National Taiwan University
Department of Computer Science
and Information Engineering

GSM System Overview

Phone Lin

Ph.D.

Email: plin@csie.ntu.edu.tw

Outlines

- Introduction
- GSM Architecture
- Location Tracking and Call Setup
- Security
- GSM Data Services
- Unstructured Supplementary Service Data
- Summary

Introduction

- Global System for Mobile Communications (GSM) is a digital wireless network standard.
- It was developed by Group Special Mobile of Conference Europeenne des Postes et Telecommunications (CEPT) and European Telecommunications Standards Institute (ETSI).
- GSM Phases 1 and 2 define digital cellular telecommunications system.
- GSM Phase 2+ targets on Speech Codec and Data Service.

The Basic Requirements of GSM (1/2)

- **Services.**
  - The system will provide service portability; that is, MS can be used in all participating countries.
- **Quality of Services and Security.**
  - The quality for voice telephony of GSM will be at least as good as the previous analog systems.
  - The system will be capable of offering information encryption with lightly extra cost.
- **Radio Frequency Utilization.**
  - The system will permit a high level of spectrum efficiency.
  - The system will be capable of operating in the entire allocated frequency band, and coexist with the earlier system in the same frequency band.

The Basic Requirements of GSM (2/2)

Network.

- The identification and numbering plans will be based on relevant ITU recommendations.
- An international standardized signaling system will be used for switching and mobility management.
- The exiting fixed public networks should not be significantly modified.

Cost.

- The system parameters will be chosen with a view to limiting the cost of the complete system, in particular MS.

PART I

GSM Architecture

Mobile Station (MS)/Mobile Terminal (MT)

- The MS consists of two parts:
  - **the Subscriber Identity Module (SIM) and**
  - **the Mobile Equipment (ME).**
- In a broader definition, the MS also includes a third part called
  - **Terminal Equipment (TE), which can be a PDA or PC connected to ME.**

Subscriber Identity Module (SIM) (1/2)

- A SIM can be
  - **A smart card, usually the size of a credit card**
  - **A smaller-sized "plug-in SIM"**
  - **A smart card that can be perforated, which contains a plug-in SIM that can be broken out of it.**
- The SIM is protected by a Personal Identity Number (PIN) between 4 to 8 digits.
  - **To use MS, the user is asked to enter the PIN.**
  - **If the number is not correctly entered in 3 time, the SIM is locked.**
  - **To unlock SIM, the user is asked to enter the 8-digit PIN unblocking Key (PUK).**

Subscriber Identity Module (SIM) (2/2)

- Subscriber-Related Information includes
  - **PIN, and PUK codes,**
  - **A list of abbreviated and Customized Short Dialing Numbers,**
  - **Short Message Received when the subscriber is not present, and**
  - **Names of Preferred Networks to provide service.**
- Parts of the SIM information can be modified by the subscriber either by keypad or a PC using an RS232 connection.
- The SIM card can be updated *over the air* through *SIM Toolkit*.

Mobile Equipment (ME)

- The ME contains
  - **The Noncustomer-Related Hardware and**
  - **Software Specific to the Radio Interface.**
- When the SIM is removed from an MS, the remaining ME cannot be used for reaching the service, except for emergency calls.
- Usually, the MS is the property of the subscriber.
- The SIM is the property of the service provider.

Base Station System (BSS): BTS

- **Base Transceiver Station (BTS)** contains
  - **Transmitter, Receiver, and**
  - **Signaling Equipment Specific to the radio interface in order to contact the MSs.**
  - **Transcoder/Rate Adapter Unit (TRAU) carries out GSM-specific speech encoding/decoding and rate adaptation in data transmission.**

Base Station System (BSS): BSC

Base Station Controller (BSC)

- is responsible for the switching functions in the BSS, and
- is in turn connected to an MSC in the NSS.
- The BSC supports radio channel allocation/release and handoff management.
- A BSC may connect to several BTSs and maintain cell configuration data of these BTSs.
- The BSC communicates with the BTSs using ISDN protocols via the *A-bis.*
- Capacity planning for BSC is very important.

Network and Switching Subsystem (NSS)

- **MSC** performs the basic switching function following a signaling protocol used in the telephone network.
- **HLR and VLR** maintain the current location of the MS.
- **Authentication Center (AuC)** is used in the security data management for the user.
- **Gateway MSC (GMSC)** routes an incoming call to an MSC by interrogating the HLR directory.
  - **A MSC can function as the GMSC by including appropriate software and HLR interrogation functions.**

Radio Interface—Um Interface

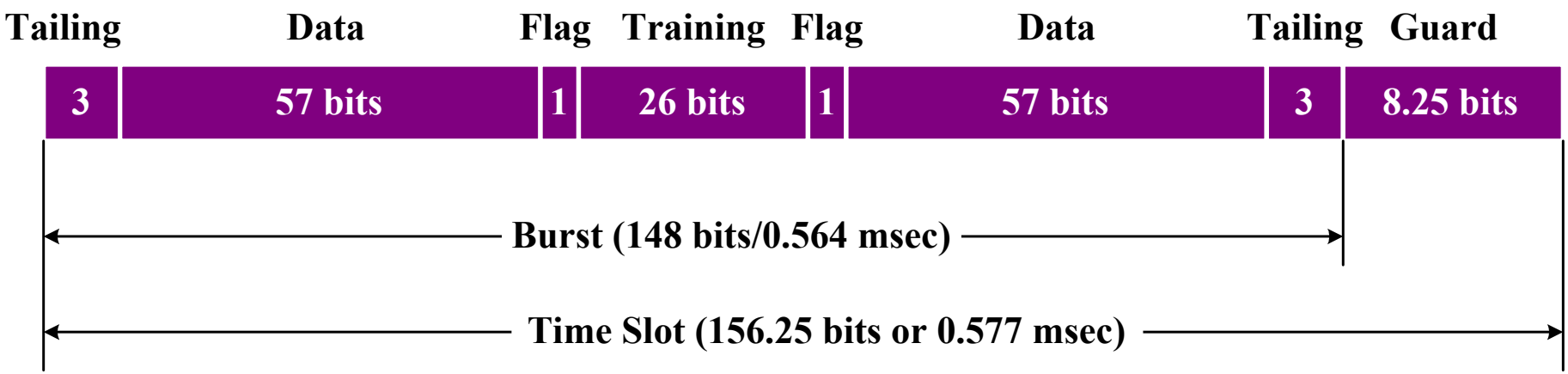
- The GSM radio link uses both FDMA and TDMA technologies.
- 935-960 MHz (downlink); 890-915 MHz (uplink)
- 124 pairs × 200 KHz
- Discontinuous transmission/reception is used to save the power consumption of the MS.

The Frame Structure

- The length of GSM frame in a frequency carrier is 4.615 msec.
- A frame consists 8 bursts (time slot) (each 0.577 msec).
- The delay between uplink and downlink is 3 time slots.
- **Timing Advance:** the exact shift between downlink and uplink seen by MS

GSM Burst Structure

- Begin with 3 head bits, and end with 3 bits.
- Two groups are separated by an equalizer training sequence of 26 bits.
- The flags indicates whether the information carried is for speech/data, signaling.



Traffic Channel (TCH)

- **TCHs** are intended to carry user information (speech or data).
  - **Full-rate TCH (TCH/F) provides transmission speed of 13 Kbps for speech or 9.6, 4.8 or 2.4 Kbps for data. Enhanced full-rate (EFR) speech coders have been implemented to improve the speech quality.**
  - **Half-rate TCH (TCH/H) allows transmission of 6.5 Kbps speech, or 4.8 or 2.4 Kbps of data.**

Common Control Channel (CCCH)

- Paging Channel (PCH) (down link) used by the network to page the destination MS in call termination.
- Access Grant Channel (AGCH) (down link) used by the network to indicate radio link allocation upon prime access of an MS.
- Random Access Channel (RACH) (up link) used by the MSs for initial access to the network.
- Several MSs may access the same RACH, potentially resulting in collisions. The slotted Aloha protocol is adopted in GSM to resolve access collision.

Dedicated Control Channel (DCCH)(1/2)

- (DCCH) is for dedicated use by a specific MS.
- Standalone Dedicated Control Channel (SDCCH; Downlink/Uplink) used only for signaling and for short message.
- Slow Associated Control Channel (SACCH; Downlink/Uplink)
  - **associated with either a TCH or and SDCCH.**
  - **This SACCH is used for non-urgent procedures,**
  - **mainly the transmission of power and time alignment control information over the downlink,**
  - **and measurement reports from the MS over the uplink.**

Dedicated Control Channel (DCCH)(2/2)

- Fast Associated Control Channel (FACCH; Downlink/Uplink)
  - Used for time-critical signaling, such as cell-establishing progress, authentication of subscriber, or handoff.
  - The FACCH makes use of the TCH during a call; thus, there is a loss of user data because the FACCH "steals" the bandwidth of the TCH.
- Cell Broadcast Channel (CBCH; downlink)
  - Carries only the short message service cell broadcast messages, which use the same time slot as the SDCCH.

Broadcast Channels (BCHs)

- BCHs are used by BTS to broadcast information to the MSs in its coverage area.
- Frequency Correction Channel (FCCH) and Synchronization Channel (SCH)
  - **carry information from the BBS to the MS.**
  - **The information allows the MS to acquire and stay synchronized with the BSS.**
- Broadcast Control Channel (BCCH)
  - **Provides system information such as access information for the selected cell and information related to the surrounding cells to support cell selection and location registration procedures in an MS.**

PART II

Location Tracking and Call Setup

MS Registration Process (2/3)

- Step 1.
  - **Part I.** The MS **periodically** listens to the BCCH broadcast from the BSS.
  - **Part II.** If the MS detects that it has entered a new location area, it sends a registration message to the new VLR by using the SDCCH channel.
- Step 2.
  - **Part I.** The new VLR communicates with the old VLR to find the HLR of the MS.
  - **Part II.** The new VLR then performs the authentication process.

MS Registration Process (3/3)

- Step 3.
  - **Part I.** After the MS is authenticated, the new VLR sends a registration message to the HLR.
  - **Part II.** If the registration request is accepted, the HLR provides the new VLR with all relevant subscriber information for call handling.
- Step 4.
  - The new VLR informs the MS of the successful registration.
- Step 5.
  - **Part I.** After Step 3, the HLR sends a deregistration (cancellation) message to the old VLR.
  - **Part II.** The old VLR cancels the record for the MS and sends an ACK to the HLR for cancellation.

The Mobile Call Termination (Delivery) Procedure (2/2)

- Step 1.
  - **Part I.** When the MSISDN is dialed, the call is forwarded to the GMSC, a switch that has the capability to interrogate the HLR for routing information.
  - **Part II.** The HLR requests the current VLR of the MS to provide the routable address, called a mobile station roaming number (MSRN).
- Step 2.
  - The VLR returns the MSRN to the GMSC through the HLR.
- Step 3.
  - The GMSC uses the MSRN to route the call to the MS through the visited MSC.

PART III

Security

Security: Authentication (1/2)

- **Ki** is used to achieve authentication.
  - Ki is stored in the AuC and SIM.
  - Ki is not known to the subscriber.
- **RAND.**
  - A 128-bit random number generated by the home system.
- **A3.**
  - A security function.
  - The inputs are **RAND** and **Ki**, and the output is **SRES**.

Security: Authentication (2/2)

- **Step 1.** The home system of the MS generates a RAND.
- **Step 2.** The home system sent the RAND to the MS.
- **Step 3.** Both the network (AuC) and the MS (SIM) use Ki and RAND to generate SRES by executing A3.
- **Step 4.** The MS sends the SRES to the home system.
- **Step 5.** The SRES generated by the MS is compared with the SRES generated by the home system at AuC.
- **Note that** if (SRES, RAND) generated by the AuC are sent from the HLR to the visited VLR in advance, the comparison can be done at the visited VLR.

Security: Encryption (1/2)

- **Kc** is generated by algorithm A8 for the Encryption.
- **A8.**
  - An algorithm stored in the home system of the MS (AuC) and the MS (SIM).
  - The inputs are Ki and RAND.
  - The output is Kc.
- **Frame Number.**
  - A TDMA frame number encoded in the data bits.
- **A5.**
  - An algorithm stored in the MS (handset hardware) and the visited system.
  - Is used for the data ciphering and deciphering.

Security: Encryption (2/2)

- **Step 1**. If the MS is accepted for access, an Kc is produced by an algorithm A8 with Ki and RAND as inputs.
- **Step 2.** After the home system has generated Kc, this Kc is sent to the visited system.
- **Step 3.** Kc and the TDMA frame number encode in the data bits are used by A5 to cipher and decipher the data steam between the MS and the visited system.

PART IV

DATA SERVICES

Data Services

- GSM phase 2 standard supports two data services.
  - **Short Message Services (SMS)**
  - **Bearer Services are similar to the ISDN services, and the maximum data rate is 9.6 Kbps.**
- GSM phase 2+ standard supports two data services.
  - **High-Speed Circuit-Switched Data (HSCSD) for high-speed file transfers and mobile video applications**
  - **General Packet Radio Service (GPRS) for bursty data applications such as e-mail and WWW.**
  - **The data rates are expected to be raised from 9.6 Kbps to 28.8 Kbps or higher.**

High-Speed Circuit-Switched Data (HSCSD)

- HSCSD is a circuit-switched protocol for large file transfer and multimedia applications.
- The physical layer of HSCSD is the same as that for the Phase 2 GSM data services.
- The data rate of HSCSD has been increased by using multiple TDMA time slots (up to 8).
- The radio interface is the same as that of the current GSM system except that multiple, independent time slots can be utilized to provide high-speed link.
- The **radio link protocol (RLP)** has been enhanced in HSCSD to support multi time-slot operation.
- In June 1999, Nokia announced Card Phone 2.0 for HSCSD with 43.2 Kbps.

General Packet Radio Service (GPRS) (1/2)

- GPRS is a packet-switched protocol for applications (e.g., Web).
- GPRS has its own transport network for the transmission of bursty data.
- Two new entities:
  - **Serving GPRS Support Node (SGSN) receives and transmits packets between the MS their counterparts in the Public-Switched Data Network (PSDN).**
  - **Gateway GPRS Support Node (GGSN) inter-works with PSDN using connectionless networks (e.g., IP or X.25).**
  - **The HLR is enhanced to accommodate GPRS.**

General Packet Radio Service (GPRS) (2/2)

- A new radio link protocol is introduced to the GPRS air interface
  - **to guarantee fast call setup procedure and low-bit error rate for data transfer between the MSs and the BSs.**
  - **A packet radio media access control (MAC) for packet switching.**
  - **GPRS supports up to 100 users with one to eight channels.**
- A new infrastructure is introduced to GPRS for the packet services.

PART V

Unstructured Supplementary Service Data

USSD

- During the evolution of GSM, supplementary services have bee introduced in various stages. These new services may not be supported in old MSs.
- To support the new services in old MSs, USSD was introduced in GSM 02.90, 03.90, and 04.90 Spec.
- USSD is used as a GSM transparent bearer for old MSs.

The Usage of USSD

- USSD is flexible in terms of message length and content.
- It uses all digits 0-9 plus "＊" and "＃" keys.
- A USSD string is a command code
  - **Typically 2 or 3 digits followed by several parameters.**
  - **The parameters (supplementary information) have variable lengths and are separated by "＊".**
  - **The whole string ends with "＃".**

＊159＊5288128＃

USSD Functionalities

- The USSD provides interaction between a GSM node (MSC, VLR, or HLR) and the MS.
- If the USSD service node is an MSC, the USSD messages are exchanged through path (1).
- If the service node is a VLR (or HLR), the messages are exchanged through path (1)<->(2) (or (1)<->(2)<->(3)).

An Example for USSD Services

- Suppose that a new USSD service that enables subscribers to obtain real-time stock quotes is implemented at the home work.
- USSD messages would be exchanged between the MS and the HLR.
- **Advantages.** Since the MS communicates directly with the HLR, the subscriber can monitor stock values even when roaming to another country.
- HLR is expensive to modified.
  - **The solution is to introduce an USSD gateway between HLR and Application servers.**
  - **GSM MAP (used between HLR and USSD Gateway), TCP/IP (used between USSD Gateway and Application Servers).**

Summary

- GSM Architecture
  - **MS, BSS, NSS**
  - **Radio Interface**
- Location Tracking
  - **Registration**
  - **Mobile Call Termination**
- Security
  - **Authentication**
  - **Encryption**
- Data Services
  - **HSCSD**
  - **GPRS**
- USSD Services