GSM (Global System for Mobile Communications) and Extensions

Mobile Communication and Mobile Computing
Prof. Dr. Alexander Schill
http://www.rn.inf.tu-dresden.de
GSM: Properties

• cellular radio network (2nd Generation)
• digital transmission, integrated data communication
• roaming (mobility between different network operators)

• good transmission quality (error detection and correction)
• scalable (large number of participants possible)
• security mechanisms (authentication, authorization, encryption)
• good resource use (frequency and time division multiplex)

• standard (ETSI, European Telecommunications Standards Institute)
GSM: Structure

- **AuC**: Authentication Center
- **BSS**: Base Station Subsystem
- **BSC**: Base Station Controller
- **BTS**: Base Transceiver Station
- **EIR**: Equipment Identity Register
- **HLR**: Home Location Register
- **OMC**: Operation and Maintenance Center
- **VLR**: Visitor Location Register
- **(G)MSC**: (Gateway) Mobile Switching Center
- **PSTN**: Public Switched Telephone Network
- **MS**: Mobile Station

**Fixed network**

**Switching Subsystems**

**Radio Subsystems**

- **Data networks**
- **PSTN**

- **Call Management**
- **Network Management**
GSM: Structure

- Operation and Maintenance Center (OMC)
  - logical, central structure with HLR, AuC und EIR
- Authentication Center (AuC)
  - authentication, storage of symmetrical keys, generation of encryption keys
- Equipment Identity Register (EIR)
  - storage of device attributes of allowed, faulty and blocked devices (white, gray, black list)
- Mobile Switching Center (MSC)
  - networking center, partially with gateways to other networks, assigned to one VLR each
- Base Station Subsystem (BSS): technical radio center
- Base Station Controller (BSC): control center
- Base Transceiver Station (BTS): radio tower / antenna
(1) Call from fixed network was switched via GMSC
(2) GMSC finds out HLR from phone number
(3) HLR checks whether participant is authorized for corresponding service and asks for MSRN at the responsible VLR
(4) MSRN will be returned to GMSC, can now contact responsible MSC
(5) GMSC transmits call to current MSC
(6) Ask for the state of the mobile station
(7) Information whether end terminal is active
(8) Call to all cells of the Location Area (LA)
(9) Answer from end terminal
(10 - 12) Security check and connection setup
(1) Connection request  
   (via random access channel, possible collision handling)
(2) Transfer by BSS
(3-4) Authorization control
(5) Switching of the call request to fixed network
Radio structure

- 1 TDMA-Slot
- 8 TDMA-channels in a total of 4,615 ms
- 124 radio frequency channels (carrier), each 200 kHz
- 2 frequency bands, each 25 MHz, divided into radio cells

- One or several frequency channels (carrier) per BSC
- Physical channels defined by frequency and time slot
GSM: channel structure

Traffic Channel
- Full-rate codec (13 kbit/s; differential encoding)
- Half-rate codec: more efficient speech encoding at 7 kbit/s (two phone calls per time slot can be encoded)

Paging Channel
- Signalize incoming calls (BSC to MS)

(Broadcast) Control Channel
- Allocation of identity, frequency order etc. (BSC to MS)
- Monitoring of BSCs for recognition of handover

Random Access Channel
- Control of channel entry with Aloha-procedure for collision handling between competing participants (MS to BSC)
Databases

**Home Location Register (HLR),** stores data of participants which are registered in an HLR-area

- **Semi-permanent data:**
  - Call number (Mobile Subscriber International ISDN Number) - MSISDN, e.g. +49/171/333 4444 (country, network, number)
  - Identity (International Mobile Subscriber Identity) - IMSI: MCC = Mobile Country Code (262 for .de) + MNC = Mobile Network Code (01-T-Mobile, 02-Vodafone, 03-eplus, 07-O2) + MSIN = Mobile Subscriber Identification Number
  - Personal data (name, address, mode of payment)
  - Service profile (call transfer, roaming-limits etc.)

- **Temporary data:**
  - MSRN (Mobile Subscriber Roaming Number) (country, network, MSC)
  - VLR-address, MSC-address
  - Authentication Sets of AuC (cryptographic key information)
  - Billing data
Databases

**Visitor Location Register (VLR)**
local database of each MSC with following data:

- IMSI, MSISDN
- Service profile
- Billing and accounting information
- TMSI (Temporary Mobile Subscriber Identity) - pseudonym for data security
- MSRN
- LAI (Location Area Identity)
- MSC-address, HLR-address
Location Area: Concept

advantage of the architecture: Location Update in case of limited mobility only at VLR, rarely at (perhaps very remote) HLR
Localization with GSM

- Participant call number in HLR
- Country code
- Network provider
- Internal area

- VLR 10
- VLR 9
- HLR 1

- IMSI
- LA 2
- 32311

- 0x62F220 01E5

- +49 (0)177-26 32311

- Participant call number in HLR
- Internal area
- Network provider
- Country code
Data transmission

- Each GSM-channel configurable as data channel
- Kinds of channels:
  - non-transparent (repeat of faulty data frames; very low error rate, but also very low throughput below 10 kbit/s)
  - transparent (only very simple forward error correction; slightly higher data rate; error rate $10^{-3}$ up to $10^{-4}$)
  - in practice, only faster extensions like GPRS, UMTS and LTE are used (explained later)
  - Speech channels have higher priority than data channels

- Short-Message-Service (SMS)
  - connectionless transmission (up to 160 Byte) on signaling channel

- Cell Broadcast (CB)
  - connectionless transmission (up to 80 Byte) on signaling channel to all participants in one cell or location area, e.g. for location based services
Data transmission - structure

- BTS
- BSC
- MSC
- IWF
- Modem
- Internet
- ISDN
- TA
- PSTN
- Modem

IWF - Inter Working Function
TA - Terminal Adapter
Security aspects:
Subscriber Identity Module (SIM)

- Chip-card (Smart Cart) to personalize a mobile subscriber (MS):
  - IMSI (International Mobile Subscriber Identity)
  - symmetric key $K_i$ of participant, stored also at AuC
  - algorithm “A3” for Challenge-Response-Authentication
  - algorithm “A8” for key generation of $K_c$ for content data
  - algorithm “A5” for encryption
  - PIN (Personal Identification Number) for access control

- Temporary data:
  - TMSI (Temporary Mobile Subscriber Identity) - pseudonym
  - LAI (Location Area Identification)
  - Encryption key $K_c$
Security aspects: Authentication

- Location Registration
- Location Update with VLR-change
- Call setup (in both directions)
- SMS (Short Message Service)
Security aspects: Session Key

- Key generation: Algorithm A8
  - Stored on SIM and in AuC
  - one way function parameterized with $K_i$
  - can be determined by network operator
  - Interfaces are standardized

$K_i$ → Authentication Request → RAND (128 Bit) → $K_c$
Security aspects: Encryption

Data encryption with algorithm A5:
- stored in the Mobile Station
- enhancement: A5/3 with improved security and 128 Bit key length
GSM-Security: assessment

- low key length $K_i$ with max. 128 Bit (could be hacked by using Brute Force Attack in less than an hour using a regular computers)

- key generation and -administration not controlled by the participants (symmetric: network operator knows all keys)

- cryptographic methods secret, so they were not „well examined“ (but A5/3 and other enhancements open now)

- no mutual authentication; attacker can pretend a GSM-Net

- no end-to-end encryption or end-to-end authentication
HSCSD: High Speed Circuit Switched Data

- GSM extension for higher data rates
- parallel usage of several time slots (TS) of one frequency on \( U_m \) (air interface)
- channel bundling with asymmetric transmission (1 TS Uplink / 3 TS or 4 TS Downlink)
- Data rates up to \( 4 \times 14.4 \text{ kbit/s} = 57.6 \text{ kbit/s} \) (theoretically 8 time slots, but limited bundling in practice)
HSCSD: structure

n time slots of each TDMA frame (theoretically max. 8)

IWF - Inter Working Function
TA - Terminal Adapter
HSCSD: changes

n time slots of each TDMA frame (theoretically max. 8)

BTS | BSC | MSC

Um | Abis | A

multiplex of the time slots on each 64 kBit/s channel

certain changes are necessary at the component
several changes of the software/firmware
minimal changes of the software/firmware
HSCSD radio interface

- parallel usage of several time slots limited to one frequency, in half-duplex mode due to technical limitations of the end devices
- Cost factor limits number of used TS to (2+2) or (1+3, uplink, downlink); (1+4) with improved timing

| MS RECEIVE | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| MS TRANSMIT | 5 | 6 | 7 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 0 | 1 | 2 | 3 | 4 |
| MS MONITOR |

Required time for setting to receiving mode
Required time for setting to transmission mode
Required time for signal strength measure and setting to receiving mode
Assessment of HSCSD

+ existing network structure and accounting model maintained; only small changes were necessary
+ HSCSD is still circuit switched
  + has defined QoS-settings (data rate, delay)
    – one logical channel will be established on all interfaces for the time of the connection (inefficient)
    – badly suited for burst-like traffic (Internet) or Flat Rate billing (Logistics)
    – Only limited international acceptance (Roaming!)
  • also uses more resources on the radio interface
    – problems with handover into a new cell
GPRS: General Packet Radio Service

- GSM extension based on packet switching service (end-to-end) and channel bundling based on multiple time slots
- Data rates up to 171.2 kbit/s (theoretical) – in practice however similar to HSCSD
- Effective and flexible administration of the radio interface; adaptive channel encoding
- Internetworking with IP networks standardized
- Dynamic sharing of resources with „classical“ GSM speech services
- Advantage: Billing and Accounting according to data volume
GPRS: Structure

GPRS Backbone
Frame Relay / ATM

SGSN - Serving GPRS Support Node
GGSN - Gateway GPRS Support Node

- Signalization data
- User data

Internet

GPRS Nets
other operators

BTS
BSC
MSC
HLR

other packet switching networks

GSM

GGSN

Border Gateway

SGSN

GGSN
GPRS: Changes

n time slots (TS) per TDMA frame (theoretically max. 8) per packet!

Circuit switched traffic

Packet switched traffic

modified network components

new components or extensively modified components

Existing components
Tasks: SGSN, GGSN

SGSN:
- packet delivery
- mobility management
- session management
- QoS
- Security
- Billing

GGSN:
- Routing and Signalization
- Mapping to PDP (Packet Data Protocol)
- Address conversion (IP to GSM)
- Resource management

External Data Domain

Internet

Intranet

Client

Server
Quality of Service

- QoS profile agrees service parameters inside the whole network for the duration of PDP (Packet Data Protocol) context (session):
  - temporary address (IP) for mobile station
  - tunneling information, among others GGSN, which is used for access to corresponding packet switched network
  - type of the connection
  - QoS profile

- QoS profile commits:
  - precedence class, priority against other services (high, normal, low)
  - packet delay class, times valid for traffic inside the GPRS network
  - reliability class
  - peak throughput class
  - mean throughput class
### Quality of Service: Examples

**Packet delay classes**

<table>
<thead>
<tr>
<th>Class</th>
<th>Size: 128 octets</th>
<th>Size: 1024 octets</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Mean Delay</td>
<td>95% Delay</td>
</tr>
<tr>
<td>1 (predictive)</td>
<td>&lt; 0,5 s</td>
<td>&lt; 1,5 s</td>
</tr>
<tr>
<td>2 (predictive)</td>
<td>&lt; 5 s</td>
<td>&lt; 25 s</td>
</tr>
<tr>
<td>3 (predictive)</td>
<td>&lt; 50 s</td>
<td>&lt; 250 s</td>
</tr>
<tr>
<td>4 (best effort)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Error classes**

<table>
<thead>
<tr>
<th>Class</th>
<th>Probability for</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10⁻⁹</td>
</tr>
<tr>
<td>2</td>
<td>10⁻⁴</td>
</tr>
<tr>
<td>3</td>
<td>10⁻²</td>
</tr>
</tbody>
</table>

**GPRS data rates**

<table>
<thead>
<tr>
<th>Coding</th>
<th># of timeslots</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheme</td>
<td>1</td>
</tr>
<tr>
<td>CS-1</td>
<td>9,05</td>
</tr>
<tr>
<td>CS-2</td>
<td>13,4</td>
</tr>
<tr>
<td>CS-3</td>
<td>15,6</td>
</tr>
<tr>
<td>CS-4</td>
<td>21,4</td>
</tr>
</tbody>
</table>

(only CS-1 and CS-2 comprise reasonable error correction and are relevant in practice)
Assessment of GPRS

+ Data rates increased due to channel bundling
+ Better resource management by packet switched service

- Quality of service (QoS) difficult to handle
- Still rather low data rates, therefore most operators migrated to UMTS and LTE where possible, e.g. in urban areas
Some further readings

- ETSI standards (GSM etc.) in general: www.etsi.org
- GSM, HSCSD, GPRS: good overviews on www.wikipedia.org