GSM/3G: cellular network

- Uses several carrier frequencies for each cell
- No overlap with frequencies in adjoining cells
- Cell sizes vary from some 100m up to 35km depending on user density, geography, transceiver power etc.
- Hexagonal shape of cells is idealized (cells overlap, actual shapes depend on geography and must be measured or simulated)
- Handover of user connection to the neighboring cell when moving
  - Provided there is capacity
Some acronyms…

• Components
  – MS (Mobile Station)
  – BS (Base Station)
  – (G)MSC ((Gateway) Mobile Switching Center)
  – LR (Location Register)

• Subsystems
  – RSS (Radio SubSystem): handles all radio aspects
  – NSS (Network and Switching Subsystem): handles call forwarding, handover, switching and others.
  – OSS (Operation SubSystem): management of the network

• Databases
  – HLR (Home Location Register)
  – VLR (Visitor Location Register)
  – EIR (Equipment Identity Register)
Mobile Services Switching Center (MSC)

- Controls all connections to/from a Mobile Terminal within the domain of the MSC.
  - several BSC can belong to a MSC
  - Separate radio channels are used for control and connection set-ups
- Databases
  - **Home Location Register (HLR)**
    Central master database containing permanent and semi-permanent data (roaming data) of all subscribers assigned to the HLR (one provider can have several HLRs)
  - **Visitor Location Register (VLR)**
    Local database for data about all users/terminals currently in the domain of the VLR.

Operation 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
- **Others – less significant…**
Mobile Terminated Call set-up

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 set-up

1, 2: connection request
3, 4: security check
5-8: check resources (free circuit)
9-10: set up call
Frequencies - GSM

GSM - TDMA/FDMA

GSM TDMA frame

GSM time-slot (normal burst)
4 types of handover

Handover decision
Handover procedure

Security services in GSM

• 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
    a successful authentication)

• Anonymity
  – temporary identity TMSI
    (Temporary Mobile Subscriber Identity)
  – Location anonymity