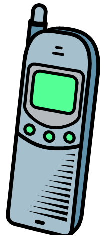
Telecommunications systems GSM

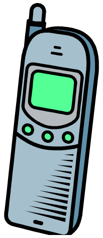
- **GSM**
  - **Overview**
  - **Services**
  - **Sub-systems**
  - **Components**

- **IS 95**
  - **Overview**
  - **Services**
  - **Sub-systems**
  - **Components**

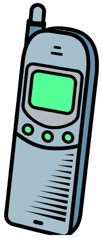


GSM: Overview

- GSM
  - ❑ Global System for Mobile Communication
  - ❑ Pan-European standard (ETSI, European Telecommunications Standardisation Institute)
  - ❑ today many providers all over the world use GSM (more than 130 countries in Asia, Africa, Europe, Australia, America)
  - ❑ more than 100 million subscribers
  - ❑ Used by more than 800 million people

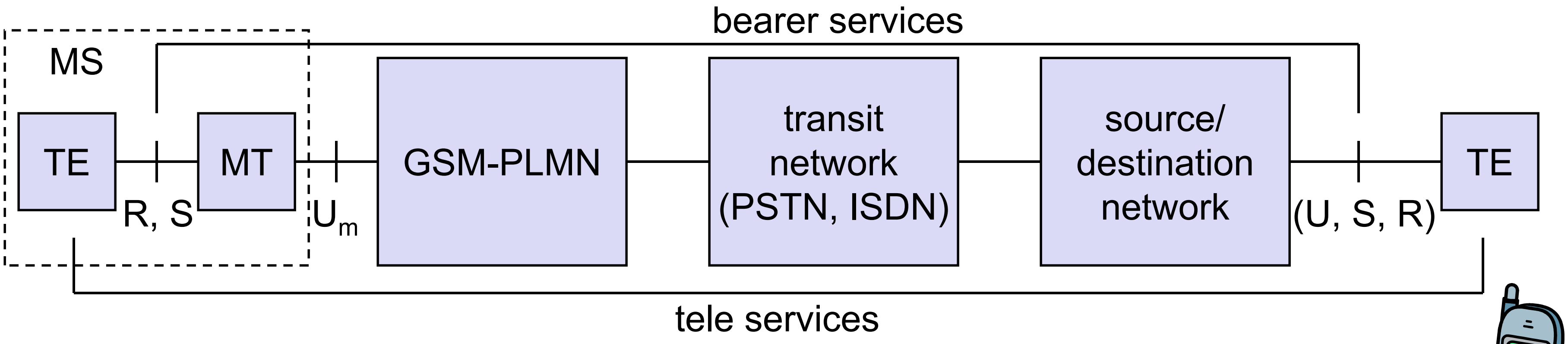


- □ The GSM standard operates in the frequency ranges of 900, 1800, and 1900 MHz
- □ Tri-band (operable in GSM 900/1800/1900) phones enable easy international roaming in GSM networks
- □ GSM— a second generation (2G) communication standard
- □ GSM 900 -> uplink – 890 – 915 MHz
  downlink – 935 – 960 MHz



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 – interface to the physical medium (transparent for example in the case of voice or non transparent for data services)
  - Tele Services – services provided by the system to the end user (e.g., voice, SMS, fax, etc.)
  - Supplementary Services – associated with the tele services: call forwarding, redirection, etc.

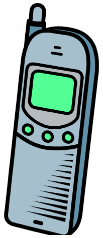


Bearer Services

- Telecommunication services to transfer data between access points
  - R and S interfaces – interfaces that provide network independent data transmission from end device to mobile termination point.
  - U interface – provides the interface to the network (TDMS, FDMA, etc.)
- Specification of services up to the terminal interface (OSI layers 1-3)
  - Transparent – no error control, flow control, only FEC(Forward Error correction)
  - Non transparent – error control, flow control
- Different data rates for voice and data (original standard)
  - voice service (circuit switched)
    - synchronous: 2.4, 4.8 or 9.6 Kbps.
  - 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 measures etc.
- Offered voice related 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)
  - Multinumbering
    several ISDN phone numbers per user possible



- **Additional services: Non-Voice-Teleservices**
  - ❑ **group 3 fax**
  - ❑ **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 (160 characters)

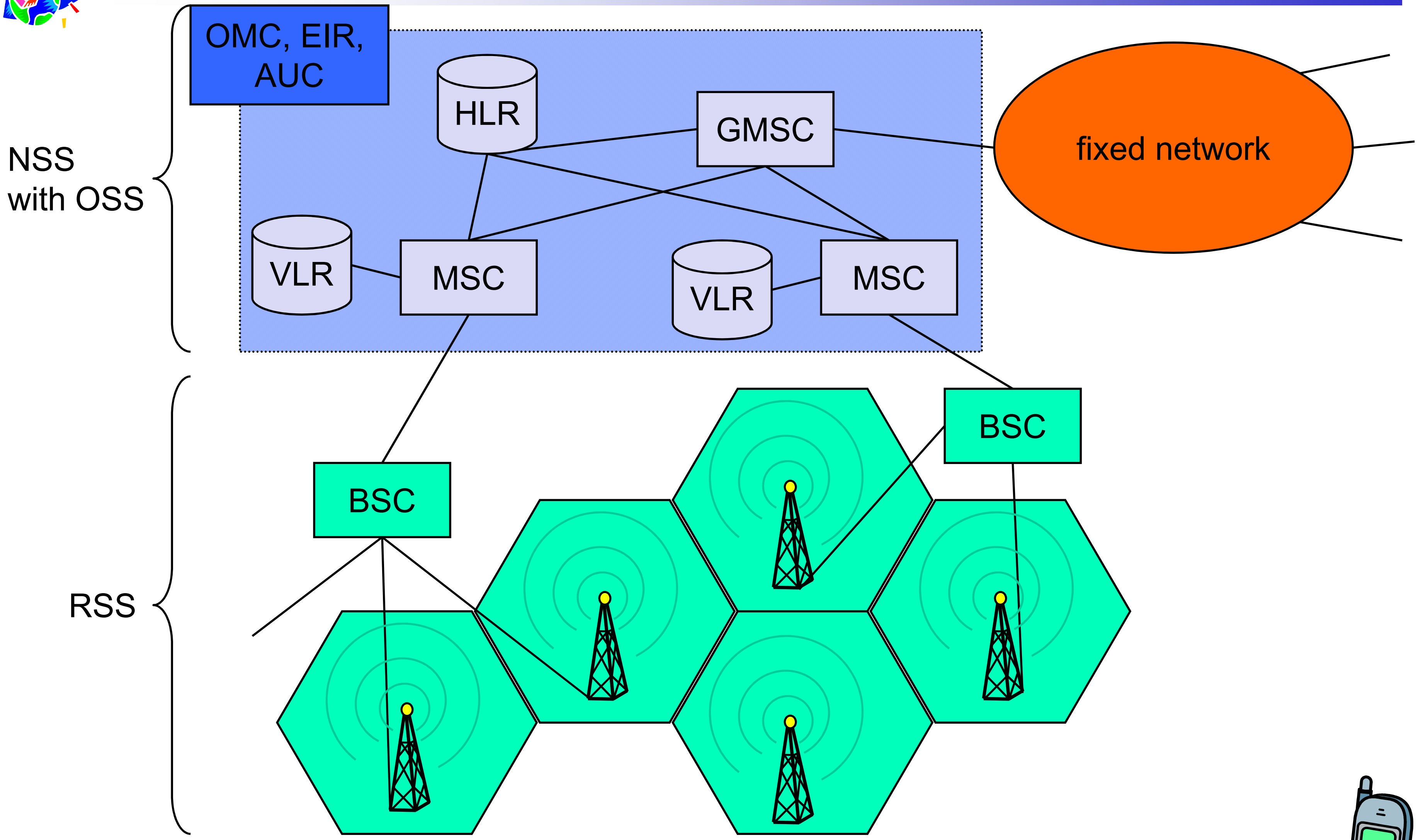
Supplementary services

- 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)
  - ❑ ...

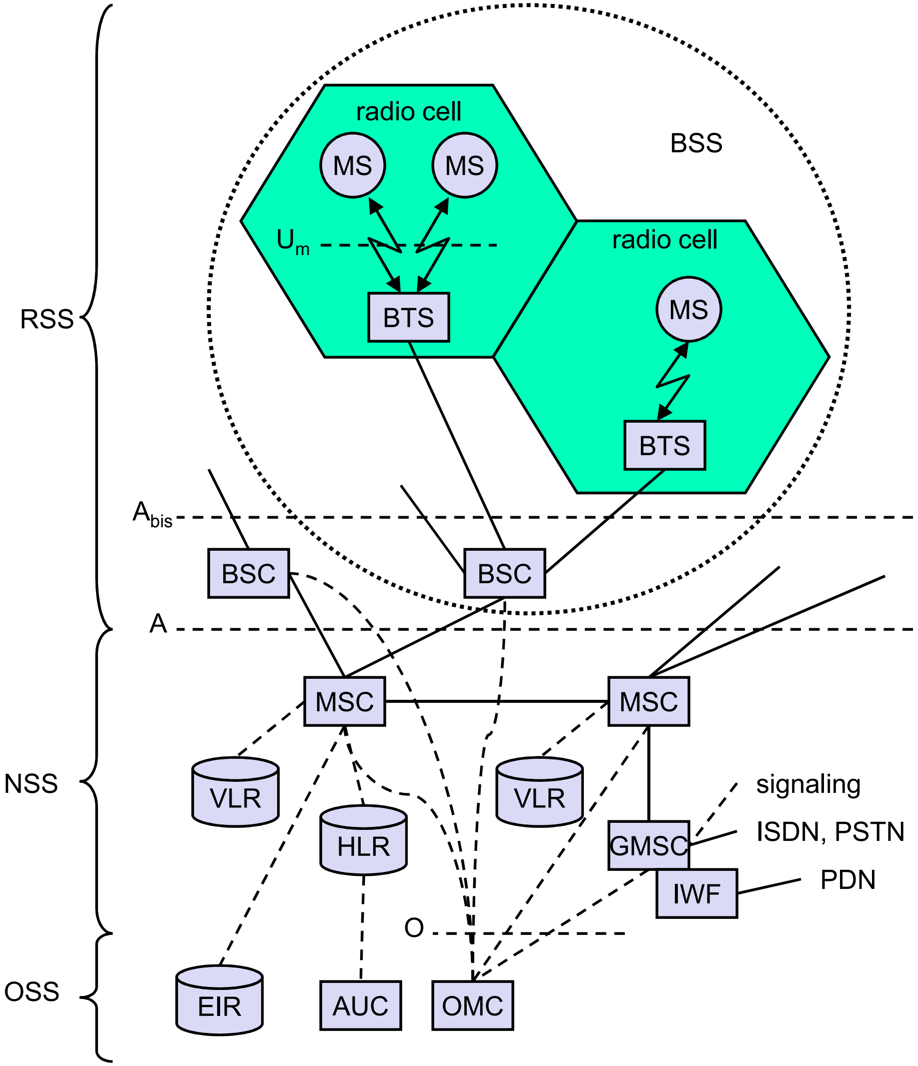
Architecture of the GSM system

- **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

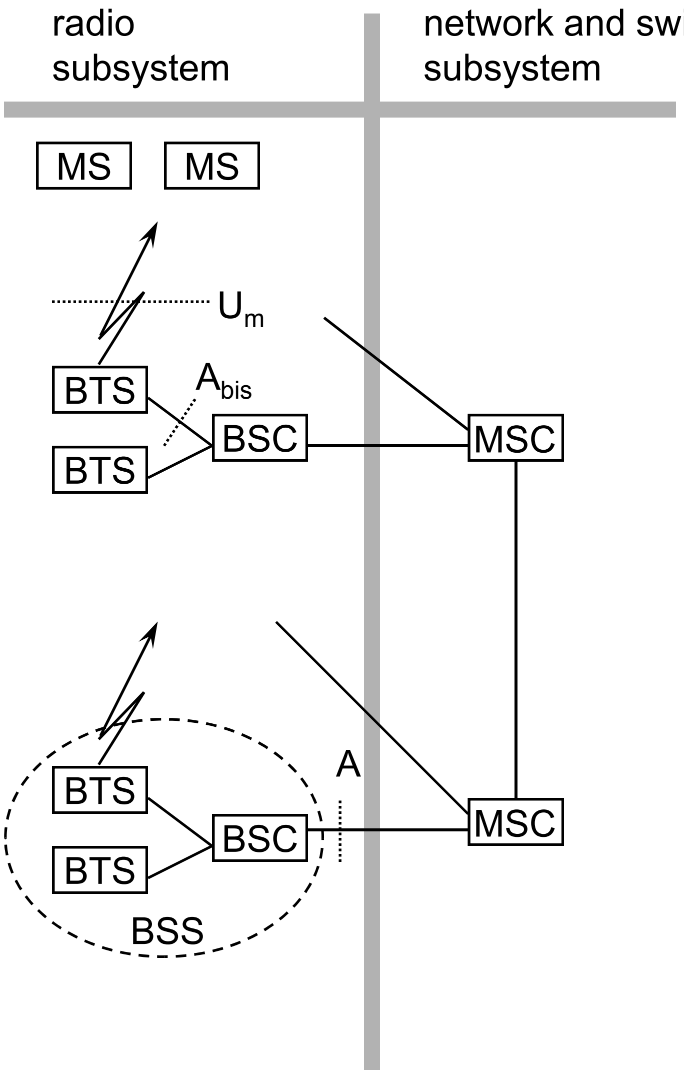
GSM: overview



GSM: elements and interfaces



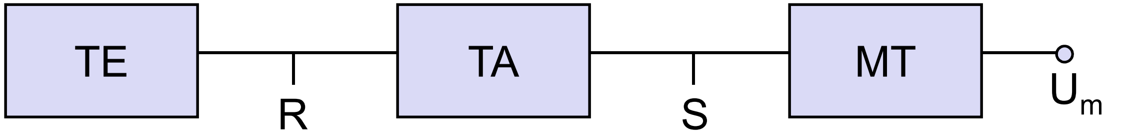
System architecture (i) radio subsystem



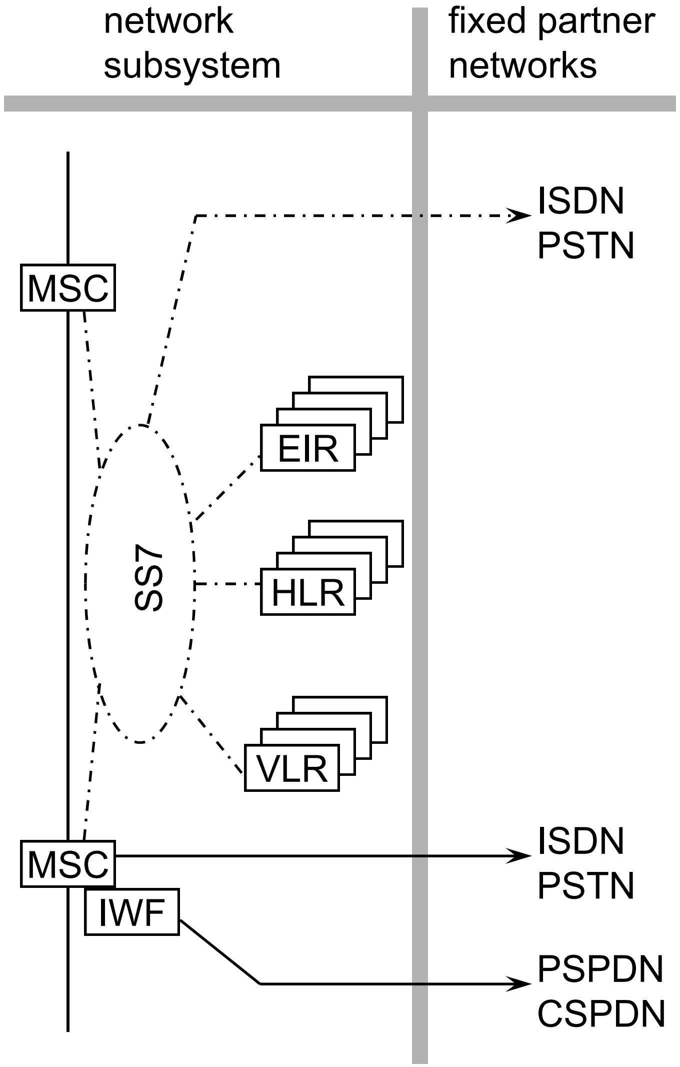
- **Components**
  - ***MS* (Mobile Station)**
  - ***BSS* (Base Station Subsystem): consisting of**
    - *BTS* (Base Transceiver Station): sender and receiver
    - *BSC* (Base Station Controller): controlling several transceivers
- **Interfaces**
  - **U_m : radio interface**
  - **A_{bis} : standardized,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

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 connects via modem, Bluetooth, IrDA etc. to MT)
  - **TE (Terminal Equipment):**
    - peripheral device of the MS, offers services to a user
    - Can be a headset, microphone, etc.
    - does not contain GSM specific functions
  - **SIM (Subscriber Identity Module):**
    - personalization of the mobile terminal, stores user parameters



System architecture: (ii) 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.)

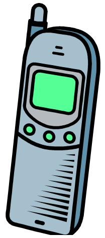
Databases

- □ *HLR* (Home Location *R*egister)
- □ *VLR* (Visitor Location *R*egister)
- □ *EIR* (Equipment Identity Register)

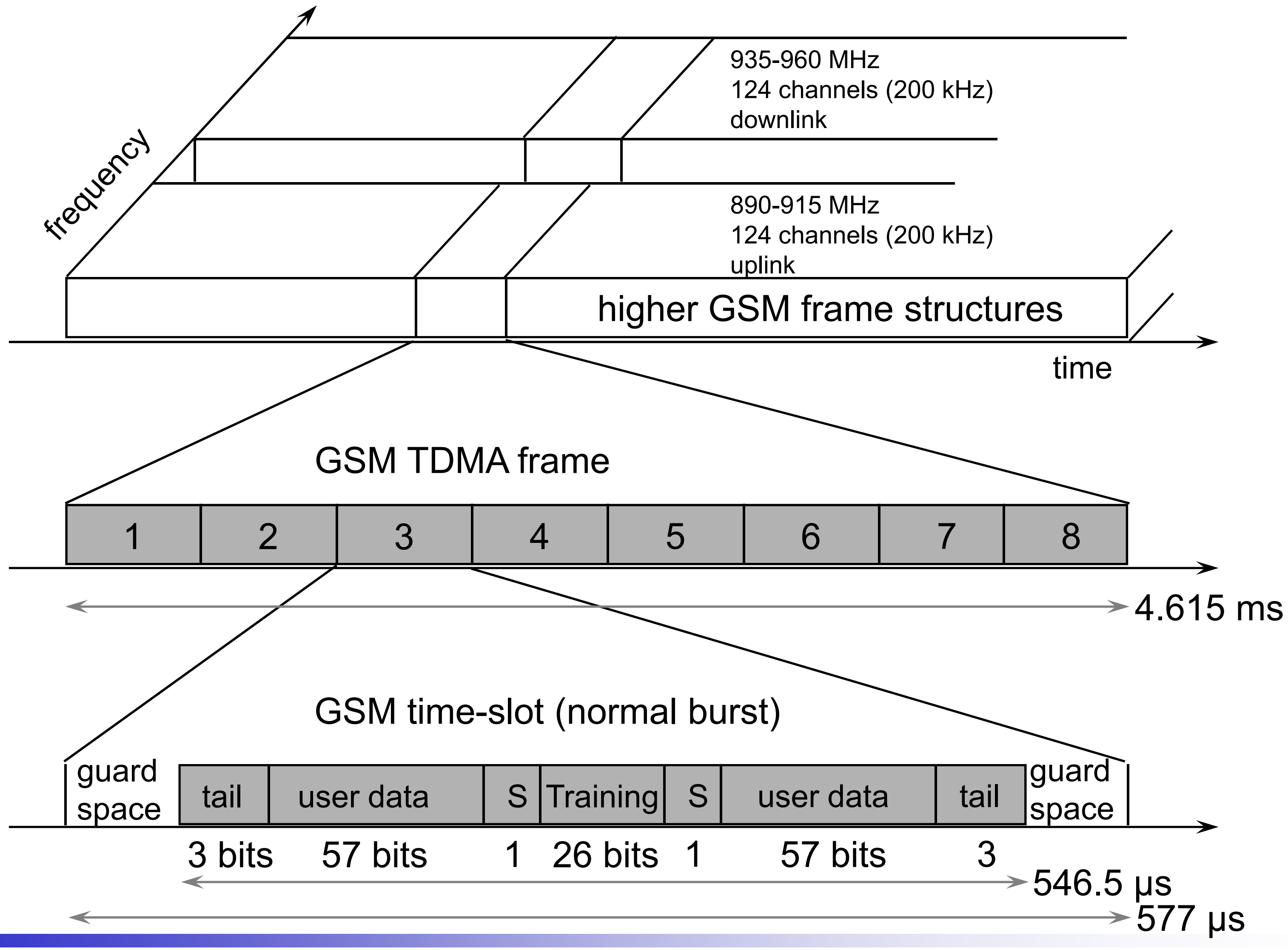
- **NSS is the main component of the public mobile network GSM**
  - **switching, mobility management, interconnection to other networks, system control**
- **Components**
  - **Mobile Services Switching Center (MSC)**
    controls all connections via a separated network to/from a mobile terminal within 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 - data about all users currently visiting in the domain of the VLR

System architecture: (iii)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



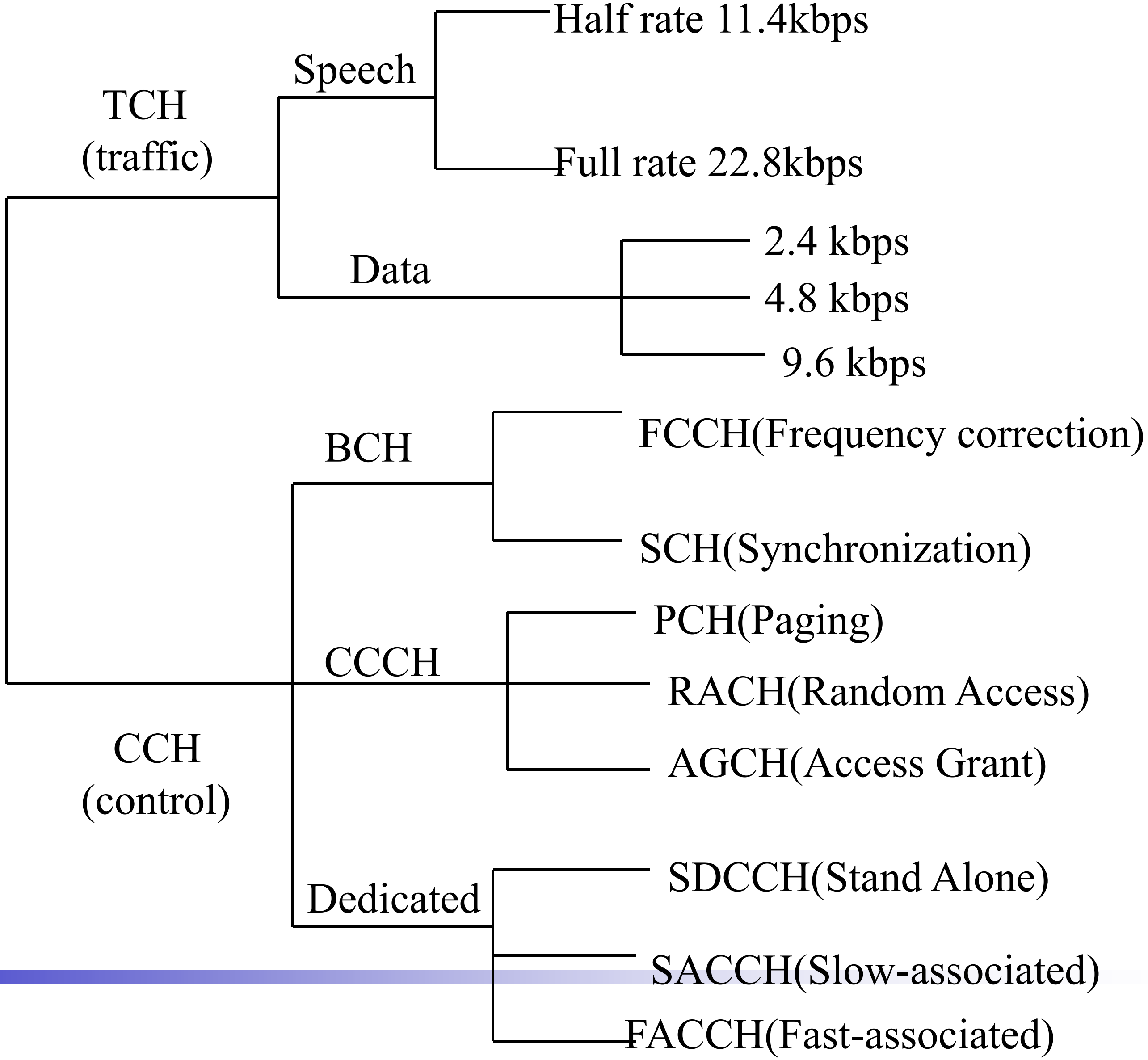
GSM Radio Interface - TDMA/FDMA



Logical channels

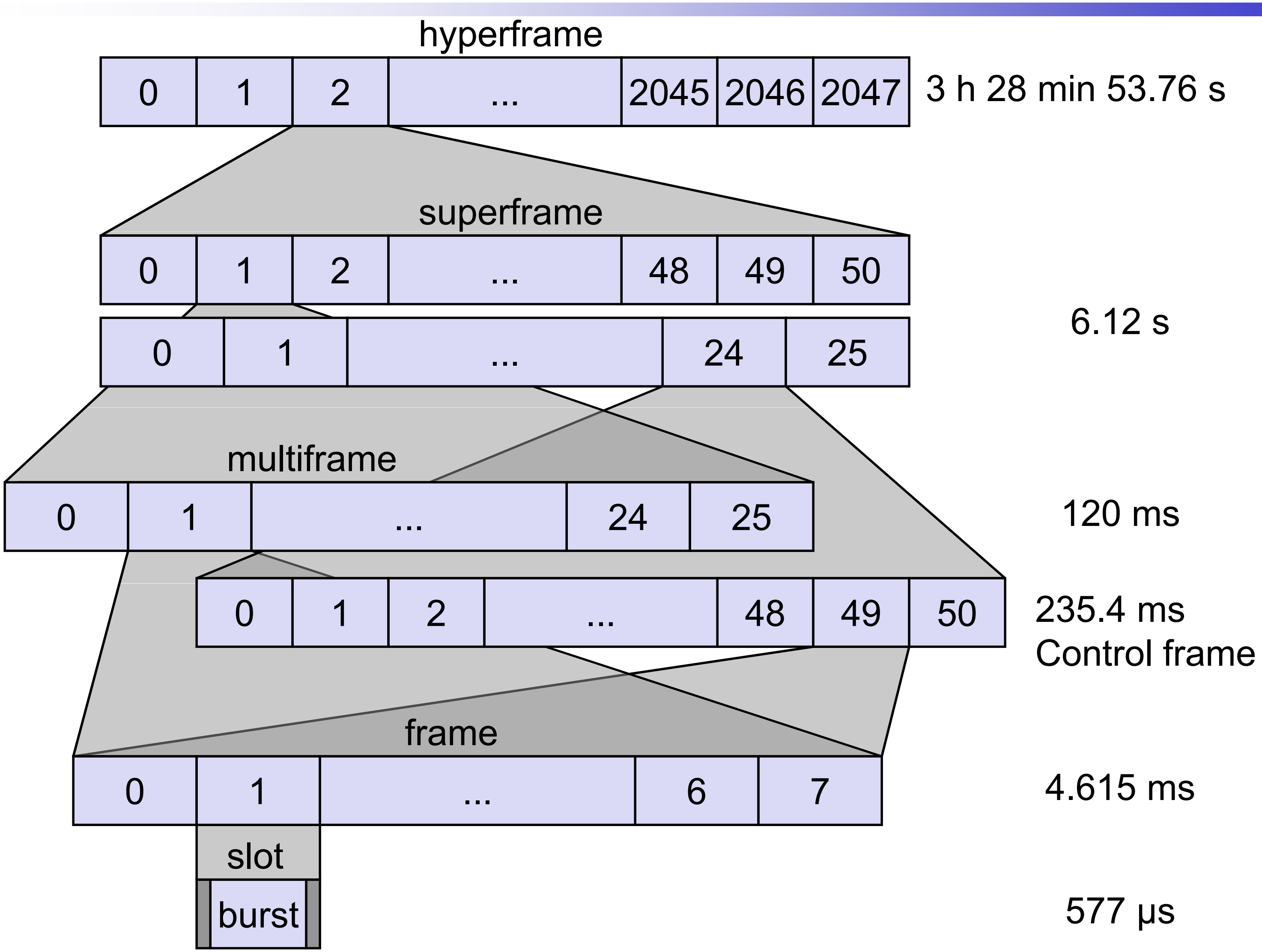
- **Traffic channels**
  - **Used to transfer user data**
- **Control Channels**
  - Used to control medium access, allocation of traffic channels or mobility management

Logical Channels

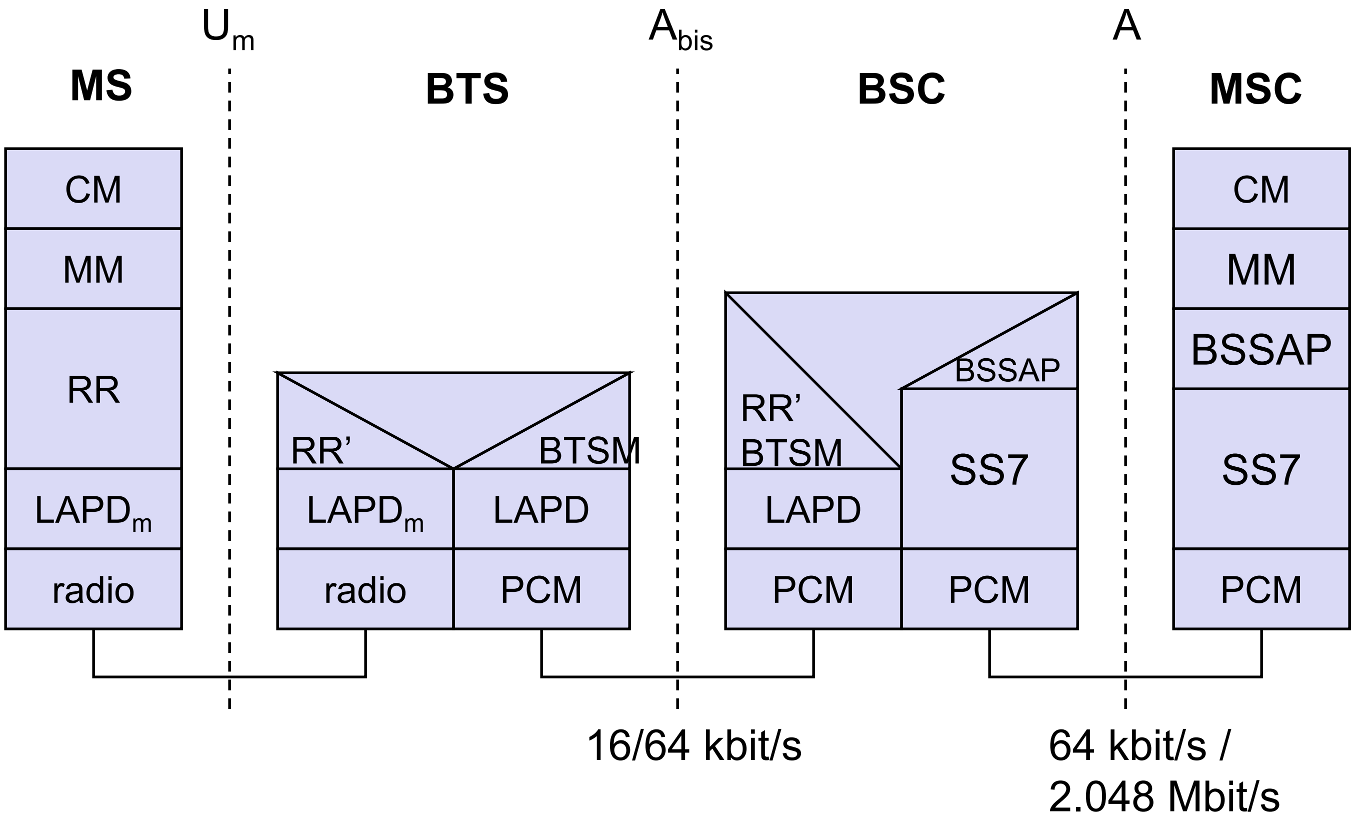


- TCH (traffic)
  - Speech
    - Half rate 11.4kbps
    - Full rate 22.8kbps
  - Data
    - 2.4 kbps
    - 4.8 kbps
    - 9.6 kbps
- CCH (control)
  - BCH
    - FCCH(Frequency correction)
    - SCH(Synchronization)
  - CCCH
    - PCH(Paging)
    - RACH(Random Access)
    - AGCH(Access Grant)
  - Dedicated
    - SDCCH(Stand Alone)
    - SACCH(Slow-associated)
    - FACCH(Fast-associated)

GSM hierarchy of frames

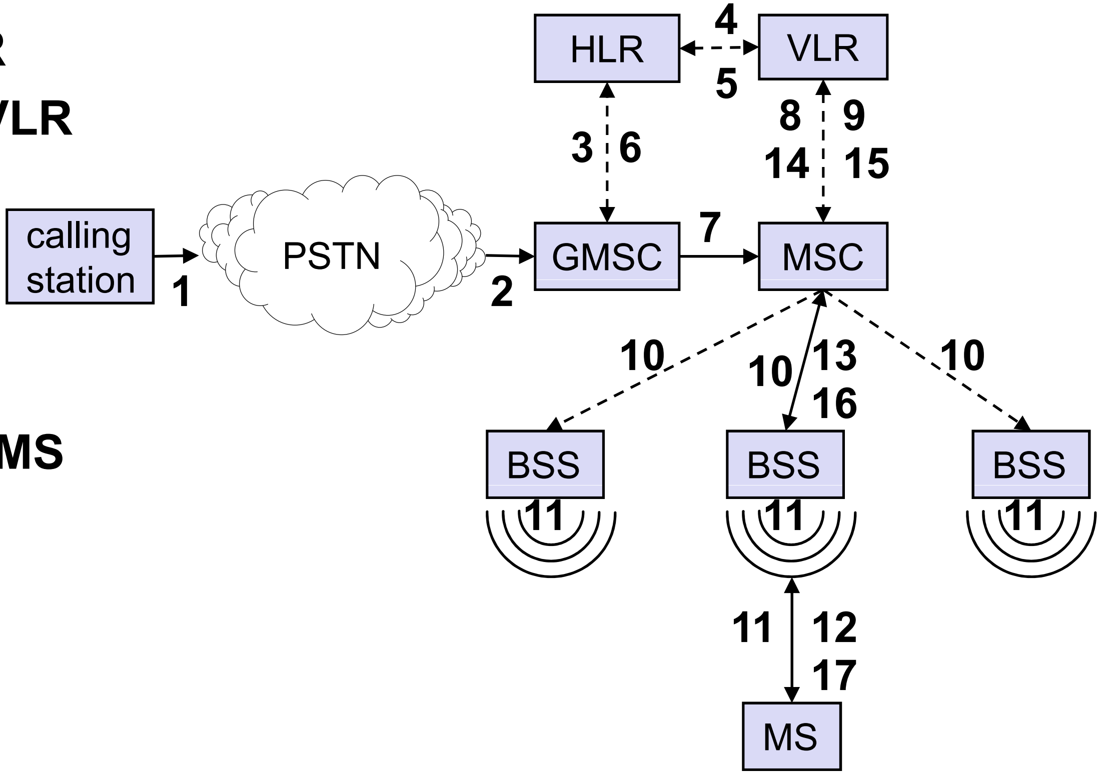


GSM protocol layers for signaling



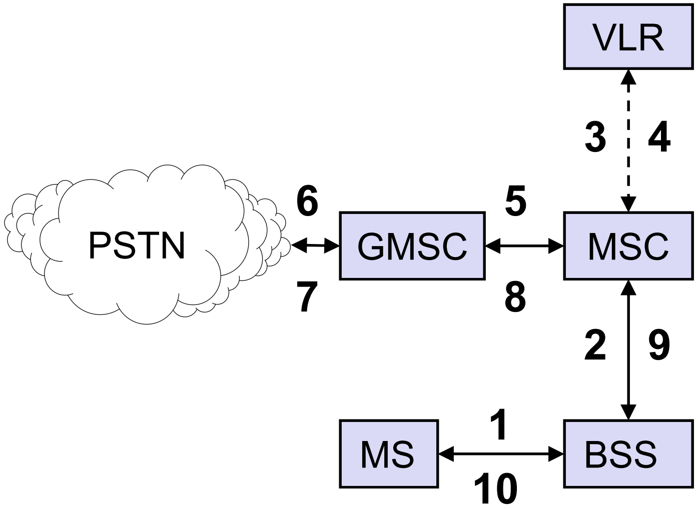
Mobile Terminated Call

- 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

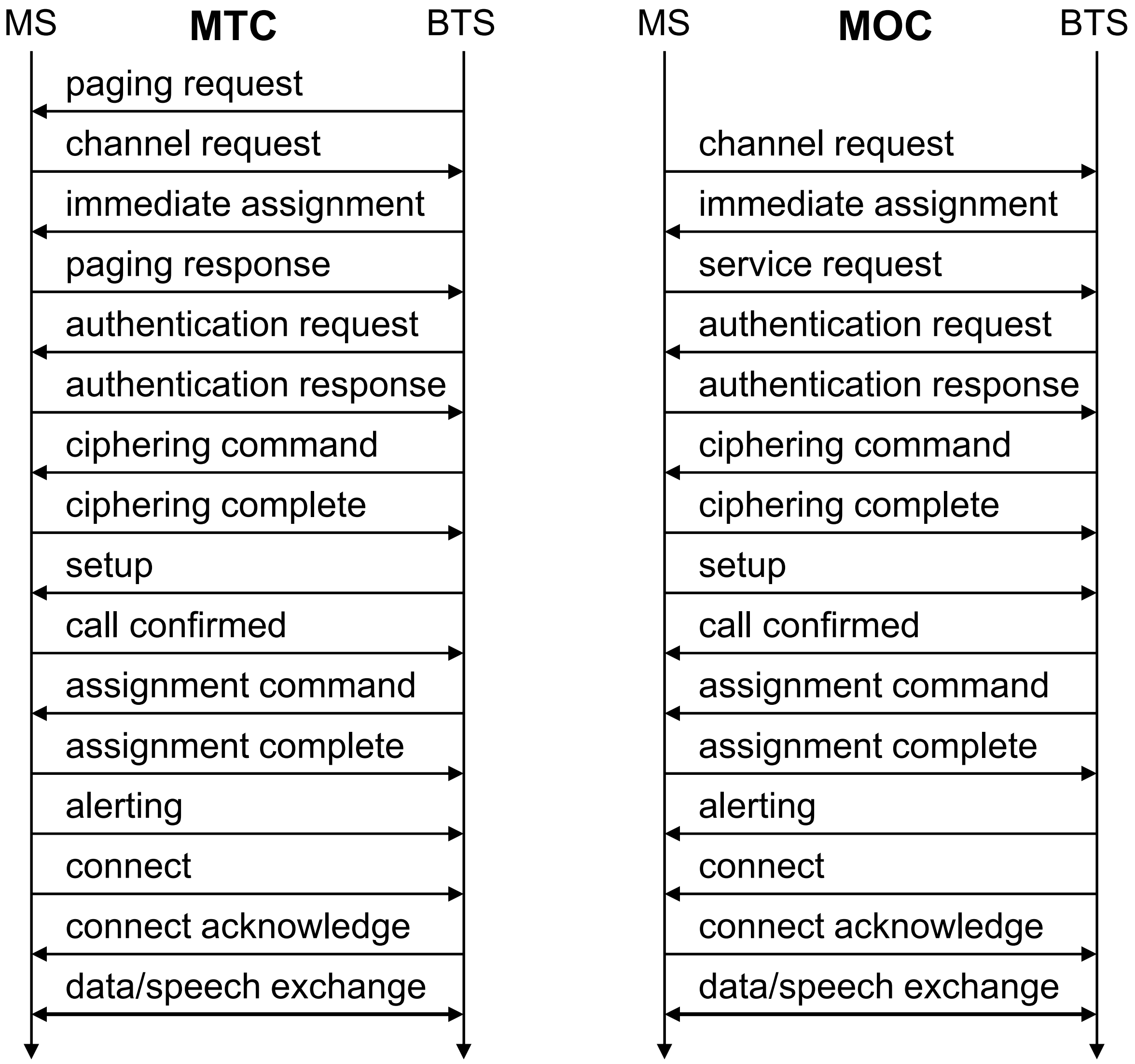


Mobile Originated Call

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



MTC/MOC



MS **MTC** BTS

paging request

channel request

immediate assignment

paging response

authentication request

authentication response

ciphering command

ciphering complete

setup

call confirmed

assignment command

assignment complete

alerting

connect

connect acknowledge

data/speech exchange

MS **MOC** BTS

channel request

immediate assignment

service request

authentication request

authentication response

ciphering command

ciphering complete

setup

call confirmed

assignment command

assignment complete

alerting

connect

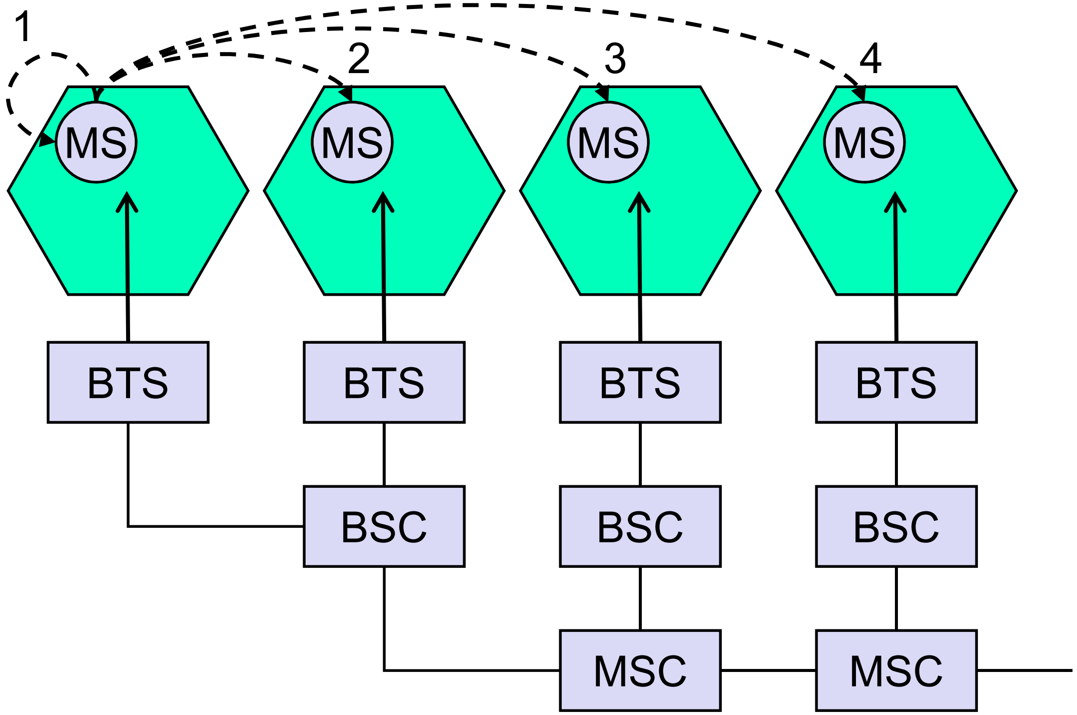
connect acknowledge

data/speech exchange

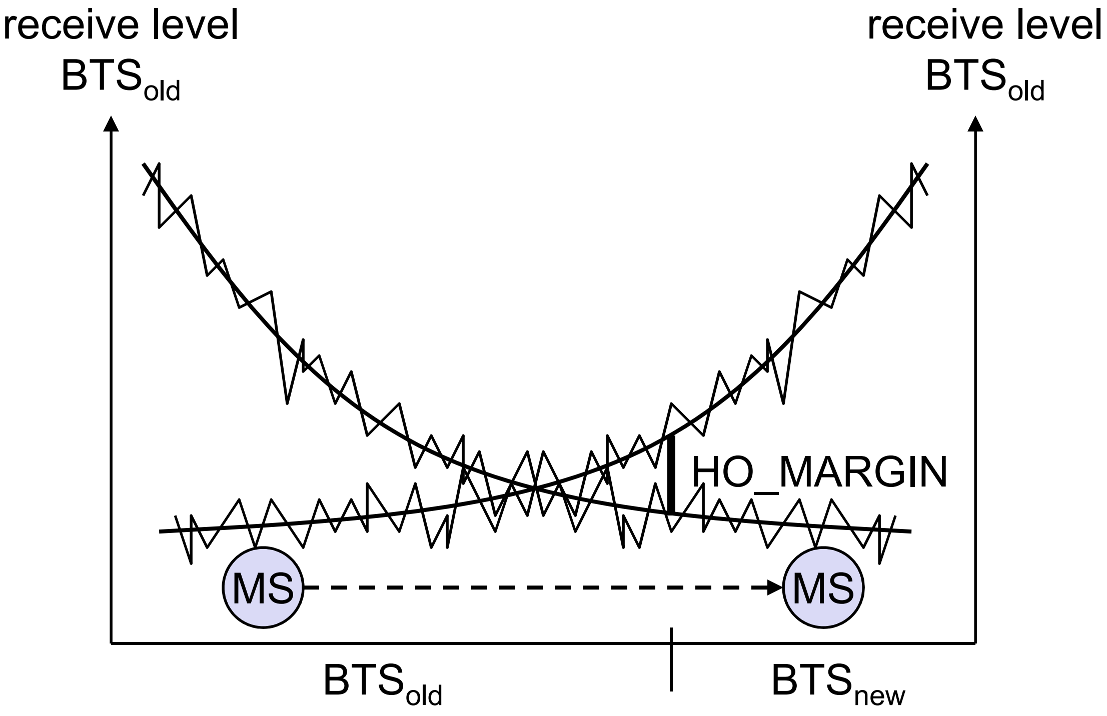
Handoffs

- GSM uses mobile assisted hand-off (MAHO). Signal strength measurements are sent to the BS from the mobile.
- The MSC decides when to do a handoff and it informs the new BS and the mobile.
- When a mobile switches to a new BS it sends a series of shortened bursts to adjust its timing (giving the bS time to calculate it and send it) and allow the new BS to synchronize its receiver to the arrival time of the messages

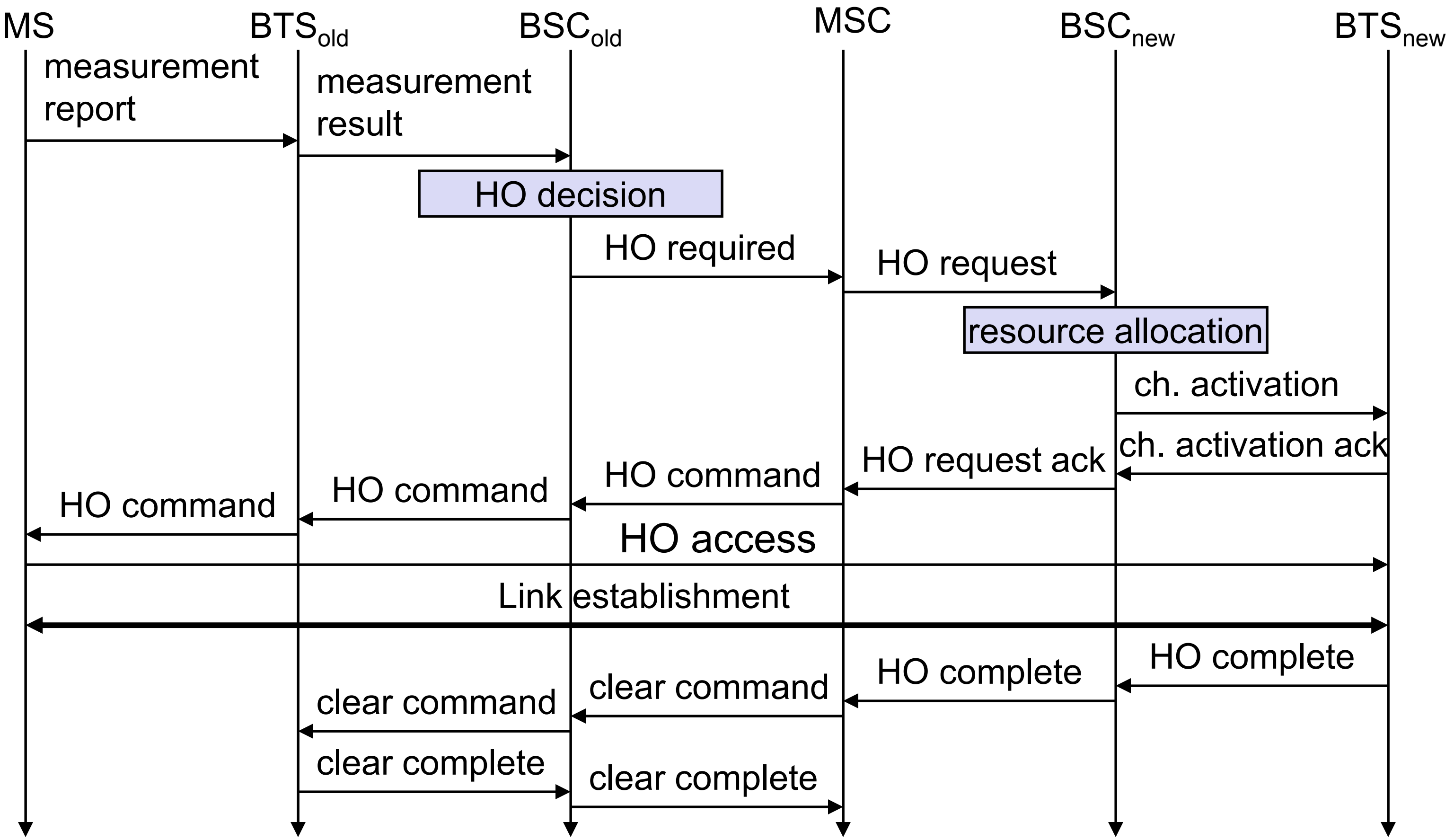
4 types of handover



Handover decision



Handover procedure

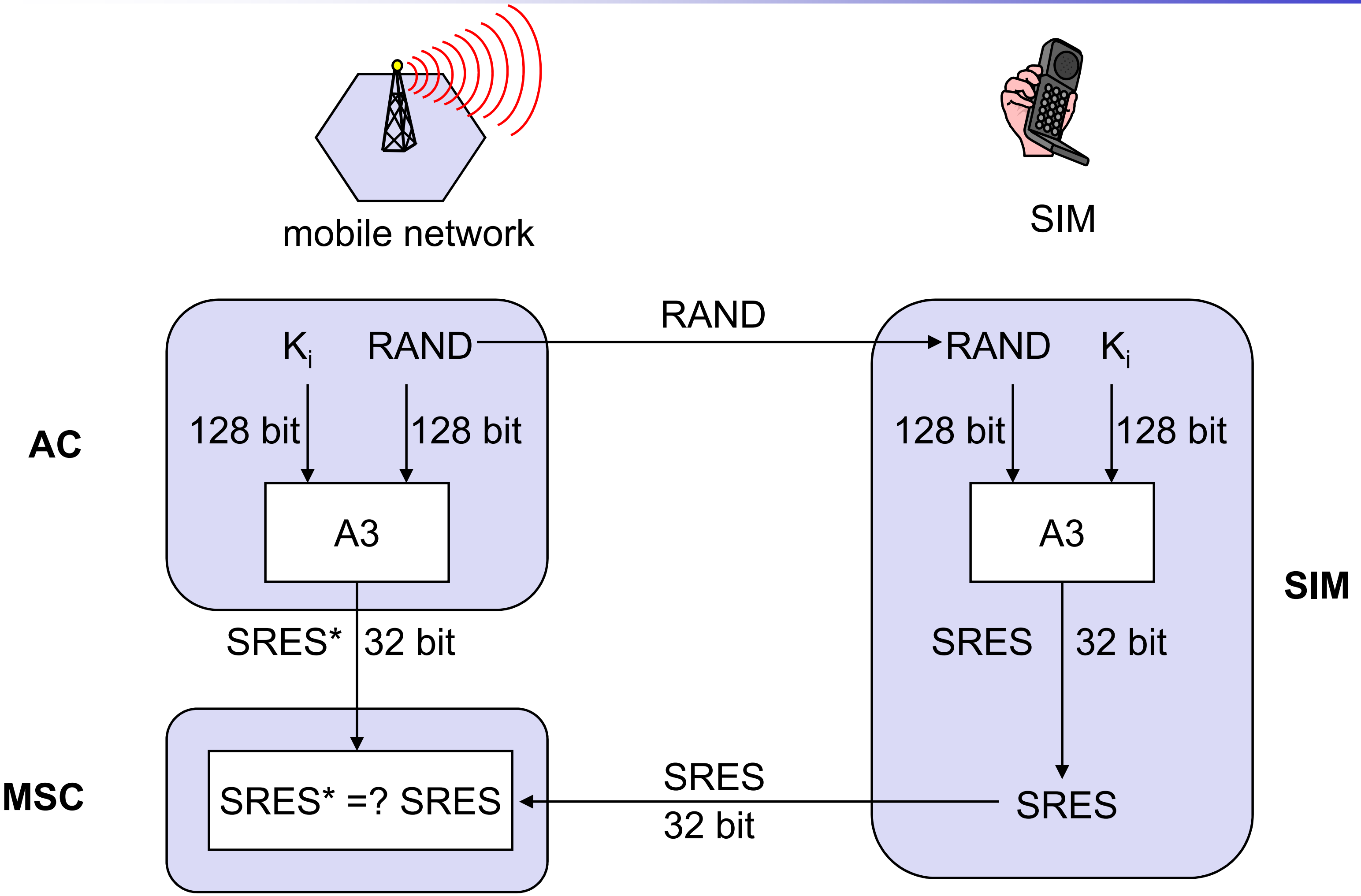


Security in GSM

- 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)**

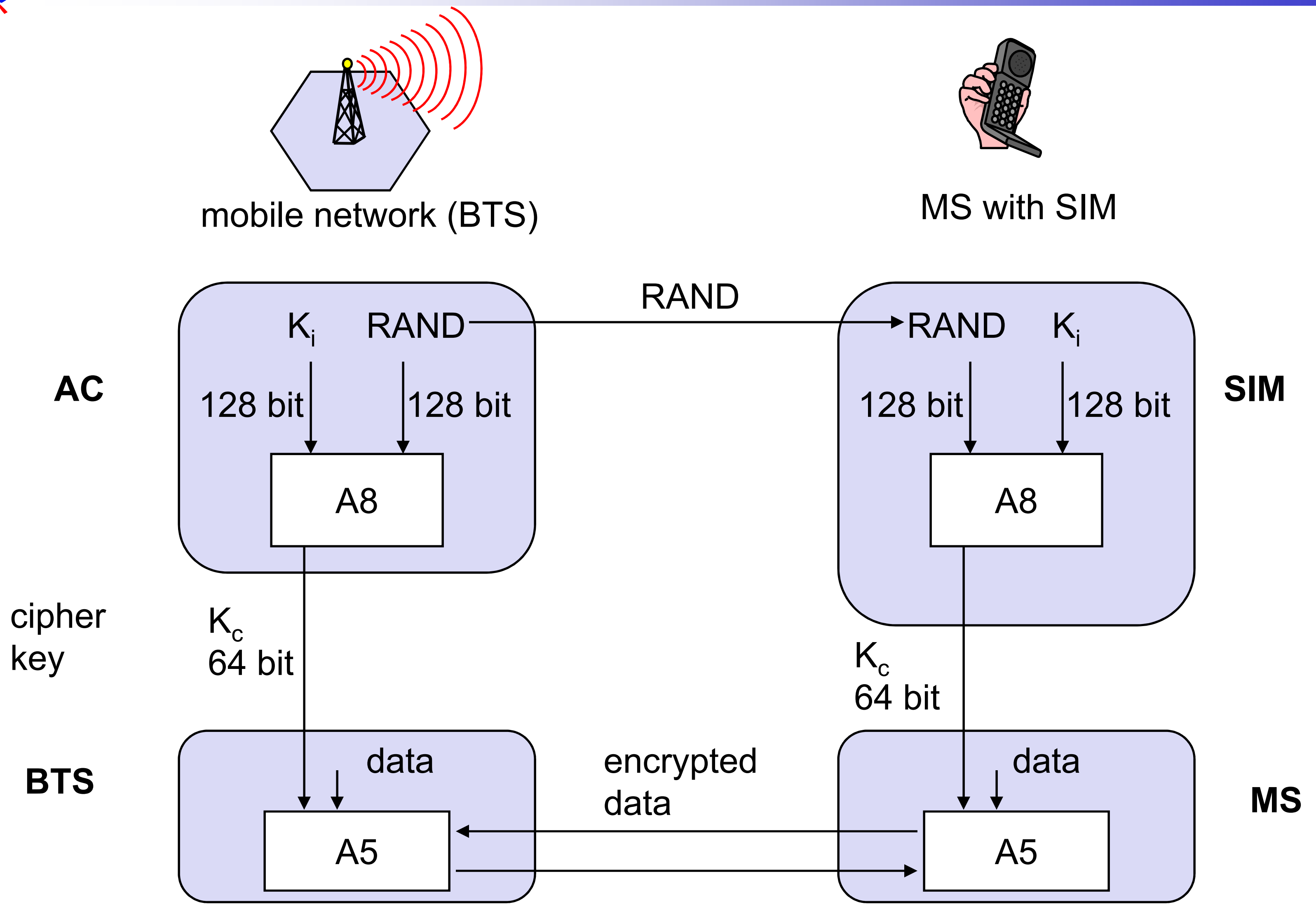
"secret":
• A3 and A8 available via the Internet
• network providers can use stronger mechanisms

GSM - authentication



K_i: individual subscriber authentication key   SRES: signed response

GSM - 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)
  - 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

AIUR [kbit/s]	TCH/F4.8	TCH/F9.6	TCH/F14.4
4.8	1		
9.6	2	1	
14.4	3		1
19.2	4	2	
28.8		3	2
38.4		4	
43.2			3
57.6			4

Data services in GSM II

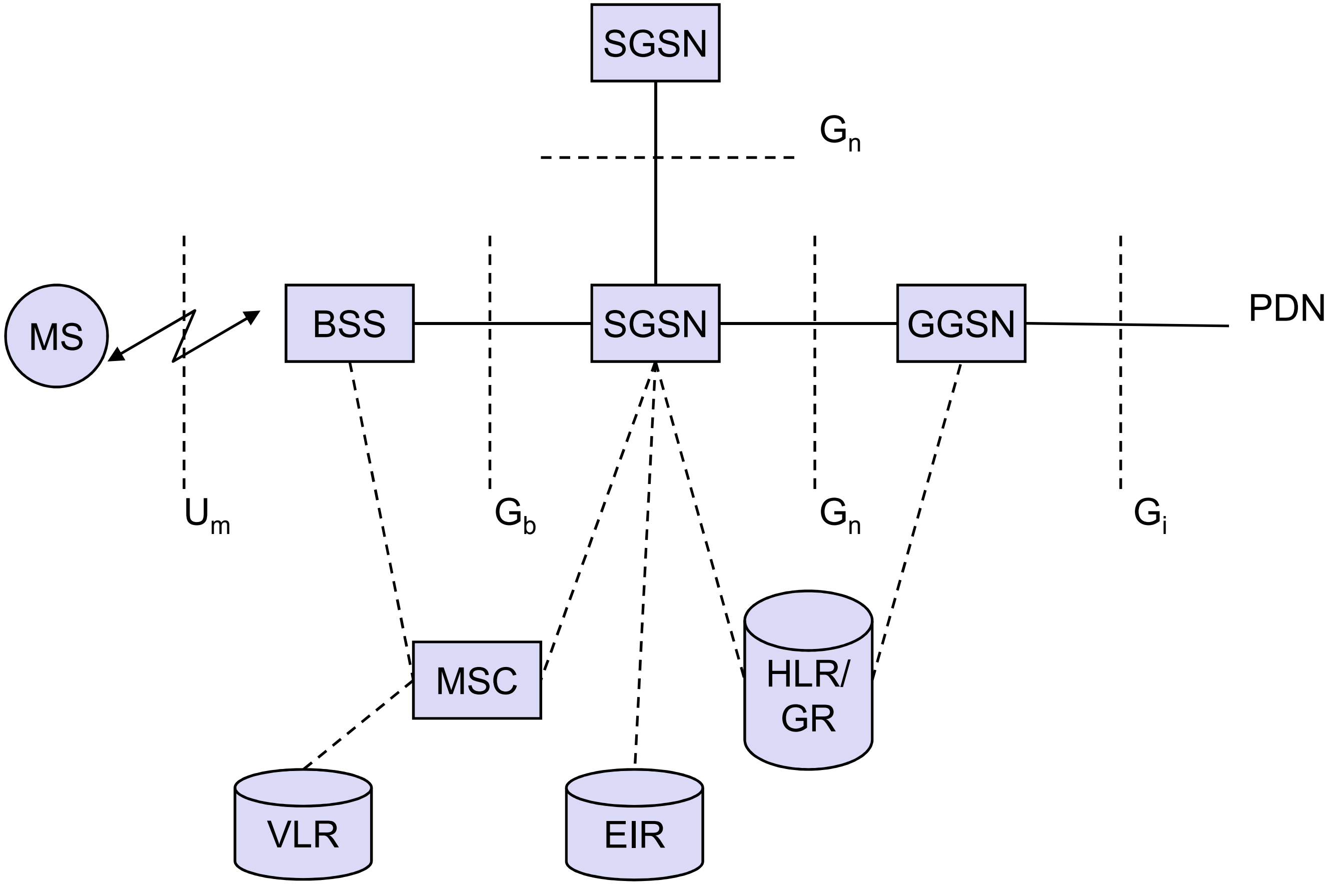
- GPRS (General Packet Radio Service)
  - packet switching
  - using free slots only if data packets ready to send (e.g., 115 kbit/s using 8 slots temporarily)
  - standardization 1998
  - advantage: one step towards UMTS, more flexible
  - disadvantage: more investment needed
- GPRS network elements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

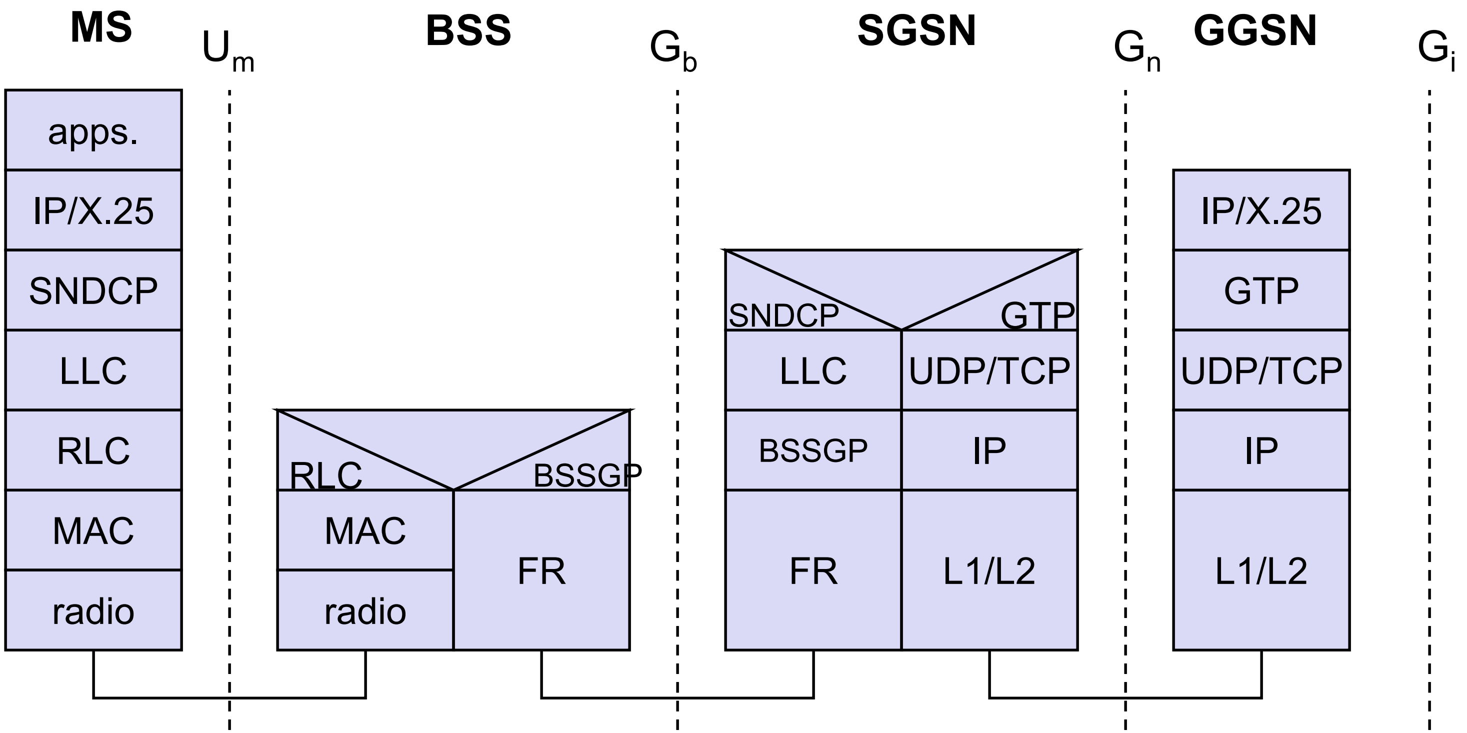
Reliability class	Lost SDU probability	Duplicate SDU probability	Out of sequence SDU probability	Corrupt SDU probability
1	10^{-9}	10^{-9}	10^{-9}	10^{-9}
2	10^{-4}	10^{-5}	10^{-5}	10^{-6}
3	10^{-2}	10^{-5}	10^{-5}	10^{-2}

Delay class	SDU size 128 byte		SDU size 1024 byte	
	mean	95 percentile	mean	95 percentile
1	< 0.5 s	< 1.5 s	< 2 s	< 7 s
2	< 5 s	< 25 s	< 15 s	< 75 s
3	< 50 s	< 250 s	< 75 s	< 375 s
4	unspecified			

GPRS architecture and interfaces



GPRS protocol architecture



IS 95

- The existing 12.5 MHz cellular bands are used to derive 10 different CDMA bands (1.25MHz per band).
- The frequency reuse factor in CDMA is 1. The channel rate is 1.2288Mbps (actually chips not bits!).
- Multipath fading is exploited in CDMA. It provides for space (path) diversity, RAKE receivers are used to combine the output of several received signals. Ofcourse fading does still occur on the individual signals but each signal is affected differently and so using several of them to make a decision improves the probability of obtaining a correct decision. This is referred to as multipath diversity combining.
  - The rake receiver at the mobile uses three correlators to receive three different signals that are spaced more than (>) .8micro secs (1 chip width) away. Signals spaced less than (<) .8microsecs cause interference and signals spaced exactly .8microsecs away will cause a maximum fade. A fourth receiver is used as a roving finger, it is used to detect new strong incoming signals. This process ensures that the RAKE receiver always uses the 3 strongest signals. At the BS all four correlators are used to receive signals (note BS use antenna diversity).

IS 95: Coding and Modulation

- 64 bit Walsh codes (proving 64 bit orthogonal codes) are used to provide 64 channels within each frequency band. They are used for spreading in the downlink. In the uplink it is used to provide orthogonal modulation but not spreading to the full 1.2288 rate.

- Besides the Walsh codes, 2 other codes are used in IS-95:
  - Long PN code:generated from a 42 bit shift register having 2^{42}-1=4.398 x 10^{12} different codes. A mask is used to overlay the codes, the mask differs from channel to channel.The chip rate is 1.2288Mcps. These codes are used for:
    - Data scrambling/encryption in the downlink
    - Data spreading and encryption in the up link
  - Short PN code: generated from a pair of 15 bit shift registers having 2^{15} - 1 = 32,767 codes. These codes are used for synchronization in the down and up links and cell identification in the down link (each cell uses one of 512 possible offsets, adjacent cells must use different offsets). The chip rate is 1.2288Mcps (i.e., not used for spreading!)

IS 95: The Channels

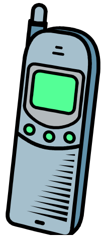
- The forward and reverse links are separated by 45MHz.
- The downlink comprises the following logical channels:
  - Pilot channel (always uses Walsh code W0)
  - Paging channel(s) (use Walsh codes W1 - W7)
  - Sync channel (always uses Walsh code W32)
  - Traffic channels (use Walsh codes W8 - W31 and W33 - W63)
- The uplink comprises the following logical channels:
  - Access channel
  - Traffic channel

IS 95: Link Protocols

- The link protocol can be summarised as follows:
  - □ Mobile acquires phase, timing, and signal strength via the pilot channel.
  - □ Mobile synchronizes via the sync channel.
  - □ Mobile gets system parameters via the paging channel.
  - □ Mobile and BS communicate over the traffic channels during a connection.
  - □ Mobile and BS communicate over the access and paging channels during system acquisition and paging.

IS 95: The different codes and their use

- The forward (downlink) channels and reverse (uplink) channels use different spreading and scrambling processes.
  - The forward channels are spread using one of 64 orthogonal Walsh functions. This provides perfect separation between the channels (in the absence of multpath!). Then, to reduce interference between mobiles that use the same Walsh function in neighboring cells, all signals in a particular cell are scrambled using the short PN sequence (cell identification) in the radio modulator. For the paging and the traffic channels, the long PN sequence is used to scramble the signal before spreading. It can also be used for encryption on the traffic channel if the mask instead of being the ESN of the mobile is a private long code exchanged during the authentication procedure.
  - The reverse channels are spread using the long PN sequence. All 64 orthogonal Walsh functions are used to provide orthogonal modulation. The stream is then scrambled using the short PN sequence for cell identification purposes.

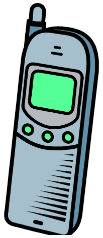


IS 95: Power Control I

- It is of paramount importance for a CDMA system.
- In order to have max. efficiency, the power received at the BS from all the mobiles must be nearly equal.
- If a terminal’s power is too low, then many bit errors will occur.
- If a terminal’s power is too high , the level of interference will go up.
- Closed loop power control at the terminals: power control information is sent to the terminal from the BS . Puncturing is used, 2 data symbols are replaced by one power control symbol (double the power). This bit either indicates a transition up or a transition down in power in 1db increments. The power bit is sent 16 times per 20ms frame (every 1.25ms)! (P_{closed})

IS 95: Power Control II

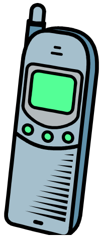
- Open loop power control at the terminals:. The mobile senses the strength of the pilot signal and can adjust its power based upon that. If signal is very strong, the assumption can be made that the mobile is very close to BS and the power should be dropped. The mobile uses P_{target} sent in the access param. msg.(P_{open})
- The transmitted power at the terminal in units of dBm is: $P_{tran}=P_{open}+P_{closed}$
- Open loop power control at the BS: the BS decreases its power level gradually and waits to hear from the mobile what the frame error rate (FER) is (power measurement report). If high then it increases its power level.



IS 95: Handoffs I

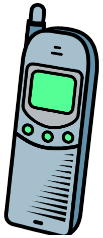
- CDMA supports two types of handoffs:
  1. hard handoff
  2. soft handoff

  A hard handoff is a break before make scenario, where prob. of dropping a call is higher. A soft handoff is a make before break scenario.
- The mobile assists in the handoff process and therefore it is referred to as Mobile Assisted Hand Off (MAHO). It reports signal measurements to the BS. The roving finger (or searcher) of the RAKE receiver is used to measure the pilot signals of neighboring BSs (neighbor list messages sent to terminals periodically). During call set-up a mobile is given a list of handoff thresholds and a list of likely new cells. The mobile keeps track of those cells that fall above the threshold and sends this information to the MSC.



IS 95: Handoffs II

- The mobile and the MSC classify the neighboring BSs to keep track of the handoff process (based upon data received from the mobile, the MSC constantly re-classifies BSs with regard to the mobile):
  - active list: contains BSs currently used for communication (contains at least one BS)
  - candidate list: contains list of BSs that could be used for communication based upon current signal strength measurements
  - neighbor list: contains a list of BSs that could soon be promoted to candidate list
  - remaining list: all other BSs that do not qualify
- The MSC, when it moves a BS from the candidate list into the active list, will direct that BS to serve the terminal. It informs both the new BS and the mobile and assigns a forward channel number (Walsh code) for communication (on condition there is one available!).



IS 95: Handoffs III

- Soft handoffs consist of the mobile being served by two BSs. That means that:
  1. A mobile receives the signal from two BSs simultaneously. That is possible because an MS always receives 4 signals (RAKE receiver - one correlator is used to receive the signal from a different BS)
  2. The signal from the mobile is received by two BSs. This is possible as a CDMA channel simply consists of a transmission by the mobile using its ESN to identify itself on the reverse channel and only requires a correlator at the BS to be used to receive the signal.
- Soft handoffs also eliminate the ping pong effect (i.e., when traveling along the boundary of two cells and switching back and forth between two BSs). The mobile is being served by two BSs and does not have to switch BSs until absolutely necessary!
- The handoff process is also unique in that the mobile initiates the hand off. The MS analyze the measurements and inform the MSC when a handoff might be necessary. (If one BS's signal strength becomes much higher than the other).

IS 95: Handoffs IV

- The handoff process is controlled by the MSC. When a handoff finally occurs all three MS correlators are switched over to the new cell and used as a RAKE receiver again, the connection to the current BS is cutoff and the new BS becomes the current BS.
- In summary: the handoff process is executed in three steps:
  - mobile is in communication with original (i.e., current) BS.
  - mobile is in communication with both the current cell and the new cell.
  - mobile is in communication with the new cell only (which becomes the current cell).