Overview

GSM

- formerly: Groupe Spéciale Mobile (founded 1982)
- now: Global System for Mobile Communication
- Pan-European standard (ETSI, European Telecommunications Standardisation Institute)
- simultaneous introduction of essential services in three phases by the European telecommunication administrations
- seamless roaming within Europe possible
- today many providers all over the world use GSM (more than 180 countries in Asia, Africa, Europe, Australia, America)
- more than 900 million subscribers
- more than 70% of all digital mobile phones use GSM
Performance characteristics of GSM

Communication
- mobile, wireless communication; support for voice and data services

Total mobility
- international access, chip-card enables use of access points of different providers

Worldwide connectivity
- one number, the network handles localization

High capacity
- better frequency efficiency, smaller cells, more customers per cell

High transmission quality
- high audio quality and reliability for wireless, uninterrupted phone calls at higher speeds (e.g., from cars, trains)

Security functions
- access control, authentication via chip-card and PIN

Mobile Services

GSM services
- basic services
  - voice services
  - data services
  - short message service
- additional services
  - emergency number
  - group 3 fax
  - electronic mail
- supplementary services
  - identification: forwarding of caller number
  - suppression of number forwarding
  - automatic call-back
  - conferencing with up to 7 participants
  - ...
Basic Services

- Services are supported by traffic channels
  - full rate: 22.8 kbit/s (gross bit rate, unprotected transmission)
  - half rate: 11.4 kbit/s (gross bit rate, unprotected transmission)

- Voice services (speech coding with protection)
  - full rate: 13 / 12.2 kbit/s (original coder / enhanced full rate coder)
  - half rate: 5.6 kbit/s (enhanced half rate coder)

- Data services (coding with different levels of protection)
  - full rate: 9.6 / 4.8 / 2.4 kbit/s
  - half rate: 4.8 / 2.4 kbit/s

- Enhanced data services
  - HSCSD (High Speed Circuit Switched Data)
    - \( n \times 14.4 / n \times 9.6 / n \times 4.8 \) kbit/s \((n=1, 2, 3, 4)\)
  - GPRS (General Packet Radio Service)
    - various rates (typically up to 53.6 kbit/s)

GSM architecture: PLMN - Public Land Mobile Network

- Public Land Mobile Network (PLMN)
- Network Support System (NSS)
- Operations Support System (OSS)
- Base Station System (BSS)
- Radio Access Network (RAN)
- Core Network (CN)
- Radio Link Control (RLC)
- Medium Access Control (MAC)
- Physical Layer (PHY)
- Signaling System (SS)
- ISDN, PSTN
- GMSC
- VLR
- HLR
- EIR
- AUC
- OMC
- BSC
GSM architecture: PLMN - Public Land Mobile Network

RSS - Radio Subsystem: covers all radio aspects

- **MS** Mobile Station: Mobile terminal equipment
- **BSC** Base Station Controller: Management of several BTS and MS
- **BTS** Base Transceiver Station: Transmitter, receiver and antennas

---

NSS - Network Subsystem: switching, mobility management, interconnection to other networks, system control

- **MSC** Mobile Switching Centre: Management of all connections
- **HLR** Home Location Register: Associated to each PLMN
- **VLR** Visitor Location Register: Associated to each MSC
- **GMSC** Gateway MSC: MSC providing interconnection to other networks

---

fixed network
GSM architecture: PLMN - Public Land Mobile Network

OSS - Operation Subsystem: centralized operation, management, and maintenance of all GSM subsystems

- OMC (Operation and Management Centre): Control of the radio and network subsystems
- AuC (Authentication Centre): Security functions
- EIR (Equipment Identity Register): Mobile station registration

---

GSM architecture: interfaces

Interfaces

- $U_m$: radio interface
- $A_{bis}$: standardized, open interface with 16/64 kbit/s user channels
- $A$: standardized, open interface with 64 kbit/s user channels
Voice transcoding and rate adaptation

- Need for transcoding and rate adaptation
  - BTS - 13 kbit/s air-interface (original coder)
  - MSC - 64 kbit/s ISDN type switching (PCM, A-law)

- 3 options for Transcoding and Rate Adapter Unit (TRAU)

Mobile addresses

- Several mobile numbers are needed
  - **IMSI** - International Mobile Subscriber Identity
    
    Mobile Country Code (MCC) + Mobile Network Code (MNC) + Mobile Subscriber Identification Number (MSIN)
    
    - uniquely identifies the user (SIM card)

  - **TMSI** - Temporary Mobile Subscriber Identity
    
    32 bits
    
    - local number allocated by VLR, may be changed periodically
    - hides the IMSI over the air interface - transmitted instead of IMSI

  - **MSRN** - Mobile Station Roaming Number
    
    Visitor Country Code (VCC) + Visitor National destination Code (VNDC) + Current MSC code + temporary subscriber number
    
    - generated by VLR for all visiting users
    - helps HLR to determine current location area
    - hides the IMSI inside the network
Mobile station functional groups

- **MT (Mobile Termination)**
  - offers common functions used by all services the MS offers
  - end-point of the radio interface (Um) - equivalent to NT of an ISDN access
  - hides GSM radio specific characteristics

- **TE (Terminal Equipment)**
  - peripheral device of the MS, offers services to a user

- **TA (Terminal Adapter)**
  - interfaces MT with different types of terminal

---

**SIM card (Subscriber Identity Module)**

- uniquely associated to a user
- stores user and location addresses
  - IMSI - International Mobile Subscriber Identity
  - TMSI - Temporary Mobile Subscriber Identity
  - LAI - Location Area Identification
- supports authentication and encryption mechanisms
  - PIN - Personal Identity Number
  - PUK - PIN Unblocking Key
  - $K_i$ - subscriber secret authentication key
  - $A3$ - authentication algorithm
  - $A8$ - cipher key generation algorithm
- contains personal data
  - list of subscribed services
  - RAM for user directory, SMS
Base transceiver station and base station controller

- Tasks of a BSS are distributed over BSC and BTS
  - BTS comprises radio specific functions
  - BSC is the switching center for radio channels
    - switch calls from MSC to correct BTS

<table>
<thead>
<tr>
<th>Functions</th>
<th>BTS</th>
<th>BSC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management of radio channels</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Frequency hopping (FH)</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Management of terrestrial channels</td>
<td></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></td>
<td>X</td>
</tr>
<tr>
<td>Rate adaptation</td>
<td>X</td>
<td></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></td>
<td>X</td>
</tr>
<tr>
<td>Traffic measurement</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Authentication</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Location registry, location update</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Handover management</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

Mobile 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

- Specific functions of a MSC
  - switching of 64 kbit/s channels
  - paging and call forwarding
  - termination of SS7 (signaling system no. 7)
  - mobility specific signaling
  - location registration and forwarding of location information
  - support of short message service (SMS)
  - generation and forwarding of accounting and billing information
Location registers

- **Database requirements**
  - scalability
  - high capacity
  - low delay

- **Home Location Register (HLR)**
  - central master database
    - data from every user that has subscribed to the operator
    - one database per operator
    - may be replicated
  - subscriber data
    - IMSI - International Mobile Subscriber Identity
    - list of subscribed services with parameters and restrictions
  - location data
    - current MSC/VLR address

Location registers

Visitor Location Register (VLR)

- local database
  - data about all users currently in the domain of the VLR
  - includes roamers and non-roamers
  - associated to each MSC

- subscriber identity
  - IMSI - International Mobile Subscriber Identity

- temporary location
  - LAI - Location Area Identification

- temporary addresses
  - MSRN - Mobile Station Roaming Number
  - TMSI - Temporary Mobile Subscriber Identity
### GSM location / mobile addresses: summary

#### HLR - Home Location Register
- **Permanent**
  - IMSI - International Mobile Subscriber Identity
- **Temporary**
  - MSRN - Mobile Station Roaming Number

#### VLR - Visitor Location Register
- **Permanent**
  - IMSI - International Mobile Subscriber Identity
- **Temporary**
  - LAI - Location Area Identification
  - MSRN - Mobile Station Roaming Number
  - TMSI - Temporary Mobile Subscriber Identity

#### SIM - Subscriber Identity Module
- **Permanent**
  - IMSI - International Mobile Subscriber Identity
- **Temporary**
  - LAI - Location Area Identification
  - TMSI - Temporary Mobile Subscriber Identity

---

### Operation subsystem elements

#### Authentication Center (AuC)
- associated to HLR
- search key: IMSI
- supports authentication and encryption mechanisms
  - $K_i$ - subscriber secret authentication key
  - A3 - authentication algorithm
  - A8 - cipher key generation algorithm

#### Equipment Identity Register (EIR)
- stores mobile stations IMEI (International Mobile Equipment Identity)
- white list - mobile stations allowed to connect without restrictions
- black list - mobile stations locked (stolen or not type approved)
- gray list - mobile stations under observation for possible problems

#### Operation and Maintenance Center (OMC)
- control capabilities for the radio and the network subsystems
GSM - TDMA/FDMA

935-960 MHz
124 channels (200 kHz)
downlink

890-915 MHz
124 channels (200 kHz)
uplink

FDMA channels

TDMA frame

Radio interface
bit rate
156.25 bits/0.5769 ms =
270.8 kbit/s

Burst structures

- **Normal Burst:** normal data transmission

  - **TB** | **CD** | **S** | **TS** | **S** | **CD** | **TB** | **GP**
  - 3 | 57 | 1 | 26 | 1 | 57 | 3 | 8.25

  - Training Sequence - allows estimation of propagation characteristics (including multipath), in order to set up the equaliser parameters
  - Stealing flags - indicate that a burst normally assigned to traffic is stolen for signalling

- **Access Burst:** MS first time access

  - **TB** | **SS** | **CD** | **TB** | **GP**
  - 8 | 41 | 36 | 3 | 68.25

  - Synchronisation Sequence - long training sequence
  - Coded Data - channel or handover access request
  - Guard Period - long period since time advance is not yet defined
  - Guard Period - avoids overlapping between bursts
  - Tail Bits - assist receiver equalisation (set to 0)
  - Coded Data - user data transmission
Burst structures

- Frequency Correction Burst: frequency synchronisation of the MS

```
<table>
<thead>
<tr>
<th>TB</th>
<th>FBS</th>
<th>TB</th>
<th>GP</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>142</td>
<td>3</td>
<td>8.25</td>
</tr>
</tbody>
</table>
```

- Frequency Correction Burst: frequency synchronisation of the MS

- Synchronisation Burst: time synchronisation of the MS

```
<table>
<thead>
<tr>
<th>TB</th>
<th>CD</th>
<th>SS</th>
<th>CD</th>
<th>TB</th>
<th>GP</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>39</td>
<td>64</td>
<td>39</td>
<td>3</td>
<td>8.25</td>
</tr>
</tbody>
</table>
```

Synchronisation Sequence - long training sequence

Coded Data - data used to align the mobile to the base station's time-slot structure

Frame hierarchy

- Frame hierarchy

```
<table>
<thead>
<tr>
<th>frame</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>4</td>
</tr>
<tr>
<td>5</td>
</tr>
<tr>
<td>6</td>
</tr>
<tr>
<td>7</td>
</tr>
</tbody>
</table>
```

- Frame hierarchy

```
<table>
<thead>
<tr>
<th>traffic multiframe</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>4</td>
</tr>
<tr>
<td>5</td>
</tr>
</tbody>
</table>
```

- Frame hierarchy

```
<table>
<thead>
<tr>
<th>control multiframe</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
</tbody>
</table>
```

- Frame hierarchy

```
<table>
<thead>
<tr>
<th>superframe (*)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 x 51</td>
</tr>
<tr>
<td>6.12 s</td>
</tr>
</tbody>
</table>
```

- Frame hierarchy

```
<table>
<thead>
<tr>
<th>hyperframe (**)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2048 x 6.12 s</td>
</tr>
<tr>
<td>35 hours</td>
</tr>
</tbody>
</table>
```

(*) - aligns traffic and control multiframe

(**) - allows cycle for frame number
### Logical channels

#### TCH Traffic Channels
- **TCH/F** Full-rate Traffic Channels
- **TCH/H** Half-rate Traffic Channels

#### BCH Broadcast Channels
- **FCCH** Frequency Correction Channel
- **SCH** Synchronization Channel
- **BCCH** Broadcast Control Channel

#### CCCH Common Control Channels
- **RACH** Random Access Channel
- **AGCH** Access Grant Channel
- **PCH** Paging Channel

#### DCCH Dedicated Control Channels
- **SDCCH** Stand-alone Dedicated Control Channel
- **SACCH** Slow Associated Control Channel
- **FACCH** Fast Associated Control Channel

#### SACCH
- **SACCH** Slow Associated Control Channel
- **FACCH** Fast Associated Control Channel

#### Application
- **User data**
- **Carrier synchronization**
- **Frame synchronisation**
- **General network information**
- **Cell information (present and adjacent)**
- **Request SDCCH for signalling**
- **Request TCH for handover**
- **Confirmation of SDCCH or TCH request**
- **Registration / location updating**
- **Control information between MS and BTS during the progress of a call or call set up**
- **Exchange of time critical control information during the progress of a call**

#### Allocation
- **Allocated by network on demand by MS**
- **Permanent**
- **Multiple access with slotted Aloha contention between MS**
- **Associated to a specific TCH or SDCCH**
- **Allocated by network or MS (*)**

(*) Fast allocation by setting S bit; bits are stolen from TCH
### Logical channels

<table>
<thead>
<tr>
<th>Channel</th>
<th>Burst type</th>
<th>Time-slot</th>
<th>Multiframe</th>
<th>Bursts / Multiframe</th>
<th>Capacity</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCH</td>
<td>Normal (114 data bits)</td>
<td>Any</td>
<td>26 frames</td>
<td>24</td>
<td>24 x 114 / 120 = 22.8 kbit/s</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(120 ms)</td>
<td></td>
<td>12 x 114 / 120 = 11.4 kbit/s</td>
</tr>
<tr>
<td>TCH/F</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BCH Broadcast Channels</td>
<td>FCCH Frequency correction</td>
<td></td>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SCH Synchronisation</td>
<td></td>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>BCCH Normal (114 data bits)</td>
<td></td>
<td>4</td>
<td>4 x 114 / 235.38 = 1.94 kbit/s</td>
<td></td>
</tr>
<tr>
<td>CCCH</td>
<td>RACH Random access</td>
<td></td>
<td>27 minimum</td>
<td>12 minimum</td>
<td>12 x 114 / 235.38 = 5.81 kbit/s</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>51 typical</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AGCH Normal (114 data bits)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>PCH</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DCCH Dedicated Control Channels</td>
<td>SDCCH TS0 - base channel (*)</td>
<td></td>
<td>4</td>
<td>4 x 114 / 120 = 3.8 kbit/s</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SACCH Same as SDCCH</td>
<td></td>
<td>2 (***)</td>
<td>2 x 114 / 120 = 1.9 kbit/s</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FACCH Same as TCH, (bits stolen from TCH)</td>
<td></td>
<td>1</td>
<td>1 x 114 / 120 = 0.95 kbit/s</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(*) Low capacity cells  
(**) High capacity cells  
(***) 4 bursts in 2 multiframes equivalent to 2 bursts/ multiframe

---

### Transmission / reception timing

- **Transmit / receive frame staggering**
  - to simplify hardware design, transmitter and receiver never operate at the same time
  - transmission is half-duplex
  - the numbering scheme is staggered by 3 time-slots

![Transmit / receive frame staggering diagram](image-url)
Transmission / reception timing

- Transmit time advance
  - Principle of operation
    - correct timing of uplink bursts at the BTS is required to avoid overlapping
    - different path delays (MS-BTS distances) must be compensated
    - transmission from the MS is advanced 0-63 bits under BTS control
    - maximum time advance of 63 bits allows 0.233 ms round trip delay
    - maximum cell radius is approximately 35 km
  - Initial ranging
    - Access Burst is transmitted without time advance
    - Guard Period of 68.25 bits allows for a path delay due to 37 km distance
    - BTS measures path delay and sends required time advance on SACCH
    - MS introduces time advance on all bursts
  - Adaptive control
    - BTS monitors burst and measures delays with specified time advance
    - if path delay varies more than 1 bit period, the new value is signalled on SACCH

Frequency hopping

- Application of frequency hoping
  - optional, but usually implemented
  - channels with no frequency hopping: BCH and CCCH

- Hoping sequence
  - several possible hoping algorithms
  - selected algorithm broadcast on BCCH

- Slow frequency hopping characteristics
  - in a given time-slot, successive TDMA frame are transmitted on different carriers
  - main hoping parameters
    - period: 4.615 ms
    - frequency: 217 hops/s
    - number of bits: 1250 bits/hop
Transmission power

- Mobile station power classes

<table>
<thead>
<tr>
<th>GSM 900</th>
<th>GSM 1800</th>
</tr>
</thead>
<tbody>
<tr>
<td>8 W</td>
<td>4 W</td>
</tr>
<tr>
<td>5 W</td>
<td>1 W</td>
</tr>
<tr>
<td>2 W</td>
<td>0.25 W</td>
</tr>
<tr>
<td>0.8 W</td>
<td>29 dBm</td>
</tr>
</tbody>
</table>

- Discontinuous transmission (DTX) for voice
  - no data transmission during periods of silence (approx. 60% of time)
    - Voice Activity Detector (VAD) algorithm suppresses TCH transmission
  - silent frames are sent to synthesise comfort noise at the receiver
  - several advantages
    - reduces interference, on average, by 3 dB
    - Increases MS battery life

Transmission power

- Power control
  - implemented on both links
  - objective: lowest power level which provides desired quality (BER)
  - procedure
    - MS measures power received and BER and sends result on SACCH
    - BTS sends new power level on SACCH, if and when necessary
  - control range

<table>
<thead>
<tr>
<th>GSM 900</th>
<th>GSM 1800</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 - 39 dBm</td>
<td>0 - 36 dBm</td>
<td>effective maxima depend on cell size and MS capability, control steps of 2 dB</td>
</tr>
</tbody>
</table>

- channels with no power control - use maximum power for the cell
  - downlink BCH and CCCH: power set by BTS
  - uplink RACH
    - BCCH broadcasts maximum power level for the cell
    - MS uses this value to set RACH transmission power
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
    - TMSI - Temporary Mobile Subscriber Identity
    - newly assigned at each new location update
    - encrypted transmission

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

---

### GSM - authentication

**AuC**

- RAND
- 128 bit
- SRES* = ? SRES
- 32 bit

**MSC**

- SRES
- 32 bit

**SIM**

- RAND
- 128 bit
- Ki
- 128 bit
- A3
- SRES
- 32 bit

*Ki*: individual subscriber authentication key

*SRES*: signed response

---

*secret*:
- A3 and A8 available via the Internet
- network providers can use stronger mechanisms
GSM - key generation and encryption

\[ \begin{align*}
\text{RAND} & \rightarrow K_i \rightarrow A8 \\
\text{Kc} & \rightarrow 64\text{ bit} \\
\text{data} & \rightarrow \text{encrypted data} \\
\text{A5} & \rightarrow \text{data}
\end{align*} \]

GSM protocol layers for signaling

\[ \begin{align*}
\text{CM} & \rightarrow \text{MM} \\
\text{RR} & \rightarrow \text{LAPD}_m \\
\text{radio} & \rightarrow 16/64\text{ kbit/s} \\
\text{BTS} & \rightarrow \text{BSC} \\
\text{BSSAP} & \rightarrow \text{SS7} \\
\text{MS} & \rightarrow \text{MSC} \\
\text{CM} & \rightarrow \text{MM} \\
\text{BSSAP} & \rightarrow \text{SS7} \\
\text{PCM} & \rightarrow 64\text{ kbit/s} / 2048\text{ kbit/s}
\end{align*} \]
GSM protocol layers for signaling

- **CM (Connection Management)**
  - call control, short message service and supplementary service
- **MM (Mobility Management)**
  - registration, authentication, location and handover management
- **RR (Radio Resource Management)**
  - setup, maintenance and release of radio channels
  - control of radio transmission quality
- **LAPDm (“Link Access Protocol D-channel” modified)**
  - modified version of ISDN LAPD protocol
- **BTSM (Base Transceiver Station Management)**
  - radio resources control messages between BSC and BTS
- **BSSAP (Base Station System Application Part)**
  - control of BSC by MSC

---

Mobile Terminated Call

1: calling a GSM subscriber
2: forwarding call to GMSC
3: signal call setup to HLR
4, 5: get routing info (MSRN) from VLR
6: forward routing info to GMSC
7: route call to current MSC
8, 9: get current status of MS (LAI + TMSI)
10, 11: paging of MS in location area
12, 13: MS answers paging and authentication request
14, 15: security checks
16, 17: set up connection
Mobile Terminated Call

Channel activity at radio interface

- **BTS**
  - **BCCH**: System parameters and other overhead
  - **PCH**: Paging message to specified TMSI
  - **AGCH**: Assign stand alone dedicated control channel
  - **SDCCH**: Authentication request
  - **SDCCH**: Request to transmit in cipher mode

- **MS**
  - **idle updated**
  - **announced TMSI matches stored value**
  - **calculate SRES / Kc**
  - **send SRES**
  - **switch to cipher mode**

Channel activity at radio interface (cont.)

- **BTS**
  - **SDCCH**: Setup message for incoming call
  - **SDCCH**: Assign traffic channel and release SDCCH
  - **FACCH**: Alerting mobile
  - **FACCH**: Connect acknowledge
  - **TCH**: data flow

- **MS**
  - **switch signaling to FACCH using assigned TCH**
  - **generate ringing sound**
  - **mobile off-hook**
  - **switch to traffic channel**
  - **FACCH**: Disconnect
  - **Release**
  - **idle updated**
Mobile Originated Call

1, 2: connection and authentication request
3, 4: security check
5-8: check resources (free circuit)
9-10: set up call

Channel activity at radio interface

- **BCCH**: System parameters and other overhead
- **RACH**: Channel request
- **AGCH**: Assign stand alone dedicated control channel
- **SDCCH**: Call establishment request
- **SDCCH**: Authentication request
- **SDCCH**: Authentication response
- **SDCCH**: Request to transmit in cipher mode
- **SDCCH**: Acknowledge cipher mode request
- **idle updated**: number dialed
- **send RAND**: calculate SRES / Kc
- **SRES confirmed**: send SRES
- **switch to cipher mode**: calculate SRES / Kc
Mobile Originated Call

Channel activity at radio interface

- Setup message for outgoing call on SDCCH
- Assign traffic channel and release SDCCH
- Acknowledge channel assignment
- Remote party ringing
- Alerting remote party
- Remote party off-hook
- Connect
- Switch to traffic channel
- Connect acknowledge
- Disconnect
- Release
- Release traffic channel
- Data flow from BTS to MS
- Mobile on-hook
- Idle updated

4 types of handover

1 - between different sectors of the same cell
2 - between different cells within the same BSC domain
3 - between different BSC domains within the same MSC domain
4 - between different MSC domains
Mobile-Assisted Handover (MAHO)

MS scans, measures and reports power received from several RF carrier based on BCCH information.
Location update

- MS is aware of location
  - BTS broadcasts Location Area Identification (LAI) on BCCH
  - SIM stores current LAI and TMSI

- Events which determine a current location update
  - MS is switched on and current LAI equals stored LAI
  - a timer set by the network expires and MS reports position
    - TMSI may be updated and stored in SIM

- Events which determine a new location update
  - MS is switched on and current LAI differs from stored LAI
  - MS enters a new location area
    - TMSI and LAI are updated and stored in SIM

[Diagram of location update process]
Location update

- Channel activity at radio interface

BTS

- **BCCH**: System parameters and other overhead
  - Channel request: RACH

MS

- **idle updated**

**successful access**

- **AGCH**: Assign stand alone dedicated control channel
  - Location updating request: SDCCH

**send RAND**

- **calculate SRES / Kc**
  - SDCCH: Authentication request
  - SDCCH: Authentication response

**SRES confirmed**

- **SDCCH**: Request to transmit in cipher mode
  - Acknowledge cipher mode request: SDCCH

**new TMSI sent (optional)**

- **SDCCH**: Location update confirmed
  - Acknowledge new location: SDCCH

- **SDCCH**: Release stand alone dedicated control channel
  - idle updated

**old LAI/TMSI sent**

- **calculate SRES / Kc**
  - send SRES
  - switch to cipher mode

- **store LAI/TMSI in SIM**

Mário Jorge Leitão

GSM