

Unit 3: Wireless Mobile Networks

Ad-hoc & Sensor Networks · Routing · QoS · Mobile Systems

Theories · Routing · Energy · Mobility · Security

Dr. Gopal Chandra Jana
Dept. of CSE, Sharda University

Course Page: <https://www.gcjana.in/courses/shardauniversity/2502/PHD650/>

April 26, 2026

- 1 Mobile Ad-hoc & Sensor Networks
- 2 Probability, Traffic & Queuing Theory
- 3 Routing in Wireless Networks
- 4 Energy Efficiency & Quality of Service
- 5 Mobile Communication Systems
- 6 Security, Privacy & Optical Networking

What is a Mobile Ad-hoc Network (MANET)?

Definition

A **Mobile Ad-hoc Network (MANET)** is a self-configuring, infrastructure-less network of mobile devices connected via wireless links, capable of forming a temporary network without centralised administration.

Key Characteristics

- No fixed infrastructure or base station
- Dynamic topology — nodes move freely
- Each node acts as both host and router
- Multi-hop communication
- Self-organising and self-healing

Applications

- Military battlefield communication
- Disaster-relief operations
- Vehicular networks (VANETs)
- Emergency search & rescue
- Collaborative computing

Wireless Sensor Networks (WSN)

Definition

A **WSN** consists of spatially distributed, autonomous sensor nodes that monitor physical or environmental conditions and cooperatively pass data to a *sink* or base station.

Sensor Node Architecture

- **Sensing unit** — transducers, ADC
- **Processing unit** — micro-controller
- **Communication unit** — RF transceiver
- **Power unit** — battery/energy harvesting

Challenges

- Severe energy constraints
- Limited computation & memory
- Unreliable wireless links
- Large-scale deployment

MANET vs WSN

Feature	MANET	WSN
Mobility	High	Low
Energy	Moderate	Critical
Node count	Tens	Thousands
Purpose	General	Sensing
Data flow	P2P	To sink

Why Probability?

Wireless channels are inherently **random**: signal fading, interference, and user mobility are all stochastic phenomena. Probability theory provides the mathematical backbone for modelling and analysis.

Key Probabilistic Models

- **Rayleigh fading** — multipath rich environments:

$$f(r) = \frac{2r}{\Omega} e^{-r^2/\Omega}$$

- **Rician fading** — LOS + multipath
- **Log-normal shadowing**:
 $P_r[\text{dB}] = \bar{P}_r - X_\sigma$
- **Poisson process** — packet arrivals, user call generation

Applications

- Outage probability calculation
- Bit Error Rate (BER) analysis
- Coverage & connectivity analysis
- Handoff probability estimation
- Channel access (CSMA/CA backoff)
- Reliability analysis in WSNs

Traffic Theory

Studies the generation, flow, and statistical properties of data or call traffic in a network to dimension resources (channels, buffers) appropriately.

Erlang Traffic Model

- Traffic intensity: $A = \lambda \cdot h$ Erlangs
(λ = call arrival rate, h = mean holding time)
- **Erlang B** (blocking, no queue):
$$B = \frac{A^N / N!}{\sum_{k=0}^N A^k / k!}$$
- **Erlang C** (queuing allowed):
Gives probability call is queued

Traffic Characteristics

- **Voice** — constant bit rate, delay-sensitive
- **Data** — bursty, self-similar (Pareto)
- **Video** — variable bit rate, loss-sensitive
- **Self-similar traffic** — Hurst parameter $H > 0.5$
- Long-range dependence \Rightarrow larger queues
- Used for **channel allocation** and **CAC**

Queuing Theory in Wireless Networks (Q25)

Queuing Theory

Mathematical study of waiting lines to predict queue length, waiting time and system throughput — essential for wireless buffer and scheduler design.

Kendall Notation: A/B/c/K

- A Arrival process (M = Markov/Poisson)
- B Service process (M, D, G)
- c Number of servers
- K System capacity

M/M/1 Queue Results

- Traffic load: $\rho = \lambda/\mu$
- Mean queue length: $L = \rho/(1 - \rho)$
- Mean waiting time: $W = 1/(\mu - \lambda)$
- Stability condition: $\rho < 1$

Wireless Applications

- **MAC layer buffer** modelling (M/M/1)
- **Multi-channel access** (M/M/c)
- **Finite buffer** packet loss (M/M/1/K)
- **Priority queuing** for QoS classes
- **Handoff queuing** — guard channels
- **Scheduling**: WFQ, PGPS in 4G/5G

Little's Law: $L = \lambda W$ (universal)

Unicast, Multicast & Broadcast Routing (Q17)

Key Distinction

Unicast: one source → one destination. **Multicast:** one source → a group. **Broadcast:** one source → all nodes.

Feature	Unicast	Multicast	Broadcast
Destination	Single node	Group of nodes	All nodes
Traffic volume	Low	Moderate	High
Routing overhead	Low per flow	Shared tree overhead	Flooding overhead
Scalability	High	Moderate	Low
Bandwidth use	Individual paths	Shared distribution	Network-wide
Example	TCP/IP session	Video conferencing	ARP request
Algorithm	AODV, DSDV	ODMRP, MAODV	Blind flooding, MPR

Unicast vs Multicast Routing — Detailed Comparison (Q18)

Unicast Routing

- **Mechanism:** finds best path from S to single D
- **Protocols:**
 - Proactive: DSDV, OLSR (maintain full table)
 - Reactive: AODV, DSR (on-demand discovery)
- **Overhead:** low — route to one destination
- **Traffic:** separate packet per destination
- **State:** per-destination route entries

Multicast Routing

- **Mechanism:** distribution tree (source or shared)
- **Protocols:**
 - ODMRP — mesh-based, on-demand
 - MAODV — tree-based extension of AODV
 - CAMP — core-assisted mesh protocol
- **Overhead:** moderate — group membership
- **Traffic:** one packet replicated at branch nodes
- **State:** per-group multicast state

Network Traffic Impact

Multicast reduces total traffic significantly when group size is large: Unicast sends N copies; Multicast sends ≈ 1 copy replicated at branches.

AODV — Ad-hoc On-Demand Distance Vector (Q18 Detail)

AODV Overview

AODV is a **reactive** (on-demand) unicast routing protocol for MANETs. Routes are created only when needed, avoiding unnecessary overhead.

Route Discovery Process

- 1 Source floods **RREQ** (Route REQuest) with sequence numbers
- 2 Intermediate nodes: if route to D known \Rightarrow send **RREP**; else rebroadcast
- 3 Destination or intermediate node sends **RREP** (Route REPLY) back
- 4 Source begins sending data along reverse path

Route Maintenance

- **RERR** (Route ERRor) sent when link breaks
- Sequence numbers prevent stale routes and loops

AODV Message Types

Msg	Purpose
RREQ	Route discovery (broadcast)
RREP	Route reply (unicast)
RERR	Route error notification
Hello	Neighbour detection

Advantages

- Minimal routing overhead
- Loop-free by sequence numbers
- Supports multicast (MAODV)

Broadcasting

Delivering a packet from one source to **all nodes** in the network. Naive flooding is simple but causes the *broadcast storm problem*.

Flooding (Blind)

- Every node retransmits once
- Guaranteed delivery (if connected)
- Redundant transmissions \Rightarrow collisions
- Bandwidth waste: $O(n)$ transmissions

Optimised Flooding

- **Probability-based**: retransmit with prob. p
- **Counter-based**: limit retransmit count
- **Distance-based**: based on spatial distance

MPR (Multipoint Relay) — OLSR

- Each node selects a set of **MPR** neighbours
- MPRs cover all 2-hop neighbours
- Only MPRs retransmit \Rightarrow far fewer transmissions
- Reduces broadcast overhead dramatically

Spanning Tree Broadcast

- Build a spanning tree rooted at source
- Each node forwards once along tree edges
- Optimal: exactly $N - 1$ transmissions
- Requires tree maintenance in mobile nets

Hierarchical Routing for Scalability (Q19, Q24)

Problem

Flat routing does not scale — routing tables of size $O(N)$ and control overhead of $O(N^2)$ become prohibitive as N grows.

Hierarchical Structure

- Nodes grouped into **clusters**
- Each cluster elects a **Cluster Head (CH)**
- CHs form a **backbone** network
- Multiple levels possible (2-level, 3-level)

Routing Process

- 1 Node \rightarrow CH (intra-cluster)
- 2 CH \rightarrow Destination CH (backbone routing)
- 3 Destination CH \rightarrow destination node

Protocols: LEACH, HARP, ZRP (Zone Routing)

Scalability Benefits

Metric	Flat	Hier.
Table size	$O(N)$	$O(\sqrt{N})$
Control msg	$O(N^2)$	$O(N)$
Path length	Optimal	Near-opt.
Scalability	Poor	Good

ZRP — Zone Routing Protocol

- Proactive within zone radius r
- Reactive beyond zone
- Best of both worlds

Energy Efficiency in Wireless Networks (Q22)

Why Energy Efficiency?

Wireless devices (especially sensors and IoT nodes) are battery-powered. Energy efficiency directly determines **network lifetime**.

Energy Consumption Sources

- **Transmission** — dominant, $\propto d^n$ ($n = 2-4$)
- **Reception** — significant (radio always on)
- **Idle listening** — often equals RX cost
- **Overhearing** — receiving unintended pkts
- **Control overhead** — headers, ACKs, beacons

MAC Strategies

- Duty cycling (SMAC, TMAC)
- Sleep scheduling
- Adaptive power control

Energy-Efficient Routing

- **Min energy path** — minimise total E_{TX}
- **Max-min battery** — maximise node lifetime
- **Load balancing** — distribute energy usage
- **LEACH protocol:**
 - Random CH rotation
 - Intra-cluster TDMA
 - Data aggregation at CH
 - 70% energy saving vs direct

Cross-layer design — combine PHY, MAC, NET layers for joint energy optimisation

Quality of Service (QoS) in Wireless Networks (Q22, Q23)

Definition

QoS is the ability of the network to provide guaranteed levels of service performance to specific traffic flows, ensuring acceptable user experience.

QoS Parameters (Q23)

- **Bandwidth** — data rate (Mbps)
- **Latency/Delay** — end-to-end delay (ms)
- **Jitter** — delay variation (ms)
- **Packet Loss Rate** — % packets dropped
- **Throughput** — effective data rate
- **Reliability** — successful delivery ratio
- **BER** — bit error rate on channel

Multimedia Transmission Requirements

App	BW	Delay	Loss
Voice	8–64 kb/s	<150 ms	<1%
Video	1–20 Mb/s	<250 ms	<0.1%
Streaming	0.5–8 Mb/s	Moderate	<2%
Data	Best ef- fort	Flexible	0%

QoS Mechanisms

IntServ (RSVP) DiffServ WEQ PGPS CAC

Effect of Each QoS Parameter

- **High Delay** (>150 ms voice): conversation becomes unnatural
- **High Jitter** (>30 ms video): frames arrive out of order \Rightarrow artifacts
- **Packet Loss** ($>5\%$ video): visible freezing, macroblocking
- **Low Bandwidth**: codec degrades gracefully (adaptive bitrate streaming — HLS, DASH)
- **High BER**: FEC (Reed-Solomon) corrects errors; ARQ retransmissions increase delay

QoS Provisioning Techniques

- 1 **Admission Control** — reject flows that violate SLA thresholds
- 2 **Traffic Shaping** — token bucket, leaky bucket
- 3 **Priority Queuing** — voice over data
- 4 **Scheduling**: WFQ ensures weighted fair share
- 5 **Buffer Management**: RED/WRED for proactive congestion control
- 6 **Adaptive Coding**: variable bitrate based on channel quality (AMR for voice, H.264 SVC)

Registration and Roaming (Q20, Q21)

Core Concepts

Registration is the process by which a mobile device announces its current location to the network.

Roaming is the ability to use services in a visited network outside the home network coverage area.

Key Network Entities

- **Home Location Register (HLR)** — permanent database of subscribers
- **Visitor Location Register (VLR)** — temporary database in visited area
- **Mobile Switching Centre (MSC)** — call routing and handoff control
- **Authentication Centre (AuC)** — security key management
- **Base Station (BS)** — radio access point

Registration Types

- **Power-on** registration — when device turns on
- **Location update** — when crossing cell boundary
- **Periodic** — timer-based keep-alive
- **IMSI attach/detach** — subscriber presence
- **Inter-VLR handoff** — new MSC area

Registration Process in Detail (Q21)

Step-by-Step Registration Procedure

- 1 Mobile device enters coverage, detects a BS and reads **system broadcast**
- 2 Device sends **Registration Request** to BS with IMSI/TMSI
- 3 BS forwards to local **VLR/MSC**
- 4 VLR queries **HLR**: “Is this subscriber valid?”
- 5 HLR sends subscriber profile and **authentication vectors** to VLR
- 6 **Authentication**: VLR sends RAND → device responds with SRES using K_i (secret key)
- 7 On success: HLR cancels old VLR record; new VLR activates subscriber
- 8 VLR assigns a **TMSI** (Temporary Mobile Subscriber Identity) for privacy
- 9 Device receives **Registration Accept** — ready for service

Security Note

The secret key K_i never leaves the SIM or AuC. Only the challenge-response (RAND, SRES) pair is transmitted over the air.

Hard Handoff vs Soft Handoff (Q21)

Handoff

The process of transferring an active call/session from one base station to another as a mobile user moves across cell boundaries.

Hard Handoff (Break-Before-Make)

- Connection to old BS released **before** new BS
- Used in TDMA/FDMA systems (GSM)
- Only one frequency/channel at a time
- Brief **interruption** in service (~ 50 ms)
- Simpler — no duplicate transmission
- Sensitive to **ping-pong effect**

Decision criteria: Received signal strength (RSS) threshold or hysteresis

Soft Handoff (Make-Before-Break)

- Mobile connected to **multiple BSs** simultaneously
- Used in CDMA systems (IS-95, WCDMA)
- Macro-diversity combining at MSC
- **No interruption** — seamless transition
- More complex — requires multiple BS resources
- Handles border areas better (**softer handoff** for same BSC)

Decision criteria: Pilot signal strength (E_c/I_o) set

Hard vs Soft Handoff — Comparison Table (Q21)

Parameter	Hard Handoff	Soft Handoff
Connectivity	Single BS at a time	Multiple BSs simultaneously
Interruption	Brief drop (~50 ms)	Seamless (none)
System	GSM, TDMA, FDMA	CDMA, WCDMA, cdma2000
Complexity	Low	High
Resource use	Efficient	Uses multiple BS resources
Reliability	Lower at boundary	Higher — diversity gain
Ping-pong effect	More susceptible	Less susceptible
Delay sensitivity	Moderate	Low (ideal for voice)
Implementation	Simple	Complex (RAKE receiver)

Key Insight

Soft handoff provides **macro-diversity gain** — the MSC selects or combines the best signal from

Mobile Multicast

Efficient delivery of a single data stream to a **group** of mobile receivers, managing group membership as nodes move.

Challenges

- Frequent topology changes break multicast trees
- Group membership changes as nodes move
- Handoff requires tree re-joining
- IP multicast (PIM-SM) not designed for mobility

Solutions

- **Bi-directional tunnelling** through home agent
- **Remote subscription** to new cell's multicast
- **ODMRP** — mesh-based, robust to mobility

ODMRP Mechanism

- 1 Source periodically floods **Join Query**
- 2 Receivers reply with **Join Table**
- 3 Intermediate nodes on paths become **Forwarding Group**
- 4 Mesh formed — more robust than tree
- 5 Membership refreshed every period T

Advantage: Mesh topology survives link failures better than tree

Security Threats

Mobile wireless networks face unique threats due to open radio medium, device mobility, and limited resources for cryptographic operations.

Attack Taxonomy

Passive Attacks

- Eavesdropping — intercept unencrypted data
- Traffic analysis — infer patterns without decryption

Active Attacks

- **Man-in-the-Middle** — intercept and modify
- **Sybil attack** — forge multiple identities
- **Black hole** — routing attack, drop all pkts
- **Wormhole** — tunnel packets to deceive routing

Security Services & Mechanisms

Service	Mechanism
Authentication	AKA (3GPP), EAP-TLS
Confidentiality	AES-128, KASUMI
Integrity	HMAC-SHA, SNOW 3G
Non-repudiation	PKI, Digital signatures
Privacy	TMSI, pseudo-identity

Privacy Challenges

Role of Optical Networking

Optical fibre networks form the **backbone** (backhaul) of mobile systems, transporting aggregated traffic from BSs to core networks at ultra-high speeds.

Key Optical Technologies

- **WDM/DWDM** — wavelength division multiplexing; up to 80+ channels on one fibre
- **OTN** (Optical Transport Network) — ITU-T G.709; structured transport with OAM
- **MPLS-TP** — packet transport for mobile backhaul
- **CWDM** — coarse WDM for metro rings
- **PON** (Passive Optical Network) — fronthaul for C-RAN

Optical Switching

- **OXC** — Optical Cross-Connect; wavelength routing
- **ROADM** — Reconfigurable Add/Drop Multiplexer
- **OBS** — Optical Burst Switching for dynamic traffic
- **OPS** — Optical Packet Switching (future)

5G Fronthaul Requirements

- Latency < 100 μ s (CPRI/eCPRI)
- Bandwidth: 10–100 Gbps per cell

Mobile IP (RFC 3344)

Enables a mobile device to maintain the **same IP address** while moving between networks, ensuring ongoing connections are not disrupted.

Key Entities

- **Home Agent (HA)** — router in home network; maintains *mobility binding*
- **Foreign Agent (FA)** — router in visited network; provides Care-of-Address
- **Care-of-Address (CoA)** — temporary address in foreign network
- **Home Address (HoA)** — permanent address, unchanged

Packet Flow

- 1 Correspondent sends pkt to HoA

Improvements

- **Route Optimisation** — Correspondent notified of CoA directly
- **Mobile IPv6** — built-in support, no FA needed; hierarchical MIPv6 (HMIPv6)
- **PMIP** — network-based; device needs no MIP stack
- **SCTP** — multi-homing at transport layer

Triangle Routing Problem

Basic MIP: all traffic goes via HA (suboptimal).
Route optimisation solves this.

What We Covered

- 1 **MANET & WSN** — self-organising wireless networks; node architecture
- 2 **Probability Theory** — fading models, outage, Poisson arrivals
- 3 **Traffic Theory** — Erlang B/C, self-similar traffic, channel planning
- 4 **Queuing Theory** — M/M/1, Little's Law, priority queuing
- 5 **Routing** — Unicast (AODV), Multicast (ODMRP), Broadcast (MPR)
- 6 **Hierarchical Routing** — ZRP, cluster heads, $O(\sqrt{N})$ tables
- 7 **Energy Efficiency** — duty cycling, LEACH, cross-layer design
- 8 **QoS** — bandwidth, delay, jitter, loss; WFQ, DiffServ, admission control
- 9 **Registration** — HLR/VLR, authentication AKA, TMSI assignment
- 10 **Handoff** — Hard (GSM) vs Soft (CDMA); diversity gain
- 11 **Multicasting** — ODMRP mesh, mobile IP multicast
- 12 **Security** — threats, AES, TMSI privacy, wormhole defence
- 13 **Optical Networking** — DWDM, eCPRI fronthaul, ROADM

Key Result

Wireless mobile networks integrate **probabilistic models**, **adaptive routing**, **energy-aware protocols**, and **secure mobility management** to deliver seamless, efficient, and reliable connectivity to mobile users.

This unifies theory, protocols, and real-world system design.

Thank You

Any Questions?

“The future of connectivity lies in seamlessly bridging the physical and digital worlds through intelligent wireless networks.”

Instructor: Dr. Gopal Chandra Jana
Dept.: CSE, Sharda University
Course: PHD650 (PhD Course Work Core Subject)
Date: April 26, 2026