Wireless Telecommunication Systems

- Market
- GSM
- DECT
- TETRA
- UMTS/IMT-2000

Mobile phone subscribers worldwide

- Approx. 1.7 bn
- 2008: >3.5 bn!

Source: ITU World Telecommunication/ICT Indicators Database

August 1997: the number of worldwide mobile subscribers surpassed 100 million.
Some statistics...

- 16th April 2008: The GSMA, the global trade group for the mobile industry, today announced that total connections to GSM mobile communications networks have now passed the 3 billion mark globally.

  - The third billion landmark has been reached just four years after the GSM industry surpassed its first billion, and just two years from the second billionth connection. The 3 Billion landmark has been reached just 17 years after the first GSM network launch in 1991. Today more than 700 mobile operators across all continents of the world are adding new connections at the rate of 15 per second, or 1.3 million per day.

- The world’s biggest GSM markets today are China (509 million), which is growing at a rate of more than 7 million new connections a month and accounts for 14% of the third billion growth; India (193 million), growing at 6 million per month accounts for 12% of the third billion growth; Russia (178 million) and Brazil (93 million) which both contributed 4% of the third billion growth.

How does it work?

- How can the system locate a user?
- Why don’t all phones ring at the same time?
- What happens if two users talk simultaneously?
- Why don’t I get the bill from my neighbor?
- Why can an Australian use her phone in Berlin?

- Why can’t I simply overhear the neighbor’s communication?
- How secure is the mobile phone system?
- What are the key components of the mobile phone network?
GSM: Overview

- GSM
  - formerly: Groupe Spéciale Mobile (founded 1982)
  - now: Global System for Mobile Communication
  - Pan-European standard (ETSI, European Telecommunications Standardization Institute)
  - simultaneous introduction of essential services in three phases (1991, 1994, 1996) by the European telecommunication administrations
    - seamless roaming within Europe possible
- Today many providers all over the world use GSM
  - (218 countries in Asia, Africa, Europe, Australia, America)
  - more than 3 billion subscribers in more than 700 networks
  - more than 75% of all digital mobile phones use GSM
  - over 550 billion SMS year worldwide (> 10% of the revenues for many operators)
    - [be aware: these are only rough numbers...]

Performance characteristics of GSM (wrt. analog sys.)

- 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

GSM: Mobile Services

- GSM offers
  - several types of connections
    - voice connections, data connections, short message service
  - multi-service options (combination of basic services)
- Three service domains
  - Bearer Services
  - Telematic Services
  - Supplementary Services
### Bearer Services
- Telecommunication services to transfer data between access points
- Specification of services up to the terminal interface (OSI layers 1-3)
- Different data rates for voice and data (original standard)
  - Data service (circuit switched)
    - Synchronous: 2.4, 4.8 or 9.6 kbit/s
    - Asynchronous: 360 - 1200 bps
  - Data service (packet switched)
    - Synchronous: 2.4, 4.8 or 9.6 kbit/s
    - Asynchronous: 360 - 9600 bps
- Today: data rates of approx. 50 kbit/s possible

### Tele Services I
- Telecommunication services that enable voice communication via mobile phones
- All these basic services have to obey cellular functions, security measurements etc.
- Offered services
  - Mobile telephony
    - Primary goal of GSM was to enable mobile telephony offering the traditional bandwidth of 3.1 kHz
  - Emergency number
    - Common number throughout Europe (112); mandatory for all service providers; free of charge; connection with the highest priority (preemption of other connections possible)

### Tele Services II
- Additional services
  - Non-Voice-Teleservices
    - Group 3 fax
    - Voice mailbox (implemented in the fixed network supporting the mobile terminals)
    - Electronic mail (MHS, Message Handling System, implemented in the fixed network)
    - Short Message Service (SMS)
      - alphanumeric data transmission to/from the mobile terminal (160 characters) using the signaling channel, thus allowing simultaneous use of basic services and SMS (almost ignored in the beginning now the most successful add-on!)
**Supplementary services**

- Services in addition to the basic services, cannot be offered stand-alone
- May differ between different service providers, countries and protocol versions
- Important services
  - identification: forwarding of caller number
  - suppression of number forwarding
  - automatic call-back
  - conferencing with up to 7 participants
  - locking of the mobile terminal (incoming or outgoing calls)
  - ...

**Architecture of the GSM system**

- GSM is a PLMN (Public Land Mobile Network)
  - several providers setup mobile networks following the GSM standard within each country
  - components
    - MS (mobile station)
    - BS (base station)
    - MSC (mobile switching center)
    - LR (location register)
  - subsystems
    - RSS (radio subsystem): covers all radio aspects
    - NSS (network and switching subsystem): call forwarding, handover, switching
    - OSS (operation subsystem): management of the network

**Ingredients 1: Mobile Phones, PDAs & Co.**

The visible but smallest part of the network!
Ingredients 2: Antennas

Still visible – cause many discussions...

Ingredients 3: Infrastructure 1

Base Stations
Cabling
Microwave links

Ingredients 3: Infrastructure 2

Not „visible”, but comprise the major part of the network (also from an investment point of view…)

Switching units
Management
Data bases
Monitoring
**System architecture: radio subsystem**

- **Components**
  - MS (Mobile Station)
  - BSS (Base Station Subsystem): consisting of
    - BTS (Base Transceiver Station): sender and receiver
    - BSC (Base Station Controller): controlling several transceivers
- **Interfaces**
  - \( U_m \): radio interface
  - \( A_{bis} \): standardized, open interface with 16 kbit/s user channels
  - \( A \): standardized, open interface with 64 kbit/s user channels

**System architecture: network and switching subsystem**

- **Components**
  - MSC (Mobile Services Switching Center)
  - IWF (Interworking Functions)
  - ISDN (Integrated Services Digital Network)
  - PSTN (Public Switched Telephone Network)
  - PSPDN (Packet Switched Public Data Net.)
  - CSPDN (Circuit Switched Public Data Net.)
- **Databases**
  - HLR (Home Location Register)
  - VLR (Visitor Location Register)
  - EIR (Equipment Identity Register)

**Radio subsystem**

- **The Radio Subsystem (RSS) comprises the cellular mobile network up to the switching centers**
- **Components**
  - Base Station Subsystem (BSS): radio components including sender, receiver, antenna - if directed antennas are used one BTS can cover several cells
  - Base Station Controller (BSC): switching between BTSs, controlling BTSs, managing of network resources, mapping of radio channels (\( U_m \)) onto terrestrial channels (A interface)
- **BSS = BSC + sum(BTS) + interconnection**
- **Mobile Stations (MS)**
The GSM (Global System for Mobile Communications) is a digital cellular network standard used in the European Union and worldwide. It operates on segmented area into cells, using several carrier frequencies. The frequency bands vary depending on geography, user density, and transceiver power. The idealized hexagonal shape of cells is not always achievable due to geographical constraints.

### GSM frequency bands (examples)

<table>
<thead>
<tr>
<th>Type</th>
<th>Channels</th>
<th>Uplink [MHz]</th>
<th>Downlink [MHz]</th>
</tr>
</thead>
<tbody>
<tr>
<td>GSM 850</td>
<td>128-251</td>
<td>824-849</td>
<td>869-894</td>
</tr>
<tr>
<td>GSM 900</td>
<td>0-124, 955-1023</td>
<td>876-915</td>
<td>921-960</td>
</tr>
<tr>
<td>GSM 900</td>
<td>124 channels +49 channels</td>
<td>890-915</td>
<td>935-960</td>
</tr>
<tr>
<td>GSM 1800</td>
<td>512-885</td>
<td>1710-1785</td>
<td>1805-1880</td>
</tr>
<tr>
<td>GSM 1900</td>
<td>512-810</td>
<td>1850-1910</td>
<td>1930-1990</td>
</tr>
<tr>
<td>GSM-R exclusive</td>
<td>955-1024, 0-124</td>
<td>876-915</td>
<td>921-960</td>
</tr>
<tr>
<td>GSM-R exclusive</td>
<td>69 channels</td>
<td>876-880</td>
<td>921-925</td>
</tr>
</tbody>
</table>

- GSM 400 (also named GSM 450 or GSM 480 at 450-458/460-480 MHz)
- Please note: frequency ranges may vary depending on the country!
- Channels at the lower/upper edge of a frequency band are typically not used.

### Example coverage of GSM networks

- **AT&T (GSM-850/1900)**: USA
- **T-Mobile (GSM-900/1800)**: Germany
- **Vodafone (GSM-900)**: South Africa
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

<table>
<thead>
<tr>
<th>Functions</th>
<th>BTS</th>
<th>BSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management of radio channels</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Frequencyjnoss (FR)</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Management of terminal group</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Mapping of terminal into radio channels</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Control coding and decoding</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Base adaptation</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Encryption and decryption</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Radio</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Control signal measurement</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Traffic measurement</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Authentication</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Location update, location update</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Handover management</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

Mobile station

- Terminal for the use of GSM services
- A mobile station (MS) comprises several functional groups
  - MT (Mobile Terminal):
    - offers common functions used by all services the MS offers
    - end-point of the radio interface (Um)
  - TA (Terminal Adapter):
    - terminal adaptation, hides radio specific characteristics
  - TE (Terminal Equipment):
    - peripheral device of the MS, offers services to a user
    - does not contain GSM specific functions
  - SIM (Subscriber Identity Module):
    - personalization of the mobile terminal, stores user parameters

Network and switching subsystem

- NSS is the main component of the public mobile network GSM
  - switching, mobility management, interconnection to other networks, system control
- Components
  - Mobile Services Switching Center (MSC)
    - controls all connections via a separated network to/from a mobile terminal within the domain of the MSC - several BSC can belong to a MSC
  - Databases (important: scalability, high capacity, low delay)
    - Home Location Register (HLR)
      - central master database containing user data, permanent and semi-permanent data of all subscribers assigned to the HLR (one provider can have several HLRs)
    - Visitor Location Register (VLR)
      - local database for a subset of user data, including data about all user currently in the domain of the VLR
Mobile Services 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

- Functions of a MSC
  - specific functions for paging and call forwarding
  - termination of SS7 (signaling system no. 7)
  - mobility specific signaling
  - location registration and forwarding of location information
  - provision of new services (fax, data calls)
  - support of short message service (SMS)
  - generation and forwarding of accounting and billing information

Operation subsystem

- The OSS (Operation Subsystem) enables centralized operation, management, and maintenance of all GSM subsystems

- Components
  - Authentication Center (AUC)
    - generates user specific authentication parameters on request of a VLR
    - authentication parameters used for authentication of mobile terminals and encryption of user data on the air interface within the GSM system
  - Equipment Identity Register (EIR)
    - registers GSM mobile stations and user rights
    - stolen or malfunctioning mobile stations can be locked and sometimes even localized
  - Operation and Maintenance Center (OMC)
    - different control capabilities for the radio subsystem and the network subsystem

GSM - TDMA/FDMA

- 1935-960 MHz
- 124 channels (200 kHz)
- downlink
- 890-915 MHz
- 124 channels (200 kHz)
- uplink

- GSM TDMA frame
- GSM time-slot (normal burst)
- 4.615 ms
- 57 bits
- 26 bits
- 11 bits
GSM hierarchy of frames

- **Hyperframe**: 3 h 28 min 53.76 s
- **Superframe**: 6.12 s
- **Multiframe**: 120 ms
- **Frame**: 4.615 ms
- **Slot**: 577 µs

GSM protocol layers for signaling

- **MS**
  - U_{um}
  - RRI
  - LAPDm
  - radio

- **BTS**
  - A_{um}
  - BSSAP

- **BSC**
  - A
  - PSTN
  - SS7
  - PCM

- **MSC**
  - CM
  - GEM
  - BSSAP
  - SS7

Mobile Terminated Call

1: calling a GSM subscriber
2: forwarding call to GMSC
3: signal call setup to HLR
4, 5: request MSRN from VLR
6: forward responsible MSC to GMSC
7: forward call to current MSC
8, 9: get current status of MS
10, 11: paging of MS
12, 13: MS answers
14, 15: security checks
16, 17: set up connection
Mobile Originated Call
- 1, 2: connection request
- 3, 4: security check
- 5-8: check resources (free circuit)
- 9-10: set up call

MTC/MOC

4 types of handover
Handover decision

Handover procedure

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
  - temporary identity TMSI (Temporary Mobile Subscriber Identity)
  - newly assigned at each new location update (LUP)
  - encrypted transmission

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

**Key Generation and Encryption**

Data services in GSM I

- Data transmission standardized with only 9.6 kbit/s
  - Advanced coding allows 14.4 kbit/s
  - Not enough for Internet and multimedia applications
- HSCSD (High-Speed Circuit Switched Data)
  - Mainly software update
  - Bundling of several time-slots to get higher AIUR (Air Interface User Rate, e.g., 57.6 kbit/s using 4 slots @ 14.4)
  - Advantage: Ready to use, constant quality, simple
  - Disadvantage: Channels blocked for voice transmission
Data services in GSM II

- **GPRS (General Packet Radio Service)**
  - packet switching
  - using free slots only if data packets ready to send (e.g., 50 kbit/s using 4 slots temporarily)
  - standardization 1998, introduction 2001
  - advantage: one step towards UMTS, more flexible
  - disadvantage: more investment needed (new hardware)

- **GPRS network elements**
  - **GSN (GPRS Support Nodes): GGSN and SGSN**
  - **GGSN (Gateway GSN)**
    - interworking unit between GPRS and PDN (Packet Data Network)
  - **SGSN (Serving GSN)**
    - supports the MS (location, billing, security)
  - **GR (GPRS Register)**
    - user addresses

---

GPRS quality of service

<table>
<thead>
<tr>
<th>Reliability class</th>
<th>Lost SDU probability</th>
<th>Duplicate SDU probability</th>
<th>Out of sequence SDU probability</th>
<th>Corrupt SDU probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$10^{-4}$</td>
<td>$10^{-4}$</td>
<td>$10^{-4}$</td>
<td>$10^{-4}$</td>
</tr>
<tr>
<td>2</td>
<td>$10^{-4}$</td>
<td>$10^{-4}$</td>
<td>$10^{-4}$</td>
<td>$10^{-4}$</td>
</tr>
<tr>
<td>3</td>
<td>$10^{-4}$</td>
<td>$10^{-4}$</td>
<td>$10^{-4}$</td>
<td>$10^{-4}$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Delay class</th>
<th>SDU size 128 byte</th>
<th>SDU size 1024 byte</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>mean</td>
<td>95 percentile</td>
</tr>
<tr>
<td>1</td>
<td>&lt; 0.5 s</td>
<td>&lt; 1.5 s</td>
</tr>
<tr>
<td>2</td>
<td>&lt; 5 s</td>
<td>&lt; 25 s</td>
</tr>
<tr>
<td>3</td>
<td>&lt; 50 s</td>
<td>&lt; 250 s</td>
</tr>
</tbody>
</table>

Examples for GPRS device classes

<table>
<thead>
<tr>
<th>Class</th>
<th>Receiving slots</th>
<th>Sending slots</th>
<th>Maximum number of slots</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>2</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>8</td>
<td>4</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>10</td>
<td>4</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>12</td>
<td>4</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>
GPRS user data rates in kbit/s

<table>
<thead>
<tr>
<th>Coding scheme</th>
<th>1 slot</th>
<th>2 slots</th>
<th>3 slots</th>
<th>4 slots</th>
<th>5 slots</th>
<th>6 slots</th>
<th>7 slots</th>
<th>8 slots</th>
</tr>
</thead>
<tbody>
<tr>
<td>CS-1</td>
<td>9.65</td>
<td>18.1</td>
<td>27.15</td>
<td>36.2</td>
<td>45.25</td>
<td>54.3</td>
<td>63.35</td>
<td>72.4</td>
</tr>
<tr>
<td>CS-2</td>
<td>13.4</td>
<td>26.8</td>
<td>40.2</td>
<td>53.6</td>
<td>67.0</td>
<td>80.4</td>
<td>93.8</td>
<td>107.2</td>
</tr>
<tr>
<td>CS-3</td>
<td>15.6</td>
<td>31.2</td>
<td>46.8</td>
<td>62.4</td>
<td>78.0</td>
<td>93.6</td>
<td>109.2</td>
<td>124.8</td>
</tr>
<tr>
<td>CS-4</td>
<td>21.4</td>
<td>42.8</td>
<td>64.2</td>
<td>85.6</td>
<td>107.4</td>
<td>128.4</td>
<td>149.8</td>
<td>171.2</td>
</tr>
</tbody>
</table>

GPRS architecture and interfaces

GPRS protocol architecture