Wireless Networks: Cellular Systems

- Concept
- GSM
- IS-95

Adapted from J. Schiller, “Mobile Communications”, Chapter 4

Wireless Networks: Cellular Systems

Cellular Concept

Several small cells instead of a single transmitter => frequency reuse: better efficiency

Fixed Channel Allocation:
- Cluster of size $N = p + ij + p$; and $D = \sqrt{3N}R$
- $R$ cell radius and
- $D$ distance at which a frequency can be reused with acceptable interference
Examples

Capacity in Cellular Systems

Blocking Probability (Grade Of Service): *Erlang B* formula

\[ GOS = \frac{(\lambda T)^c / C!}{\sum_{n=0}^{C} (\lambda T)^n / n!} \]

\( \lambda \): calls arrival rate; \( T \): calls average duration (service time: 1/\( \mu \))
Increasing Capacity

Cells splitting

Sectoring: 3 sectoring ($120^\circ$) or 6 sectoring

GSM: Overview

GSM
- formerly: Groupe Spéciale Mobile (founded 1982)
- now: Global System for Mobile Communication
- today many providers all over the world use GSM (more than 130 countries in America, Asia, Africa, Europe, Australia)
- 500 million subscribers
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

Disadvantages of GSM

There is no perfect system!!
- no end-to-end encryption of user data
- no full ISDN bandwidth of 64 kbit/s to the user

- electromagnetic radiation

- abuse of private data possible
- roaming profiles accessible

- high complexity of the system (over 5000 pages)
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: 300 - 1200 bit/s
  - data service (packet switched)
    - synchronous: 2.4, 4.8 or 9.6 kbit/s
    - asynchronous: 300 - 9600 bit/s
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 (911); mandatory for all service providers; free of charge; connection with the highest priority (preemption of other connections possible)
  - Multinumbering
    - several ISDN phone numbers per user 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 using the signaling channel, thus allowing simultaneous use of basic services and SMS
Supplementary services

- Services in addition to the basic services, cannot be offered stand-alone
- Similar to ISDN services besides lower bandwidth due to the radio link
- 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
GSM: overview

GSM: elements and interfaces
GSM: system architecture

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
- \( A_{_{B_{\text{is}}}} \): 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):
    - Base Transceiver Station (BTS): 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)
GSM: cellular network

segmentation of the area into cells

- use of several carrier frequencies
- not the same frequency in adjoining cells
- cell sizes vary from some 300 feet up to 20 miles depending on user density, geography, transceiver power etc.
- hexagonal shape of cells is idealized (cells overlap, shapes depend on geography)
- if a mobile user changes cells
  - handover of the connection to the neighbor cell

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>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>X</td>
</tr>
<tr>
<td>Mapping of terrestrial onto radio channels</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Channel coding and decoding</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Rate adaptation</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Encryption and decryption</td>
<td></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></td>
<td>X</td>
</tr>
<tr>
<td>Handover management</td>
<td></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
    - corresponds to the network termination (NT) of an ISDN access
    - end-point of the radio interface ($U_m$)
  - 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

- 935-960 MHz
  - 124 channels (200 kHz)
  - Downlink
- 890-915 MHz
  - 124 channels (200 kHz)
  - Uplink

GSM TDMA frame

- Time: 4.615 ms
- Guard space and user data slots
- Burst duration: 577 µs

GSM hierarchy of frames

- Hyperframe: 3 h 28 min 53.76 s
- Superframe: 6.12 s
- Multiframe: 120 ms
- Frame: 4.615 ms
- Slot/burst: 577 µs
GSM protocol layers for signaling

![Diagram of GSM protocol layers for signaling]

- **U_m**
- **A_{bis}**
- **A**

### 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

1. MS \rightarrow BTS \rightarrow BSC \rightarrow MSC
2. MS \rightarrow BTS \rightarrow BSC \rightarrow MSC
3. MS \rightarrow BTS \rightarrow BSC \rightarrow MSC
4. MS \rightarrow BTS \rightarrow BSC \rightarrow MSC

Handover decision

receive level $BTS_{old}$

receive level $BTS_{old}$
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

```
K_i \rightarrow RAND \\
128 bit \downarrow 128 bit

A3

SRES* 32 bit

SRES =? SRES

SRES 32 bit
```

K_i: individual subscriber authentication key

SRES: signed response

---

GSM - key generation and encryption

```
K_i \rightarrow RAND \\
128 bit \downarrow 128 bit

A8

K_c 64 bit

cipher key

BTS

MS

A5

data

A5

data

encrypted data
```

Wireless Networks: Cellular Systems
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)
- already standardized
- bundling of several time-slots to get higher AIUR (Air Interface User Rate)
  (e.g., 57.6 kbit/s using 4 slots, 14.4 each)
- advantage: ready to use, constant quality, simple
- disadvantage: channels blocked for voice transmission

<table>
<thead>
<tr>
<th>AIUR [kbit/s]</th>
<th>TCH/F4.8</th>
<th>TCH/F9.6</th>
<th>TCH/F14.4</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.8</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9.6</td>
<td>2</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>14.4</td>
<td>3</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>19.2</td>
<td>4</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>28.8</td>
<td>4</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>38.4</td>
<td></td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>43.2</td>
<td></td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>57.6</td>
<td></td>
<td></td>
<td>4</td>
</tr>
</tbody>
</table>

Data services in GSM II

GPRS (General Packet Radio Service)
- packet switching
- using free slots only if data packets ready to send
  (e.g., 115 kbit/s using 8 slots temporarily)
- standardization 1998, introduced 2000
- advantage: one step towards 3G, more flexible
- disadvantage: more investment needed

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>$10^{-9}$</td>
<td>$10^{-9}$</td>
<td>$10^{-9}$</td>
</tr>
<tr>
<td>2</td>
<td>$10^{-4}$</td>
<td>$10^{-5}$</td>
<td>$10^{-5}$</td>
<td>$10^{-6}$</td>
</tr>
<tr>
<td>3</td>
<td>$10^{-2}$</td>
<td>$10^{-5}$</td>
<td>$10^{-5}$</td>
<td>$10^{-2}$</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>
<tr>
<td>4</td>
<td>unspecified</td>
<td></td>
</tr>
</tbody>
</table>

GPRS architecture and interfaces
GPRS protocol architecture

IS-95 (CdmaOne): [TIA/EIA IS-95]

IS-95: standard for the radio interface
IS-41: standard for the network part

Operates of 800MHz and 1900MHz bands

Uses DS-CDMA technology (1.2288 Mchips/s)

Forward link (downlink): $\frac{1}{2}$ convolutional code, interleaved, 64 chips spreading sequence (Walsh-Hadamard functions)
- pilot channel (code 0), synchronization channel (code 32), 7 paging channels, up to 63 traffic channels

Reverse link (uplink): $\frac{1}{3}$ convolutional code, interleaved, 6 bits are mapped into a Walsh-Hadamard sequence, spreading using a User-BaseStation specific code (with period $2^{42} \cdot 1/2^{15}$)

Tight power control (open-loop, fast closed loop)