Global System for Mobile Communication (GSM)

Li-Hsing Yen
Assistant Prof.
Dept. of CSIE, Chung Hua Univ.

GSM System Architecture
Nomenclature

• MS (Mobile Station) =
  MT (Mobile Terminal ) +
  TE (Terminal Equipment)
• BSS (Base Station Subsystem) =
  BTS (Base Transceiver Station) +
  BSC (Base Station Controller)
• NSS (Network Switching Subsystem)
• MSC (Mobile Switching Center): telephony
  switching function and authentication of user

HLR and VLR

• HLR (Home Location Register)
  – a database to store and management
    permanent data of subscribers
• VLR (Visitor Location Register)
  – a database to store temporary information
    about subscribers
  – needed by MSC in order to service visiting
    subscribers
AuC and EIR

• Authentication Center (AuC)
  – used in the security data management for the authentication of subscribers.
• Equipment Identity Register (EIR)
  – used to maintain a list of legitimate, fraudulent, or faulty MSs.
  – optional in GSM network, and is not used generally.

GSM Interfaces

• Um
  – Radio interface between MS and BTS
  – each physical channel supports a number of logical channels
• A_{bis}
  – between BTS and BSC (vendor specific)
  – primary functions: traffic channel transmission, terrestrial channel management, and radio channel management
Frequency Division Duplex

\[ F_{\text{ul}}(n) = 890 + 0.2n \text{ MHz} \]

\[ F_{\text{dl}}(n) = F_{\text{ul}}(n) + 45 \text{ MHz} \]

Time Division Duplex

MS and BTS do not transmit simultaneously (MS transmits 3 time slots after the BTS)

Timing advance: MS transmits its data a little earlier as demanded by the “three time slots delay rule”.

Uplink

\[
\begin{array}{cccccccc}
2 & 3 & 4 & 5 & 6 & 7 & 0 & 1 \hline
1 & 2 & 3 & 4 & 5 & 6 & 7 & 0 \hline
\end{array}
\]

Downlink

\[
\begin{array}{cccccccc}
5 & 6 & 7 & 0 & 1 & 2 & 3 & 4 \hline
6 & 7 & 0 & 1 & 2 & 3 & 4 & 5 \hline
\end{array}
\]
Timing Advance

Base station

Mobile station

Propagation delay

send recv
recv send

send recv

Original timing

Timing advance

~ Propagation delay * 2

GSM Frame Structure

- 1 hyperframe = 2048 superframes (~3.5hr)
- For speech
  - 1 superframe = 51 multiframes = 6.12s
  - 1 multiframe = 26 frames = 120ms
- For Signaling
  - 1 superframe = 26 multiframes
  - 1 multiframe = 51 frames
- 1 frame = 8 time slots = 4.615 ms
- 1 time slot = 156.25 bit duration = 0.577ms
GSM Frame Hierarchy

- **Hyper frame**
  - Duration: 3.48hr
  - Format: 0 1 ... 2047

- **Super frame**
  - Duration: 6.12s
  - Format: 0 1 ... 48 49 50

- **Multi-frame**
  - Duration: 120ms
  - Format: 0 1 ... 23 24 25

- **Frame**
  - Duration: 4.615ms
  - Format: 0 1 2 3 4 5 6 7

- **Time Slot**
  - Duration: 0.57692ms
  - Format: 8.25 guard bits

Normal Burst Format

- **Trail bits**
  - Always (0,0,0); provide start and stop bit pattern

- **Encrypted bits**
  - Data is encrypted

- **Stealing bits**
  - Indicate whether the burst was stolen for urgent control signaling (FACCH signaling)

- **Guard bits**
  - Avoid overlapping with other bursts due to different path delay
Training Sequence

- A known bit pattern that differs for different adjacent cells
- to adapt the parameters of the receiver to the current path propagation characteristics
- to select the strongest signal in case of multipath propagation
- for multipath equalization
  - extract the desired signal from unwanted reflections

GSM Protocol Stack
Layer 1 - Physical Layer

- Modulation
- Equalization
- Channel coding
  - block code
  - convolutional code
- Interleaving
  - to distribute burst error

GSM Physical Layer (MS Side)

[Diagram showing the flow of signals through the physical layer processes, including signaling, voice, speech decoding, channel decoding, de-interleaving, burst de-formatting, deciphering, demodulation, modulation, ciphering, burst formatting, interleaving, channel coding, and R/F.]
GSM Speech Transmission

20 ms

speech encoding (RPE-LTP)

channel encoding

260 bits

456 bits

interleaving

burst formatting

GSM Speech Channel Coding

260 bits

Class 1a

Class 1b

Class 2

260 bits

50 bits

132 bits

78 bits

Parity bits protecting 1a

reordering

91 bits

91 bits

4

Tail Bits

Convolutional Coding

378 bits

78 bits

456 bits
Parity Bits

- The first 50 bits are protected by 3 parity bits p(0), p(2), p(3)
- generator polynomial \( g(D) = D^3 + D + 1 \)
- the remainder of \( d(0)D^{52} + d(1)D^{51} + \ldots + d(49)D^3 + p(0)D^2 + p(1)D + p(2) \) divided by \( g(D) \) should be \( 1 + D + D^2 \)
Convolutional Encoder for GSM Speech (Rate=1/2, K=5)

Interleaving

<table>
<thead>
<tr>
<th>0</th>
<th>64</th>
<th>128</th>
<th>192</th>
<th>256</th>
<th>320</th>
<th>384</th>
<th>448</th>
<th>56</th>
<th>120</th>
<th>184</th>
<th>248</th>
<th>312</th>
<th>392</th>
</tr>
</thead>
<tbody>
<tr>
<td>57</td>
<td>121</td>
<td>178</td>
<td>235</td>
<td>292</td>
<td>349</td>
<td>406</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>114</td>
<td>176</td>
<td>235</td>
<td>292</td>
<td>349</td>
<td>406</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>171</td>
<td>235</td>
<td>292</td>
<td>349</td>
<td>406</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>228</td>
<td>285</td>
<td>342</td>
<td>399</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>285</td>
<td>342</td>
<td>399</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>342</td>
<td>399</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>399</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>121</td>
<td>178</td>
<td>235</td>
<td>292</td>
<td>349</td>
<td>406</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>176</td>
<td>235</td>
<td>292</td>
<td>349</td>
<td>406</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>235</td>
<td>292</td>
<td>349</td>
<td>406</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>292</td>
<td>349</td>
<td>406</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>349</td>
<td>406</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>406</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>178</td>
<td>235</td>
<td>292</td>
<td>349</td>
<td>406</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>235</td>
<td>292</td>
<td>349</td>
<td>406</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>292</td>
<td>349</td>
<td>406</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>349</td>
<td>406</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>406</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>176</td>
<td>235</td>
<td>292</td>
<td>349</td>
<td>406</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>235</td>
<td>292</td>
<td>349</td>
<td>406</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>292</td>
<td>349</td>
<td>406</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>349</td>
<td>406</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>406</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>235</td>
<td>292</td>
<td>349</td>
<td>406</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>292</td>
<td>349</td>
<td>406</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>349</td>
<td>406</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>406</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>292</td>
<td>349</td>
<td>406</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>349</td>
<td>406</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>406</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>349</td>
<td>406</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>406</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>399</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>127</td>
<td>191</td>
<td>255</td>
<td>335</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>134</td>
<td>191</td>
<td>255</td>
<td>335</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>191</td>
<td>255</td>
<td>335</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>255</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>335</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
GSM Normal Burst Formatting

Physical Vs. Logical Channels

- Physical channels are all the available time slots of a BTS
  - a BTS with 6 carriers has 48 physical channels
- Logical channels are piggybacked on the physical channels
  - logical channels are laid over the grid of physical channels
  - each logical channel performs a specific task
GSM Logical Channels (I)

• Speech traffic channels (TCH)
  – Full-rate TCH (TCH/F)
  – Half-rate TCH (TCH/H)
• Broadcast channels (BCH)
  – Frequency correction channel (FCCH)
  – Synchronization channel (SCH)
  – Broadcast control channel (BCCH)
• Cell broadcast channel (CBCH)

GSM Logical Channels (II)

• Common control channels (CCCH)
  – Paging channel (PCH)
  – Access grant channel (AGCH)
  – Random access channel (RACH)
• Dedicated control channel (DCCH)
  – Slow associated control channel (SACCH)
  – Stand-alone dedicated control channel (SDCCH)
  – Fast associated control channel (FACCH)
Broadcast Channels (BCH)

- Frequency correction channel (FCCH)
  - the “lighthouse” of a BTS
- Synchronization channel (SCH)
  - PLMN/base identifier of a BTS plus synchronization information (frame number)
- Broadcast control channel (BCCH)
  - to transmit system information 1-4, 7-8 (differs in GSM 900, GSM 1800, and PCS 1900)

CBCH and CCCH

- CBCH (Cell Broadcast Channel)
  - transmits cell broadcast messages
- PCH (Paging Channel)
  - carries PAG_REQ message
- AGCH (Access Grant Channel)
  - SDCCH channel assignment
- RACH (Random Access Channel)
  - communication request from MS to BTS
Mapping of Logical Channels

- Each BTS has a particular frequency carrier called BCCH-TRX to transmit BCCH info
- The following channel structure can be found on time slot 0 of carrier BCCH-TRX
  - FCCH
  - SCH
  - BCCH information 1-4
  - Four SDCCH subchannels (optional)
  - CBCH (optional)

Example Mapping of Logical Channels on Time Slot 0 (Downlink)

<table>
<thead>
<tr>
<th>FN= 0 - 5</th>
<th>FCCH + SCH + BCCH 1 - 4</th>
<th>Block 4 CCCH/SDCCH</th>
<th>FN= 26 - 29</th>
</tr>
</thead>
<tbody>
<tr>
<td>FN= 6 - 9</td>
<td>Block 0 reserved for CCCH</td>
<td>FCCH/SCH</td>
<td>FN= 30 - 31</td>
</tr>
<tr>
<td>FN= 10 - 11</td>
<td>FCCH/SCH</td>
<td>Block 5 CCCH/SDCCH</td>
<td>FN= 32 - 35</td>
</tr>
<tr>
<td>FN= 12 - 15</td>
<td>Block 1 reserved for CCCH</td>
<td>FCCH/SCH</td>
<td>FN= 36 - 39</td>
</tr>
<tr>
<td>FN= 16 - 19</td>
<td>Block 2 reserved for CCCH</td>
<td>Block 6 CCCH/SDCCH</td>
<td>FN= 40 - 41</td>
</tr>
<tr>
<td>FN= 20 - 21</td>
<td>FCCH/SCH</td>
<td>Block 7 CCCH/SACCH</td>
<td>FN= 42 - 45</td>
</tr>
<tr>
<td>FN= 22 - 25</td>
<td>Block 3 CCCH/SDCCH</td>
<td>Block 7 CCCH/SACCH</td>
<td>FN= 46 - 49</td>
</tr>
<tr>
<td></td>
<td></td>
<td>not used</td>
<td>FN= 50</td>
</tr>
</tbody>
</table>
Example Mapping of Logical Channels on Time Slot 2 (Downlink)

- **FN= 0 - 11**: TCH
- **FN= 12**: SACCH
- **FN= 13 - 24**: TCH
- **FN= 25**: not used

**GSM Layer 2: LAPDm**

- **Functions**
  - organization of Layer 3 information into frames
  - peer-to-peer transmission of signaling data in defined frame formats
  - recognition of frame formats
  - establishment, maintenance, and termination of one or more (parallel) data links on signaling channels
Layer 3 Protocol Architecture: Mobile Station Side

Layer 3 - RR Sublayer

- The RR sublayer handles all the procedures necessary to establish, maintain, and release dedicated radio connections
  - channel allocation
  - handover
  - timing advance
  - power control
  - frequency hopping
Three Cases of Hand-over

1. different BTS, same BSC
2. different BSC, same MSC
3. different MSC, same PLMN
   (old MSC=anchor MSC
    new MSC=relay MSC)

Layer 3 - MM Sublayer

- The MM sublayer copes with all the effects of handling a mobile user that are not directly related to radio functions
  - location area
  - location registration & call delivery
  - location update & paging
Authentication & Encryption/Decryption in GSM

Mobile Station

SIM

A8

A3

Ki

SRES

Kc

A5

S1

S2

Visited System

A5

S1

S2

Home System

RAND

Ki

A3

A8

SRES

Kc

frame number

visited

System

plain text

ciphered data

plain text

channel request

channel activation command

channel activation acknowledge

channel assignment

location update request

authentication request

authentication response

comparison of authentication parameters

assignment of TMSI

acknowledgement of TMSI

entry of the new area and identity into the VLR & HLR

channel release

old IMSI

old auth. para.

old TMSI

old VLR ID

new IMSI

new TMSI

MS

BTS

BSC

MSC

VLR

HLR

cancellation

ack

subscriber information

location update

new VLR

old VLR

1

2

3

4

ack

subscriber information

new TMSI

old TMSI

old VLR ID
Layer 3 - CM Sublayer

- The CM sublayer manages all the functions necessary for circuit-switched call control
  - call establishment procedures for mobile-originated calls and mobile-terminated calls
  - in-call modification
  - call reestablishment
  - Dual Tone Multi Frequency (DTMF) control procedure for DTMF transmission

Contents of CM

- Call Control (CC)
- Short Message Service (SMS)
- Supplementary Service (SS)
Paging Procedure

Call Setup Procedure: Mobile Terminated Call

INTerrogating eXchange (INTX)
Mobile Station ISDN Number (MSISDN) (Country Code, see E.164)
Mobile Station Roaming Number (MSRN) (Mobile Country Code, see E.212)
Dual Tone Multiple Frequency (DTMF) in PSTN

DTMF in GSM