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.**