Overview

- GSM Overview
- Services
- Architecture
- Cell management
- TDMA, FDMA
- Orientation
- Handover
- Authentications
- HSCSD, GPRS
Mobile phones worldwide

- **W. Europe**
- **USA**
- **Japan**
- **China**
- **ROW**

Years: 1993 to 2003

Units: [ct./dk]
Mobile phone subscribers worldwide

- Analog total
- GSM total
- CDMA total
- TDMA total
- PDC/PHS total
- Total

[subscribers (x 1000)]


- 0
- 100000
- 200000
- 300000
- 400000
- 500000
- 600000
- 700000

GSM: Overview

- 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 (more than 184 countries in Asia, Africa, Europe, Australia, America)
- more than 750 million subscribers
- more than 70% of mobile phones use GSM
- more than 360 billion SMS/year worldwide
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

- no end-to-end encryption of user data
- no full ISDN bandwidth of 64 kbit/s to the user
- reduced concentration while driving
- electromagnetic radiation
- abuse of private data possible
- roaming profiles accessible
- high complexity of the system
- several incompatibilities within the GSM standards
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

- 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, without contract; connection with the highest priority (preemption of other connections possible)
Additional Tele Services

• Non-Voice-Teleservices
  – Short Message Service (SMS)
    up to 160 character alphanumeric data transmission to/from the mobile terminal using the signaling channel, thus allowing simultaneous use of basic services and SMS
  – 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)
  – etc.
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)
  - ...
GSM: overview

NSS with OSS

OMC, EIR, AUC

VLR

MSC

HLR

GMSC

NSS with OSS

VLR

MSC

BSC

BSC

fixed network

RSS
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: elements and interfaces

RSS

BSC

A

NSS

VLR

MSC

OMC

OSS

EIR

AUC

GMSC

IWF

PDN

signaling

ISDN, PSTN

U_m

radio cell

BTS

BSS

radio cell

BTS

BTS

MSC

HLR

VLR

GMSC

MOBILE COMPUTING R. Wattenhofer
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
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></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>X</td>
<td></td>
</tr>
<tr>
<td>Rate adaptation</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Encryption and decryption</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Paging</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Uplink signal measurements</td>
<td>X</td>
<td></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
System architecture: network and switching subsystem

- **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)
System architecture: operation subsystem

- The OSS (Operation Subsystem) enables centralized operation, management, and maintenance of all GSM subsystems
- Components
  - Operation and Maintenance Center (OMC)
    - different control capabilities for the radio subsystem and the network subsystem
  - 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
GSM: system architecture

radio subsystem

- MS
- MS
- BTS
- BTS
- BSC

network and switching subsystem

- MSC
- SS7
- EIR
- HLR
- VLR
- IWF

fixed partner networks

- ISDN
- PSTN
- PSPDN
- CSPDN
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 100 m up to 35 km depending on user density, geography, transceiver power etc.
- hexagonal shape of cells is idealized (cells overlap)
- if a mobile user changes cells:
  handover of the connection to the neighbor cell
Example for space multiplexing: Cellular network

- Simplified hexagonal model
- Signal propagation ranges: Frequency reuse only with a certain distance between the base stations
- Can you reuse frequencies in distance 2 or 3 (or more)?
- Graph coloring problem
- Example: fixed frequency assignment for reuse with distance 2
- Interference from neighbor cells (other color) can be controlled with transmit and receive filters
Channel Assignment

- Formal definition of the problem:

- Input: A Graph G, the nodes of G are the cells, there is an edge between two nodes if the cells interfere. Each node u has an integer weight $w(u)$ that represents the number of users in cell u.

- Output: We assign $w(u)$ colors to each node, such that no two neighboring nodes have the same color. We are interested in the minimum number of colors needed.

- This problem known as Graph Multicoloring. It is NP-hard.
Channel Assignment Variations

- Special types of graphs, e.g. the hexagon graph.

- Dynamic version: the weight of a node $u$ is a function that changes over time: $w_t(u)$. If a future $w_t(u)$ is not known, the algorithm is online.

- Recoloring vs. non-recoloring algorithms: A dynamic algorithm is a non-recoloring algorithm if the frequency of a user is not allowed to change once it is assigned. Note that a recoloring algorithm is more powerful.

- Centralized vs. Distributed Control. In particular an algorithm is $k$-local if each node can only communicate with nodes within distance $k$. 
Basic Types of Algorithms

• Fixed Assignment (FA): Nodes are partitioned into independent sets, and each such set is assigned a separate set of channels. This works very well if the traffic is balanced well. Example: Hexagon graph with reuse distance 3 is on the right.

• Borrowing Algorithms: Improvement of FA. If traffic is not balanced, cells can borrow frequencies from neighboring cells.

• Hybrid Channel Assignment: Divide the frequencies into “reserved” and “borrowable” ones.

• Dynamic Channel Assignment: A centrally coordinated pool of frequencies is distributed to cells.
Online Channel Assignment

• Problem: We are given the hexagon graph with reuse distance 2. Callers arrive at cells in online fashion, that is, one after the other in an input sequence $\sigma$. We need to give each caller a channel (an integer), such that no caller in the same or a neighboring hexagon has the same channel. We assume that calls have infinite duration (which is the same as assuming that all calls have the same duration).

• Cost: The cost of the algorithm is the value of the highest channel we used.

• Competitive Analysis: If $\text{cost}_{\text{ALG}}(\sigma) \leq \rho \cdot \text{cost}_{\text{OPT}}(\sigma) + \text{const}$ for all input sequences $\sigma$ and an optimal offline algorithm OPT, then the Algorithm ALG is called $\rho$-competitive. (Note: if $\text{const} = 0$ the ALG is strictly $\rho$-competitive.)
The Greedy Algorithm for Online Channel Assignment

• Algorithm: When a new call arrives, it is assigned the minimum available channel, that is, the minimum integer that is not used in the cell and the neighboring cells.

• Theorem: The Greedy Algorithm is 2.5-competitive. This is optimal.

• Unfortunately, both upper bound and lower bound are too intricate to be presented here. But we can easily show that

• Theorem for lazy professors: The Greedy Algorithm is 3-competitive.
Wait a minute…

- So far: If two antennas “overlap” they are assigned different frequencies.

- Is this really true? Check this example with 3 antennas

- You may assign the two outer antennas the same frequency!
Online Call Control

- Problem: In a real GSM network, we have only a fixed amount of channels available. If there are more callers, we have to reject some.
- Simplification: We have only 1 frequency available.
- Problem Statement: We are given the hexagon graph with reuse distance 2. Callers arrive at cells in online fashion, that is, one after the other in an input sequence $\sigma$. We need to accept or reject each caller, such that there is at most 1 caller in a cell and its 6 neighboring cells. We assume that calls have infinite duration (which is the same as assuming that all calls have the same duration).
- Benefit: The benefit of the algorithm is the number of callers we accept.
- Competitive Analysis: If $\rho \cdot \text{benefit}_{\text{ALG}}(\sigma) \geq \text{benefit}_{\text{OPT}}(\sigma)$ for all input sequences $\sigma$ and an optimal offline algorithm OPT, then the Algorithm ALG is called $\rho$-competitive.
The Greedy Algorithm for Online Call Control

• Algorithm: When a new call arrives, it is accepted whenever possible.

• Theorem: The Greedy Algorithm is 3-competitive.

• Problem of algorithm is obvious already with the first call: If we do not accept the call, we are not at all competitive (because it might be the only call); if we accept the call might have to discard 3 calls in the neighboring calls later.
A Randomized Algorithm for Online Call Control

- It was long believed that the greedy algorithm is the best possible.

- New idea: Maybe randomization helps. Don’t accept every call that you might accept.

- Problem: Maybe adversary presents the same cell over and over until we (randomly) accept and then presents the 3 callers in the neighboring cells.

- Solution: If once a caller was (randomly) rejected in a cell, we should not accept any caller anymore in this cell (we mark the cell).
A Randomized Algorithm for Online Call Control

• Algorithm: Initially, all cells are unmarked.

• For a new call in cell $u$:
  – If $u$ is marked or a call in $N^*(u)$ is accepted, then we reject the call.
  – Else: With probability $p$, we accept the call.
  – With probability $1-p$, we reject the call and mark the cell $u$.

• Theorem: The randomized algorithm is 2.97-competitive.

• Remarks:
  • For randomized algorithms, we use the expected benefit.
  • An improved version of the algorithm is 2.651-competitive.
  • The algorithm can be generalized and is $\frac{27}{28} \Delta$-competitive.
GSM - TDMA/FDMA

935-960 MHz
124 channels (200 kHz)
downlink

890-915 MHz
124 channels (200 kHz)
uplink

higher GSM frame structures

green

green

green

GSM TDMA frame

GSM time-slot (normal burst)

tail
user data S Training S user data tail

guard space

guard space

guard space

3 bits 57 bits 1 26 bits 1 57 bits 3

546.5 µs 577 µs

4.615 ms
Logical Channels

• Traffic Channel TCH: For speech and data
  – Full rate TCH/F (22.8 kbit/s), Half rate TCH/H (11.8 kbit/s)
  - Speech codec needed 13 kbit/s – remaining bandwidth is used for strong error correction TCH/FS; now some use TCH/HS
  - For data there are TCH/F4.8, TCH/F9.6, and TCH/F14.4

• Control Channel CCH
  – Broadcast Control Channel BCCH: global variables in cell (such as hopping scheme, frequencies, frequencies of neighbor cells, etc.)
    • Frequency Correction Channel FCCH, Synchronization Channel SCH
  – Common Control Channel CCCH
    • Paging Channel PCH, Random Access Channel RACH (slotted Aloha!)
  – Dedicated Control Channel DCCH: Bidirectional
    • Stand-alone Dedicated Control Channel SDCCH (for stations without TCH, with only 782 bit/s), Slow Associated Dedicated Control Channel SACCH (for each station), Fast Associated Dedicated Control Channel FACCH (in case of handover)
### GSM hierarchy of frames

<table>
<thead>
<tr>
<th>Frame Type</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Burst</td>
<td>577 µs</td>
</tr>
<tr>
<td>Slot</td>
<td></td>
</tr>
<tr>
<td>Multiframe</td>
<td>120 ms</td>
</tr>
<tr>
<td>Superframe</td>
<td>6.12 s</td>
</tr>
<tr>
<td>Hyperframe</td>
<td>3 h 28 min 53.76 s</td>
</tr>
</tbody>
</table>

- Burst: 577 µs
- Slot: No specific duration provided
- Multiframe: 120 ms
- Superframe: 6.12 s
- Hyperframe: 3 h 28 min 53.76 s
GSM protocol layers for signaling

- **MS**
  - CM
  - MM
  - RR
  - LAPD_m
  - radio

- **BTS**
  - U_m
  - BTSM
  - LAPD
  - radio
  - PCM

- **BSC**
  - A_bis
  - BSSAP
  - SS7
  - LAPD
  - PCM

- **MSC**
  - CM
  - MM
  - BSSAP
  - SS7
  - PCM

- **Bandwidths**
  - 16/64 kbit/s
  - 64 kbit/s / 2.048 Mbit/s
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