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.**