COMP4310/6310 Wireless Mobile Computing
Cellular Networks II
Difference: WiFi and Cellular

- Services
- Data Rate
- Coverage
- Reliability
Review: GSM key components

- **MS** (mobile station)
- **BSS** (Base Station Subsystem):
  - **BTS** (Base Transceiver Station): sender and receiver
  - **BSC** (Base Station Controller): controlling several transceivers
- **MSC** (mobile switching center)
- **LR** (location register)
- **SS7** (Signaling System 7)
Review: GSM Architecture

- **Radio Subsystem**: MS → BTS → BSC → A
  - U_m (Um)
  - A_bis

- **Network and Switching Subsystem**: MSC
  - SS7
  - IWF
  - ISDN
  - PSTN
  - EIR
  - HLR
  - VLR

- **Fixed Partner Networks**: ISDN, PSTN, ISDN, PSPDN, CSPDN
## Channels in GSM

<table>
<thead>
<tr>
<th>Control Channel</th>
<th>Group</th>
<th>Channel</th>
<th>Direction</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>BCCH (Broadcast control channel)</td>
<td>BCCH (Broadcast control channel)</td>
<td>BS → MS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FCCH (Frequency correction channel)</td>
<td>BS → MS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SCH (Synchronization channel)</td>
<td>BS → MS</td>
</tr>
<tr>
<td></td>
<td>CCCH (Common control channel)</td>
<td>PCH (Paging channel)</td>
<td>BS → MS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RACH (Random access channel)</td>
<td>MS → BS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AGCH (Access grant channel)</td>
<td>BS → MS</td>
</tr>
<tr>
<td></td>
<td>DCCH (Dedicated control channel)</td>
<td>SDCCH (Stand-alone dedicated control channel)</td>
<td>BS ↔ MS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SACCH (Slow associated control channel)</td>
<td>BS ↔ MS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FACCH (Fast associated control channel)</td>
<td>BS ↔ MS</td>
</tr>
<tr>
<td>Traffic Channel</td>
<td>TCH (Traffic Channel)</td>
<td>TCH/f (Full-rate traffic channel)</td>
<td>BS ↔ MS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCH/s (Half-rate traffic channel)</td>
<td>BS ↔ MS</td>
</tr>
</tbody>
</table>
Control Channels of GSM

Control Channels used to Broadcast Information to all MSs.
- **Broadcast Control Channel (BCCH):** Used to transmit the system parameters like the frequency of operation in the cell, operator identifiers, etc.,
- **Frequency Correction Channel (FCCH):** Used for transmission of frequency references and frequency correction bursts
- **Synchronization Channel (SCH):** Used to provide the synchronization training sequences burst of 64 bits length to the MSs.

Control Channels used to establish link between MS and BS
- **Random Access Channel (RACH):** Used by the MS to transmit information regarding the requested dedicated channel from GSM.
- **Paging Channel:** Used by the BS to communicate with individual MS in the cell.
- **Access Grant Channel:** Used by the BS to send information about timing and synchronization (opens a dedicated channel).
Control Channels of GSM

Dedicated Control Channels used to serve for any control information transmission during the actual communication

- **Stand-alone dedicated Control Channel**: Allocated with SACCH, used for transfer of signaling information between the BS and the MS before a TCH has been allocated.
  - Slow: 782 bps; used to setup the TCH (authentication, registration, etc.)

- **Slow Associated Control Channel (SACCH)**: Allocated along with a user channel (TCH), for transmission of control information during the actual transmission. Slow: 950 bps.

- **Fast Associated Control Channel (FACCH)**: Not a dedicated channel but carries the same information as SDCCH. But, it is a part of Traffic channel while SDCCH is a part of control channel. Used in emergencies.
Traffic Channels of GSM (TCH)

- For user data (voice, fax)
- Full rate (TCH/F): 22.8kbps and half rate (TCH/H): 11.4kbps
- New codecs can squeeze a voice channel in a TCH/H effectively doubling the capacity of the system
- For data many options are available: TCH/F4.8, TCH/F9.6 and TCH/F14.4 at 4.8kbps, 9.6kbps and 14.4kbps respectively (different FEC capabilities).
GSM - TDMA/FDMA

higher GSM frame structures

GSM frames

1 2 3 4 5 6 7 8

935-960 MHz
124 channels (200 kHz)
downlink

890-915 MHz
124 channels (200 kHz)
uplink

frequency

time
# Frames in GSM

1 hyperframe = 2048 superframes = 2715684 TDMA frames (3 hr, 28 min, 53 s, 750 ms)

<table>
<thead>
<tr>
<th>Hyperframe</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>……</th>
<th>2046</th>
<th>2047</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Superframe</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>……</th>
<th>49</th>
<th>50</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0</td>
<td>1</td>
<td></td>
<td>……</td>
<td>24</td>
<td>25</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multiframe</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>……</td>
<td>24</td>
<td>25</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TDMA frame</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>……</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **TCH, SACCH, FACCH**

- **FCCH, SCH, BCCH, RACH, AGCH, PCH, SDCCH, CBCH, SACCH**
Subscriber Identity Module (SIM)

- SIM contains subscriber-specific information such as:
  - Phone numbers,
  - Personal identification number (PIN),
  - Security/Authentication parameters.
- SIM can also be used to store short message.
- SIM can be a small plug-in module that is placed (somewhat permanently) in the mobile unit, or it can be a card (like a credit card).
- A modular portable SIM allows a user to use different terminal sets.
- SIM supports roaming.
Mobile Station ISDN (MSISDN)

- MSISDN is the number that the calling party dials in order to reach the subscriber.
- It is used by the land network to route calls toward an appropriate MSC.
- Associated with the SIM, not with the phone

The format of MSISDN

```
<table>
<thead>
<tr>
<th>Country code (MCC)</th>
<th>National destination code (NDC)</th>
<th>Subscriber number (SN)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 to 3 digits</td>
<td>Variable</td>
<td>Variable</td>
</tr>
<tr>
<td>15 digits or less</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```
International Mobile Subscriber Identity (IMSI)

• Each mobile unit is identified uniquely with a set of values. These values are used to identify the country in which the mobile system resides, the mobile network, and the mobile subscriber.

• The remainder of the IMSI is made up of the mobile subscriber identification code (MSIC), which is the customer identification number.

• The IMSI is also used for an MSC/VLR to find out the subscriber’s home PLMN (Public land mobile network).
## Format of IMSI

The International Mobile Subscriber Identity (IMSI) is a unique identifier for each mobile subscriber. It consists of 15 digits or less, divided into three main parts:

- **Mobile country code (MCC)**: 3 digits
- **Mobile network code (MNC)**: 2 digits
- **Mobile subscriber identification code (MSIC)**: Up to 9 digits

### Example:

<table>
<thead>
<tr>
<th>MCC</th>
<th>MNC</th>
<th>MSIC</th>
</tr>
</thead>
<tbody>
<tr>
<td>05</td>
<td>01</td>
<td>Telecom Australia;</td>
</tr>
<tr>
<td>234</td>
<td>234</td>
<td>UK Vodafone;</td>
</tr>
</tbody>
</table>

Note: MCC and MNC codes are specific to each country and network operator.
Mobile Station Roaming Number (MSRN)

- MSRN is allocated on a temporary basis when the MS roams into another numbering area.
- MSRN is used by the HLR for rerouting call to the MS.

The format of MSRN

<table>
<thead>
<tr>
<th>Country code (MCC)</th>
<th>National destination code (NDC)</th>
<th>Subscriber number (SN)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 to 3 digits</td>
<td>Variable</td>
<td>Variable</td>
</tr>
<tr>
<td>15 digits or less</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
International MS Equipment Identity (IMSEI)

- IMSEI is assigned to each GSM unit at the factory.

The format of IMSEI

<table>
<thead>
<tr>
<th>Type approval code (TAC)</th>
<th>Final assembly code (FAC)</th>
<th>Serial number (MSIC)</th>
</tr>
</thead>
</table>

15 digits or less

- 3 digits
- 1 or 2 digits
- Up to 9 digits

Spare 1 digit
Handover decision

receive level
BTS_{old}

receive level
BTS_{new}

HO_MARGIN

f_2

f_3

MS

BTS_{old}

BTS_{new}
# Handover (Handoff)

<table>
<thead>
<tr>
<th>Handover</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intra-cell / Intra-BTS</td>
<td>The channel for the connection is changed within the cell, e.g., if the channel has a high level of interference. The change can apply to another frequency of the same cell or to another time slot of the same frequency.</td>
</tr>
<tr>
<td>Inter-cell / Intra-BSC</td>
<td>In this case there is a change in radio channel between two cells that are served by the same BSC.</td>
</tr>
<tr>
<td>Inter-BSC / Intra-MSC</td>
<td>A connection is changed between two cells that are served by different BSCs but operate in the area of the same MSC.</td>
</tr>
<tr>
<td>Inter-MSC</td>
<td>A connection is changed between two cells that are in different MSC areas.</td>
</tr>
</tbody>
</table>
Security

• Access control and authentication
  - Authenticates the user to the SIM
  - Authenticates the SIM to the network - A3

• Confidentiality
  - All user-related data is encrypted - A5

- A3, A5: security algorithms
GSM - authentication

Step 1: RAND

Step 2: SRES

AC

MSC

K_i: individual subscriber authentication key

SRES: signed response
GSM - key generation and encryption

mobile network (BTS)

MS with SIM

AC

K_i

128 bit

RAND

128 bit

A8

cipher key

BTS

K_c

64 bit

data

A5

SIM

K_i

128 bit

RAND

128 bit

A8

data

A5

encrypted data

www.memphis.edu
Summary: GSM

- **Key components:**
  - **MS** (mobile station)
  - **BSS** (Base Station Subsystem):
    - **BTS** (Base Transceiver Station): sender and receiver
    - **BSC** (Base Station Controller): controlling several transceivers
  - **MSC** (mobile switching center)
  - **LR** (location register)
  - **SS7** (Signaling System 7)

- **FDMA/TDMA**

- Comprehensive and successful
  - Handover, security, ......
## LTE vs. LTE-Advanced

<table>
<thead>
<tr>
<th>Technology</th>
<th>LTE</th>
<th>LTE-A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peak data rate Down Link (DL)</td>
<td>150 Mbps</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>Peak data rate Up Link (UL)</td>
<td>75 Mbps</td>
<td>500 Mbps</td>
</tr>
<tr>
<td>Transmission bandwidth (DL)</td>
<td>20MHz</td>
<td>100 MHz</td>
</tr>
<tr>
<td>Transmission bandwidth (UL)</td>
<td>20MHz</td>
<td>40 MHz (requirements as defined by ITU)</td>
</tr>
<tr>
<td>Mobility</td>
<td>Optimized for low speeds ($\leq 15$ km/hr) High Performance At speeds up to 120 km/hr Maintain Links at speeds up to 350 km/hr</td>
<td>Same as that in LTE</td>
</tr>
</tbody>
</table>
| Coverage                          | Full performance up to 5 km | a) Same as LTE requirement  
b) Should be optimized or deployment in local areas/micro cell environments. |
| Scalable Band Widths              | 1.3, 3, 5, 10, and 20 MHz | Up to 20–100 MHz                                                      |
| Capacity                          | 200 active users per cell in 5 MHz | 3 times higher than that in LTE                                       |
LTE Adoption (as of May 2012)

- Red - countries with LTE service
- Blue - planned or ongoing deployment
LTE Adoption (as of December 2014)

- Red - countries with LTE service
- Blue - planned or ongoing deployment
Features

- All IP Network (VoIP for voice)
  - Can also use other 3GPP technologies for voice
- Spectrum Flexibility
  - (1.25MHz - 20MHz)
  - TDD/FDD (full-duplex and half-duplex)
- Multi-antenna transmissions (4 MIMO on downlink, 2 MIMO on uplink)
- 300 Mbps peak downlink in 20MHz x 4 MIMO x 64 QAM
- 75 Mbps peak uplink
Features (cont)

- 100 km macro cells (5 km with optimal performance)
- Up to 200 active users in a cell
- OFDM downlink and Single Carrier FDMA (SC-FDMA) uplink
- HARQ (Hybrid ARQ)
- Co-existence with existing technologies (calls can be started in LTE and transferred to GSM/GPRS, WCDMA)