure hardware (e.g., Hardware Security Modules - HSMs) or software environments. •Preventing unauthorized access is critical. **4. Key Usage:** •Keys are used for encryption, decryption, signing, or verifying data. •Usage must comply with defined policies (e.g., who can use the key and for what purpose). **5. Key Rotation/Renewal:** •Periodically replacing keys to limit the risk of compromise. •Helps maintain cryptographic strength over time. **6. Key Revocation:** •If a key is compromised or no longer needed, it must be revoked. •Revocation lists or certificate revocation mechanisms (in PKI) are used. **7. Key Destruction:** •Securely erasing keys when they are no longer needed. •Prevents future misuse of the key. **Importance of Key Management:** •Ensures the security of encrypted communications. •Supports compliance with security standards (e.g., GDPR, HIPAA). •Prevents unauthorized access and data breaches.

---

**What is the main challenge to implement TCP over adhoc networks?**

TCP is originally designed for wired networks, where packet loss is typically caused by network congestion. Therefore, when TCP detects packet loss (e.g., via timeout or triple duplicate ACKs), it assumes the network is congested and reduces the transmission rate (congestion control).

However, in ad hoc wireless networks, packet loss can occur due to: •**Node mobility** (frequent route changes or disconnections) •**Wireless interference** •**Signal fading** •**Limited bandwidth and collisions**. The primary challenge in implementing TCP (Transmission Control Protocol) over ad hoc networks lies in the misinterpretation of packet loss. TCP, by design, was created for wired networks, where packet loss is almost always a result of network congestion. In such cases, TCP uses mechanisms like congestion control and avoidance to reduce the transmission rate and avoid further congestion. **Key Challenges: 1. Misinterpretation of Packet Loss:** •In ad hoc networks, packet loss is often due to node mobility, signal fading, interference, or route breakages. •TCP, unaware of these conditions, assumes all losses are due to congestion and triggers unnecessary congestion control mechanisms. •This leads to reduction in throughput, increased delay, and poor performance. **2. Dynamic Topology:** •Nodes in an ad hoc network frequently move, causing frequent route changes and even route failures. •TCP doesn't have a mechanism to handle such dynamic route changes efficiently, leading to timeouts and retransmissions. **3. Hidden Terminal and Exposed Terminal Problems:** •In wireless communication, these issues cause data collisions, further increasing the chances of packet loss. •TCP, again, cannot differentiate this from congestion. **4. Lack of End-to-End Connectivity:** •Due to the multi-hop nature, the end-to-end path can frequently change or break. •TCP does not have a mechanism to adapt to changing paths, which leads to further retransmissions and connection drops. **5. High Bit Error Rates:** •Wireless channels are more prone to errors compared to wired links. •These errors cause corrupted or lost packets, which TCP interprets incorrectly.

---

**What is sensor network? Explain definition, operation.**

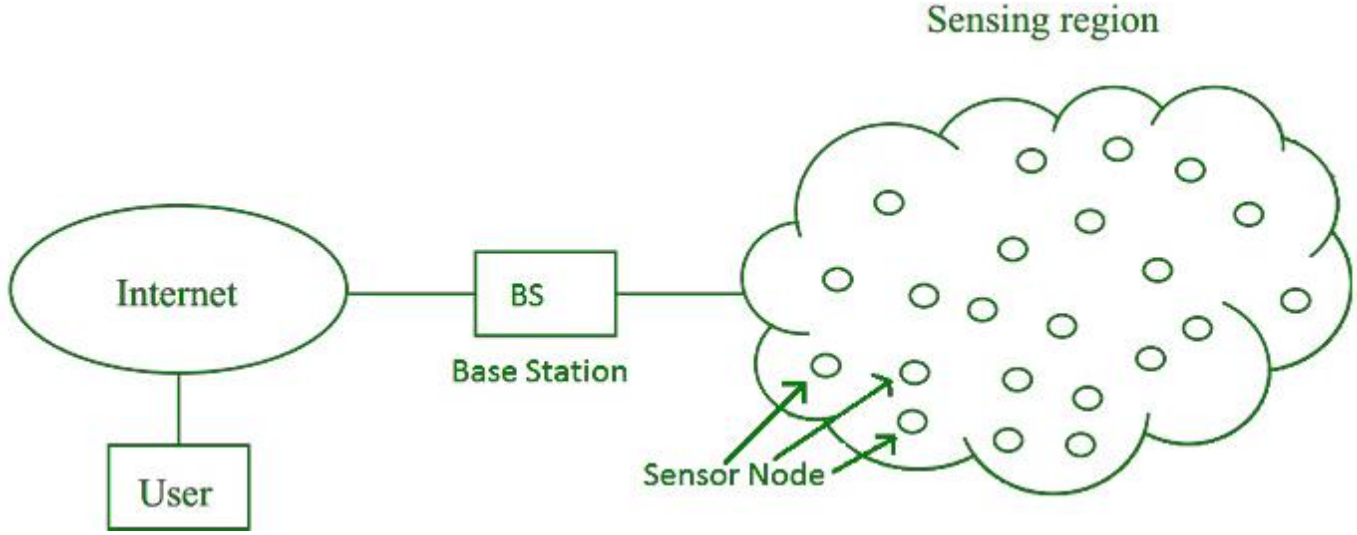
•A Sensor Network (or Wireless Sensor Network – WSN) is a collection of spatially distributed autonomous sensor nodes that monitor physical or environmental conditions, such as temperature, sound, pressure, motion, or pollutants, and cooperatively pass their data through the network to a central location or base station for processing and analysis. •A Sensor Network is a network of small, low-power, and intelligent sensor nodes that are capable of sensing, processing, and communicating environmental data wirelessly to achieve specific monitoring or control tasks. •**Operation of a Sensor Network:** The operation of a sensor network involves the following steps: **1. Sensing:** •Each sensor node is equipped with one or more sensors that detect physical phenomena such as temperature, light, humidity, or motion. •The sensed data is typically analogy in nature and is converted to digital signals using ADCs (Analog-to-Digital Converters). **2. Processing:** •After sensing, the node's microcontroller or processor processes the data locally to reduce communication overhead. •Simple processing may include data aggregation, filtering, or threshold-based triggering. **3. Communication:** •The processed data is then transmitted wirelessly to a sink node or base station. •Data is often routed through multiple

intermediate nodes using wireless communication protocols such as Zigbee, Bluetooth, or custom RF protocols. **4. Data Collection and Analysis:** •The base station collects the data from various sensor nodes and forwards it to a central server or cloud platform for further analysis, visualization, and decision-making. **Components of a Sensor Node:** •**Sensor(s)** – For physical data collection •**Microcontroller** – For local data processing •**Transceiver** – For wireless communication •**Power Source** – Typically batteries or energy harvesting devices **Applications of Sensor Networks:** •Environmental Monitoring (e.g., forest fire detection, pollution tracking) •Health Monitoring (e.g., patient vital signs) •Industrial Automation •Smart Homes and Cities •Military Surveillance •Disaster Management

---

**Discuss the architecture of wireless sensor network with diagrammatic illustration.**

A Wireless Sensor Network (WSN) is a network of spatially distributed sensor nodes that monitor physical or environmental conditions and cooperatively communicate the data to a central location for processing and analysis. These networks are used in applications like environmental monitoring, industrial automation, smart agriculture, military surveillance, and more.




**Components of WSN Architecture: 1. Sensor Nodes:** •These are small, battery-powered devices equipped with sensors to detect physical parameters like temperature, pressure, humidity, motion, etc. •Each sensor node typically contains: •A **sensor** (for sensing environment) •A **microcontroller** (for processing) •A **transceiver** (for wireless communication) •A **power unit** (battery or energy-harvesting device) •Sensor nodes may also act as **routers** by forwarding data from other nodes. **2. Sensing Region:** •The physical area or environment where sensor nodes are deployed is known as the sensing region. •Nodes within this region form a mesh and collaborate to collect and transmit data. **3. Base Station (BS):** •Acts as a gateway between the sensor network and the external world. •It collects data from sensor nodes and forwards it to the user via the internet. •Often equipped with higher processing and energy capacity than regular sensor nodes. **4. User:** •The end-user accesses the sensor data through applications running on computers or mobile devices. •Users may also send commands or configurations back to the sensor nodes via the base station. **5. Internet:** •Facilitates remote access and control of the sensor network. •Enables data to be shared, stored, and analyzed in real time.

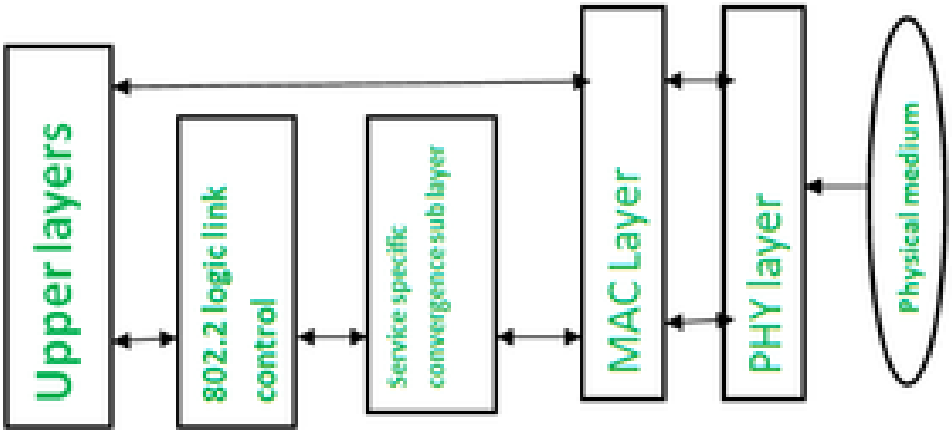
**Working of WSN Architecture: 1.** Sensor nodes sense environmental parameters. 2. Collected data is processed locally to remove redundancy or perform basic aggregation. 3. Data is transmitted wirelessly to the base station using multi-hop or direct communication. 4. The base station forwards the data to the internet. 5. Users can analyze or visualize the data through applications and dashboards. 6. In some applications, users may send control signals back to the network (e.g., to trigger an alarm or activate an actuator).

---

**Explain the architecture of IEEE 802.15 standard.**

**IEEE 802.15 Architecture:** The IEEE 802.15 standard defines the architecture and communication protocols for Wireless Personal Area Networks (WPANs). This standard is designed for short-range

wireless communication and supports low-data-rate and low-power-consumption applications such as Bluetooth, ZigBee, and Body Area Networks (BANs).



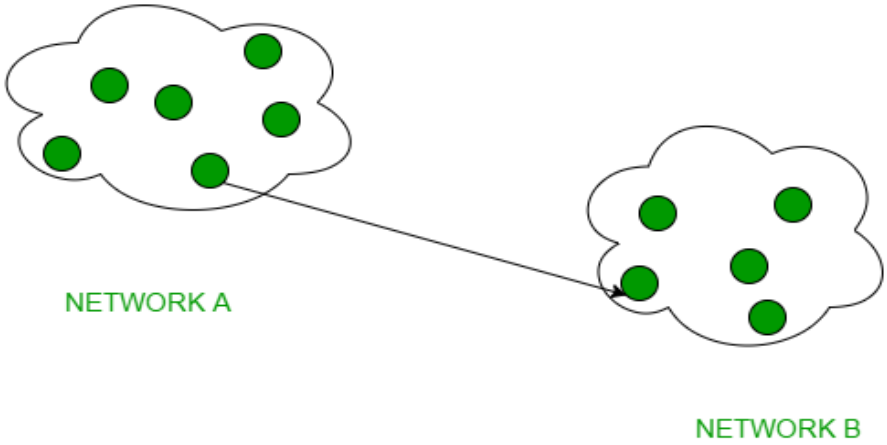

**1. Overview of the Architecture:** The architecture of IEEE 802.15 is layered and follows the OSI model. It mainly comprises the following components: **2. Upper Layers:** •These layers are not defined by IEEE 802.15 but are implemented by the application developer. •They include network, transport, session, presentation, and application layers. •These layers interact with the lower layers through standard interfaces. **3. IEEE 802.2 Logical Link Control (LLC):** •This sublayer sits above the MAC layer and provides a standard interface to the upper layers. •Responsible for flow control, error control, and framing. •LLC is common across all IEEE 802 standards. **4. Service-Specific Convergence Sublayer (SSCS):** •It acts as a bridge between the LLC and the MAC layer. •Converts data from the upper layers into a format suitable for the MAC layer. •Allows the IEEE 802.15 MAC layer to support a variety of upper-layer protocols. **5. Medium Access Control (MAC) Layer:** •Manages access to the physical medium. •Responsible for frame validation, acknowledgment, channel access mechanisms, and association/disassociation of devices. •Supports multiple topologies such as star and peer-to-peer. **6. Physical (PHY) Layer:** •Defines the actual transmission and reception of data over the wireless medium. •Includes modulation, demodulation, transmission power control, and data encoding. •Supports various frequency bands (e.g., 2.4 GHz ISM band in 802.15.4). **7. Physical Medium:** •The actual wireless channel used for data transmission. •Examples include RF (Radio Frequency), IR (Infrared), or UWB (Ultra-Wide Band).

---

**Explain in detail working of S-MAC protocol.**

S-MAC (Sensor-MAC) is a medium access control (MAC) protocol designed specifically for Wireless Sensor Networks (WSNs). The primary goal of S-MAC is to reduce energy consumption while maintaining adequate network performance. Traditional MAC protocols like IEEE 802.11 are not suitable for WSNs due to high energy usage. **Key Features of S-MAC: 1.** Periodic Sleep and Listen Cycles **2.** Synchronization of Sleep Schedules **3.** Message Passing (Data Fragmentation and Reassembly) **4.** Collision and Overhearing Avoidance **Working of S-MAC Protocol: 1. Periodic Sleep-Listen Mechanism:** •Each node alternates between sleep and listen periods. •During the sleep period, the node turns off its radio to conserve energy. •During the listen period, the node wakes up to send or receive data. •This approach significantly reduces idle listening, which is a major source of energy waste. **2. Schedule Synchronization:** •Nodes exchange SYNC packets to synchronize their sleep schedules. •Each node follows a neighbour's schedule to ensure proper communication. •A node may maintain multiple schedules if it is part of multiple neighbourhoods. **3. Collision Avoidance:** •S-MAC uses RTS/CTS (Request to Send/Clear to Send) handshaking to avoid collisions. •When a node wants to send data: -It sends an RTS. -The receiver replies with a CTS. -Neighbours that hear either RTS or CTS keep silent to avoid interference. **4. Overhearing Avoidance:** •If a node hears RTS or CTS not intended for it, it goes back to sleep, reducing unnecessary energy use. •This avoids listening to packets not meant for the node, saving power. **5. Message Passing Mechanism:** •Large messages are broken into smaller packets (fragments) and sent in bursts. •This reduces overhead and delay from multiple handshakes. •The receiver reassembles the message upon receiving all fragments. **Advantages of S-MAC: •Significant energy savings •Collision and overhearing reduction**

**Explain various protocols used in Unicast Geographic Routing.**




Unicast Geographic Routing is a technique where the location of the destination node is used to route a message from a source to a single destination in wireless ad hoc or sensor networks. These protocols reduce the overhead of route maintenance and discovery by relying on geographic positions rather than traditional hop-based routing tables. **1. GPSR (Greedy Perimeter Stateless Routing): •Greedy Mode:** Forwards packets to the neighbour closest to the destination. **•Perimeter Mode:** Used when greedy forwarding fails (local maximum); it routes around the obstacle using a right-hand rule. **•Pros:** Stateless, scalable, efficient. **•Cons:** Perimeter mode may increase latency. **2. GFG (Greedy-Face-Greedy):** •Combines greedy forwarding with face routing. •Starts with greedy forwarding; switches to face routing at dead ends. •Efficient for networks with irregular topology. **3. GOAFR (Greedy Other Adaptive Face Routing):** •Uses ellipse-based restricted search for face routing. •Adapts based on network density and topology. •Reduces path stretch and routing overhead compared to GPSR. **4. LAR (Location-Aided Routing):** •Limits route discovery to a "request zone", reducing control packet flooding. •Uses GPS or similar location data to estimate the destination's location. •Ideal for mobile ad hoc networks (MANETs). **5. DREAM (Distance Routing Effect Algorithm for Mobility):** •Uses the distance effect—nodes farther away need less frequent updates. •Maintains a location table with mobility predictions. •Reduces overhead in highly mobile networks. **6. Trajectory-Based Routing:** •The source defines a trajectory toward the destination based on waypoints or expected paths. •Intermediate nodes forward packets along this path. •Useful in vehicular networks or drone communication.

---

**Explain the Curve based routing.**

Curve-Based Routing is a type of geographic routing protocol used in wireless sensor networks (WSNs) and mobile ad hoc networks (MANETs). Instead of using shortest-path or greedy forwarding strategies, this approach uses predefined or dynamically generated curves (paths) to route packets from the source to the destination. •This routing technique is useful when: •The network topology is irregular, •There are obstacles, •Or load balancing is required. **Key Concepts of Curve-Based Routing: 1. Routing along a Curve:** •The routing path is shaped like a curve (e.g., a spiral, ellipse, or Bezier curve). •Packets are forwarded through nodes that are geographically close to this curve. •The curve acts as a virtual guide path. **2. Forwarding Region:** •Only nodes that fall within a certain distance (threshold) from the curve are considered as potential forwarding candidates. •This reduces broadcast and focuses energy usage. **3. Localized Decision Making:** •Nodes make forwarding decisions based on local information, such as their position relative to the curve and destination. •No need for global topology knowledge or routing tables. **How Curve-Based Routing Works: 1. Path Generation:** •The curve is generated based on source and destination locations. •It may avoid obstacles, conserve energy, or support load balancing. **2. Forwarding Strategy:** •Packets are forwarded to the next-hop neighbour closest to the curve and in the forwarding direction. •Curve can be static (pre-defined) or dynamic (adaptive to network conditions). **3. Termination:** The packet reaches the destination by following nodes near the curve. **•Applications:** •Wireless Sensor Networks (WSNs) •Underwater Sensor Networks (UWSNs) •Mobile Ad Hoc Networks (MANETs) •Delay-tolerant and Obstacle-prone environments.

**What is the Attribute-Based routing?**

Attribute-Based Routing (ABR) is a type of data-centric routing protocol mainly used in Wireless Sensor Networks (WSNs). Unlike traditional IP-based routing, which focuses on node addresses, ABR routes data based on specific attributes or data values. •In this approach, users or sink nodes send queries using attributes, such as: • "Find temperature readings > 30°C" • "Send humidity data from region X" Only the nodes that match the requested attributes will respond or forward the data.

**How It Works: 1. Query-Based Communication:** •The sink node broadcasts a **query or interest** based on data attributes. •Example: type = temperature AND value > 30°C **2. Matching Nodes Respond:** Only those sensor nodes whose data **match the query conditions** respond by sending the required information. **3. Data Aggregation (Optional):** •Intermediate nodes can aggregate data to reduce redundancy and save energy. **4. Route Formation:** •Routes are formed dynamically based on which nodes respond to the query. •Routing decisions are driven by data attributes, not fixed paths. **Key Features: •Data-Centric:** Routing decisions are made based on the content (attributes) of the data. **•Query-Driven:** Data is pulled from the network when needed. **•Energy Efficient:** Reduces unnecessary data transmission. **•Scalable:** Good for large-scale sensor deployments.

**Example Protocol: Directed Diffusion •**One of the first and most well-known attribute-based routing protocols. •Sink node floods an interest. •Nodes with matching data respond, and gradients are formed for data flow. **Advantages:** •Reduces routing overhead as it avoids route discovery. •Supports in-network processing like data aggregation. **Disadvantages:** •Requires complex matching logic at sensor nodes. •Less effective in highly mobile networks.

---

**Explain the advantages of it. Explain Unicast Geographic Routing.**

Unicast Geographic Routing is a routing technique used in wireless ad hoc networks (like sensor networks and MANETs) where data is sent from a single source to a single destination using the geographic (location) information of nodes. •Instead of using traditional routing tables, these protocols rely on the positions (latitude, longitude) of the sender, receiver, and intermediate nodes to forward the packet. **•How It Works: 1.** The source node knows the destination's geographic coordinates. **2.** It forwards the packet to the neighbouring node that is closest to the destination. **3.** This process continues hop-by-hop until the packet reaches the destination. **Common Examples of Protocols:** •GPSR (Greedy Perimeter Stateless Routing) •GFG (Greedy-Face-Greedy) •LAR (Location-Aided Routing) •DREAM (Distance Routing Effect Algorithm for Mobility)

**Advantages of Unicast Geographic Routing:** 1.**Scalability:** This routing method is highly scalable as it does not require maintaining complex routing tables or global network topology. It performs well even in large-scale networks with thousands of nodes. **2. Localized Decision-Making:** Routing decisions are made locally by each node based on the geographic positions of its immediate neighbors and the destination. This eliminates the need for a central coordinator or global knowledge. **3. Low Communication Overhead:** Since there is no need for route discovery, route maintenance, or control packet flooding, the overall routing overhead is significantly reduced. This leads to more efficient use of bandwidth. **4. Energy Efficiency:** Only the nodes that are geographically close to the path between the source and destination are involved in data forwarding. This minimizes unnecessary transmissions and conserves battery power, which is critical in wireless sensor networks. **5. Adaptability to Node Mobility:** Geographic routing is well-suited for mobile networks because it relies on node positions rather than static routing paths. This makes it robust and adaptive in dynamic environments where node movement is frequent. **6. Fast and Efficient Routing:** By always forwarding the packet to the neighbor closest to the destination, the protocol ensures relatively short and efficient paths, leading to reduced latency in communication.

---

**Write a note on Geographic Hash table.**

A Geographic Hash Table (GHT) is a distributed data structure designed to store and retrieve data in wireless sensor networks or mobile ad hoc networks, where nodes are distributed geographically. It combines concepts of geographic routing with hash tables to enable efficient data storage and lookup based on geographic location.

**Key Concepts: 1. Motivation:** •Traditional distributed hash tables (DHTs) work well in structured peer-to-peer networks but are not suitable for networks with geographical constraints and dynamic topologies, such as sensor networks. •GHT addresses this by leveraging geographic information to store data at nodes closest to a hashed geographic key. **2. How it Works:** •Each data item (key-value pair) is associated with a geographic location derived by hashing the key. •This geographic location acts as the address where the data is stored. •The network uses geographic routing to forward queries and insertions toward the node nearest to this hashed location. •For example, if a key is hashed to coordinates (x, y), the data is stored at the node geographically closest to (x, y). **3. Data Insertion and Lookup: •Insertion:** When a node wants to insert data, it computes the geographic hash of the key and routes the data to the node closest to that location. **•Lookup:** To retrieve data, a node similarly routes a query toward the hashed location, reaching the node holding the data. **•Advantages: 1. Scalability:** GHT scales well as nodes only need to know their neighbors and geographic locations. **2. Load Balancing:** Since the hash distributes keys geographically, data is evenly spread across the network. **3. Fault Tolerance:** Replication can be done in nearby nodes to ensure data persistence. **4. Energy Efficiency:** Geographic routing reduces overhead by limiting routing to geographic proximity rather than global flooding. **•Applications: •**Used in sensor networks to store sensed data efficiently. •Supports queries like "where is the temperature sensor reading for location X?" •Useful for location-based services in mobile networks. **•Challenges:** •Requires accurate location information for nodes. •Mobility of nodes can cause frequent updates and increased overhead. •Handling node failures and ensuring data consistency can be complex.

---

**Explain Range-Based Localization Algorithms.**

Range-based localization algorithms are techniques used in wireless sensor networks, robotics, and other applications to determine the physical position of a node or device based on distance or angle measurements relative to known reference points called anchors or beacons. **Key Concepts: 1. Purpose of Localization:** Localization is essential for applications like tracking, navigation, environmental monitoring, and network management. Range-based methods estimate the location by measuring physical quantities such as distance or angle from multiple known reference nodes. **2. How Range-Based Localization Works: •**The unknown node measures some form of range-related data (distance or angle) from multiple anchors. •Using these measurements, it calculates its position using geometric or mathematical techniques like trilateration or triangulation. **3. Common Range Measurements Used: •Time of Arrival (ToA):** Measures the time it takes for a signal to travel from sender to receiver; distance is calculated from time multiplied by signal speed. **•Time Difference of Arrival (TDoA):** Measures the difference in arrival times of signals at different receivers; useful in systems with multiple anchors. **•Received Signal Strength Indicator (RSSI):** Estimates distance based on the signal strength attenuation; cheaper but less accurate due to environmental effects. **•Angle of Arrival (AoA):** Measures the angle at which the signal arrives; helps in triangulation. **•Main Algorithms: •Trilateration:** •Uses distance measurements from at least three known anchors. •Each distance forms a circle around an anchor; the intersection point of these circles gives the estimated position. • **Triangulation:** •Uses angle measurements (AoA) from at least two known anchors. •Lines drawn at measured angles intersect at the target's position. **•Challenges and Limitations:** •Require special hardware or synchronization for accurate time measurements (e.g., ToA). •Signal attenuation, multipath effects, and noise can degrade measurement accuracy. •Anchor placement and density affect localization precision. •High energy consumption for continuous measurement in sensor networks.

---

**Explain Localization and its services with examples.**

Localization refers to the process of determining the physical location (coordinates) of a device, node, or object within a specific environment — such as a building, city, or geographical area.

It plays a crucial role in various domains such as wireless sensor networks (WSNs), mobile computing, robotics, and the Internet of Things (IoT), where knowing the location of devices or sensors is essential

for decision-making and context-aware services. •**Types of Localization:** •**Indoor Localization:** Used within buildings using technologies like Wi-Fi, Bluetooth, RFID. •**Outdoor Localization:** Uses GPS or satellite-based systems to determine location in open environments. •**Methods of Localization:** •**Range-Based Methods:** Use distance or angle measurements (e.g., RSSI, ToA, TDoA, AoA). •**Range-Free Methods:** Use connectivity or neighbourhood information without measuring distances. •**Anchor-Based:** Use known reference nodes (anchors) to estimate the position of unknown nodes. •**Anchor-Free:** Estimate positions relatively among nodes without known references.
•**Localization Services:** Localization is not just about finding coordinates; it enables several useful **services**, such as: **A. Location Discovery:** Helps nodes or users find their own position in a network or environment. **Example:** In a wireless sensor network deployed for forest monitoring, each sensor node discovers its position to tag environmental data with location information. **B. Geographic Routing:** Uses the physical location of nodes for efficient message delivery, especially in large networks. **Example:** A drone delivery system uses the geographic location of delivery addresses to calculate the shortest flying route. **C. Target Tracking:** Tracks moving objects or persons in real time. **Example:** A wildlife tracking system monitors the real-time location of animals wearing GPS collars. **D. Context-Aware Services:** Provides services or information based on the user's location. **Example:** Google Maps provides nearby restaurant suggestions based on your current location. **E. Asset/Personnel Monitoring:** Used in industries or hospitals to track the location of equipment, staff, or patients. **Example:** In a hospital, staff wear badges with RFID tags to track their movement and availability. **F. Emergency Response:** Assists in locating people during disasters or emergency situations. **Example:** When someone dials an emergency number, the system locates their position to dispatch help quickly.

**What are the advantages of Clustering?**
Clustering is a technique used in data analysis, machine learning, and wireless sensor networks to group similar data points or nodes into clusters. In the context of networking (especially wireless sensor networks) and data mining, clustering offers several significant advantages: **1. Improved Energy Efficiency (In WSNs):** •In wireless sensor networks (WSNs), clustering reduces energy consumption by minimizing communication distances. •Sensor nodes send data to a **cluster head**, which aggregates the data and forwards it to the base station, reducing overall network energy usage. •**Example:** LEACH (Low Energy Adaptive Clustering Hierarchy) protocol helps prolong the network's lifetime by using clustering. **2. Scalability:** •Clustering allows systems to handle large volumes of data or many nodes effectively. •By grouping similar elements, clustering reduces complexity and makes large datasets manageable. **3. Load Balancing:** •Clustering distributes workload among different clusters or cluster heads, preventing any single node from becoming overloaded. •This ensures optimal use of resources and extends the lifespan of systems in sensor networks. **4. Faster Data Access and Processing:** •By grouping similar data or nodes, clustering enables faster search, retrieval, and processing. •This is particularly beneficial in large databases and high-dimensional data spaces. •**Example:** In customer segmentation, clustering helps quickly identify target customer groups based on similar behaviour. **5. Data Aggregation and Compression:** •Cluster heads can perform data aggregation to remove redundancy before sending data, reducing transmission overhead. •This improves bandwidth utilization and saves storage. **6. Fault Tolerance and Reliability:** •If one node fails, other nodes in the cluster can take over or reroute the data. •Cluster-based systems can be designed to be robust and continue functioning even during partial failures. **7. Enhanced Network Lifetime:** •In sensor networks, rotating the role of the cluster head among nodes ensures that no single node dies early due to battery exhaustion. •This rotation prolongs the overall lifetime of the network.

**Explain the concepts of clustering, its advantages and algorithm for determining independent sets.**
Clustering in the context of wireless sensor networks (WSNs) or graph theory refers to the grouping of nodes into clusters. Each cluster has a central node known as the Cluster Head (CH) which coordinates communication within the cluster and may aggregate or forward data to a base station or other nodes. Clustering improves efficiency, scalability, and resource utilization by organizing nodes into

manageable groups, especially in large-scale networks. **Advantages of Clustering: •Energy Efficiency:** Reduces communication overhead by enabling local data aggregation at cluster heads. **•Scalability:** Supports the management of large networks by dividing them into smaller, easier-to-handle clusters. **•Load Balancing:** Distributes network tasks (e.g., communication, processing) evenly across cluster heads. **•Improved Data Aggregation:** Reduces data redundancy by merging similar data from multiple nodes. **•Extended Network Lifetime:** Clustering allows rotating the cluster head role, conserving energy in sensor networks. **•Simplified Network Management:** Local decision-making within clusters reduces the complexity of global coordination. **•Fault Tolerance:** If one cluster fails, it doesn't affect the entire network.

**Algorithm for Determining Independent Sets (Used in Clustering):** In graph theory, an Independent Set is a set of vertices in a graph, no two of which are adjacent. In clustering, such sets can be used to identify non-interfering nodes which can become cluster heads.

**Algorithm: Maximal Independent Set (MIS) Algorithm:** This algorithm helps to identify a set of nodes that are not directly connected to each other — ideal for selecting initial cluster heads.

**Steps: 1. Initialization:** All nodes are marked as undecided. **2. Random Priority Assignment:** Each node generates a random priority (e.g., a number between 0 and 1). **3. Selection:** A node becomes part of the Independent Set (IS) if it has the highest priority among its neighbours. **4. Mark Neighbours:** All neighbours of a selected node are marked as not eligible to join the IS (to avoid adjacency). **5. Repeat:** The process continues with the remaining undecided nodes until all are either in the IS or are neighbours of IS members. **6. Clustering:** Nodes in the MIS become Cluster Heads (CHs). The remaining nodes join the nearest CH.

---

**Distinguish between absolute and relative localization in Detail**

| **Absolute Localization** | **Relative Localization** |
|---|---|
| Determines the exact position of a node in a global coordinate system (e.g., latitude and longitude). | Determines the position of a node relative to other nodes in the network. |
| Requires external systems like GPS or known anchor nodes. | Does not require GPS; relies on measurements like distance or angle between nodes. |
| Provides location in terms of real-world coordinates. | Provides location in terms of relative distances or directions. |
| Higher accuracy is possible with appropriate infrastructure. | Accuracy depends on local connectivity and measurement precision. |
| Suitable for applications needing precise geolocation (e.g., mapping, navigation). | Suitable for applications like topology control or relative tracking in sensor networks. |
| More expensive due to hardware requirements like GPS. | Cost-effective as it avoids external localization hardware. |
| Vulnerable to signal loss or interference from external systems. | More robust in GPS-denied environments like indoors or underwater. |