Ad hoc & Network Sensors

Unit-1.0: Introduction to Ad Hoc and Sensor Networks 3 0 0 3 7 hrs Characteristics of ad hoc wireless networks, Applications of ad hoc networks, Challenges in ad hoc networks, Wireless sensor networks (WSN) – Characteristics and applications, Design issues in WSN, Sensor network architecture – Layered architecture, Cross-layer design.

📡 Ad Hoc Wireless Networks

Definition: An ad hoc wireless network is a decentralized type of wireless network where nodes (devices) communicate directly without relying on a fixed infrastructure like routers or access points. Each node acts as both a host and a router.

Characteristics

- **Decentralized architecture** – no central controller.
- **Dynamic topology** – nodes can join/leave anytime.
- **Multi-hop communication** – data may pass through multiple nodes.
- **Self-organizing** – nodes configure themselves automatically.
- **Limited resources** – constrained bandwidth, battery, and processing power.
- **Scalability** – can expand or shrink easily depending on nodes.

Applications

- **Military communication** – battlefield networks without infrastructure.
- **Disaster recovery** – emergency communication when infrastructure is damaged.
- **Vehicular networks** – cars communicating for traffic safety.
- **Sensor-based monitoring** – environmental or industrial monitoring.
- **Temporary events** – conferences, festivals, or expeditions.

Challenges

- **Routing complexity** – frequent topology changes.
- **Security risks** – vulnerable to attacks due to open medium.
- **Energy constraints** – battery-powered devices.
- **Quality of Service (QoS)** – difficult to guarantee stable performance.
- **Scalability issues** – performance may degrade with large networks.
- **Interference** – shared wireless medium causes collisions.

🌐 Wireless Sensor Networks (WSN)

Definition: A WSN is a network of spatially distributed autonomous sensors that monitor physical or environmental conditions (temperature, pressure, sound, etc.) and cooperatively transmit data to a central location.

Characteristics

- **Large number of sensor nodes** – often hundreds or thousands.
- **Low power consumption** – designed for long-term deployment.
- **Self-configuring** – nodes organize themselves.
- **Data-centric communication** – focus on sensed data rather than node identity.
- **Redundancy** – multiple sensors may cover the same area.
- **Short-range communication** – typically low-power wireless links.

Applications

- **Environmental monitoring** – forest fire detection, pollution tracking.
- **Health care** – patient monitoring with wearable sensors.
- **Industrial automation** – machinery monitoring, fault detection.
- **Agriculture** – soil moisture, crop health monitoring.
- **Smart homes/cities** – energy management, traffic monitoring.
- **Military surveillance** – battlefield monitoring.

⚙ **Design Issues in WSN**

- **Energy efficiency** – prolonging battery life.
- **Fault tolerance** – network should work even if some nodes fail.
- **Scalability** – must handle thousands of nodes.
- **Data aggregation** – reduce redundancy and save bandwidth.
- **Latency vs. accuracy trade-off** – balance speed and precision.
- **Deployment environment** – harsh conditions (underwater, forest, battlefield).
- **Security** – protect data integrity and privacy.

🏗 **Sensor Network Architecture**

Layered Architecture

Similar to the OSI model but adapted for sensor networks:

1. **Physical Layer** – deals with energy-efficient modulation, transmission.

2. **Data Link Layer** – medium access control (MAC), error detection.
3. **Network Layer** – routing protocols optimized for energy and reliability.
4. **Transport Layer** – ensures reliable data delivery.
5. **Application Layer** – provides services like monitoring, tracking, alerts.

Cross-Layer Design

- Traditional networks follow strict layered separation.
- In WSN, **cross-layer design** allows interaction between layers to optimize performance.
- Example: Routing decisions may depend on physical layer energy levels.
- Benefits: improved energy efficiency, reduced latency, better QoS.

✅ In summary, **ad hoc networks** are flexible, infrastructure-less systems useful in dynamic environments, while **WSNs** are specialized ad hoc networks focused on sensing and monitoring. Both face challenges like energy efficiency, scalability, and security, but their layered and cross-layer architectures help manage these issues.

Unit-2.0: MAC Protocols for Ad Hoc and Sensor Networks 7 hrs Fundamentals of MAC design, Issues in designing MAC protocols, MAC protocols for ad hoc networks – Contention-based protocols (Aloha, CSMA, MACA, MACAW), Scheduling-based MAC protocols, MAC protocols for WSN – S-MAC, T-MAC, B-MAC, X-MAC, Energy-efficient MAC protocols.

🛠️ Fundamentals of MAC Design

Definition: MAC (Medium Access Control) protocols are responsible for coordinating how multiple nodes share the wireless communication medium without collisions, ensuring efficient and fair access.

Key Fundamentals

- **Channel access** – deciding which node transmits at a given time.
- **Collision avoidance** – minimizing packet loss due to simultaneous transmissions.
- **Fairness** – ensuring all nodes get a chance to transmit.
- **Efficiency** – maximizing throughput and minimizing delay.
- **Energy conservation** – crucial for battery-powered nodes.
- **Scalability** – should work well as the number of nodes increases.

⚠️ Issues in Designing MAC Protocols

- **Hidden terminal problem** – nodes out of each other's range cause collisions.

- **Exposed terminal problem** – nodes unnecessarily defer transmission.
- **Dynamic topology** – frequent changes in node positions.
- **Limited bandwidth** – shared wireless medium.
- **Energy constraints** – especially in sensor networks.
- **QoS requirements** – delay-sensitive applications need guaranteed performance.
- **Synchronization** – coordinating nodes without centralized control.

📡 MAC Protocols for Ad Hoc Networks

Contention-Based Protocols

These rely on competition among nodes to access the medium.

1. **ALOHA**
    - Simple protocol: nodes transmit whenever they have data.
    - Collisions are resolved by retransmissions.
    - **Pros:** simplicity.
    - **Cons:** high collision rate, low efficiency.
2. **CSMA (Carrier Sense Multiple Access)**
    - Nodes sense the channel before transmitting.
    - If busy, they wait; if idle, they transmit.
    - **Pros:** reduces collisions compared to ALOHA.
    - **Cons:** still suffers from hidden terminal problem.
3. **MACA (Multiple Access with Collision Avoidance)**
    - Uses RTS (Request to Send) and CTS (Clear to Send) control packets.
    - Helps avoid hidden terminal problem.
    - **Pros:** better collision avoidance.
    - **Cons:** overhead due to control packets.
4. **MACAW (MACA for Wireless)**
    - Enhancement of MACA with additional signaling (ACK, DS packets).
    - Improves fairness and reliability.
    - **Pros:** better throughput and fairness.

- **Cons:** more complex, higher overhead.

Scheduling-Based MAC Protocols

- Nodes are assigned specific time slots or frequencies.
- Examples: TDMA (Time Division Multiple Access).
- **Pros:** collision-free, predictable performance.
- **Cons:** requires synchronization, less flexible in dynamic networks.

🌐 **MAC Protocols for Wireless Sensor Networks (WSN)**

1. **S-MAC (Sensor MAC)**
    - Uses periodic sleep and listen cycles to save energy.
    - Reduces idle listening.
    - **Pros:** energy-efficient.
    - **Cons:** may increase latency.
2. **T-MAC (Timeout MAC)**
    - Improvement over S-MAC with adaptive duty cycles.
    - Nodes sleep if no activity is detected.
    - **Pros:** better energy savings in low traffic.
    - **Cons:** risk of early sleeping (missing packets).
3. **B-MAC (Berkeley MAC)**
    - Uses low-power listening and preamble sampling.
    - Flexible and simple design.
    - **Pros:** high adaptability, efficient.
    - **Cons:** long preambles increase overhead.
4. **X-MAC**
    - Improvement over B-MAC with shorter preambles.
    - Allows early termination of preambles when receiver responds.
    - **Pros:** reduces energy waste, lower latency.
    - **Cons:** more complex than B-MAC.

Energy-Efficient MAC Protocols

- **Goal:** minimize energy consumption while maintaining performance.
- Techniques include:
    - Duty cycling (sleep/wake schedules).
    - Data aggregation to reduce transmissions.
    - Adaptive listening based on traffic.
    - Cross-layer optimization (MAC + routing + physical layer).

✅ In summary:

- **Ad hoc MAC protocols** focus on handling contention and scheduling in dynamic, infrastructure-less environments.
- **WSN MAC protocols** prioritize **energy efficiency** and scalability, with designs like S-MAC, T-MAC, B-MAC, and X-MAC tailored for sensor nodes.

Unit-3.0: Routing Protocols in Ad Hoc and Sensor Networks Challenges in routing, Proactive vs. Reactive routing, Ad hoc routing protocols – AODV, DSR, DSDV, OLSR, Hybrid routing (ZRP), Hierarchical routing, Geographic routing, Routing protocols for WSN – Flooding, SPIN, LEACH, TEEN, Directed diffusion, Geographic and Energy-Aware Routing (GEAR).

🚦 **Challenges in Routing**

Definition: Routing is the process of finding paths for data packets from source to destination. In ad hoc and sensor networks, routing is complex due to dynamic and resource-constrained environments.

Key Challenges

- **Dynamic topology** – nodes frequently join/leave or move.
- **Limited resources** – low battery, bandwidth, and processing power.
- **Scalability** – must handle large numbers of nodes.
- **Security threats** – vulnerable to attacks due to open medium.
- **QoS requirements** – delay, reliability, throughput must be balanced.
- **Energy efficiency** – critical in sensor networks.
- **Fault tolerance** – network must survive node failures.

🔄 **Proactive vs. Reactive Routing**

- **Proactive (Table-driven):**

- Nodes maintain up-to-date routing tables.
- Example: DSDV, OLSR.
- **Pros:** low latency, immediate route availability.
- **Cons:** high overhead due to constant updates.

- **Reactive (On-demand):**
  - Routes are discovered only when needed.
  - Example: AODV, DSR.
  - **Pros:** lower overhead, energy-efficient.
  - **Cons:** higher latency during route discovery.

Ad Hoc Routing Protocols

1. **AODV (Ad hoc On-Demand Distance Vector)**
   - Reactive protocol.
   - Uses route request (RREQ) and route reply (RREP).
   - **Pros:** efficient for dynamic networks.
   - **Cons:** initial delay in route discovery.
2. **DSR (Dynamic Source Routing)**
   - Reactive protocol.
   - Source node stores complete route in packet header.
   - **Pros:** no need for routing tables.
   - **Cons:** overhead increases with path length.
3. **DSDV (Destination-Sequenced Distance Vector)**
   - Proactive protocol.
   - Uses sequence numbers to avoid loops.
   - **Pros:** stable routes, loop-free.
   - **Cons:** high overhead in dynamic networks.
4. **OLSR (Optimized Link State Routing)**
   - Proactive protocol.
   - Uses multipoint relays (MPRs) to reduce flooding.

- **Pros:** efficient in dense networks.
- **Cons:** requires frequent updates.

5. **Hybrid Routing (ZRP – Zone Routing Protocol)**
   - Combines proactive (within zone) and reactive (outside zone).
   - **Pros:** balances overhead and latency.
   - **Cons:** complexity in zone management.
6. **Hierarchical Routing**
   - Nodes are grouped into clusters.
   - Cluster heads manage communication.
   - **Pros:** scalable, energy-efficient.
   - **Cons:** cluster head overload possible.
7. **Geographic Routing**
   - Uses node location information (GPS or coordinates).
   - Packets forwarded based on geographic position.
   - **Pros:** scalable, stateless routing.
   - **Cons:** requires location information.

🌐 **Routing Protocols for WSN**

1. **Flooding**
   - Each node forwards received packets to all neighbors.
   - **Pros:** simple, ensures delivery.
   - **Cons:** high redundancy, energy waste.
2. **SPIN (Sensor Protocols for Information via Negotiation)**
   - Uses metadata negotiation to avoid redundant data transmission.
   - **Pros:** energy-efficient compared to flooding.
   - **Cons:** may not guarantee delivery to all nodes.
3. **LEACH (Low-Energy Adaptive Clustering Hierarchy)**
   - Hierarchical protocol with rotating cluster heads.
   - **Pros:** balances energy consumption.

- **Cons:** not suitable for large-scale networks.

4. **TEEN (Threshold-sensitive Energy Efficient sensor Network protocol)**
    - Designed for time-critical applications.
    - Nodes transmit only when sensed value crosses threshold.
    - **Pros:** energy-efficient, suitable for reactive monitoring.
    - **Cons:** not good for continuous data collection.
5. **Directed Diffusion**
    - Data-centric protocol.
    - Queries are flooded, and data is routed along reinforced paths.
    - **Pros:** efficient for query-driven applications.
    - **Cons:** overhead in query flooding.
6. **GEAR (Geographic and Energy-Aware Routing)**
    - Combines location information with energy awareness.
    - Routes packets towards target region considering energy levels.
    - **Pros:** energy-efficient, scalable.
    - **Cons:** requires geographic info.

✅ In summary:

- **Ad hoc routing protocols** (AODV, DSR, DSDV, OLSR, ZRP) focus on handling dynamic topologies and scalability.
- **WSN routing protocols** (Flooding, SPIN, LEACH, TEEN, Directed Diffusion, GEAR) emphasize **energy efficiency** and data-centric communication.

Unit-4.0: Transport and Energy Management in Wireless Sensor Networks 7 hrs Issues in transport protocols, TCP over ad hoc networks, Transport protocols for WSN – CODA, RMST, PSFQ, ESRT, Energy-efficient routing in WSN, Data aggregation, Clustering techniques for WSN, Energy harvesting in sensor networks, Sleep-wake scheduling algorithms.

🚦 **Issues in Transport Protocols**

Definition: Transport protocols ensure reliable data delivery between nodes. In WSNs, they must balance reliability, latency, and energy efficiency.

Key Issues

- **Reliability** – packet loss due to wireless errors or node failures.
- **Congestion control** – avoiding buffer overflow and excessive retransmissions.
- **Energy constraints** – retransmissions consume battery power.
- **Scalability** – must handle thousands of nodes.
- **Latency** – critical for real-time applications.
- **Asymmetric traffic** – many-to-one communication (sensors → sink).

TCP over Ad Hoc Networks

- TCP is designed for wired networks, assumes congestion causes packet loss.
- In ad hoc/WSN, packet loss may be due to mobility, interference, or energy depletion.
- Problems:
    - Misinterprets wireless losses as congestion.
    - Retransmissions waste energy.
    - Poor performance in dynamic topologies.
- Solutions: modified TCP variants or specialized transport protocols for WSN.

Transport Protocols for WSN

1. **CODA (Congestion Detection and Avoidance)**
    - Detects congestion using buffer occupancy and channel load.
    - Uses open-loop (rate adjustment) and closed-loop (feedback) mechanisms.
    - **Pros:** reduces packet loss, saves energy.
    - **Cons:** overhead due to feedback messages.
2. **RMST (Reliable Multi-Segment Transport)**
    - Provides reliable delivery of large data objects.
    - Works with Directed Diffusion routing.
    - **Pros:** ensures complete data delivery.
    - **Cons:** higher overhead.
3. **PSFQ (Pump Slowly, Fetch Quickly)**
    - Source pumps data slowly, receivers fetch missing packets quickly.
    - Suitable for error-prone wireless links.

- **Pros:** reliable, efficient for broadcasting.
- **Cons:** delay due to slow pumping.

4. **ESRT (Event-to-Sink Reliable Transport)**
   - Focuses on reliable event reporting rather than individual packet delivery.
   - Adjusts reporting rate based on reliability feedback.
   - **Pros:** energy-efficient, scalable.
   - **Cons:** not suitable for applications needing per-packet reliability.

⚡ Energy-Efficient Routing in WSN

- **Goal:** maximize network lifetime by minimizing energy consumption.
- Techniques:
  - Multi-hop routing to reduce transmission distance.
  - Energy-aware path selection.
  - Load balancing among nodes.
  - Adaptive duty cycling.

📊 Data Aggregation

- Combines data from multiple sensors to reduce redundancy.
- Example: average temperature instead of individual readings.
- Benefits:
  - Saves bandwidth.
  - Reduces energy consumption.
  - Improves scalability.

🏗️ Clustering Techniques for WSN

- Nodes grouped into clusters, each with a **cluster head**.
- Cluster head aggregates and forwards data to sink.
- Examples: LEACH, HEED.
- Benefits:
  - Energy savings.
  - Scalability.

- Load balancing.

🌞 **Energy Harvesting in Sensor Networks**

- Sensors can harvest energy from environment:
  - **Solar power**
  - **Vibration/kinetic energy**
  - **Thermal gradients**
  - **RF energy harvesting**
- Extends network lifetime, reduces battery dependency.

😴 **Sleep-Wake Scheduling Algorithms**

- Nodes alternate between sleep and active states to save energy.
- Techniques:
  - **S-MAC/T-MAC** duty cycling.
  - **Adaptive sleep scheduling** based on traffic.
  - **Cluster-based scheduling** (cluster heads stay awake).
- Benefits:
  - Reduces idle listening.
  - Conserves energy.
  - Extends network lifetime.

✅ In summary:

- Transport protocols in WSN (CODA, RMST, PSFQ, ESRT) are designed to balance **reliability and energy efficiency**.
- Energy management techniques (aggregation, clustering, harvesting, sleep scheduling) are crucial to prolong network lifetime.

Unit-5.0: Localization, Synchronization, and Data Dissemination in WSN 7 hrs Localization techniques – GPS-based localization, Range-based localization (RSSI, TOA, TDOA, AOA), Range-free localization (Centroid, DV-Hop, APIT), Time synchronization in WSN – RBS, TPSN, Data dissemination and query processing in WSN, Mobile sink-based data collection.

📍 **Localization Techniques**

Definition: Localization is the process of determining the physical position of sensor nodes in a WSN. Accurate location information is essential for routing, coverage, and data interpretation.

1. GPS-Based Localization

- Each node equipped with GPS receiver.
- Provides precise location coordinates.
- **Pros:** high accuracy.
- **Cons:** costly, high energy consumption, not suitable for indoor/underground environments.

2. Range-Based Localization

Uses physical measurements to estimate distance/angle between nodes.

- **RSSI (Received Signal Strength Indicator):** distance estimated from signal strength.
- **TOA (Time of Arrival):** distance calculated using signal travel time.
- **TDOA (Time Difference of Arrival):** difference in arrival times at multiple nodes.
- **AOA (Angle of Arrival):** angle of incoming signal used for triangulation.
- **Pros:** better accuracy than range-free methods.
- **Cons:** requires extra hardware, sensitive to noise.

3. Range-Free Localization

Does not rely on precise measurements, uses connectivity information.

- **Centroid:** nodes estimate position as centroid of nearby anchor nodes.
- **DV-Hop:** uses hop count between nodes and anchors to estimate distance.
- **APIT (Approximate Point-In-Triangulation):** node checks if it lies inside triangle formed by anchors.
- **Pros:** low cost, simple.
- **Cons:** less accurate compared to range-based methods.

⏱ **Time Synchronization in WSN**

Definition: Synchronization ensures all nodes in the network have a common notion of time, crucial for coordinated sensing, communication, and scheduling.

Protocols

- **RBS (Reference Broadcast Synchronization):**
    - Nodes synchronize by comparing arrival times of reference broadcasts.

    - Eliminates sender-side uncertainty.
    - **Pros:** high accuracy.
    - **Cons:** requires multiple exchanges.
- **TPSN (Timing-sync Protocol for Sensor Networks):**
    - Builds a hierarchical structure (levels).
    - Synchronization achieved via pairwise message exchanges.
    - **Pros:** simple, accurate.
    - **Cons:** overhead in maintaining hierarchy.

📊 Data Dissemination and Query Processing in WSN

Definition: Data dissemination is the process of distributing information across the network, while query processing involves retrieving relevant data from sensors.

Techniques

- **Flooding:** simple but energy-inefficient.
- **Data-centric dissemination:** queries are based on data attributes rather than node IDs.
- **In-network processing:** data aggregated at intermediate nodes to reduce redundancy.
- **Pros:** efficient retrieval, reduced communication cost.
- **Cons:** query flooding may cause overhead.

🚶 Mobile Sink-Based Data Collection

Definition: A mobile sink (data collector) moves through the network to gather data from sensor nodes.

Benefits

- Reduces energy consumption (nodes transmit shorter distances).
- Balances load across network.
- Extends network lifetime.

Challenges

- Path planning for sink mobility.
- Delay in data collection.
- Synchronization with sensor reporting schedules.

✅ In summary:

- **Localization** ensures nodes know their positions (GPS, range-based, range-free).
- **Synchronization** aligns node clocks (RBS, TPSN).
- **Data dissemination** enables efficient query-driven communication.
- **Mobile sinks** improve energy efficiency and scalability in WSN.

6.0: Security and Emerging Trends in Ad Hoc and Sensor Networks Security issues in ad hoc and sensor networks, Attack models – Eavesdropping, Sybil attack, Blackhole, Wormhole, Intrusion detection in WSN, Secure routing in ad hoc networks, Privacy-preserving techniques, Emerging trends – Mobile ad hoc networks (MANETs), Vehicular ad hoc networks (VANETs), Cognitive radio sensor networks (CRSN), AI/ML applications in WSN.

🔒 Security Issues in Ad Hoc and Sensor Networks

Definition: Security in ad hoc and sensor networks is critical because they operate in open, decentralized, and resource-constrained environments, making them vulnerable to attacks.

Key Issues

- **Confidentiality** – protecting data from unauthorized access.
- **Integrity** – ensuring data is not altered during transmission.
- **Authentication** – verifying node identities.
- **Availability** – keeping the network operational despite attacks.
- **Resource constraints** – limited power and memory make strong cryptography difficult.
- **Dynamic topology** – frequent changes complicate secure routing.

⚠️ Attack Models

1. **Eavesdropping**
    - Attacker listens to communication without altering it.
    - Breaches confidentiality.
2. **Sybil Attack**
    - A node presents multiple fake identities.
    - Disrupts routing, voting, and resource allocation.
3. **Blackhole Attack**
    - Malicious node advertises shortest path but drops all packets.

- Causes denial of service.

4. **Wormhole Attack**
    - Two colluding nodes tunnel packets to disrupt routing.
    - Creates false topology information.

🛡️ Intrusion Detection in WSN

- **Definition:** Mechanisms to detect abnormal or malicious activities.
- Techniques:
    - Signature-based detection (known attack patterns).
    - Anomaly-based detection (deviation from normal behavior).
    - Hybrid approaches.
- Challenges: limited resources, distributed environment.

🚦 Secure Routing in Ad Hoc Networks

- Ensures data packets follow safe paths.
- Techniques:
    - Authentication of routing messages.
    - Encryption of control packets.
    - Trust-based routing (nodes rated for reliability).
- Examples: SAODV (Secure AODV), ARAN (Authenticated Routing for Ad hoc Networks).

🔐 Privacy-Preserving Techniques

- **Data anonymization** – hiding node identity.
- **Secure aggregation** – combining data without revealing individual values.
- **Location privacy** – hiding node positions from attackers.
- **Encryption** – lightweight cryptographic methods suitable for WSN.

🌟 Emerging Trends

1. **Mobile Ad Hoc Networks (MANETs)**
    - Infrastructure-less mobile networks.
    - Applications: disaster recovery, military, temporary events.
2. **Vehicular Ad Hoc Networks (VANETs)**

- Vehicles communicate with each other and roadside units.
- Applications: traffic safety, navigation, infotainment.

3. **Cognitive Radio Sensor Networks (CRSN)**
   - Sensors equipped with cognitive radios that dynamically access spectrum.
   - Benefits: efficient spectrum usage, adaptability.
4. **AI/ML Applications in WSN**
   - Machine learning used for:
     - Intrusion detection.
     - Energy management.
     - Data aggregation and prediction.
     - Fault detection.
   - Enables intelligent, adaptive sensor networks.

✅ **In summary:**

- Security in ad hoc and sensor networks faces challenges like eavesdropping, Sybil, blackhole, and wormhole attacks.
- Solutions include intrusion detection, secure routing, and privacy-preserving techniques.
- Emerging trends such as MANETs, VANETs, CRSN, and AI/ML integration are shaping the future of these networks.