GSM
Global System for Mobile communication

GPRS
General Packet Radio Service
Examples of digital wireless systems
(all originally specified by ETSI)

GSM (Global System for Mobile communication) is a cellular mobile system
• cellular concept
• high mobility (international roaming)

TETRA (TErrestrial Trunked RAdio) is an example of a Professional/Privat Mobile Radio (PMR) system
• limited access (mainly for professional usage)
• limited mobility (but other advanced features)

DECT (Digital Enhanced Cordless Telecommunications) is a cordless system
• low mobility (only within “isolated islands”)

Digital PLMN systems (status 2004)
(PLMN = Public Land Mobile Network)

2nd Generation (2G)
- GSM
- IS-136
- IS-95
- GPRS
- EDGE
- Packet services
- More radio capacity

3rd Generation (3G)
- IMT-2000
- UMTS:
  - UTRA FDD
  - UTRA TDD
- USA

4G
- CDMA 2000
Duplexing
(separation of uplink/downlink transmission directions)

FDD (Frequency Division Duplexing)
(GSM/GPRS, TETRA, UTRA FDD)

TDD (Time Division Duplexing)
(DECT, UTRA TDD)
FDD vs. TDD

FDD

- Duplex filter is large and expensive
- Different fading in UL/DL
- Same UL/DL bandwidth

TDD

- Large MS-BS separation => inefficient
- Same fading in UL/DL => effect on power control
- Flexible UL/DL bandwidth allocation
- asymmetric services
- => indoor
The GSM network contains a large number of cells with a base station (BS) at the center of each cell to which mobile stations (MS) are connected during a call. If a connected MS (MS in call phase) moves between two cells, the call is not dropped. Instead, the network performs a handover (US: hand-off).
GSM => mobility concept

The GSM network is divided into location areas (LA), each containing a certain number of cells.

As long as an idle MS (idle = switched on) moves within a location area, it can be reached through paging.

If an idle MS moves between two location areas, it cannot be reached before it performs a location update.
Original GSM system architecture
GSM: circuit switched connections

BSS

MS

ME

SIM

BTS

BSC

TRAU

NSS

MSC

VLR

GMSC

HLR

AuC

EIR

PSTN

Circuit switched connection

Signaling

Database
GPRS: packet switched connections

BSS
- TE
- ME
- SIM
- MS
- BTS
- BSC
- PCU

NSS
- MSC
- VLR
- SGSN
- HLR
- AuC
- EIR
- GMSC
- GGSN

Packet switched connection
- Signaling
- Database

Internet
Upgrading from GSM to GSM/GPRS

- New MS/terminals
- Packet Control Unit (PCU)
- SGSN and GGSN routers
- software updates (BTS, HLR)
Purpose of TRAU
(TRAU = Transcoding and Rate Adaptation Unit)

BSS

BSC for signalling only

BTS

TRAU

NSS

MSC

VLR

Conventional 64 kbit/s PCM signal

13 kbit/s encoded speech is packed into 16 kbit/s frame
Radio interface - multiple access techniques

- Frequency division
- Time division
- Code division
- Code nr.
Physical channel = repetitive time slot

Carrier 0

Physical channel = time slot

Typically used for signaling

Carrier 1

Carrier 2

Carrier 3

Frame of length 8 time slots

Time Slot
GSM logical channels

Traffic channels
- TCH/F
- TCH/H
- bidirectional
downlink uplink

Control channels (for signaling)
- Broadcast
- Common control
- Dedicated
  - SCH
  - FCCH
  - BCCH
  - PCH
  - AGCH
  - SDCCH
  - SACCH
  - FACCH
  - RACH

bidirectional
downlink uplink
GSM burst structure

GSM normal burst: 156.25 bits (0.577 ms)

TDMA frame (4.615 ms):

= 26 TDMA frames (in case of TCH)

traffic or signaling info in burst?

TDMA multiframe:

SACCH

Idle

23 24 25 26
GSM speech encoding

Voice coding: 260 bits in 20 ms blocks (13 kbit/s)  MS - TRAU

| 260 bits | 260 bits |

Channel coding: 456 coded bits (22.8 kbit/s)  MS - BTS

| 456 bits |

Interleaving: 8 x 57 bits (22.8 kbit/s)

| 57 bits | 57 bits | 57 bits |

bits 4, 12, 20, 28, 36, 44, etc. from the 456 bit frame
GSM signaling message encoding

Signaling message is segmented into blocks of 184 bits:

- 184 bits

Each block is coded into 456 bits (22.8 kbit/s)

- 456 bits

Interleaving: 8 x 57 bits (22.8 kbit/s)

- 57 bits
- 57 bits
- 57 bits
- 57 bits

bits 4, 12, 20, 28, 36, 44, etc. from the 456 bit frame
Purpose of interleaving

**Transmitter**

Bits are interleaved ... 

... and will be de-interleaved in the receiver

**Channel**

Fading affects many adjacent bits

Bit errors in the receiver

**Receiver**

After de-interleaving of bits, bit errors are spread

(better error correction)
Task Management in GSM/GPRS

**Radio Resource Management (RM)**

1. Random access and channel reservation
2. Handover management
3. Ciphering (encryption) over radio interface

**Mobility Management (MM)**

4. IMSI/GPRS Attach (switch on) and Detach (switch off)
5. Location updating (MS moves to other Location/Routing Area)
6. Authentication

**Call Control (CC) in GSM**

- MOC, MTC

**Session Management (SM) in GPRS**

- PDP Context

Number refers to the remaining slides
Who is involved in what?

- MS
- BTS
- BSC
- MSC/VLR
- SGSN

Relations:
- RR
- MM
- CM / SM
Random access in GSM/GPRS (1)

Communication between MS and network is not possible before going through a procedure called *random access*.

Random access must consequently be used in

- **network originated activity**
  - paging, e.g. for a mobile terminated call in GSM

- **MS originated activity**
  - IMSI attach, IMSI detach
  - GPRS attach, GPRS detach
  - location updating in GSM or GPRS
  - mobile originated call in GSM
  - SMS (short message service) message transfer
Random access in GSM/GPRS (2)

1. MS sends a short access burst over the Random Access Channel (RACH) in uplink using Slotted Aloha (in case of collision => retransmission after random time)

2. After detecting the access burst, the network (BSC) returns an "immediate assignment" message which includes the following information:
   - allocated physical channel (frequency, time slot) in which the assigned signalling channel is located
   - timing advance (for correct time slot alignment)

3. The MS now sends a message on the dedicated signalling channel assigned by the network, indicating the reason for performing random access.
Four security measures in GSM

1) PIN code (authentication of user using terminal => local security measure, network is not involved)
2) SIM authentication (performed by network)
3) Ciphering of information sent over air interface
4) Usage of TMSI (instead of IMSI) over air interface

**IMSI** = International Mobile Subscriber Identity (globally unique identity)

**TMSI** = Temporary Mobile Subscriber Identity (local and temporary identity)
2 Basic principle of user authentication

SIM (in terminal) → Air Interface

Challenge ← RAND

algorithm → Response

algorithm

Authentication key

The same? If yes, authentication is successful

Network

Random number

Ki

Ki

2Ki
For each call, a new ciphering key (Kc) is generated during authentication both in MS and MSC (in same way as authentication “response”).
Three security algorithms in GSM
(in UMTS many more ...)

Mobile Station (MS)

Ki
A3
A8
Kc
A5
Data

Network

RAND (from network)
SRES (to network)
Time info (from network)
Ciphered data
Three security algorithms in GSM at the network side...

Radio network

Authentication Center (AuC)

- RAND
- SRES
- Kc

A5

Ciphering in BTS

A3

A8

Ki

SRES

Authentication vector
Algorithm considerations

Using output and one or more inputs, it is in practice not possible to calculate “backwards” other input(s) “brute force approach”, “extensive search”

Key length in bits \((N)\) is important (in case of brute force approach \(2^N\) calculation attempts may be needed)

Strength of algorithm is that it is secret \(\Rightarrow\) bad idea! “security through obscurity”

Better: open algorithm can be tested by engineering community (security through strong algorithm)
Usage of TMSI in GSM

- Random access
- Authentication
- Start ciphering
- CM or MM transaction
- IMSI detach

New TMSI stored in SIM

New TMSI allocated by network

IMSI is never sent over air interface if not absolutely necessary!
## Connectivity states in GSM/GPRS

### GSM
- **Disconnected**: MS is switched off (circuit mode)
- **Idle**: location updates on LA basis
- **Connected**: handovers, not location updates

### GPRS
- **Idle**: MS is switched off (packet mode)
- **Standby**: location updates on RA basis
- **Ready**: location updates on cell basis
GPRS connectivity state model

- **Idle**
  - GPRS attach
  - GPRS detach
  - Standby timer expired

- **Ready**
  - Timer expired
  - Transmission of packet
  - Location update when MS changes cell

- **Standby**
  - No location management, MS not reachable
  - Location update when MS changes routing area
MM “areas” in GSM/GPRS

Cell

Location Area (LA)

Routing Area (RA)

Location updating in GPRS (ready state)

Location updating in GPRS (standby state)

Location updating in GSM
4 Trade-off when choosing LA/RA size

If LA/RA size is very large (e.g. whole mobile network)

+ location updates not needed very often
  – paging load is very heavy

If LA/RA size is very small (e.g. single cell)

+ small paging load
  – location updates must be done very often

Affects capacity

Affects signalling load
Most recently allocated TMSI and last visited LAI (Location Area ID) are stored in SIM even after switch-off.

After switch-on, MS monitors LAI. If stored and monitored LAI values are the same, no location updating is needed.
Different LAI values => location update required!
SIM sends old LAI and TMSI to VLR 2.
VLR 2 does not recognize TMSI since there is no TMSI-IMSI context. Who is this user?
However, VLR 2 can contact VLR 1 (address: LAI 1) and request IMSI.

IMSI is sent to VLR 2.
**Important:** HLR must be updated (new LAI). If this is not done, incoming calls can not be routed to new MSC/VLR. HLR also requests VLR 1 to remove old user data.
VLR 2 generates new TMSI and sends this to user. User stores new LAI and TMSI safely in SIM.

Location update successful!
GSM identifiers (1)

**Globally unique**

- **IMSI** = GSM “internal information”
  - MCC = Mobile Country Code (3 digits)
  - MNC = Mobile Network Code (2 digits)
  - MSIN = Mobile Subscriber Identity Number (≤10 digits)

- **LAI** = LAI + CI
  - MCC = Mobile Country Code (3 digits)
  - MNC = Mobile Network Code (2 digits)
  - LAC = Location Area Code (≤10 digits)
  - CI = Cell Identity
GSM identifiers (2)

**MSISDN**

- **Globally unique**
- For routing to GMSC
- E.164 numbering format
- CC = Country Code (1-3 digits)
- NDC = National Destination Code (1-3 digits)
- SN = Subscriber Number

**MRSN**

- **Temporary allocation**
- For routing to MSC/VLR
- Temporary subscriber ID
- E.164 numbering format
- CC = Country Code (1-3 digits)
- NDC = National Destination Code (1-3 digits)
- TN = Temporary Number
Case study: GSM MTC (1)

MTC = mobile terminated call

Circuit switched connection
(64 kb/s PCM, 16 kb/s between TRAU and BTS, 13 kb/s encoded speech over air interface)

Signaling (ISUP, MAP)
GSM mobile terminated call (2)

Call is routed to GMSC using MSISDN number of called user (e.g. 040 1234567).

MSISDN number in fact points to database in HLR.

HLR is contacted. Under which MSC/VLR is user?
HLR knows location of Serving MSC/VLR (when user moves to another VLR, this is always recorded in HLR).

HLR requests MSRN (roaming number) from VLR.

MSRN is forwarded to GMSC.
Call can now be routed to Serving MSC/VLR using ISUP (may involve several intermediate switching centers).

MSC/VLR starts paging within Location Area (LA) in which user is located, using TMSI for identification.
Only the mobile user with the corresponding TMSI responds to the paging.

Using random access procedure, user requests a channel, e.g. SDCCH, for call control signaling.
Signaling channel is set up. After authentication and ciphering procedures, call control signaling continues.

Finally, a **GSM traffic channel** is set up over the radio interface. The circuit switched connection is now ready.
GPRS attach / PDP session

**GPRS attach**
Separate or combined GSM/GPRS attach
MS registers with an SGSN (authentication...)
Location updates possible

**PDP context is created**
MS is assigned PDP (IP) address
Packet transmission can take place

**GPRS detach**
PDP context terminated
Allocated IP address released

In case of dynamic address allocation
DHCP (Dynamic Host Configuration Protocol)
PDP context describes characteristics of GPRS session (session = “always on” connection)

PDP context information is stored in MS, SGSN and GGSN

One user may have several PDP context sessions active

- **PDP type**: (e.g. IPv4)
- **PDP address**: = IP address of MS (e.g. 123.12.223.9)
- **Requested QoS**: (priority, delay ...)
- **Access Point Name**: = IP address of GGSN (e.g. 123.12.223.0)
PDP context activation

Activate PDP context request

Security functions

Create PDP context request

IP address allocated to MS

Create PDP context response

Activate PDP context accept
Dynamic IP address allocation has one problem: it is difficult to handle a mobile terminated transaction (external source does not know IP address of MS).

Fortunately, packet services are usually of client-server type

$\Rightarrow$ MS initiates packet transmission
Packet transmission (2)

Packet is sent to SGSN. SGSN sends packet to GGSN through GTP (GPRS Tunneling Protocol) tunnel.

Tunneling = encapsulation of IP packet in GTP packet

<table>
<thead>
<tr>
<th>IP address ...</th>
<th>IP address</th>
<th>IP payload</th>
</tr>
</thead>
</table>

... = APN of GGSN, used for routing through tunnel
GGSN sends packet through external IP network (i.e. Internet) to the server.

<table>
<thead>
<tr>
<th>Source IP addr.</th>
<th>Dest. IP addr.</th>
<th>IP payload</th>
</tr>
</thead>
<tbody>
<tr>
<td>GGSN</td>
<td>Server</td>
<td></td>
</tr>
</tbody>
</table>
Packet transmission (4)

Server sends return packet via GGSN, GTP tunnel and SGSN to MS.

Packets from server to MS are always routed via GGSN (since this node has PDP context information).
Further information on GSM/GPRS

Books:
Many good books available (GSM)
GPRS is more problematic ...

Web link (GPRS basics):
www.comsoc.org/livepubs/surveys/public/3q99issue/bettstetter.html