Global System for Mobile (GSM)

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

Telcom 2720 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 2002**

- GSM 68.67%
- CDMA 12.20%
- Analogue 3.40%
- TDMA 0.01%
- W-CDMA 3.33%
- PDC 5.72%

**GSM subscribers by region - June 2002**

- Americas
- Europe
- Africa
- Asia Pacific
- Middle East
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 registers): 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
GSM System Architecture

Radio Station Subsystem

Network Switching Subsystem

Public Networks

Functional Architecture

Radio Subsystem (RSS)

Base Station Subsystem (BSS)

Network and Switching Subsystem (NSS)

Operation Subsystem (OSS)
Mobile station

Terminal for the use of GSM services

- 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 ($U_m$)
  - 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, map 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>X</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 measurements</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 Air Interface Uₘ

- Uses Physical **FDMA/TDMA/FDD** physical
  - In 900 MHz band: 890-915 MHz Uplink band, 935-960 MHz Downlink
  - Radio carrier is a 200kHz channel => 125 pairs of radio channels
    - Called Absolute Radio Frequency Channel Number (ARFCN)
    - ARFCN numbers given by \( f(n) = 890 + 0.2n \) MHz 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/FDMA

- GSM TDMA frame: 4.615 ms
- GSM time-slot (normal burst): 546.5 µs
- Higher GSM frame structures
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 Normal Burst

Training sequence is utilized for setting adaptive equalizer parameters.

Guard Period = 30.5 microsecs
Needed to allow for clock misalignment and propagation time of mobiles at different distances from BTS.

T: tail bits, S: flag, Train: equalizer training sequence
GSM operation from speech Input to Output

Speech
- Digitizing and source coding
- Channel coding
- Interleaving
- Burst Formatting
- Ciphering
- Modulation

Radio Channel

GSM Speech Coding

Analog speech
- Low-pass filter
- A/D
- RPE-LTP speech encoder

104 kbps
13 kbps

Channel encoder

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

Regular pulse excited - long term prediction (RPE-LRP) speech encoder (RELP 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 \( \frac{1}{2} \), constraint length 5

456 bits per 20ms speech frame
Interleaving Format

Speech coder

Channel encoding

456 bit

20 ms

RPE LTP encoding

456 bit

Interleaving

Stream of timeslots (only one time slot sent in a frame)

Single frame

Out of first 20 msec

Out of second 20 msec

Guard

Normal burst

57 bit 1 26 bit (training) 1 57 bit 3 8.25

Interleave distance = 8

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

- Even bits: 1 1 1 0 0 1 0
- Odd bits: 0 1 0 1

Signal value:
- h: high frequency
- n: low frequency
- +: original signal
- -: inverted 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

Frequency-hopped signal in GSM

GSM Air Interface Specifications Summary

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reverse Channel Frequency</td>
<td>890 – 915 MHz</td>
</tr>
<tr>
<td>Forward Channel Frequency</td>
<td>935 – 960 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 Coder Bit Rate</td>
<td>13.3 kbps</td>
</tr>
</tbody>
</table>
GSM System Identifiers

<table>
<thead>
<tr>
<th>Notation</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 (50 bits)</td>
<td>Directory number conforming to international convention – assigned by operating company to subscriber</td>
</tr>
<tr>
<td>TMSI</td>
<td>Temporary mobile subscriber identity</td>
<td>32 bits</td>
<td>Assigned by visitor location register to a subscriber</td>
</tr>
<tr>
<td>IMEI</td>
<td>International mobile equipment identifier</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>64 bits</td>
<td>Computed by network and mobile station</td>
</tr>
<tr>
<td></td>
<td>Mobile Station class mark</td>
<td>32 bits</td>
<td>Indicates properties of a mobile station</td>
</tr>
<tr>
<td>BSC</td>
<td>Base Station identity code</td>
<td>6 bits</td>
<td>Assigned by operating company to each BTS</td>
</tr>
<tr>
<td></td>
<td>Training Sequence</td>
<td>26 bits</td>
<td>Assigned by operating company to each BTS</td>
</tr>
<tr>
<td>LAI</td>
<td>Location Area Identity</td>
<td>40 bits</td>
<td>Assigned by operating company to each BTS</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 channels): 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
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)**

Control Multiframe = 51 TDMA Frames

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>20</th>
<th>21</th>
<th>22</th>
<th>39</th>
<th>40</th>
<th>41</th>
<th>42</th>
<th>49</th>
<th>50</th>
</tr>
</thead>
<tbody>
<tr>
<td>F</td>
<td>B</td>
<td>B</td>
<td>B</td>
<td>B</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>F</td>
<td>S</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>S</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
</tr>
</tbody>
</table>

- **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)**

Control Multiframe = 51 TDMA Frames

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>20</th>
<th>21</th>
<th>22</th>
<th>39</th>
<th>40</th>
<th>41</th>
<th>42</th>
<th>49</th>
<th>50</th>
</tr>
</thead>
<tbody>
<tr>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
</tbody>
</table>

- **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

GSM Protocol Stack

- 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 LAPD_m
- Physical layer (already discussed)
  - Time slot on a 200 KHz carrier – absolute radio frequency channel number (ARFCN)
GSM Protocol Stack

Air Interface

- CM: call management
- MM: mobility management
- RRM: radio resources management

Abis

- LAPDm
- radio
- 64 kbps

A

- CM
- MM
- RRM
- SCCP
- MTP
- 64 kbps

Mobile station

Base transceiver station

Base transceiver controller

Mobile services switching center

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

GSM Data Link LAPD<sub>m</sub> Messages

<table>
<thead>
<tr>
<th>Message Name</th>
<th>Function</th>
<th>Type</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>SET ASYNCHRONOUS</td>
<td>command</td>
<td>Unnumbered</td>
<td>initiate transfer of information messages</td>
</tr>
<tr>
<td>BRING INTO DORMANT (SAB)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DISCONNECT</td>
<td>command</td>
<td>Unnumbered</td>
<td>terminate transfer of information messages</td>
</tr>
<tr>
<td>TIME OUT RESPONSE (TOD)</td>
<td>response</td>
<td>Unnumbered</td>
<td>confirm a command</td>
</tr>
<tr>
<td>RECEIVE READY</td>
<td>command or</td>
<td>Supervisory</td>
<td>request transmission of information message</td>
</tr>
<tr>
<td>RECEIVE NOT READY</td>
<td>response</td>
<td>Supervisory</td>
<td>request retransmission of information message</td>
</tr>
<tr>
<td>REJECT</td>
<td>command or</td>
<td>Supervisory</td>
<td>suspend transmission of information messages</td>
</tr>
<tr>
<td></td>
<td>response</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Telom 2720
## GSM RRM Messages

Table 7.4 Radio Resources Management Messages

<table>
<thead>
<tr>
<th>Message Name</th>
<th>Logical Channel</th>
<th>Transmitted by</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sync Channel Information</td>
<td>SCH</td>
<td>Base</td>
</tr>
<tr>
<td>System Information Type 1, 2, 3, 4, 5</td>
<td>BCCH</td>
<td>Base</td>
</tr>
<tr>
<td>System Information Type B</td>
<td>SACCH</td>
<td>Base</td>
</tr>
<tr>
<td>Channel Request</td>
<td>RACH</td>
<td>Mobile</td>
</tr>
<tr>
<td>Paging Request Type 1, 2, 3, 8, 9</td>
<td>PCH</td>
<td>Base</td>
</tr>
<tr>
<td>Immediate Assignment</td>
<td>AGCH</td>
<td>Base</td>
</tr>
<tr>
<td>Immediate Assignment Extended</td>
<td>AGCH</td>
<td>Base</td>
</tr>
<tr>
<td>Immediate Assignment Reject</td>
<td>AGCH</td>
<td>Base</td>
</tr>
<tr>
<td>Assignment Complete</td>
<td>FACCH</td>
<td>Base</td>
</tr>
<tr>
<td>Additional Assignment</td>
<td>FACCH</td>
<td>Base</td>
</tr>
<tr>
<td>Paging Response</td>
<td>SDCCH</td>
<td>Mobile</td>
</tr>
<tr>
<td>Movement Report</td>
<td>SACCH</td>
<td>Mobile</td>
</tr>
<tr>
<td>Handover Command</td>
<td>FACCH</td>
<td>Base</td>
</tr>
<tr>
<td>Handover Access</td>
<td>TCH</td>
<td>Mobile</td>
</tr>
<tr>
<td>Physical Information</td>
<td>FACCH</td>
<td>Base</td>
</tr>
<tr>
<td>Handover Complete</td>
<td>FACCH</td>
<td>Mobile</td>
</tr>
<tr>
<td>Channel Release</td>
<td>FACCH</td>
<td>Base</td>
</tr>
<tr>
<td>Partial Release</td>
<td>FACCH</td>
<td>Base</td>
</tr>
<tr>
<td>Frequency Reconfiguration</td>
<td>SACCH/FACCH</td>
<td>Base</td>
</tr>
<tr>
<td>Classmark Change</td>
<td>SACCH/FACCH</td>
<td>Mobile</td>
</tr>
<tr>
<td>Channel Mode Modify</td>
<td>FACCH</td>
<td>Base</td>
</tr>
<tr>
<td>RN Status</td>
<td>FACCH/SACCH</td>
<td>Mobile/Base</td>
</tr>
</tbody>
</table>

## GSM MM Messages

Table 7.5 Mobility Management Messages

<table>
<thead>
<tr>
<th>Message Name</th>
<th>Transmitted by</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Request</td>
<td>Base</td>
</tr>
<tr>
<td>Authentication Response</td>
<td>Mobile</td>
</tr>
<tr>
<td>Authentication ReJECT</td>
<td>Base</td>
</tr>
<tr>
<td>Identity Request</td>
<td>Base</td>
</tr>
<tr>
<td>Identity Response</td>
<td>Base</td>
</tr>
<tr>
<td>TMSI Reallocation Command*</td>
<td>Mobile</td>
</tr>
<tr>
<td>Location Updating Request</td>
<td>Base</td>
</tr>
<tr>
<td>Location Updating Accept</td>
<td>Mobile</td>
</tr>
<tr>
<td>Location Updating Reject</td>
<td>Base</td>
</tr>
<tr>
<td>IMSIDetach Indication</td>
<td>Base</td>
</tr>
<tr>
<td>CM Service Request*</td>
<td>Mobile</td>
</tr>
<tr>
<td>CM Re-Establishment Request*</td>
<td>Mobile</td>
</tr>
<tr>
<td>MN Status</td>
<td>Mobile/Base</td>
</tr>
</tbody>
</table>
Sample GSM Message

Assignment Command
message on FACCH used in handoff to inform of new channel info

<table>
<thead>
<tr>
<th>Bit Position</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-4</td>
<td>Protocol Discriminator 0110 (RRM – message)</td>
</tr>
<tr>
<td>5-8</td>
<td>Transaction identifier</td>
</tr>
<tr>
<td>9-16</td>
<td>Message Type 00101110</td>
</tr>
<tr>
<td>17-40</td>
<td>Channel Description</td>
</tr>
<tr>
<td>41-48</td>
<td>Power Command</td>
</tr>
<tr>
<td>variable</td>
<td>Optional Data</td>
</tr>
</tbody>
</table>

Mobile Originating Call
Assignment Command on the downlink contains the most critical setup information

<table>
<thead>
<tr>
<th>0</th>
<th>UL: CHANNEL REQUEST</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DL: ASSIGNMENT COMPLETE</td>
</tr>
<tr>
<td>2</td>
<td>UL: CM SERVICE REQUEST</td>
</tr>
<tr>
<td>3</td>
<td>DL: CM SERVICE COMPLETE</td>
</tr>
<tr>
<td>4</td>
<td>UL: SETUP</td>
</tr>
<tr>
<td>5</td>
<td>DL: CALL PROCEEDING</td>
</tr>
<tr>
<td>6</td>
<td>UL: ASSIGNMENT COMMAND</td>
</tr>
<tr>
<td>7</td>
<td>DL: PROGRESS</td>
</tr>
<tr>
<td>8</td>
<td>DL: CONNECT</td>
</tr>
<tr>
<td>9</td>
<td>UL: CONNECT ACKNOWLEDGE</td>
</tr>
<tr>
<td>10</td>
<td>UL: RELEASE</td>
</tr>
<tr>
<td>11</td>
<td>UL: RELEASE COMPLETE</td>
</tr>
<tr>
<td>12</td>
<td>DL: CHANNEL RELEASE</td>
</tr>
</tbody>
</table>

Telcom 2720
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

- **RF + FCCH**
  - SCH sync + training
  - BCCH system parameters
  - RACH channel request
  - AGCH channel assignment

- 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 → SDCCH location update
Computes challenge response to verify identity → SDCCH challenge
SDCCH ciphered mode → Location update confirm
Initiate encryption of data for transmission → Ack ciphered mode
Complete location update process → 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

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>channel request</td>
<td>immediate assignment</td>
<td>service request</td>
</tr>
<tr>
<td>channel request</td>
<td>paging response</td>
<td>authentication request</td>
<td>authentication request</td>
<td>authentication response</td>
<td></td>
</tr>
<tr>
<td>immediate assignment</td>
<td>authentication response</td>
<td>ciphering command</td>
<td>ciphering command</td>
<td>ciphering complete</td>
<td></td>
</tr>
<tr>
<td>paging response</td>
<td>authentication response</td>
<td>ciphering complete</td>
<td>setup</td>
<td>setup</td>
<td></td>
</tr>
<tr>
<td>authentication request</td>
<td>ciphering command</td>
<td>assignment command</td>
<td>call confirmed</td>
<td>call confirmed</td>
<td></td>
</tr>
<tr>
<td>authentication response</td>
<td>ciphering complete</td>
<td>assignment complete</td>
<td>assignment command</td>
<td>assignment complete</td>
<td></td>
</tr>
<tr>
<td>ciphering command</td>
<td>setup</td>
<td>alerting</td>
<td>alerting</td>
<td>connect</td>
<td></td>
</tr>
<tr>
<td>ciphering complete</td>
<td>call confirmed</td>
<td>connect</td>
<td>connect</td>
<td>connect acknowledge</td>
<td></td>
</tr>
<tr>
<td>setup</td>
<td>assignment command</td>
<td>alerting</td>
<td>data/speech exchange</td>
<td>data/speech exchange</td>
<td></td>
</tr>
</tbody>
</table>
GSM MOC → Calling from MS

Dial called party → Setup Request → Call Proceeding

Tune to radio freq. → Radio channel → Ack → Complete

Calling from MS

Fetches subscriber info from VLR to process call, acks caller

Allocates trunk + radio channel

Call connected through PSTN

Alerts caller

Called party picks up

Call can proceed

GSM MTC → Calling to MS

Request dedicated control channel → PCH page request

Answer page

Computes response

Begin ciphering

Incoming call from PSTN

Allocates control channel

Request authentication

Request ciphering on channel
GSM MTC → Calling to MS (cont)

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

GSM Features

- Discontinuous Transmission (DTX)
  - Handset/BSC contain voice activity detectors (much of a conversation is silence!)
  - 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 signals 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 identifies 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
  - Made up 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
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 - Mobile Assisted Handoff

Mobile listens to the BCCH of six neighboring base stations

Break before Make handoff (hard handoff)

Handoff Procedure

<table>
<thead>
<tr>
<th>MS (measurement report)</th>
<th>BTS&lt;sub&gt;old&lt;/sub&gt; (measurement result)</th>
<th>BSC&lt;sub&gt;old&lt;/sub&gt; (HO decision)</th>
<th>MSC (HO required)</th>
<th>BSC&lt;sub&gt;new&lt;/sub&gt; (resource allocation)</th>
<th>BTS&lt;sub&gt;new&lt;/sub&gt; (link establishment)</th>
</tr>
</thead>
<tbody>
<tr>
<td>HO command</td>
<td>HO command</td>
<td>HO command</td>
<td>HO request</td>
<td>ch. activation</td>
<td>HO complete</td>
</tr>
<tr>
<td>HO command</td>
<td>HO command</td>
<td>HO command</td>
<td>HO request ack</td>
<td>ch. activation ack</td>
<td>HO complete</td>
</tr>
<tr>
<td>clear command</td>
<td>clear command</td>
<td>HO complete</td>
<td>clear command</td>
<td>clear complete</td>
<td>HO complete</td>
</tr>
<tr>
<td>clear complete</td>
<td>clear complete</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Security in GSM

Security services
- access control/authentication
  - user & SIM (Subscriber Identity Module): secret PIN (personal identification number)
  - SIM & 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

GSM System Architecture

VLR = Visitor Location Register
HLR = Home Location Register
EIR = Equipment Identity Register
AUC = Authentication Center
OMC = Operation Maintenance Center
ADC = Admission Data Center
PSTN = Public Switched Telephone Network
### Authentication and Encoding

- **Mobile Station**: Ki → RAND → A3 → A8 → SRES → Speech and Data in clear → Encoded Speech, Data, and Signaling → A5
- **Base Station Controller**: Speech and data in clear → Encoded Speech, Data, and Signaling → A5 → RAND → SRES
- **Base Station Switching Point**: VLR
- **Radio Control Point**: A Interface

**Speech and data in clear**
- **RAND**, **SRES**
- **Kc**
- **A5**

### Authentication Procedure in GSM

**AUC**
- **SRES**: Signed Response 32 bit
- **A3**: Authentication Algorithm
- **Ki**: 128-bit subscriber key unique to each subscriber
- **RAND**: 128-bit random number

**Random Number**
- **RAND**, **IMSI (1)**, **Ki(1)**
- **RAND**, **IMSI (X)**, **Ki(X)**

**A3**
- **SRES**

**MS**
- **Ki**, **RAND**, **A3**, **SRES**

**MSC**
- **RAND**, **SRES**

**COMPARES SRES VALUES RECEIVED FROM AUC AND MOBILE STATION**
- **IF IDENTICAL THEN MS IS AUTHENTICATED**
Ciphering Procedure in GSM

- **Kc**: 64-bit Ciphering Key
- **A8**: Ciphering Algorithm
- **Ki**: 128-bit subscriber key unique to each subscriber
- **RAND**: 128-bit random number

**SEND RAND TO MOBILE STATION AND Kc TO BSC FOR CIPHERING**

---

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