GSM: Global System for Mobile Communication

Dr Yousef Dama

An-Najah National University

GSM frequency bands (examples)

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

- Additionally: GSM 400 (also named GSM 450 or GSM 480 at 450-458/460-468 or 479-486/489-496 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

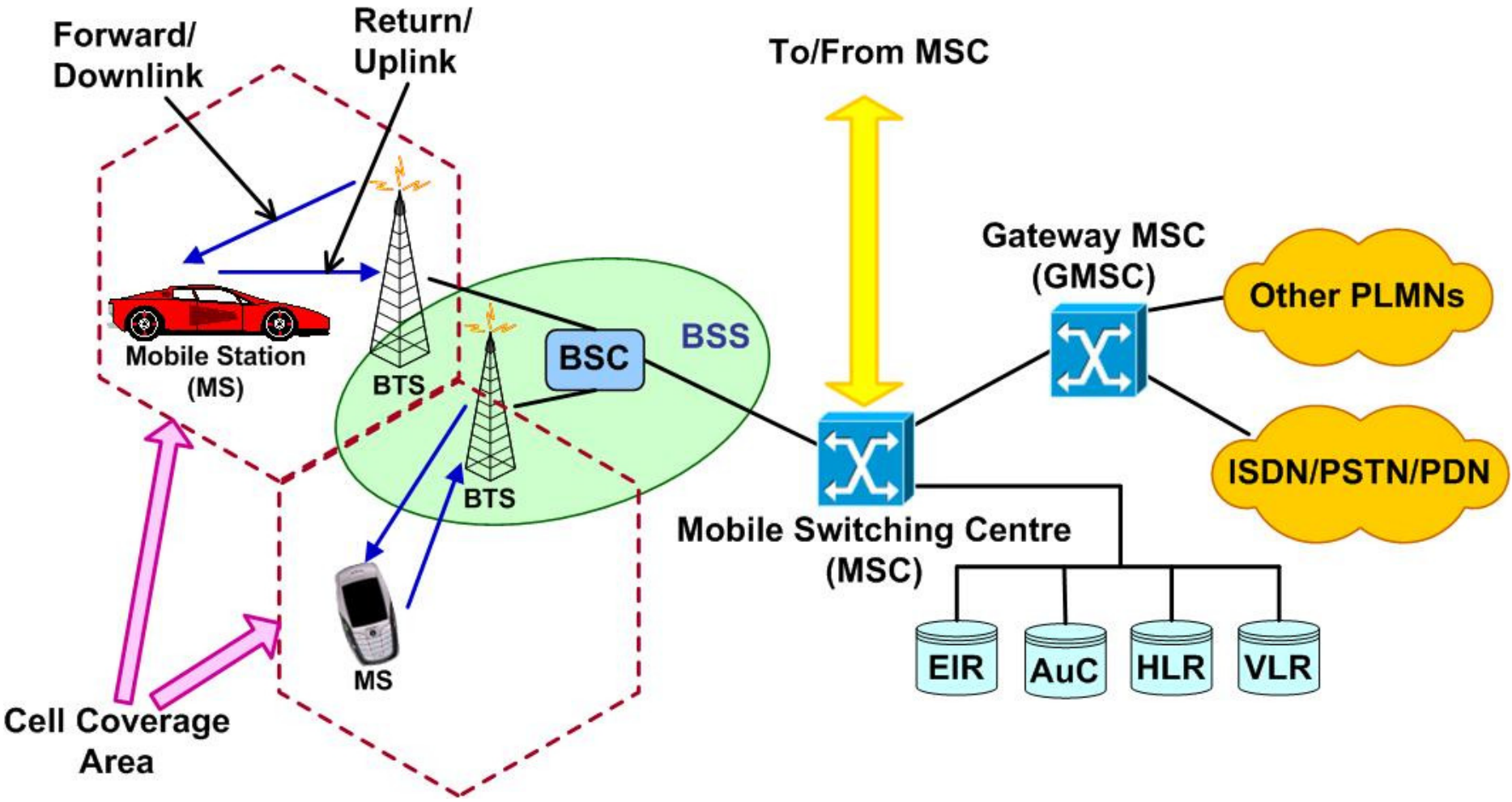
Network Components

Base Station Subsystem

Network Subsystem

Operations and Maintenance Subsystem

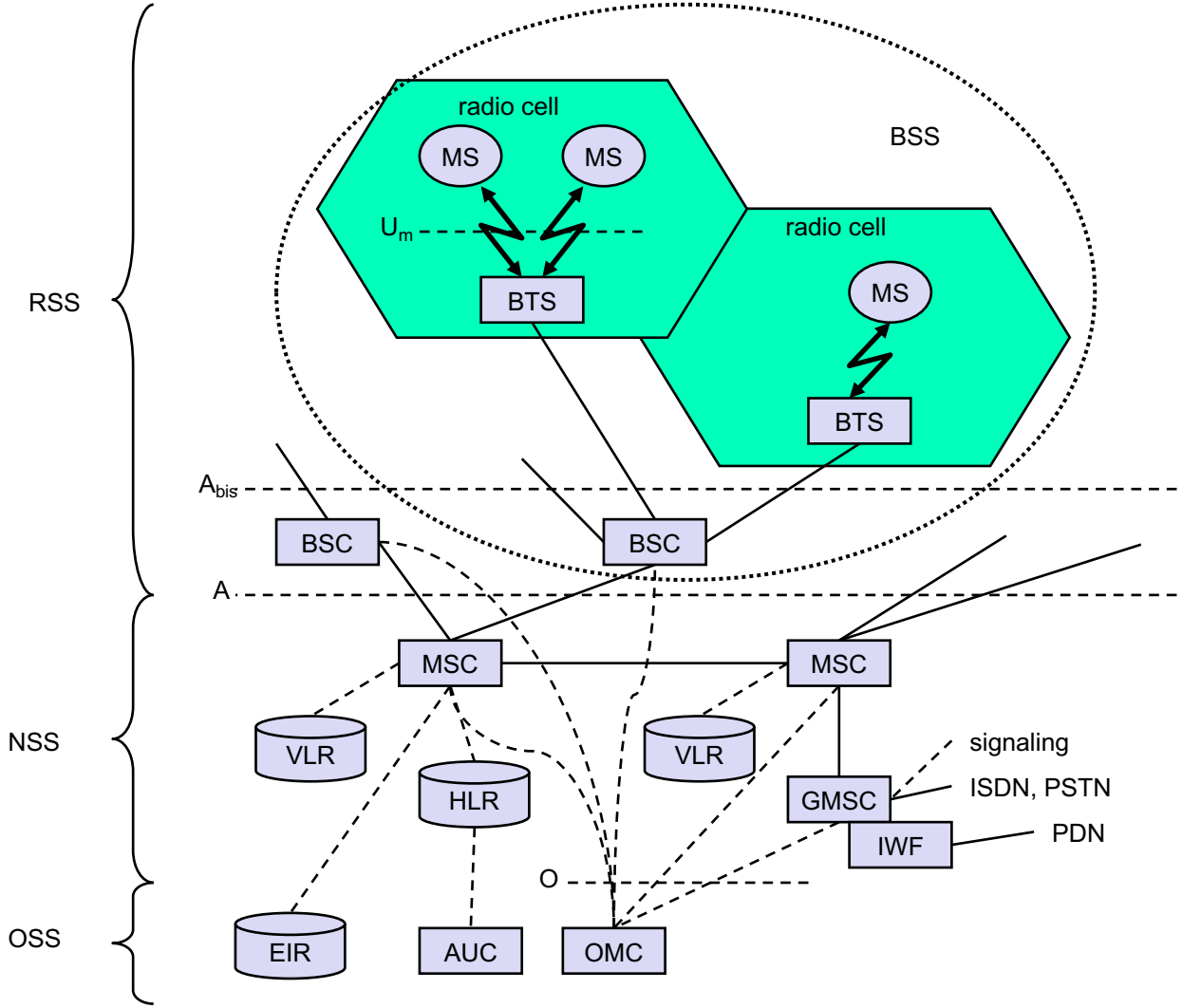
GSM Cellular Network Architecture



Architecture of the GSM system

- 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 (**R**adio **S**ubsystem): covers all radio aspects
    - Base station subsystem
  - NSS (**N**etwork and **S**witching **S**ubsystem): call forwarding, handover, switching
  - OSS (**O**peration **S**ubsystem): management of the network

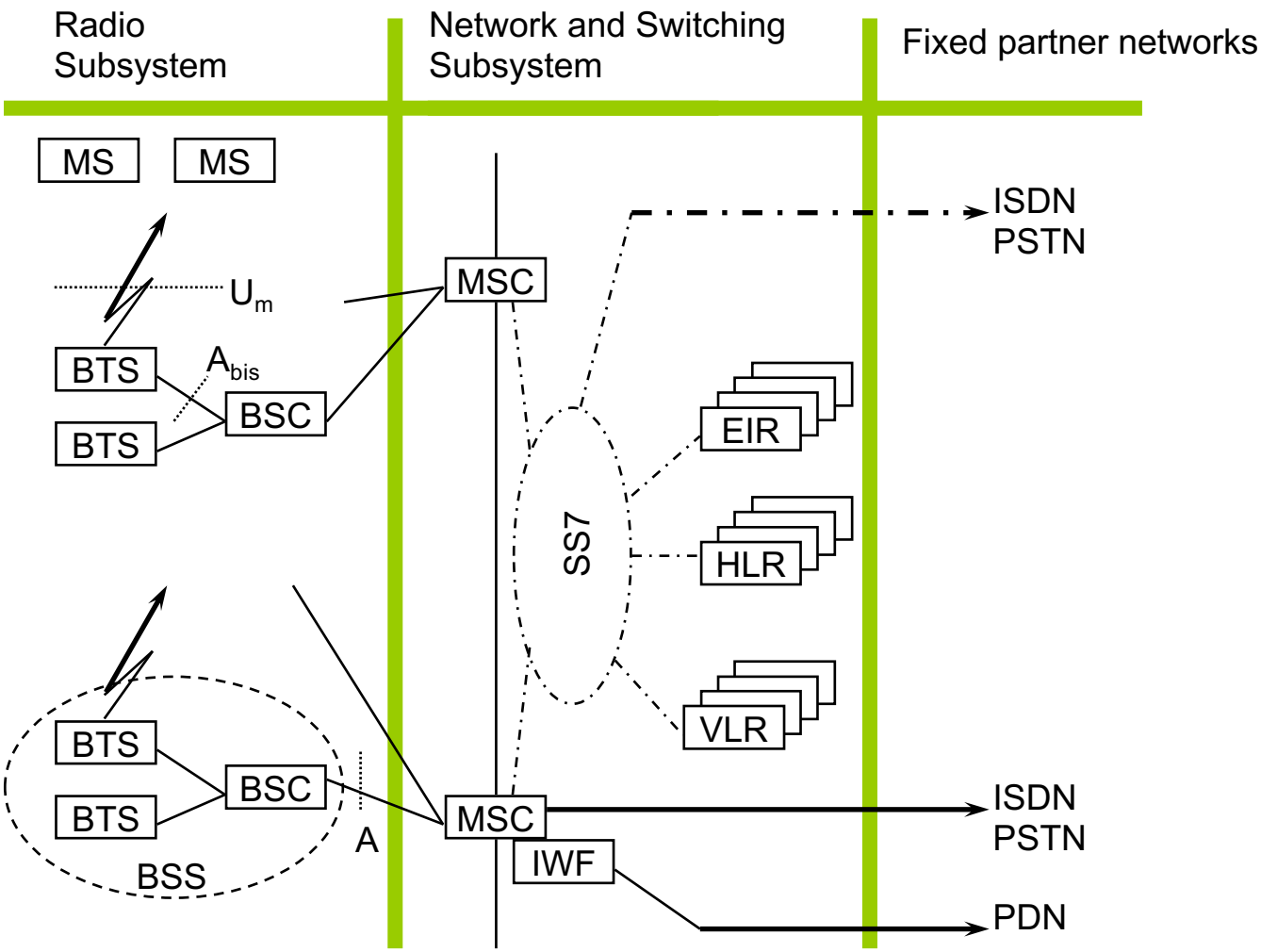
GSM: Elements and Interfaces



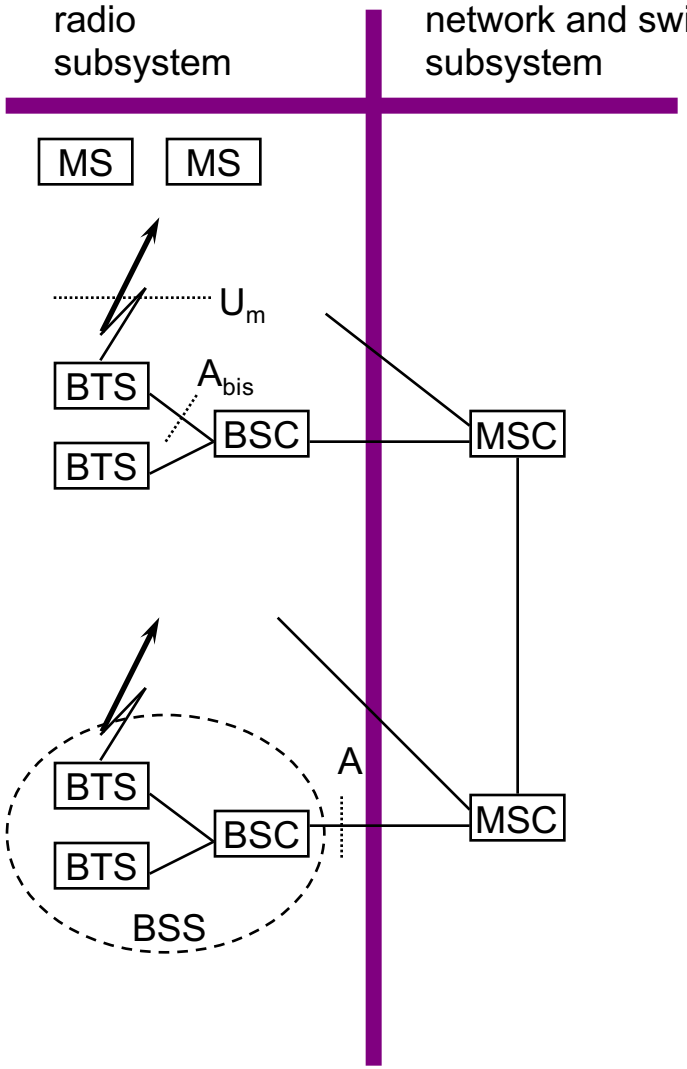
Typical Mobile operator

- One to ten MSC per 1 M subscribers
- Ten to one hundred BSC per MSC
- Thousands of BTS per 1 M subscribers
- BSC serves up to 40 BTSs

GSM: System Architecture



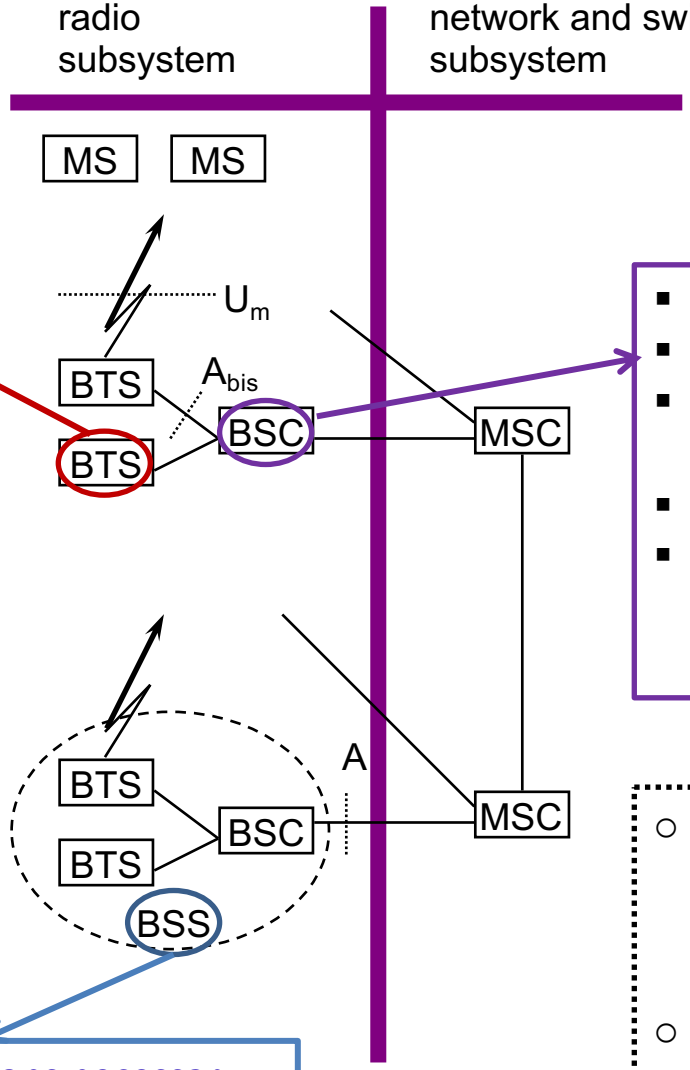
Radio subsystem



- 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

Radio subsystem

- The Radio Subsystem (RSS) comprises the cellular mobile network up to the switching centers
- Components
  - Base Station Subsystem (BSS):
  - A GSM network comprises many BTSs, each controlled by a base station controller (BSC).
  - The BSS performs all functions necessary to maintain radio connections to an MS.
    - Base Transceiver Station (BTS): radio components including sender, receiver, antenna, connected to MS via the U_m interface and to the BSC via the A_{bis}
    - Base Station Controller (BSC): The BSC basically manages the BTSs. It reserves radio frequencies, handles the handover from one BTS to another within the BSS, and performs paging of the MS. Also it multiplexes the radio channels onto the fixed network connections at the A interface
  - Mobile Stations (MS)



- antennas, signal processing, amplifiers necessary for radio transmission.
- A BTS can form a radio cell or, using sectorized antennas, several cells
- Connected to MS via the **U_m interface**
- to the BSC via the **A_{bis} interface**

- Manages the BTSs.
- It reserves radio frequencies.
- Handles the handover from one BTS to another within the BSS.
- Performs paging of the MS.
- Multiplexes the radio channels onto the fixed network connections at the A interface

- The U_m interface contains all the mechanisms necessary for wireless transmission (TDMA, FDMA etc.)
- The A_{bis} interface consists of 16 or 64 kbit/s connections

Performs all functions necessary to maintain radio connections to an MS. Provides the link between the MS and the MSC

BTS Coverage

➔Either

- Omni-directional
  - High output mainly associated with a sparsely populated region
- Sectored radio cell
  - BTS supplies up to 3 radio cells in 120º sectors
- Densely populated areas use combination of both
  - Omni-directional cell acts as an umbrella for fast moving vehicles and for filling in gaps
  - Known as hierarchical cell structure

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

Functions	BTS	BSC
Management of radio channels		X
Frequency hopping (FH)	X	X
Management of terrestrial channels		X
Mapping of terrestrial onto radio channels		X
Channel coding and decoding	X	
Rate adaptation	X	
Encryption and decryption	X	X
Paging	X	X
Uplink signal measurements	X	
Traffic measurement		X
Authentication		X
Location registry, location update		X
Handover management		X

Mobile Stations (MS)

- The MS comprises all User Equipment (UE) and software needed for communication with a GSM network.
- MS consists of user independent hard- and software and of the **subscriber identity module (SIM).**
- MS can be identified via the **international mobile equipment identity (IMEI)**, a user can personalize any MS using his or her SIM.
- The SIM card contains many identifiers and tables, such as,
  - Serial number,
  - A list of subscribed services,
  - A **personal identity number (PIN)**,
  - A **PIN unblocking key (PUK)**,
  - **Subscriber authentication key K_i,** used to authenticate the SIM card
  - The **international mobile subscriber identity (IMSI),** This number identifies the **MS subscriber**.

- The MS stores dynamic information while logged onto the GSM system, such as,
  - the **cipher key K_c ,**
  - the location information consisting of a **temporary mobile subscriber identity (TMSI).** This number identifies the subscriber, it is periodically changed by the system management to protect the subscriber from being identified by someone attempting to monitor the radio interface.
  - The **location area identification (LAI)**. Identifies the current location of the subscriber.
  - **Mobile Station International Services Digital Network (MSISDN).** This is the telephone number of the mobile subscriber. It is comprised of a country code, a network code and a subscriber number.

International mobile subscriber identity (IMSI)

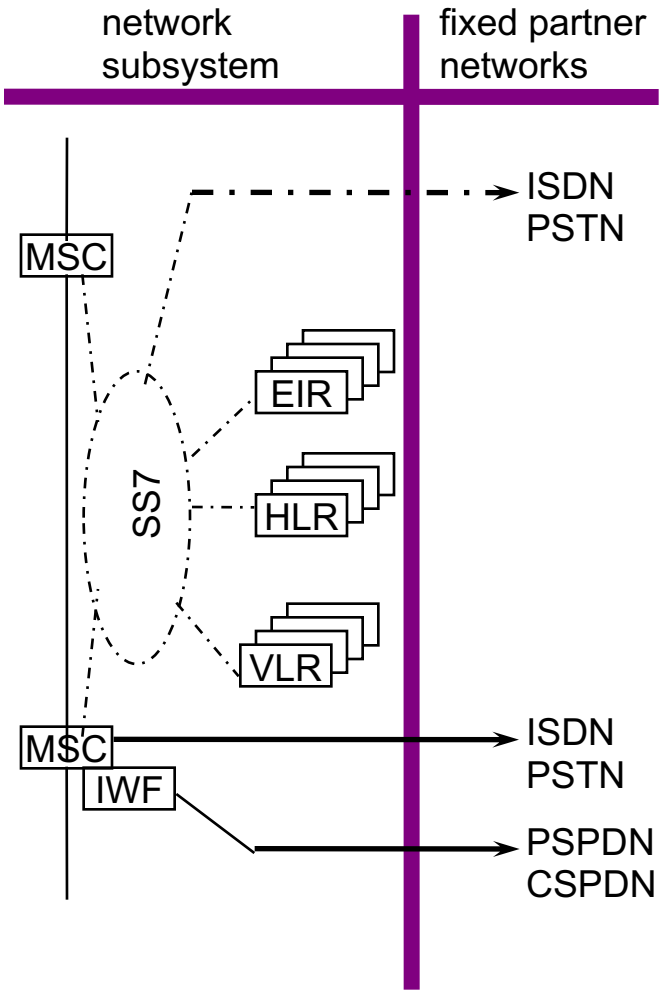
- **Each registered** user is uniquely identified by its IMSI. It is stored in the subscriber SIM. A mobile station can only be operated if a SIM with a valid IMSI is inserted into equipment with a valid IMEI.
- **There are following parts of an IMSI:**
  - **Mobile Country Code (MCC):** 3 decimal places, internationally standardized. (JAWWAL 425, WATANIYA 425)
  - **Mobile Network Code (MNC):** 2 decimal places, for unique identification of mobile network within the country. (JAWWAL 05, WATANIYA 06)
  - **Mobile Subscriber Identification Number (MSIN):** Maximum 10 decimal places, identification number of the subscriber in the home mobile network

Mobile Subscriber ISDN Number (MSISDN):

- The *real telephone number* of a mobile station is the mobile subscriber ISDN number (MSISDN). It is assigned to the subscriber (his or her SIM, respectively), such that a mobile station set can have several MSISDNs depending on the SIM.

- The MSISDN categories follow the international ISDN number plan and therefore have the following structure:
- **Country Code (CC) :** Up to 3 decimal places.
- **National Destination Code (NDC):** Typically 2-3 decimal places.
- **Subscriber Number (SN):** Maximum 10 decimal places.

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)

- Signalling System 7 (SS7) is an **international telecommunications standard that defines how network elements in a public switched telephone network (PSTN) exchange information over a digital signalling network.**
- SS7 consists of a set of reserved or dedicated channels known as signalling links. i.e. control channels
- **SS7 is used for these and other services:**

1. Setting up and managing the connection for a call
2. Tearing down the connection when the call is complete
3. Billing
4. Managing call forwarding and number display, three-way calling, and other Intelligent Network (IN) services
5. Toll-free (800 and 888) and toll (900) calls
6. Wireless as well as wireline call service including mobile telephone subscriber authentication and roaming

Network and switching subsystem (NSS)

- NSS is the main component of the public mobile network GSM
  - connects the wireless network with standard public networks.
  - performs handovers between different BSSs.
  - comprises functions for worldwide localization of users.
  - supports charging, accounting, and roaming of users between different providers in different countries.
- **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
- The MSC (mobile services 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

– A Gateway MSC (GMSC):

- Delivers calls between mobile networks and fixed networks (e.g. ISTN, ISDN, etc.)
- Performs the routing function to the actual location of the MS
- Often implemented in the same machines as the MSC.

– VLR & HLR Functionality

➢ Home Location Register (HLR)

- The HLR is the reference database for subscriber parameters
- Network operator registers customer data (central master database containing user data)
- Data made available to VLR in which customer is found, e.g. access rights
- VLR informs HLR of location of customer
- Location update occurs when a mobile moves from one location area to another
- permanent and semi-permanent data of all subscribers assigned to the HLR (one provider can have several HLRs)

➢ Visitor Location Register (HLR)

- The VLR contains a copy of most of the data stored at the HLR.
- It is, however, temporary data which exists for only as long as the subscriber is “active” in the particular area covered by the VLR.
- The VLR database will therefore contain some duplicate data as well as more precise data relevant to the subscriber remaining within the VLR coverage.
- The VLR provides a local database for the subscriber wherever they are physically located within a PLMN.

➢ The additional data stored in the VLR is listed below:

- Mobile status (busy/free/no answer etc.).
- Location Area Identity (LAI).
- Temporary Mobile Subscriber Identity (TMSI).
- Mobile Station Roaming Number (MSRN).

❑Location Area Identity

- Cells within the Public Land Mobile Network (PLMN) are grouped together into geographical areas.
- Each area is assigned a Location Area Identity (LAI), a location area may typically contain 30 cells.
- Each VLR controls several LAIs and as a subscriber moves from one LAI to another, the LAI is updated in the VLR.
- As the subscriber moves from one VLR to another, the VLR address is updated at the HLR.

❑Temporary Mobile Subscriber Identity (TMSI)

- The VLR controls the allocation of new Temporary Mobile Subscriber Identity (TMSI) numbers and notifies them to the HLR.
- The TMSI will be updated frequently, this makes it very difficult for the call to be traced and therefore provides a high degree of security for the subscriber.
- The TMSI may be updated in any of the following situations:
    - Call setup.
    - On entry to a new LAI.
    - On entry to a new VLR.

❑Mobile Subscriber Roaming Number

- As a subscriber may wish to operate outside its “home” system at some time, the VLR can also allocate a Mobile Station Roaming Number (MSRN).
- This number is assigned from a list of numbers held at the VLR (MSC).
- The MSRN is then used to route the call to the MSC which controls the base station in the MSs current location.
- The database in the VLR can be accessed by the IMSI, the TMSI or the MSRN.
- Typically there will be one VLR per MSC.

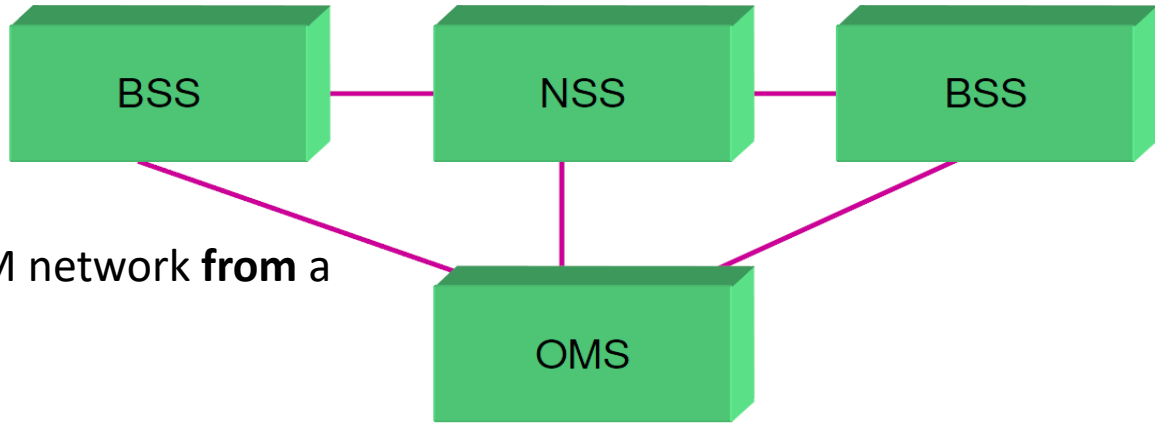
Mobile Switching Center (MSC) Databases

- Home location register (HLR) database – stores information about each subscriber that belongs to it
- Visitor location register (VLR) database – maintains information about subscribers currently physically in the region
- Authentication center database (AuC) – used for authentication activities, holds encryption keys
- Equipment identity register database (EIR) – keeps track of the type of equipment that exists at the mobile station

Operation subsystem

- The OSS (Operation Subsystem) enables centralized operation, management, and maintenance of all GSM subsystems
- Components
  - Authentication Center (AUC)
    - Provides protection against unauthorised access
    - Checks International Mobile Subscriber Identity (IMSI) information stored on the SIM for correspondence with own register Identical data results in approval to enter the network, otherwise access is disabled
  - Equipment Identity Register (EIR)
    - Optional implementation by network operator
    - 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



❑ Monitors and controls the GSM network **from** a central point

➢ **Tasks**

❖ Fault Management System (Analyses alarms from BSS elements)

❖ Configuration Management System (Installs software, changes operation parameters, manages hardware inventory list)

❖ Software Management System (Feeds in new software and manages software inventory list)

Equipment Identity Register (EIR)

- The EIR contains a centralized database for validating the International Mobile Equipment Identity (IMEI).
- This database is concerned solely with MS equipment and not with the subscriber who is using it to make or receive a call.
- The EIR database consists of lists of IMEIs (or ranges of IMEIs) organized as follows:
- **White List** Contains those IMEIs which are known to have been assigned to valid MS equipment.
- **Black List** Contains IMEIs of MS which have been reported stolen or which are to be denied service for some other reason.
- **Grey List** Contains IMEIs of MS which have problems (for example, faulty software).
- The EIR database is remotely accessed by the MSCs in the network and can also be accessed by an MSC in a different PLMN.

Radio Components

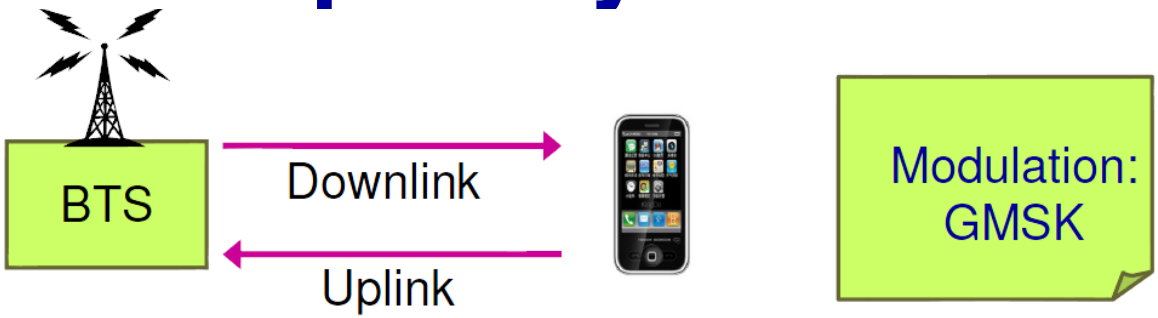
Channel Structure

Frame Format

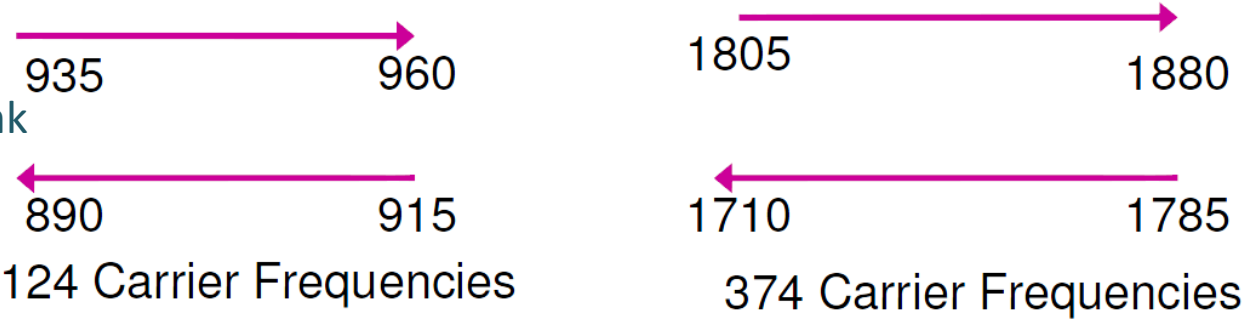
Channel Types

Um Interface: Operating Frequency

GSM implements SDMA using cells with BTS and assigns an MS to a BTS



FDD is used to separate downlink and uplink

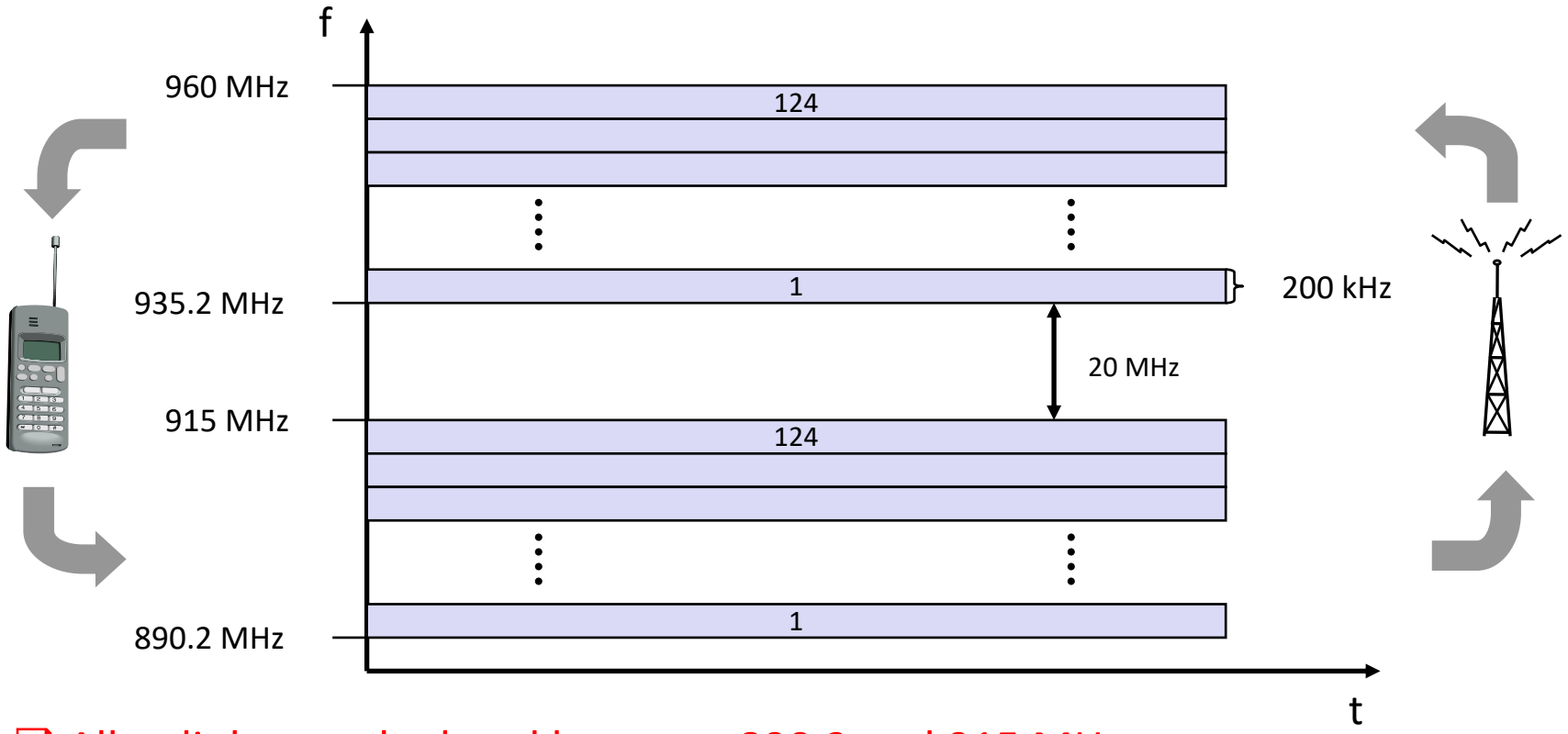


- 32 channels are reserved for organizational data.
- the remaining 90 are used for customers.
- Each BTS then manages a single channel for organizational data and, e.g., up to 10 channels for user data.

GSM Radio interface

- Frequency allocation
- Two frequency bands, of 25 MHz each one, have been allocated for the GSM system:
- The band 890-915 MHz has been allocated for the uplink direction (transmitting from the mobile station to the base station).
- The band 935-960 MHz has been allocated for the downlink direction (transmitting from the base station to the mobile station).

FDD/FDMA - general scheme, example GSM



- All uplinks use the band between 890.2 and 915 MHz.
- All downlinks use 935.2 to 960 MHz.
- Up- and downlink have a fixed relation

If the uplink frequency for a certain channel n is

$$f_u = 890\ MHz + n \times 0.2\ MHz$$

the downlink frequency is

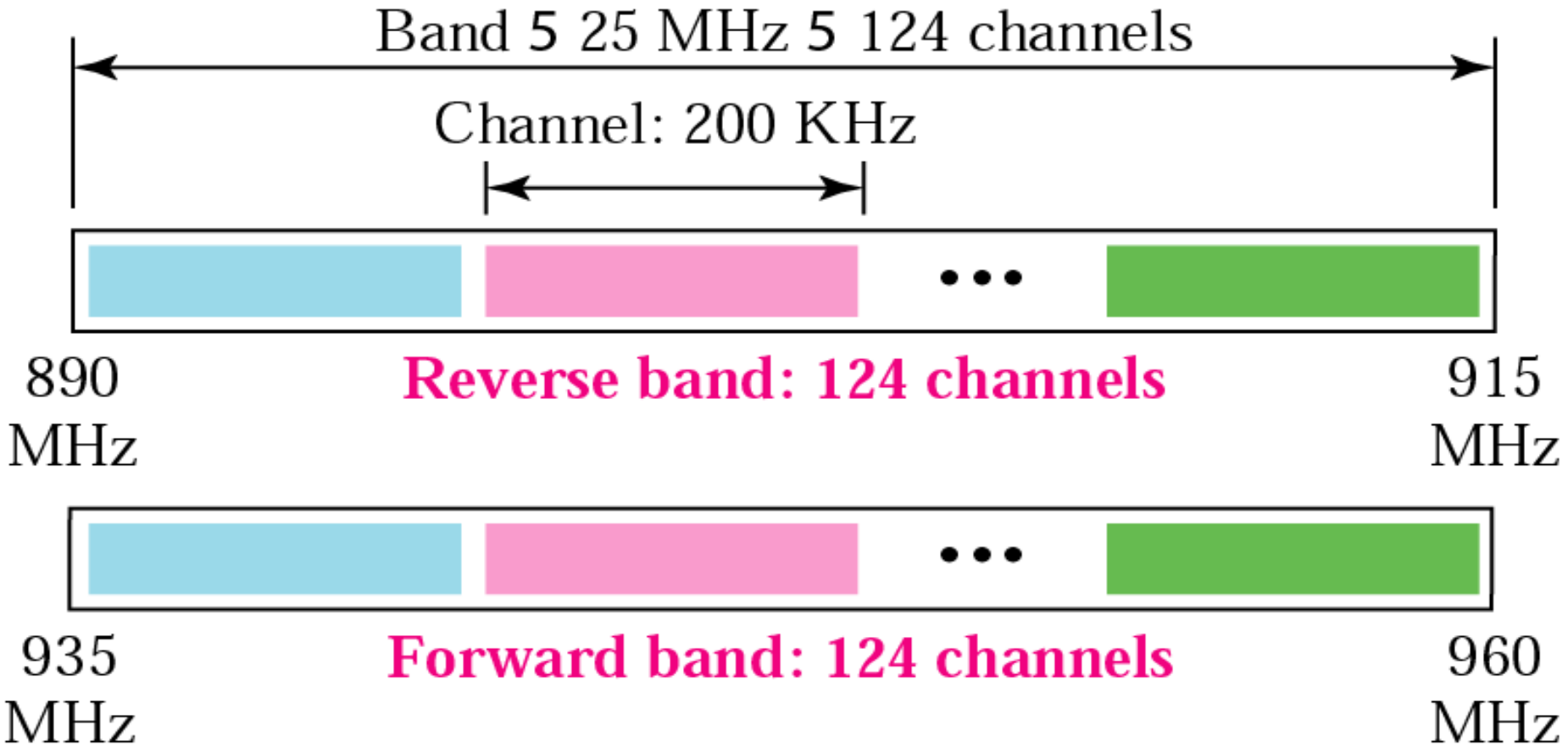
$$f_d = f_u + 45\ MHz$$

i.e.,

$$f_d = 935\ MHz + n \times 0.2\ MHz$$

- The base station selects the channel.
- Each channel (uplink and downlink) has a bandwidth of 200 kHz.
- 124 channels per direction are available at 900 MHz

GSM bands

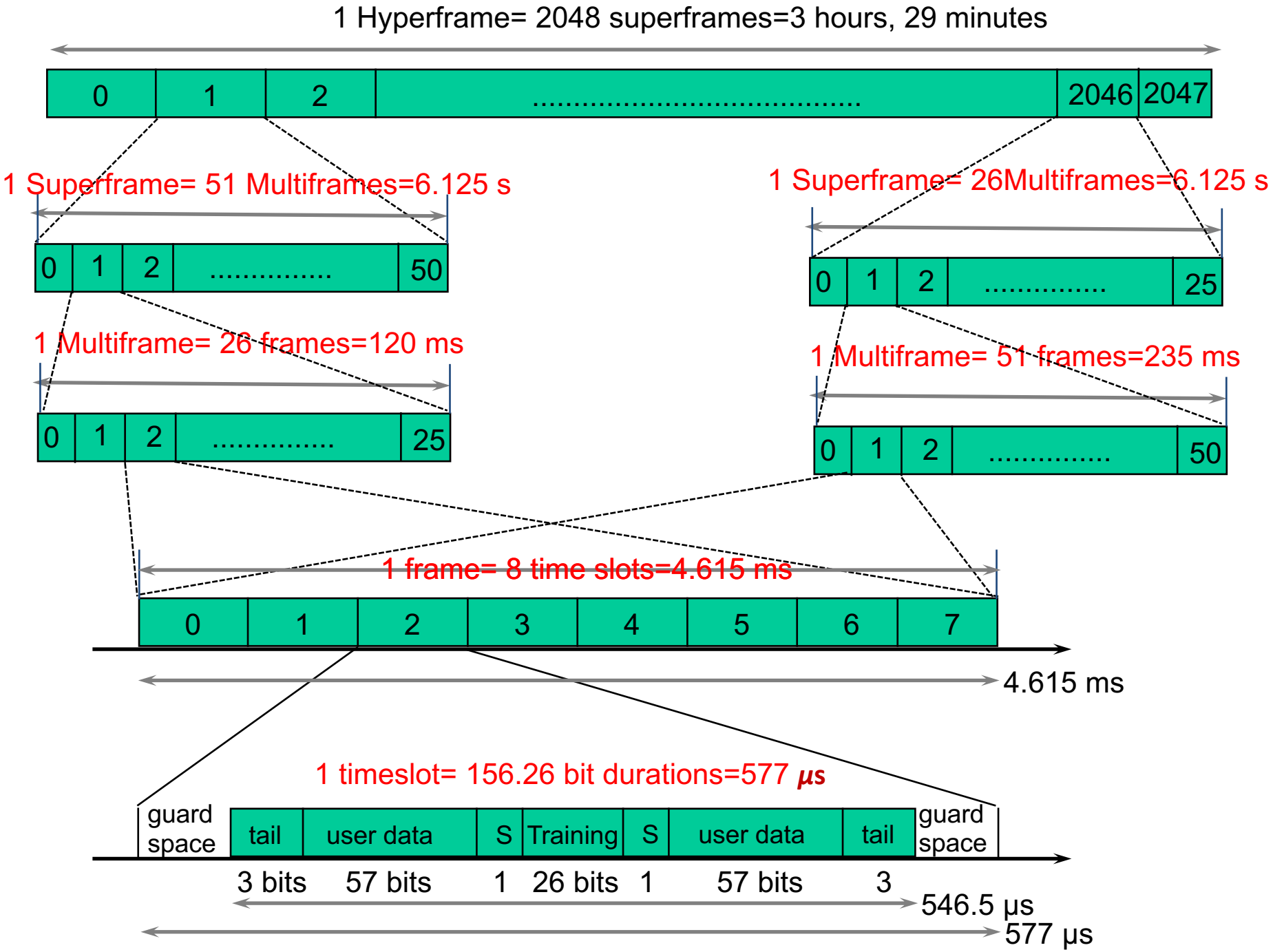

Band 5 25 MHz 5 124 channels
Channel: 200 KHz
890 MHz
Reverse band: 124 channels
915 MHz
935 MHz
Forward band: 124 channels
960 MHz

- In GSM, a 25 MHz frequency band is divided, using a **FDMA**, into 124 carrier frequencies spaced one from each other by a 200 kHz frequency band.
- Each carrier frequency is then divided in time using a **TDMA**. This scheme splits the radio channel into 8 bursts.
- A burst is the unit of time in a TDMA system, and it lasts approximately 0.577 ms.
- A TDMA frame is formed with 8 bursts and lasts, consequently, 4.615 ms.
- Each of the eight bursts, that form a TDMA frame, are then assigned to a single user.

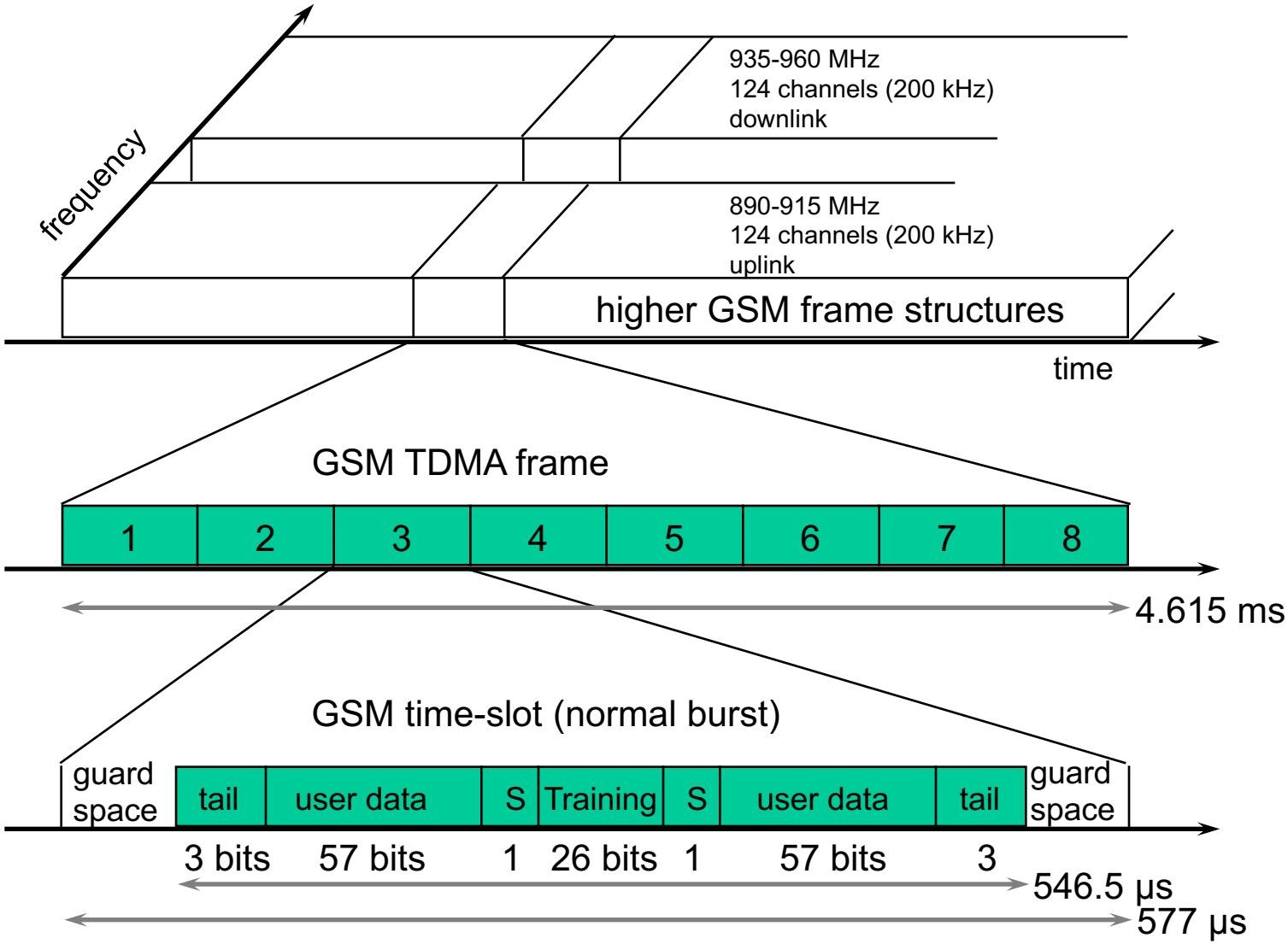
GSM - TDMA/FDMA

- Each of the 248 channels is additionally separated in time via a **GSM TDMA frame**
- Each 200 kHz carrier is **subdivided** into **frames** that are repeated continuously
- The **duration of a frame** is 4.615 ms
- A frame is again subdivided into **8 GSM time slots**, where each slot represents a physical TDM channel and **lasts for 577 μs.**
- Each TDM channel occupies the 200 kHz carrier for 577 μs every 4.615 ms.
- The burst is only 546.5 μs long and contains 148 bits.
- The remaining 30.5 μs are used as **guard space** to avoid overlapping with other bursts due to different path delays and to give the transmitter time to turn on and off.
- Filling the whole slot with data allows for the transmission of 156.25 bit within 577 μs.
- Each physical TDM channel has a raw data rate of about 33.8 kbit/s,

- The **GSM frame structure** is designated as hyperframe, superframe, multiframe and frame. The minimum unit being frame (or TDMA frame) is made of 8 time slots.
- One GSM hyperframe composed of 2048 superframes.
- Each GSM superframe composed of multiframes (either 26 or 51)
- Each GSM multiframe composed of frames (either 51 or 26)
- Each frame composed of 8 time slots.
- Hence there will be total of 2,715,648 TDMA frames available in GSM and the same cycle continues.
- there are two variants to multiframe structure.
- 26 frame multiframe - Called traffic multiframe, composed of 26 bursts in a duration of 120ms, out of these 24 are used for traffic, one for Slow Associated Control Channel (SACCH) and one is not used.
- 51 frame multiframe- Called control multiframe, composed of 51 bursts in a duration of 235.4 ms.

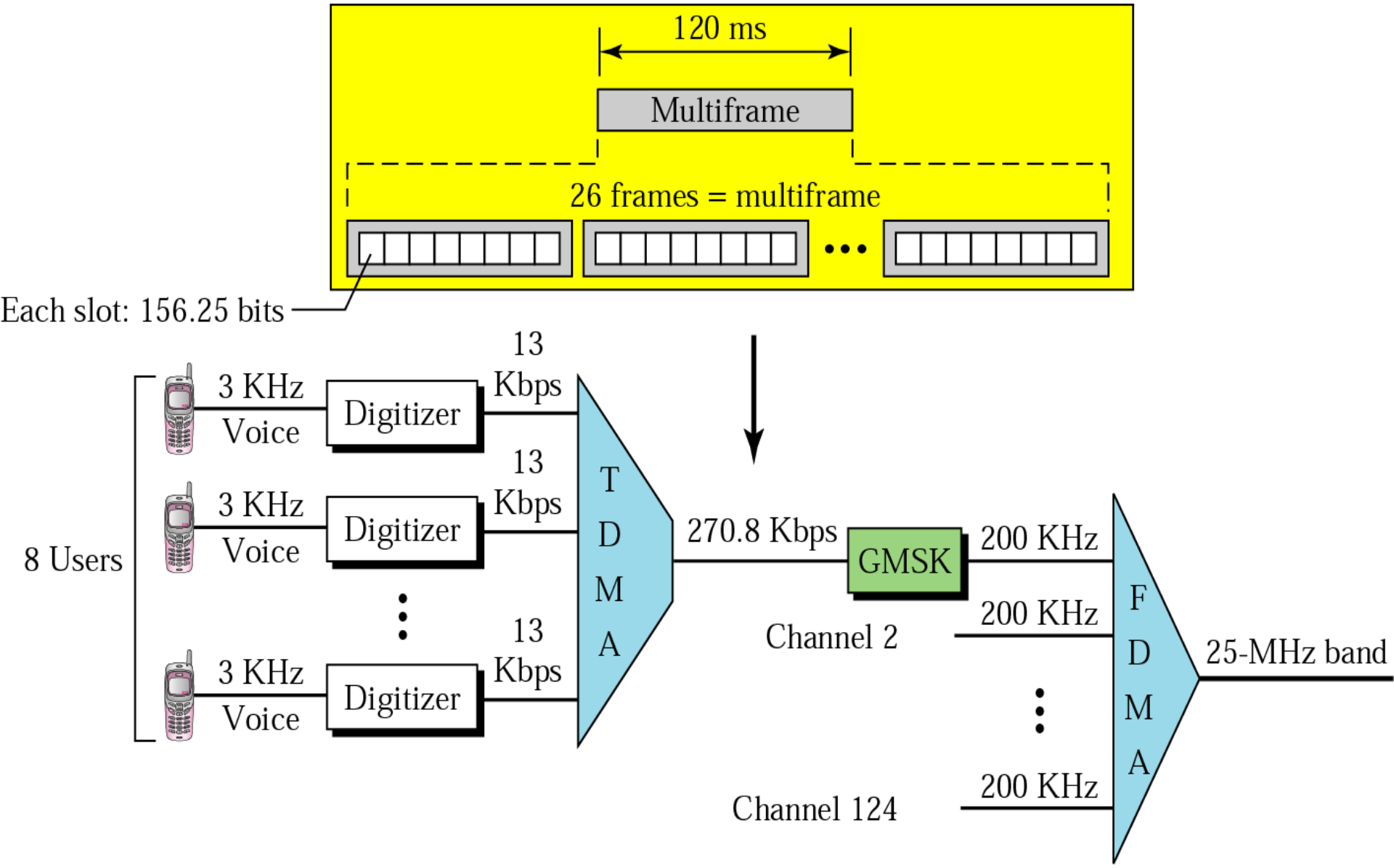

1 Hyperframe= 2048 superframes=3 hours, 29 minutes
0
1
2
2046
2047
1 Superframe= 51 Multiframes=6.125 s
0
1
2
50
1 Superframe= 26Multiframes=6.125 s
0
1
2
25
1 Multiframe= 26 frames=120 ms
0
1
2
25
1 Multiframe= 51 frames=235 ms
0
1
2
50
1 frame= 8 time slots=4.615 ms
0
1
2
3
4
5
6
7
4.615 ms
1 timeslot= 156.26 bit durations=577 µs
guard space
tail
user data
S
Training
S
user data
tail
guard space
3 bits
57 bits
1
26 bits
1
57 bits
3
546.5 µs
577 µs

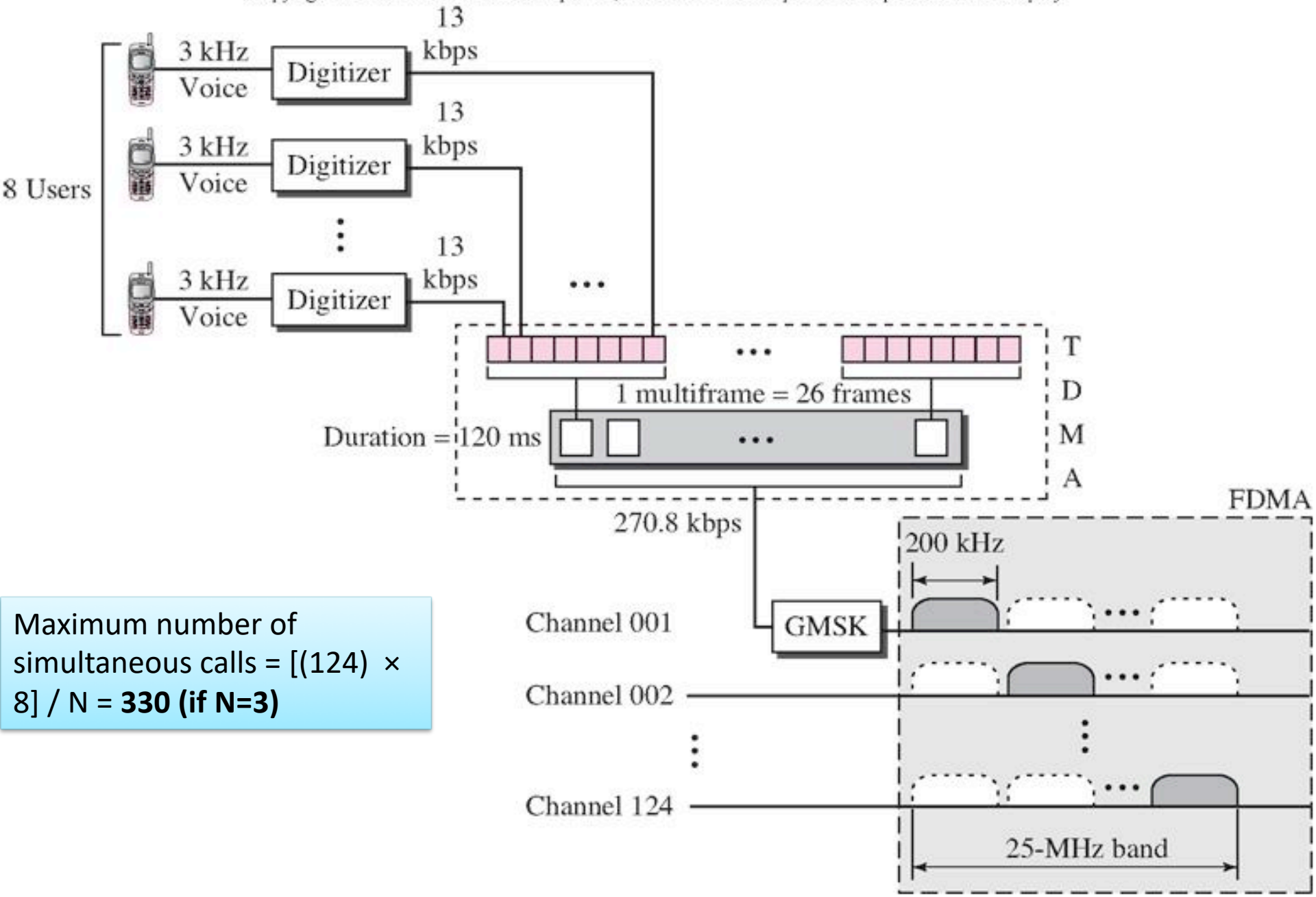
GSM - TDMA/FDMA



GSM TDMA frame, slots, and bursts

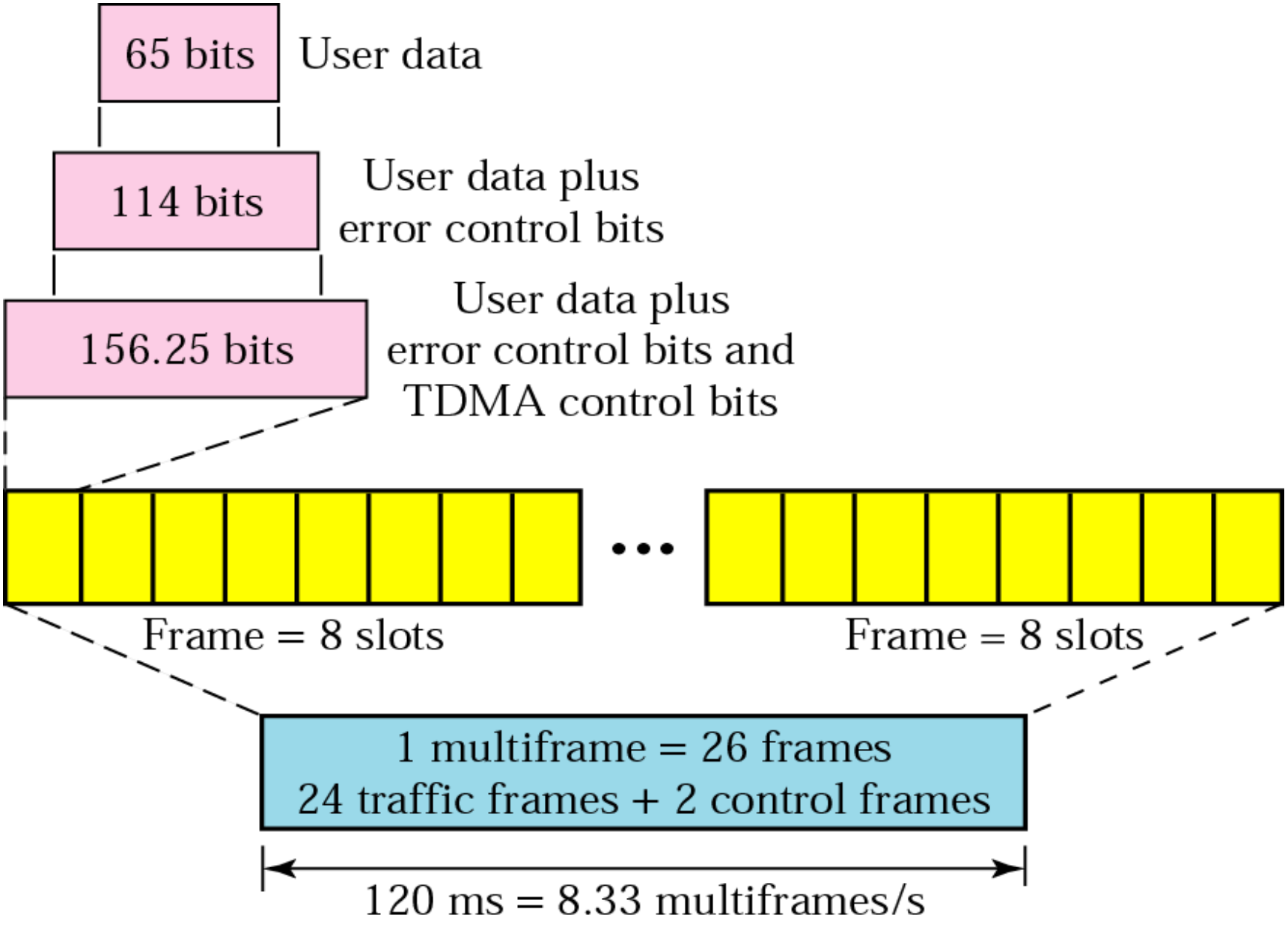
- Each radio carrier transmits approximately 270 kbit/s over the Um interface.
- **Tail** are all set to 0
- The **training sequence** is used to adapt the parameters of the receiver to the current path propagation characteristics and to select the strongest signal in case of multi-path propagation.
- A flag **S** indicates whether the **data** field contains user or network control data.
- This type of multiframe is divided into logical channels. These logical channels are time scheduled by BTS.


120 ms
Multiframe
26 frames = multiframe
Each slot: 156.25 bits
8 Users
3 KHz
Voice
Digitizer
13
Kbps
TDMA
270.8 Kbps
GMSK
200 KHz
Channel 2
Channel 124
FDMA
25-MHz band



Maximum number of simultaneous calls = [(124) × 8] / N = **330 (if N=3)**

~~Multiframe components~~



Type of bursts

- Normal Burst: GSM time slot
- **Frequency correction burst allows the MS to correct the** local oscillator to avoid interference with neighbouring channels
- **Synchronization burst** with an extended training sequence synchronizes the MS with the BTS in time.
- **Access burst is used for the initial connection setup between MS** and BTS.
- **Dummy burst is used if no data is available for a slot.**

- Two factors allow for the use of simple transmitter hardware,

1. The slots for uplink and downlink of a physical TDM channel are separated in frequency.
2. The TDMA frames are shifted in time for three slots, i.e., if the BTS sends data at time t_0 in slot one on the downlink, the MS accesses slot one on the uplink at time t_0+3.77μs.

- To avoid frequency selective fading, GSM specifies an optional **slow frequency hopping** mechanism.
- MS and BTS may change the carrier frequency after each frame based on a common hopping sequence.
- An MS changes its frequency between up and downlink slots respectively.

Data rate

- channel data rate in GSM

(1/120 ms) × 26 × 8 × 156.25 = 270.8 33Kbps

- User data rate

Each user channel receives one slot per frame

$$\frac{114\,\text{bits/slot} \times 24\,\text{slots/multiframe}}{120\,\text{ms/multifram}} = 22.8\text{kbps}$$

With error control

$$\frac{65\text{data bits/slot} \times 24\,\text{slots/multiframe}}{120\,\text{ms/multifram}} = 13\text{kbps}$$

Logical channels and frame hierarchy

GSM specifies two basic groups of logical channels, i.e., traffic channels and control channels

Traffic channels (TCH):

Traffic channels (TCH): GSM uses a TCH to transmit user data
Full-rate TCH (TCH/F) has a data rate of 22.8 kbit/s
Half-rate TCH (TCH/H) has 11.4 kbit/s.

- 13 kbit/s were required, whereas the remaining capacity of the TCH/F was used for error correction (**TCH/FS**).
- Improved codes allow for better voice coding and can use a TCH/H.
- Using these **TCH/HS**s doubles the capacity of the GSM system for voice transmission. However, speech quality decreases with the use of TCH/HS.
- The standard codecs for voice are called **full rate** (FR, 13 kbit/s) and **half rate** (HR, 5.6 kbit/s).
- A newer codec, **enhanced full rate** (EFR), provides better voice quality than FR as long as the transmission error rate is low

- Data transmission in GSM is possible at many different data rates, e.g.
- **TCH/F4.8** for 4.8 kbit/s, **TCH/F9.6** for 9.6 kbit/s, and, as a newer specification, **TCH/F14.4** for 14.4 kbit/s.
- These logical channels differ in terms of their coding schemes and error correction capabilities.

Control channels (CCH):

- Used to control medium access, allocation of traffic channels or mobility management

1. **Broadcast control channel (BCCH).**
2. **The Common Control Channel (CCCH)**
3. **Dedicated Control Channels (DCCH)**

Broadcast control channel (BCCH): are downlink only (BSS to MS).

- **BCCH** is transmitted by the BTS at all times. The information carried on the BCCH is monitored by the MS periodically (at least every 30 secs), when it is switched on and not in a call.
- BCCH Carries the following information
  - Location Area Identity (LAI).
  - List of neighbouring cells which should be monitored by the MS.
  - List of frequencies used in the cell.
  - Cell identity.
  - Power control indicator.
  - Access control (for example, emergency calls, call barring).
- The BCCH is transmitted at constant power at all times.
- Its signal strength is measured by all MS which may seek to use it.

- The Synchronizing Channel (SCH) carries information for frame synchronization. (training sequence to demodulate the downlink information)
- The Frequency Control Channel (FCCH) provides information for carrier synchronization. (i.e. gives the MS the reference frequency of the system)

The Common Control Channel (CCCH) works in both uplink and downlink directions.

- Random Access Channel (RACH) is used by MSs to gain access to the system.
- Paging Channel (PCH) and Access Granted Channel (AGCH) operate in the "downlink" direction.
- The AGCH is used to assign resources to the MS, such as a Stand-alone Dedicated Control Channel (SDCCH).
- The PCH is used by the system to call a MS. The PCH and AGCH are never used at the same time.
- Cell Broadcast Channel (CBCH) is used to transmit messages to be broadcast to all MSs within a cell, for example, road traffic information, sporting results.

Dedicated Control Channels (DCCH) are assigned to a single MS for call setup and subscriber validation. DCCH comprises:

- Stand-alone Dedicated Control Channel (SDCCH) which supports the transfer of Data to and from the MS during call setup and validation.
- Associated Control Channel (ACCH).
  - Slow ACCH which is used for radio link measurement and power control messages.
  - Fast ACCH is used to pass "event" type messages, for example, handover messages.
- Both f**ast associated dedicated control channel (**FACCH) and **slow associated dedicated control channel (**SACCH) operate in uplink and downlink directions.

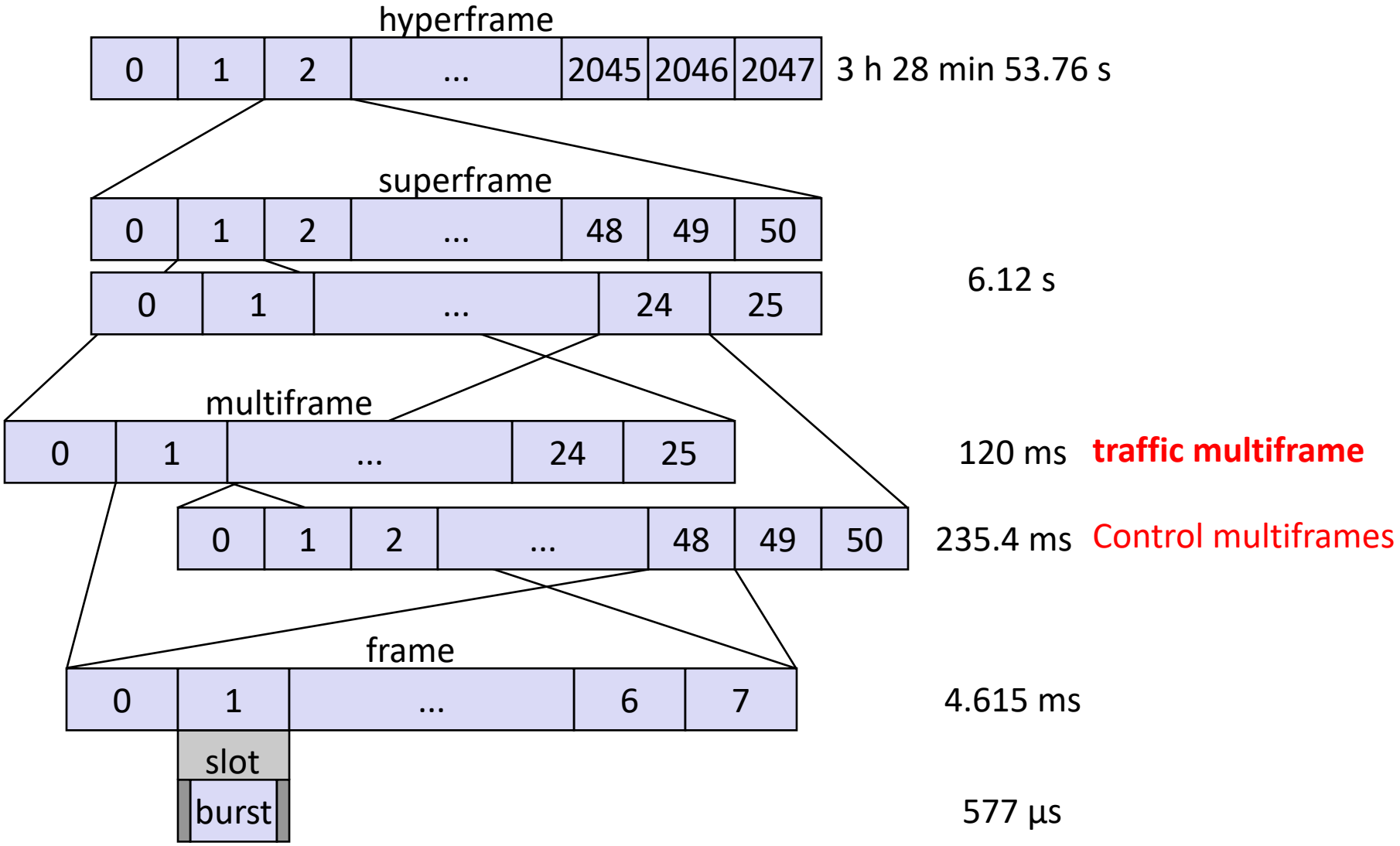
- These channels cannot use time slots randomly
- GSM specifies a very elaborate multiplexing scheme that integrates several hierarchies of frames
- If we take a simple TCH/F for user data transmission,
- Each TCH/F will have an associated SACCH for slow signalling or FACCH for fast signalling
- FACCH uses the time slots for the TCH/F.
- A typical usage pattern of a physical channel for data transmission looks like this (with T indicating the user traffic in the TCH/F and S indicating the signalling traffic in the SACCH),

TTTTTTTTTTTTSTTTTTTTTTTTTx

TTTTTTTTTTTTSTTTTTTTTTTTTx

- Twelve slots with user data are followed by a signalling slot. Again 12 slots with user data follow, then an unused slot

- This pattern of 26 slots is repeated over and over again.
- In this case, only 24 out of 26 physical slots are used for the TCH/F.
- Each normal burst used for data transmission carries 114 bit user data and is repeated every 4.615 ms.
- This results in a data rate of 24.7 kbit/s.
- As the TCH/F only uses 24/26 of the slots, the final data rate is 22.8 kbit/s as specified for the TCH/F.
- The SACCH thus has a capacity of 950 bit/s.
- This periodic pattern of 26 slots occurs in all TDMA frames with a TCH
- The combination of these frames is called **traffic multiframe**
- Combining 26 multiframes with 51 frames or 51 multiframes with 26 frames to form a **superframe**. 2,048 superframes build a **hyperframe** with a duration of almost 3.5 hours.
- Altogether, 2,715,648 TDMA frames form a hyperframe.


hyperframe
0
1
2
...
2045
2046
2047
3 h 28 min 53.76 s
superframe
0
1
2
...
48
49
50
0
1
...
24
25
6.12 s
multiframe
0
1
...
24
25
120 ms
traffic multiframe
0
1
2
...
48
49
50
235.4 ms
Control multiframes
frame
0
1
...
6
7
4.615 ms
slot
burst
577 µs

Localization and calling

- GSM performs periodic location updates even if a user does not use the mobile station
- The HLR always contains information about the current location
- VLR currently responsible for the MS informs the HLR about location changes
- As soon as the MS moves into the range of a new VLR (a new location area), the HLR sends all user data needed to the new VLR.
- Changing VLRs with uninterrupted availability of all services is also called **roaming.**
- **Roaming can take place within the network** of one provider, between two providers in one country also between different providers in different countries

To locate an MS and to address the MS, **several numbers are needed**

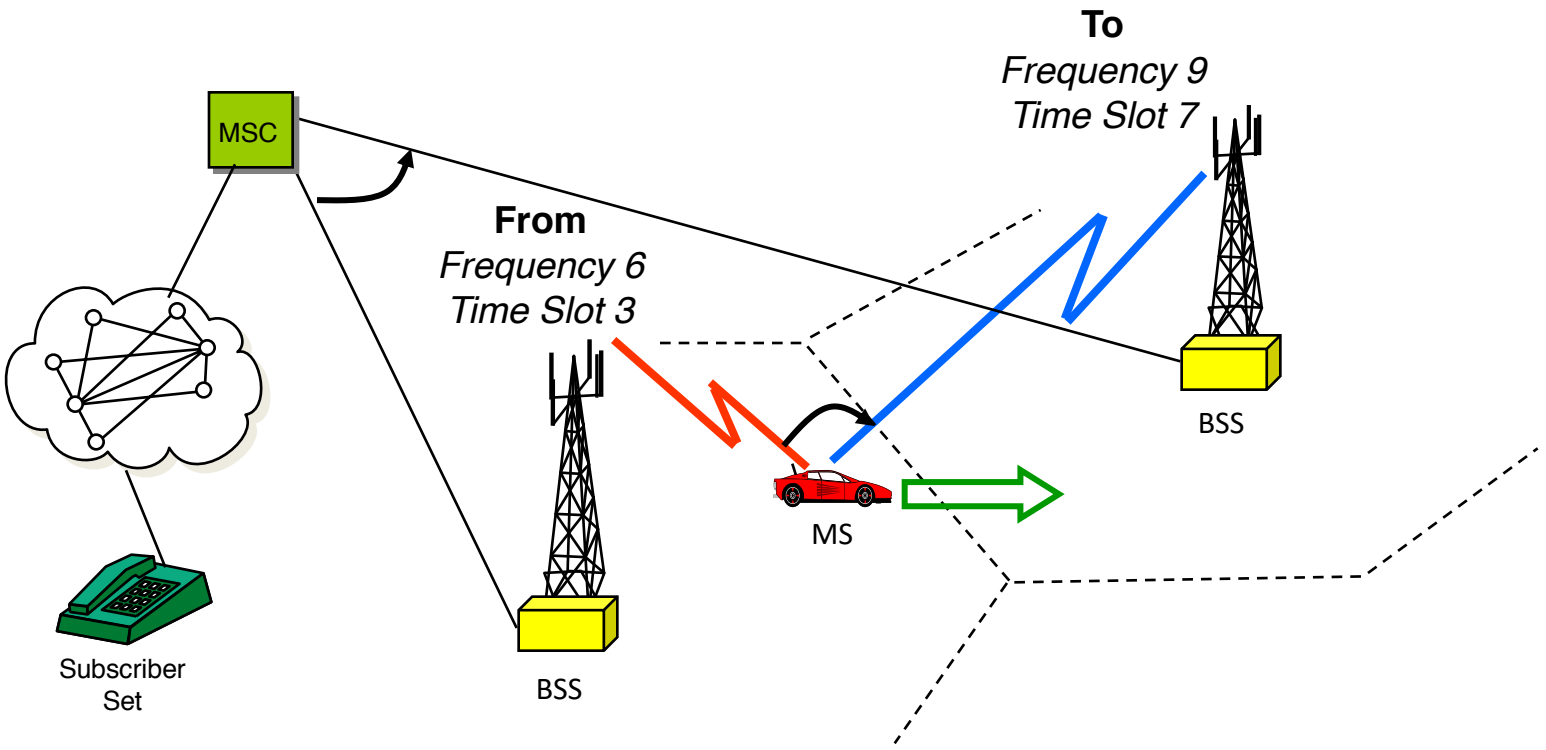
- **Mobile station international ISDN number (MSISDN): The only important** number for a user of GSM is the phone number it consists of the **country code (CC),** the **national destination code (NDC),** i.e., the address of the network provider and the **subscriber number (SN).**
- **International mobile subscriber identity (IMSI): GSM uses the IMSI for** internal unique identification of a subscriber. It consists of a **mobile country code (MCC) (e.g.,** 425 **for Jawwal), the mobile network code (MNC) (i.e., the code of the network provider), and** the **mobile subscriber identification number (MSIN).**
- **Temporary mobile subscriber identity (TMSI): To hide the IMSI, which** would give away the exact identity of the user signalling over the air interface.
- **Mobile station roaming number (MSRN):** The VLR generates this address on request from the MSC, and the address is also stored in the HLR. MSRN contains the current **visitor country code (VCC), the visitor national destination code (VNDC)**. The MSRN helps the HLR to find a subscriber for an incoming call.

Handover

- There are two basic reasons for a handover

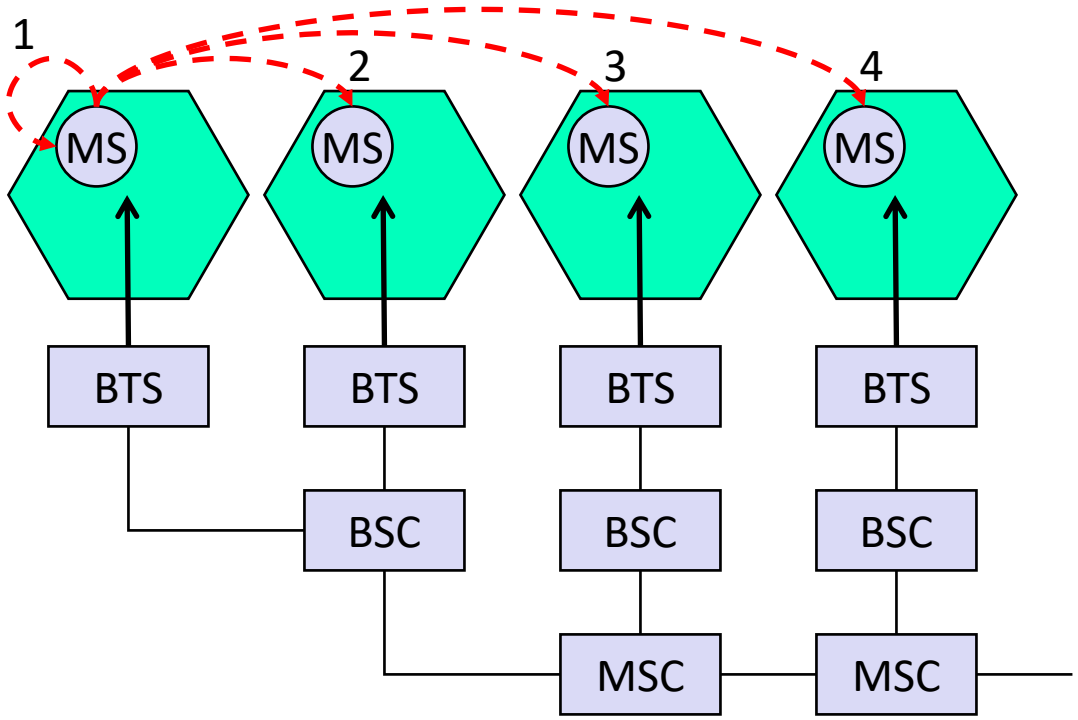
1. The mobile station **moves out of the range of a BTS or a certain antenna of** a BTS.
   - The received **signal level decreases** **continuously until it** falls below the minimal requirements for communication.
   - The **error rate** may grow due to interference, the distance to the BTS may be too high (max. 35 km) etc. – all these effects may diminish the **quality of the radio link** and make radio transmission impossible in the near future.
2. The wired infrastructure (MSC, BSC) may decide that the **traffic in one cell is too high and shift some MS to other cells with a lower load (if possible).** Handover may be due to **load balancing.**

GSM Handover



- *Lanline switched at MSC*
- *Frequency and time slot changed at MS*

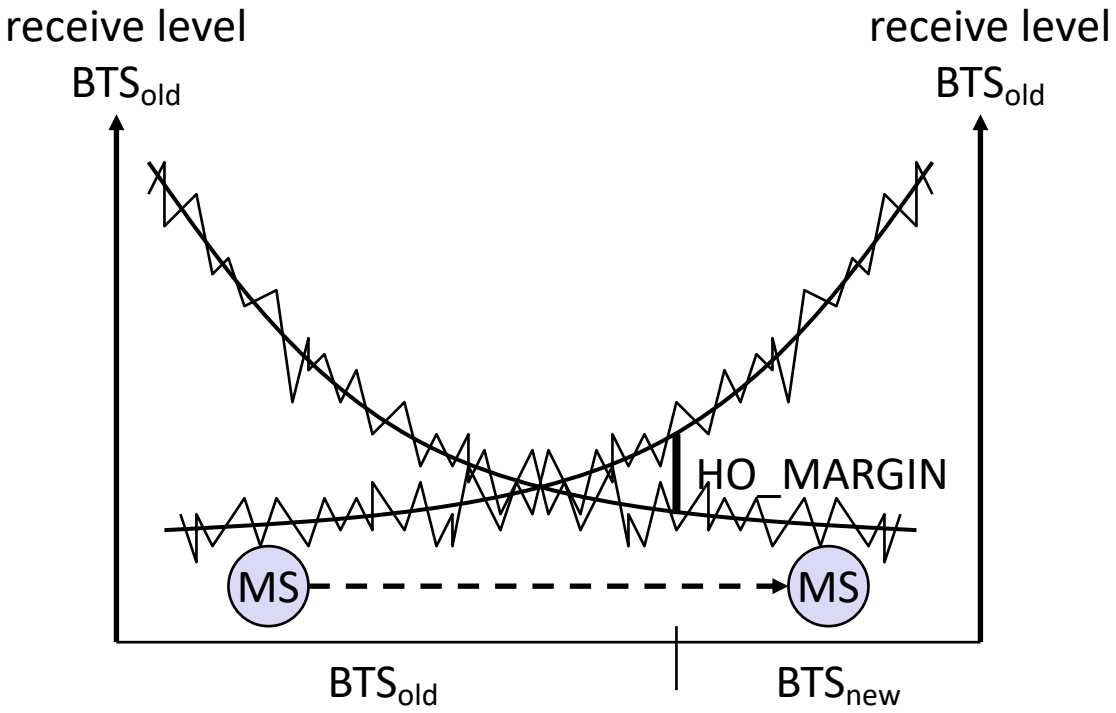
Types of handover



1. **Intra-cell handover**
2. **Inter-cell, intra-BSC handover**
3. **Inter-BSC, intra-MSC handover**
4. **Inter MSC handover**

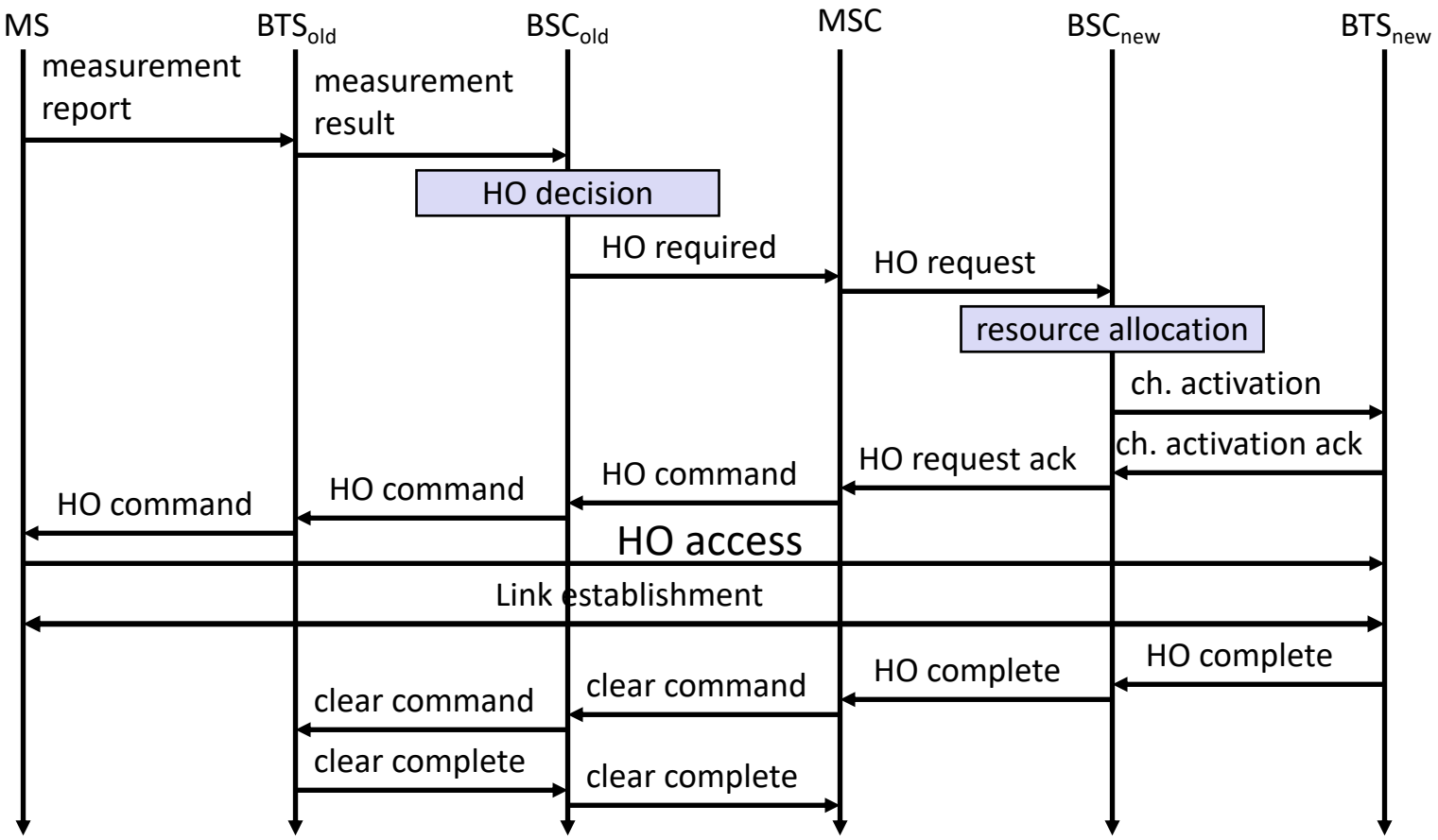
1) **Intra-cell handover: Within a cell, narrow-band interference could make** transmission at a certain frequency impossible. The BSC could then decide to **change the carrier frequency**.
2) **Inter-cell, intra-BSC handover: This is a typical handover scenario. The** mobile station moves from one cell to another, but stays within the control of the same BSC. The BSC then performs a handover, assigns a new radio channel in the new cell and releases the old one.
3) **Inter-BSC, intra-MSC handover: As a BSC only controls a limited number of** cells; GSM also has to perform handovers between cells controlled by different BSCs. This handover then has to be controlled by the MSC
4) **Inter MSC handover: A handover could be required** between two cells belonging to different MSCs. Now both MSCs perform the handover together.

Handover decision



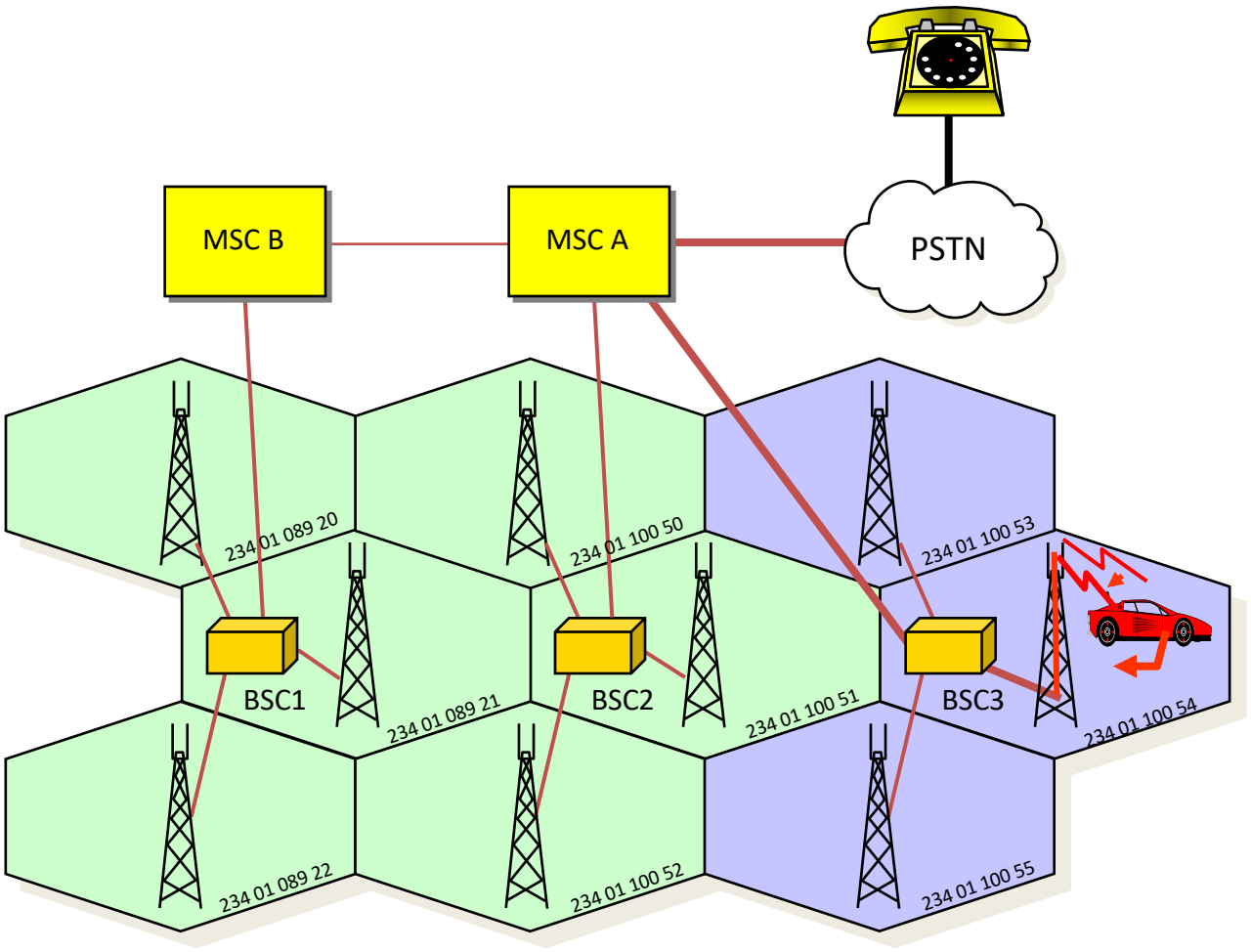
- The handover decision does not depend on the actual value of the received signal level, but on the average value.
- The BSC collects all values (bit error rate and signal levels from uplink and downlink) from BTS and MS and calculates average values.

- These values are then compared to thresholds, i.e., the handover margin (HO_MARGIN), which includes some hysteresis to avoid a ping-pong effect



Handover procedure Intra-MSC handover

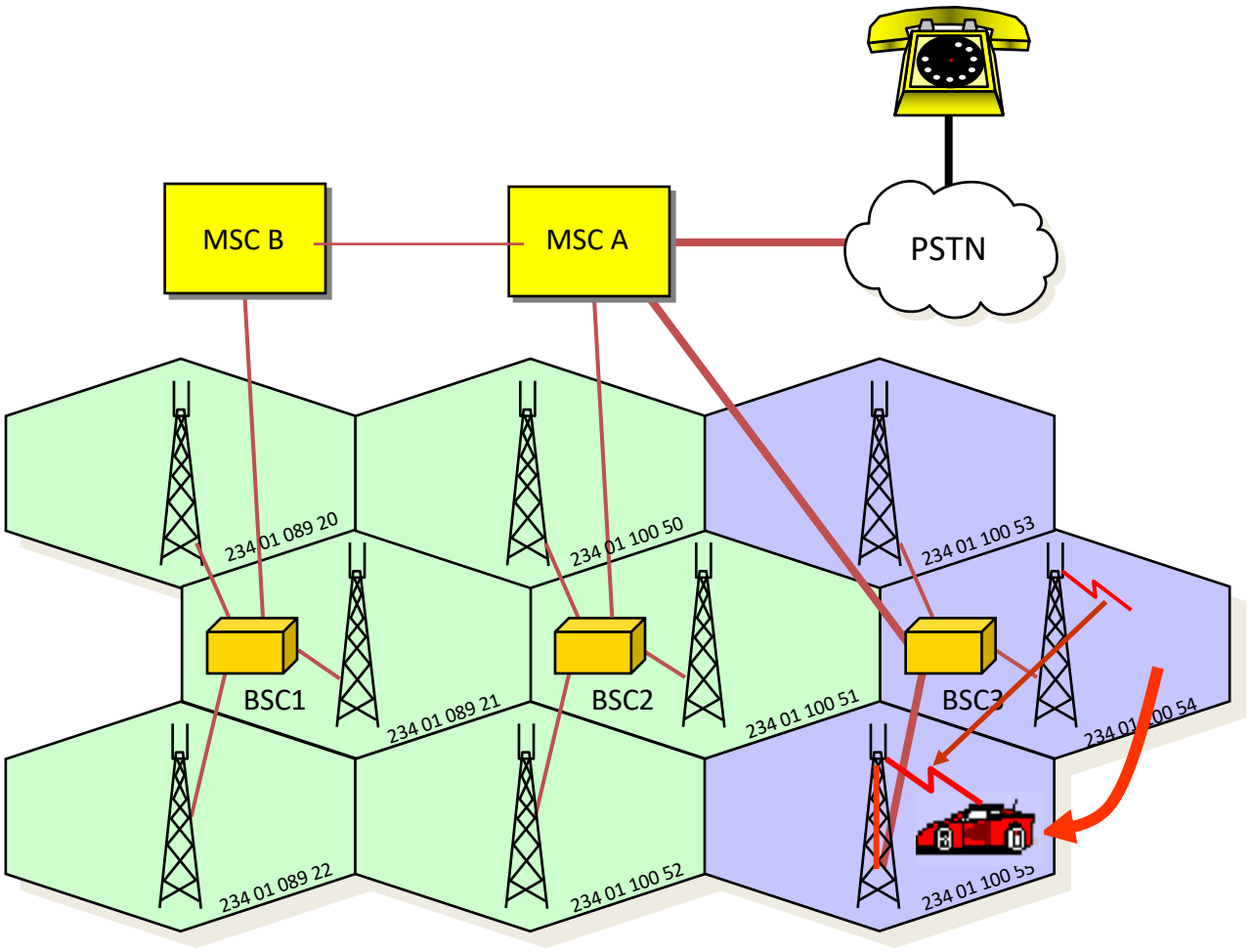
Intra-BTS Handover



Global Cell Identification

Country Code	Network Code	Location Area Code	Cell Identity

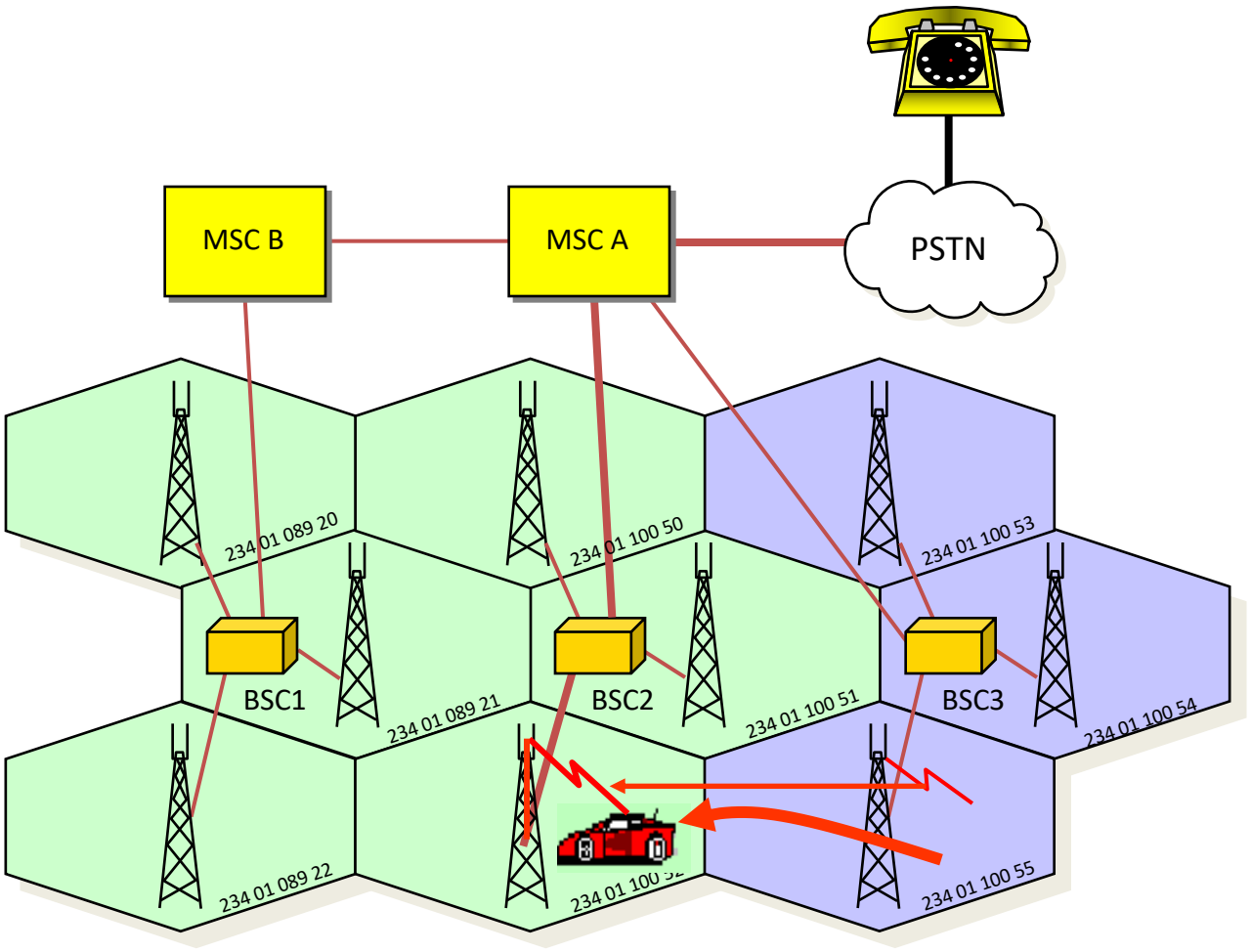
Intra-BSS/Inter-BTS Handover



Global Cell Identification

Country Code	Network Code	Location Area Code	Cell Identity

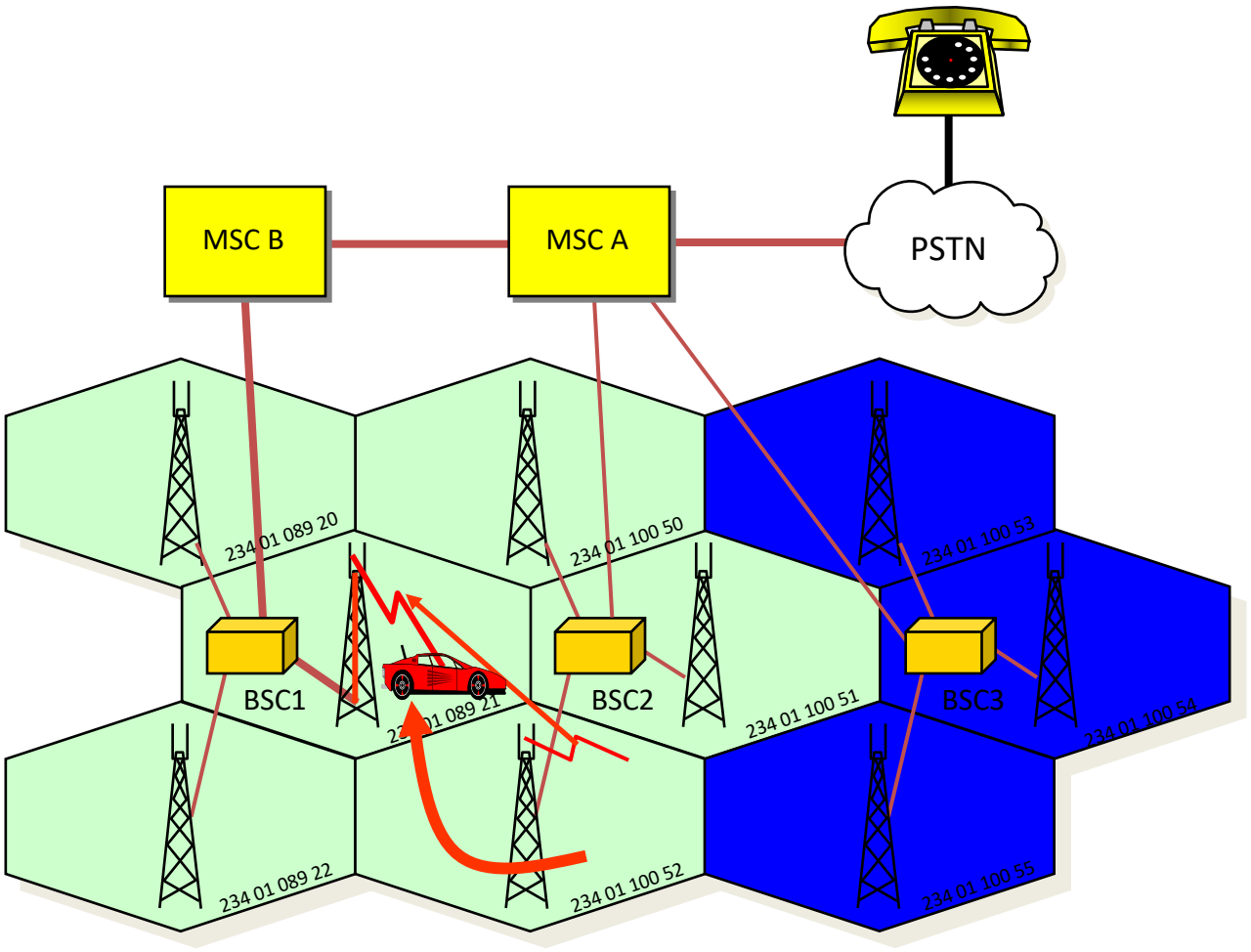
Intra-MSC, Inter-BSS Handover



Global Cell Identification

Country Code	Network Code	Location Area Code	Cell Identity

Intra-BSC, Inter-BTS Handover



Global Cell Identification

Country Code	Network Code	Location Area Code	Cell Identity

Mobile terminated call (MTC)

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

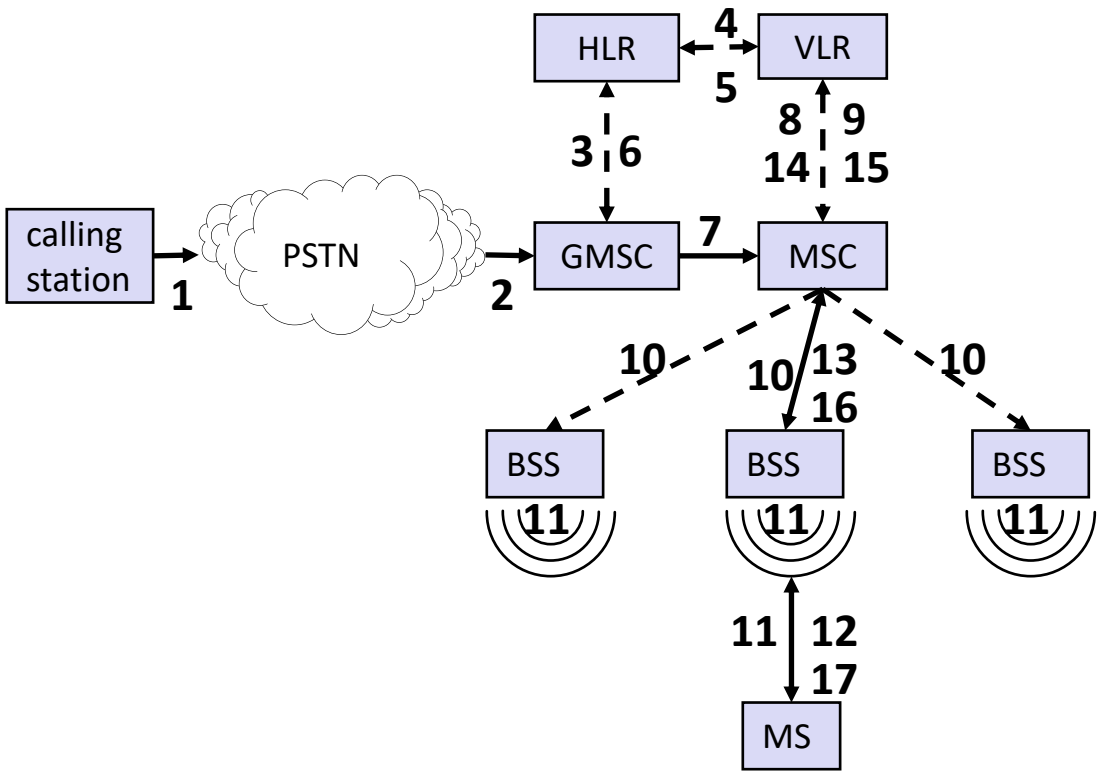
8, 9: get current status of MS

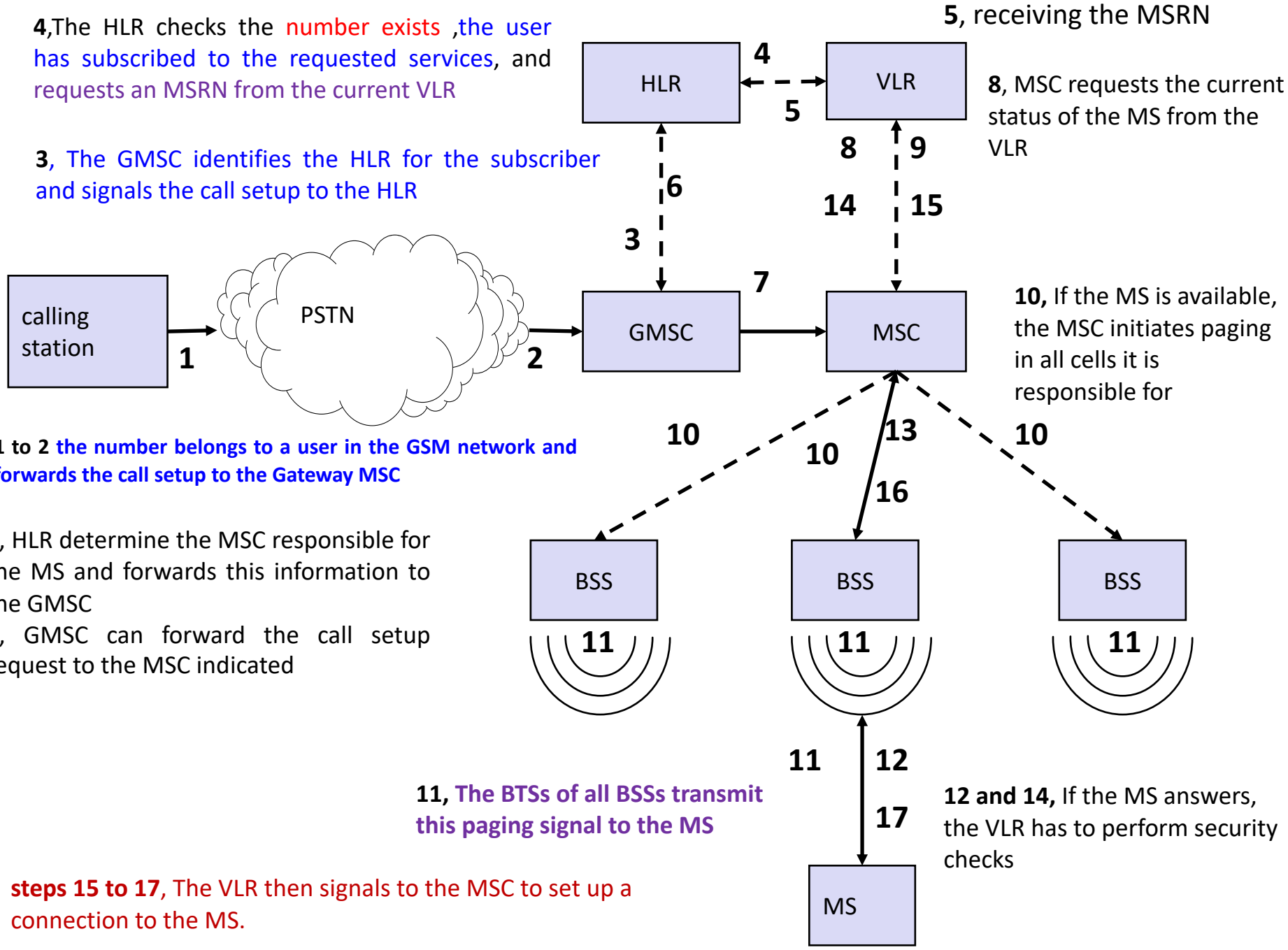
10, 11: paging of MS

12, 13: MS answers

14, 15: security checks

16, 17: set up connection



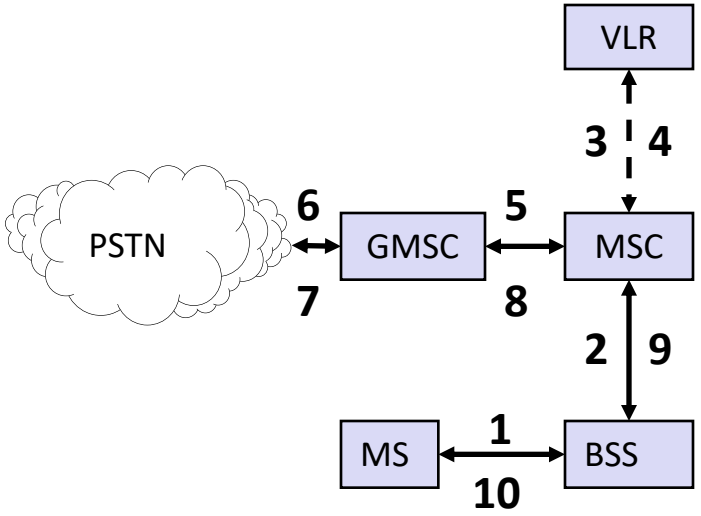

4,The HLR checks the number exists ,the user has subscribed to the requested services, and requests an MSRN from the current VLR
5, receiving the MSRN
HLR
VLR
4
5
8, MSC requests the current status of the MS from the VLR
3, The GMSC identifies the HLR for the subscriber and signals the call setup to the HLR
8
9
6
14
15
3
7
calling station
PSTN
GMSC
MSC
1
2
10, If the MS is available, the MSC initiates paging in all cells it is responsible for
1 to 2 the number belongs to a user in the GSM network and forwards the call setup to the Gateway MSC
10
10
13
10
16
6, HLR determine the MSC responsible for the MS and forwards this information to the GMSC
7, GMSC can forward the call setup request to the MSC indicated
BSS
BSS
BSS
11
11
11
11
12
11, The BTSs of all BSSs transmit this paging signal to the MS
12 and 14, If the MS answers, the VLR has to perform security checks
17
steps 15 to 17, The VLR then signals to the MSC to set up a connection to the MS.
MS

Mobile Originated Call **(MOC)**

1: The MS transmits a request for a new connection.
2: the BSS forwards this request to the MSC.

3 and 4: The MSC then checks if this user is allowed to set up a call with the requested service.
5 to 8: checks the availability of resources through the GSM network and into the PSTN

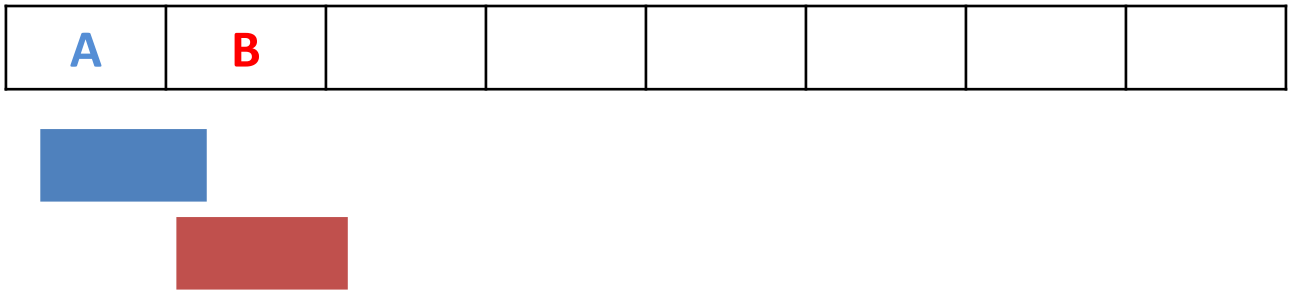
9 and 10: set up call



- The main interest lies in the U_m interface
- **Layer 1**, the physical layer, handles all **radio**-specific functions which includes,
    - The creation of bursts
    - **Multiplexing** of bursts into a TDMA frame,
    - **Synchronization** with the BTS,
    - Detection of idle channels,
    - Measurement of the **channel quality** on the downlink
- Synchronization also includes the correction of the individual path delay between an MS and the BTS,
- All MSs within a cell use the same BTS and thus must be synchronized to this BTS.
- The BTS generates the time-structure of frames, slots etc.
- A problematic aspect in this context are the different **round trip times (RTT).**
- An MS close to the BTS has a very short RTT, whereas an MS 35 km away already exhibits an RTT of around 0.23 ms

- If the delay is too high, the timeslots of the signal from a certain mobile station and that of the next signal from another mobile station received by the base station will overlap each other, thus causing interference.
- The Timing Advance is a parameter that allows the GSM BTS to control the signal delays in their communication with the mobile.
- More specifically, is calculated by the delay of information bits in Data Access Burst received by BTS.
- A burst represents the physical content of a timeslot and can be of 5 types: Normal, Frequency Correction, Synchronization, Access or Dummy.
- Each burst carry bits of different types: Information, Tail, Training Sequence.
- We have eight timeslots, each user transmits within 1 / 8 of that time, periodically. The arrival time in each slot is then known.
- Users are randomly located around the station, a closer and more distant, yet we can consider the propagation environment as being the same for everyone.
- So if we know the time and speed that the signal travels, we calculate the distance (location)

- A major application of this parameter, you control the time at which each mobile can transmit a burst of traffic within a timeslot in order to avoid collisions of transmissions of the other adjacent users.



- The Timing Advance (TA) signal is transmitted in the SACCH as a number between 0 and 63, in units of bit periods (3.69 microseconds)
- If the signal travels at 300 meters per microsecond, each TA is a distance of approximately 1100 meters
- Because this is the distance round, each increase in the value of TA corresponds to a distance 550 between the mobile and BTS.
- For example, TA = 0 means that the mobile is up to 550 meters from the station, TA = 1 means it is between 550 and 1100 meters, TA = 2, from 1100 to 1650 meters and so on.

- The maximum distance allowed by the TA between the MS and BTS is 35 km (GSM 850 / 900) * 63 or 550 meters.
- Controlling interference by continually adjusting the TA, we have less data loss, and **improve the quality of our signal**.
- As this is a parameter directly related to distance, it is natural that the TA is also used in **locating applications**.
- Another good application is the **handover control**.

- If the MS far away used the slot structure without correction, large guard spaces would be required, as 0.23 ms are already 40 per cent of the 0.577 ms available for each slot.
- Therefore, the BTS sends the current RTT to the MS, which then adjusts its access time so that all bursts reach the BTS within their limits.
- This mechanism reduces the guard space to only 30.5 μs or five per cent.
- Adjusting the access is controlled via the variable **timing advance**, where a burst can be shifted up to 63 bit times earlier, with each bit having a duration of 3.69 μs (which results in the 0.23 ms needed).
- The main tasks of the physical layer comprise **channel coding** and **error detection/correction**, which is directly combined with the coding mechanisms.
- Channel coding makes extensive use of different **forward error correction (FEC)** schemes.
- FEC adds redundancy to user data, allowing for the detection and correction of selected errors.
- The power of an FEC scheme depends on the amount of redundancy, coding algorithm and further interleaving of data to minimize the effects of burst errors.

Security in GSM

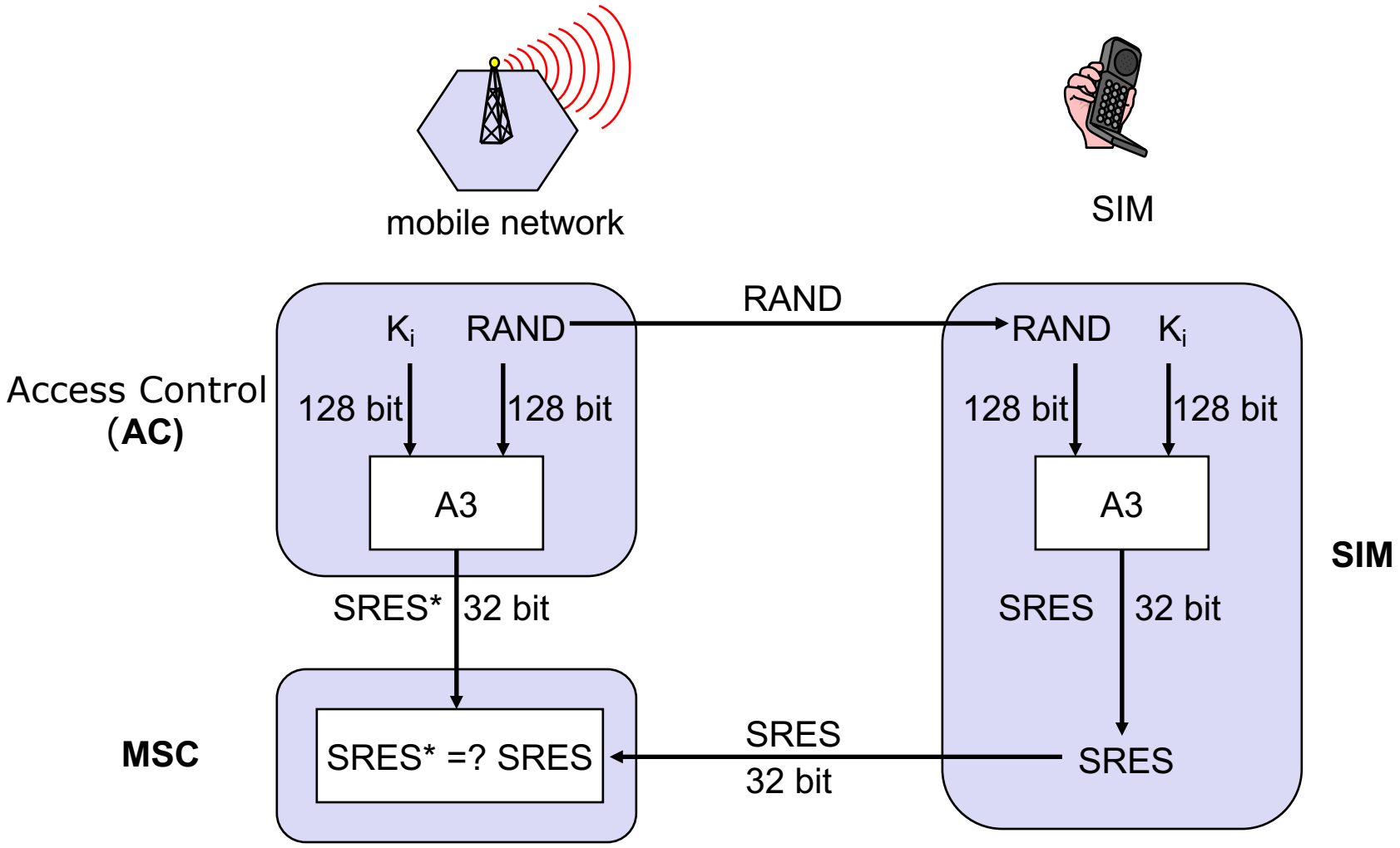
- The security services offered by GSM are,
- **Access control and authentication:**
  - The first step includes the authentication of a valid user for the SIM.
  - The next step is the subscriber authentication
- **Confidentiality:** All user-related data is encrypted.
  - After authentication, BTS and MS apply encryption to voice, data, and signalling
  - This confidentiality exists only between MS and BTS, but it does not exist end-to-end or within the whole fixed GSM/telephone network.
- **Anonymity:** To provide user anonymity, all data is encrypted before transmission, and user identifiers are not used over the air.
  - Instead, GSM transmits a temporary identifier (TMSI), which is newly assigned by the VLR after each location update. Additionally, the VLR can change the TMSI at any time.

- Three algorithms have been specified to provide security services in GSM
  1) **Algorithm A3** is used for **authentication**.
  2) **A5** for **encryption.**
  3) **A8** for the **generation of a cipher key**.
- Algorithms A3 and A8 (or their replacements) are located on the SIM and in the AuC and can be proprietary.
- Only A5 which is implemented in the devices has to be identical for all providers

GSM - Authentication

- Authentication is based on the SIM, which stores the **individual authentication key K_i**, the **user identification IMSI**, and the algorithm used for authentication **A3**.
- The AuC performs the basic generation of random values RAND, signed responses SRES, and cipher keys Kc for each IMSI, and then forwards this information to the HLR.
- The current VLR requests the appropriate values for RAND, SRES, and Kc from the HLR.
- The VLR sends the random value RAND to the SIM.
- Both sides, **network and subscriber** module, perform the same operation with RAND and the key Ki, called A3.
- The MS sends back the SRES generated by the SIM; the VLR can now **compare** both values. If they are the same, the VLR accepts the subscriber, otherwise the subscriber is rejected.

GSM - Authentication

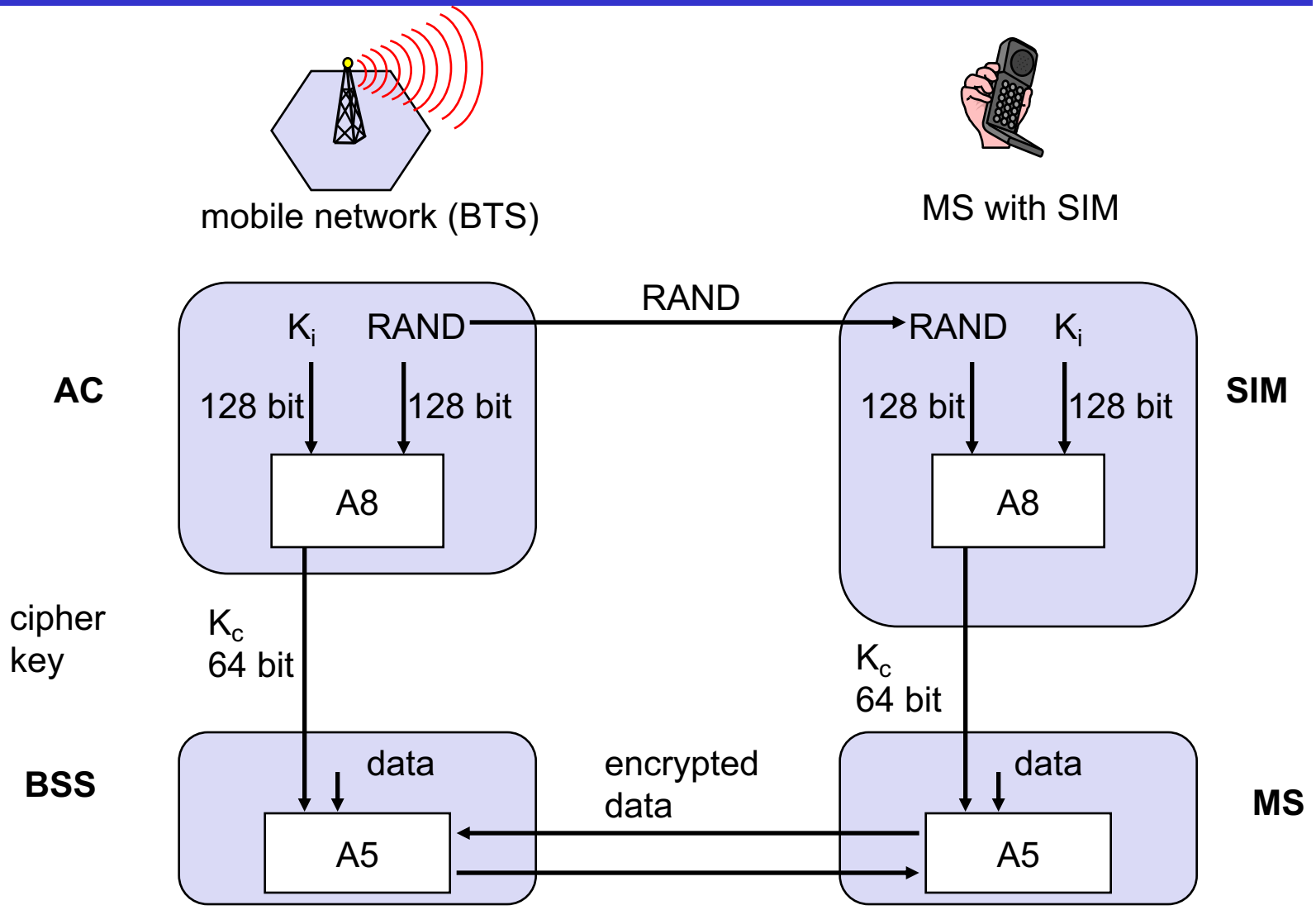


K_i: individual subscriber authentication key SRES: signed response

GSM - key generation and encryption

- After authentication, MS and BSS can start using encryption by applying the cipher key K_c.
- K_c is generated using the individual key K_i and a random value by applying the algorithm A8
- Note that the SIM in the MS and the network both calculate the same K_c based on the random value RAND.
- The key K_c itself is not transmitted over the air interface.
- MS and BTS encrypt and decrypt data using the algorithm A5 and the cipher key Kc

GSM - key generation and encryption



- **Further reading:**
  John Schiller, “Mobile Communications”,
- http://www.rfwirelessworld.com/Tutorials/gsm-frame-structure.html