Global System for Mobile (GSM)

David Tipper
Associate Professor
Graduate Program of Telecommunications and Networking
University of Pittsburgh

Telcom 2700 Slides 8
Based largely on material from Jochen Schiller, Mobile Communications
2nd edition

Second Generation Cellular Systems

Motivation for 2G Digital Cellular:
- Increase System Capacity
- Add additional services/features (SMS, caller ID, etc.)
- Reduce Cost
- Improve Security
- Interoperability among components/systems (GSM only)

2G Systems
- Pacific Digital Cellular ← orphan technology
- North American TDMA (NA-TDMA) ← orphan technology
- Global System for Mobile (GSM)
- IS-95 (cellular CDMA)

GSM: History

- 1982 CEPT establishes Groupe Speciale Mobile
- Motivation develop Pan-European mobile network
- Support European roaming and interoperability in landline
- Increase system capacity
- Provide advanced features
- Emphasis on STANDARDIZATION, supplier independence
- Low cost infrastructure and terminals
- 1989 European Telecommunications Standardization Institute (ETSI) takes over standardization
- Changes name: Global System for Mobile communication
- 1990 First Official Commercial launch in Europe
- 1995 GSM Specifications ported to 1900 MHz band
- GSM is the most popular 2G technology
GSM Market

World cellular subscribers by technology June 1992

GSM Overview

- FDD/ FDMA/TDMA – channel structure - 200 KHz channels – each carriers 8 voice channels
- Higher Quality than Analog Systems
  - Digital Voice 13.3Kbps
  - Slow frequency hopping, adaptive equalizer, error control coding, DTX
- Low power handsets – support sleep mode
- Security with encryption
- Wide roaming capability
- Subscriber Identity Modules (SIM cards)
- Digital data service
  - fax, circuit switched data
- SMS short messaging service
- Additional features: call waiting, voice mail, group calling, caller id etc.

Architecture of the GSM system

GSM is a PLMN (Public Land Mobile Network)

- Several providers can setup mobile networks following the GSM standard within each country
- Major components
  - MS (mobile station)
  - BTS (base transceiver station) or BS or cell site
  - BSC (base station controller)
  - MSC (mobile switching center)
  - LR (location register): VLR, HLR
  - AUC (Authentication database), EIR (Equipment Identity Register)
- Subsystems
  - RSS (radio subsystem): covers all radio aspects
  - NSS (network and switching subsystem): call forwarding, handoff, switching, location tracking, etc.
  - OSS (operation support subsystem): management of the network
- Standardized interfaces
  - Allows provider to mix and match vendor equipment
Mobile station

- A mobile station (MS) comprises several functional groups
  - MT (Mobile Terminal):
    - offers common functions used by all services the MS offers
    - end-point of the radio interface (Um)
  - TA (Terminal Adapter):
    - terminal adaptation, hides radio specific characteristics
  - TE (Terminal Equipment):
    - peripheral device of the MS, offers services to a user
    - does not contain GSM specific functions
  - SIM (Subscriber Identity Module):
    - personalization of the mobile terminal, stores user parameters (subscriber number, authentication key, PIN, etc.)

Radio Station Subsystem (RSS)

- Components
  - MS (Mobile Station)
  - BSS (Base Station Subsystem): consisting of
    - BTS (Base Transceiver Station): antenna + digital radio equipment
    - BSC (Base Station Controller): controlling several transceivers, maps radio channels (Um) onto terrestrial channels A

- Interfaces
  - Um: radio interface
  - Abis: standardized, open interface with 16 kbit/s user channels
  - A: standardized, open interface with 64 kbit/s user channels as in wired telephone network

Base Transceiver Station and Base Station Controller

- Tasks of a RSS are distributed over BSC and BTS
- BTS comprises radio specific functions
- BSC is the switching center for radio channels

<table>
<thead>
<tr>
<th>Functions</th>
<th>BTS</th>
<th>BSC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management of radio channels</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Frequency hopping (FH)</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Management of terrestrial channels</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Mapping of terrestrial onto radio channels</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Channel coding and decoding</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Rate adaptation</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Encryption and decryption</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Paging</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Uplink signal measurement</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Traffic measurement</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Handover management</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
GSM - TDMA/FDMA

GSM: FDD Channels

Uplink and Downlink channels have a 3 slot offset – so that MS doesn’t have to transmit and receive simultaneously. MS can also take measurements during this offset time and delay between next frame.

GSM Air Interface $U_m$

- **Use Physical FDMA/TDMA/FDD physical**
  - In 900 MHz band: 890-915 MHz Uplink band, 935-960 MHz Downlink
  - Radio carrier is a 200kHz channel $\Rightarrow$ 125 pairs of radio channels
  - Called Absolute Radio Frequency Channel Number (ARFCN)
  - ARFCN numbers given by $f(n) = 890 + 2n$ kHz for Uplink band $n = 0, \ldots, 124$
  - Corresponding downlink is $f(n) = 45$ MHz
  - Channels and ARFCN slightly different in other frequency bands
  - A TDMA frame is defined on the radio carrier (8 users per carrier)
  - Channel rate is 270.833 kbps
  - (RELPC) digital speech 13.3kbps
  - Two types of logical channels map onto physical channels
  - Control Channels (call setup, power adjustment, etc.)
  - Traffic Channels (voice or data) = 22.8kbps = 1 slot in a TDMA frame

GSM: TDMA frame

- BS to MS Downlink
- MS to BS Uplink

Frame = 4.62 ms

45 MHz

Uplink and Downlink channels have a 3 slot offset – so that MS doesn’t have to transmit and receive simultaneously. MS can also take measurements during this offset time and delay between next frame.
GSM Normal Burst

Training sequence is utilized for setting adaptive equalizer parameters.

Guard Period = 30.5 microseconds

Needed to allow for clock misalignment and propagation time of mobiles at different distances from BTS.

577 us

T: tail bits, S: flag, Train: equalizer training sequence

GSM operation from speech Input to Output

Speech

Speech

Source coding

Speech decoding

Channel coding

Channel decoding

Interleaving

De-interleaving

De-ciphering

Ciphering

De-modulation

Modulation

GSM Speech Coding

Analog speech

Low-pass filter

A/D

RPE-LTP speech encoder

Channel encoder

104 kbps

13 kbps

8000 samples/s, 13 bits/sample
GSM Speech Coding (cont)

Regular pulse excited - long term prediction (RPE-LRP) speech encoder (RELPS speech coder)

160 samples/20 ms from A/D (= 2080 bits)

RPE-LTP speech encoder → 36 LPC bits/20 ms → 9 LTP bits/5 ms → 47 RPE bits/5 ms → 260 bits/20 ms to channel encoder

LPC: linear prediction coding filter
LTP: long term prediction → pitch + input
RPE: Residual Prediction Error

Error protection for speech signals in GSM

Parity check

Convolutional Code
Rate 1/2, constraint length 5

Type Ia

50 bits
3 bits
132 bits
4 bits

Type Ib

Type II

50 bits
132 bits
78 bits

456 bits per 20 ms speech frame

Interleaving Format

Interleaving

Interleave distance = 8

Normal burst

1

57 bits

Out of first 20 ms

8

24 bits

Interleave

Interleave distance = 8

Out of second 20 ms

Tail

1

57 bits

1

825 bits

Guard
Modulation

- Variation on Frequency Shift Keying (FSK)
- Avoids sudden phase shifts → MSK (Minimum Shift Keying)
- Bit stream separated into even and odd bits, the duration of each bit is doubled

NRZ Data → Gaussian Low Pass Filter → FM Transmitter → GMSK Output at RF

Depending on the bit values (even, odd) the higher or lower frequency, original or inverted is chosen

The frequency of one carrier is twice the frequency of the other

Example of MSK

<table>
<thead>
<tr>
<th>Data</th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>0</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Even</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Odd</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Low Frequency</td>
<td>h</td>
<td>n</td>
<td>h</td>
<td>h</td>
<td></td>
</tr>
<tr>
<td>High Frequency</td>
<td>n</td>
<td>h</td>
<td>n</td>
<td>n</td>
<td></td>
</tr>
</tbody>
</table>

MSK signal

No phase shifts!

GSM Frequency Hopping

- Optionally, TDMA is combined with frequency hopping to address problem of channel fading
  - TDMA bursts are transmitted in a precalculated sequence of different frequencies (algorithm programmed in mobile station)
  - If a TDMA burst happens to be in a deep fade, then next burst most probably will not be
  - Helps to make transmission quality more uniform among all subscribers
  - Improves frequency reuse
  - Hops at the frame level – 217 hops/sec
**Frequency-hopped signal in GSM**

- **Frame N**
- **Frame N-1**
- **Frame 3**
- **Frame 1**
- **Frame 3**

**Time**

**Frequency**

---

**GSM Air Interface Specifications Summary**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reverse Channel Frequency</td>
<td>896 – 915 MHz</td>
</tr>
<tr>
<td>Forward Channel Frequency</td>
<td>935 – 962 MHz</td>
</tr>
<tr>
<td>ARFCN Number</td>
<td>0 to 124</td>
</tr>
<tr>
<td>Tx/Rx Frequency Spacing</td>
<td>45 MHz</td>
</tr>
<tr>
<td>Tx/Rx Time Slot Spacing</td>
<td>3 Time slots</td>
</tr>
<tr>
<td>Modulation Data Rate</td>
<td>270.833333 kbps</td>
</tr>
<tr>
<td>Frame Period</td>
<td>4.615 ms</td>
</tr>
<tr>
<td>Users per Frame (Full Rate)</td>
<td>8</td>
</tr>
<tr>
<td>Time slot Period</td>
<td>576.9 µs</td>
</tr>
<tr>
<td>Bit Period</td>
<td>3.692 µs</td>
</tr>
<tr>
<td>Modulation</td>
<td>GMSK</td>
</tr>
<tr>
<td>ARFCN Channel Spacing</td>
<td>200 kHz</td>
</tr>
<tr>
<td>Interleaving (max. delay)</td>
<td>40 ms</td>
</tr>
<tr>
<td>Voice Codec Bit Rate</td>
<td>13.3 kbps</td>
</tr>
</tbody>
</table>

---

**GSM System Identifiers**

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Name</th>
<th>Size (bits)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IMSI</td>
<td>International mobile subscriber identity</td>
<td>15 digits</td>
<td>Chosen number conforming to international convention – assigned by operating company to subscriber</td>
</tr>
<tr>
<td>TMSI</td>
<td>Temporary mobile subscriber identity</td>
<td>64 bits</td>
<td>Generated by visitor location register to a subscriber</td>
</tr>
<tr>
<td>IMSI</td>
<td>International mobile equipment identity</td>
<td>15 digits</td>
<td>Assigned by manufacturer to a mobile station</td>
</tr>
<tr>
<td>Ki</td>
<td>Authentication Key</td>
<td>128 bits</td>
<td>Secret key assigned by the operating company to a subscriber</td>
</tr>
<tr>
<td>Kc</td>
<td>Cipher Key</td>
<td>40 bits</td>
<td>Composed by network and mobile station</td>
</tr>
<tr>
<td>-</td>
<td>Mobile Station Class mark</td>
<td>12 bits</td>
<td>Indicates properties of a mobile station</td>
</tr>
<tr>
<td>BSI</td>
<td>Base Station Identity code</td>
<td>4 bits</td>
<td>Assigned by operating company to each BS</td>
</tr>
<tr>
<td>-</td>
<td>Timing Sequence</td>
<td>20 bits</td>
<td>Assigned by operating company to each BS</td>
</tr>
<tr>
<td>LAI</td>
<td>Location Area Identity</td>
<td>40 bits</td>
<td>Assigned by operating company to each LA</td>
</tr>
</tbody>
</table>

---
GSM Channels

Physical Channel – 1 time slot on a uplink/downlink radio carrier.
- 125 radio carriers, 8 slots per carrier => 1000 physical channels

Traffic Channels
- Full rate (TCH/F) at 22.8 kb/s or half rate (TCH/H) at 11.4 kb/s
- Physical channel = full rate traffic channel (1 timeslot) or 2 half rate traffic channels (1 timeslot in alternating frames)
- Full rate channel may carry 13 kb/s speech or data at 12, 6, or 3.6 kb/s
- Half rate channel may carry 6.5 kb/s speech or data at 6 or 3.6 kb/s

Control Channels
- Three groups of logical control channels
  1. BCH (broadcast channel): point-to-multipoint downlink only
  2. CCCH (common control channel): for paging and access
  3. DCCH (dedicated control channel): bi-directional point-to-point signaling

Logical Channel Structure...

Framing Scheme in GSM (Traffic Channels)

Framing scheme is implemented for encryption and identifying time slots

- Hyperframe: 3 hours 28 min 53.76 s
- Superframe: 6.12 s
- Traffic Multiframe: 120 ms
- Frame: 4.615 ms
- Slot: 577 μs
GSM Logical Channels (cont)

- **BCH (broadcast channels):** point-to-multipoint downlink only
  - BCCH (broadcast control channel): send cell identities, organization info about common control channels, cell service available, etc
  - FCCH (frequency correction channel): send a frequency correction data burst to effect a constant frequency shift of RF carrier
  - SCH (synchronization channel): send TDMA frame number and base station identity code to synchronize MSs

- **CCCH (common control channel):** for paging and access
  - PCH (paging channel): to page MSs
  - AGCH (access grant channel): to assign MSs to stand-alone dedicated control channels for initial assignment
  - RACH (random access channel): for MS to send requests for dedicated connections

GSM Logical Channels (cont)

- **DCCH (dedicated control channel):** bidirectional point-to-point – main signaling channels
  - SDCCH (stand-alone dedicated control channel): for service request, subscriber authentication, equipment validation, assignment to a traffic channel
  - SACCH (slow associated control channel): for signaling associated with a traffic channel, eg, signal strength measurements
  - FACCH (fast associated control channel): for preemptive signaling on a traffic channel, eg, for handoff messages – sets S (stealing Flag in traffic slot)

- Control channels are organized in a complex frame structure
  - Certain ARFCNs are assigned as having a control channel – TS0 is used for control channel
  - One control channel per sector per cell.

Framing Scheme in GSM (Control Channels)

Framing scheme is implemented for encryption and identifying time slots:

- **Hyperframe:** 3 hours 28 min 53.76 s
- **Superframe:** 6.12 s
- **Control Multiframe:** 235.4 ms
- **Frame:** 4.615 ms
- **Slot:** 577 μs
Control Channel Multiframe (Forward link TS0)

F: FCCH burst (BCH)
S: SCH burst (BCH)
B: BCCH burst (BCH)
C: PCH/AGCH burst (CCCH)
I: Idle

Control Channel Multiframe (Reverse link for TS0)

R: Reverse RACH burst (CH)

GSM Reverse Access Channel Protocol

System architecture: network and switching subsystem

Components
- MSC (Mobile Services Switching Center)
- IWF (Interworking Functions)
- ISDN (Integrated Services Digital Network)
- PSTN (Public Switched Telephone Network)
- PSPDN (Packet Switched Public Data Net.)
- CSPDN (Circuit Switched Public Data Net.)

Databases
- HLR (Home Location Register)
- VLR (Visitor Location Register)
- EIR (Equipment Identity Register)
Network and switching subsystem

NSS is the main component of the public mobile network GSM
- switching, mobility management, interconnection to other networks, system control

- Components
  - Mobile Services Switching Center (MSC) controls all connections via a separated network to/from a mobile terminal within the domain of the MSC - several BSC can belong to a MSC

- Databases (important: scalability, high capacity, low delay)
  - Home Location Register (HLR) central master database containing static user data, (mobile number, billing address, service subscribed, etc.) and dynamic data of all subscribers last VLR location
  - Visitor Location Register (VLR) local dynamic database for a subset of HLR data, including data about all user currently in the domain of the MSC attached to VLR

Mobile Services Switching Center

The MSC (mobile switching center) plays a central role in GSM
- switching functions
- additional functions for mobility support
- management of network resources
- interworking functions via Gateway MSC (GMSC)
- integration of several databases

- Functions of a MSC
  - specific functions for paging and call forwarding
  - termination of SS7 (signaling system no. 7)
  - mobility specific signaling
  - location registration and forwarding of location information
  - provision of new services (fax, data calls)
  - support of short message service (SMS)
  - generation and forwarding of accounting and billing information

Operation subsystem

- OSS (Operation Subsystem) enables centralized operation, management, and maintenance

- Components
  - Authentication Center (AUC)
    - generates user specific authentication parameters on request of a VLR
    - authentication parameters used for authentication of mobile terminals and encryption of user data on the air interface within the GSM system
  - Equipment Identity Register (EIR)
    - registers GSM mobile stations and user rights
    - stolen or malfunctioning mobile stations can be locked and sometimes even localized
  - Operation and Maintenance Center (OMC)
    - different control capabilities for the radio subsystem and the network subsystem
Three Layers specified in the protocol

Network layer has three sublayers

1. Call Management
   - Establishment, maintenance, and termination of circuit-switched calls
2. Mobility Management
   - Registration, authentication, and location tracking
   - Establishment, maintenance, and termination of radio channel connections

Link Layer

- Uses variation of ISDN LAPD protocol – termed LAPDm

Physical layer (already discussed)

- Time slot on a 200 KHz carrier – absolute radio frequency channel number (ARFCN)

GSM Protocol Stack

- CM: call management
- MM: mobility management
- RRM: radio resources management
- LAPD: link access protocol-D channel (ISDN)
- MTP: message transfer part (SS7)
- SCCP: signal connection control part (SS7)

GSM Data Link LAPDm Messages

Table 7.2 Data Link Control Messages

<table>
<thead>
<tr>
<th>Message Name</th>
<th>Function</th>
<th>Type</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>SETUP/TEARDOWN</td>
<td>command</td>
<td>Unacknowledged</td>
<td>Initiate transfer of information messages</td>
</tr>
<tr>
<td>DISCONNECT</td>
<td>command</td>
<td>Unacknowledged</td>
<td>Terminate of information messages</td>
</tr>
<tr>
<td>UNNUMBERED RESPONSE</td>
<td>response</td>
<td>Unacknowledged</td>
<td>Confirm a command</td>
</tr>
<tr>
<td>REQUEST AUTHENTICATION</td>
<td>command</td>
<td>Supervisory</td>
<td>Request transmission of interworking messages</td>
</tr>
<tr>
<td>ACKNOWLEDGE</td>
<td>response</td>
<td>Supervisory</td>
<td>Request transmission of interworking messages</td>
</tr>
<tr>
<td>OBJECT SET RESPONSE</td>
<td>command</td>
<td>Supervisory</td>
<td>Request transmission of interworking messages</td>
</tr>
<tr>
<td>OBJECT RESPONSE</td>
<td>response</td>
<td>Supervisory</td>
<td>Request transmission of interworking messages</td>
</tr>
</tbody>
</table>
### GSM RRM Messages

<table>
<thead>
<tr>
<th>Message Name</th>
<th>Logical Channel</th>
<th>Transmitted by</th>
</tr>
</thead>
<tbody>
<tr>
<td>CALL CONTROL</td>
<td>PCH</td>
<td>Base</td>
</tr>
<tr>
<td>GOS CONTROL</td>
<td>SCCH</td>
<td>Base</td>
</tr>
<tr>
<td>GOS RESERVATION</td>
<td>RACH</td>
<td>Base</td>
</tr>
<tr>
<td>CALL RESERVATION</td>
<td>SACCH</td>
<td>Mobile</td>
</tr>
<tr>
<td>HANDOVER</td>
<td>PCCH</td>
<td>Base</td>
</tr>
<tr>
<td>HANDOVER CONFIRM</td>
<td>SACCH</td>
<td>Mobile</td>
</tr>
<tr>
<td>HANDOVER COMPLETE</td>
<td>SACCH</td>
<td>Base</td>
</tr>
<tr>
<td>HANDOVER RX</td>
<td>SACCH</td>
<td>Mobile</td>
</tr>
<tr>
<td>HANDOVER RX COMPLETE</td>
<td>SACCH</td>
<td>Base</td>
</tr>
<tr>
<td>HANDOVER RX</td>
<td>SACCH</td>
<td>Mobile</td>
</tr>
<tr>
<td>HANDOVER RX COMPLETE</td>
<td>SACCH</td>
<td>Base</td>
</tr>
<tr>
<td>COMMAND CONTROL</td>
<td>SACCH</td>
<td>Mobile</td>
</tr>
<tr>
<td>CHANNEL RESEAT*</td>
<td>SACCH</td>
<td>Mobile/Base</td>
</tr>
</tbody>
</table>

### GSM MM Messages

<table>
<thead>
<tr>
<th>Message Name</th>
<th>Transmitted by</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUTHENTICATION REQUEST</td>
<td>Mobile</td>
</tr>
<tr>
<td>AUTHENTICATION RESPONSE</td>
<td>Base</td>
</tr>
<tr>
<td>AUTHENTICATION REJECT</td>
<td>Base</td>
</tr>
<tr>
<td>IDENTITY REQUEST</td>
<td>Mobile</td>
</tr>
<tr>
<td>IDENTITY RESPONSE</td>
<td>Base</td>
</tr>
<tr>
<td>LOCATION UPDATION REQUEST</td>
<td>Location Updation Request</td>
</tr>
<tr>
<td>LOCATION UPDATION ACCEPT</td>
<td>Location Updation Accept</td>
</tr>
<tr>
<td>LOCATION UPDATION COMPLETE</td>
<td>Location Updation Complete</td>
</tr>
<tr>
<td>SIM DEATH INDICATION</td>
<td>SIM Status</td>
</tr>
<tr>
<td>CM SERVICE REQUEST*</td>
<td>CM Service Request*</td>
</tr>
<tr>
<td>CM RE-ESTABLISHMENT REQUEST**</td>
<td>CM Re-establishment Request**</td>
</tr>
</tbody>
</table>

### GSM CM Messages

<table>
<thead>
<tr>
<th>Message Name</th>
<th>Direction in Call</th>
</tr>
</thead>
<tbody>
<tr>
<td>SETUP DETECTION/R</td>
<td>Call Setup</td>
</tr>
<tr>
<td>CANCEL CONFIRM</td>
<td>Call Cancel</td>
</tr>
<tr>
<td>ADD ALERT Indication</td>
<td>Alert Indication</td>
</tr>
<tr>
<td>VS</td>
<td>Call Setup</td>
</tr>
<tr>
<td>VS CONFIRM</td>
<td>Call Cancel</td>
</tr>
<tr>
<td>VS COMPLETE</td>
<td>Alert Indication</td>
</tr>
<tr>
<td>VS CONFIRM</td>
<td>Alert Indication</td>
</tr>
<tr>
<td>VS COMPLETE</td>
<td>Alert Indication</td>
</tr>
</tbody>
</table>

* Information in calls are subject to development requirements. ** Information in calls is subject to development requirements. Base: Base Station, Mobile: Mobile Station.
Sample GSM Message

Assignment Command
message on FACCH used in handoff to inform of new channel info
Bit Position Information
1-4 Protocol Discriminator 0110 (RRM – message)
5-8 Transaction identifier
9-16 Message Type 00101110
17-40 Channel Description
41-48 Power Command
variable Optional Data

GSM Call Management

Call Operation Types
- Registration
  Upon powering up, the MS scans common control channels and locks onto channel with strongest signal
  Searches for FCCH on RF carrier, finds SCH to synch up
  After synchronization the MS decodes BCCH – decides whether to update location register or not.
  Once registered or locked on to BCCH
- Mobile Originating (MO) Call
  Mobile types in number presses Send
- Mobile Terminating (MT) Call
  Mobile registered and phone On – received incoming call

GSM Registration

Lock on strong freq. and find FCCH
Find SCH channel for sync. and training
Gets cell and system parameters
Request stand alone dedicated channel
SDCCH established
GSM Registration (cont)

- Make location update request
- Computes challenge response to verify identity
- Initiate encryption of data for transmission
- Complete location update process

SDCCH location update
SDCCH challenge
SDCCH challenge response

SDCCH ciphered mode
Ack ciphered mode

Location update confirm
Ack

Location Registration

Register at power up/call placement/(power down)/ when detect a new location area id

Walkthrough Roaming case
1. Mobile-> MSC signals HLR update VLR pointer
2. Auc verifies user- may issue challenge/response
3. HLR – gives VLR mobile service profile
4. HLR – deregisters mobile from last VLR location

Target ITU-T bound on location registration ≤ 4sec

Location Update Types
- Intra – VLR (LAs attached to same VLR)
  - Only change LA id in VLR (local signaling)
  - Target ITU-T location update time ≤ 2 sec
- Inter – VLR (LAs attached to different VLR)
  - must signal HLR to update VLR pointer
  - Target ITU-T Location update time ≤ 4 sec

Location Update Call Flow

![Diagram of location update call flow]
MTC/MOC general behavior

<table>
<thead>
<tr>
<th>MS</th>
<th>MTC</th>
<th>BTS</th>
<th>MS</th>
<th>MOC</th>
<th>BTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>paging request</td>
<td>channel request</td>
<td>immediate assignment</td>
<td>paging response</td>
<td>authentication request</td>
<td>ciphering command</td>
</tr>
<tr>
<td>immediate assignment</td>
<td>authentication response</td>
<td>ciphering complete</td>
<td>setup</td>
<td>call confirmed</td>
<td>alerting</td>
</tr>
<tr>
<td>assignment command</td>
<td>assignment complete</td>
<td>connect</td>
<td>connect acknowledge</td>
<td>data/speech exchange</td>
<td></td>
</tr>
</tbody>
</table>

GSM MOC → Calling from MS

1. **Setup Request**
   - Fetches subscriber info from VLR to process call, acks caller
2. **Call Proceeding**
   - Allocates trunk + radio channel
3. **Radio channel**
   - Call connected through PSTN
4. **Complete**
   - Alerts caller
5. **Alerting**
   - Called party picks up
6. **Connect**
   - Call can proceed
7. **Connect ack**

GSM MTC → Calling to MS

1. **PCH page request**
   - Incoming call from PSTN
2. **RACH channel request**
   - Allocates control channel
3. **AGCH assignment**
4. **SDCCH paging response**
5. **SDCCH challenge**
6. **SDCCH challenge response**
7. **SDCCH ciphering mode**
8. **Ciphering mode complete**
9. **Request authentication**
10. **Request ciphering on channel**
**GSM MTC → Calling to MS (cont)**

- Notify call
- Accept call
- SDCCH setup
- SDCCH setup ack
- SDCCH assignment
- Assignment complete
- Assign traffic channel
- Alert called party
- FACCH alerting/connect
- FACCH connect ack
- Tune to freq.
- Start connection

**GSM Features**

- **Discontinuous Transmission (DTX)**
  - Handset/BSC contain voice activity detectors (much of a conversation is silent)
  - If no speech detected NO information is transmitted – TDMA slot left empty
  - Saves battery power in mobile
  - Reduces co-channel and adjacent channel interference
  - Comfort Noise is periodically played back if long silence period
- **Power control**
  - Both mobile and BTS regulate power (increase and decrease)
  - Mobile power adjusted in 2 dB levels, BTS power adjusted in 4 dB levels
  - Conserves battery power in mobile
  - Reduces interference
- **Mobile Assisted Handoff (MAHO)**
  - Mobile takes measurements of signal strength of radio channels in adjacent cells - reports to BSC and MSC to pick cell for handoff
- **Sleep Mode**
  - Handset once registered with network will be assigned a sleep mode level
  - Checks paging channel for page/SMS periodically depending on level

**GSM Mobility Management**

- **Mobility Types**
  - Track location of users for incoming calls/SMS
    - Location registration/authentication/paging
    - Divide coverage area into non-overlapping groups of cells – assign each a unique id
    - Location Area ID periodically broadcast by each cell
      - As a mobile moves/turns phone on – it listens to location area id – if different from last one registered in – performs a location update/authentication procedure with VLR and possibly HLR
  - Call in progress mobility
    - Handoff call from one BTS to another BTS
    - MAHO by mobile reporting measurements of signal strength
Location Management

**Location Area (LA)**
- Divide coverage into non-overlapping groups of cells
- Assign each LA a unique id
- Location Area ID is periodically broadcast by each cell

Two level database hierarchy HLR/VLR
- HLR points to VLR where mobile located
- VLR entry points to LA where mobile last located

In large networks may have HLR split among regions with aggregate info cross region

---

**Location Area and Cell Identification Parameters**

- **MCC** – Mobile Country Code
  - Uniquely identify the country of the GSM subscriber
- **MNC** – Mobile Network Code
  - Identifies the GSM operator within the country. Each country can have several GSM operators each having a unique MNC.
- **LAC** – Location Area Code
  - Defines a location area, which consists of a group of cells. Each MNC can have several LACs.
- **CI** – Cell Identity
  - Uniquely identifies a cell in a location area
- **LAI** – Location Area Identity
  - Uniquely identifies a location area in the network
  - Composed of MCC + MNC + LAC
- **CGI** – Cell Global Identifier
  - Uniquely identifies the cell within the network
  - Made up of LAI + CI

---

**GSM Handoffs**

Handoff major decision-making stages
- Identify the need
- Identify the candidate
- Evaluate the candidates
- Select a target cell

Types of handoffs
- **Intra-Cell**: Handoff between sectors of same cell
- **Intra-BSS**: if old and new BTSs are attached to same base station
  - MSC is not involved
- **Intra-MSC**: if old and new BTSs are attached to different base stations but within same MSC
- **Inter-MSC**: if MSCs are changed
  - Handoff Forward, Handoff Back, Handoff to a Third
Types of Handoff

- Intracell Standard Inter-BSC Intersystem handoff

Handoff initiation:
- Base station or MS notices signal is weakening (when the received signal strength goes below a certain threshold value)
- Base station or MS sends a handoff measurement request message to its BSC/MSC
- BSC/MSC requests neighbor base stations to report their reception of mobile’s signal strength
- MS to measure strength of neighbor base stations on downlink
  - (called Mobile Assisted Handoff)
- BSC/MSC picks neighbor base station with highest received signal strength combination in up and downlink to handoff too

GSM - Handoff

1. Report measurements
2. Request channel
3. Activate Channel
4. Send Handoff Command
5. Handoff Access
6. Handoff Detection
7. Communication Resumes

GSM - Mobile Assisted Handoff

Mobile listens to the BCCH of six neighboring base stations
- Break before Make handoff (hard handoff)
### Security in GSM

- **Security services**
  - access control/authentication
  - SIM (Subscriber Identity Module): secret PIN (personal identification number)
  - SIM-3G network: challenge response method
  - confidentiality
    - voice and signaling encrypted on the wireless link (after successful authentication)
  - anonymity
    - temporary identity TMSI (Temporary Mobile Subscriber Identity)
    - newly assigned at each new location update (LUP)
  - encrypted transmission

3 algorithms specified in GSM
- A3 for authentication ("secret", open interface)
- A5 for encryption (standardized)
- A8 for key generation ("secret", open interface)

**'secret'**
- A3 and A8 available via the Internet
- network providers can use stronger mechanisms
Authentication and Encoding

Authentication Procedure in GSM

Ciphering Procedure in GSM
Data services in GSM

Circuit Switched Data transmission standardized at 9.6 kbit/s
- advanced coding allows 14.4 kbit/s in a standard TDMA slot
- Widely deployed and used by WAP GSM phones
- not enough bandwidth for multimedia applications

HSCSD (High-Speed Circuit Switched Data)
- already standardized
- bundling of several time-slots on a radio carrier to get higher data rate: called AIUR (Air Interface User Rate)
  - maximum rate 57.6 kbit/s using 4 slots, 14.4 kbps each
  - (4 slot limit to allow MS to transmit then listen to downlink channel)
- Advantages: ready to use, constant quality, simple no additional equipment needed in network just software upgrades
- Disadvantage: channels blocked for voice transmission, expensive, not supported by all service providers

Most operators now have 2.5G solutions like GRPS or EDGE in place – 3G slowly being rolled out