Lecture 1: 1.1 Evolution of Cellular communication (1G to 5G)

Fundamental of Cellular Communication

DI05011011: Mobile Communication

Agenda for Today

- 1. Introduction to Mobile Communication
- 2. The First Generation (1G): Analog Voice
- 3. The Second Generation (2G): Digital Voice & SMS
- 4. Transition (2.5G & 2.75G): GPRS and EDGE
- 5. The Third Generation (3G): Mobile Broadband
- 6. The Fourth Generation (4G): IP-Based High Speed
- 7. The Fifth Generation (5G): IoT and Ultra-Low Latency
- 8. Summary of Generations

Introduction to Mobile Communication

- Mobile communication allows transmission of voice and data to users on the move.
- It relies on electromagnetic waves to transmit signals without physical wires.
- Generations of mobile communication are denoted by 'G' (Generation).
- Each generation introduces significant improvements in data speed, capacity, and technology.

1G: The Analog Era (1980s)

- Introduced in the early 1980s.
- **Technology:** Analog signal transmission.
- **Primary Use:** Voice calls only.
- **Key Standard:** AMPS (Advanced Mobile Phone System).
- **Limitations:**
- - Poor voice quality and high background noise.
- - No data or text messaging capabilities.
- - Very poor security (easily tapped).
- - Large, bulky phones with short battery life.

2G: The Digital Revolution (Early 1990s)

- Introduced in the early 1990s.
- **Technology:** Digital signal transmission (Circuit Switching).
- **Primary Use:** High-quality voice, SMS (Short Message Service), and MMS.
- **Key Standards:** GSM (Global System for Mobile Communications) and CDMA.
- **Improvements over 1G:**
- - Digital encryption (improved security).
- - Better voice clarity and less static.
- - Introduction of the SIM card (in GSM).
- - Lower power consumption.

The Bridge: 2.5G and 2.75G

- Before jumping to 3G, the network needed interim data upgrades.
- **2.5G (GPRS - General Packet Radio Service):**
- - Introduced Packet Switching alongside Circuit Switching.
- - Speeds up to 114 Kbps.
- - Enabled basic web browsing (WAP) and email.
- **2.75G (EDGE - Enhanced Data rates for GSM Evolution):**
- - Pushed 2G technology to its limits.
- - Speeds up to 384 Kbps.
- - Allowed better multimedia transmission.

3G: Mobile Broadband (Early 2000s)

- Introduced around 2001.
- **Technology:** UMTS (Universal Mobile Telecommunications System), WCDMA.
- **Primary Use:** High-speed internet, video calling, mobile TV.
- **Speeds:** 2 Mbps to 21 Mbps (with HSPA).
- **Key Features:**
- - True mobile broadband experience.
- - Always-on data connection.
- - Rise of smartphones (early iPhones and Androids).
- - Heavier focus on data rather than just voice.

4G: The IP Era and LTE (2010s)

- Introduced around 2010.
- **Technology:** LTE (Long Term Evolution) and WiMAX.
- **Architecture:** Entirely IP-based (Packet Switched only).
- **Primary Use:** HD video streaming, online gaming, fast browsing.
- **Speeds:** 100 Mbps to 1 Gbps.
- **Key Features:**
- - Voice over LTE (VoLTE) - Voice calls sent as data packets.
- - Dramatically reduced latency.
- - High spectral efficiency and capacity.

5G: The Era of IoT and Ultra-Low Latency (2020s)

- Currently rolling out globally.
- **Technology:** NR (New Radio), Massive MIMO, Millimeter Wave.
- **Speeds:** Up to 10 Gbps (100x faster than 4G).
- **Key Pillars of 5G:**
- - **eMBB (Enhanced Mobile Broadband):** Blazing fast speeds for VR/AR.
- - **URLLC (Ultra-Reliable Low Latency Comms):** ¡1ms latency for remote surgery, autonomous cars.
- - **mMTC (Massive Machine Type Comms):** Connecting millions of IoT devices per sq km.

Speed and Capability Comparison

- **Downloading a 2-Hour HD Movie (approx. 2GB):**
- - **1G:** Impossible (No data).
- - **2G (GPRS):** ~20 days.
- - **3G:** ~2 hours.
- - **4G:** ~5 to 10 minutes.
- - **5G:** ~10 to 20 seconds.

Summary of Network Architectures

- \- **1G:** Analog, Circuit Switched (Voice).
- \- **2G:** Digital, Circuit Switched (Voice + SMS).
- \- **3G:** Digital, Circuit Switched (Voice) + Packet Switched (Data).
- \- **4G:** Digital, All-IP Packet Switched (Data and Voice over IP).
- \- **5G:** Digital, All-IP, Cloud-native, Network Slicing.

Lecture Summary

- The evolution of mobile communication happens roughly every 10 years.
- **1G:** Analog voice.
- **2G:** Digital voice and text (GSM, CDMA).
- **3G:** Mobile broadband and video calling.
- **4G:** All-IP networks, LTE, and HD streaming.
- **5G:** IoT, autonomous systems, and ultra-low latency.

Next Lecture Preview

- Now that we know the history, how do these networks actually cover large areas?
- In the next lecture, we will cover:
- **1.2 Basic Cellular Concept and Cellular System**
- - Why do we use 'cells'?
- - How frequency allocation works.
- - The basic architecture of a cellular system.

Lecture 2: 1.2 Basic cellular concept and cellular system

Fundamental of Cellular Communication

DI05011011: Mobile Communication

Agenda for Today

- 1. The Problem with Early Mobile Radios
- 2. What is the Cellular Concept?
- 3. Shape of a Cell (Why Hexagons?)
- 4. Components of a Cellular System
- 5. The Base Station (BS) & Mobile Station (MS)
- 6. Mobile Switching Center (MSC)
- 7. Advantages of the Cellular System
- 8. Summary

The Problem with Early Mobile Radios

- Before cellular systems, Mobile Telephone Systems (MTS) used a single high-power transmitter to cover a large city (e.g., 50 km radius).
- **Limitations:**
- - **Limited Capacity:** Only a few dozen channels were available. If 50 people were talking, the 51st person couldn't make a call.
- - **High Power:** Mobile devices needed huge batteries and high transmission power to reach the central tower.
- - **Inefficient Frequency Use:** A frequency used by one user couldn't be used by anyone else in the entire city.

What is the Cellular Concept?

- Instead of one large area with a high-power transmitter, the city is divided into smaller geographic areas called **Cells**.
- Each cell is served by its own low-power transmitter (Base Station).
- **Key Idea:** Since the transmitter power is low, the radio signal doesn't travel far.
- Therefore, the same frequency channels can be reused in a different cell some distance away without causing interference.

The Shape of a Cell

- In reality, a cell's footprint is irregular, determined by terrain, buildings, and antenna design.
- For mathematical modeling and design, we need a regular geometric shape.
- **Options considered:** Circle, Square, Equilateral Triangle, Hexagon.
- - **Circles:** Leave gaps or overlap too much.
- - **Squares & Triangles:** Don't approximate an omnidirectional antenna's radiation pattern well.
- - **Hexagon:** Best approximation of a circle, covers area without gaps or overlaps.

Visualizing the Hexagonal Grid

- Imagine a honeycomb structure.
- Each hexagon represents one cell.
- At the center (or corners) of the hexagon sits the Base Station antenna.
- The distance from the center to any vertex is the cell radius (R).
- This grid allows engineers to calculate distances between towers and manage interference systematically.

Basic Components of a Cellular System

- A cellular network consists of three main components:
- 1. **Mobile Station (MS):** The user's device (smartphone).
- 2. **Base Station (BS):** The cell tower that communicates with the MS via radio waves.
- 3. **Mobile Switching Center (MSC):** The brain of the network that connects base stations to each other and to the public telephone network.

1. Mobile Station (MS)

- The mobile device used by the subscriber.
- Consists of two parts:
- - **Mobile Equipment (ME):** The hardware (radio transceiver, display, processor).
- - **Subscriber Identity Module (SIM):** A smart card containing the user's subscription details, security keys, and phone number.
- The MS continuously monitors the signal strength of nearby Base Stations to ensure connection.

2. Base Station (BS)

- Also called Base Transceiver Station (BTS).
- Located at the center or edge of a cell.
- Contains transmitters, receivers, and antennas.
- Functions:
- - Provides the radio interface to the Mobile Station.
- - Allocates radio channels to the mobile device for calls.
- - Monitors signal quality and relays data to the MSC.

3. Mobile Switching Center (MSC)

- The central coordinating element for all Base Stations in a given area.
- Also known as the Mobile Telephone Switching Office (MTSO).
- Functions:
- - Sets up and routes calls between users.
- - Connects cellular calls to the PSTN (Public Switched Telephone Network - landlines).
- - Manages mobility: tracks where the user is and handles handoffs when moving between cells.
- - Handles billing and authentication.

Advantages of the Cellular System

- **1. Higher Capacity:** Frequency reuse allows millions of users to be supported on a limited spectrum.
- **2. Lower Power Consumption:** Mobile phones only need enough power to reach the nearest cell tower (1-5 km), drastically saving battery life.
- **3. Scalability:** As demand grows, cells can be split into smaller cells to add more capacity.
- **4. Decentralization:** If one Base Station fails, only that small cell goes down, not the whole city.

Lecture Summary

- Cellular systems replaced single high-power towers with a grid of low-power Base Stations.
- Hexagons are used for theoretical modeling because they cover areas without gaps.
- The core architecture consists of the Mobile Station (MS), Base Station (BS), and Mobile Switching Center (MSC).
- The cellular concept revolutionized mobile capacity and device battery life.

Next Lecture Preview

- Are all cells the same size?
- In the next lecture, we will explore:
- **1.3 Cell types: Macro, Micro, Pico, Selective and Umbrella cell**
- - How cell sizes vary based on user density.
- - Different types of cells for rural vs. urban vs. indoor environments.

Lecture 3: 1.3 Cell types: Macro, Micro, Pico, Selective and Umbrella cell

Fundamental of Cellular Communication

DI05011011: Mobile Communication

Agenda for Today

- 1. Why do we need different cell sizes?
- 2. Macro Cells: Wide Area Coverage
- 3. Micro Cells: Urban Capacity
- 4. Pico Cells & Femto Cells: Indoor & Targeted Coverage
- 5. Selective Cells: Directed Coverage
- 6. Umbrella Cells: Managing Fast-Moving Users
- 7. Comparison of Cell Types
- 8. Summary

Why Different Cell Sizes?

- A cellular network must serve varying landscapes and user densities:
- - **Rural areas:** Few users over vast distances. Need large coverage to save cost.
- - **Urban areas:** Dense population. A large cell would run out of capacity instantly.
- - **Indoors:** Radio waves from outdoor towers struggle to penetrate large buildings.
- **Solution:** Vary the transmission power and antenna height to create cells of different sizes tailored to the specific environment.

1. Macro Cell

- **Coverage:** 1 km to 30 km radius.
- **Location:** Rural areas, highways, and suburbs.
- **Antenna Placement:** High up on tall towers, hills, or tall building roofs.
- **Transmitter Power:** High (tens of Watts).
- **Characteristics:**
- - Provides basic wide-area coverage.
- - Low capacity per square kilometer.
- - Good for fast-moving users (e.g., cars on a highway) as it minimizes handoffs.

2. Micro Cell

- **Coverage:** 200 meters to 1 km radius.
- **Location:** Dense urban areas, city centers, shopping districts.
- **Antenna Placement:** Below rooftop level, on streetlamps, utility poles, or side of buildings.
- **Transmitter Power:** Medium/Low.
- **Characteristics:**
- - Designed to increase network capacity in crowded areas.
- - Overcomes blocking by tall city buildings.
- - Relies heavily on frequency reuse over small distances.

3. Pico Cell

- **Coverage:** 4 to 200 meters.
- **Location:** Indoors, airports, train stations, large office buildings, malls.
- **Antenna Placement:** Inside buildings, on ceilings or walls.
- **Transmitter Power:** Very Low.
- **Characteristics:**
- - Fills in 'dead zones' where outdoor macro/micro signals cannot penetrate.
- - Handles extremely dense, localized traffic (e.g., thousands of people waiting in an airport terminal).

Femto Cell (Bonus Context)

- **Coverage:** ~10 meters.
- **Location:** Homes or small businesses.
- **Characteristics:**
- - Essentially a personal base station.
- - Connects to the mobile operator's network via the user's home broadband internet (DSL/Fiber).
- - Used to solve severe indoor coverage issues in residential areas.
- - Extremely low power, basically the size of a Wi-Fi router.

4. Selective Cell

- Not defined merely by size, but by the *shape* of coverage.
- **Concept:** Using directional antennas to shape coverage into specific sectors rather than a 360-degree circle/hexagon.
- **Location:** Tunnels, valleys, long corridors, or edges of a network.
- **Characteristics:**
- - Focuses radio energy only where it's needed.
- - Reduces interference in unwanted directions.
- - Example: A cell specifically pointing down a highway, rather than radiating into empty fields.

5. Umbrella Cell Concept

- **The Problem:** In a city full of small micro cells, a fast-moving car will have to switch (handoff) from cell to cell every few seconds, straining the network.
- **The Solution:** The Umbrella Cell.
- - A large Macro cell (the Umbrella) is overlaid on top of several Micro cells.
- - **Slow users (pedestrians):** Handled by the Micro cells for high capacity.
- - **Fast users (cars):** Handled by the large Umbrella cell to minimize frequent handoffs.

Visualizing the Umbrella Cell

- - Imagine a large circle (Umbrella Cell) covering a 5km radius.
- - Inside that circle, there are 20 small hexagons (Micro Cells).
- - The system uses speed estimation:
- - User in a car -¿ Assigned to Umbrella Cell.
- - User sitting in a cafe -¿ Assigned to Micro Cell.
- - Result: Reduced switching load on the Mobile Switching Center (MSC).

Comparison Summary Table

- — Cell Type — Coverage Radius — Environment — Transmit Power —
- ————————————————————————-—————————-——
- — Macro — 1 - 30 km — Rural / Hwy — High —
- — Micro — 0.2 - 1 km — Urban — Medium —
- — Pico — 4 - 200 m — Indoors — Low —
- — Femto — ˜10 m — Home — Very Low —

Lecture Summary

- Networks use a mix of cell sizes to balance coverage, capacity, and cost.
- **Macro cells:** Large coverage, low capacity, rural areas.
- **Micro/Pico cells:** Small coverage, high capacity, urban/indoor areas.
- **Selective cells:** Custom-shaped coverage using directional antennas.
- **Umbrella cells:** Macro cells overlapping micro cells to serve fast-moving users and reduce handoffs.

Next Lecture Preview

- Now that we know what a cell is, how do we arrange them together without their frequencies interfering with each other?
- In the next lecture, we will cover:
- **1.4 Explain concept of cluster**
- - Grouping cells together.
- - Rules of frequency reuse within a cluster.

Lecture 4: 1.4 Explain concept of cluster

Fundamental of Cellular Communication

DI05011011: Mobile Communication

Agenda for Today

- 1. The Frequency Allocation Problem
- 2. What is a Cluster?
- 3. Characteristics of a Cluster
- 4. Determining Cluster Size (N)
- 5. The Magic Numbers of Cellular Design
- 6. Concept of Co-channel Cells
- 7. Visualizing a Cluster
- 8. Summary

The Frequency Allocation Problem

- A network operator (like AT&T or Vodafone) buys a limited block of radio spectrum from the government.
- This spectrum is divided into a finite number of voice/data channels (denoted as 'S').
- **The Problem:** If two adjacent cells use the exact same frequency channel, their signals will collide, causing severe interference.
- **The Solution:** We must distribute these 'S' channels among a group of cells in such a way that neighboring cells never use the same frequency.

What is a Cluster?

- A **Cluster** is a group of adjacent cells that collectively use the entire allocated frequency spectrum.
- If a cluster has 'N' cells, the total available channels (S) are divided among these N cells.
- Channels per cell (k) = S / N.
- Inside a single cluster, no two cells share the same frequency. This ensures zero interference within the cluster.

Characteristics of a Cluster

- **1. Completeness:** A cluster contains all the frequency channels available to the system.
- **2. Uniqueness:** Frequencies are not repeated within a single cluster.
- **3. Tesselation:** Clusters must interlock perfectly with other clusters of the same size to cover a large geographic area without gaps.
- **4. Size (N):** The number of cells in a cluster is denoted by N. Common sizes are 3, 4, 7, 12, etc.

Determining Cluster Size (N)

- Because cells are modeled as hexagons, we cannot just arbitrarily choose a cluster size (N).
- To ensure that clusters fit together without gaps, N must satisfy the following geometric equation:
- $\mathbf{N = i^2 + ij + j^2}$
- Where:
- - 'i' and 'j' are non-negative integers (0, 1, 2, 3...).
- - They represent the number of steps taken along the hexagonal grid to find the next nearest co-channel cell.

The 'Magic Numbers' of Cellular Design

- Let's calculate possible cluster sizes using $N = i^2 + ij + j^2$:
- - If i=1, j=1: $N = (1)^2 + (1)(1) + (1)^2 = 1 + 1 + 1 = \mathbf{3}$
- - If i=2, j=0: $N = (2)^2 + (2)(0) + (0)^2 = \mathbf{4}$
- - If i=2, j=1: $N = (2)^2 + (2)(1) + (1)^2 = 4 + 2 + 1 = \mathbf{7}$
- - If i=3, j=0: $N = (3)^2 + (3)(0) + (0)^2 = \mathbf{9}$
- - If i=2, j=2: $N = (2)^2 + (2)(2) + (2)^2 = 4 + 4 + 4 = \mathbf{12}$
- Therefore, valid cluster sizes (N) are: 3, 4, 7, 9, 12, 19, etc.

Concept of Co-channel Cells

- Once a cluster uses all the frequencies, the pattern is repeated geographically.
- A cell in Cluster 1 that uses 'Frequency Group A' will have a counterpart in Cluster 2 that also uses 'Frequency Group A'.
- These two cells are called **Co-channel Cells**.
- The design goal is to ensure that the distance between co-channel cells is large enough so their radio waves don't interfere with each other.

How to Locate Co-channel Cells

- To find a co-channel cell in a neighboring cluster using the 'i' and 'j' parameters:
- 1. Start at the center of the original cell.
- 2. Move 'i' cells across the centers of adjacent hexagons.
- 3. Turn 60 degrees counter-clockwise.
- 4. Move 'j' cells forward.
- You have now landed exactly on the nearest co-channel cell!

Visualizing a 7-Cell Cluster

- \- Imagine a central hexagon (Cell A).
- \- It is completely surrounded by 6 other hexagons (Cells B, C, D, E, F, G).
- \- This forms a relatively circular block of 7 cells.
- \- This block can seamlessly connect with another identical 7-cell block, covering a city map like perfectly laid floor tiles.
- \- Frequency 'A' in the first block is physically separated from Frequency 'A' in the second block by at least two other cells.

Trade-offs in Cluster Size (N)

- **Small Cluster Size (e.g., N = 3 or 4):**
- - **Pros:** High capacity. The total spectrum 'S' is divided into fewer groups, so each cell gets more channels.
- - **Cons:** Co-channel cells are physically closer together, increasing interference.
-
- **Large Cluster Size (e.g., N = 7 or 12):**
- - **Pros:** Co-channel cells are farther apart, meaning less interference and better call quality.
- - **Cons:** Lower capacity. The spectrum 'S' is divided into many groups, so each cell gets fewer channels.

Lecture Summary

- A cluster is a group of 'N' cells that collectively use the entire frequency spectrum available to the operator.
- Frequencies are unique within a cluster (no interference).
- Cluster sizes are determined by the equation $N = i^2 + ij + j^2$.
- Valid cluster sizes include 3, 4, 7, 9, and 12.
- Cells in different clusters using the same frequencies are called Co-channel cells.
- Cluster size dictates the trade-off between network capacity and interference.

Next Lecture Preview

- Now that we know how frequencies are grouped into clusters, how do we reuse them across a whole city to increase capacity?
- In the next lecture, we will cover:
- **1.5 Frequency reuse and system capacity**
- - The core concept of frequency reuse.
- - Mathematical formulas to calculate total system capacity (C).
- - How frequency reuse makes cellular networks scalable.

Lecture 5: 1.5 Frequency reuse and system capacity

Fundamental of Cellular Communication

DI05011011: Mobile Communication

Agenda for Today

- 1. What is Frequency Reuse?
- 2. The Frequency Reuse Factor
- 3. Defining System Capacity
- 4. Mathematical Formulation of Capacity
- 5. Example Calculation 1
- 6. Example Calculation 2
- 7. Impact of Cluster Size on Capacity
- 8. Summary

What is Frequency Reuse?

- Spectrum is scarce and expensive.
- **Frequency Reuse** is the process of using the exact same radio frequencies repeatedly in different geographic areas.
- As long as the coverage areas (cells) are far enough apart, the radio signals will decay over distance and won't interfere with each other.
- This allows a network to provide service to millions of users using only a few hundred channels.

The Frequency Reuse Factor

- In a cluster of 'N' cells, the total available spectrum is divided into N groups.
- Each cell in the cluster uses exactly **1/N** of the total available channels.
- Therefore, the **Frequency Reuse Factor** is defined as **1/N**.
- - For a 7-cell cluster, the frequency reuse factor is $1/7$.
- - For a 4-cell cluster, the factor is $1/4$.
- This factor tells us what fraction of the total spectrum is allocated to a single cell.

Defining System Capacity

- **System Capacity (C)** is the total number of simultaneous calls or data connections a cellular network can handle.
- It depends on:
- 1. The total number of channels allocated by the government (S).
- 2. The number of times the cluster is replicated across the geographic area (M).
- If you want to increase capacity, you either need more spectrum (hard/expensive) or you need to reuse your existing spectrum more times (M).

Mathematical Formulation of Capacity

- Let's define the variables:
- - **S:** Total number of channels available to the operator.
- - **N:** Cluster size (number of cells in a cluster).
- - **k:** Number of channels per cell (k = S / N).
- - **M:** Number of times the cluster is repeated over the coverage area.
- - **C:** Total system capacity.
- **Formula 1:** Total channels in a cluster = k * N = S
- **Formula 2:** Total System Capacity = M k N
- **Simplified:** C = M * S

Example Calculation 1

- **Scenario:**
- - An operator has a total of 700 channels ($S = 700$).
- - They design a system using a 7-cell cluster ($N = 7$).
- **Questions:**
- 1. How many channels does each cell get?
- 2. If the cluster is repeated 10 times across a city, what is the total system capacity?
- **Answers:**
- 1. Channels per cell (k) $= S / N = 700 / 7 = 100$ channels/cell.
- 2. Total Capacity (C) $= M * S = 10\ 700 = 7{,}000$ simultaneous users.

Example Calculation 2: Splitting Cells

- **Scenario:** The city from Example 1 grows rapidly. The operator needs more capacity but has no more spectrum.
- **Solution:** Make the cells smaller (Cell Splitting).
- - Original: 10 clusters (M = 10). Capacity = 7,000.
- - New Design: By cutting the cell radius in half, the same city area can now fit 40 smaller clusters (M = 40).
- **New Capacity:**
- - C = M $S = 40$ 700 = **28,000 simultaneous users.**

Impact of Cluster Size (N) on Capacity

- Let's look at capacity from the perspective of an individual cell.
- Channels per cell: **k = S / N**
- For a fixed total spectrum (S), if we *decrease* the cluster size (N), the number of channels per cell (k) *increases*.
- - e.g., S=700. If N=7, k=100. If N=4, k=175.
- Therefore, smaller cluster sizes provide higher capacity per cell.
- **But remember:** Smaller N means co-channel cells are closer together, increasing interference.

How to Increase Capacity? (Summary of Strategies)

- If a cellular network gets congested, engineers can:
- **1. Add new channels:** (Obtain more spectrum 'S' from the government - Very expensive).
- **2. Borrow channels:** (Dynamic channel allocation - complex to manage).
- **3. Cell Splitting:** (Reduce cell radius, build more base stations to increase 'M' - High infrastructure cost).
- **4. Cell Sectoring:** (Use directional antennas to reduce interference, allowing a smaller 'N' to be used).

Lecture Summary

- Frequency Reuse allows the same spectrum to be used repeatedly across a geographic area.
- The Frequency Reuse Factor is 1/N, representing the fraction of spectrum allocated per cell.
- Total System Capacity (C) is calculated as $C = M * S$.
- Capacity can be drastically increased by reducing cell sizes (increasing M).
- Decreasing cluster size (N) increases capacity but risks higher interference.

Next Lecture Preview

- We mentioned that reusing frequencies causes interference. What exactly is this interference?
- In the next lecture, we will cover:
- **1.6 Co-channel and adjacent channel interference**
- - Understanding Co-channel interference (CCI).
- - Understanding Adjacent channel interference (ACI).
- - How to calculate the Signal-to-Interference Ratio (SIR).

Lecture 6: 1.6 Co-channel and adjacent channel interference

Fundamental of Cellular Communication

DI05011011: Mobile Communication

Agenda for Today

- 1. Introduction to Interference
- 2. Concept of Co-channel Interference (CCI)
- 3. Signal to Interference Ratio (SIR)
- 4. Mitigating Co-channel Interference
- 5. Concept of Adjacent Channel Interference (ACI)
- 6. Near-Far Effect
- 7. Mitigating Adjacent Channel Interference
- 8. Comparing CCI and ACI
- 9. Summary and Next Steps

What is Interference?

- Interference is the major limiting factor in the performance of cellular radio systems.
- It causes crosstalk, noise, and dropped calls.
- Sources of interference:
- - Another mobile in the same cell
- - A call in progress in a neighboring cell
- - Other base stations operating in the same frequency band
- - Non-cellular systems leaking energy into the cellular frequency band

Co-Channel Interference (CCI)

- Frequency reuse implies that in a given coverage area, there are several cells that use the same set of frequencies.
- These cells are called co-channel cells.
- Interference between signals from these co-channel cells is called co-channel interference.
- CCI cannot be combated by simply increasing the carrier power of a transmitter.

Visualizing Co-Channel Cells

- Consider a cellular cluster of size $N = 7$.
- Cell 'A' in the center cluster uses frequency set 1.
- The first tier of co-channel cells (also using frequency set 1) surrounds the center cluster.
- There are 6 equidistant co-channel cells in the first tier.
- These 6 cells are the primary source of co-channel interference for Cell 'A'.

Signal to Interference Ratio (SIR)

- Quality of a voice channel is determined by the Signal-to-Interference Ratio (SIR).
- SIR = S / I, where S is the desired signal power, and I is the interference power.
- For a mobile unit, I = sum of interference from all co-channel cells.
- In a fully equipped hexagonal grid, there are 6 primary co-channel interferers.
- SIR is heavily dependent on the ratio D/R (co-channel reuse ratio).

Co-Channel Reuse Ratio (Q)

- The co-channel reuse ratio, Q, is defined as Q = D / R.
- Where D is the distance to the nearest co-channel cell, and R is the cell radius.
- For hexagonal geometry, Q = sqrt(3 * N).
- A small Q means small cluster size (N), leading to higher capacity but lower SIR (more interference).
- A large Q means larger cluster size, lower capacity, but higher SIR (better quality).

Calculating SIR Requirements

- Assume a system requires an SIR of 18 dB for acceptable voice quality.
- Using propagation models, we can relate SIR to Q.
- If SIR = (sqrt(3N))^4 / 6 (assuming path loss exponent n=4).
- Solving for N, we find that N=7 provides an SIR of approximately 18.66 dB.
- Therefore, a cluster size of N=7 is often chosen as a baseline for acceptable CCI.

Adjacent Channel Interference (ACI)

- Interference resulting from signals which are adjacent in frequency to the desired signal.
- Results from imperfect receiver filters which allow nearby frequencies to leak into the passband.
- Most severe when an adjacent channel user is transmitting in close proximity to a receiver while the receiver attempts to receive a signal from a distant station.

The Near-Far Effect

- ACI becomes a severe problem due to the 'Near-Far Effect'.
- Scenario: A mobile close to the base station is transmitting on a channel adjacent to a mobile far from the base station.
- The base station receives a very strong signal from the near mobile and a very weak signal from the far mobile.
- The strong signal can 'bleed' through the filter and drown out the weak desired signal.

Mitigating Adjacent Channel Interference

- 1. Precise Filtering: Better receiver filters with sharp cutoffs reduce leakage.
- 2. Channel Assignment: Do not assign adjacent channels to the same cell.
- - E.g., if a cell uses channel 1, do not assign channels 2 or 3 to the same cell.
- - Maximize frequency separation between channels in the same cell.
- 3. Power Control: Force mobile units to adjust their transmit power based on distance to the base station.

CCI vs. ACI

- **Co-Channel (CCI):**
- - Same frequency.
- - Caused by frequency reuse in different cells.
- - Mitigated by increasing cluster size (N) or distance (D).
- **Adjacent Channel (ACI):**
- - Neighboring frequency.
- - Caused by imperfect filtering and near-far effect.
- - Mitigated by channel allocation and power control.

Lecture Summary

- Interference limits capacity and quality in cellular systems.
- Co-channel interference arises from reusing the same frequencies in distant cells.
- CCI is managed by controlling the D/R ratio (cluster size).
- Adjacent channel interference comes from signals on nearby frequencies leaking through filters.
- ACI is exacerbated by the near-far effect.
- ACI is managed through clever channel assignment and strict power control.

Next Lecture Preview

- In the next lecture, we will discuss Channel Assignment Strategies:
- 1. Fixed Channel Assignment (FCA)
- 2. Dynamic Channel Assignment (DCA)
- 3. How to allocate our precious frequency resources efficiently to manage traffic and minimize interference.

Lecture 7: 1.7 Channel assignment strategies

Fundamental of Cellular Communication

DI05011011: Mobile Communication

Agenda for Today

- 1. Why Channel Assignment?
- 2. Goals of Channel Assignment
- 3. Fixed Channel Assignment (FCA)
- 4. Borrowing Strategies in FCA
- 5. Dynamic Channel Assignment (DCA)
- 6. Advantages and Disadvantages of DCA
- 7. Comparison: FCA vs DCA
- 8. Summary and Next Steps

The Need for Channel Assignment

- The frequency spectrum allocated for cellular communication is strictly limited.
- To maximize capacity and minimize interference, this spectrum must be managed efficiently.
- When a user makes a call, the system must assign a specific radio channel for that communication.
- The strategy used to allocate these channels significantly impacts the system's overall capacity and call blocking probability.

Goals of Channel Assignment

- 1. Maximize spectrum utilization (serve as many users as possible).
- 2. Minimize the probability of a blocked call (user getting a 'busy' signal).
- 3. Minimize the probability of a dropped call (losing connection mid-conversation).
- 4. Maintain acceptable Signal-to-Interference Ratio (SIR) by managing co-channel and adjacent channel interference.

Types of Channel Assignment

- Channel assignment strategies can be broadly classified into two categories:
- **1. Fixed Channel Assignment (FCA):** Channels are permanently allocated to specific cells.
- **2. Dynamic Channel Assignment (DCA):** Channels are not allocated to cells permanently but are pooled and assigned on demand.

Fixed Channel Assignment (FCA)

- In FCA, each cell is allocated a predetermined set of voice channels.
- Any call attempt within the cell can only be served by the unused channels in that specific cell.
- If all channels in that cell are occupied, the call is blocked (user receives a busy signal).
- The assignment is done based on expected traffic patterns during network planning.

FCA: Channel Borrowing

- To handle sudden spikes in traffic, FCA is often augmented with a 'borrowing' strategy.
- If a cell's channels are full, the base station can request (borrow) a free channel from a neighboring cell.
- The Mobile Switching Center (MSC) supervises this borrowing process.
- Borrowed channels are locked in the donor cell to prevent co-channel interference.

Example: FCA with Borrowing

- Cell A is assigned channels 1-10. Cell B is assigned channels 11-20.
- Currently, 10 active calls are in Cell A. Channel 1-10 are busy.
- An 11th user tries to make a call in Cell A.
- Cell A's Base Station requests MSC to borrow a channel.
- MSC sees Cell B has channel 20 free. MSC assigns Channel 20 to the user in Cell A.
- Channel 20 cannot be used by Cell B until the call in Cell A finishes.

Dynamic Channel Assignment (DCA)

- In DCA, channels are not allocated to cells on a permanent basis.
- Instead, all channels are kept in a central pool maintained by the MSC.
- When a call request arrives, the Base Station requests a channel from the MSC.
- The MSC assigns a channel based on an algorithm that evaluates current interference levels and channel usage.

DCA Mechanism

- When MSC receives a request, it checks for available channels in the pool.
- It evaluates candidate channels to ensure assigning them won't violate the minimum required Signal-to-Interference Ratio (SIR).
- If a channel meets the criteria, it is assigned.
- When the call ends, the channel is immediately returned to the central pool.

Advantages of DCA

- **1. Increased Efficiency:** Better utilization of spectrum, especially under varying or uneven traffic loads.
- **2. Lower Call Blocking:** Significantly reduces the probability of blocked calls during unexpected peaks.
- **3. No Need for Precise Planning:** Less upfront effort required for frequency planning compared to FCA.

Disadvantages of DCA

- **1. High Computational Load:** MSC must perform complex calculations for every call request in real-time.
- **2. Increased Signaling:** Constant communication between Base Stations and the MSC to update channel status.
- **3. Delay:** The time taken to calculate and assign a channel can introduce setup delays for the call.

FCA vs. DCA Summary

- — Feature — Fixed (FCA) — Dynamic (DCA) —
- — :— — :— — :— —
- — Allocation — Permanent to cell — Central pool —
- — Flexibility — Low (without borrowing) — High —
- — Complexity — Low — High —
- — Signaling Overhead — Low — High —
- — Best For — Uniform, predictable traffic — Bursty, unpredictable traffic —

Lecture Summary

- Channel assignment is necessary to manage limited spectrum efficiently.
- FCA permanently assigns channels to cells based on predicted traffic.
- FCA can use borrowing to handle unexpected traffic spikes.
- DCA pools all channels and assigns them on-demand based on real-time conditions.
- DCA handles varied traffic better but requires more processing and signaling overhead than FCA.

Next Lecture Preview

- In the next lecture, we will explore techniques to increase network capacity:
- **Cell Splitting and Sectoring:**
- 1. How to divide cells when they become congested.
- 2. Using directional antennas to reduce interference.
- 3. Methods to accommodate more users in a growing network.

Lecture 8: 1.8 Cell splitting and sectoring

Fundamental of Cellular Communication

DI05011011: Mobile Communication

Agenda for Today

- 1. The Need for Capacity Expansion
- 2. Concept of Cell Splitting
- 3. Mechanics of Cell Splitting
- 4. Advantages and Drawbacks of Splitting
- 5. Concept of Sectoring
- 6. Antenna Configurations in Sectoring (120° and 60°)
- 7. Impact of Sectoring on Interference (SIR)
- 8. Comparing Splitting and Sectoring
- 9. Summary and Next Steps

The Need for Capacity Expansion

- As cellular systems mature, traffic demand increases.
- Eventually, all available channels in a given cell will be occupied, leading to high call blocking rates.
- Adding new frequency spectrum is often impossible or prohibitively expensive.
- Solution: We must reuse the existing spectrum more frequently in the same geographical area.

What is Cell Splitting?

- Cell splitting is the process of subdividing a congested cell into smaller cells (microcells).
- Each new smaller cell has its own base station with a reduced antenna height and reduced transmitter power.
- By making cells smaller, the same number of channels is available over a smaller geographical area.
- This drastically increases the number of channels available per square kilometer (capacity).

Mechanics of Cell Splitting

- Original cell radius: R.
- New split cell radius is typically: R / 2.
- Since Area is proportional to R squared, the new cell area is 1/4th the original area.
- Therefore, one original cell is replaced by four smaller cells.
- Capacity increases theoretically by a factor of 4 in that area.

Adjusting Power in Cell Splitting

- When a cell is split, the transmission power must be reduced to avoid co-channel interference with neighboring cells.
- If radius is reduced from R to R/2, the transmit power is reduced.
- Assuming a path loss exponent of n=4, the new power is roughly 1/16th of the original power.
- Formula: P_new = P_old * (R_new / R_old)^n

Pros and Cons of Cell Splitting

- **Advantages:**
- - Massive increase in system capacity.
- - Solves severe congestion in urban hotspots.
- **Disadvantages:**
- - Very high cost: requires purchasing new real estate and installing new base stations.
- - Handoff issues: smaller cells mean mobiles cross boundaries more often, requiring more handoffs and processing.

What is Sectoring?

- Sectoring increases capacity by keeping the cell radius the same but replacing a single omni-directional antenna with several directional antennas.
- A single cell is divided into sectors (e.g., 3 sectors of 120° or 6 sectors of 60°).
- Each sector acts like a distinct cell and uses a portion of the cell's allocated channels.
- Primary goal: Reduce co-channel interference to allow for a smaller cluster size (N).

How Sectoring Reduces Interference

- Recall that with an omnidirectional antenna, a mobile receives interference from all 6 surrounding co-channel cells.
- With 120° sectoring, the antenna only 'looks' in one direction.
- The mobile now only receives interference from 2 of the 6 co-channel cells (those facing the same direction).
- With 60° sectoring, interference is reduced to just 1 co-channel cell.

Sectoring and Capacity (The Catch)

- Sectoring improves the Signal-to-Interference Ratio (SIR).
- Higher SIR allows network planners to use a smaller cluster size (e.g., reducing N from 7 to 4 or 3).
- A smaller cluster size means frequencies are reused more often across the network.
- More frequent reuse $=$ Higher overall system capacity.

Pros and Cons of Sectoring

- **Advantages:**
- - Improves SIR significantly.
- - Cheaper than cell splitting (no new real estate needed, just new antennas).
- **Disadvantages:**
- - Decreases trunking efficiency (channels are partitioned into smaller pools per sector).
- - Increases handoffs (mobiles now handoff between sectors of the same cell).

Comparison: Splitting vs Sectoring

- — Feature — Cell Splitting — Sectoring —
- — :— — :— — :— —
- — Mechanism — Reduces cell radius (R) — Uses directional antennas —
- — Number of Base Stations — Increases — Remains the same —
- — Cost — Very High (New sites) — Low to Medium (New antennas) —
- — Primary Effect — Direct capacity increase — Improves SIR, leading to smaller N —
- — Handoffs — Increased (Inter-cell) — Increased (Intra-cell and Inter-cell) —

Lecture Summary

- When networks run out of capacity, we must manipulate geometry to reuse frequencies more often.
- Cell splitting reduces cell radius, massively increasing capacity but requiring expensive new base stations.
- Transmit power must be carefully reduced when splitting cells.
- Sectoring uses directional antennas to reduce co-channel interference.
- Reduced interference allows for smaller cluster sizes, which increases overall capacity.
- Both methods increase the frequency of handoffs.

Next Lecture Preview

- In the next lecture, we will dive into Handoffs:
- 1. What exactly happens when you move from one cell to another?
- 2. Soft vs. Hard handoffs.
- 3. How the network ensures your call doesn't drop while driving.

Lecture 9: 1.9 Define handoff and differentiate various Handoff techniques

Fundamental of Cellular Communication

DI05011011: Mobile Communication

Agenda for Today

- 1. Definition of Handoff
- 2. Why Handoffs are Necessary
- 3. Handoff Initiation (When to handoff?)
- 4. Signal Strength and Thresholds
- 5. Hard Handoff ('Break before make')
- 6. Soft Handoff ('Make before break')
- 7. Mobile Assisted Handoff (MAHO)
- 8. Practical Handoff Problems (Ping-pong effect)
- 9. Summary and Next Steps

What is a Handoff (Handover)?

- A handoff (or handover) is the process of transferring an active call or data session from one cell (or base station) to another.
- It occurs without disconnecting the ongoing session.
- It is required when a mobile user travels out of the coverage area of one cell and enters another.
- The system must allocate a new voice/data channel in the new cell for the call to continue.

Handoff Initiation Parameters

- How does the network know when to trigger a handoff?
- It constantly monitors the Received Signal Strength Indicator (RSSI) from the mobile.
- **Threshold 1 (Minimum Acceptable):** The minimum signal level required to maintain a call (e.g., -100 dBm). If it drops below this, the call drops.
- **Threshold 2 (Handoff Threshold):** A level slightly above the minimum acceptable level. When signal hits this, the handoff process begins.

The Handoff Margin (Delta)

- The difference between the Handoff Threshold and the Minimum Acceptable Signal is called the Margin (Delta).
- **Delta = P_handoff - P_minimum_acceptable**
- - If Delta is too large: Handoffs occur too early, burdening the MSC with unnecessary processing.
- - If Delta is too small: Handoffs occur too late, and calls drop before the handoff completes.
- Engineers must carefully tune this margin based on user speeds (highway vs. pedestrian).

Hard Handoff

- Also known as **'Break before make'**.
- The connection to the current base station is completely broken before the connection to the new base station is established.
- There is a brief, unnoticeable interruption in the call.
- Typically used in systems where different cells use different frequencies (like FDMA/TDMA in GSM).
- A mobile cannot tune to two different frequencies simultaneously with a standard receiver.

Soft Handoff

- Also known as **'Make before break'**.
- The connection to the new base station is established before the connection to the old base station is broken.
- The mobile is simultaneously connected to two (or more) base stations for a brief period.
- Used primarily in CDMA (and 3G) systems where all cells share the same frequency band.

Softer Handoff

- A specialized version of Soft Handoff.
- Occurs when a mobile moves from one sector of a cell to another sector of the *same* cell.
- The handoff is handled entirely by the single Base Station, without needing the MSC's involvement.
- Highly efficient and fast.

Mobile Assisted Handoff (MAHO)

- In older systems (1G), the Base Station measured the mobile's signal and initiated the handoff.
- In modern systems (2G onwards), we use MAHO.
- The mobile handset continuously measures the signal strength of neighboring base stations.
- It periodically sends these reports back to its current base station.
- The network uses the mobile's measurements to decide when and where to handoff.

Handoff Problems: The Ping-Pong Effect

- Occurs when a user is on the boundary between two cells.
- Due to fading and environmental obstacles, the signal strength fluctuates rapidly.
- The system might repeatedly hand the call back and forth between Cell A and Cell B.
- This causes massive signaling overhead and can degrade call quality.

Mitigating the Ping-Pong Effect

- **Solution:** Hysteresis.
- Instead of just handing off when Cell B is stronger than Cell A, the system requires Cell B to be stronger by a certain margin (Hysteresis Margin) for a specific duration.
- Example: Handoff only if (Signal_B ¿ Signal_A + 3dB).
- This prevents handoffs based on momentary signal spikes.

Lecture Summary

- Handoffs allow mobile users to maintain connections while crossing cell boundaries.
- Initiated based on signal strength dropping below a specific threshold (plus a margin).
- Hard handoff breaks the old connection before making the new one (FDMA/TDMA).
- Soft handoff makes the new connection before breaking the old one (CDMA).
- MAHO utilizes the handset to measure neighboring signals, improving efficiency.
- Hysteresis is used to prevent the ping-pong effect at cell boundaries.

Next Lecture Preview

- In the next lecture, we conclude Unit 1 by looking at Multiple Access Techniques:
- How do hundreds of users share the same cell tower simultaneously?
- 1. FDMA (Frequency Division)
- 2. TDMA (Time Division)
- 3. CDMA (Code Division)
- 4. SDMA (Space Division)

Lecture 10: 1.10 Multiple Access Techniques: FDMA, TDMA, CDMA, SDMA

Fundamental of Cellular Communication

DI05011011: Mobile Communication

Agenda for Today

- 1. What is Multiple Access?
- 2. The Cocktail Party Analogy
- 3. Frequency Division Multiple Access (FDMA)
- 4. Time Division Multiple Access (TDMA)
- 5. Code Division Multiple Access (CDMA)
- 6. Space Division Multiple Access (SDMA)
- 7. Comparison of Techniques
- 8. Summary and Unit 1 Conclusion

The Problem of Multiple Access

- In a cellular system, a single Base Station serves hundreds of mobile users.
- The wireless medium (air) is shared by everyone.
- If everyone transmits at the same time on the same frequency, the signals collide and interfere.
- Multiple Access techniques are protocols that coordinate how users share the spectrum without causing unacceptable interference.

The Cocktail Party Analogy

- Imagine a large room where many pairs of people want to talk.
- **FDMA (Frequency):** Each pair talks in a different pitch (some high, some low).
- **TDMA (Time):** Everyone takes turns. Pair 1 talks for a second, then Pair 2, then Pair 3...
- **CDMA (Code):** Everyone talks at the same time, but each pair speaks a completely different language. You tune out the languages you don't understand as background noise.
- **SDMA (Space):** People go to different corners of the room to talk.

Frequency Division Multiple Access (FDMA)

- The available frequency band is divided into multiple narrow frequency channels.
- Each user is assigned a specific, dedicated frequency channel for the duration of the call.
- Guard bands are placed between channels to prevent adjacent channel interference.
- Primarily used in 1G Analog systems (like AMPS).

FDMA Characteristics

- **Advantages:**
- - Simple to implement.
- - Low overhead.
- **Disadvantages:**
- - Wastes capacity: If a user is not talking, the channel sits idle.
- - Maximum capacity is strictly limited by the number of available frequencies.
- - Requires strict filtering.

Time Division Multiple Access (TDMA)

- The frequency band is divided into time slots.
- Multiple users share the same frequency, but they transmit in rapid, sequential time slots.
- The mobile device buffers audio, transmits a quick burst during its slot, and waits for its turn again.
- Used in 2G Digital systems (like GSM).

TDMA Characteristics

- **Advantages:**
- - More efficient than FDMA (3 to 8 times higher capacity).
- - Handsets can turn off the transmitter between slots, saving battery life.
- **Disadvantages:**
- - Requires strict synchronization between the base station and all mobiles.
- - Multipath interference can cause time slots to overlap.

Code Division Multiple Access (CDMA)

- All users transmit at the same time, using the entire frequency band.
- Signals are separated by assigning a unique mathematical code (pseudorandom sequence) to each user.
- The receiver uses the same code to extract the desired signal from the combined noise.
- Used in 3G systems.

CDMA Characteristics

- **Advantages:**
- - High capacity (soft capacity limit).
- - Excellent security and resistance to jamming.
- - No strict time synchronization required.
- **Disadvantages:**
- - Suffers severely from the 'Near-Far Problem'.
- - Requires extremely fast and accurate power control.

Space Division Multiple Access (SDMA)

- Controls radiated energy in space to serve users.
- Uses advanced 'smart antennas' (phased arrays) to direct a narrow beam exactly at a specific user.
- Users in different physical locations can reuse the exact same frequency and time slot because the beams do not overlap.
- A foundational technology for 5G (Massive MIMO).

Comparison Summary

- — Technique — Resource Split — Key Requirement — Technology Era —
- — :— — :— — :— — :— —
- — **FDMA** — Frequency — Sharp Filters — 1G (Analog) —
- — **TDMA** — Time — Synchronization — 2G (GSM) —
- — **CDMA** — Code — Power Control — 3G —
- — **SDMA** — Space — Smart Antennas — 4G/5G —

Lecture & Unit 1 Summary

- Multiple access is essential for sharing limited spectrum.
- FDMA gives users specific frequencies.
- TDMA gives users specific time slots on a shared frequency.
- CDMA separates users by mathematical codes, sharing all time and frequency.
- SDMA separates users by physical location using smart antennas.
- This concludes Unit 1! We have covered the foundations of cellular concepts, interference, and architecture.

Next Lecture Preview

- In the next lecture, we begin Unit 2: GSM and CDMA Systems.
- We will dive deep into the most successful cellular standard in history:
- **GSM Architecture:**
- - What is the MSC, BSC, and BTS?
- - How does the network know who you are and where you are?

Lecture 11: GSM Architecture and Specifications

GSM and CDMA Systems

DI05011011: Mobile Communication

Agenda for Today

- 1. Introduction to GSM
- 2. GSM Architecture Overview
- 3. Mobile Station (MS)
- 4. Base Station Subsystem (BSS)
- 5. Network and Switching Subsystem (NSS)
- 6. Operation and Support Subsystem (OSS)
- 7. Specifications of GSM 900
- 8. Summary and Next Steps

Introduction to GSM

- **Global System for Mobile Communications (GSM)** is a 2nd Generation (2G) digital cellular network standard.
- Developed by the European Telecommunications Standards Institute (ETSI).
- Designed to replace 1G analog networks, providing better voice quality and security.
- Uses a combination of **TDMA (Time Division Multiple Access)** and **FDMA (Frequency Division Multiple Access)**.
- Offers services like voice telephony, Short Message Service (SMS), and basic data services.

GSM Architecture Overview

- The GSM network is divided into four main subsystems:
- **1. Mobile Station (MS):** The user's mobile device.
- **2. Base Station Subsystem (BSS):** Manages the radio link with the MS.
- **3. Network and Switching Subsystem (NSS):** The core network managing switching and mobility.
- **4. Operation and Support Subsystem (OSS):** For network management and maintenance.

1. Mobile Station (MS)

- The Mobile Station consists of two main elements:
- **Mobile Equipment (ME):**
- - The physical hardware (the phone).
- - Identified by a unique IMEI (International Mobile Equipment Identity).
- **Subscriber Identity Module (SIM):**
- - A smart card containing user account info and security keys.
- - Identified by an IMSI (International Mobile Subscriber Identity).
- Separating ME and SIM allows users to change phones while keeping their number and network identity.

2. Base Station Subsystem (BSS)

- The BSS handles all radio-related functions. It connects the MS to the core network.
- It consists of two main components:
- **a. Base Transceiver Station (BTS):**
- - The physical antennas and radio transceivers.
- - Defines a single 'cell'.
- - Handles radio-link protocols and modulation.
- **b. Base Station Controller (BSC):**
- - Controls multiple BTSs.
- - Manages radio resources, channel setup, and frequency hopping.
- - Handles intracell and intercell handoffs.

3. Network and Switching Subsystem (NSS)

- The NSS (Core Network) performs call routing, mobility management, and switching.
- **Mobile Switching Center (MSC):**
- - The central router of the GSM network.
- - Sets up, routes, and tears down calls.
- - Interfaces with the PSTN (Public Switched Telephone Network).
- **Gateway MSC (GMSC):**
- - A special MSC that acts as a gateway to external networks (like landlines or other mobile networks).

NSS Databases: HLR and VLR

- To manage user mobility, the NSS uses two crucial databases:
- **Home Location Register (HLR):**
- - The central, permanent database of all subscribers.
- - Stores IMSI, MSISDN (phone number), current VLR location, and service profiles.
- **Visitor Location Register (VLR):**
- - A temporary, local database attached to an MSC.
- - Stores data about MSs currently roaming in its specific area.
- - Reduces lookup traffic to the HLR by keeping local copies of user data.

NSS Security: AUC and EIR

- **Authentication Center (AUC):**
- - Highly secure database connected to the HLR.
- - Generates security keys (triplets) used for user authentication and voice encryption.
- - Ensures only valid SIM cards access the network.
- **Equipment Identity Register (EIR):**
- - Database of mobile equipment (IMEI numbers).
- - White List: Valid devices.
- - Black List: Stolen or blocked devices (denied service).
- - Grey List: Tracked devices (e.g., malfunctioning).

4. Operation and Support Subsystem (OSS)

- The OSS is the central management layer for the network operator.
- **Functions include:**
- - Network configuration and maintenance.
- - Fault management (alarms and monitoring).
- - Performance management and optimization.
- - Billing and accounting collection.
- It connects to all other network elements (BSC, MSC, HLR, etc.) to ensure the entire system runs smoothly.

Specifications of GSM 900

- GSM was originally designed to operate in the 900 MHz band.
- **Frequency Bands:**
- - **Uplink (MS to BTS):** 890 MHz to 915 MHz
- - **Downlink (BTS to MS):** 935 MHz to 960 MHz
- **Bandwidth:**
- - Total bandwidth per direction: 25 MHz
- - Duplex Distance (separation between uplink and downlink): 45 MHz

GSM 900 Channels and Capacity

- **Carrier Separation:**
- - The 25 MHz band is divided into 124 radio frequency (RF) carrier channels.
- - Channel spacing (bandwidth of one carrier) is **200 kHz** (0.2 MHz).
- **Time Slots (TDMA):**
- - Each 200 kHz RF carrier is divided in time into **8 Time Slots (TS)**.
- - Therefore, one carrier can support 8 simultaneous voice calls.
- **Total Capacity:**
- - 124 carriers $\times$ 8 time slots $=$ **992 physical channels** per cell (theoretically).

GSM 900 Modulation and Data Rate

- **Modulation Technique:**
- - GSM uses **GMSK (Gaussian Minimum Shift Keying)**.
- - GMSK is highly spectrum-efficient and power-efficient, making it ideal for mobile devices.
- **Data Rates:**
- - Raw bit rate on one RF carrier is **270.833 kbps**.
- - Voice encoding rate is **13 kbps** (using Regular Pulse Excitation - Long Term Prediction).
- **Frame Duration:**
- - A basic TDMA frame (containing 8 time slots) lasts **4.615 ms**.

Lecture Summary

- GSM architecture is composed of the MS, BSS, NSS, and OSS.
- MS includes the ME (hardware) and SIM (user identity).
- BSS manages the radio link via BTS and BSC.
- NSS acts as the core network with the MSC routing calls, and HLR/VLR managing mobility.
- GSM 900 uses the 890-915 MHz (Uplink) and 935-960 MHz (Downlink) bands.
- It employs a hybrid FDMA/TDMA scheme with 200 kHz spacing and 8 time slots per carrier.

Next Lecture Preview

- In the next lecture, we will look deeper into how communication actually happens over the air:
- **1. GSM Channels:** Logical vs Physical channels.
- **2. Traffic Channels (TCH):** For voice data.
- **3. Control Channels (CCH):** For signaling and setup.
- **4. GSM Call Procedure:** Step-by-step process of placing a Mobile-to-Mobile call.

Lecture 12: GSM Channels and Call Procedure

GSM and CDMA Systems

DI05011011: Mobile Communication

Agenda for Today

- 1. Physical vs. Logical Channels
- 2. Traffic Channels (TCH)
- 3. Control Channels (CCH) Overview
- 4. Broadcast Channels (BCH)
- 5. Common Control Channels (CCCH)
- 6. Dedicated Control Channels (DCCH)
- 7. GSM Call Procedure: Overview
- 8. Mobile Originating Call (MOC)
- 9. Mobile Terminating Call (MTC)
- 10. Summary

Physical vs. Logical Channels

- **Physical Channel:**
- - Defined by a specific radio frequency (FDMA) and a specific time slot (TDMA).
- - Example: Carrier frequency 890.2 MHz, Time Slot 3.
- **Logical Channel:**
- - Represents the *type of information* carried over the physical channel.
- - Multiple logical channels can be multiplexed onto a single physical channel.
- - Divided into two main categories: **Traffic Channels** and **Control Channels**.

Traffic Channels (TCH)

- Traffic Channels carry the actual payload: user speech or data.
- **TCH/F (Full Rate):**
- - Uses one full time slot per TDMA frame.
- - Carries voice encoded at 13 kbps.
- **TCH/H (Half Rate):**
- - Users share a time slot on alternate frames.
- - Carries voice encoded at 5.6 kbps.
- - Doubles network capacity at the cost of slightly lower voice quality.

Control Channels (CCH) Overview

- Control Channels carry signaling and synchronization data. They are crucial for network management.
- There are three main groups of Control Channels:
- **1. Broadcast Channels (BCH):** Downlink only. Network broadcasting to all MSs.
- **2. Common Control Channels (CCCH):** Uplink and Downlink. Used for call setup and paging.
- **3. Dedicated Control Channels (DCCH):** Bi-directional. Dedicated to a specific MS during a call.

1. Broadcast Channels (BCH)

- Transmitted by the BTS (Downlink) to all mobiles in the cell.
- **FCCH (Frequency Correction Channel):**
- - Helps the MS tune exactly to the BTS frequency.
- **SCH (Synchronization Channel):**
- - Provides TDMA frame synchronization and the BSIC (Base Station Identity Code).
- **BCCH (Broadcast Control Channel):**
- - Broadcasts general network info (Location Area Identity, network rules, adjacent cell frequencies for handoff monitoring).

2. Common Control Channels (CCCH)

- Used for access and paging before a dedicated connection is established.
- **PCH (Paging Channel) - Downlink:**
- - BTS uses PCH to alert an MS of an incoming call (paging).
- **RACH (Random Access Channel) - Uplink:**
- - MS uses RACH to request connection to the network (e.g., to make a call).
- - Uses Slotted ALOHA protocol.
- **AGCH (Access Grant Channel) - Downlink:**
- - BTS responds to a RACH request, assigning a specific dedicated channel to the MS.

3. Dedicated Control Channels (DCCH)

- Assigned to a specific MS for signaling during call setup or while a call is ongoing.
- **SDCCH (Stand-alone Dedicated Control Channel):**
- - Used for call setup, authentication, and SMS transfer before a Traffic Channel is assigned.
- **SACCH (Slow Associated Control Channel):**
- - Always paired with a TCH or SDCCH.
- - Carries continuous background signaling (power control, radio link measurements).
- **FACCH (Fast Associated Control Channel):**
- - Steals a TCH time slot for urgent signaling, like Handoff commands.

GSM Call Procedure: Overview

- A Mobile-to-Mobile call involves two main phases:
- **1. Mobile Originating Call (MOC):**
- - The process from the caller dialing the number to the network routing the call.
- **2. Mobile Terminating Call (MTC):**
- - The process of the network locating the receiver and ringing their phone.
- Both processes rely heavily on the logical channels we just discussed.

Mobile Originating Call (MOC) - Step 1

- **User A dials User B's number.**
- 1. **Channel Request:** MS-A sends a request on **RACH**.
- 2. **Channel Assignment:** BSC responds on **AGCH**, assigning an **SDCCH**.
- 3. **Service Request:** MS-A sends a connection request over **SDCCH** to the MSC.
- 4. **Authentication:** MSC/VLR authenticates MS-A (via AUC keys).
- 5. **Ciphering:** Network instructs MS-A to start encrypting data.

Mobile Originating Call (MOC) - Step 2

- 6. **Call Setup Message:** MS-A sends dialed number (User B) to MSC.
- 7. **Routing Analysis:** MSC analyzes the number and queries HLR to route the call.
- 8. **Traffic Channel Assignment:** BSC assigns a **TCH** to MS-A.
- 9. **Ringing:** MSC sends an 'Alerting' message back to MS-A (user hears ringback tone).
- - MS-A waits on the TCH for User B to answer.

Mobile Terminating Call (MTC)

- **Network needs to find User B.**
- 1. **Routing:** GMSC queries HLR to find User B's current VLR/MSC.
- 2. **Paging:** Destination MSC broadcasts a page on **PCH** in User B's Location Area.
- 3. **Response:** MS-B hears the page, requests access on **RACH**.
- 4. **Assignment:** BSC assigns an **SDCCH** via **AGCH**.
- 5. **Security:** Authentication and ciphering performed on MS-B.
- 6. **Setup:** MSC sends Call Setup message; MS-B rings.
- 7. **Answer:** User B answers, assigned a **TCH**. Call is connected!

Lecture Summary

- Logical channels define the type of data sent over physical RF timeslots.
- Traffic Channels (TCH) carry voice at full or half rates.
- Control Channels handle signaling: BCH (broadcast info), CCCH (access/paging), DCCH (dedicated signaling).
- A call consists of Mobile Originating (MOC) and Mobile Terminating (MTC) phases.
- Call setup requires sequential use of RACH, AGCH, SDCCH, and finally TCH.

Next Lecture Preview

- In the next lecture, we will focus on the security and performance enhancements in GSM:
- **1. Authentication and Security:** How A3, A5, and A8 algorithms protect your data.
- **2. Frequency Hopping:** Fast and Slow hopping.
- **3. Why do we need Frequency Hopping?** (Combating fading and interference).

Lecture 13: GSM Security and Frequency Hopping

GSM and CDMA Systems

DI05011011: Mobile Communication

Agenda for Today

- 1. The Need for Security in Mobile Networks
- 2. GSM Security Goals
- 3. Authentication Process (A3 Algorithm)
- 4. Encryption / Ciphering (A5 Algorithm)
- 5. Key Generation (A8 Algorithm)
- 6. Concept of Frequency Hopping
- 7. Fast vs. Slow Frequency Hopping
- 8. Advantages of Frequency Hopping
- 9. Summary

The Need for Security in Mobile Networks

- 1G analog networks had severe security flaws:
- - **Eavesdropping:** Anyone with a radio scanner could listen to phone calls.
- - **Cloning:** Fraudsters could easily copy a phone's electronic serial number to make free calls.
- GSM was designed with digital security from the ground up to solve these issues.
- Security relies on the **SIM card** (Subscriber Identity Module) and the **AUC** (Authentication Center).

GSM Security Goals

- GSM security architecture aims to provide:
- **1. Subscriber Authentication:** Proving the user is who they claim to be (preventing cloning).
- **2. Data Confidentiality:** Encrypting voice and data over the radio path (preventing eavesdropping).
- **3. Subscriber Identity Confidentiality:** Protecting the user's permanent identity (IMSI) from being tracked over the air.
- **4. Equipment Authentication:** Ensuring the mobile hardware is not stolen (using EIR).

The Authentication Process (A3 Algorithm)

- Challenge-Response mechanism used to verify the SIM:
- 1. Network (AUC) sends a 128-bit **RAND** (Random Number) to the MS.
- 2. The SIM card uses the **A3 Algorithm** and a secret key (**Ki**) stored on the SIM to process the RAND.
- 3. The output is a 32-bit **SRES** (Signed Response).
- 4. MS sends SRES back to the network.
- 5. The network compares the MS's SRES with its own internally calculated SRES. If they match, authentication is successful.

Key Generation (A8 Algorithm)

- Once authenticated, the data needs to be encrypted.
- - Both the SIM card and the AUC run the **A8 Algorithm** simultaneously with the A3 algorithm.
- - Inputs: The same **RAND** and secret key (**Ki**).
- - Output: A 64-bit ciphering key called **Kc**.
- The **Kc** key is what will actually be used to encrypt the voice traffic during the call.

Encryption / Ciphering (A5 Algorithm)

- Protects the voice and data over the vulnerable air interface.
- - Uses the **A5 Algorithm** (a stream cipher).
- - Inputs: The session key (**Kc**) and the current TDMA **Frame Number**.
- - The data is encrypted at the MS before transmission and decrypted at the BTS.
- - *Note:* Encryption only happens over the radio link (MS to BTS). It is typically unencrypted on the core network.

Introduction to Frequency Hopping

- **What is it?**
- Instead of transmitting a call on a single fixed frequency, the transmitter and receiver rapidly change frequencies according to a pre-defined pattern.
- **Why is it needed in GSM?**
- - **Multipath Fading:** Radio waves bounce off buildings. Sometimes they cancel each other out at specific frequencies (deep fades).
- - **Co-Channel Interference:** Interference from neighboring cells using the same frequency.
- Hopping ensures a call doesn't stay stuck on a "bad" frequency.

How Frequency Hopping Works

- \- The network assigns a **Hopping Sequence Number (HSN)** and a **Mobile Allocation (MA)** (a list of available frequencies) to the MS.
- \- Both the BTS and the MS change their transmission/reception frequency synchronously.
- \- If a packet is lost due to fading on frequency F1, the next packet is sent on F2, which might be perfectly clear.
- \- Combined with error correction (interleaving), the lost data can be recovered.

Slow vs. Fast Frequency Hopping

- **Slow Frequency Hopping (SFH):**
- - The hopping rate is *lower* than the modulation symbol rate.
- - One or more data bits/bursts are transmitted on a frequency before hopping.
- - **GSM uses Slow Frequency Hopping.** It hops 217 times per second (once per TDMA frame).
-
- **Fast Frequency Hopping (FFH):**
- - The hopping rate is *higher* than the symbol rate.
- - Frequencies change multiple times during the transmission of a single bit.
- - Very complex hardware required; used more in military applications.

Advantages of Frequency Hopping in GSM

- **1. Frequency Diversity:**
- Mitigates Rayleigh fading. If one frequency is in a deep fade, the call isn't dropped because the next burst uses a different frequency.
- **2. Interference Averaging:**
- Instead of one user experiencing continuous severe interference from a co-channel cell, the interference is spread out among many users as short, correctable bursts of noise.
- **3. Added Security:**
- Makes it harder for a simple radio scanner to track a single conversation.

Lecture Summary

- GSM security uses three main algorithms: A3 (Authentication), A8 (Key Generation), and A5 (Ciphering).
- Authentication relies on a Challenge-Response mechanism using a secret Ki.
- Data is encrypted over the air interface using the Kc key.
- Frequency hopping involves synchronously changing carrier frequencies.
- GSM implements Slow Frequency Hopping (217 hops/sec) to combat multipath fading and co-channel interference.

Next Lecture Preview

- In the next lecture, we will cover:
- **1. GSM Identifiers:** What exactly are IMSI, IMEI, TMSI, MSISDN, and LAI?
- **2. Introduction to Spread Spectrum:** The foundation for CDMA technology.
- **3. Concept of spreading bandwidth.**

Lecture 14: GSM Identifiers and Spread Spectrum Concept

GSM and CDMA Systems

DI05011011: Mobile Communication

Agenda for Today

- 1. Why do we need Identifiers?
- 2. IMSI (Subscriber Identity)
- 3. TMSI (Temporary Identity)
- 4. IMEI (Equipment Identity)
- 5. MSISDN (Phone Number)
- 6. LAI & BSIC (Location/Cell Identities)
- 7. Introduction to Spread Spectrum
- 8. Why spread the spectrum?
- 9. Summary

Why do we need Identifiers?

- A cellular network must track millions of users and devices seamlessly.
- Identifiers are required to:
- - Route calls to the correct user.
- - Bill the correct account.
- - Prevent stolen devices from accessing the network.
- - Maintain user privacy over the airwaves.
- - Distinguish between different network operators and cell towers.

IMSI: International Mobile Subscriber Identity

- **What is it?** The permanent, unique identifier for a mobile subscriber.
- **Where is it?** Stored securely on the SIM card and in the HLR.
- **Structure (up to 15 digits):**
- - **MCC (Mobile Country Code):** 3 digits (e.g., 404 for India).
- - **MNC (Mobile Network Code):** 2 or 3 digits (identifies the operator, e.g., Airtel, Jio).
- - **MSIN (Mobile Subscriber Identification Number):** Unique serial number for the user.
- **Usage:** Internal network routing and authentication. Rarely transmitted over the air to prevent tracking.

TMSI: Temporary Mobile Subscriber Identity

- **What is it?** A temporary alias for the IMSI.
- **Where is it?** Assigned by the VLR and stored in the SIM and VLR.
- **Purpose:**
- - Protects user privacy.
- - If the IMSI is constantly broadcast, eavesdroppers could track a user's physical location.
- - Instead, the network assigns a TMSI. Only the VLR knows which TMSI maps to which IMSI.
- - The TMSI is changed frequently (e.g., after every call or location update).

IMEI & MSISDN

- **IMEI (International Mobile Equipment Identity):**
- - Identifies the *hardware* (the phone itself), not the user.
- - 15-digit number.
- - Used by the EIR (Equipment Identity Register) to block stolen phones.
-
- **MSISDN (Mobile Station International Subscriber Directory Number):**
- - The actual 'phone number' dialed by other people.
- - Includes Country Code (e.g., +91), National Destination Code, and Subscriber Number.
- - The network maps the MSISDN to the IMSI to route the call.

LAI & BSIC

- **LAI (Location Area Identity):**
- - Identifies a specific Location Area (a group of cells) within a network.
- - Used for paging. When a call comes in, the network pages the MS in its last known LAI.
-
- **BSIC (Base Station Identity Code):**
- - Allows the MS to distinguish between neighboring cells using the same frequencies (co-channel cells).
- - Broadcast on the SCH (Synchronization Channel).
- - Prevents the MS from connecting to the wrong tower during handoff.

Introduction to Spread Spectrum

- Let's shift gears from GSM to the foundational theory of CDMA.
- **What is Spread Spectrum?**
- \- A transmission technique where the signal occupies a bandwidth much wider than the minimum required for information transmission.
- \- In standard AM/FM or GSM, we try to compress signals into the smallest bandwidth possible.
- \- In Spread Spectrum, we intentionally *spread* the signal over a massive frequency band.

Why Spread the Spectrum?

- It seems counter-intuitive to waste bandwidth. However, spreading offers massive advantages:
- **1. Interference Resistance:** Highly immune to narrow-band jamming and interference.
- **2. Low Intercept Probability:** The signal power is spread so thin it looks like background noise. Hard to detect (originally designed for military).
- **3. Multiple Access (CDMA):** Multiple users can share the *exact same* wide frequency band simultaneously without interfering, separated only by unique codes.

How is spreading achieved?

- Spreading is achieved by multiplying the original data signal with a high-speed pseudo-random sequence (Spreading Code).
- - **Data Rate (R):** Original speed of voice/data (e.g., 10 kbps).
- - **Chip Rate (W):** Speed of the spreading code (e.g., 1.25 Mbps).
- **Processing Gain (PG):**
- - The ratio of Spread Bandwidth to Data Bandwidth: 'PG = W / R'
- - Higher processing gain means better resistance to interference.

Lecture Summary

- **GSM Identifiers:**
- - **IMSI/TMSI:** Permanent and temporary subscriber IDs.
- - **IMEI:** Hardware ID.
- - **MSISDN:** Dialable phone number.
- - **LAI/BSIC:** Location and cell tower IDs.
- **Spread Spectrum:**
- - Intentionally spreading a signal over a wide bandwidth.
- - Provides interference immunity, security, and enables multiple access via unique codes (CDMA).

Next Lecture Preview

- In the next lecture, we will dive fully into CDMA systems:
- **1. CDMA Principle:** How users share the same frequency and time.
- **2. Orthogonal Codes:** The mathematical "languages" used to separate users.
- **3. Advantages of CDMA:** Soft handoff, power control, and capacity improvements.

Lecture 15: CDMA Principles and Spread Spectrum Types

GSM and CDMA Systems

DI05011011: Mobile Communication

Agenda for Today

- 1. What is CDMA?
- 2. The Principle of CDMA (Orthogonality)
- 3. The Cocktail Party Analogy
- 4. Power Control in CDMA
- 5. Soft Handoff
- 6. Advantages of CDMA
- 7. Types of Spread Spectrum Techniques
- 8. DSSS vs. FHSS (Brief Intro)
- 9. Summary

What is CDMA?

- **Code Division Multiple Access (CDMA):**
- - Based on Spread Spectrum technology.
- - Unlike FDMA (separating users by frequency) or TDMA (separating users by time slots).
- - In CDMA, **all users transmit on the same frequency at the exact same time.**
- - Users are separated mathematically using unique, orthogonal codes assigned to each transmitter.

The Principle of CDMA: Orthogonal Codes

- How do signals not interfere?
- - Each user's data is multiplied by a unique 'spreading code' (e.g., Walsh codes).
- - These codes are **Orthogonal**.
- - Mathematical property: When you multiply two different orthogonal codes together and sum the result, it equals zero.
- - The receiver multiplies the incoming combined signal by the *desired* user's code. Only that user's data emerges; the rest of the signals cancel out to zero (noise).

The Cocktail Party Analogy

- **FDMA:** People talking in separate rooms.
- **TDMA:** People in the same room, but taking turns talking one by one.
- **CDMA:** Everyone in the same room, talking at the same time, but in completely **different languages**.
- - If you only understand English, the Spanish and French conversations just sound like background noise.
- - The 'language' is the spreading code.

Crucial Requirement: Power Control

- The Near-Far Problem:
- - If User A is close to the tower and User B is far away, User A's signal will drown out User B's signal (the loud person at the party).
- - Since everyone shares the same frequency, strict power control is mandatory.
- **Solution:**
- - The Base Station constantly commands mobiles to adjust their transmit power (hundreds of times per second).
- - Goal: Every mobile's signal must arrive at the Base Station with the **exact same power level**.

Soft Handoff in CDMA

- **Hard Handoff (GSM):** "Break before make."
- - MS disconnects from Tower A, then connects to Tower B. Brief interruption.
- **Soft Handoff (CDMA):** "Make before break."
- - Because all cells use the same frequency, an MS can communicate with Tower A and Tower B *simultaneously* during the transition.
- - The core network combines the signals from both towers, improving call quality at cell edges.
- - Eliminates dropped calls during handoffs.

Advantages of CDMA

- **1. Increased Capacity:** Soft capacity limits. You can always add one more user, it just slightly increases the noise floor for everyone else.
- **2. Better Call Quality:** Soft handoffs prevent drops; multipath fading is mitigated.
- **3. Security:** Spread spectrum is inherently difficult to intercept without knowing the specific code.
- **4. Frequency Reuse of 1:** Every cell uses the same frequency band. No complex frequency planning required like in GSM.

Types of Spread Spectrum Techniques

- Spread Spectrum can be implemented in several ways to achieve the bandwidth spreading we discussed in Lecture 14.
- The two primary techniques are:
- **1. DSSS (Direct Sequence Spread Spectrum):**
- - The data is directly multiplied by a high-speed code sequence.
- **2. FHSS (Frequency Hopping Spread Spectrum):**
- - The carrier frequency hops around rapidly across a wide band.

Direct Sequence Spread Spectrum (DSSS) - Concept

- - Each bit of user data is represented by multiple bits in the transmitted signal, called **chips**.
- - A spreading code (e.g., 11 bits long) represents a '1', and its inverse represents a '0'.
- - The signal is continuously spread across the entire wide bandwidth simultaneously.
- - Used heavily in 3G Cellular (WCDMA), Wi-Fi (802.11b), and GPS.

Frequency Hopping Spread Spectrum (FHSS) - Concept

- - The data is transmitted using a narrow bandwidth.
- - However, that narrow band changes frequency rapidly, hopping across a very wide total bandwidth.
- - The spreading occurs over time, rather than simultaneously.
- - Used heavily in Bluetooth and military radios.

Lecture Summary

- CDMA allows users to share the exact same frequency and time using orthogonal codes.
- It solves the Near-Far problem through strict, rapid power control.
- Soft Handoff (make before break) improves reliability.
- CDMA offers higher capacity and a frequency reuse factor of 1.
- Spread Spectrum is mainly categorized into DSSS (spreading via chips) and FHSS (spreading via hopping).

Next Lecture Preview

- In the next lecture, we will look deeper into the spread spectrum techniques:
- **1. Deep Dive into DSSS:** How chips multiply data.
- **2. Deep Dive into FHSS:** Hop sequences.
- **3. Comparison:** GSM vs. CDMA Technology.

Lecture 16: a. DSSS- Direct sequence spread spectrum

GSM and CDMA Systems

DI05011011: Mobile Communication

Agenda for Today

- 1. Recap of Spread Spectrum Concept
- 2. Direct Sequence Spread Spectrum (DSSS) Overview
- 3. DSSS Spreading and De-spreading Process
- 4. Advantages of DSSS
- 5. Frequency Hopping Spread Spectrum (FHSS) Overview
- 6. Hopping Patterns and Types (Slow vs. Fast)
- 7. Advantages of FHSS
- 8. Comparison: DSSS vs. FHSS
- 9. Real-world Examples
- 10. Summary

Spread Spectrum Recap

- **Concept:** Transmission of a signal over a bandwidth much larger than the minimum required bandwidth.
- **Purpose:** Reduces interference, increases security, and allows multiple users to share the same frequency band.
- **Key Mechanism:** Spreading is accomplished using a Pseudo-Noise (PN) sequence, which is independent of the original data.
- **Two Main Types:**
- - Direct Sequence Spread Spectrum (DSSS)
- - Frequency Hopping Spread Spectrum (FHSS)

Direct Sequence Spread Spectrum (DSSS)

- **Definition:** DSSS multiplies the original data signal directly with a high bit-rate Pseudo-Noise (PN) code.
- **Chipping Code:** The PN code bits are called 'chips'. The chip rate is significantly higher than the data bit rate.
- **Effect on Bandwidth:** The multiplication spreads the narrow-band data signal over a wide frequency band.
- **Noise-like Appearance:** The resulting wideband signal looks like random noise to anyone without the exact PN code.

DSSS Spreading Process

- **1. Data Signal:** Original information signal with bit rate Rb.
- **2. PN Sequence Generator:** Generates a high-speed pseudo-random sequence with chip rate Rc (Rc ¿¿ Rb).
- **3. Modulation/Multiplication:** The data signal is XORed (multiplied) with the PN sequence.
- **4. RF Carrier Modulation:** The spread baseband signal then modulates an RF carrier (e.g., using BPSK) for transmission.
- **Processing Gain:** Defined as the ratio of Chip Rate to Data Rate (Rc / Rb).

DSSS De-spreading Process

- **Synchronization:** The receiver must locally generate the *exact* same PN code, perfectly aligned in time with the received signal.
- **Correlation:** The received wideband signal is multiplied by the synchronized local PN code.
- **Result:** This operation 'collapses' the wideband signal back into the original narrow-band data signal.
- **Interference Rejection:** Any narrow-band interference picked up during transmission is actually *spread* by this process, reducing its impact on the data.

Advantages of DSSS

- **Jamming Resistance:** Highly resistant to narrow-band jamming and intentional interference.
- **Low Probability of Intercept (LPI):** Hard for eavesdroppers to detect the signal since it operates near or below the noise floor.
- **Multi-Path Mitigation:** DSSS can resolve multipath components using a RAKE receiver, actually improving signal quality.
- **Multiple Access:** Basis for CDMA, allowing many users to share the channel simultaneously using different orthogonal PN codes.

Frequency Hopping Spread Spectrum (FHSS)

- **Definition:** The carrier frequency of the transmitted signal changes ('hops') rapidly according to a pseudo-random sequence.
- **Mechanism:** Instead of spreading the baseband signal, FHSS jumps across many narrow frequency channels over time.
- **Bandwidth Usage:** At any instant, the signal is narrow-band. Over time, it covers a wide frequency band.
- **Requirement:** Both transmitter and receiver must agree on the hopping sequence and be strictly synchronized.

How FHSS Works

- **1. Digital Data:** Modulates a baseband signal (e.g., FSK).
- **2. PN Sequence Generator:** Drives a frequency synthesizer.
- **3. Frequency Synthesizer:** Outputs a different carrier frequency based on the PN code.
- **4. Mixer:** The baseband signal is mixed with the hopping carrier frequency.
- **5. Transmission:** The signal is transmitted on the new frequency for a short duration (dwell time) before hopping again.

Slow vs. Fast Frequency Hopping

- **Slow FHSS:**
- - Hopping rate is slower than the symbol rate.
- - Multiple symbols (data bits) are transmitted per frequency hop.
- - Cheaper to implement, used in GSM (for interference averaging).
- **Fast FHSS:**
- - Hopping rate is faster than the symbol rate.
- - One symbol is transmitted over multiple frequency hops.
- - High resistance to narrow-band jamming, highly secure (military use).

Advantages of FHSS

- **Avoids Interception:** Difficult for unauthorized receivers to follow the rapid frequency changes.
- **Mitigates Interference:** If a specific frequency is jammed or noisy, only a small fraction of data is lost (easily corrected with error coding).
- **Near-Far Problem Resilience:** Much less susceptible to the near-far problem compared to DSSS.
- **Coexistence:** Multiple FHSS networks can coexist in the same area if they use orthogonal hopping sequences.

Comparison: DSSS vs. FHSS

- — Feature — DSSS — FHSS —
- ———————
- — **Spreading Method** — Multiplies baseband with PN code — Changes carrier frequency via PN code —
- — **Bandwidth usage** — Occupies full band simultaneously — Occupies narrow band at any instant —
- — **Near-Far Problem** — Highly susceptible, needs tight power control — Resistant —
- — **Hardware Complexity**— High (complex correlators, RAKE) — Moderate (agile synthesizers) —
- — **Data Rates** — Generally higher — Generally lower —

Engineering Example: Wi-Fi vs. Bluetooth

- **Wi-Fi (Early 802.11b):**
- - Uses **DSSS** to achieve higher data rates (up to 11 Mbps).
- - Spreads the signal across a 22 MHz channel in the 2.4 GHz band.
- - Better for continuous, high-throughput data transfer.
-
- **Bluetooth:**
- - Uses **FHSS**.
- - Hops across 79 channels (1 MHz wide) at 1600 hops per second.
- - Better for low-power, robust connections in noisy environments, avoiding interference from Wi-Fi.

Lecture Summary

- Spread spectrum techniques (DSSS and FHSS) provide security, interference rejection, and multiple access capabilities.
- **DSSS** spreads the signal by multiplying it with a high-rate chipping sequence, appearing as noise.
- **FHSS** spreads the signal by rapidly changing the carrier frequency across a wide band.
- DSSS offers higher data rates and multi-path mitigation but is susceptible to the near-far problem.
- FHSS is robust against jamming and the near-far problem but generally supports lower data rates.

Next Lecture Preview

- In the next lecture, we will perform a comprehensive comparison between the two major 2G/3G technologies:
- **1. GSM vs CDMA:** The ultimate showdown.
- **2. Multiple Access:** TDMA/FDMA vs CDMA.
- **3. Performance Metrics:** Capacity, Security, and Handoffs.
- **4. Introduction to limitations of both technologies.**

Lecture 17: 2.11 Comparison: GSM vs CDMA

GSM and CDMA Systems

DI05011011: Mobile Communication

Agenda for Today

- 1. Recap of GSM and CDMA Principles
- 2. Multiple Access: TDMA/FDMA vs CDMA
- 3. Spectrum Utilization and Capacity
- 4. Call Quality and Handoff Types
- 5. Security and Encryption
- 6. Global Adoption and Roaming
- 7. Comparison Summary Table
- 8. Introduction to Limitations
- 9. Summary and Next Steps

Core Principles Recap

- **GSM (Global System for Mobile Communications):**
- - Originally a European standard.
- - Uses a combination of TDMA (Time Division) and FDMA (Frequency Division).
- - Defines specific time slots on specific frequencies for users.
-
- **CDMA (Code Division Multiple Access):**
- - Developed by Qualcomm (IS-95 standard).
- - Uses spread spectrum technology (DSSS).
- - All users transmit on the same frequency at the same time, separated by unique PN codes.

Multiple Access Technique Comparison

- **GSM Approach:**
- - Like a dinner party where people take turns speaking (Time slots) in different rooms (Frequencies).
- - Hard limit on the number of users per channel (e.g., 8 time slots per 200 kHz carrier).
-
- **CDMA Approach:**
- - Like a dinner party where everyone speaks at once in the same room, but in different languages (Codes).
- - Soft limit on capacity; as more users join, the background noise (interference) gradually increases.

Spectrum Utilization & Capacity

- **GSM:**
- - Requires careful frequency planning to avoid co-channel interference.
- - Frequency reuse factor is typically 3, 4, or 7 (cluster size).
- - Lower spectral efficiency compared to CDMA.
-
- **CDMA:**
- - Universal frequency reuse (Reuse factor $= 1$). Every cell uses the same frequency.
- - Much higher spectral efficiency.
- - Can support 4 to 5 times more users than GSM in the same spectrum.

Call Quality and Handoffs

- **GSM (Hard Handoff):**
- - Break-before-make. The mobile disconnects from the old base station before connecting to the new one.
- - Can result in dropped calls if the transition isn't perfect.
-
- **CDMA (Soft Handoff):**
- - Make-before-break. The mobile connects to multiple base stations simultaneously during the transition.
- - Results in fewer dropped calls and better voice quality at cell edges.
- - Requires a RAKE receiver to combine signals.

Security and Encryption

- **GSM Security:**
- - Uses A5/1 (and later A5/3) encryption algorithms.
- - Security is mostly confined to the SIM card and network authentication.
- - Easier to intercept using IMSI catchers (Stingrays).
-
- **CDMA Security:**
- - Inherently more secure due to spread spectrum (signal looks like noise without the code).
- - Additionally uses built-in encryption.
- - Historically much harder for eavesdroppers to intercept than early GSM.

Device Architecture & Global Adoption

- **GSM (SIM Cards):**
- - Separates subscriber identity (SIM) from the handset hardware.
- - Easy to switch phones, highly adopted globally (over 80% of the global 2G/3G market).
- - Seamless international roaming.
-
- **CDMA (Device Bound):**
- - Subscriber identity was historically tied directly to the phone's ESN (Electronic Serial Number).
- - Harder to switch devices (required carrier intervention).
- - Mostly adopted in North America (Verizon, Sprint) and parts of Asia.

Summary Comparison Table

- — Feature — GSM — CDMA —
- ——————————
- — **Access Method** — TDMA + FDMA — Spread Spectrum (CDMA) —
- — **Frequency Reuse**— Cluster (3, 4, 7) — Universal (1) —
- — **Handoff** — Hard Handoff — Soft Handoff —
- — **Subscriber ID** — SIM Card — Handset (ESN/MEID) —
- — **Capacity** — Lower — Higher (4x - 5x) —
- — **Global Roaming** — Excellent — Limited —

Introduction to Limitations

- While GSM and CDMA revolutionized mobile voice communication, they both eventually hit technological roadblocks.
- **The Shift in Demand:** Networks designed primarily for voice (circuit-switched) struggled with the rise of the internet and packet-data (IP).
- **Common Bottlenecks:**
- - Limited data rates (Bandwidth).
- - Scalability issues in dense urban areas.
- - Inefficiencies in handling bursty IP traffic.

Engineering Example: The Cost of Upgrades

- **The GPRS/EDGE patch for GSM:**
- - GSM introduced GPRS (2.5G) and EDGE (2.75G) to handle packet data.
- - However, it still had to steal time-slots from voice calls, leading to poor data performance during peak voice hours.
-
- **The EV-DO patch for CDMA:**
- - CDMA introduced EV-DO to provide high-speed data.
- - It required a separate dedicated carrier frequency just for data, complicating spectrum management for operators.

Lecture Summary

- GSM utilizes TDMA/FDMA, requires frequency planning, and uses hard handoffs, but excels in global roaming via SIM cards.
- CDMA utilizes spread spectrum, allows universal frequency reuse, supports soft handoffs, and offers higher capacity, but historically lacked easy device swapping.
- While GSM won the global market share battle, CDMA's core technology (spread spectrum) proved superior for capacity and was adopted for 3G (WCDMA/UMTS).
- Both systems ultimately faced severe limitations when mobile internet demand surged.

Next Lecture Preview

- In the next lecture, we will dive deep into the specific limitations of these technologies:
- **1. Limitations of GSM Technology.**
- **2. Technical bottlenecks of TDMA.**
- **3. Why 2G GSM is being shut down globally.**

Lecture 18: 2.12 Limitations of GSM and CDMA Technology (Part 1)

GSM and CDMA Systems

DI05011011: Mobile Communication

Agenda for Today

- 1. The Original Design Goal of GSM
- 2. Limitation 1: Low Data Rates
- 3. Limitation 2: Spectral Inefficiency
- 4. Limitation 3: Hard Handoff Issues
- 5. Limitation 4: Security Vulnerabilities
- 6. Limitation 5: Core Network Inflexibility
- 7. Real-world Example: The 2G Shutdown
- 8. Summary

The Original Design Goal of GSM

- **Built for Voice:** GSM was designed in the late 1980s primarily to replace analog 1G voice systems with digital voice.
- **Circuit-Switched Architecture:** It establishes a dedicated, fixed circuit between the caller and receiver for the duration of the call.
- **The Mismatch:** This architecture is perfect for continuous voice conversations but highly inefficient for 'bursty' internet traffic (web browsing, emails).
- **Result:** As data demand grew, GSM's foundational design became its biggest weakness.

Limitation 1: Low Data Rates

- **Basic GSM Data:** Originally supported only 9.6 kbps for data transfer.
- **GPRS (2.5G):** Introduced packet switching, pushing speeds to ~114 kbps, but shared among users.
- **EDGE (2.75G):** Improved modulation (8-PSK) raised theoretical speeds to ~384 kbps.
- **The Problem:** Even with EDGE, data rates were vastly insufficient for modern multimedia, video streaming, or rapid web browsing.

Limitation 2: Spectral Inefficiency

- **TDMA/FDMA Limits:** GSM uses a fixed 200 kHz channel divided into 8 time slots.
- **Hard Capacity:** A single base station transceiver can only handle 8 simultaneous full-rate calls per carrier frequency.
- **Frequency Planning Overhead:** Operators must maintain complex frequency reuse patterns (e.g., clusters of 7) to avoid co-channel interference.
- **Wasted Spectrum:** Much of the spectrum is wasted on guard bands and spatial separation between cells using the same frequency.

Limitation 3: Hard Handoff Issues

- **Break-Before-Make:** When moving between cells, a GSM mobile must break its connection with the current tower before establishing a connection with the new one.
- **Delay:** This switching process takes a fraction of a second.
- **Dropped Calls:** If the new tower is congested or the signal drops faster than expected, the handoff fails, resulting in a dropped call.
- **Ping-Pong Effect:** At cell edges, the mobile might rapidly switch back and forth between towers, causing signaling overhead and potential drops.

Limitation 4: Security Vulnerabilities

- **Unilateral Authentication:** In GSM, the network authenticates the phone (via the SIM), but the phone *does not* authenticate the network.
- **IMSI Catchers:** This flaw allows malicious actors to set up fake cell towers (Stingrays) to intercept calls and data.
- **Weak Encryption:** The original A5/1 encryption algorithm was cracked. A5/2 was intentionally weakened for export.
- **Lack of Data Integrity:** No strong protection against the modification of transmitted data.

Limitation 5: Core Network Inflexibility

- **Complex Signaling:** The SS7 (Signaling System No. 7) protocol used for call setup and routing is highly complex and has its own security vulnerabilities.
- **High Latency:** The architecture involves multiple nodes (BTS, BSC, MSC) resulting in high latency for data transmission (ping times often ¿ 200ms).
- **Cost of Scaling:** Adding capacity required adding substantial physical hardware at the BSC and MSC levels, which is costly and slow to deploy.

Engineering Example: The Global 2G Shutdown

- **The Phenomenon:** Carriers worldwide (AT&T, Verizon, Vodafone, Jio) have shut down or are shutting down their 2G GSM/CDMA networks.
- **The Reason:**
- - **Spectrum Re-farming:** 2G is spectrally inefficient. Carriers want to re-use those valuable sub-1GHz frequencies for 4G LTE and 5G.
- - **Maintenance Cost:** Maintaining legacy hardware and SS7 networks is expensive.
- **The Impact:** Millions of legacy M2M (Machine-to-Machine) devices, like older point-of-sale terminals and alarm systems, had to be replaced.

Lecture Summary

- GSM's primary limitation stems from its circuit-switched, voice-centric original design.
- Data rates are severely limited by the narrow 200 kHz channel and TDMA time slots.
- Spectral inefficiency is high due to the requirement for frequency reuse clusters.
- Hard handoffs cause dropped calls, and lack of mutual authentication creates severe security risks.
- These limitations necessitated the development of 3G (UMTS) and eventually 4G (LTE).

Next Lecture Preview

- In the next lecture, we will look at the other side of the coin:
- **1. Limitations of CDMA Technology.**
- **2. The Near-Far Problem.**
- **3. Cell Breathing and Self-Interference.**
- **4. PN Code exhaustion.**

Lecture 19: 2.12 Limitations of GSM and CDMA Technology (Part 2)

GSM and CDMA Systems

DI05011011: Mobile Communication

Agenda for Today

- 1. The CDMA Promise vs. Reality
- 2. Limitation 1: The Near-Far Problem
- 3. Limitation 2: Strict Power Control Requirements
- 4. Limitation 3: Self-Interference and Cell Breathing
- 5. Limitation 4: PN Code Exhaustion
- 6. Limitation 5: Lack of Global Roaming & SIMs
- 7. Real-world Example: Cell Breathing in Urban Areas
- 8. Summary

The CDMA Promise vs. Reality

- **The Promise:** Universal frequency reuse (Reuse $= 1$), massive capacity, high security, and smooth soft handoffs.
- **The Reality:** While theoretically vastly superior to GSM, CDMA is extremely complex to implement at the radio frequency (RF) level.
- **The Core Issue:** Because everyone shares the *exact same frequency at the same time*, every other user on the network acts as interference to your signal.
- **Consequence:** CDMA is completely bounded by interference. Manage the interference, and the network works; fail to manage it, and the network collapses.

Limitation 1: The Near-Far Problem

- **The Scenario:** Imagine two mobile users connected to the same base station.
- - User A is very close to the tower.
- - User B is at the edge of the cell, far away.
- **The Problem:** If both transmit at the same power level, User A's signal will arrive at the tower vastly stronger than User B's.
- **The Result:** The strong signal from User A will completely drown out (jam) the weak signal from User B, dropping User B's call.
- **Significance:** This is the most critical flaw in any DSSS system.

Limitation 2: Strict Power Control

- **The Solution to Near-Far:** The base station must constantly command all phones to adjust their transmit power.
- **The Goal:** Every signal from every phone *must* arrive at the base station at the exact same power level.
- **The Limitation:**
- - Requires incredibly fast, continuous feedback loops (up to 800 times per second).
- - Consumes network signaling bandwidth.
- - Drains mobile battery if the phone is forced to transmit at max power at the cell edge.
- - If power control fails, the whole cell drops calls.

Limitation 3: Self-Interference & Cell Breathing

- **Self-Interference:** As more users join a CDMA cell, the overall noise floor (interference) rises.
- **Cell Breathing Phenomenon:**
- - As the noise floor rises, phones at the edge of the cell can no longer penetrate the noise to reach the tower, even at max power.
- - The effective coverage area (footprint) of the cell physically *shrinks* under heavy load.
- - When the load decreases, the cell footprint expands again.
- **Impact:** Makes network planning incredibly difficult, leading to coverage holes during busy hours.

Limitation 4: PN Code Exhaustion

- **Finite Codes:** While CDMA has a 'soft capacity', it is still constrained by the number of available orthogonal Pseudo-Noise (PN) codes.
- **Walsh Codes:** Used to separate users in the forward link (Tower to Mobile). There are typically 64 Walsh codes available per carrier.
- **Overhead:** Several codes are consumed by pilot, paging, and sync channels.
- **Exhaustion:** In a highly dense area, a base station might run out of available Walsh codes before it reaches its RF interference limit, creating a hard cap on capacity.

Limitation 5: Roaming & Ecosystem

- **No SIM Standard (Initially):** Early CDMA networks did not use SIM cards. Subscriber IDs were hardcoded into the phone.
- **Device Lock-in:** Users could not simply swap a card to change phones or networks. They needed carrier intervention.
- **Global Fragmentation:** Because GSM captured Europe and most of Asia, CDMA users from the US (Verizon/Sprint) often could not roam internationally without carrying a separate GSM 'world phone'.
- **Ecosystem Cost:** Lower global volume meant CDMA network equipment and handsets were often more expensive than GSM counterparts.

Engineering Example: Urban Cell Breathing

- **Scenario:** A downtown business district covered by a CDMA network.
- **9:00 AM (Low Traffic):** Cell towers cover a 2 km radius. A user in a suburban fringe connects perfectly.
- **12:00 PM (Lunch Rush):** Thousands of workers make calls. Interference spikes.
- **The Effect:** The cell radius shrinks to 1 km due to cell breathing. The user in the suburban fringe drops their call, not because they moved, but because the cell shrank away from them.
- **The Fix:** RF Engineers have to over-deploy base stations (adding more towers) to ensure coverage overlaps even at maximum shrinkage.

Lecture Summary

- CDMA is fundamentally interference-limited, meaning capacity is determined by the total noise on the shared frequency.
- The Near-Far problem is a critical vulnerability requiring complex, high-speed power control to manage.
- Cell Breathing causes coverage areas to shrink dynamically under heavy load, complicating network design.
- Commercial limitations, such as the lack of SIM cards and global roaming standardization, hindered CDMA's market share against GSM.

Next Lecture Preview

- In the next lecture, we will wrap up our discussion on 2G/3G limitations by looking at how they drove the industry forward:
- **1. The Evolution to 3G (UMTS/WCDMA & CDMA2000).**
- **2. The shift from Circuit Switched to Packet Switched.**
- **3. Why both GSM and CDMA were abandoned for OFDM in 4G LTE.**

Lecture 20: 2.12 Limitations of GSM and CDMA Technology (Part 3 - Evolution)

GSM and CDMA Systems

DI05011011: Mobile Communication

Agenda for Today

- 1. Summary of 2G Bottlenecks
- 2. The Data Demand Explosion
- 3. How 3G Addressed GSM Limitations (UMTS/WCDMA)
- 4. How 3G Addressed CDMA Limitations (EV-DO)
- 5. The Ultimate Limit of Spread Spectrum
- 6. The Paradigm Shift: Leaving CDMA for OFDM
- 7. Introduction to 4G LTE Concepts
- 8. Summary of Unit 2

Summary of 2G Bottlenecks

- **GSM's Core Flaws:**
- - Spectrally inefficient (TDMA rigid time slots).
- - Hard handoffs dropping calls.
- - Circuit-switched architecture unable to handle bursty IP data efficiently.
-
- **CDMA's Core Flaws:**
- - Interference limited (Near-far problem, cell breathing).
- - Enormous signaling overhead for power control.
- - Closed ecosystem, lacking global standardization initially.

The Data Demand Explosion

- **The Paradigm Shift:** Communication shifted from symmetrical voice (same data rate up and down) to asymmetrical data (heavy download, light upload).
- **Multimedia:** Users wanted to browse HTML web pages, send MMS, and eventually stream video.
- **IP Networking:** The world standardized on Internet Protocol (IP). 2G networks had to 'translate' IP packets over circuit-switched voice channels, which was incredibly slow and expensive.

3G: The WCDMA Compromise

- **The Solution to GSM:** The GSM world recognized CDMA's superior capacity and adopted it for 3G, creating **WCDMA (Wideband CDMA)**, part of the UMTS standard.
- **How it fixed GSM:**
- - Replaced rigid TDMA with spread spectrum, increasing capacity.
- - Implemented soft handoffs.
- - Used a wider 5 MHz channel (compared to GSM's 200 kHz) for higher data rates.
- **Retaining the Good:** Kept the GSM core network and SIM card architecture for seamless roaming.

3G: The CDMA2000 Path

- **The Solution for CDMA:** The CDMA camp evolved into CDMA2000 (and EV-DO).
- **How it improved:**
- - Dedicated entire carrier frequencies solely for packet data (EV-DO).
- - Implemented adaptive modulation (changing encoding based on signal strength).
- - Added SIM-like capabilities (CSIM/RUIM) to improve roaming.
- **The Result:** Provided broadband-like speeds (up to 3.1 Mbps) but maintained the inherent complexity of power control.

The Ultimate Limit of Spread Spectrum

- Even with 3G (WCDMA/EV-DO), the industry hit a new ceiling.
- **Multipath at High Speeds:** At very high data rates (broadband speeds), the multipath echoes in CDMA become so severe that the RAKE receivers cannot resolve them.
- **Inter-Symbol Interference (ISI):** The symbols arrive so fast they smear into each other.
- **The Conclusion:** Spread spectrum (CDMA) is excellent for voice and moderate data, but mathematically breaks down when trying to push 100+ Mbps.

The Paradigm Shift: OFDM

- **The 4G Solution:** To achieve true broadband speeds (LTE), the industry abandoned both TDMA (GSM) and CDMA completely.
- **Enter OFDM (Orthogonal Frequency Division Multiplexing):**
- - Instead of one fast, wide signal (CDMA), OFDM splits the data into hundreds of slow, narrow signals transmitted simultaneously.
- - Because each sub-signal is slow, multipath (ISI) is essentially eliminated.
- - Highly spectrally efficient and easily scalable.

The Shift to All-IP

- **4G LTE Core:** Alongside changing the RF technology to OFDM, 4G fundamentally changed the core network.
- **Death of Circuit Switching:** LTE is an 'All-IP' network. There are no dedicated voice circuits.
- **VoLTE (Voice over LTE):** Even voice calls are treated as IP data packets, just like a Skype or WhatsApp call, but with guaranteed Quality of Service (QoS) by the carrier.

Case Study: The Complete Transition

- **The Journey of a Carrier (e.g., AT&T/Vodafone):**
- - **1990s:** Deploys GSM (TDMA). Excellent roaming, poor data.
- - **2000s:** Upgrades to 3G UMTS (WCDMA). Adopts CDMA RF tech for better capacity, keeps SIMs.
- - **2010s:** Deploys 4G LTE (OFDM). Abandons CDMA RF tech entirely for OFDM, moves to All-IP core.
- - **2020s:** Shuts down 2G and 3G networks to refarm spectrum for 5G (Advanced OFDM).

Unit 2 Summary

- GSM (TDMA) provided global roaming and standardized digital voice but failed at high-speed data due to spectral inefficiency.
- CDMA provided higher capacity and soft handoffs but was plagued by complex power control and the near-far problem.
- 3G technologies attempted to blend the best of both (e.g., WCDMA).
- Ultimately, the limitations of spread spectrum at high data rates forced the entire industry to adopt OFDM and All-IP architectures for 4G LTE.

Next Lecture Preview

- In the next lecture, we transition to Unit 3, looking at the hardware in the user's hand:
- **1. Mobile Device Architecture.**
- **2. Mobile Handset Block Diagram.**
- **3. Baseband and RF Sections.**

Lecture 21: Limitations of GSM Technology - Part 1

GSM and CDMA Systems

DI05011011: Mobile Communication

Agenda for Today

- 1. Overview of GSM Limitations
- 2. Bandwidth and Data Rate Constraints
- 3. Spectral Efficiency Issues
- 4. Hard Handoff Drawbacks
- 5. Multipath Fading Vulnerabilities
- 6. Summary and Next Steps

1. Overview of GSM Limitations

- Designed primarily for voice communication, not high-speed data.
- Based on Circuit Switched technology, which is inefficient for bursty data traffic.
- Maximum basic data rate of only 9.6 kbps.
- Fixed channel bandwidth of 200 kHz limits flexibility.

2. The Data Rate Bottleneck

- **Original GSM Data Rate:** 9.6 kbps per user.
- Each user is assigned one time slot out of 8 in a TDMA frame.
- Voice is highly compressed (13 kbps vocoder), leaving little room for data.
- To download a 1 MB image at 9.6 kbps takes over 14 minutes.

Engineering Example: File Transfer over GSM

- **Scenario:** Sending a 500 KB email attachment over basic GSM.
- **Calculation:**
- - File size: 500 KB = 500 *1024* 8 bits = 4,096,000 bits.
- - Data Rate: 9.6 kbps = 9,600 bits per second.
- - Time = 4,096,000 / 9,600 = ˜426 seconds (over 7 minutes).
- **Conclusion:** Practical data applications required the development of GPRS (2.5G) and EDGE (2.75G) to combine multiple time slots.

3. Spectral Efficiency Issues

- **Spectral Efficiency:** Data rate transmitted over a given bandwidth (bps/Hz).
- GSM uses GMSK (Gaussian Minimum Shift Keying) modulation.
- GMSK provides constant envelope (good for battery) but poor spectral efficiency (˜1.35 bps/Hz).
- Requires frequency reuse planning (e.g., cluster size of 4, 7, or 12), wasting spectrum.

Frequency Reuse Constraint

- Adjacent cells cannot use the same frequencies (Co-channel interference).
- Only a fraction of the total allocated spectrum is available in a single cell (e.g., 1/7th in a 7-cell cluster).
- Unlike CDMA, where reuse factor is 1, GSM strictly partitions its spectrum.
- **Result:** Lower overall user capacity per square kilometer.

4. Hard Handoff Drawbacks

- GSM utilizes 'Hard Handoff' (Break-before-make).
- The mobile device drops the connection with the old base station before connecting to the new one.
- Creates a noticeable gap (interruption) in voice or data.
- Can lead to dropped calls if the target base station is congested.

5. Vulnerability to Multipath Fading

- Radio signals bounce off buildings, arriving at the receiver at different times (Multipath).
- In TDMA/GSM, delay spreads can cause Inter-Symbol Interference (ISI).
- If delay ¿ bit duration, symbols overlap and corrupt data.
- Requires complex Equalizers in the receiver to reconstruct the signal.

Timing Advance Limitation

- To prevent time slots from overlapping at the base station, mobiles far away must transmit earlier.
- This is called 'Timing Advance' (TA).
- GSM TA is limited to 63 steps, where each step is 3.69 microseconds.
- **Max Range:** This limits the absolute maximum radius of a standard GSM cell to exactly 35 kilometers.

Summary of GSM Limitations

- Low data rates (9.6 kbps).
- Circuit-switched inefficiency.
- Low spectral efficiency due to GMSK and frequency reuse.
- Hard handoffs causing dropped calls.
- Strict 35 km cell size limit due to Timing Advance.

Next Lecture Preview

- In the next lecture, we will explore:
- **Limitations of CDMA Technology:**
- 1. The Near-Far Problem
- 2. Cell Breathing
- 3. Complex Power Control Requirements

Lecture 22: Limitations of CDMA Technology

GSM and CDMA Systems

DI05011011: Mobile Communication

Agenda for Today

- 1. The Interference-Limited Nature of CDMA
- 2. The Near-Far Problem
- 3. Strict Power Control Requirements
- 4. Cell Breathing Phenomenon
- 5. Soft Handoff Overhead
- 6. Summary

1. CDMA: An Interference-Limited System

- In CDMA, all users transmit on the SAME frequency at the SAME time.
- Users are separated only by their unique spreading codes.
- Other users' signals act as background noise (interference).
- **Core Limitation:** The capacity of a CDMA cell is strictly limited by the total amount of interference the base station can tolerate.

2. The Near-Far Problem

- A critical issue in Direct Sequence CDMA (DS-CDMA).
- If a mobile device is very near the base station, its signal is received strongly.
- If another device is far away, its signal is received weakly.
- The strong signal from the near user will drown out the weak signal from the far user, acting as overwhelming interference.

3. Strict Power Control Requirements

- **The Solution:** The base station must ensure that signals from ALL mobile devices arrive at the exact same power level.
- Requires highly complex, fast power control algorithms.
- Base station sends power adjustment commands 800-1500 times per second.
- **Limitation:** If power control fails or is delayed, the entire cell's capacity degrades instantly.

Example: Power Control Loop

- **Scenario:** User A is driving towards the base station.
- 1. User A's signal gets stronger at the receiver.
- 2. Interference for User B (who is stationary) increases.
- 3. Base station detects User A is too loud.
- 4. BS sends 'Power Down' command to User A.
- 5. User A reduces power.
- 6. Equilibrium is restored.
- *This cycle repeats every 1.25 milliseconds.*

4. Cell Breathing Phenomenon

- In CDMA, the coverage area (footprint) of a cell changes dynamically based on traffic load.
- **Low Traffic:** Less interference, cell footprint expands, reaching users further away.
- **High Traffic:** More users = more interference. The base station cannot hear users at the edge. The effective cell footprint shrinks.
- This dynamic shrinking and expanding is called 'Cell Breathing'.

Consequences of Cell Breathing

- Network planners cannot guarantee coverage at the edges of a cell.
- A user who has a signal in the morning might lose it in the afternoon without moving, simply because the cell got busy and shrank.
- Requires complex deployment of overlapping cells to ensure no coverage gaps appear during peak load.

5. Soft Handoff Overhead

- CDMA uses 'Soft Handoff' (Make-before-break).
- A mobile device can connect to 2 or 3 base stations simultaneously during a handoff.
- **Advantage:** Very few dropped calls.
- **Limitation:** Consumes extra network resources (channel cards at multiple base stations) for a single user.

Code Scarcity and Orthogonality

- CDMA uses Walsh Codes to separate users within a cell.
- There is a finite number of mathematically perfectly orthogonal codes (e.g., 64 in IS-95).
- Multipath fading can destroy the orthogonality of these codes.
- When orthogonality is lost, users start interfering with each other, rapidly reducing capacity.

Summary of CDMA Limitations

- **Interference-Limited:** Capacity drops as noise increases.
- **Near-Far Problem:** Requires strict, rapid power control.
- **Cell Breathing:** Cell coverage shrinks as traffic increases.
- **Resource Overhead:** Soft handoffs tie up multiple base stations.
- **Code Limits:** Multipath interference ruins orthogonal codes.

Next Lecture Preview

- In the next lecture, we will conclude our discussion on 2G systems by comparing GSM and CDMA limitations, and discussing the specific security vulnerabilities of both systems that drove the push for 3G/4G standards.

Lecture 23: Security and System-Level Limitations

GSM and CDMA Systems

DI05011011: Mobile Communication

Agenda for Today

- 1. GSM Security Vulnerabilities (Unilateral Authentication)
- 2. The 'Stingray' / IMSI Catcher Threat
- 3. Ciphering Algorithm Weaknesses
- 4. CDMA Security Limitations
- 5. The Global Roaming Problem
- 6. Summary of the 2G Era

1. GSM Security: Unilateral Authentication

- In GSM, the network authenticates the mobile device (SIM card).
- **Major Flaw:** The mobile device DOES NOT authenticate the network.
- The phone simply trusts that any tower claiming to be its home network is legitimate.
- This is called 'Unilateral Authentication'.

2. The IMSI Catcher ('Stingray') Threat

- Because of Unilateral Authentication, attackers can create 'Fake Base Stations' (IMSI Catchers).
- The fake tower broadcasts a stronger signal than the legitimate tower.
- Phones automatically connect to the fake tower.
- The attacker can then intercept calls, read SMS, or track the user's location.

3. Ciphering Algorithm Weaknesses

- GSM uses A5/1 and A5/2 stream ciphers to encrypt voice data over the air.
- These algorithms were kept secret initially (Security by Obscurity).
- Both have been heavily reverse-engineered and cracked.
- A5/1 can now be decrypted in real-time using rainbow tables and a standard laptop.

Lack of End-to-End Encryption

- GSM encryption only exists 'Over-The-Air' (from the phone to the base station).
- Once the signal reaches the base station, it is decrypted and sent over the core network in plain text.
- Anyone with access to the core network (or the microwave links connecting towers) can intercept the communication.

4. CDMA Security Limitations

- CDMA inherently offers better privacy because signals are spread across a wide band and look like noise.
- However, early CDMA (IS-95) also lacked mutual authentication.
- While harder to intercept than GSM, it is not impossible.
- Key management and distribution in early CDMA networks were complex and prone to administrative errors.

5. The Global Roaming Problem

- 2G fragmented the world into two camps: GSM and CDMA.
- A GSM phone could not talk to a CDMA tower (different modulation, different protocols).
- Even within GSM, different regions used different frequencies (900/1800 MHz in Europe/Asia, 850/1900 MHz in the Americas).
- **Result:** Early phones only worked in their home continent.

The Push for a Unified Standard

- The limitations of 2G (low speed, poor security, lack of global roaming) drove the ITU to create the IMT-2000 standard (3G).
- Goals for 3G/4G included:
- 1. Mutual Authentication.
- 2. IP-based packet switching for high-speed data.
- 3. Unified global standards to allow true worldwide roaming.

Summary of Unit 2 Limitations

- **GSM:** Limited by TDMA slots, hard handoffs, and weak (unilateral) security.
- **CDMA:** Limited by interference (near-far problem, cell breathing).
- **Systemic:** Lack of mutual authentication allows IMSI catchers.
- **Global:** Incompatible standards and frequencies prevented easy international roaming.

Next Lecture Preview

- In Unit 3, we move away from the network and look at the device in your pocket.
- **Next Lecture:**
- 1. Mobile Handset Block Diagram
- 2. The Baseband Processor
- 3. The RF Transceiver Section

Lecture 24: Mobile Handset Architecture

Mobile Device

DI05011011: Mobile Communication

Agenda for Today

- 1. Overview of a Mobile Handset
- 2. General Block Diagram
- 3. The Antenna Section
- 4. The RF (Radio Frequency) Section
- 5. The Baseband Processor
- 6. Power Management and User Interface
- 7. Summary

1. Overview of a Mobile Handset

- A mobile handset is a highly complex, miniaturized two-way radio.
- It must simultaneously transmit and receive (Full Duplex).
- It contains computers (processors) more powerful than early desktop PCs.
- Requires extreme power efficiency to run on a small battery.

2. General Block Diagram

- The core architecture is divided into three main sections:
- **1. Radio Frequency (RF) Section:** Handles transmission and reception of analog radio waves.
- **2. Baseband Section:** Handles digital signal processing, coding, and modulation.
- **3. Application/UI Section:** Handles the OS, display, camera, and user inputs.

3. The Antenna Section

- The interface between the handset and the electromagnetic environment.
- Modern phones use internal antennas (e.g., PIFA - Planar Inverted-F Antenna).
- Must support multiple frequency bands (GSM, LTE, Wi-Fi, Bluetooth).
- Includes an **Antenna Switch** or **Duplexer** to separate transmit (Tx) and receive (Rx) signals.

4. The RF (Radio Frequency) Section

- **Receiver Path (Rx):**
- - Receives weak signal from the antenna.
- - Passes through an LNA (Low Noise Amplifier).
- - Down-converts the high-frequency radio signal to a lower intermediate frequency (IF) or directly to baseband.
- **Transmitter Path (Tx):**
- - Up-converts baseband signal to high radio frequencies.
- - Passes through a PA (Power Amplifier) before hitting the antenna.

The Role of the Power Amplifier (PA)

- The PA is located just before the transmitting antenna.
- It amplifies the signal to the required power level commanded by the base station.
- Draws heavy current from the battery.
- Generates significant heat, requiring careful thermal management in the handset design.

5. The Baseband Processor

- The 'brain' of the radio communications.
- A specialized DSP (Digital Signal Processor).
- **Functions:**
- - Analog-to-Digital (ADC) and Digital-to-Analog (DAC) conversion.
- - Speech coding/decoding (Vocoders).
- - Channel coding (adding error correction bits).
- - Encryption and Decryption.

Signal Flow: Transmitting Voice

- 1. Microphone captures sound (Analog audio).
- 2. Baseband ADC converts audio to Digital data.
- 3. Baseband compresses data and adds error correction.
- 4. Baseband passes digital data to RF Section.
- 5. RF Section up-converts data to a 1900MHz analog radio wave.
- 6. PA boosts the signal.
- 7. Antenna radiates the wave to the cell tower.

6. Power Management Unit (PMU)

- The unsung hero of the mobile handset.
- Takes the raw voltage from the battery and converts it into precisely regulated voltages for different chips.
- The RF PA might need 3.4V, the baseband processor might need 1.2V, and the screen might need 5V.
- Manages sleep modes to conserve battery when the phone is idle.

Summary

- A mobile handset consists of an Antenna, RF Section, Baseband Section, and Power Management.
- The **RF Section** handles high-frequency analog radio waves (amplification, up/down conversion).
- The **Baseband Section** handles digital signal processing (coding, encryption, modulation logic).
- The **PMU** ensures all these components receive the correct power efficiently.

Next Lecture Preview

- In the next lecture, we will dive deeper into power management:
- **1. Charging Control Section:** How does a phone safely charge?
- **2. Battery Types:** Lithium-Ion vs. Lithium-Polymer.
- **3. Battery Management Systems (BMS).**

Lecture 25: Charging Control & Battery Management

Mobile Device

DI05011011: Mobile Communication

Agenda for Today

- 1. Introduction to Mobile Batteries
- 2. Battery Types: Li-Ion vs. Li-Po
- 3. Battery Management System (BMS)
- 4. The Charging Control Section
- 5. Charging Phases (CC / CV)
- 6. Fast Charging Technologies
- 7. Summary

1. Introduction to Mobile Batteries

- Mobile phones require energy storage that is light, compact, and offers high energy density.
- Early phones used Nickel-Cadmium (NiCd) or Nickel-Metal Hydride (NiMH).
- These suffered from the 'Memory Effect' (losing maximum capacity if repeatedly partially discharged).
- Modern devices rely exclusively on Lithium-based chemistries.

2. Battery Types: Lithium-Ion (Li-Ion)

- **Lithium-Ion (Li-Ion):**
- - Uses a liquid solvent as an electrolyte.
- - Encased in a rigid metal shell (cylindrical or prismatic).
- - **Pros:** High energy density, relatively low manufacturing cost.
- - **Cons:** Heavier, rigid shape dictates phone design, liquid electrolyte is flammable if punctured.

Battery Types: Lithium-Polymer (Li-Po)

- **Lithium-Polymer (Li-Po):**
- - Uses a solid or gel-like polymer electrolyte.
- - Encased in a flexible foil pouch.
- - **Pros:** Ultra-thin, lightweight, can be molded into various shapes to fill empty space in a handset. Safer (less prone to leaking).
- - **Cons:** Slightly lower energy density than Li-Ion, higher manufacturing cost.

3. The Battery Management System (BMS)

- Lithium batteries are volatile and easily damaged by overcharging or deep discharging.
- A BMS is a small circuit board physically attached to the battery cell.
- **Functions:**
- - Prevents over-voltage during charging.
- - Prevents under-voltage (over-discharge) during use.
- - Monitors temperature to prevent thermal runaway.

4. The Charging Control Section

- Located on the main motherboard (PMIC - Power Management IC).
- Regulates the power coming from the USB port adapter.
- Communicates with the charger to negotiate voltage and current.
- Dynamically adjusts the charging current based on battery temperature and state of charge.

5. Charging Phases: CC and CV

- Charging a Lithium battery occurs in two main phases:
- **1. Constant Current (CC) Phase:**
- - Used from 0% to about 80% charge.
- - Charger supplies maximum safe current.
- - Battery voltage slowly rises.
- **2. Constant Voltage (CV) Phase:**
- - Used from 80% to 100%.
- - Voltage is held steady (usually 4.2V or 4.35V).
- - Current gradually decreases to near zero as the battery tops off.

Graph: CC-CV Charging Profile

- (Imagine a graph here)
- - **X-Axis:** Time
- - **Y-Axis:** Current / Voltage
- - **Phase 1 (CC):** Current line is flat (high), Voltage line curves upward.
- - **Phase 2 (CV):** Voltage line is flat (max), Current line curves steeply downward.
- When Current drops below a termination threshold (e.g., 50mA), the charging control IC stops charging completely.

6. Fast Charging Technologies

- Standard USB provides 5V at 1A or 2A (5W or 10W).
- Fast charging (Qualcomm Quick Charge, USB-PD, VOOC) negotiates higher voltages (9V, 12V, 20V) to deliver more power (18W, 65W, 100W+).
- Higher voltage means less current for the same power, reducing heat in the charging cable.
- The Charging IC in the phone steps the voltage back down to safely charge the battery.

Summary

- Modern handsets rely on Lithium-Ion or Lithium-Polymer batteries.
- The Battery Management System (BMS) ensures safe operation limits (voltage, temperature).
- The Charging Control IC manages the CC (Constant Current) and CV (Constant Voltage) charging phases.
- Fast charging standards dynamically negotiate voltage to decrease charge times safely.

Next Lecture Preview

- In the next lecture, we will explore:
- **1. The SIM Card:** What is inside it?
- **2. SIM Interface:** How does the phone talk to it?
- **3. eSIM Technology:** The shift away from physical cards.

Lecture 26: SIM Card and Interface, eSIM Concept and Advantages

Mobile Device

DI05011011: Mobile Communication

Agenda for Today

- 1. Introduction to SIM (Subscriber Identity Module)
- 2. SIM Card Physical Evolution
- 3. SIM Card Architecture
- 4. Security in SIM (Ki, PIN, PUK)
- 5. SIM Card Interface
- 6. What is eSIM? (Embedded SIM)
- 7. eSIM Architecture (eUICC)
- 8. Remote SIM Provisioning (RSP)
- 9. Advantages of eSIM
- 10. Traditional SIM vs eSIM Comparison

Introduction to SIM

- **SIM** stands for Subscriber Identity Module.
- It is an integrated circuit (IC) that securely stores the International Mobile Subscriber Identity (IMSI) number.
- The IMSI uniquely identifies a subscriber on a mobile network.
- Without a SIM card, a GSM or LTE phone cannot authenticate and connect to a carrier's network.
- It also stores SMS messages, contact information, and network-specific data.

SIM Card Physical Evolution

- Over the years, the physical size of SIM cards has drastically reduced to save space in mobile devices.
- **Full-size SIM (1FF):** Credit card size, used in early cell phones.
- **Mini-SIM (2FF):** The 'standard' SIM used in early 2000s.
- **Micro-SIM (3FF):** Introduced with smartphones like iPhone 4.
- **Nano-SIM (4FF):** Currently the most common physical SIM, with almost zero plastic border around the chip.

SIM Card Architecture

- A SIM card is a smart card containing a microcomputer.
- **CPU:** A microprocessor for executing security algorithms.
- **ROM (Read-Only Memory):** Contains the operating system of the SIM.
- **RAM (Random Access Memory):** Used for temporary data processing during execution.
- **EEPROM (Electrically Erasable Programmable Read-Only Memory):** Non-volatile memory storing user data (IMSI, contacts, SMS, Ki).

Security in SIM

- **Ki (Authentication Key):** A 128-bit key stored securely on the SIM. It never leaves the SIM card. It is used to authenticate the user to the network.
- **PIN (Personal Identification Number):** Protects the SIM from unauthorized use. User must enter it when turning on the phone.
- **PUK (Personal Unblocking Key):** Used to unblock a SIM if the PIN is entered incorrectly too many times.

SIM Card Interface Pins

- A standard SIM card has electrical contacts (pads) that interface with the mobile phone.
- **VCC (C1):** Power supply voltage.
- **RST (C2):** Reset signal.
- **CLK (C3):** Clock signal for timing.
- **GND (C5):** Ground reference.
- **VPP (C6):** Programming voltage (rarely used in modern SIMs).
- **I/O (C7):** Serial Input/Output for data transfer.

Example: SIM Interface Communication

- **Scenario:** Mobile phone powers on.
- 1. Phone applies **VCC** (Power) to the SIM.
- 2. Phone provides **CLK** (Clock) signal.
- 3. Phone sends **RST** (Reset) to initialize the SIM.
- 4. SIM responds on the **I/O** line with an ATR (Answer To Reset) string, indicating its capabilities.
- 5. Phone and SIM begin exchanging APDUs (Application Protocol Data Units) for authentication.

What is eSIM? (Embedded SIM)

- **eSIM (embedded SIM)** is a programmable SIM card that is permanently soldered into the device's motherboard.
- It eliminates the need for a physical, removable SIM card.
- Standardized by the GSMA (Global System for Mobile Communications Association).
- Allows users to change service providers over-the-air (OTA) without swapping physical cards.

eSIM Architecture (eUICC)

- The hardware component of an eSIM is called **eUICC (embedded Universal Integrated Circuit Card)**.
- Unlike a traditional SIM which holds a single network profile, an eUICC can hold multiple profiles simultaneously.
- Only one profile is typically active at a time, but switching is instant.
- Contains strong cryptographic enclaves to securely download and install operator credentials.

Remote SIM Provisioning (RSP)

- **RSP** is the GSMA specification that allows a device to securely download a SIM profile over the internet.
- **SM-DP+ (Subscription Manager Data Preparation):** The server that securely encrypts and delivers the operator profile to the eSIM.
- **LPA (Local Profile Assistant):** Software on the device that interacts with the SM-DP+ and user interface to manage profiles.
- User typically scans a QR code or uses a carrier app to trigger RSP.

Advantages of eSIM

- **Space Saving:** Tiny footprint compared to a Nano-SIM tray mechanism, allowing for larger batteries or thinner devices.
- **Water/Dust Resistance:** Removing the SIM tray removes a major point of ingress for water and dust.
- **Easy Switching:** Users can switch carriers instantly, beneficial for international travel.
- **IoT Enabler:** Ideal for connected cars, smartwatches, and industrial IoT where swapping physical SIMs is impractical.
- **Logistics:** Carriers don't need to manufacture and ship plastic cards.

Traditional SIM vs eSIM Comparison

- — Feature — Traditional SIM — eSIM (eUICC) —
- ——————————
- — **Form Factor** — Removable Plastic Card — Soldered IC (MFF2) —
- — **Provisioning** — Pre-programmed by carrier — Remote SIM Provisioning (OTA) —
- — **Profiles** — Single Profile — Multiple Profiles —
- — **Device Design** — Requires slot/tray — Saves space, better sealing —
- — **Logistics** — Physical shipping required — Digital delivery (QR code/App) —

Summary

- The SIM card is a smart card that securely authenticates a mobile subscriber to a network.
- It contains a CPU, memory, and interfaces via standardized pins (VCC, CLK, I/O).
- eSIM (eUICC) replaces the removable card with a soldered, programmable chip.
- Remote SIM Provisioning (RSP) allows for OTA carrier switching.
- eSIMs offer significant advantages in device design, IoT scalability, and user convenience.

Next Lecture Preview

- In the next lecture, we will explore the internal architecture of the smartphone itself:
- **1. Smartphone Architecture:** System on Chip (SoC)
- **2. Mobile Sensors:** Accelerometer, Gyroscope, etc.
- **3. Introduction to Mobile OS:** Basics of Android architecture.

Lecture 27: Smartphone Architecture and Mobile OS (Android)

Mobile Device

DI05011011: Mobile Communication

Agenda for Today

- 1. Introduction to Smartphone Architecture
- 2. System on Chip (SoC) Concept
- 3. Core Components of SoC
- 4. Modems and Connectivity in SoC
- 5. Smartphone Sensors Overview
- 6. Common Sensors (Motion & Position)
- 7. Environmental Sensors
- 8. Sensor Fusion Example
- 9. Introduction to Mobile OS
- 10. What is Android?
- 11. Android Architecture: Linux Kernel
- 12. Android Architecture: Middleware & Runtime
- 13. Android Architecture: Application Framework
- 14. Summary
- 15. Preview

Smartphone Architecture Overview

- A smartphone is fundamentally a highly integrated, battery-powered, miniaturized computer.
- **Key Modules:**
- 1. **Processing & Control:** System on Chip (SoC)
- 2. **Memory:** RAM (Volatile) and Storage (NAND Flash, UFS)
- 3. **Power Management:** PMIC (Power Management IC) and Battery
- 4. **I/O and Sensors:** Display, touch, cameras, audio, and environmental sensors.
- 5. **Connectivity:** Cellular modem, Wi-Fi, Bluetooth, NFC, GPS.

System on Chip (SoC) Concept

- An **SoC** integrates almost all critical components of a computer or electronic system into a single silicon chip.
- In a smartphone, it replaces the traditional CPU, GPU, chipset, and modem found on separate chips in a PC.
- **Why SoC?**
- - Space saving (critical for mobile devices).
- - Lower power consumption.
- - Faster communication between integrated components.
- Examples: Qualcomm Snapdragon, Apple A-Series, Samsung Exynos, MediaTek Dimensity.

Core Components of an SoC

- **CPU (Central Processing Unit):** General-purpose processing, runs the OS and apps (usually ARM architecture).
- **GPU (Graphics Processing Unit):** Handles UI rendering, gaming, and video playback.
- **NPU (Neural Processing Unit):** Specialized for AI/Machine Learning tasks (e.g., face recognition, computational photography).
- **ISP (Image Signal Processor):** Processes raw data from the camera sensors into JPEG/HEIC images.
- **DSP (Digital Signal Processor):** Handles audio processing and sensor data efficiently.

Modems and Connectivity in SoC

- Modern SoCs integrate the cellular modem directly into the silicon to save power.
- **Baseband Processor/Modem:** Handles all radio functions, modulation, demodulation, and encoding for 4G/5G.
- **Wi-Fi/Bluetooth Subsystem:** Manages local wireless connections.
- **Location Subsystem:** Integrates GPS, GLONASS, Galileo for positioning.
- Integrating the modem requires complex shielding to prevent interference with the CPU/GPU.

Smartphone Sensors Overview

- Sensors provide the smartphone with awareness of its physical environment.
- They are micro-electromechanical systems (MEMS), incredibly small mechanical devices built on silicon chips.
- They operate via the I2C or SPI interface to communicate with the SoC's sensor hub or DSP.
- Without sensors, a smartphone cannot adapt to user context (orientation, brightness, movement).

Common Sensors (Motion & Position)

- **Accelerometer:** Measures linear acceleration (including gravity) across 3 axes (X, Y, Z). Used for step counting and basic tilt detection.
- **Gyroscope:** Measures angular rotational velocity. Used for precise motion tracking, VR, and camera stabilization (OIS).
- **Magnetometer (Compass):** Measures magnetic fields to determine North. Used for maps and navigation.

Environmental & User Sensors

- **Proximity Sensor:** Emits infrared light to detect objects near the screen. Used to turn off the display during calls to prevent accidental touches.
- **Ambient Light Sensor (ALS):** Measures environmental light levels. Used to auto-adjust screen brightness.
- **Barometer:** Measures atmospheric pressure. Helps determine altitude for fitness tracking and faster GPS locks.
- **Biometric Sensors:** Fingerprint scanners (optical/ultrasonic) and 3D facial recognition (IR dot projectors).

Sensor Fusion Example: Auto-Rotate

- How does a phone know to switch from Portrait to Landscape?
- 1. **Accelerometer** detects a change in the direction of gravity across its X/Y axes.
- 2. **Gyroscope** confirms a rotational movement occurred.
- 3. **Sensor Hub (DSP)** combines this data ('Sensor Fusion') to confidently conclude the phone was rotated.
- 4. DSP interrupts the **CPU**, which tells the **OS** to redraw the UI in landscape mode via the **GPU**.

Introduction to Mobile Operating Systems

- A Mobile OS is software that manages mobile hardware resources and provides common services for mobile applications.
- It acts as a bridge between the user/apps and the complex SoC hardware.
- **Key constraints for Mobile OS:**
- - Strict power management (Battery limits).
- - Limited RAM compared to PCs.
- - Touch-based user interfaces.
- - Security and app sandboxing.

What is Android?

- Android is an open-source mobile operating system developed by Google (via the Open Handset Alliance).
- It is based on a modified version of the Linux kernel.
- It uses a software stack architecture to isolate different levels of functionality.
- Applications are primarily written in Java or Kotlin.
- Dominates the global smartphone market share due to its open nature.

Android Architecture: Kernel & HAL

- **1. Linux Kernel (The Foundation):**
- - Handles core system services: memory management, process management, network stack, and drivers.
- - Provides power management (wakelocks).
- **2. Hardware Abstraction Layer (HAL):**
- - Defines standard interfaces for hardware vendors to implement.
- - Allows the higher-level OS to interact with hardware (camera, bluetooth, audio) without knowing the low-level driver specifics.

Android Architecture: Runtime & Libraries

- **3. Android Runtime (ART):**
- - The engine that runs Android applications.
- - Compiles Java/Kotlin bytecode into native machine code (Ahead-Of-Time compilation).
- - Includes Core Libraries providing Java API interfaces.
- **4. Native C/C++ Libraries:**
- - Core libraries used by the OS for heavy lifting.
- - Includes WebKit/Blink (browser engine), OpenGL/Vulkan (graphics), and SQLite (database).

Android Architecture: Framework & Apps

- **5. Application Framework:**
- - The API block that developers use to write apps.
- - Includes Activity Manager (lifecycle), Window Manager (UI), Location Manager, and Notification Manager.
- **6. System and User Apps:**
- - The top layer that users interact with.
- - Includes pre-installed apps (Dialer, SMS, Settings) and third-party apps downloaded from the Play Store.

Summary

- An SoC integrates CPU, GPU, NPU, ISP, and Modems into a single power-efficient chip.
- MEMS sensors (Accelerometer, Gyroscope, Proximity) provide environmental context.
- Sensor Fusion combines data for accurate tracking.
- Android is a Linux-based OS designed for power efficiency and touch interfaces.
- Its architecture relies on a stack: Kernel -¿ HAL -¿ Runtime/Libraries -¿ Framework -¿ Apps.

Next Lecture Preview

- In the next lecture, we will discuss a critical safety aspect of mobile communication:
- **1. Radiation Hazards:** Understanding electromagnetic radiation.
- **2. Ionizing vs. Non-Ionizing Radiation.**
- **3. Specific Absorption Rate (SAR):** Definition and basics.

Lecture 28: Radiation Hazards and SAR (Part 1: Fundamentals)

Mobile Device

DI05011011: Mobile Communication

Agenda for Today

- 1. Introduction to Electromagnetic Radiation
- 2. The Electromagnetic Spectrum
- 3. Ionizing vs. Non-Ionizing Radiation
- 4. Mobile Phones and RF Radiation
- 5. How RF Waves Interact with the Human Body
- 6. Thermal Effects of RF Radiation
- 7. Non-Thermal Effects (Ongoing Debate)
- 8. What is SAR? (Specific Absorption Rate)
- 9. SAR Definition and Formula
- 10. Understanding SAR Values
- 11. Tissue Types and SAR Absorption
- 12. Factors Influencing Radiation Exposure
- 13. Summary
- 14. Preview

Introduction to Electromagnetic Radiation

- **Electromagnetic (EM) Radiation** is energy that travels through space at the speed of light in the form of waves.
- It consists of oscillating electric and magnetic fields.
- Characterized by:
- - **Wavelength:** Distance between consecutive peaks.
- - **Frequency (Hz):** Number of cycles per second.
- - **Energy:** Higher frequency = Higher energy.
- Mobile communication relies entirely on transmitting and receiving EM radiation.

The Electromagnetic Spectrum

- The EM spectrum spans from very low frequencies to extremely high frequencies.
- 1. Radio Waves (AM/FM, Mobile Phones)
- 2. Microwaves (Wi-Fi, Radar, Ovens)
- 3. Infrared (Heat)
- 4. Visible Light
- 5. Ultraviolet (UV)
- 6. X-Rays
- 7. Gamma Rays
- Mobile phones operate in the Radio Frequency (RF) and Microwave spectrum (approx. 700 MHz to 39 GHz).

Ionizing vs. Non-Ionizing Radiation

- This is the most critical distinction in radiation safety.
- **Ionizing Radiation (Harmful):**
- - High energy (UV, X-Rays, Gamma Rays).
- - Has enough energy to tightly strip electrons from atoms, breaking chemical bonds and damaging DNA directly. Causes cancer.
- **Non-Ionizing Radiation (Safe/Heating):**
- - Low energy (Radio, Microwave, Infrared, Visible).
- - Does NOT have enough energy to break molecular bonds or damage DNA.
- - Primary effect is excitation/heating of molecules.

Mobile Phones and RF Radiation

- Mobile phones are low-power, two-way radio transceivers.
- They contain transmitters that emit RF energy (radiation) via their antennas.
- Because the phone is held close to the head or body, a portion of this RF energy is absorbed by human tissues.
- The amount of power emitted varies dynamically based on distance to the cell tower and data transmission rates.

How RF Waves Interact with the Human Body

- When RF waves penetrate the human body, they interact with tissues, which are largely composed of water.
- Water molecules are polar. The oscillating EM field causes these molecules to vibrate and rotate rapidly.
- This rapid vibration creates friction at the molecular level.
- Friction produces heat. This is the exact same principle used in a microwave oven, but at a vastly smaller power scale.

Thermal Effects of RF Radiation

- The only universally scientifically proven biological effect of RF radiation is **heating (thermal effect)**.
- The human body's thermoregulatory system (blood flow, sweating) can easily dissipate small amounts of localized heat.
- However, excessive RF power could potentially cause tissue damage (e.g., in the eyes, which have poor blood flow).
- Regulatory limits are established well below the threshold where harmful heating occurs.

Non-Thermal Effects (The Debate)

- Some studies suggest that RF radiation might cause biological effects without raising temperature (Non-thermal effects).
- Proposed non-thermal effects include:
- - Blood-brain barrier permeability changes.
- - Altered sleep patterns or EEG activity.
- - Cellular stress responses.
- **Consensus:** The WHO and major health organizations maintain that there is currently no conclusive evidence that low-level, non-thermal RF exposure causes adverse health effects.

What is SAR? (Specific Absorption Rate)

- Because we know RF causes heating, we need a way to measure how much RF energy the body absorbs.
- **Specific Absorption Rate (SAR)** is the measure of the rate at which energy is absorbed by the human body when exposed to a radio frequency (RF) electromagnetic field.
- It provides a standardized metric to evaluate the safety of mobile devices.
- Lower SAR means less energy is absorbed.

SAR Definition and Formula

- SAR is defined as the power absorbed per mass of tissue.
- **Formula:** SAR $= \sigma$—E—^2 / ρ
- Where:
- - σ **(sigma):** Electrical conductivity of the tissue (S/m)
- - **E:** RMS electric field strength (V/m) inside the tissue
- - ρ **(rho):** Mass density of the tissue (kg/m^3)
- **Unit of Measurement:** Watts per kilogram (W/kg).

Understanding SAR Values

- A SAR value represents the maximum exposure condition.
- Phones are tested at their highest possible power level, in various positions against the head and body.
- The SAR value reported for a phone is the highest single value found during all these tests.
- In normal daily use, a phone operates at a fraction of its maximum SAR value.

Tissue Types and SAR Absorption

- SAR is not uniform across the body. Different tissues absorb RF differently.
- Tissues with high water and ion content (like muscle, brain) have higher conductivity and absorb more RF.
- Tissues with low water content (like bone, fat) absorb less RF.
- Frequencies also matter: Lower frequencies penetrate deeper into the body, while higher frequencies (like 5G mmWave) are absorbed mostly by the skin.

Factors Influencing Radiation Exposure

- Even with a phone of a specific SAR rating, your actual exposure depends on:
- 1. **Distance from Cell Tower:** Poor signal forces the phone to transmit at max power.
- 2. **Distance from Body:** Using a speakerphone reduces exposure exponentially (Inverse Square Law).
- 3. **Call Duration:** Longer calls = longer exposure.
- 4. **Data Transmission vs Voice:** Downloading files uses more continuous power than listening during a call.

Summary

- Mobile phones emit non-ionizing RF radiation, which cannot break DNA but can cause localized tissue heating.
- The thermal effect is the only proven biological impact of RF radiation.
- SAR (Specific Absorption Rate) measures how much RF energy the body absorbs.
- SAR is measured in W/kg and represents a worst-case scenario at maximum power.
- Actual exposure depends heavily on usage habits and network conditions.

Next Lecture Preview

- In Part 2 of Radiation Hazards and SAR, we will cover:
- **1. SAR Measurement:** How is SAR practically measured in labs using phantoms?
- **2. Regulatory Standards:** ICNIRP and FCC limits.
- **3. Mobile Design:** How engineers design antennas to minimize SAR.

Lecture 29: Radiation Hazards and SAR (Part 2: Measurement & Standards)

Mobile Device

DI05011011: Mobile Communication

Agenda for Today

- 1. How is SAR Measured?
- 2. SAR Measurement Equipment (Phantoms)
- 3. SAR Measurement Equipment (Probes & Liquid)
- 4. International Regulatory Bodies
- 5. SAR Limits by ICNIRP (10g Tissue)
- 6. SAR Limits by FCC (1g Tissue)
- 7. Comparing ICNIRP vs FCC
- 8. Mobile Phone Design and SAR Reduction
- 9. Antenna Placement Strategies
- 10. Dynamic Power Control (DPC)
- 11. SAR Sensors in Modern Smartphones
- 12. Real-world SAR Testing Scenarios
- 13. Summary
- 14. Preview

How is SAR Measured?

- You cannot accurately measure SAR on a living human due to obvious ethical and practical reasons.
- Instead, SAR is measured in specialized RF laboratories using simulated human heads and bodies.
- The device under test (DUT) is forced to transmit at its absolute maximum power across all its frequency bands.
- A robotic arm with an electric field probe maps the RF energy absorbed inside the simulated tissue.

SAR Measurement Equipment (Phantoms)

- **Phantoms** are physical models representing the human body.
- **SAM (Specific Anthropomorphic Mannequin):** A standardized head phantom based on the 90th percentile of adult male head sizes.
- **Flat Phantoms:** Used to simulate body-worn usage (e.g., phone in a pocket).
- The phantoms are constructed from a thin fiberglass shell.

SAR Measurement Equipment (Probes & Liquid)

- **Tissue Simulating Liquid (TSL):** The phantoms are filled with a liquid recipe (water, sugar, salt, cellulose) that exactly mimics the dielectric properties of human brain/muscle tissue.
- Different frequencies require different liquid recipes.
- **E-Field Probes:** Miniature antennas on the end of a robotic arm that dip into the liquid.
- The probe measures the electric field strength at hundreds of points inside the phantom.

International Regulatory Bodies

- Two main organizations set the global guidelines for RF exposure limits:
- 1. **ICNIRP** (International Commission on Non-Ionizing Radiation Protection): Adopted by Europe, Australia, and most of the world.
- 2. **FCC** (Federal Communications Commission): Adopted by the USA, Canada, and parts of Asia.
- Both base their limits on preventing the body temperature from rising by 1°C.

SAR Limits by ICNIRP

- **Limit:** 2.0 W/kg.
- **Averaging Mass:** Averaged over 10 grams of contiguous tissue.
- **Why 10g?** It represents a volume roughly the size of a golf ball. ICNIRP believes this better represents the macroscopic heating effect.
- Generally considered a slightly less stringent measurement method than the FCC.

SAR Limits by FCC

- **Limit:** 1.6 W/kg.
- **Averaging Mass:** Averaged over 1 gram of contiguous tissue.
- **Why 1g?** It represents a much smaller volume, roughly the size of a sugar cube. It is designed to capture peak localized hotspots more aggressively.
- Generally considered the most stringent SAR standard in the world.

Comparing ICNIRP vs FCC

- You cannot directly compare an FCC SAR value with an ICNIRP SAR value.
- - A phone might have an FCC SAR of 1.2 W/kg (1g) and an ICNIRP SAR of 0.8 W/kg (10g).
- - The 1g measurement will almost always result in a higher calculated number because it finds smaller, more intense hotspots.
- - Both limits incorporate a safety factor of 50x below the known threshold for thermal damage.

Mobile Phone Design and SAR Reduction

- Engineers must carefully design smartphones to pass these strict regulations.
- Key strategies include:
- 1. Antenna Placement.
- 2. Material selection (RF shielding).
- 3. Software-controlled Dynamic Power Control.
- 4. Hardware SAR sensors.

Antenna Placement Strategies

- The antenna is the source of the radiation.
- **Historically:** Antennas were at the top of the phone (near the ear/brain).
- **Modern Design:** Primary cellular antennas are often moved to the bottom of the phone, near the microphone.
- This places the radiation source closer to the jaw/neck and further from the brain, reducing head SAR significantly.

Dynamic Power Control (DPC)

- The base station (cell tower) and the mobile phone constantly talk to adjust transmit power.
- If a phone has a strong signal, the tower tells it to turn its transmit power down.
- This saves battery and dramatically reduces SAR.
- A phone only transmits at maximum power (the tested SAR value) when it has a very weak signal (e.g., deep inside a building).

SAR Sensors in Modern Smartphones

- Many modern smartphones, especially tablets and 5G devices, include dedicated 'SAR Sensors' (usually capacitive proximity sensors).
- These sensors detect if a human body part is very close to the transmitting antenna.
- If flesh is detected, the phone automatically forces the modem to lower its transmit power limit to ensure it stays below regulatory limits.
- If the phone is placed on a table (no flesh detected), it transmits at higher power.

Summary

- SAR is measured in labs using SAM phantoms and tissue-simulating liquids.
- ICNIRP (10g, 2.0 W/kg) and FCC (1g, 1.6 W/kg) set the global safety limits.
- Both standards provide a 50x safety margin against thermal damage.
- Engineers reduce SAR via antenna placement (bottom of phone) and dynamic power control.
- Modern devices use capacitive sensors to back off power when near the body.

Next Lecture Preview

- In our final lecture on Radiation Hazards, we will explore:
- **1. Mitigation Techniques for Users:** How you can reduce your exposure.
- **2. Public Perception:** Addressing common myths and fears.
- **3. 5G Technology:** Are millimeter waves more dangerous?

Lecture 30: Radiation Hazards and SAR (Part 3: Mitigation & Future)

Mobile Device

DI05011011: Mobile Communication

Agenda for Today

- 1. Mitigation Techniques for Users
- 2. The Inverse Square Law in Practice
- 3. Impact of Network Coverage
- 4. Base Station vs. Mobile Device Radiation
- 5. Public Perception and Misconceptions
- 6. Epidemiological Studies
- 7. The Precautionary Principle
- 8. 5G Technology and Radiation
- 9. Millimeter Waves (mmWave)
- 10. Skin Depth and Absorption
- 11. Beamforming in 5G
- 12. Example: 4G Broadcast vs 5G Beamforming
- 13. Summary of Radiation Hazards
- 14. Preview

Mitigation Techniques for Users

- While compliant phones are considered safe, users who wish to apply the precautionary principle can reduce their exposure:
- 1. **Use Hands-Free Options:** Speakerphone, wired earphones, or Bluetooth headsets.
- 2. **Text Instead of Call:** Texting keeps the phone away from the head and transmits data in short bursts.
- 3. **Limit Call Duration:** Shorter calls mean less total energy absorbed.
- 4. **Avoid Low Signal Areas:** Do not make long calls when you have 1 bar of signal.

The Inverse Square Law in Practice

- RF energy obeys the **Inverse Square Law**: Intensity is inversely proportional to the square of the distance from the source.
- Moving a phone just a few inches away from your head drops the absorbed energy dramatically.
- - Distance = 1 cm -¿ Power = 100%
- - Distance = 2 cm -¿ Power = 25%
- - Distance = 10 cm -¿ Power = 1%
- This is why speakerphones and headsets are so effective.

Base Station vs. Mobile Device Radiation

- A common public fear is living near a cell tower (Base Station).
- **Fact:** You receive vastly more radiation from the phone in your pocket than from a tower 100 meters away.
- Base stations transmit at higher power (20W - 100W), but because of the inverse square law, the energy reaching the ground is minuscule.
- Protesting a cell tower in your neighborhood ironically forces your phone to transmit at maximum power, increasing your personal exposure.

Public Perception and Misconceptions

- **Myth:** 'Radiation from phones causes brain tumors.'
- **Reality:** Major epidemiological studies (studying millions of users over decades) have not found a conclusive link between phone use and brain cancer rates.
- While cell phone use has skyrocketed since the 1990s, brain cancer incidence rates have remained flat.
- Organizations like IARC classify RF as 'possibly carcinogenic' (Group 2B)—the same category as pickled vegetables and aloe vera extract.

The Precautionary Principle

- Because latency periods for some cancers can be 20-30 years, continuous monitoring is required.
- Health agencies advocate the **Precautionary Principle**: taking reasonable measures to avoid exposure just in case unknown risks exist.
- This is why SAR limits have massive safety margins (50x below harm threshold) built into them.
- Special attention is given to children, as their skulls are thinner and brains are still developing.

5G Technology and Radiation

- The rollout of 5G caused significant public concern.
- 5G uses three spectrum bands:
- 1. **Low-band:** Similar to 4G (sub-1 GHz).
- 2. **Mid-band:** Similar to Wi-Fi (1 - 6 GHz).
- 3. **High-band (mmWave):** 24 GHz to 100 GHz. (This is the new part).
- Despite the higher frequencies, 5G is still **strictly non-ionizing**.

Millimeter Waves (mmWave) and Skin Depth

- Physics dictates that the higher the frequency, the lower the penetration depth into biological tissue.
- 4G frequencies penetrate a few centimeters into the body.
- **5G mmWave frequencies penetrate only a few millimeters.**
- They are almost entirely absorbed by the outer layers of the skin and the cornea of the eye.
- They do not reach the brain or internal organs.

Beamforming in 5G

- 4G cell towers broadcast RF energy in a wide sector (like a floodlight), exposing everyone in the area.
- 5G uses **Massive MIMO and Beamforming**.
- Beamforming acts like a spotlight. It directs a focused beam of RF energy directly to the user's device, and nowhere else.
- Result: Ambient RF exposure for people not actively using their devices is significantly reduced in a 5G network compared to 4G.

Example: 4G Broadcast vs 5G Beamforming

- **Scenario:** You are sitting on a park bench. Someone 10 meters away is downloading a large movie.
- - **In a 4G network:** The tower blasts a wide signal. Both you and the downloader are bathed in the RF energy.
- - **In a 5G network:** The tower creates a targeted beam to the downloader's phone. You, sitting 10m away, receive almost zero RF energy from that transmission.

Summary of Radiation Hazards

- Users can minimize exposure via distance (headsets) and ensuring good signal.
- Living near cell towers actually reduces your personal device's transmit power.
- Decades of research show no conclusive link between non-ionizing RF and cancer.
- 5G utilizes mmWaves which do not penetrate deep into the body.
- 5G beamforming reduces ambient RF pollution compared to older broadcast technologies.

Next Lecture Preview

- In the next lecture, we transition to a new unit: 4G and 5G Networks.
- **1. Introduction to 4G technology:** The shift to pure IP networks.
- **2. Features of 4G.**
- **3. Types of 4G:** LTE vs WiMAX.

Lecture 31: Radiation hazards and SAR - Advanced Topics and Safety Standards

Mobile Device

DI05011011: Mobile Communication

Agenda for Today

- 1. Recap of SAR
- 2. Thermal vs. Non-Thermal Effects
- 3. Safety Standards (ICNIRP, FCC)
- 4. SAR Measurement Techniques
- 5. The SAM Phantom Model
- 6. Factors Affecting SAR Values
- 7. Mitigation and Safety Guidelines
- 8. Example: Calculating SAR Limits
- 9. Summary & Q&A

Recap: What is SAR?

- **Specific Absorption Rate (SAR)** measures the rate at which RF energy is absorbed by the human body.
- It is measured in Watts per kilogram (W/kg).
- SAR values indicate the maximum energy absorbed from a mobile device under worst-case operating conditions.
- A lower SAR value indicates less radiation absorption.

Biological Effects of RF Radiation

- **Thermal Effects:**
- - Heating of biological tissue due to energy absorption.
- - Human body can dissipate small amounts of heat, but excessive heat can cause tissue damage.
- **Non-Thermal Effects:**
- - Biological changes occurring without significant temperature rise.
- - Still a subject of ongoing scientific debate and extensive research.

Regulatory Bodies and Safety Standards

- **1. ICNIRP (International Commission on Non-Ionizing Radiation Protection):**
- - Sets the SAR limit at 2.0 W/kg averaged over 10 grams of tissue.
- **2. FCC (Federal Communications Commission):**
- - Sets a more stringent SAR limit of 1.6 W/kg averaged over 1 gram of tissue.
- - Devices must comply with these limits.

How is SAR Measured?

- SAR measurement is a highly standardized laboratory process.
- **Key Components:**
- 1. **Anechoic Chamber:** An RF-shielded room to block external interference.
- 2. **Phantom:** A realistic model of a human head or body.
- 3. **Tissue-Simulating Liquid:** Mimics the electrical properties of human tissue.
- 4. **Robotic Arm:** Moves an E-field probe inside the liquid to measure RF energy.

The SAM Phantom

- The Specific Anthropomorphic Mannequin (SAM) phantom.
- - Based on the anatomical dimensions of a large adult male.
- - Represents the 90th percentile of the male population.
- - Ensures that the model overestimates the exposure for most users.
- - Includes specific reference points for standardized placement.

Testing Configurations

- Mobile phones are tested in various positions to reflect real-world usage:
- **Head SAR:**
- - 'Cheek' position: Phone pressed flat against the ear.
- - 'Tilt' position: Phone angled at 15 degrees.
- **Body-Worn SAR:**
- - Tested with a separation distance (usually 5mm to 15mm) to simulate carrying.

Factors Affecting SAR Values in Devices

- 1. **Distance to the Base Station:** Phones reduce power when close to a tower.
- 2. **Obstacles:** Being indoors forces the phone to transmit at higher power.
- 3. **Frequency Band:** Different frequencies penetrate tissue differently.
- 4. **How the Phone is Held:** Covering the antenna can force increased power.
- 5. **Network Technology:** Modern networks use power control more efficiently.

Example: Comparing Two Handsets

- **Scenario:** Choose between two phones.
- - **Phone A:** Max SAR = 1.2 W/kg.
- - **Phone B:** Max SAR = 0.6 W/kg.
- **Reality:** If Phone B has a poor antenna, it may frequently transmit at its maximum 0.6 W/kg.
- If Phone A has an excellent antenna, it might typically operate at only 0.1 W/kg in the same location.

Mitigation and Safety Guidelines

- - **Use Hands-Free Options:** Speakerphone or Bluetooth headsets.
- - **Text Instead of Calling:** Reduces time the phone is near the body.
- - **Wait for a Good Signal:** Avoid making calls when the signal is weak.
- - **Limit Call Duration:** Keep voice calls short.
- - **Keep Distance:** Do not sleep with the phone directly under your pillow.

Lecture Summary

- SAR measures the maximum RF energy absorbed by the body in W/kg.
- Current safety standards (ICNIRP, FCC) prevent thermal effects.
- SAR is measured rigorously using phantoms and tissue liquids.
- Actual RF exposure depends heavily on network conditions.
- Simple mitigation strategies, primarily involving distance, can drastically reduce exposure.

Next Lecture Preview

- Next unit: **4G and 5G Networks**.
- We will explore:
- 1. Introduction to 4G Technology
- 2. Features of 4G
- 3. Types of 4G Technologies

Lecture 32: 4.1 Introduction to 4G technology

4G and 5G Networks

DI05011011: Mobile Communication

Agenda for Today

- 1. Evolution: 1G to 4G
- 2. What is 4G?
- 3. IMT-Advanced Requirements
- 4. Key Features of 4G
- 5. All-IP Network Architecture
- 6. Types of 4G Technologies
- 7. Summary and Preview

Evolution: From 1G to 4G

- \- **1G:** Analog voice.
- \- **2G:** Digital voice, SMS (GSM, CDMA).
- \- **3G:** Mobile broadband, video calling, internet access (UMTS, CDMA2000).
- \- **4G:** Ultra-broadband internet access, IP telephony, gaming, high-definition mobile TV.
- 4G represented a fundamental shift from circuit-switched to packet-switched networks for everything, including voice.

What is 4G?

- 4G is the fourth generation of broadband cellular network technology, succeeding 3G.
- It provides mobile ultra-broadband Internet access.
- Designed to offer higher data rates, improved quality of service (QoS), and lower latency.
- Provides a comprehensive and secure all-IP based mobile broadband solution to laptop computer wireless modems, smartphones, and other mobile devices.

IMT-Advanced Requirements

- The ITU (International Telecommunication Union) defined 'True 4G' under the IMT-Advanced specification:
- - Data rates of **100 Mbps** for high mobility (e.g., in cars/trains).
- - Data rates of **1 Gbps** for low mobility (e.g., stationary or walking).
- - Scalable channel bandwidths of 5 to 20 MHz, optionally up to 40 MHz.
- - Seamless connectivity and global roaming across multiple networks.

Key Features of 4G Technology

- 1. **High Speed:** Supports peak data rates of 100 Mbps to 1 Gbps.
- 2. **High Capacity:** Can support more active users per cell.
- 3. **Low Latency:** Reduced delay in packet delivery (crucial for gaming and voice).
- 4. **All-IP Network:** Complete transition to packet switching (IPv6 support).
- 5. **High Spectral Efficiency:** Delivers more bits per hertz than 3G.

The All-IP Network

- Previous generations used Circuit Switching for voice and Packet Switching for data.
- **4G Paradigm:**
- - Entirely Packet Switched.
- - Voice is treated as just another data application (Voice over LTE or VoLTE).
- - Uses IP (Internet Protocol) for all services: voice, data, and multimedia.
- - Simplifies network architecture and reduces costs.

Improved Quality of Service (QoS)

- Because 4G is All-IP, managing different types of traffic is critical.
- - **QoS Mechanisms:** Ensure time-sensitive packets (like voice or live video) get priority over less sensitive ones (like file downloads).
- - End-to-end QoS support is a mandatory feature in 4G to guarantee user experience.
- - Prevents jitter and packet loss during critical communications.

Technologies Enabling 4G

- Achieving IMT-Advanced speeds requires advanced physical layer technologies:
- 1. **OFDM (Orthogonal Frequency Division Multiplexing):** Deals efficiently with multipath interference.
- 2. **MIMO (Multiple Input Multiple Output):** Uses multiple antennas to increase data rates and reliability.
- We will cover these in detail in upcoming lectures.

Types of 4G Technologies

- Two main candidate technologies competed for the 4G standard:
- 1. **WiMAX (IEEE 802.16m):** Driven by the computer/IT industry.
- 2. **LTE-Advanced (Long-Term Evolution):** Driven by the telecommunications industry (3GPP).

WiMAX (Worldwide Interoperability for Microwave Access)

- - Based on the IEEE 802.16 standard.
- - Designed primarily as a broadband wireless access technology (like long-range Wi-Fi).
- - Early versions offered fixed wireless, later adapted for mobile (Mobile WiMAX).
- - Deployed early in some markets but ultimately lost out to LTE due to lack of global ecosystem support.

LTE (Long-Term Evolution)

- - Developed by the 3GPP (3rd Generation Partnership Project).
- - Represents a smooth evolution path for existing GSM/UMTS networks.
- - Adopted globally as the de facto 4G standard.
- - LTE-Advanced (Release 10 onwards) formally met the IMT-Advanced 4G requirements.

Real-World Application: Streaming and Video Calls

- **Pre-4G Era:** Video streaming over cellular was heavily buffered, low-resolution, and unreliable.
- **4G Era:**
- - Enabled HD Netflix/YouTube streaming on mobile.
- - Made FaceTime and WhatsApp video calls seamless.
- - Allowed real-time multiplayer mobile gaming (e.g., PUBG Mobile) due to low latency.
- 4G fundamentally changed how we consume media on the go.

Lecture Summary

- 4G networks provide ultra-broadband speeds and low latency.
- The ITU's IMT-Advanced defines true 4G as 100 Mbps (mobile) and 1 Gbps (stationary).
- 4G is an All-IP network, transitioning away from circuit-switched voice.
- Key enabling technologies are OFDM and MIMO.
- LTE-Advanced emerged as the global standard, defeating WiMAX.

Next Lecture Preview

- In the next lecture, we will dive deeper into **LTE and WiMAX**.
- We will explore:
- 1. LTE Architecture (EPC and E-UTRAN)
- 2. Detailed comparison of LTE and WiMAX
- 3. How LTE handles handovers and mobility.

Lecture 33: LTE and WiMAX - 4.4 LTE Architecture

4G and 5G Networks

DI05011011: Mobile Communication

Agenda for Today

- 1. WiMAX Overview (Brief)
- 2. Introduction to LTE Architecture
- 3. The E-UTRAN (Radio Access Network)
- 4. eNodeB Functions
- 5. The EPC (Evolved Packet Core)
- 6. Key EPC Components (MME, SGW, PGW, HSS)
- 7. Summary and Q&A

WiMAX: A Brief Look Back

- Worldwide Interoperability for Microwave Access (IEEE 802.16)
- - Aimed to deliver wireless broadband access as an alternative to cable and DSL.
- - Architecture was simpler, resembling a large-scale Wi-Fi network.
- - Struggled with backward compatibility to 2G/3G voice networks.
- - Lacked the immense ecosystem support that 3GPP (LTE) enjoyed.

Introduction to LTE Architecture

- LTE architecture is designed to be flat, IP-based, and highly efficient.
- It is broadly divided into two main parts:
- 1. **E-UTRAN (Evolved Universal Terrestrial Radio Access Network):** The radio access network (the cell towers and air interface).
- 2. **EPC (Evolved Packet Core):** The core network that handles routing, authentication, and connection to the internet.

The E-UTRAN

- The E-UTRAN handles the radio communications between the mobile device and the EPC.
- **Simplification from 3G:**
- - 3G had NodeBs (towers) and RNCs (controllers).
- - LTE eliminates the RNC. All radio control functions are integrated into a single node called the **eNodeB (evolved Node B)**.
- - This 'flat' architecture significantly reduces latency.

Functions of the eNodeB

- The eNodeB is the only node in the E-UTRAN.
- **Key Functions:**
- - Radio Resource Management (RRM).
- - Routing of user plane data towards the Serving Gateway (SGW).
- - Scheduling and transmission of paging messages.
- - Measurement and reporting for mobility (handovers).

The EPC (Evolved Packet Core)

- The EPC is a purely IP-based core network.
- It consists of several specialized nodes:
- 1. **MME (Mobility Management Entity):** The control plane brain.
- 2. **SGW (Serving Gateway):** The local mobility anchor for data.
- 3. **PGW (PDN Gateway):** The exit point to the external internet.
- 4. **HSS (Home Subscriber Server):** The master database of users.

EPC Deep Dive: MME

- **Mobility Management Entity (MME):**
- - The main control node for the LTE access network.
- - Operates strictly in the control plane (no user data passes through it).
- - Handles user authentication (talking to the HSS).
- - Manages idle state mobility (tracking where the phone is).
- - Selects the appropriate SGW for the user.

EPC Deep Dive: SGW and PGW

- **Serving Gateway (SGW):**
- - Routes and forwards user data packets.
- - Acts as the mobility anchor during inter-eNodeB handovers.
-
- **Packet Data Network Gateway (PGW):**
- - Provides connectivity from the user equipment to external packet data networks (the Internet).
- - Performs policy enforcement, packet filtering, and charging support.
- - Assigns IP addresses to the mobile devices.

EPC Deep Dive: HSS and PCRF

- **Home Subscriber Server (HSS):**
- - Central database containing user-related and subscription-related information.
- - Provides authentication vectors to the MME.
-
- **Policy and Charging Rules Function (PCRF):**
- - Determines policy rules in real-time.
- - Tells the PGW how to handle traffic (e.g., throttling speed if data cap is reached, or prioritizing VoLTE).

Trace a Packet: Loading a Webpage

- Let's trace the path of data when you open a website on LTE:
- 1. **Phone** sends a request via radio waves.
- 2. **eNodeB** receives it and forwards the packet.
- 3. Packet goes to the **SGW**.
- 4. **SGW** forwards it to the **PGW**.
- 5. **PGW** routes it to the **Internet**.
- 6. Data returns via PGW -¿ SGW -¿ eNodeB -¿ Phone.
- *(Notice the MME is not involved in this data path!)*

Lecture Summary

- LTE architecture is flat and IP-based.
- E-UTRAN consists only of eNodeBs, removing the need for a separate controller node.
- The EPC handles the core network functions.
- Key EPC nodes: MME (Control), SGW (Data routing), PGW (Internet gateway), HSS (User database).
- Separation of control and user planes enhances performance and scalability.

Next Lecture Preview

- Next time, we will look at the specific physical layer technologies that make LTE's speed possible.
- We will focus on **4.5 OFDM Technology**:
- - What is Orthogonal Frequency Division Multiplexing?
- - How does it solve multipath fading?
- - What are its advantages in 4G systems?

Lecture 34: 4.5 OFDM Technology (Basic concept and Advantages)

4G and 5G Networks

DI05011011: Mobile Communication

Agenda for Today

- 1. The Problem: Multipath Fading & ISI
- 2. Evolution: From FDM to OFDM
- 3. Basic Concept of OFDM
- 4. What does 'Orthogonal' mean?
- 5. How OFDM Works
- 6. The Role of the Cyclic Prefix
- 7. Advantages of OFDM
- 8. Summary and Q&A

The Problem: Multipath Fading and ISI

- In a wireless channel, signals bounce off buildings, trees, and cars.
- **Multipath:** The receiver gets multiple delayed copies of the same signal.
- **Inter-Symbol Interference (ISI):** At high data rates, symbols are very short. A delayed copy of Symbol 1 can overlap with Symbol 2, causing interference and errors.
- Traditional single-carrier systems require complex equalizers to fix this.

From FDM to OFDM

- **FDM (Frequency Division Multiplexing):**
- - Divides the total bandwidth into non-overlapping sub-bands.
- - Requires large 'guard bands' between channels to prevent interference.
- - Inefficient use of the spectrum.
-
- **OFDM (Orthogonal FDM):**
- - Allows subcarriers to overlap tightly without interfering with each other.
- - Saves massive amounts of spectral space (no large guard bands needed).

Basic Concept of OFDM

- Instead of transmitting a high-speed data stream over a single wideband carrier, OFDM divides the stream.
- - The high-rate data stream is split into multiple parallel low-rate data streams.
- - Each low-rate stream is modulated onto a separate, narrow subcarrier.
- - Because the data rate on each subcarrier is low, the symbol duration is long.
- - **Result:** Long symbol durations are highly resistant to multipath delay (ISI).

Understanding 'Orthogonality'

- In mathematics, orthogonal means independent or uncorrelated.
- In OFDM, subcarriers are mathematically orthogonal to each other.
- - The peak of one subcarrier perfectly aligns with the nulls (zero-crossings) of all other subcarriers.
- - When the receiver samples a specific frequency, the interference from all other overlapping subcarriers is mathematically zero.

The Role of the Cyclic Prefix (CP)

- While OFDM is robust against ISI, it isn't perfect.
- To completely eliminate ISI, OFDM adds a **Cyclic Prefix (CP)**.
- - The end of an OFDM symbol is copied and appended to the front of the symbol.
- - This acts as a 'guard time' between symbols.
- - As long as the multipath delay is shorter than the CP length, there is zero ISI.

Advantages of OFDM (Part 1)

- 1. **High Spectral Efficiency:** Overlapping subcarriers save significant bandwidth compared to traditional FDM.
- 2. **Robustness to Multipath Fading:** The combination of parallel low-rate streams and the Cyclic Prefix makes it highly immune to ISI.
- 3. **Simple Equalization:** Because each subcarrier is narrow, the channel response across it is flat. This eliminates the need for complex time-domain equalizers.

Advantages of OFDM (Part 2)

- 4. **Scalability:** OFDM can easily scale to different channel bandwidths (e.g., 1.4 MHz to 20 MHz in LTE) simply by changing the number of active subcarriers.
- 5. **Flexibility:** Different modulation schemes (QPSK, 16-QAM, 64-QAM) can be applied to different subcarriers based on channel conditions (Link Adaptation).
- 6. **Synergy with MIMO:** OFDM is naturally suited to be combined with MIMO technology to further boost data rates.

Real-World Application: Wi-Fi and 4G

- OFDM isn't just for cellular networks.
- - **Wi-Fi:** 802.11a/g/n/ac/ax all use OFDM.
- - **Broadcasting:** Digital Audio Broadcasting (DAB) and Digital Video Broadcasting (DVB-T) use OFDM to handle multipath from tall buildings and mountains.
- It is the universal standard for high-speed wireless data today.

Lecture Summary

- OFDM mitigates multipath ISI by splitting a high-rate data stream into many low-rate parallel streams.
- Orthogonal subcarriers can overlap without interference, maximizing spectral efficiency.
- The Cyclic Prefix provides a guard time to completely absorb multipath delay.
- OFDM offers high scalability, simple equalization, and excellent synergy with MIMO.
- It is the foundational physical layer technology for LTE, Wi-Fi, and 5G.

Next Lecture Preview

- In the next lecture, we will explore the perfect companion to OFDM:
- **4.6 MIMO Technology (Multiple Input Multiple Output)**
- - How can using multiple antennas increase data rates?
- - Spatial Multiplexing vs. Transmit Diversity.
- - The advantages of MIMO in 4G networks.

Lecture 35: 4.6 MIMO Technology (Basic concept and Advantages)

4G and 5G Networks

DI05011011: Mobile Communication

Agenda for Today

- 1. What is MIMO?
- 2. Traditional Systems (SISO, SIMO, MISO)
- 3. Basic Concept of MIMO
- 4. Mode 1: Spatial Multiplexing
- 5. Mode 2: Transmit Diversity
- 6. Beamforming
- 7. Advantages of MIMO
- 8. Summary and Q&A

What is MIMO?

- **MIMO (Multiple Input Multiple Output)** refers to the use of multiple antennas at both the transmitter (eNodeB) and the receiver (Mobile Phone).
- - 'Input' refers to the signals entering the wireless channel (transmitter antennas).
- - 'Output' refers to the signals leaving the channel (receiver antennas).
- - It leverages multipath propagation—which used to be a problem—and turns it into a benefit.

Antenna Configurations

- Before MIMO, we had other setups:
- 1. **SISO (Single Input Single Output):** 1 Tx, 1 Rx. The traditional baseline. Vulnerable to fading.
- 2. **SIMO (Single Input Multiple Output):** 1 Tx, 2+ Rx. Uses 'Receive Diversity' to improve signal strength at the receiver.
- 3. **MISO (Multiple Input Single Output):** 2+ Tx, 1 Rx. Uses 'Transmit Diversity' to ensure the signal reaches a simple receiver.
- 4. **MIMO:** 2+ Tx, 2+ Rx. The ultimate configuration for modern networks.

How MIMO Works: The Magic of Multipath

- In a rich scattering environment (like a city with buildings), signals take multiple different paths from Tx to Rx.
- - Because the transmit antennas are physically separated, each path is slightly different (independent fading).
- - The receiver, with its multiple antennas and powerful signal processing, can separate these mixed signals mathematically.
- - This requires complex matrix mathematics to decode.

MIMO Mode 1: Spatial Multiplexing

- **Goal: Maximum Speed / Data Rate**
- - The transmitter splits a high-rate data stream into multiple independent data streams.
- - Each independent stream is sent out of a different antenna simultaneously, on the same frequency.
- - The receiver separates them.
- - **Result:** If you use a 2x2 MIMO system, you can potentially double the data rate without using extra bandwidth.

MIMO Mode 2: Transmit Diversity

- **Goal: Maximum Reliability / Coverage**
- - Used when the signal is weak (e.g., cell edge).
- - The transmitter sends the *same* data stream (or specially coded versions of it) out of multiple antennas.
- - The receiver combines these multiple copies to create one strong, clear signal.
- - **Result:** Does not increase peak data rate, but significantly reduces errors and dropped calls.

Beamforming (Related Concept)

- While not strictly basic MIMO, multiple antennas enable **Beamforming**.
- - Instead of broadcasting the signal in all directions (like a lightbulb), the antennas coordinate their phases to focus the RF energy into a narrow beam (like a laser).
- - Points the beam directly at the user.
- - Improves signal-to-noise ratio and reduces interference to other users.

Advantages of MIMO (Part 1)

- 1. **Increased Spectral Efficiency:** Spatial multiplexing multiplies data rates without requiring additional frequency spectrum.
- 2. **Improved Link Reliability:** Diversity techniques combat fading and improve coverage, especially at the cell edges.
- 3. **Higher Capacity:** The overall cell capacity is increased, allowing more users to be served simultaneously at high speeds.

Advantages of MIMO (Part 2)

- 4. **Reduced Interference:** Techniques like beamforming can steer nulls (areas of zero signal) toward interfering users.
- 5. **Synergy with OFDM:** OFDM flattens the frequency channel, making the complex matrix math required to decode MIMO signals much easier to calculate in real-time.

Real-World Application: Wi-Fi Routers

- Look at modern Wi-Fi routers at home:
- - Old routers (802.11g) had 1 antenna (SISO).
- - Modern routers (802.11n, ac, ax) have 4, 6, or 8 antennas sticking out.
- - This is MIMO in action! The router uses spatial multiplexing to stream 4K video to your TV while simultaneously handling a Zoom call on your laptop.

Lecture Summary

- MIMO utilizes multiple antennas at the transmitter and receiver.
- It turns multipath propagation into an advantage.
- **Spatial Multiplexing** splits data into parallel streams to multiply speed.
- **Transmit Diversity** sends copies of the same data to improve reliability.
- MIMO provides massive gains in spectral efficiency, capacity, and coverage, making it essential for 4G.

Next Lecture Preview

- In the next lecture, we will wrap up our discussion on 4G and introduce 5G.
- **Topics:**
- 1. Advantages and limitations of overall 4G technology.
- 2. Introduction to 5G technology.
- 3. The 5G Architecture.

Lecture 36: 4.7 Advantages and limitations of 4G technology

4G and 5G Networks

DI05011011: Mobile Communication

Lecture 37: 4.10 Advantages of 5G technology

4G and 5G Networks

DI05011011: Mobile Communication

Lecture 38: b. Architecture

4G and 5G Networks

DI05011011: Mobile Communication

Lecture 39: 4.12 Comparison between 4G and 5G network architec...

4G and 5G Networks

DI05011011: Mobile Communication

Lecture 40: 5.1 Bluetooth Technology: Architecture, feature ad...

Wireless Technologies

DI05011011: Mobile Communication

Lecture 41: Wi-Fi (IEEE 802.11): Basic concept and overview of modern standards

Wireless Technologies

DI05011011: Mobile Communication

Agenda for Today

- 1. Introduction to Wi-Fi
- 2. What is IEEE 802.11?
- 3. Wi-Fi Architecture (BSS and ESS)
- 4. Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
- 5. Evolution of Wi-Fi Standards
- 6. Modern Standards (Wi-Fi 4 to Wi-Fi 7)
- 7. Wi-Fi Security Basics
- 8. Summary and Next Steps

Introduction to Wi-Fi

- **Wi-Fi** stands for Wireless Fidelity.
- It is a family of wireless networking technologies used for Local Area Networking of devices and Internet access.
- Wi-Fi allows smartphones, computers, and IoT devices to connect to the network without physical cables.
- Typically operates in the **2.4 GHz, 5 GHz, and recently 6 GHz** ISM (Industrial, Scientific, and Medical) radio bands.

What is IEEE 802.11?

- **IEEE 802.11** is part of the IEEE 802 set of LAN protocols.
- Specifies the set of media access control (MAC) and physical layer (PHY) protocols for implementing WLAN computer communication.
- Created and maintained by the IEEE LAN/MAN Standards Committee (IEEE 802).
- The Wi-Fi Alliance tests and certifies that equipment complies with the 802.11 standards.

Wi-Fi Architecture: Basic Service Set (BSS)

- The fundamental building block of an 802.11 architecture is the **Basic Service Set (BSS)**.
- **Infrastructure BSS:** Contains an Access Point (AP) and one or more wireless clients (stations or STAs). All traffic flows through the AP.
- **Independent BSS (IBSS):** Also known as an ad-hoc network. STAs communicate directly with each other without an AP.
- Each BSS has a unique ID called the **BSSID** (usually the MAC address of the AP).

Wi-Fi Architecture: Extended Service Set (ESS)

- An **Extended Service Set (ESS)** connects two or more BSSs together.
- Connected via a Distribution System (DS), typically a wired Ethernet network.
- All APs in an ESS share the same **SSID (Service Set Identifier)**, which is the network name users see.
- Allows for **Roaming**: Users can move from one BSS to another without losing network connectivity.

Media Access Control: CSMA/CA

- Wi-Fi uses **Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)**.
- Unlike wired Ethernet (which uses Collision Detection - CSMA/CD), wireless radios cannot send and receive simultaneously to detect collisions.
- **Mechanism:**
- 1. Station listens to the channel (Carrier Sense).
- 2. If idle, it waits a random backoff time.
- 3. If still idle, it transmits the data.
- 4. Waits for an ACK (Acknowledgment) from the receiver.

Evolution of Wi-Fi Standards

- The IEEE 802.11 standard has evolved continuously to provide higher speeds, better range, and more capacity.
- To make it easier for consumers, the Wi-Fi Alliance introduced generational naming (Wi-Fi 4, 5, 6, etc.).
- **Legacy Standards:**
- - **802.11b (1999):** 11 Mbps, 2.4 GHz
- - **802.11g (2003):** 54 Mbps, 2.4 GHz
- - **802.11a (1999):** 54 Mbps, 5 GHz

Modern Standards: Wi-Fi 4 (802.11n)

- **Introduced:** 2009
- **Bands:** 2.4 GHz and 5 GHz (Dual-band)
- **Max Data Rate:** Up to 600 Mbps
- **Key Innovation: MIMO (Multiple Input Multiple Output)**
- - Uses multiple antennas to send and receive multiple spatial streams of data simultaneously.
- - Significantly improved range and throughput over 802.11g.

Modern Standards: Wi-Fi 5 (802.11ac)

- **Introduced:** 2014
- **Bands:** 5 GHz only
- **Max Data Rate:** Up to 3.5 Gbps (Wave 2) or 6.9 Gbps theoretically
- **Key Innovations:**
- - Wider channel bandwidths (up to 160 MHz).
- - **Downlink MU-MIMO** (Multi-User MIMO): AP can talk to multiple clients simultaneously.
- - Higher order modulation (256-QAM).

Modern Standards: Wi-Fi 6 and 6E (802.11ax)

- **Introduced:** 2019 (Wi-Fi 6), 2020 (Wi-Fi 6E)
- **Bands:** 2.4 GHz, 5 GHz, and **6 GHz (Wi-Fi 6E only)**
- **Max Data Rate:** Up to 9.6 Gbps
- **Key Innovations:**
- - **OFDMA:** Divides channels into sub-carriers, allowing simultaneous transmission to multiple users.
- - **BSS Coloring:** Reduces interference in dense environments (like apartment buildings).
- - **Target Wake Time (TWT):** Improves battery life for IoT devices.

Modern Standards: Wi-Fi 7 (802.11be)

- **Introduced:** Expected finalization in 2024
- **Goal:** Extremely High Throughput (EHT)
- **Bands:** 2.4, 5, and 6 GHz
- **Max Data Rate:** Up to 46 Gbps
- **Key Innovations:**
- - **320 MHz channels:** Double the width of Wi-Fi 6.
- - **Multi-Link Operation (MLO):** Devices can connect and transmit on multiple bands (e.g., 5GHz and 6GHz) simultaneously to reduce latency.
- - **4K-QAM:** Packing more data into each signal.

Wi-Fi Security Protocols

- Since wireless signals travel through the air, security and encryption are critical.
- **WEP (Wired Equivalent Privacy):** The original security, now easily broken and obsolete.
- **WPA (Wi-Fi Protected Access):** A temporary patch over WEP.
- **WPA2:** The standard for over a decade, uses strong AES encryption.
- **WPA3:** The latest standard (mandatory for Wi-Fi 6 certified devices). It provides robust protection against dictionary attacks and better security on public open networks (via OWE).

Lecture Summary

- Wi-Fi operates in unlicensed ISM bands using the IEEE 802.11 standard.
- Networks are structured into BSS (single AP) and ESS (multiple APs).
- CSMA/CA is used to avoid collisions in the half-duplex wireless medium.
- Standards have evolved rapidly: Wi-Fi 4 (MIMO), Wi-Fi 5 (Gigabit/5GHz), Wi-Fi 6/6E (Efficiency/6GHz), to Wi-Fi 7 (MLO/46 Gbps).
- Security has evolved from WEP to the highly secure WPA3.

Next Lecture Preview

- In the next lecture, we will explore short-range identification technologies:
- **RFID (Radio Frequency Identification):** Used for inventory, toll tags, and logistics.
- **NFC (Near Field Communication):** Used for contactless payments (Apple Pay, Google Pay) and fast pairing.
- We will understand their working principles and how they differ from Wi-Fi and Bluetooth.

Lecture 42: RFID and NFC systems: Working principle and applications

Wireless Technologies

DI05011011: Mobile Communication

Agenda for Today

- 1. Introduction to RFID
- 2. Components of an RFID System
- 3. Active vs. Passive RFID Tags
- 4. Operating Frequencies of RFID
- 5. Working Principle of RFID
- 6. Applications of RFID
- 7. Introduction to NFC
- 8. NFC Operating Modes
- 9. Applications of NFC
- 10. Comparison: RFID vs NFC
- 11. Summary and Next Steps

Introduction to RFID

- **RFID (Radio Frequency Identification)** uses electromagnetic fields to automatically identify and track tags attached to objects.
- It acts like a wireless barcode but does not require direct line-of-sight.
- An RFID tag can hold unique identification data (like a serial number) and other information.
- Widely used to track inventory, animals, vehicles, and assets.

Components of an RFID System

- An RFID system consists of three main components:
- **1. RFID Tag (Transponder):** Attached to the object. Contains a microchip (to store data) and an antenna (to transmit/receive).
- **2. RFID Reader (Interrogator):** A device that transmits a radio signal to the tag and receives the data back.
- **3. Backend System/Database:** A computer system that processes the data received from the reader to take actionable decisions (e.g., deducting inventory).

Types of RFID Tags

- **Passive Tags:**
- - Have no internal power source (no battery).
- - Draw power from the electromagnetic energy transmitted by the RFID reader.
- - Short read range (up to a few meters).
- - Cheaper, smaller, and have a long operational life.
- **Active Tags:**
- - Have their own battery.
- - Can broadcast their signal continuously.
- - Long read range (up to 100 meters or more).
- - Larger, more expensive, and limited by battery life.

Working Principle of Passive RFID

- 1. The **Reader** continuously emits radio waves through its antenna.
- 2. When a **Passive Tag** enters the field, its antenna picks up the energy.
- 3. This energy induces a small current that powers up the microchip inside the tag.
- 4. The microchip retrieves its stored ID data.
- 5. The tag transmits the data back to the reader using a technique called **Backscatter Modulation**.
- 6. The reader decodes the signal and sends the ID to the database.

Applications of RFID

- **Supply Chain & Logistics:** Tracking pallets and cartons in warehouses.
- **Retail:** Anti-theft systems and automated checkout (e.g., Decathlon stores).
- **Toll Collection:** FASTag in India uses passive RFID.
- **Access Control:** Employee ID cards to open doors.
- **Animal Tracking:** Implantable chips for pets and livestock.

Introduction to NFC

- **NFC (Near Field Communication)** is a specialized subset of RFID technology.
- Operates specifically at the **13.56 MHz** frequency.
- Designed for extremely short-range communication (usually **under 4 centimeters** or 1.5 inches).
- Unlike standard RFID, NFC is designed for **secure, two-way communication** between complex devices like smartphones.

NFC Operating Modes

- NFC devices (like smartphones) can operate in three distinct modes:
- **1. Reader/Writer Mode:** The phone acts like an RFID reader to read a passive NFC tag (e.g., tapping a smart poster to get a URL).
- **2. Peer-to-Peer (P2P) Mode:** Two active NFC devices exchange data (e.g., Android Beam sharing a contact).
- **3. Card Emulation Mode:** The phone pretends to be a passive NFC smart card. Used for contactless payments (Apple Pay, Google Pay) or transit passes.

Working Principle and Security of NFC

- NFC uses **magnetic induction** to couple devices.
- **Security advantage of short range:** Because the range is ¡ 4cm, it is very difficult for a hacker to intercept or eavesdrop on the signal without being physically noticed.
- **Secure Element (SE):** When used for payments, NFC relies on a highly secure hardware chip (Secure Element) inside the phone to store credit card tokens securely.
- Transactions are encrypted and often require biometric authentication (Face ID/Fingerprint).

Applications of NFC

- **Contactless Payments:** Tap-to-pay via smartphones or contactless credit cards.
- **Transit Systems:** Tapping your phone for Metro or Bus tickets.
- **Device Pairing:** Tapping a phone to a Bluetooth speaker to instantly pair them without menus.
- **Smart Posters/Tags:** Tapping a museum exhibit for information or an NFC tag at home to automate smart home settings.
- **Digital Identity:** Mobile passports and digital driver's licenses.

Comparison: RFID vs. NFC

- — Feature — RFID — NFC —
- — :— — :— — :— —
- — **Range** — Up to 100 meters (Active) — Less than 4 cm —
- — **Communication** — Mostly one-way (Tag to Reader) — Two-way (Peer-to-Peer) —
- — **Multiple Items**— Can read hundreds of tags at once — Usually one-to-one interaction —
- — **Primary Use** — Asset tracking, Logistics, Tolls — Payments, Pairing, Access —
- — **Frequency** — LF, HF, UHF — 13.56 MHz (HF) only —

Lecture Summary

- RFID is a technology using RF fields to identify and track tags.
- Passive RFID tags draw power from the reader, while active tags have batteries.
- NFC is a subset of RFID operating at 13.56 MHz with a range of under 4 cm.
- NFC supports three modes: Reader/Writer, Peer-to-Peer, and Card Emulation.
- RFID dominates supply chains and tracking, while NFC dominates secure mobile payments.

Next Lecture Preview

- In our next lecture, we will look at a technology designed for the Internet of Things (IoT) and smart homes:
- **Zigbee:**
- - Basic concepts and IEEE 802.15.4 standard.
- - Mesh networking capabilities.
- - Why use Zigbee instead of Wi-Fi for smart home sensors?

Lecture 43: Zigbee: Basic concept, features and applications

Wireless Technologies

DI05011011: Mobile Communication

Agenda for Today

- 1. What is Zigbee?
- 2. The IEEE 802.15.4 Standard
- 3. Zigbee Network Topologies
- 4. Zigbee Device Types
- 5. Zigbee Protocol Stack
- 6. Key Features of Zigbee
- 7. Zigbee vs. Wi-Fi vs. Bluetooth
- 8. Real-world Applications
- 9. Summary and Next Steps

What is Zigbee?

- **Zigbee** is a wireless technology developed as an open global standard to address the unique needs of low-cost, low-power wireless IoT networks.
- It operates in the **2.4 GHz ISM band** globally (alongside Wi-Fi and Bluetooth), and also 915 MHz in the Americas and 868 MHz in Europe.
- Maintained by the **Connectivity Standards Alliance (CSA)** (formerly Zigbee Alliance).
- Designed for scenarios where devices only need to transmit small amounts of data infrequently.

The IEEE 802.15.4 Standard

- Zigbee is built on top of the **IEEE 802.15.4** standard.
- **IEEE 802.15.4** defines the **Physical (PHY) Layer** and the **Medium Access Control (MAC) Layer** for Low-Rate Wireless Personal Area Networks (LR-WPANs).
- **Zigbee** defines the higher layers: the **Network Layer**, **Security Layer**, and **Application Layer**.
- Think of 802.15.4 as the road and vehicles, while Zigbee is the traffic laws and delivery system.

Zigbee Device Types

- A Zigbee network has three types of devices based on their roles:
- **1. Zigbee Coordinator (ZC):**
- - The 'brain' of the network. Creates and manages the network.
- - Only one Coordinator per network. Stores network information and security keys.
- **2. Zigbee Router (ZR):**
- - Acts as an intermediate node, passing data from other devices.
- - Must be constantly powered (plugged in) as it keeps the network mesh alive.
- **3. Zigbee End Device (ZED):**
- - Battery-powered sensors or switches.
- - Spends most of its time asleep to save battery. Wakes up, sends data to a parent (Router or Coordinator), and sleeps again.

Zigbee Network Topologies

- Zigbee supports multiple network topologies:
- **1. Star Topology:** All devices connect directly to the central Coordinator. (Simple but limited range).
- **2. Tree Topology:** Coordinator is the root, Routers form branches, End Devices are leaves.
- **3. Mesh Topology (Most Common):**
- - Devices communicate with each other dynamically.
- - **Self-Healing:** If a Router fails, data finds a new path through another Router.
- - Highly reliable and can cover large areas by hopping messages across devices.

Key Features of Zigbee

- **Low Power Consumption:** End devices can run for years on a single coin-cell battery.
- **Low Data Rate:** Maximum 250 kbps (at 2.4 GHz). Sufficient for sensor data.
- **High Capacity:** Can support up to **65,000 devices** on a single network.
- **Secure:** Uses AES-128 encryption to secure data packets.
- **Self-Organizing & Self-Healing:** The mesh network automatically configures and repairs itself if a node goes down.

Zigbee vs. Wi-Fi vs. Bluetooth

- — Feature — Wi-Fi (802.11) — Bluetooth (LE) — Zigbee (802.15.4) —
- — :— — :— — :— — :— —
- — **Data Rate** — High (Gbps) — Medium (1-2 Mbps)— Low (250 kbps) —
- — **Power Usage**— High — Low — Extremely Low —
- — **Topology** — Star (BSS) — Star / Mesh — Star / Tree / Mesh —
- — **Max Devices**— ˜250 per AP — Few / Mesh limits — Up to 65,000 —
- — **Use Case** — Internet, Video — Audio, Wearables — Sensors, Automation —

Applications of Zigbee

- **Smart Home Automation:** Smart bulbs (Philips Hue), smart locks, thermostats, window sensors.
- **Industrial Control:** Monitoring factory equipment, temperature, and humidity sensors across large warehouses.
- **Smart Metering:** Automated meter reading for electricity and water.
- **Healthcare:** Patient monitoring systems requiring low power wearable sensors.
- **Smart Agriculture:** Soil moisture sensors spread across large fields utilizing the mesh network to reach the central hub.

Limitations of Zigbee

- **Not for High Data Rates:** Cannot be used to transmit audio, video, or large files.
- **Requires a Hub/Gateway:** Unlike Wi-Fi, smartphones cannot connect to Zigbee directly. A Zigbee-to-Wi-Fi hub (Coordinator) is always required to control them via phone.
- **Interference:** Operates in the crowded 2.4 GHz band, which can suffer interference from Wi-Fi networks and microwaves.
- **Interoperability Issues:** Historically, different manufacturers implemented custom Zigbee profiles, though recent standards (Zigbee 3.0, Matter) aim to fix this.

Lecture Summary

- Zigbee is a low-power, low-data rate wireless standard designed for IoT and sensor networks.
- It builds upon the IEEE 802.15.4 PHY and MAC layers.
- A Zigbee network consists of a Coordinator, Routers, and sleeping End Devices.
- Mesh networking allows for extended range, reliability, and self-healing.
- Ideal for applications like smart homes, industrial monitoring, and smart metering, where battery life is more important than bandwidth.

Next Lecture Preview

- In the next lecture, we will explore networks that form entirely on their own without any infrastructure:
- **Mobile Adhoc Networks (MANET):**
- - What happens when there is no cell tower or Wi-Fi router?
- - How devices dynamically form a network and route data.
- - Architecture and characteristics of MANETs.

Lecture 44: Mobile Adhoc Network (MANET): Concept, Architecture, and Advantages

Wireless Technologies

DI05011011: Mobile Communication

Agenda for Today

- 1. What is a MANET?
- 2. Infrastructure vs. Infrastructure-less Networks
- 3. Core Characteristics of MANET
- 4. MANET Architecture
- 5. How Routing Works in MANET
- 6. Advantages of MANETs
- 7. Real-world Deployment Scenarios
- 8. Summary and Next Steps

What is a MANET?

- A **Mobile Adhoc Network (MANET)** is a continuously self-configuring, infrastructure-less network of mobile devices connected wirelessly.
- **Adhoc** means 'for this purpose'. The network is formed on-the-fly for a specific need and can be dissolved when the need is over.
- Each device in a MANET acts as both a **host** (an endpoint generating data) and a **router** (forwarding data for others).
- There are no fixed base stations, no central servers, and no wired backbone.

Infrastructure vs. Infrastructure-less

- **Infrastructure Networks (Cellular, Wi-Fi BSS):**
- - Rely on fixed Access Points or Base Stations.
- - Devices communicate only through the AP.
- - If the AP fails, the network goes down (single point of failure).
-
- **Infrastructure-less Networks (MANET):**
- - No fixed APs.
- - Devices communicate peer-to-peer (P2P) directly or via intermediate nodes.
- - Highly resilient; if one node fails, traffic routes around it.

Characteristics of MANETs

- **1. Dynamic Topology:** Nodes move freely. The network structure changes unpredictably and rapidly.
- **2. Multi-hop Routing:** If node A wants to talk to node C, but they are out of range, node B in the middle can forward the packets.
- **3. Autonomous Operation:** Operates independently without any central administration.
- **4. Energy Constrained:** Nodes usually rely on battery power, and routing data for others drains batteries faster.
- **5. Variable Capacity:** Wireless links are subject to noise, fading, and interference, making bandwidth unpredictable.

MANET Architecture

- MANET architecture is primarily flat or hierarchical:
- **Flat Architecture:**
- - All nodes are equal and share the same responsibilities.
- - Suitable for small networks.
- - Can suffer from excessive routing overhead as the network grows.
- **Hierarchical (Cluster-based) Architecture:**
- - Nodes are grouped into clusters.
- - One node is elected as the **Cluster Head**.
- - Cluster Heads route traffic between clusters, reducing routing overhead for ordinary nodes.
- - Better scalability for large networks.

Routing in MANETs

- Routing is complex because the network changes constantly. Protocols are categorized into:
- **1. Proactive (Table-driven):**
- - Nodes continuously maintain routing tables to all other nodes.
- - Routes are always available immediately, but consumes high bandwidth maintaining updates.
- - E.g., DSDV (Destination-Sequenced Distance-Vector).
- **2. Reactive (On-demand):**
- - Routes are discovered only when a node actually needs to send data.
- - Saves bandwidth, but introduces a delay when initially sending data.
- - E.g., AODV (Ad hoc On-Demand Distance Vector), DSR.

Advantages of MANETs

- **1. Rapid Deployment:** Can be set up instantly anywhere, without laying cables or installing towers.
- **2. High Fault Tolerance:** Decentralized nature means there is no single point of failure. The network adapts to node failures.
- **3. Cost-Effective:** No infrastructure costs (no cell towers to build or maintain).
- **4. Flexibility:** Nodes can join or leave the network freely. The network expands and shrinks organically.
- **5. Unrestricted Mobility:** Supports communication even when all participants are moving at high speeds.

Scenarios for MANET Deployment

- **Disaster Recovery:** Earthquakes or floods destroy cellular infrastructure. Rescue workers form a MANET to coordinate.
- **Military Operations:** Soldiers, tanks, and drones in a battlefield form a secure, mobile network where towers are impossible or easily targeted.
- **Temporary Events:** Conferences, concerts, or sporting events where temporary high bandwidth is needed between peers.
- **Personal Area Networks (PAN):** Connecting a smartphone, laptop, and smartwatch dynamically.

Lecture Summary

- MANETs are infrastructure-less, self-configuring networks of mobile devices.
- Devices function as both hosts and routers, enabling multi-hop communication.
- Networks have dynamic topologies and can be organized flat or hierarchically.
- Routing can be proactive (table-driven) or reactive (on-demand).
- Advantages include rapid deployment, fault tolerance, and cost-effectiveness, making them ideal for disaster recovery and military applications.

Next Lecture Preview

- In our final lecture, we will complete our study of MANETs:
- **1. Limitations and Challenges:** Security, battery, and bandwidth issues.
- **2. Comparison:** MANET vs. Cellular Networks.
- **3. Specialized MANETs:** Introduction to Vehicular Adhoc Networks (VANETs).
- This will conclude Unit 5 and the Mobile Communication course!

Lecture 45: Mobile Adhoc Network (MANET): Limitations, VANETs, and Comparison with Cellular Systems

Wireless Technologies

DI05011011: Mobile Communication

Agenda for Today

- 1. Recap of MANET Basics
- 2. Limitations and Challenges of MANET
- 3. Security Issues in MANETs
- 4. Introduction to VANETs (Vehicular Adhoc Networks)
- 5. Comparison: MANET vs Cellular Networks (Architecture)
- 6. Comparison: MANET vs Cellular (Routing & Cost)
- 7. Summary of MANETs
- 8. Course Conclusion

Limitations and Challenges of MANETs

- Despite their flexibility, MANETs face significant challenges:
- **1. Limited Battery Power:** Nodes act as routers. Forwarding packets for other nodes drains battery quickly.
- **2. Bandwidth Constraints:** Wireless links have lower capacity than wired backbones. Frequent routing updates consume valuable bandwidth.
- **3. Dynamic Topology:** Rapid node movement causes routes to break frequently, leading to packet drops and high latency.
- **4. Hidden Terminal Problem:** Collisions occur easily without centralized coordination (AP).

Security Issues in MANETs

- MANETs are highly vulnerable to security attacks:
- **No Centralized Firewalls:** Without a central server, authenticating nodes and enforcing security policies is very difficult.
- **Eavesdropping:** Wireless medium is open to interception.
- **Black Hole Attack:** A malicious node advertises it has the shortest path to all destinations, intercepts the traffic, and drops the packets.
- **Node Compromise:** If an attacker physically captures a node (e.g., in military scenarios), they can disrupt the entire network from within.

A Specialized MANET: VANET

- **Vehicular Adhoc Network (VANET)** is a sub-class of MANET where the nodes are moving vehicles.
- **Characteristics:**
- - Extremely high mobility (cars moving at 120 km/h).
- - No battery constraints (cars have large alternators/batteries).
- - Predictable movement (cars follow roads and lanes).
- **Applications:**
- - Accident warnings (car ahead brakes hard, alerts cars behind instantly).
- - Traffic congestion updates.
- - Automated toll collection and intersection control.

Comparison: MANET vs. Cellular Networks

- **Architecture & Infrastructure:**
- — Feature — Cellular Networks — MANET —
- — :— — :— — :— —
- — **Infrastructure** — Centralized (Base Stations, MSC) — Decentralized (No infrastructure) —
- — **Topology** — Fixed backbone, Single-hop to BS — Highly dynamic, Multi-hop P2P —
- — **Node Roles** — End terminals only — Both end terminals and routers —
- — **Single Point of Failure** — Yes (if BS goes down) — No (self-healing, routes around failures) —

Comparison: MANET vs. Cellular Networks

- **Routing, Cost, and Deployment:**
- — Feature — Cellular Networks — MANET —
- — :— — :— — :— —
- — **Routing** — Determined by fixed switches/MSC — Computed by end nodes (AODV/DSR) —
- — **Deployment Time** — Months/Years (planning, licensing) — Instant (seconds/minutes) —
- — **Cost** — Extremely high (billions of dollars)— Minimal (only cost of devices) —
- — **Bandwidth** — High and guaranteed (licensed) — Variable and limited (unlicensed) —
- — **Security** — High (SIM auth, telecom backbone) — Low (difficult to trust peers) —

MANET Summary

- While MANETs offer unparalleled flexibility and instant deployment, they suffer from power, routing overhead, and security challenges.
- They are not a replacement for cellular networks, but a complementary technology for specific scenarios (military, disaster, V2V).
- Cellular networks trade massive infrastructure costs for reliability, security, and high bandwidth.

Course Conclusion

- Congratulations on completing Mobile Communication!
- **Unit 1 & 2:** You learned the foundations of Cellular concepts, GSM, and CDMA.
- **Unit 3:** You explored the internal hardware and OS of mobile devices.
- **Unit 4:** You understood the shift to high-speed IP data with 4G LTE and 5G.
- **Unit 5:** You expanded your view to Wi-Fi, RFID, Zigbee, and Adhoc networks.
- You now understand how the wireless world connects!