Introduction to cellular systems

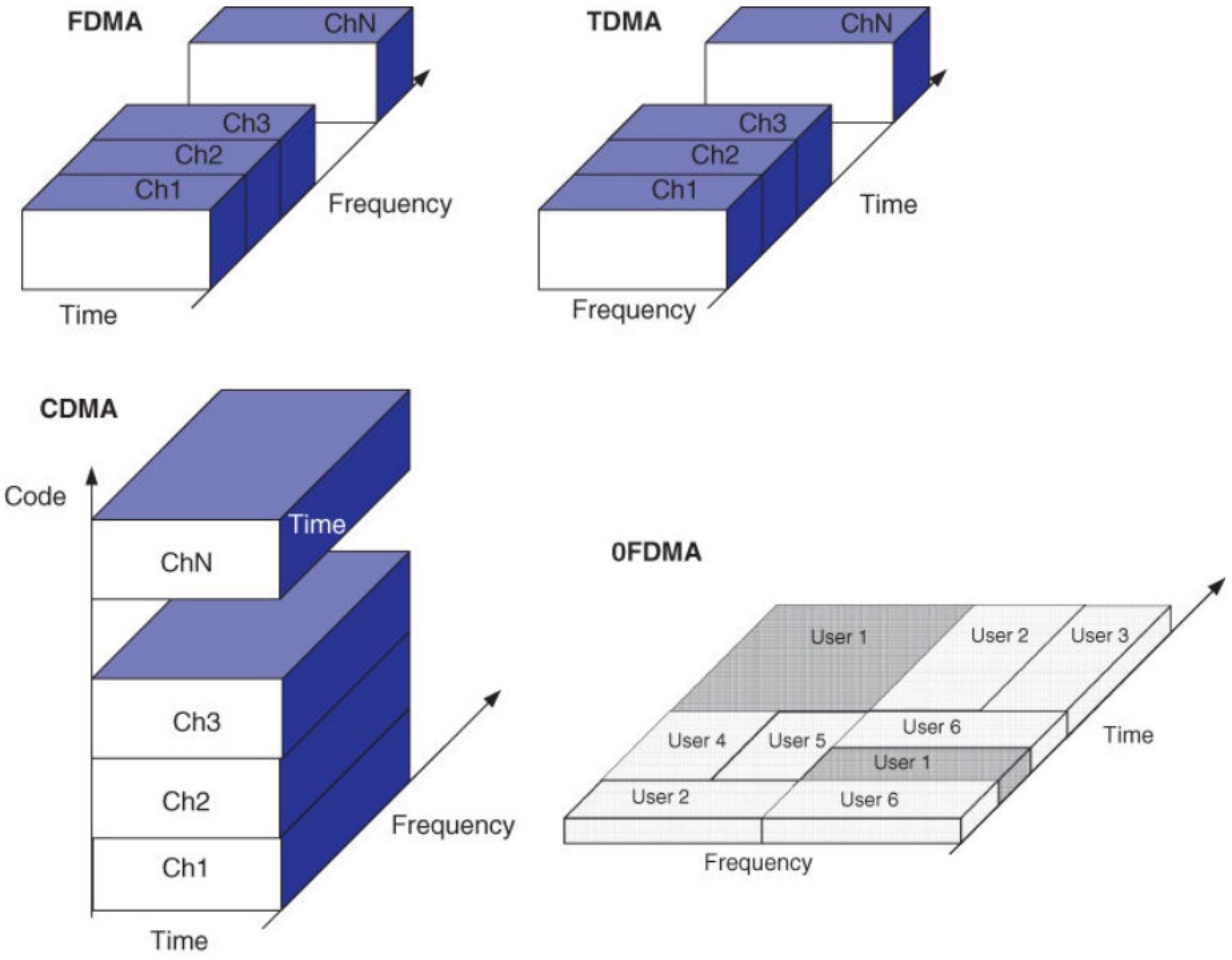
IoT, a.a. 2023/2024

Un. of Rome "La Sapienza"

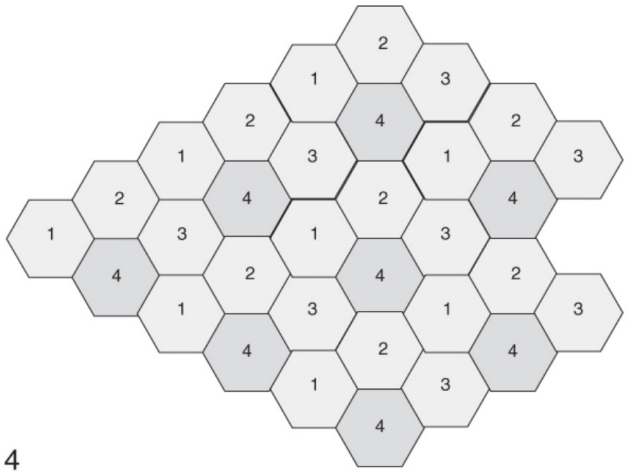
Chiara Petrioli[†]

[†]*Department of Computer Engineering – University of Rome "Sapienza" – Italy*

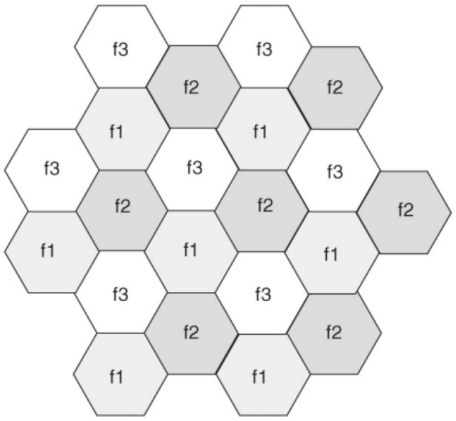
How physical resources are shared among users



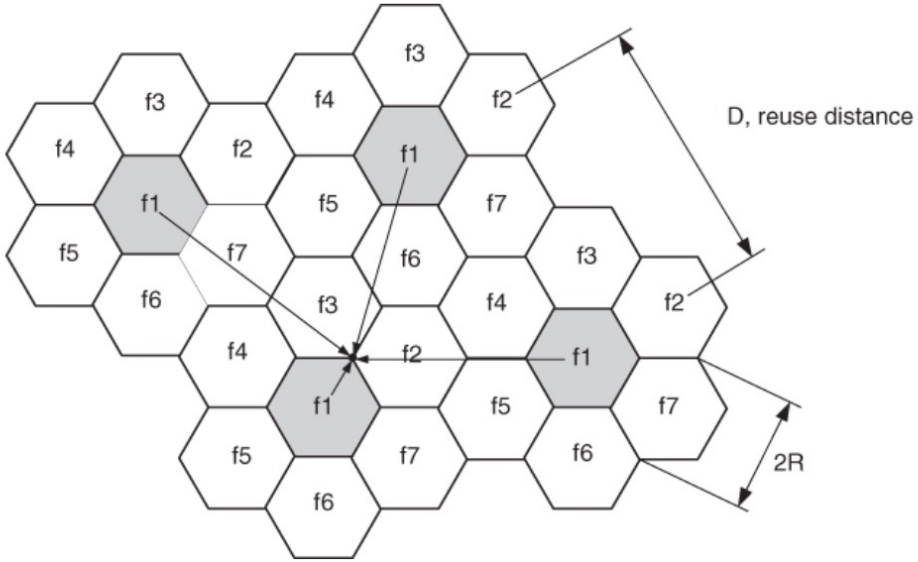
How frequencies are reused



K = 4



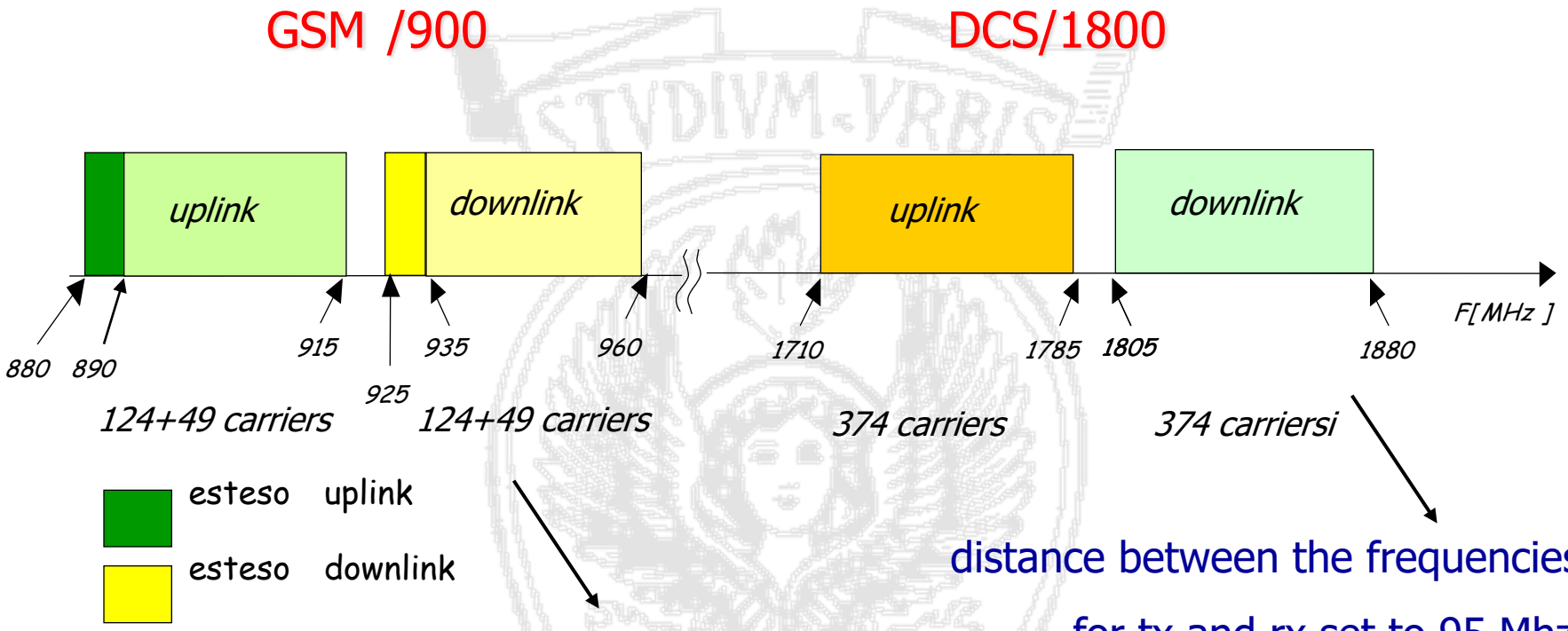
K = 3



GSM General features

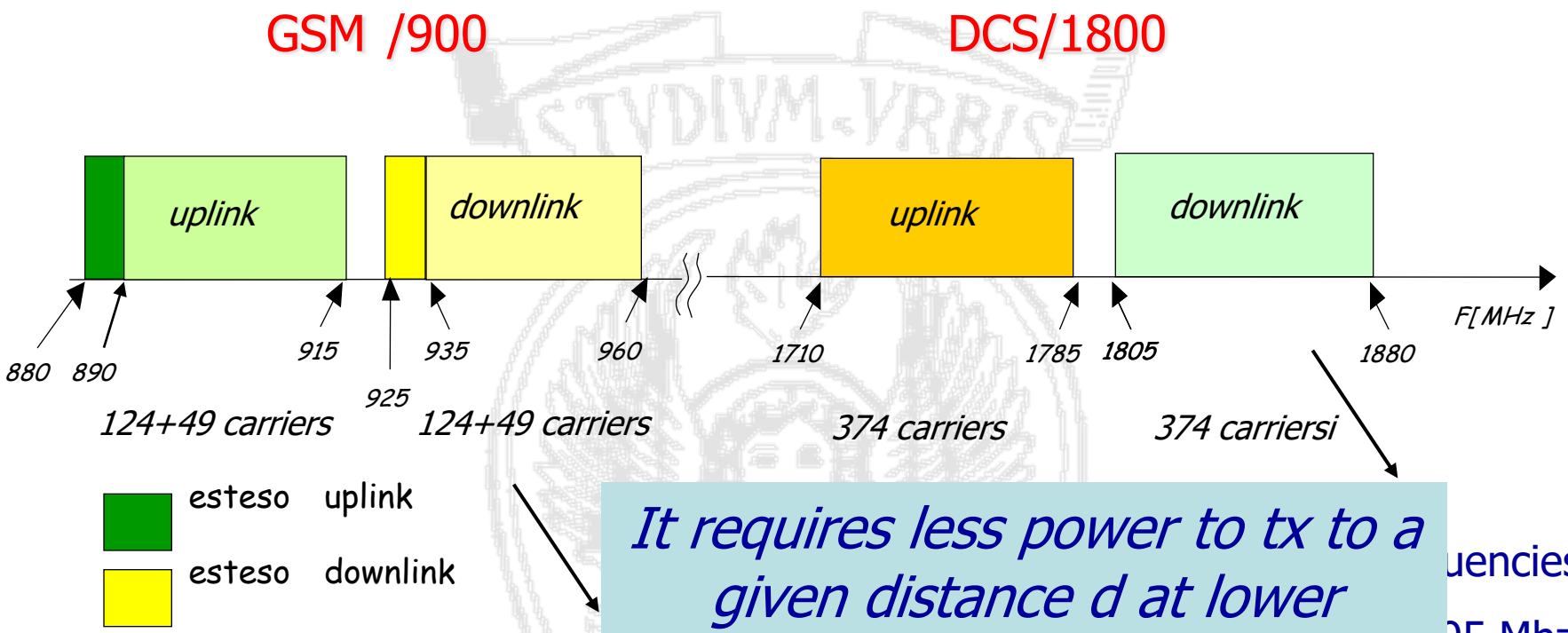
- 2ª Generation (2G) cellular system
- Carrier bandwidth=200KHz
- Multicarrier TDMA multiple access (8 slots per carrier, thus 8 channels per carrier)→ TDMA/FDMA
- Full Duplex: Frequency Division Duplex (FDD)
- Modulation: GMSK; Spectrum efficiency: 1,35bps/Hz; Gross bit rate per carrier: 270,822 kbit/s
- 13Kbps full rate coder, 6.5Kbps half rate coder
- 992 full rate channels at 900Mhz, 2992 full rate channels for DCS 1800Mhz
- Frequency reuse
- Power control, discontineous transmission
- Adaptive equalization
- Services
  - telephony with many additional services
  - circuit swirching data network (single-channel or multi-channel)
  - packet switching data network (GPRS - General Packet Radio Service)

Allocated frequencies



- In UK and USA it uses bands around 1900 MHz instead of around 1800 MHz (1850÷1910 uplink, 1930÷1990 downlink).

Allocated frequencies



It requires less power to tx to a given distance d at lower frequencies.

The lower portion of the spectrum is allocated to uplink channels, saving MS consumed power

uencies used

95 Mhz

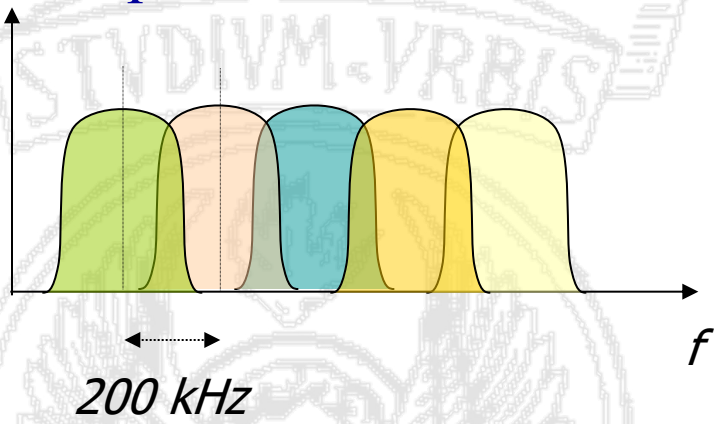
distance between the

for tx and rx s

- In UK and USA it of around 1800 MHz downlink).

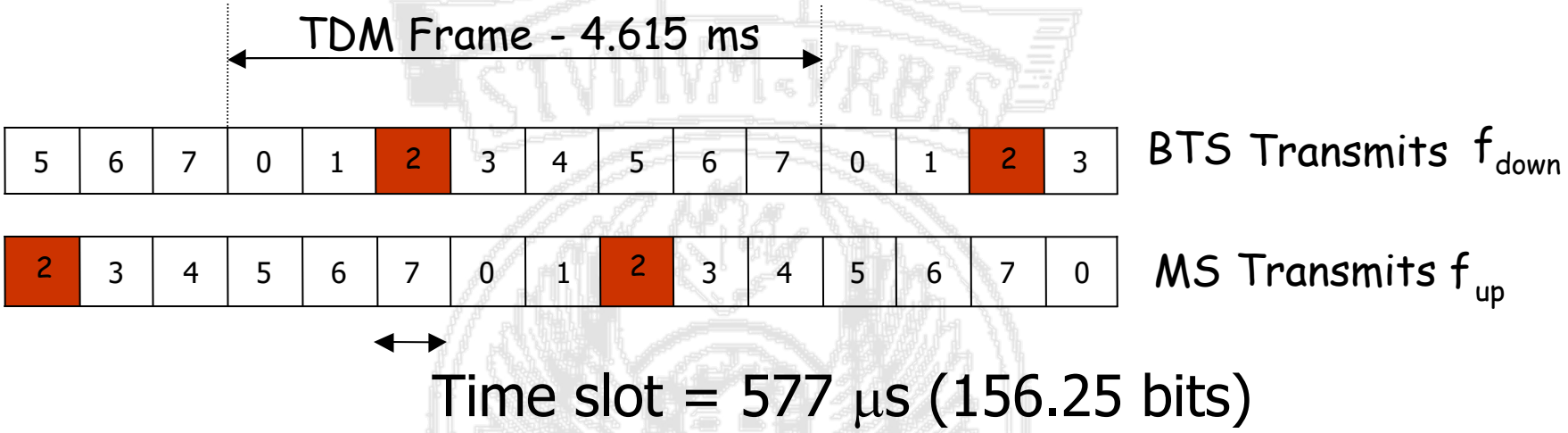
Carriers and channels

- Center frequencies are spaced 200 kHz



- Gross bit rate per channel: 270.833 Kb/s
- Carriers are identified by a ARFCN (Absolute Radio Frequency Channel Number)
- GMSK (Gaussian Minimum Shift Keying) modulation
- The two carriers used for transmission/reception to/from a device are always 45 MHz apart in GSM 900- They are spaced of a different fixed bandwidth (95 MHz) in DCS 1800

TDMA Frame



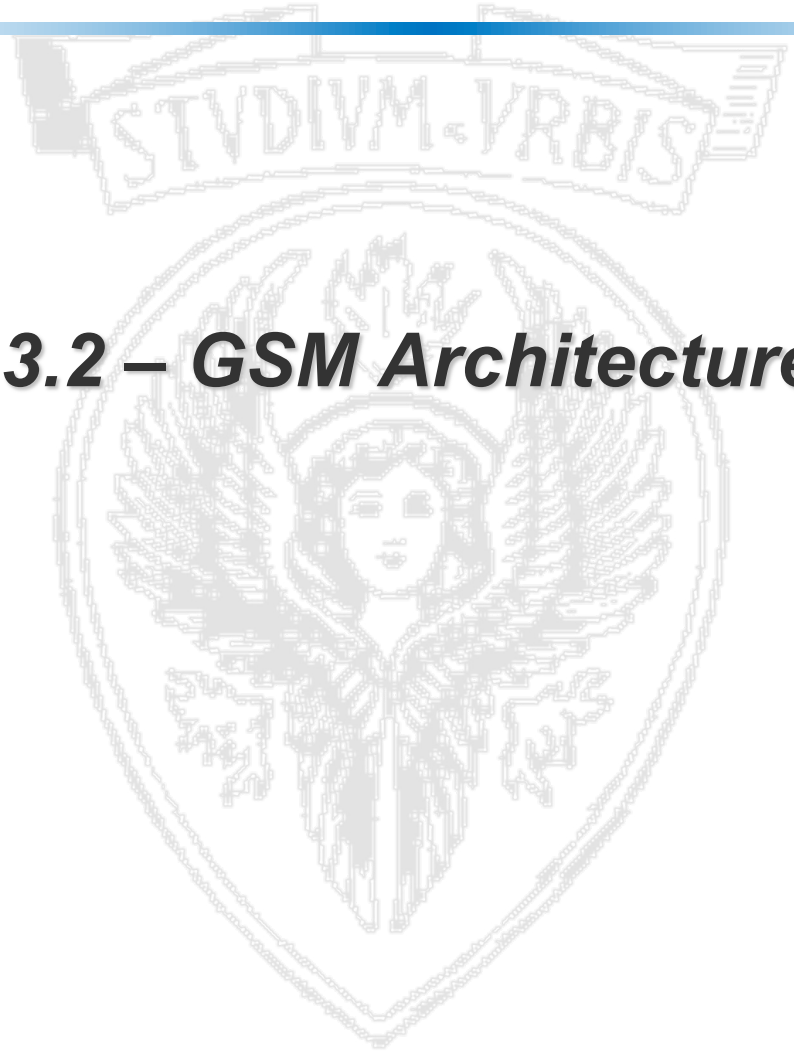
- On each radio carrier the TDMA structure allows us to create up to 8 channels for the transmission of voice encoded at 13 Kb / s

GSM General features

- **2ª Generation (2G) cellular system**
- **Carrier bandwidth=200KHz**
- **Multicarrier TDMA multiple access (8 slots per carrier, thus 8 channels per carrier)→ TDMA/FDMA**
- **Full Duplex: Frequency Division Duplex (FDD)**
- **Modulation: GMSK; Spectrum efficiency: 1,35bps/Hz; Gross bit rate per carrier: 270,822 kbit/s**
- 13Kbps full rate coder, 6.5Kbps half rate coder
- **992 full rate channels at 900Mhz, 2992 full rate channels for DCS 1800Mhz**
- **Frequency reuse**
- Power control, discontineous transmission
- Adaptive equalization
- **Services**
  - **telephony with many additional services**
  - **circuit swirching data network (single-channel or multi-channel)**
  - **packet switching data network (GPRS - General Packet Radio Service)**

Other key features

- Power Control
  - *the power emitted from the stations, mobile and base, is adjusted according to the conditions of propagation*
- Discontinous Trasmission
  - *during pauses in speech, coded voice transmission is interrupted to reduce interference and energy consumption*



3.2 – GSM Architecture

High level network architecture (1/2)

Services / Applications

SIM

ME:

Mobile equipment

UE: User equipment

Access Network (AN)

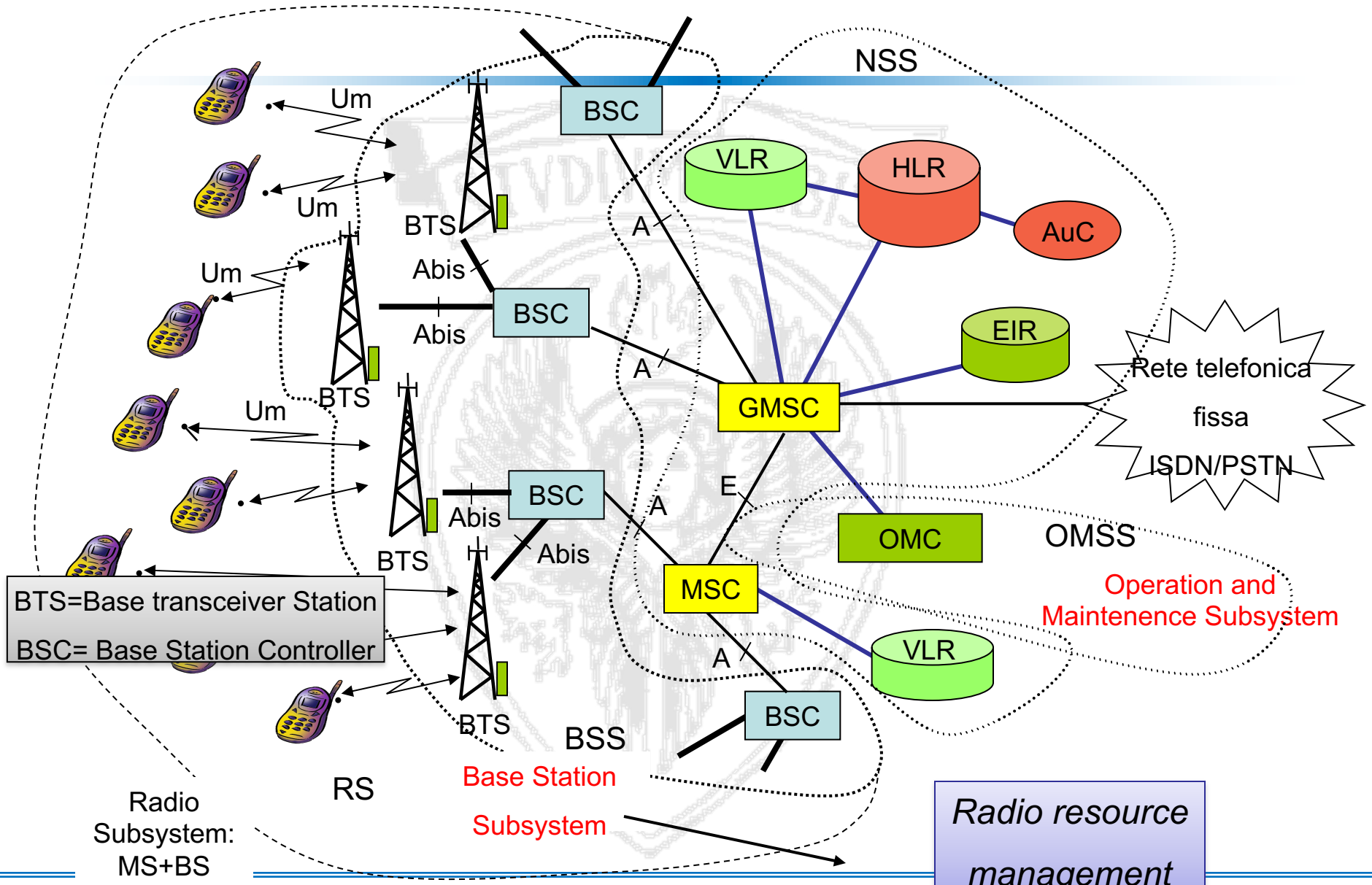
Core Network (CN)

Ext. network

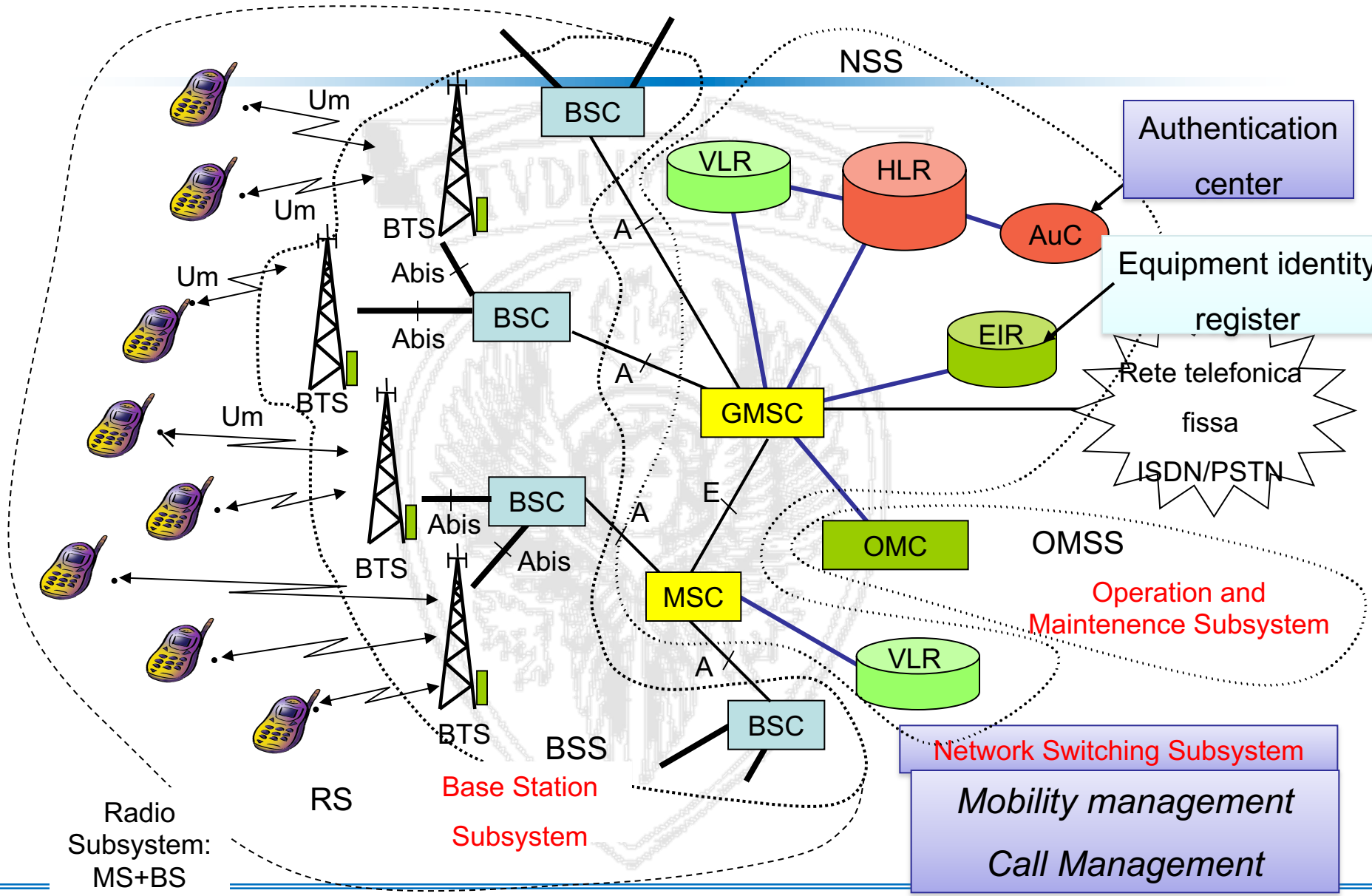
High level network architecture (2/2)

- The network contains functionally of: User Equipment (UE), Access Network (AN), and Core Network (CN)
  - User equipment: Interfaces the user, handles radio functionality
  - Access network: Communication to and from the user equipment, handles all radio related functionality in the network
  - Core network: Communication between access network and external networks, handles all switching and routing
- Services and applications lie above the network

Network architecture



Network architecture



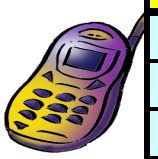
GSM Areas

- *PLMN (Public Land Mobile Network) Area:*
  - Service area of a cellular network
- *MSC/VLR Area:*
  - Area managed by an MSC. Data regarding users in the area are temporarly stored in a database called VLR associated to the MSC
- *Location Area:*
  - a MSC/VLR area is logically divided into one or more Location Area (LA). If a user changes LA he(she has to perform a location update. LA are identified by the *LAI (Location Area Identifier),* which is transmitted by the BTS of the LA over the broadcast control channel.
- *Cell:*
  - Area covered by a BTS. It is identified by a *BSIC (Base Station Identity Code),* which is transmitted by the BTS over the broadcast control channel.

(Mobile Station - MS)

- It is the terminal owned by the user
- Three categories depending on the nominal power:
  - Vehicular: antenna can emit up to 20 W
  - laptops: the antenna can emit up to 8 W to the antenna, are transportable, but they need a considerable source of power to operate (eg. laptops, fax, etc.)
  - personal (hand-terminal): the antenna can transmit up to 2, it is the "mobile phone"

(Mobile Station - MS)

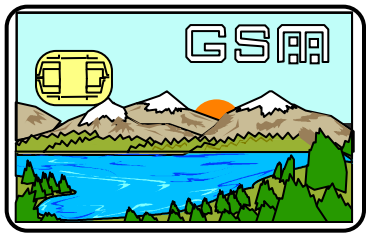


Classe	Potenza massima nominale [W]		Potenza media nominale [mW]	
	GSM 900 MHz	DCS 1800 MHz	GSM 900 MHz	DCS 1800 MHz
1	.	1	.	120
2	8	0,25	960	30
3	5	4	600	480
4	2	.	240	.
5	0,8	.	96	.

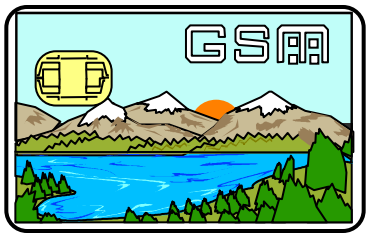
- Features
  - MS multi-band: can operate on different frequency bands (900, 1800, 1900, …)
  - MS multi-slot: can operate over different channels, in different slots (only for GPRS)
- MS is composed of an ME (Mobile Equipment) and a SIM (Subscriber Identity Module)
  - ME is the terminal through which we access the cellular network (HW, radio interface HW/SW, interface to the final user). It is identified by the *IMEI (International Mobile Equipment Identifier)*
  - SIM activates the terminal for a given user and stores all the needed information: it identifies the user, enables terminal personalization

Subscriber Identity Module - SIM

- Smart card (with processor and memory) which is needed to activate/operate an ME
- It mustbe inserted in ME reader
- There are different formats (from credit card like to small plug-in SIM)



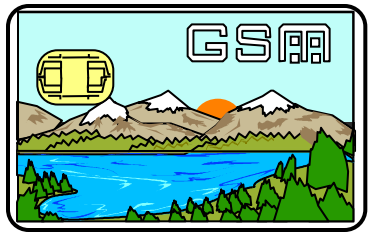
Information stored in the SIM



- *Serial number*
  - Uniquely Identifies SIM card (and card holder)
- *International Mobile Subscriber Identity (IMSI)*
  - Uniquely identifies the user in the network
- Security authentication and cyphering information
  - *A3* and *A8* algorithm (procedures to perform authentication and encryption)
  - K_i, K_c (keys for authentication and encryption)
- Temporary Network information
  - *LAI (Location Area Identifier)*, last visited location area identifier
  - *TMSI (Temporary Mobile Subscriber Identity)*, temporary identifier assigned by the network; TMSI is transmitted to identify the user instead of the IMSI

Information stored in the SIM

- List of services to which the user subscribed
- Personal Identification Number (PIN)
- Personal Unblocking Number (PUK)
- Access rights
- Prohibited networks
- Call messages
- Phone numbers



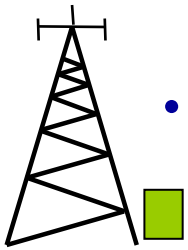
A Mobile Equipment without SIM is enabled to make only emergency calls

A Mobile Equipment is identified by a unique IMEI identifier (International Mobile Equipment Identity) that can be used to identify stolen mobile terminals.

Base Station System (BSS)

- BSS includes the functional units that deal with aspects of the radio system related to coverage and radio communication via a radio interface with the MS. The BSS also performs radio resource management
- BSS includes:
  - Base Transceiver Station (BTS)
  - HW / SW components that enable the transmission and reception of information through the radio interface. It has purely executive tasks (e.g. encryption, modulation, coding): resource management is handled by the BSC
- Base Station Controller (BSC)
  - monitors and manages the resources of a group of BTS. From the BTS it receives the information about the state of the radio interface. It uses information on the quality of the links to make decisions on handover. The BSC sends the commands to the BTS for configuration and management. It also allocates radio resources and channels connecting BSC/BTS in order to initiate a call or perform handover. Examples of functionality carried out by the BSC: reservation / release of radio channels, handover (intraBSC), transcoding etc ....

Base Transceiver Station (BTS)

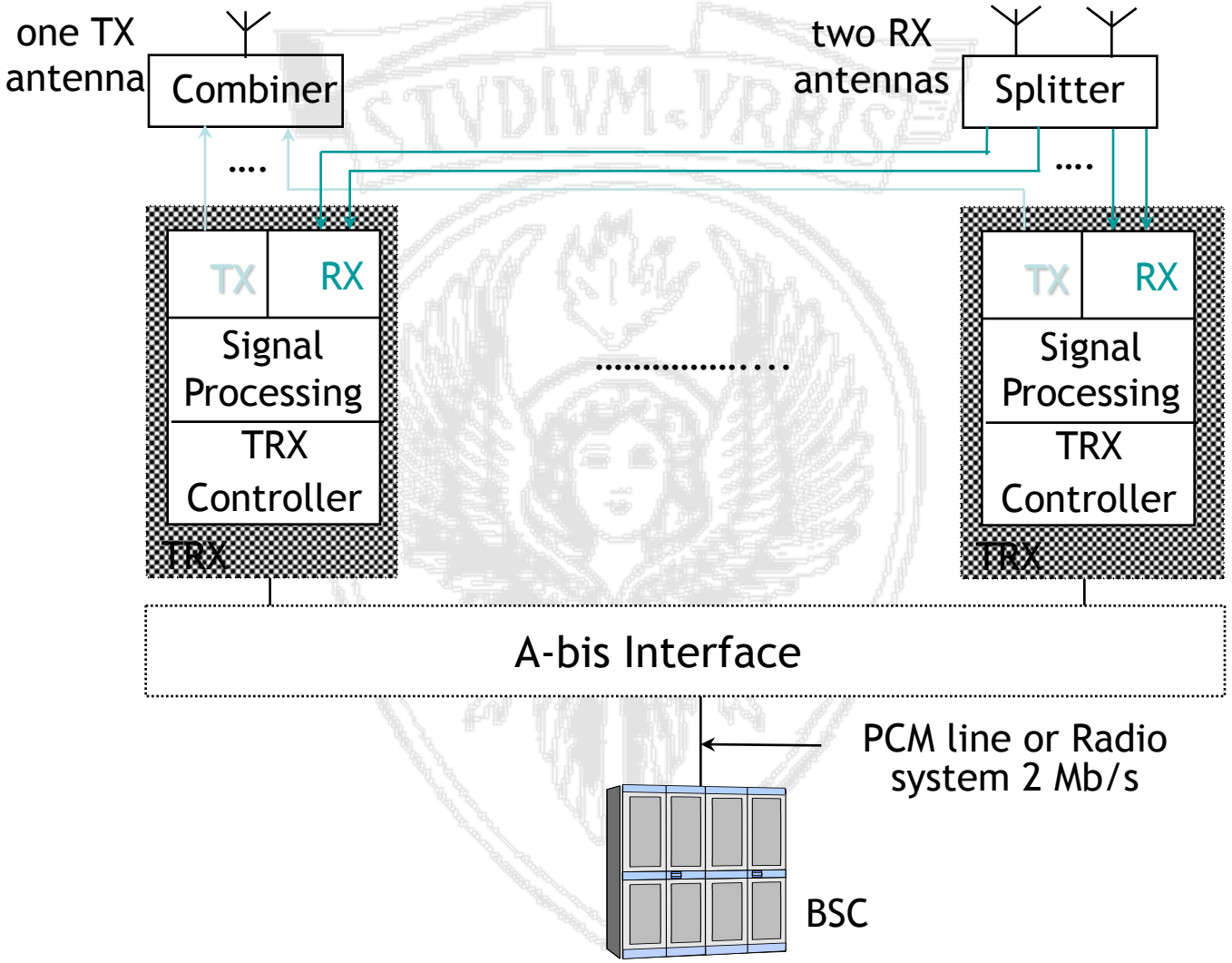


- The BTS is the element that has the task of implementing the low-level protocols of the radio interface
- And then to transmit and receive signals from MS implementing the functionality of modulation, coding and multiplexing of physical channels. It performs frequency hopping (if enabled) and encryption.
- Its task is also to perform quality measurements on the physical channels and to receive those made by MS (all measurements are then reported to the BSC that makes the decisions on when/whether to handoff)
- The BTS brodcasts on a control channel the System Information message, which contains data and parameters that are needed for the MS to access the network (Cell identity, Location Area identity, the minimum received signal level required to access the network, etc.);
- The BTS is also in charge of sending paging messages to locate the current position of a user.
- It interfaces to the BSC (only services in the circuit) by means of PCM channels at 64 kbit / s
- Connect the PCM channels with those of the radio interface (traffic and signaling)

Struttura BTS

- The BTS (Base Transceiver Station) is usually functionally divided into
  - TRX (Transceiver)
    - ✓ radio elements responsible for reception and transmission of a single radio carrier:
      - Transmitter: modulation, power amplifier,…
      - Receiver: diversity, demodulation,…
      - Signal processing
      - TRX controller
- BCF (Common Base Function)
  - control element of TRX that performs the common functions
    - ✓ synchronization, frequency hopping computation
  - and interface with the BSC

BTS functional scheme



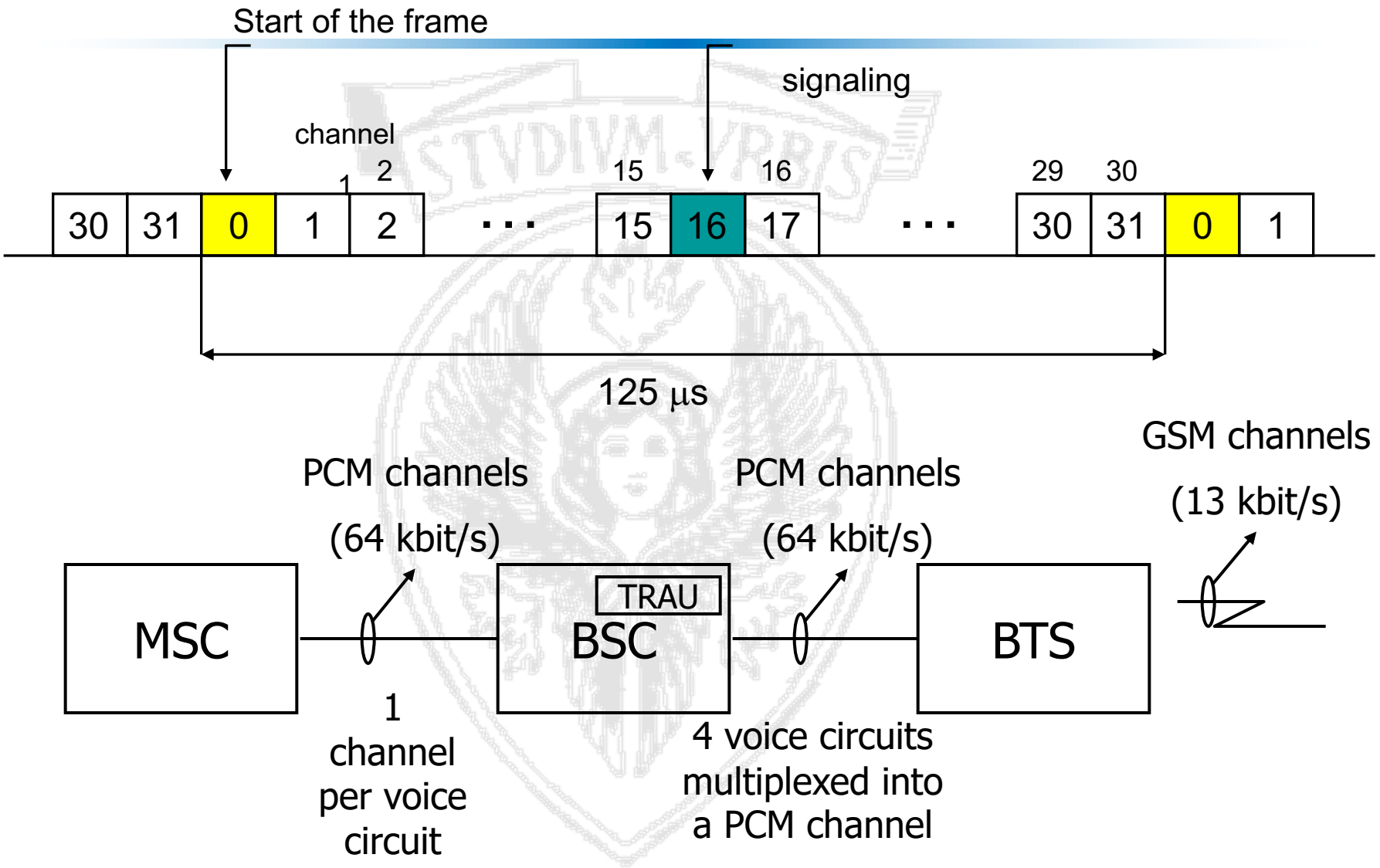
BCF

Base Common Functions

Transcoder Rate Adaptation Unit (TRAU)

- GSM voice coding is 13 kbps while the PCM provides 64 kbps
- The transcoding is performed by the TRAU
- The TRAU may be in the BTS, but more often it is in the BSC
- In this case, the 13 kbps flows must be transported without coding in the channels at 64 kbps
- On each PCM channel 4 13Kbps flows are multiplexed (after transformation into streams at 16Kbps with the addition of redundancy)
- For each GSM carrier (8 channels at 13 kbps)we need 3 PCM channels at 64 kbps
  - one for the signal carried by control protocol LAPD
  - 2 to carry the information of the multiplexed 8 telephone channels

Transcoder Rate Adaptation Unit (TRAU)



Base Station Controller (BSC)

- A BSC controls a large number of BTS: from several tens to several hundreds
- The main tasks of the BSC are:
  - the configuration of each cell by assigning traffic and control channels
  - The set up and release of connections between channels related to the A and Abis interface
  - the management of handovers between controlled BTS
  - the management of the paging messages: paging messages are distributed to the BTS in the LA where the user is located
  - the analysis of the link quality and power level measurements performed by the BTS and MS, and the decision of the necessity of handover

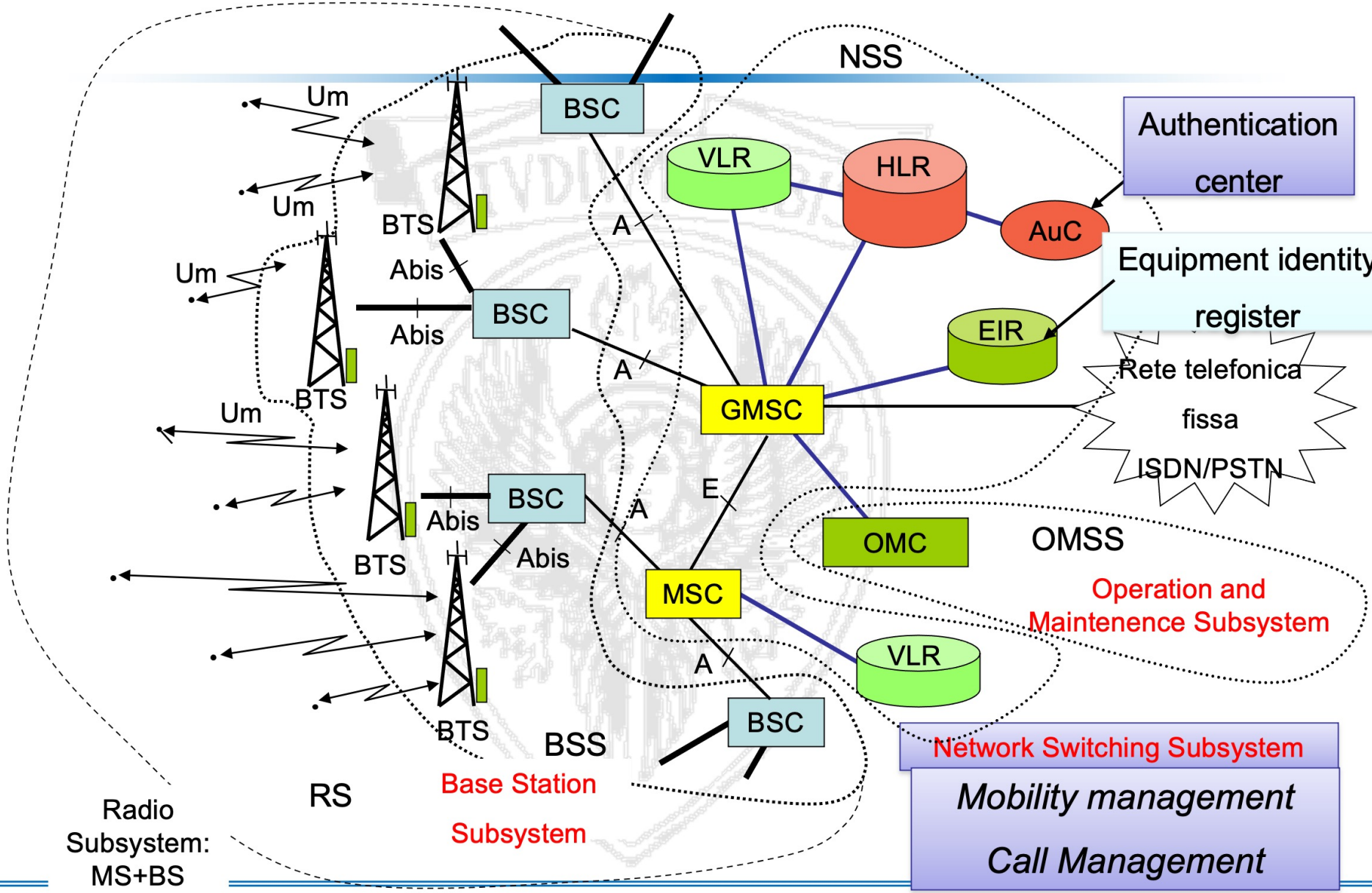
Base Station Controller (BSC)

- The BSC is basically concerned with the management of radio resources (Radio Resource Management)
- From the functional point of view it is a switching node,
  - but it does not perform the task of routing calls (that task is performed by the MSC)
  - instead it connects the circuits of the BTS with those of the MSC, possibly carrying out the trans-coding (TRAU)
  - It switches the circuits in case of handover (intra-BSC)
- The BSC can be placed at the site of an MSC or be standalone, or it can be positioned near (or together) to some BTS

Summary: BTS vs BSC

Main Function	BS	BSC
Management of radio channels		x
Mapping of upper layers to radio channels		x
Channel coding and rate adaptation	x	
Authentication		x
Encryption	x	x
Frequency hopping	x	
Uplink signal measurement	x	
Traffic measurement		x
Paging	x	x
Handover management		x
Location update		x

Network architecture



Network Switching Subsystem (NSS)

- It is the subsystem that is responsible for circuit switching to the mobile users, managing alsouse mobility. It includes:

- Mobile Switching Center (MSC):
  - ✓ Telephone switching center for mobile users
- Visitor Location Register (VLR):
  - ✓ It is a database (usually implemented in the central MSC) that contains information about users in the area managed by the MSC
- Home Location Register (HLR):
  - ✓ It is the main database that is responsible for storing the information of mobile users. It contains, among others, the information necessary to identify the VLR which is in charge of each subscribed user.
- Authentication Center (AuC):
  - ✓ normally associated with the HLR which contains the keys and the procedures for authenticating a mobile user. The AuC computes the keys for authentication and encryption.
- Equipmente Identity Register (EIR):
  - ✓ contains the IMEI of all devices authorized to access the service

Mobile Switching Centre (MSC)

- The MSC is a switching element which additionally performs mobility management
- It is normally associated with a VLR that stores data of those users currently located under its area
- The MSC is connected to the BSC of its (MSC/VLR) area as well as to other MSC
  - Connection is through PCM channels
  - part of the resources allocated for the interconnection support control information exchange, performed through SS7 common channel signaling.
  - One or more MSC (Gateway MSC) for each PLMN network us interfaced to the fixed telephone network for routing to and from fixed users.

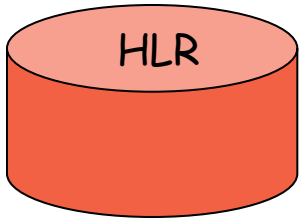
Mobile Switching Centre (MSC)

- An MS can be reached by fixed users using the phone number (MSISDN)
- The call is routed to the GMSC, which identifies the HLR that contains user information associated with the MSISDN and queries it to determine how to route to the mobile user current MSC
- the HLR returns the MSRN (Mobile Station Roaming Number)
  - It has in its record the VLR/MSC associated to the user and queries it to get the MSRN
- Temporary MSRN number (same struct. MSISDN) is assigned by the visited VLR
- MSRN to the GMSC allows the GMSC to route the call to the MSC area where the user is located

Mobile Switching Centre (MSC)

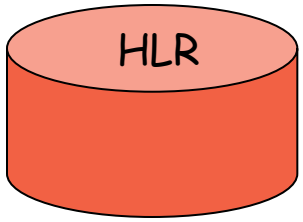
- The MSC provides the following functionalities
  - CM (Connection Management)
    - ✓originating call, terminating call, gateway
  - MM (Mobility Management)
    - ✓location updating, periodic registration, authentication, ecc.
- The MSC is the core entity in charge of signaling; It implements protocols to exchange information with other elements of the network
  - DTAP (Direct Tranfer Application Part)-protocol to exchange information over a logical channel with the MS
  - BSSMAP (BSS Management Application Part) protocol to exchange information with the BSC
  - MAP (Mobile Application Part) protocol to exchange information with the other network elements (MSC, VLR, HLR, EIR, AuC)

Home Location Register (HLR)



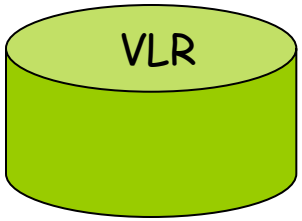
- It is a permanent database uniquely associated to a GMSC
- It stores information about all MS whose default location is at the considered GMSC
- HLR stores permanent information such as the IMSI (International Mobile Subscriber Identity), the identifier of the SIM card and its associated authentication key, supplementary services to which the user has subscribed, etc..
- HLR also stores temporary information such as the address of the VLR at which the user can be found, parameters for identification and encryption, any phone number listed for call forwarding, etc..

Home Location Register (HLR)



- Main tasks:
  - Managing localization, store the VLR number of each registered user
  - Sending routing information (MSRN) to the GMSC
  - Registration, Cancellation and activation/deactivation of additional services
  - storage and supply to the VLR of the parameters of authentication and encryption
  - management of user data

Visitor Location Register (VLR)



- It is a temporary database that contains important data for serving the MS currently under the jurisdiction of the MSC to which the VLR is associated.
- All the permanent data of a user currently under that MSC/VLR area are duplicated in the VLR (i.e., they are not only stored in the HLR but also in that VLR), with the difference that the IMSI is "mapped" on a TMSI (Temporary Mobile Subscriber Identity) to avoid transmitting the IMSI in clear and protect the user from "intrusion". The TMSI is changed frequently and is also linked to the location of the mobile (cell identifier)
- VLR plays a fundamental role in the management of the calls that come from MS

Security procedures

- Authentication:
  - has the task of verifying the user's identity and protect against fraudulent use of identification
- Encryption:
  - The confidentiality of the communication itself on the radio link is performed by the application of encryption algorithms and frequency hopping, which could only be realized using digital systems and signaling.

- The subscriber's anonymity is also ensured through the use of temporary identification numbers.

Security procedures

- K_i
  - ✓ user authentication key of 128 bits stored in the SIM and AUC
- *RAND*
  - ✓ 128-bit random number generated by the AuC and then sent to the MSC
- *A3*
  - ✓ authentication algorithm stored in the SIM and AuC
- *A8*
  - ✓ algorithm that determines the encryption key Kc, which is stored in the SIM and AuC

Output of the procedures:

- K_c
  - Encryption key
- *SRES*
  - Output of the authentication algorithm

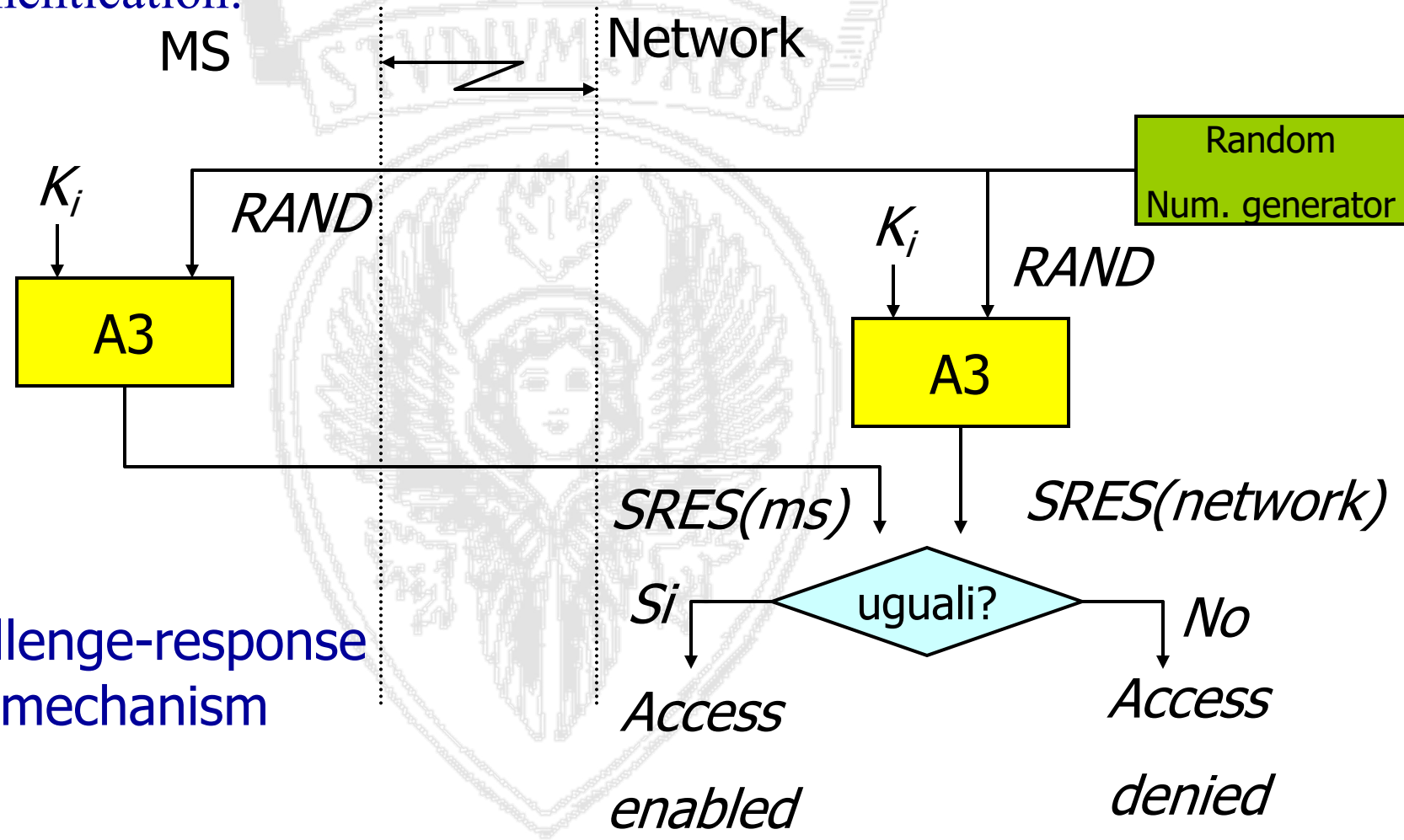
Triplets

(*RAND, SRES,* K_c)

are generated sequentially for each IMSI and stored in in the HLR

Security procedures

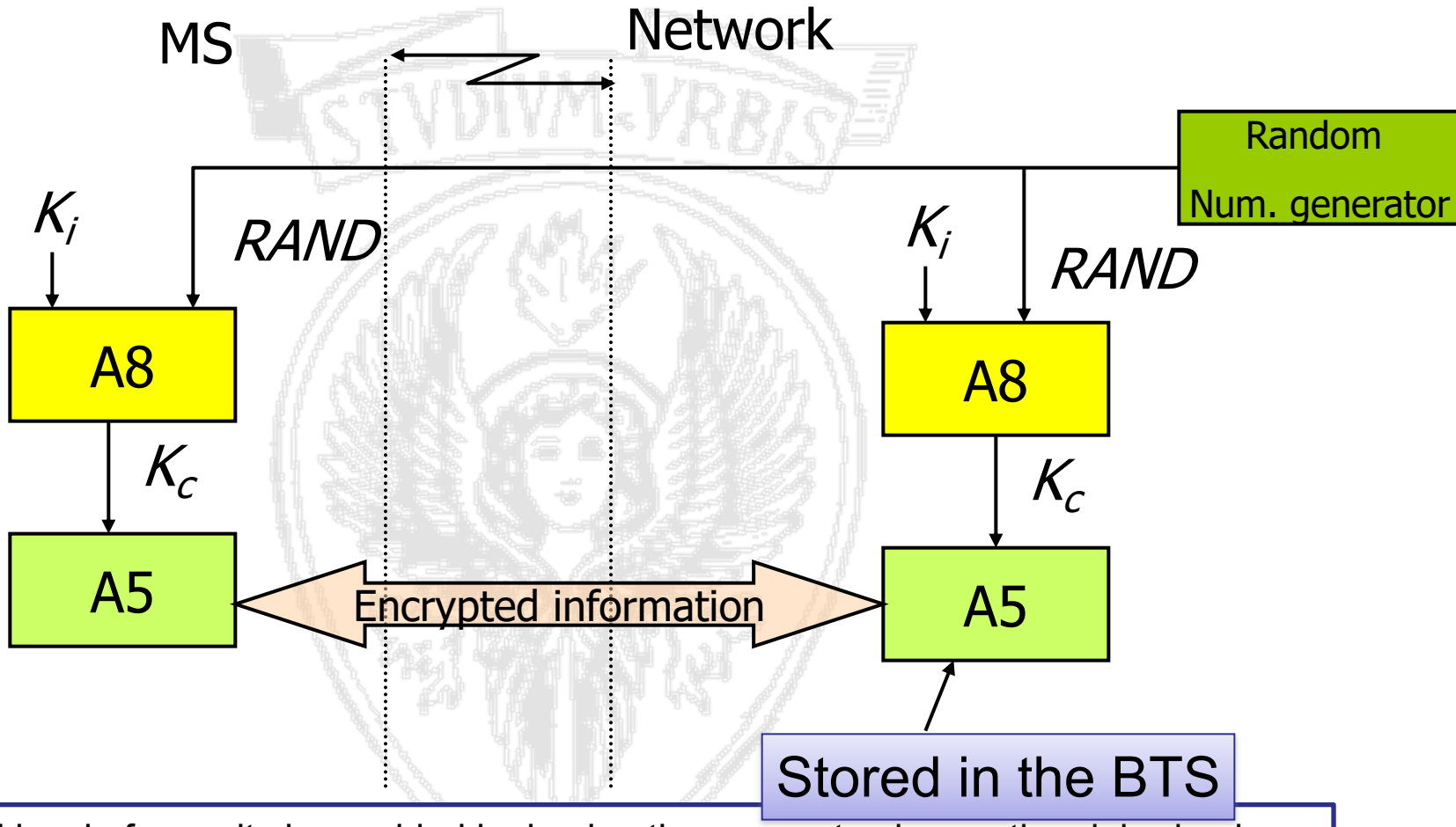
- Authentication:



Challenge-response mechanism

Security procedures

- Encryption

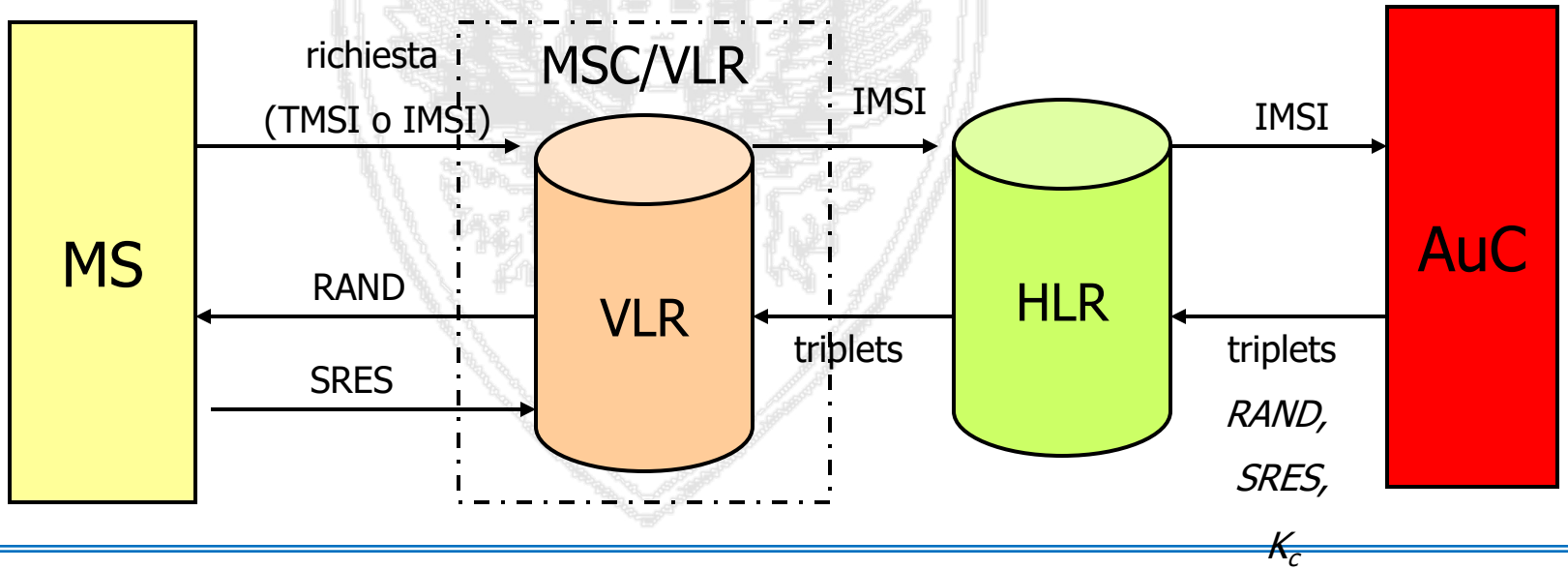


An additional level of security is provided by having the means to change the ciphering key, making the system more resistant to eavesdropping. The ciphering key may be changed at regular intervals as required by network design and security considerations.

Security procedure: network elements involved

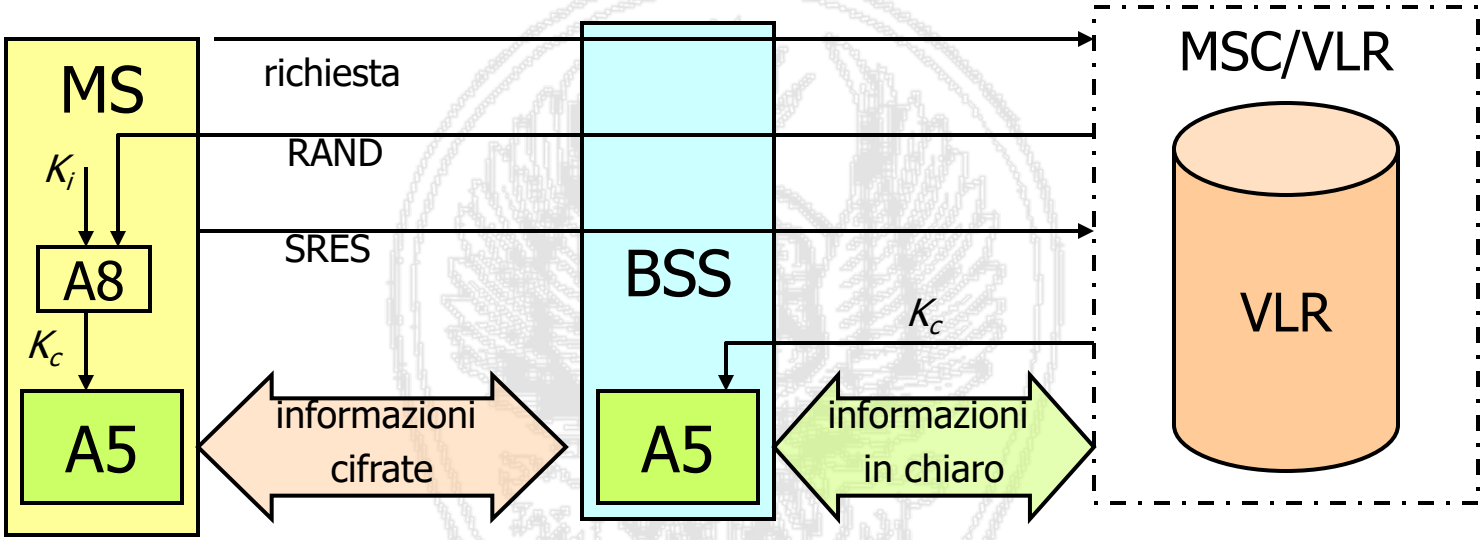
- Autentication Centre (AuC)
  - stores the secret keys K_i for each user
  - generates random numbers and calculates SRES and the encryption key K_c
  - Provides the triplets to the other network elements

AuC



Security procedure: network elements involved

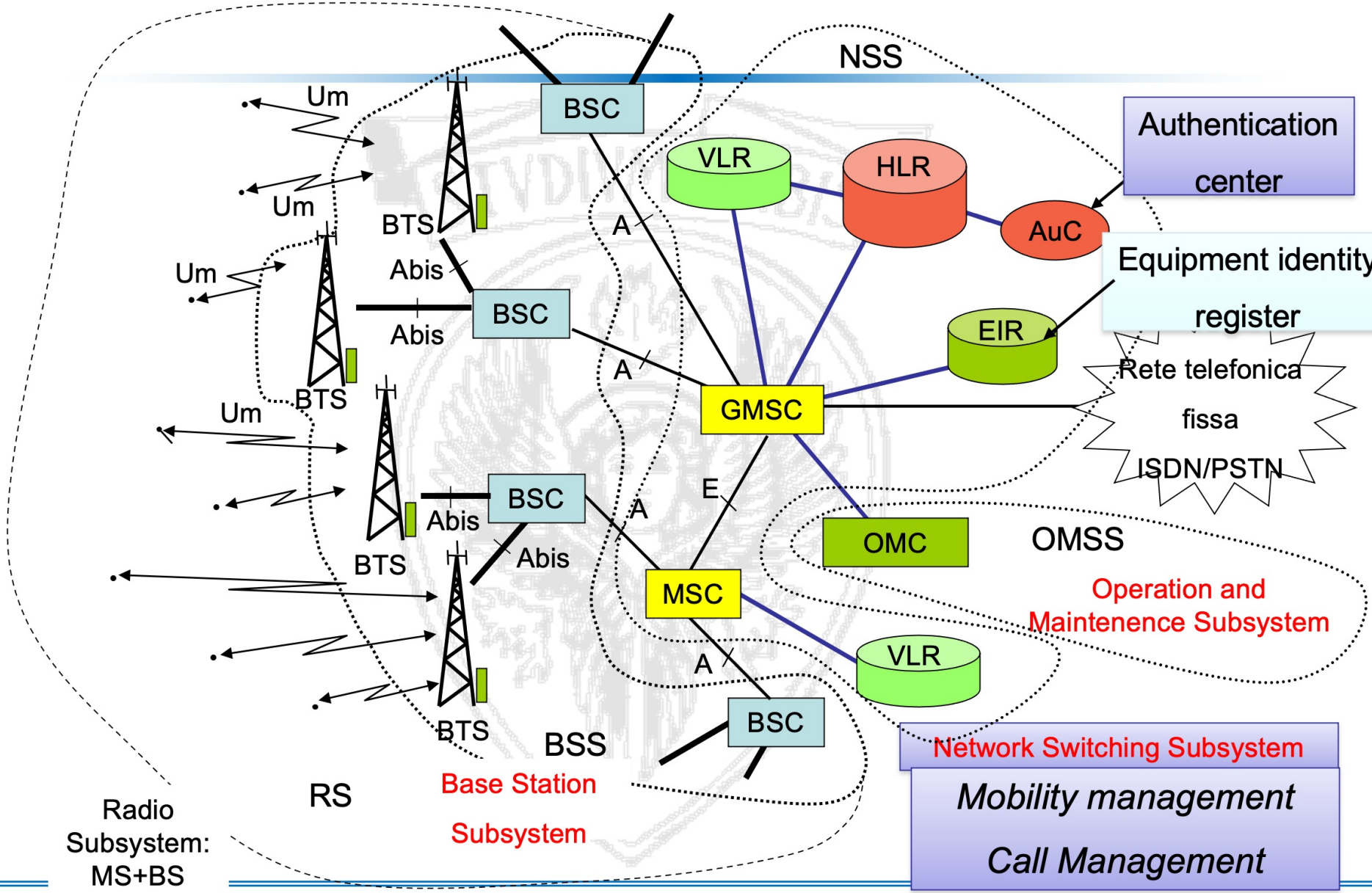
- BSS/NSS elements involved in data encryption



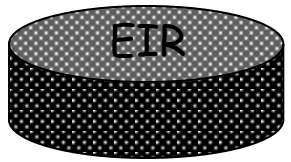
Security procedures: TMSI allocation

- To initiate a communication the MS sends its ID (IMSI) to identify itself before starting the authentication procedure
- To minimize risk of malicious devices being able to intercept the IMSI, the VLR allocates a TMSI to each MS (TMSI=Temporary Mobile Subscriber Identity)
- IMSI is transmitted only upon the MS gets a TMSI, then. The TMSI is used to identify the MS
- Every time a location update is performed the VLR allocates a new TMSI to the MS.

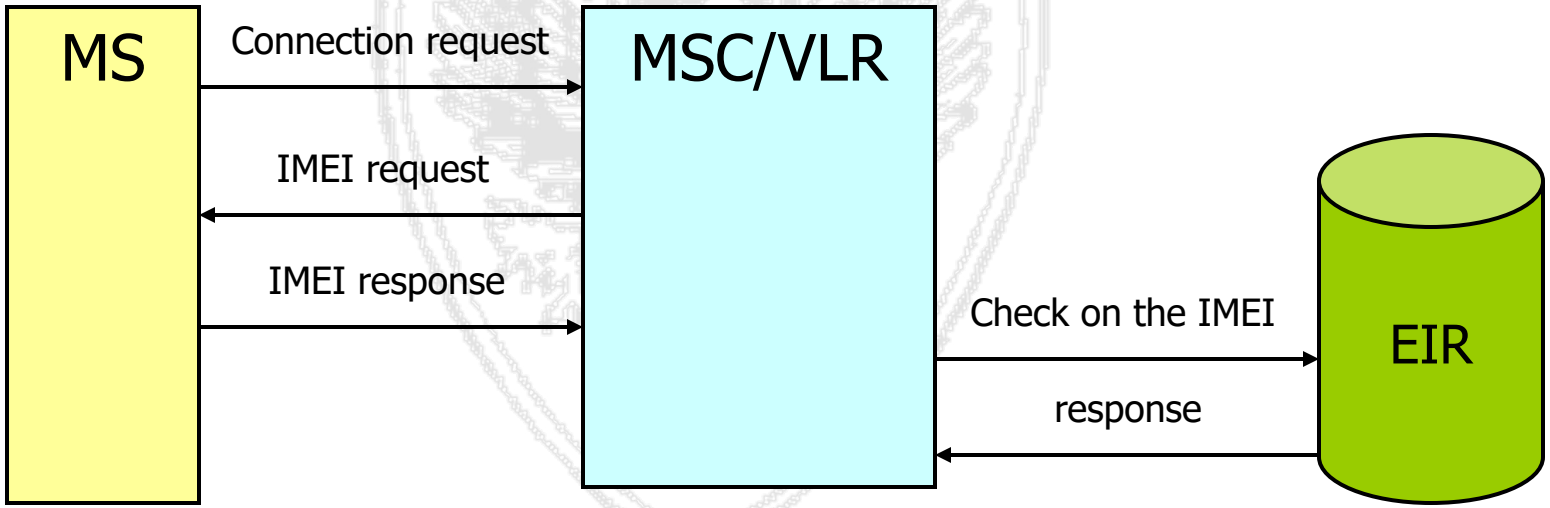
Network architecture



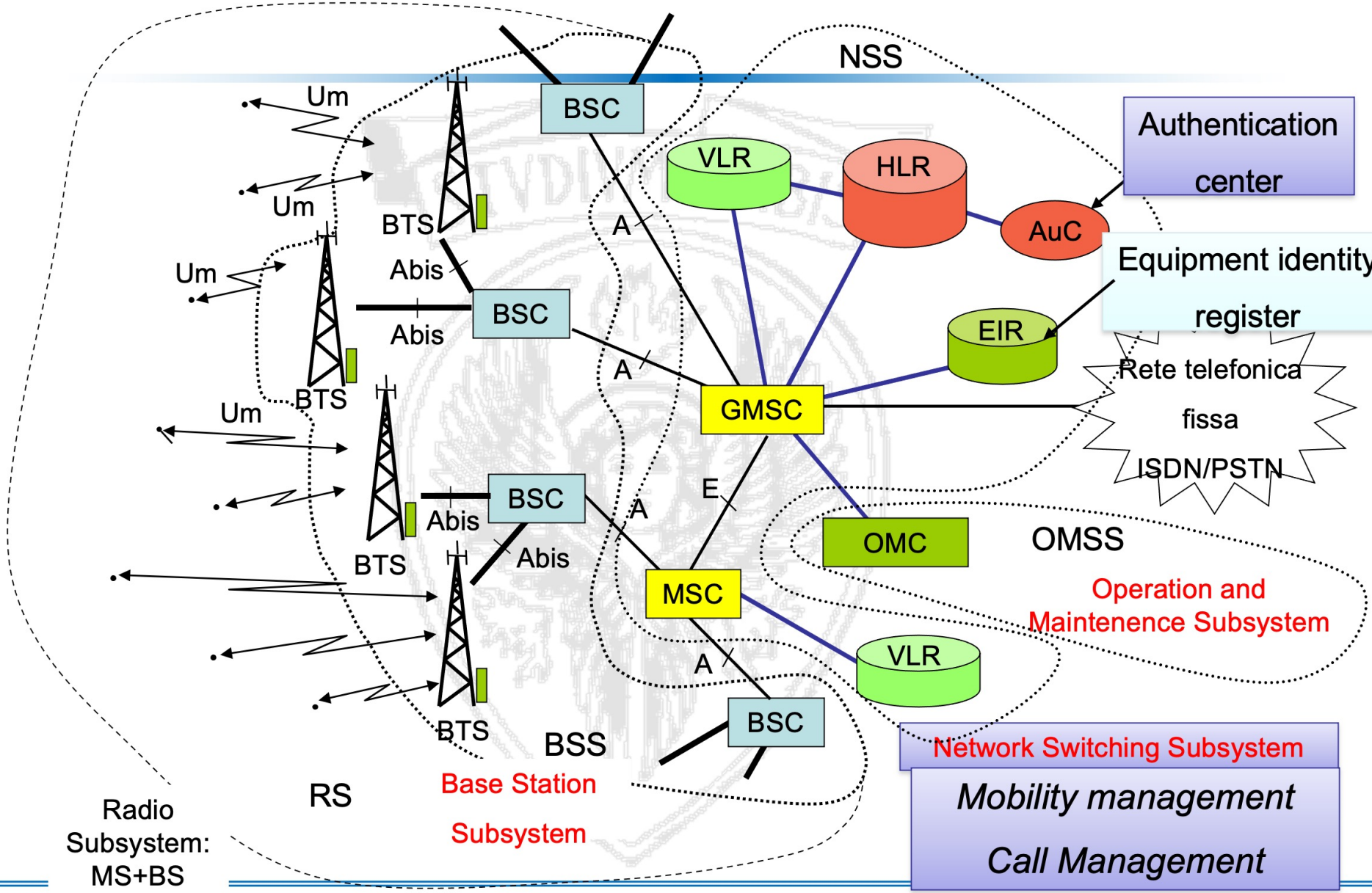
Equipment Identity Register (EIR)



- Database whose use is at the discretion of the operator
- Contains the identification and characteristics of GSM terminal equipment (TE), together with the manufacturer, country of manufacture, etc.
- It can be used to protect the network from the use of equipment stolen or not compliant to standard



Network architecture



Operation and Maintenence Subsystem (OMSS)

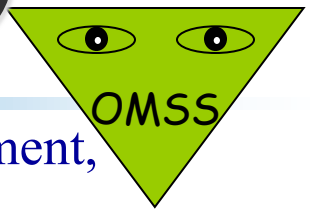
- Include the functional units responsible for monitoring the network, its maintenance and remote management
- It deals with:
  - configuring the functionality of all network devices
  - displayed alarms on malfunctioning elements
  - shows the statistics on data traffic
- etc..

Operation & Maintenance Sub-system (OSS)

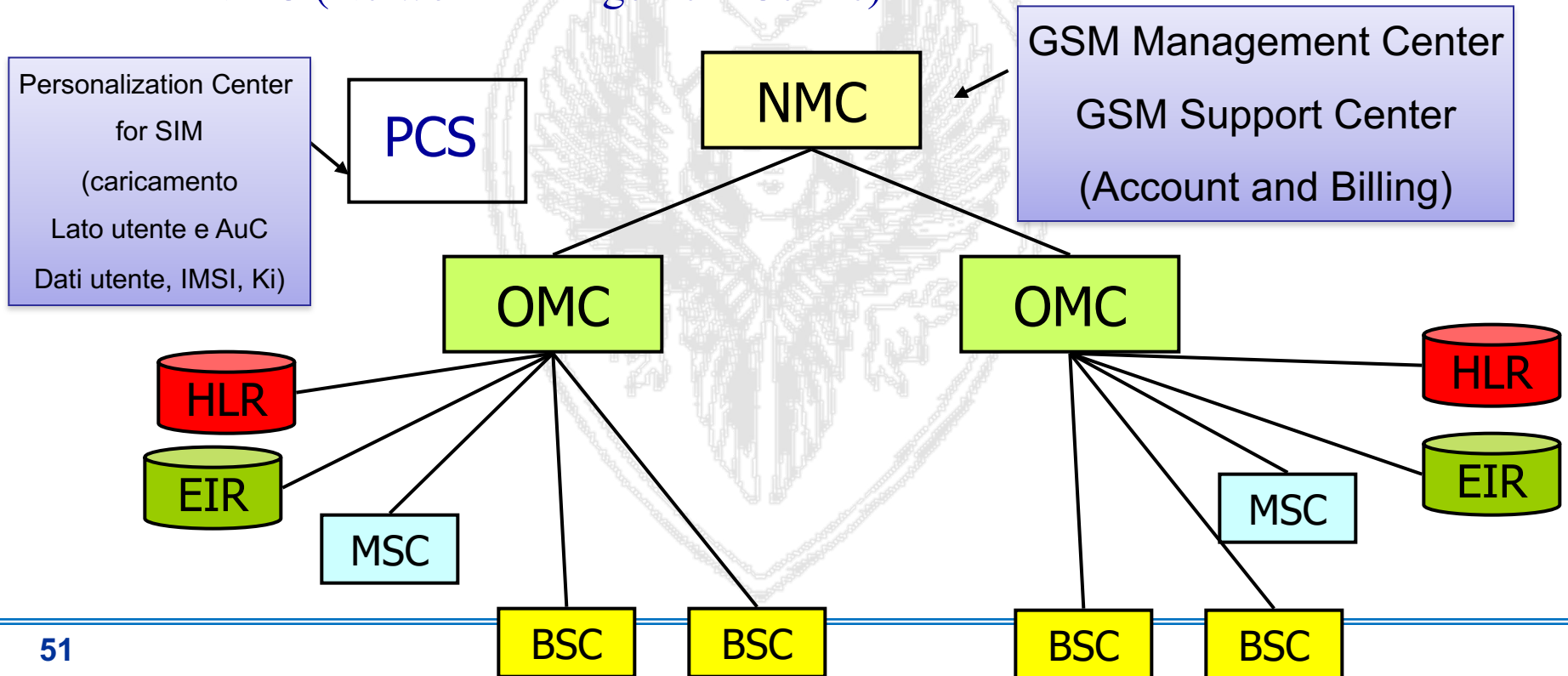
- Network measurement and control functions
- Monitored and initiated from the OMC (Operation and Maintenance Center)
- Basic functions
  - Network Administration
    - ✓ configuration, operation, performance management, statistics collection and analysis, network maintenance
  - Commercial operation & charging
    - ✓ Accounting & billing
  - Security Management
    - ✓ E.g. Equipment Identity Register (EIR) management

O&M functions based on ITU-T TMN standards (Telecommunication Network Management) – complex topic out of the scopes of this course

Operation and Maintenance Subsystem (OMSS)



- Includes the functional entities in charge of network management, operation and maintenance
- Hierarchical structure
  - Regional OMC (Operation & Maintenence Centre)
  - NMC (Network Management Centre)



Numbers and IDs in GSM

Utsed for routing

- Mobile Station ISDN Number (MSISDN)

It is the user mobile telephone number

Country Code - National Destination Code –Subscriber Number

It is associated to a specific HLR

- Mobile Station Roaming Number (MSRN)

It is assigned by the current VLR; it is communicated (upon request) to the HLR which gives it to the requesting GMSC; it allows the GMSC to establish a circuit till the current Mobile User position

- Handover Number (communicated by the target MSC to the initial MSC in case of inter-MSC handover; it allows to reroute the call till the target MSC)

Numbers and IDs in GSM

- International Mobile Subscriber Identity (IMSI)

Permanently stored in the SIM and HLR, temporarly in the VLR; uniquely indetifies the subscriber

Mobile Country Code (3 cifre)--Mobile Network Code(2)—Mobile Subscriber Identification Number

- Temporary Mobile Subscrier Identity (TMSI)

Temporary ID assigned by a VLR to an MS; it allows to avoid transmitting the IMSI in clear on the radio channel (or to transmit it only when switching on). It has a non standardized structure, and a size equal to 4 octects.

- International Mobile Equipment Identity (IMEI)

Uniquely identifies a terminal equipment (HW). It is stored in HW at the time the HW is produced.

TAC =Type Approval Code (6 cifre); FAC (Final Assembly Code), 2 digits (production/assembly site), SNR(Serial Number), 6 digits

ID associated to a mobile entity

Numbers and IDs in GSM

- Location Area Identity (LAI)

It uniquely identifies the location area under which the MS is currently located. It is stored in the VLR. Structure:

Mobile Country Code, Mobile Network Code (operatore), Location Area Code

- Cell Global Identity (CGI), it identifies the cell (Structure: LAI+Cell Identity that is the ID which identifies the cell within its location area)
- Regional Subscription Zone Identity (RSZI)
- Used in case of subscription only to a service within a regional area. The ID allows to specify within which regiones users can roam.
- Base Station Identity Code (BSIC)

It is a "color code" which allows the MS to distinguish among signals received by adiacent BTS. Each BTS broadcasts its BSIC on the logical Synchronization channel (SCH) on a predefined carrier.

Info stored in GSM network

- IMSI (→HLR,VLR)
- MSISDN (→HLR, VLR)
- TMSI (→VLR)
- MS category (→HLR,VLR)
- RAND,SRES,Kc (→HLR, provided upon request to the VLR)
- MSRN (→VLR, provided to the HLR upon request)
- LAI (→VLR)
- VLR number (→HLR)
- HLR number (→VLR)
- subscription restrictions (→HLR)
- data associated to basic and supplementary services (→HLR,VLR)
- IMSI detached flag (→VLR)
- Call barring (→HLR, some VLR)

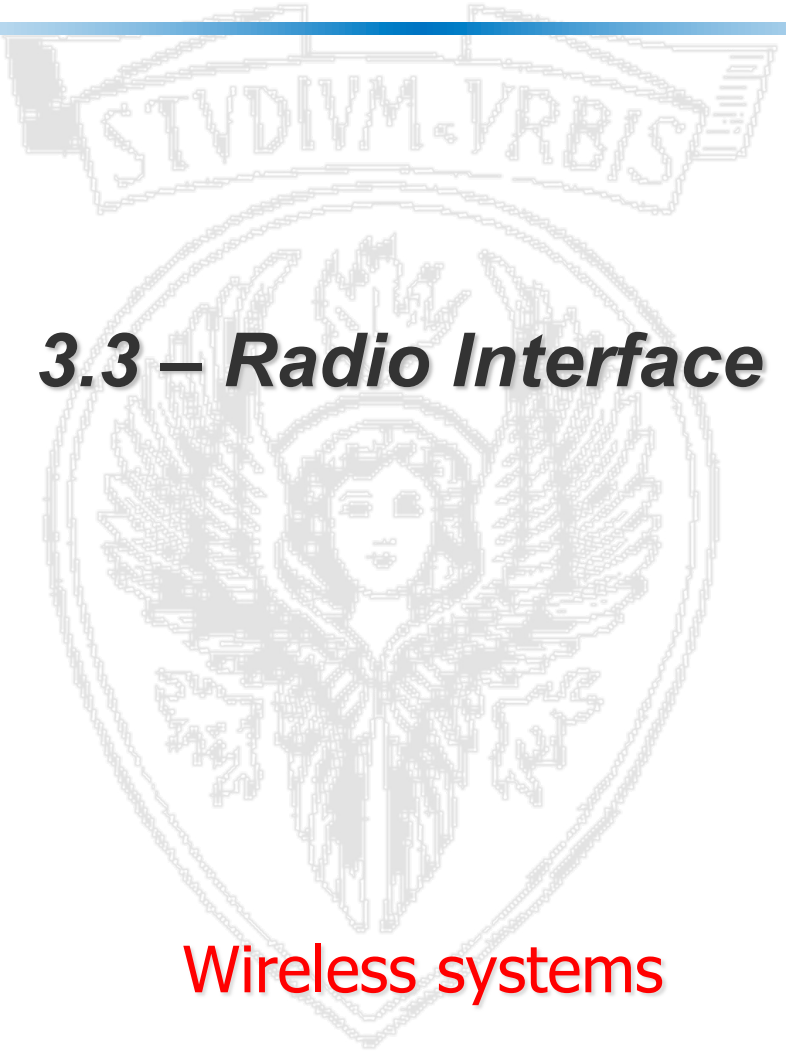
IoT, Course introduction

Internet of Things a.a. 2023/2024

Un. of Rome “La Sapienza”

Chiara Petrioli

Department of Computer Engineering – University of Rome “Sapienza” – Italy



3.3 – Radio Interface

Wireless systems

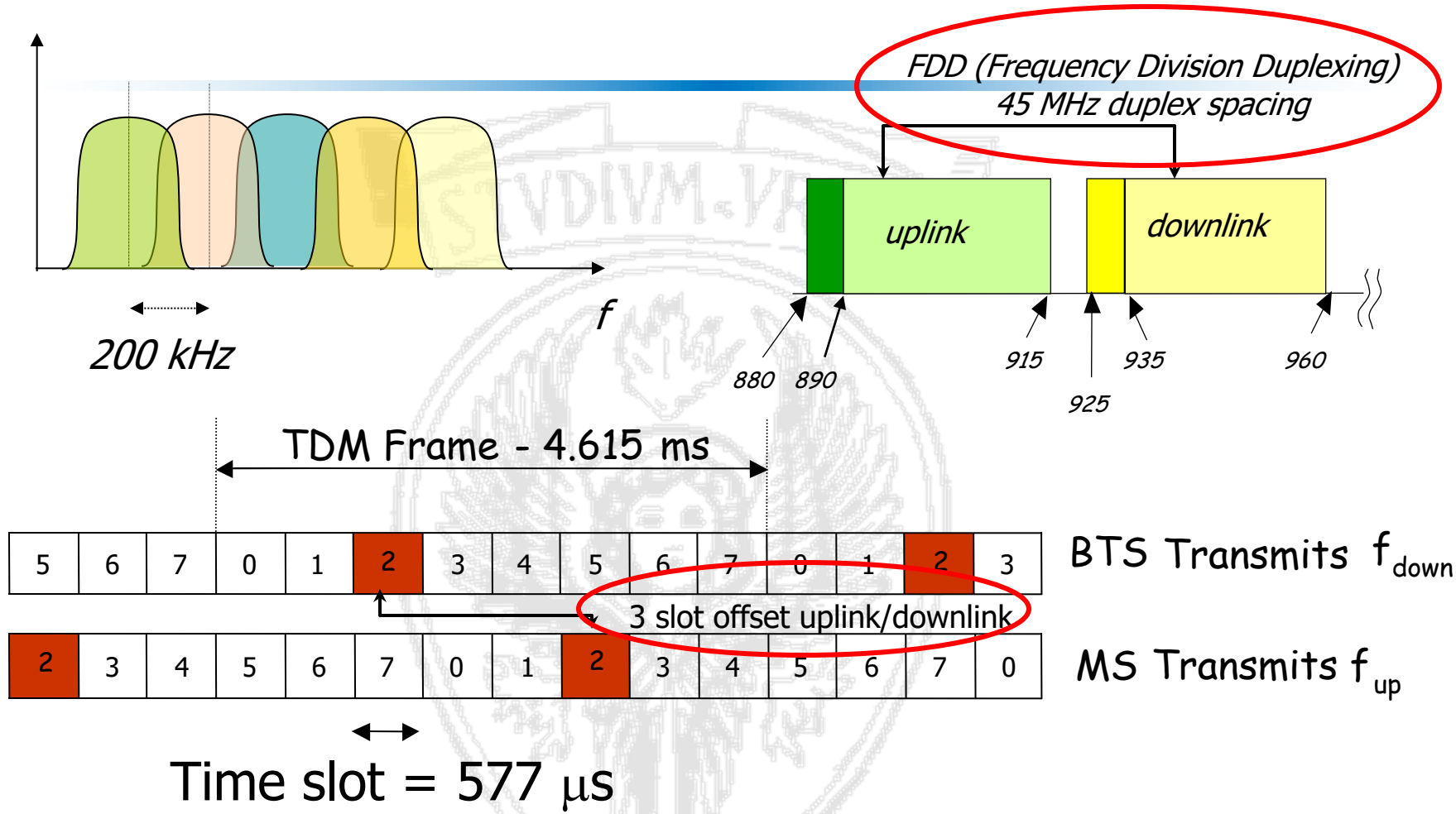
Radio Interface

si veda

- O. Bertazioli, L. Favalli, *GSM-GPRS*, Hoepli Informatica 2002

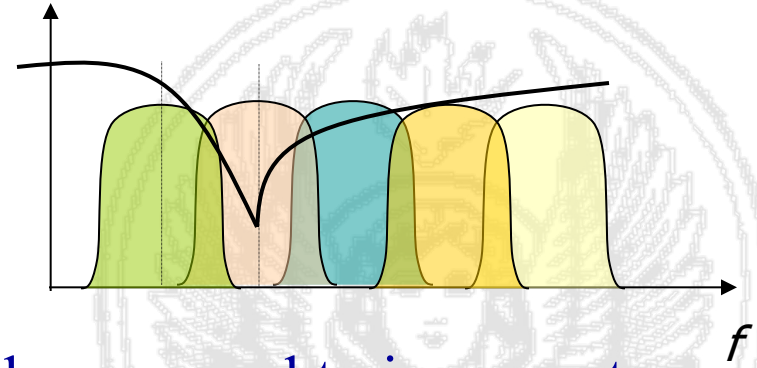
Capitolo 6

Radio Interface



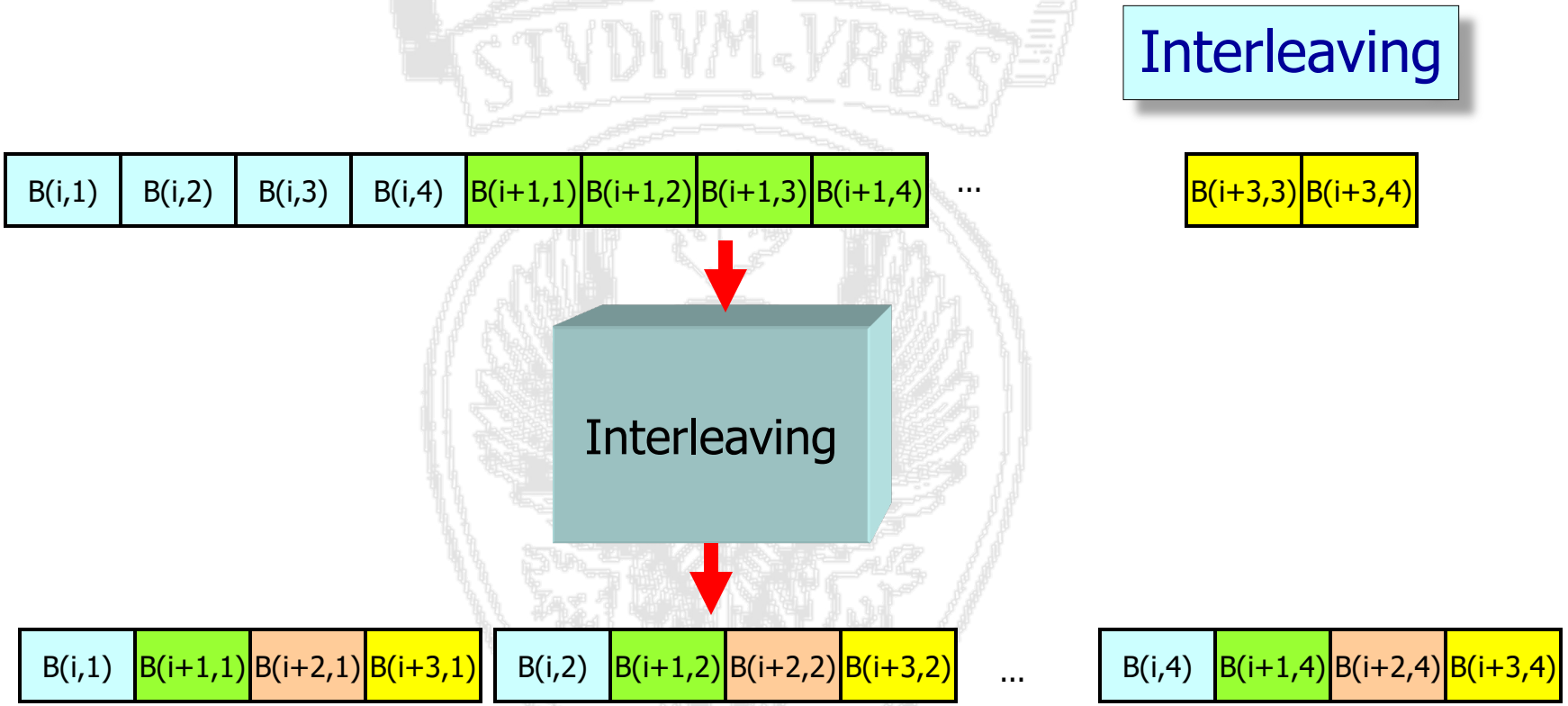
Frequency Hopping

- Multipath fading depends on the carrier used for transmission
- At a given time, when transmitting to a user some carriers may suffer high attenuation while others low attenuation



- Since FEC codes are used to increase transmission robustness, it is better if the errors due to the high attenuation suffered by a carrier are spread over multiple information flows (similarly to what we have seen when we discussed interleaving techniques)
- Frequency hopping changes the carrier used for transmission on a per slot basis, according to a predefined pseudorandom sequence

Interleaving



Power Control

- The output power of the MS is controlled by the BTS
- The BTS sends power control commands that require the MS to raise or lower the transmit power
- The step increment / decrement is 2 dB
- The objective of the control is to bring the power received from the BTS to a predetermined level (just above what needed for reception)
- The power control reduces the interference in the system by reducing the average power of the MS with little attenuation of the channel (close to BTS)
- The power control also reduces the energy consumption of the MS

GSM Syncrhonization

- Carrier frequency synchronization
  - Each MS must retrieve precisely the frequency of the radio carrier
- Slot synchronization
  - Each MS must have information on the current slot
- Frame synchronization
  - Each MS must know the current Frame Number
- Base station synchronization (optional)
  - The base stations have synchronous clocks
  - The base stations have the same Frame Number

Carrier frequency synchronization

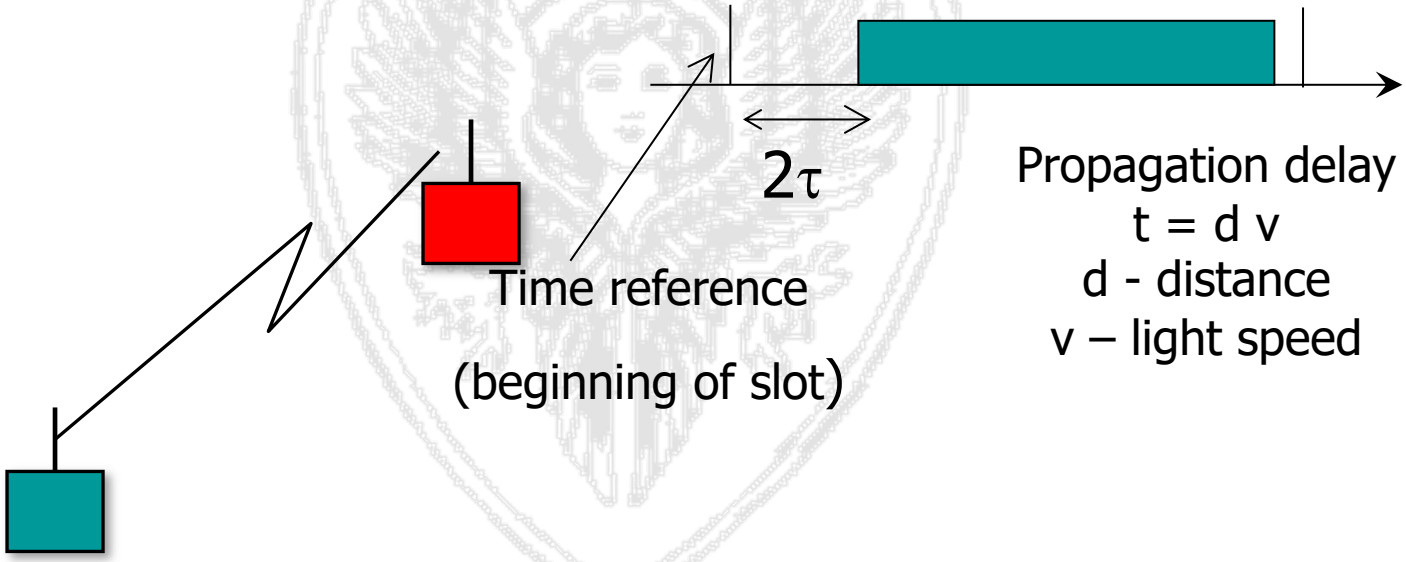
- The frequency of the radio carrier is obtained by the MS listening to the broadcast common control channel transmitted by the BTS
- On this channel, at regular intervals, a special fixed sequence of bits is transmitted at high power that is used to select the carrier frequency, and then adjust the frequency of the local oscillator

Slot and frame synchronization

- Many channels in GSM follow a multiframe structure (for example, the broadcast channel is broadcast every x frames)
- The sequence of frequency hopping depends on the multiframe structure
- Each MS must therefore know the number of the current frame to correctly interpret the information
- The BTS transmits on the broadcast channel the information needed for the MS to be able to reconstruct the current time slot and Frame Number

Slot synchronization

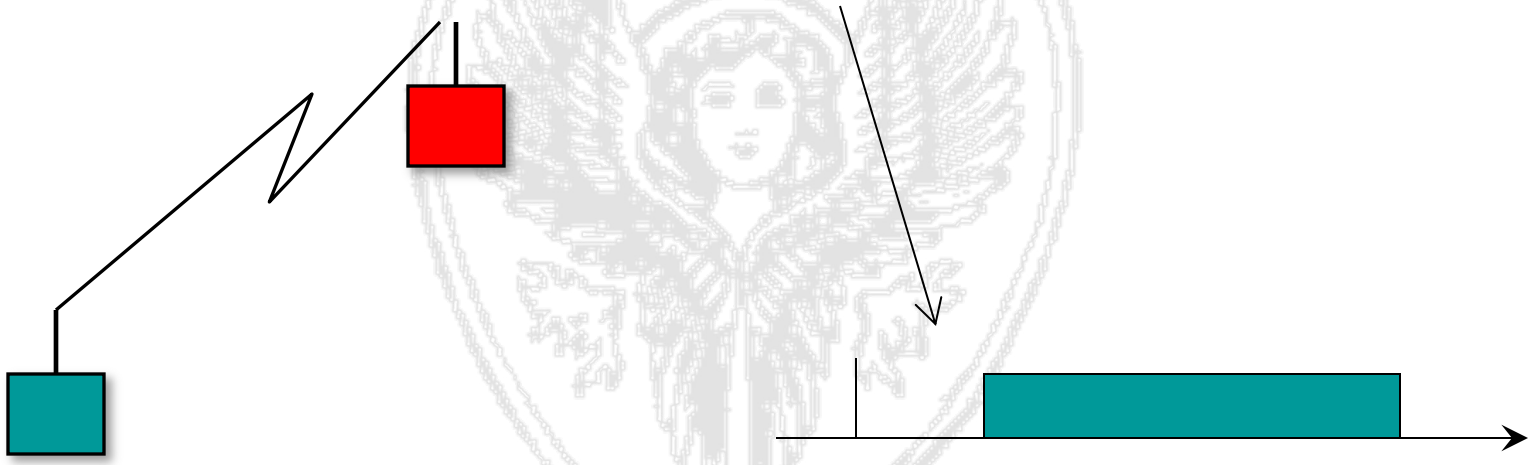
- Up/down link transmissions go through propagation delays which depend on the relative distance between the BTS and the MS
- Each slot needs to have a guard period to compensate for synchronization errors



Slot synchronization

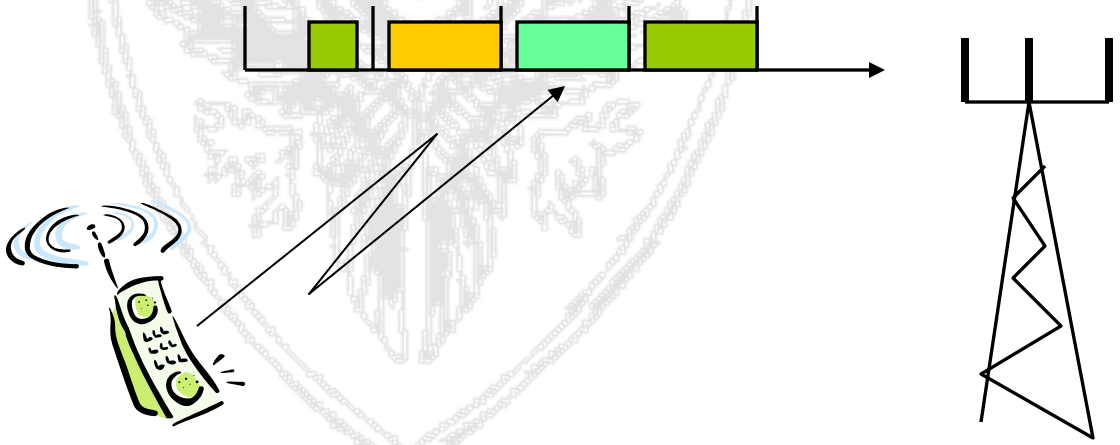
- We could make a conservative selection, setting the guard time to

$$T_g = \max_i (2\tau_i)$$



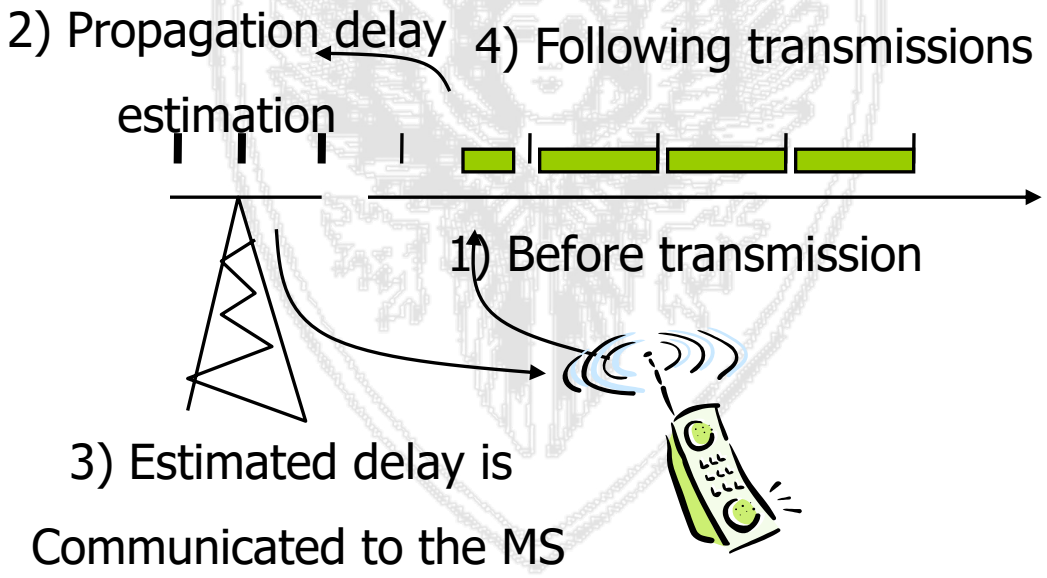
Slot synchronization

- The GSM network is designed to have cells with R_{max} = 35 Km
- In the worst situation (at the borders of the cell) there is a guard time of $2\tau = 2 \times 35 / 3 \times 10^8 = 233\ \mu s$
- which corresponds to 68.25 bits at the rate of 270.8 kb / s



Slot synchronization: Timing Advance

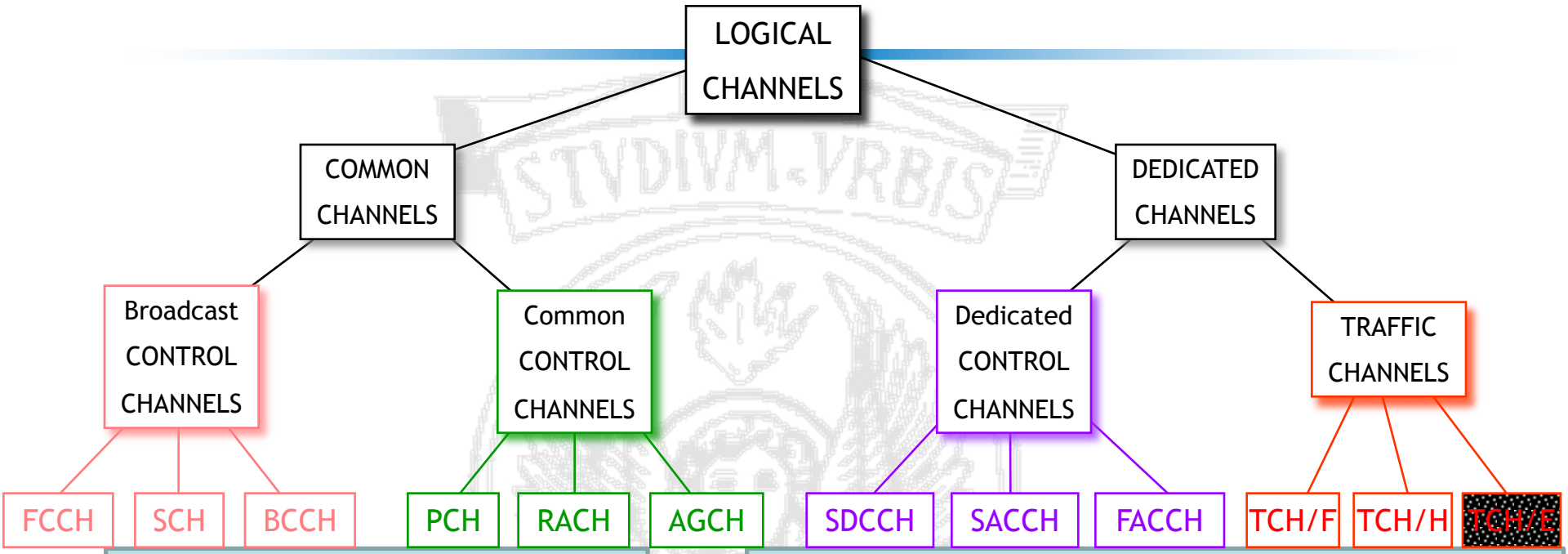
- To limit guard time:
- the BTS estimates the delay and sends the information to the MS which can then compensate by anticipating the transmission
- used in GSM : transmission is anticipated as the MS moves away from the BTS (timing advance, reduces the guard time to about 9 bits, equal to 33,3 msec)



Logical Channels

- Uniquely identify the type of information they carry:
  - Signaling (e.g., synchronization info, ...)
  - Data traffic
- Channels types:
  - Traffic channels vs. control channels
  - Common channels vs. dedicated channels

Logical Channels

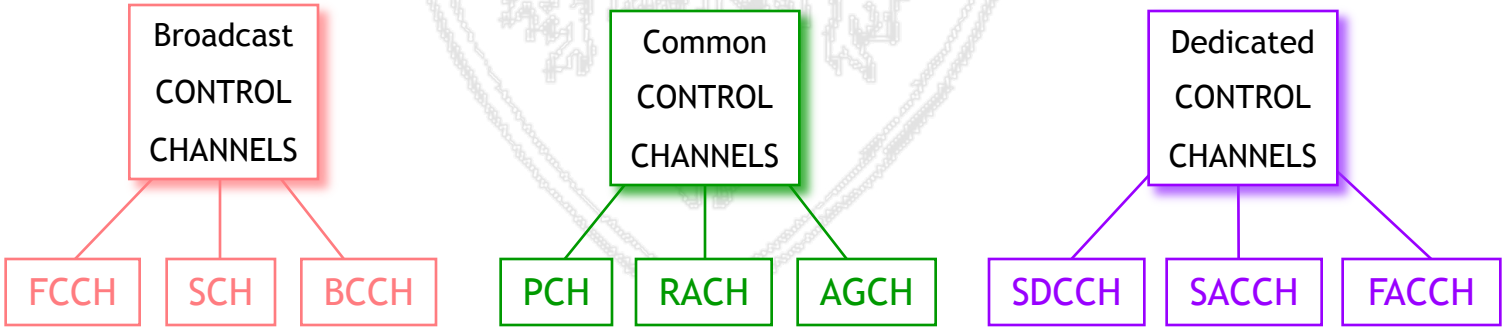


FCCH=Frequency Correction CHannel
SCH=Synchronisation Channel
BCCH=Broadcast Control CHannel
PCH=Paging CHannel
RACH=Random Access CHannel
AGCH=Access Grant CHannel

SDCCH=Stand-alone Dedicated Control CHannel
SACCH=Slow Associated Control CHannel
FACCH=Fast Associated Control CHannel
TCH/F=Traffic CHannel Full rate
TCH/H=Traffic CHannel Half rate
TCH/E=Traffic CHannel Enhanced Full rate

Control Channels-CCH

- Control channels carry signaling information (14 types of control channels are defined!!)
- Three main categories of CCH:
  - Broadcast Channels (BCH): unidirectional downlink channels providing general information about the network
  - Common Control Channels (CCCH): carry information for initiating a connection (shared between multiple connections)
  - Dedicated Control Channels (DCCH): carry signaling information specific for a single connection



Broadcast Channels - BCH

- FCCH (Frequency Correction Channel): downlink channel used to correct MS frequency, 148 bits without coding
- SCH (Synchronization Channel): carry the Base Station Identity Code (BSIC) and the frame number (FN), 25 bits + channel coding
- BCCH (Broadcast Control Channel): carry general information that are broadcasted to all user of a base station, 184 bytes after coding (parameters of the frequency hopping algorithm, number of common control channels allocated, number of blocks for the AGCH channel, info on adjacent cells, Location Area Code etc.).

Broadcast CONTROL CHANNELS

Common Control Channels - CCCH

- PCH (Paging Channel): downlink channel used by the BTS to notify an incoming call to a MS, broadcasted over a LA
- RACH (Random Access Channel): uplink channel used by a MS to request access to the network (Location Update, call request). Prone to collisions.
- AGCH (Access Grant Channel): downlink channel carrying reply to RACH requests.

Common
CONTROL
CHANNELS

Random Access Channel (RACH)

- Access to the RACH channel is random, i.e., not coordinated with other MSs
- The RACH channel is thus prone to collisions
- Access messages that are correctly received by the BS are acknowledged on the AGCH channel
- RACH messages include a temporary pseudo-random sequence that is included on the acknowledgment sent on the AGCH channel

Random Access Channel (RACH)

- Access to the RACH channel is random, i.e., not coordinated with other MSs
- The RACH channel is thus prone to collisions
- Access messages that are correctly received by the BS are acknowledged on the AGCH channel
- RACH messages include a temporary pseudo-random sequence that is included on the acknowledgment sent on the AGCH channel
- Transmissions on the RACH channel use the *Slotted-ALOHA* protocol

Dedicated Control Channels – DCCH

- SACCH (Slow Associated Control Channel): bidirectional channel used to exchange connection metrics between MS/BS and BS/MS (e.g., received signal strength, quality….). Multiplexed with user traffic (184 bits)
- FACCH (Fast Associated Control Channel): used for exchange of time critical information (urgent handover request). The FACCH transmits control information by "stealing" capacity from the associated traffic channel.
- SDCCH (Stand-alone Dedicated Channel): stand-alone dedicated control channel that is assigned after a RACH request (authentication messages, call set-up…)

Dedicated CONTROL CHANNELS

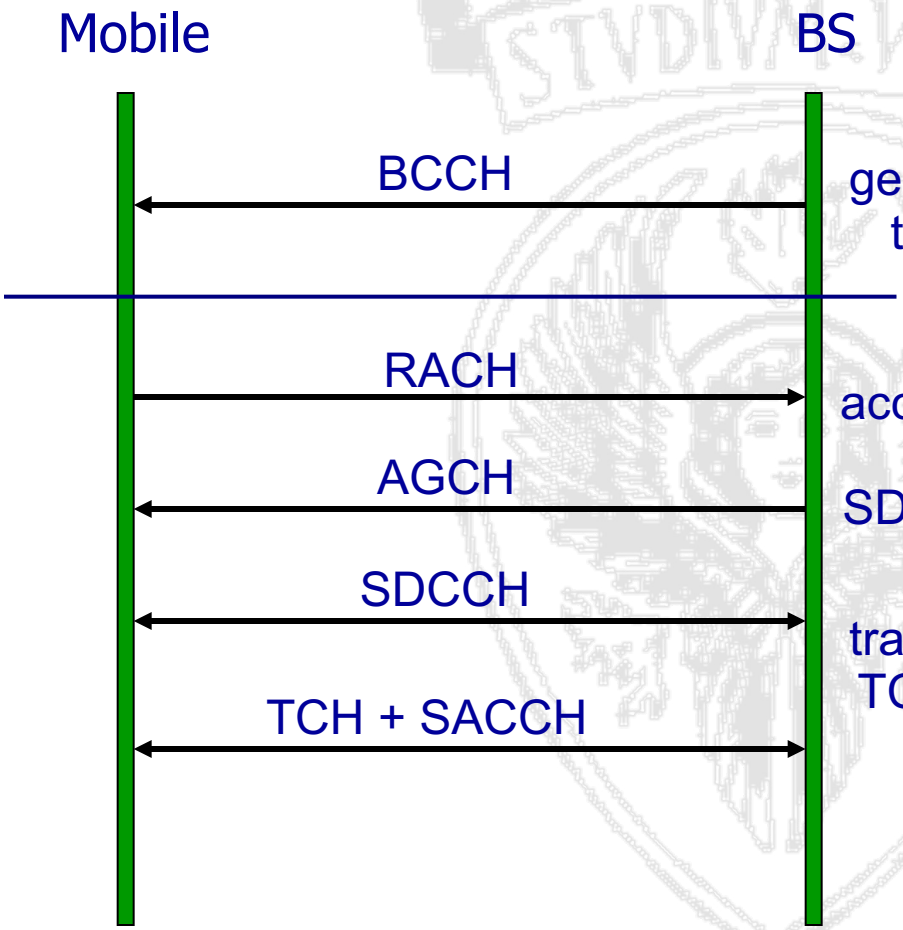
Slow Associated Control Channel (SACCH)

- Downlink:
  - Power control commands
  - Timing advance commands
  - BCCH information (that can no longer be decoded by the MS after it switches to the traffic channel)
- Uplink: MS measurements report:
  - RXLEV-SERVING-CELL (signal strength from own BTS) RXQUAL-SERVING-CELL (downlink BER)
  - RXLEV-NCELL “N” (signal strength from adjacent cells)
  - BCCH-FREQ-NCELL “N” (# BCCH carrier of adjacent cells)
  - BSIC-NCELL “N” (BSIC of adjacent cells)

Dedicated CONTROL CHANNELS

Set-up of a traffic channel

The MS tunes to a BTS and synchronizes with the frame structure in its cell by using FCCH, SCH, and BCCH.



general information about the network, the cell in which the MS is currently located and adjacent cells

access request

SDCCH assignment

traffic signaling + TCH assignment

SACCH info

The following signalling messages are sent on the downlink SACCH:

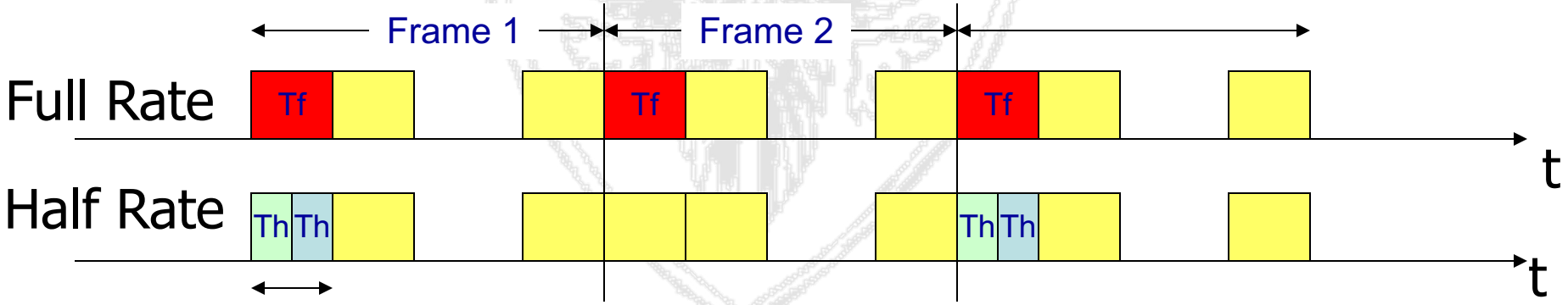
- power command,
- time advancement,
- frequency hopping sequence,
- frequencies used by adjacent channel.

he uplink SACCH contains values of:

- Frame–Error Rate (FER) of the downlink traffic channel,
- Received signal level from neighbour cells.

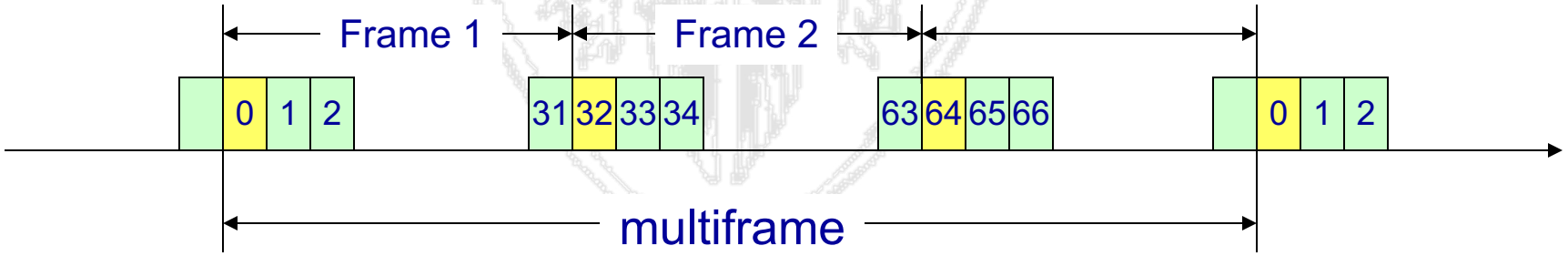
Traffic Channels-TCH

- Traffic channels (TCH) carry speech and data
- Two types of TCH:
  - Full Rate channels: gross rate of 22,8 Kb/sec (including coding incorporated for error protection)
  - Half Rate channels: gross rate of 11,4 Kb/s



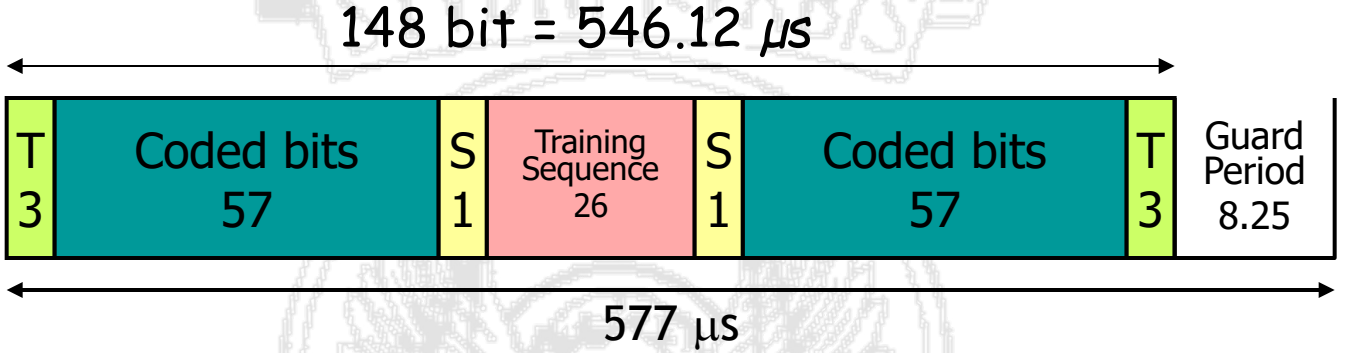
Mapping of logical channels onto physical channels

- Signaling requires lower bit rates than user transmissions (it wouldn't be efficient to assign a whole slot per frame to signaling)
- Actual transmission rate may be reduce by using **multiframes**
- IDEA: slots are associated with IDs, and may be assigned over a period of multiple frames, i.e., over a multiframe



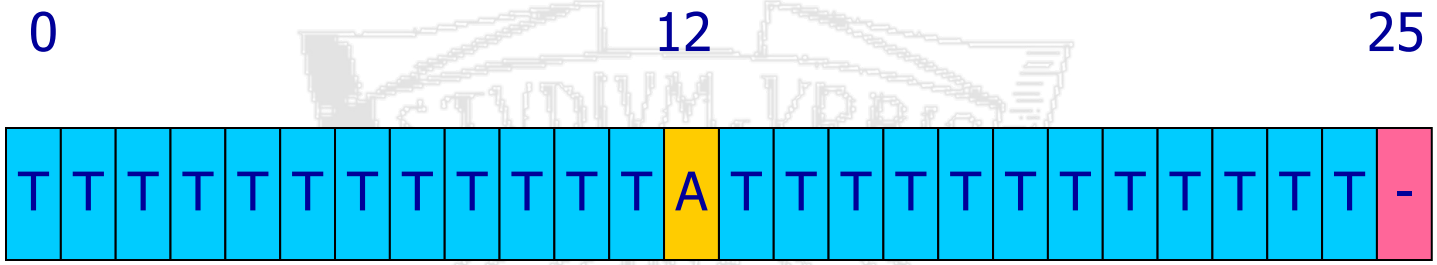
Multiframe example: SACCH

- A normal data burst carries 114 bits of data



- A channel using one slot per frame has a rate of 114 [bit]/4.6 [ms]=24.7 Kb/s
- Coded speech is transmitted at a rate of 22,8 Kb/s
- 1,9 Kb/s are not used, equal to 1 SLOT every 13 frames
- SACCH: 1 SLOT every 26 frames = rate of 950 bit/sec.

SACCH Signaling channels

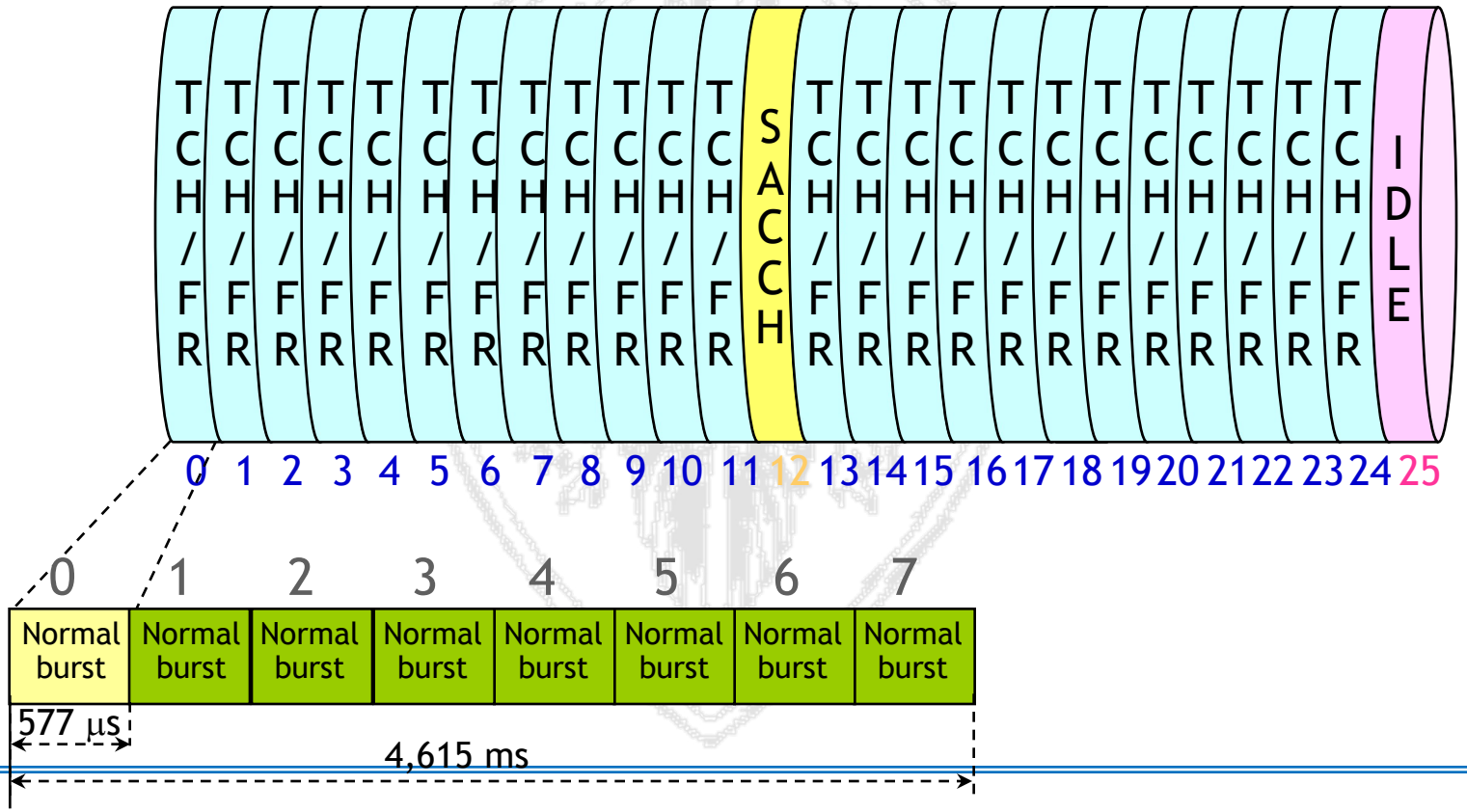


- The figure shows mapping of a full-rate traffic channel (TCH) (T) and its Slow Associated Control Channel (SACCH) (A) onto one physical channel
- SACCH is used for measurements exchange and commands
- A super-frame of 26 frames (120 ms) is used.

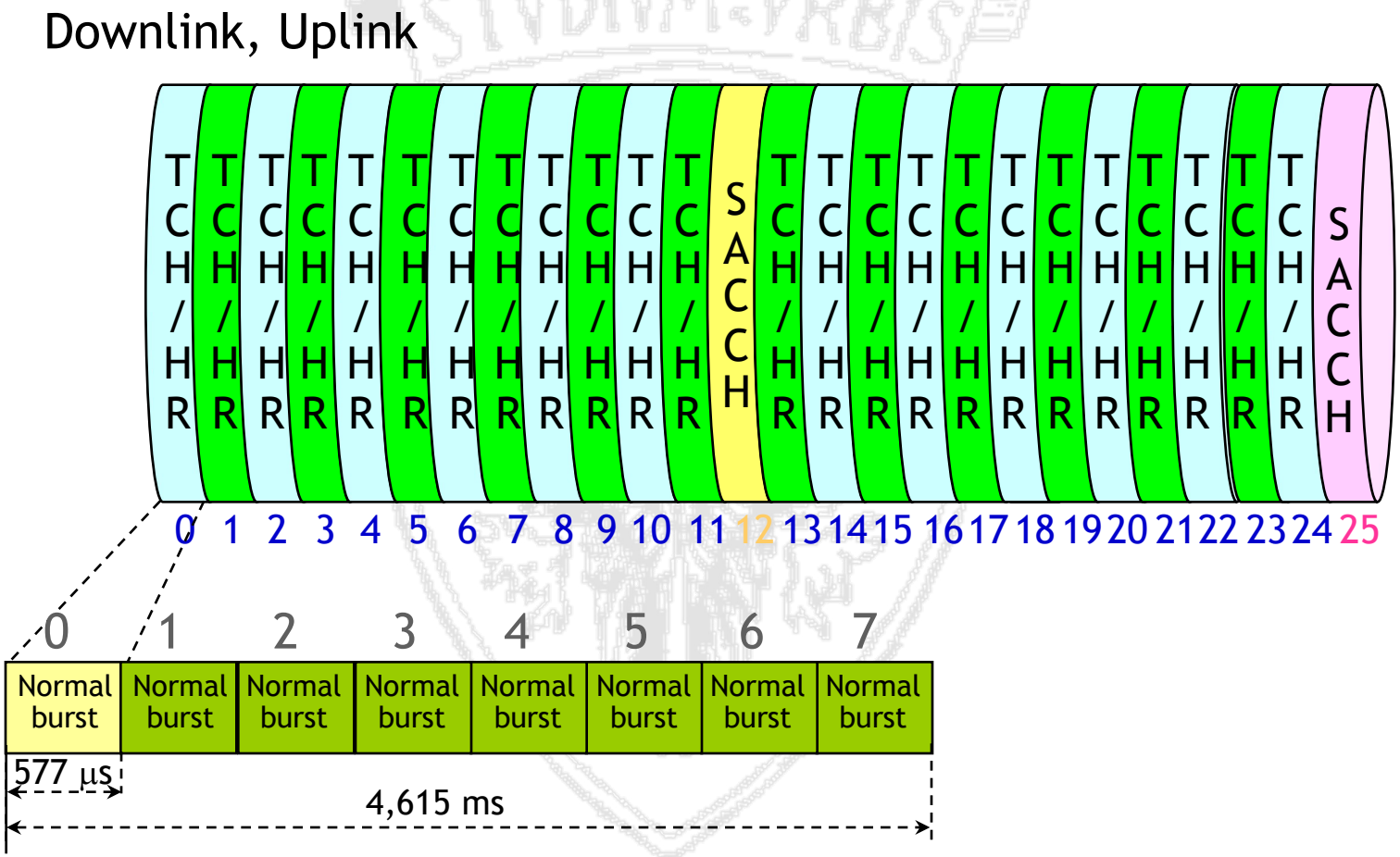
Multiframe TCH full duplex

- *A temporal diagram is the sequence of slots of the same traffic channel, i.e., of a slot of a frame*

Downlink, Uplink

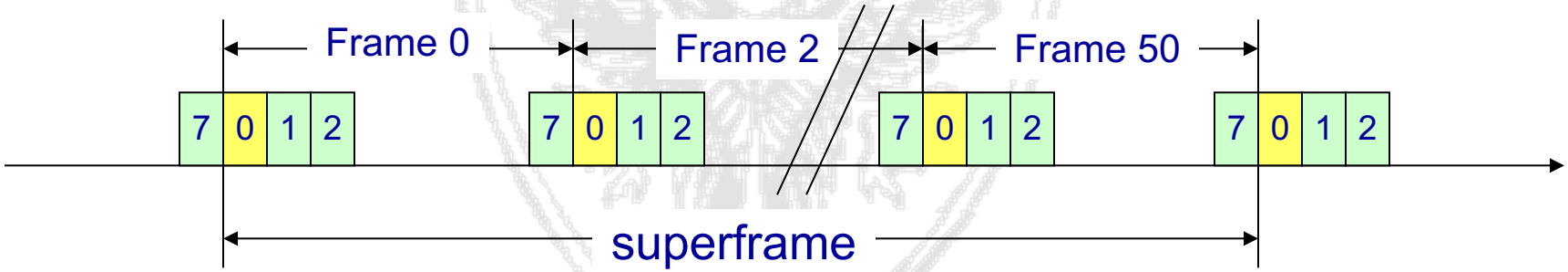


Multiframe TCH half rate encoding



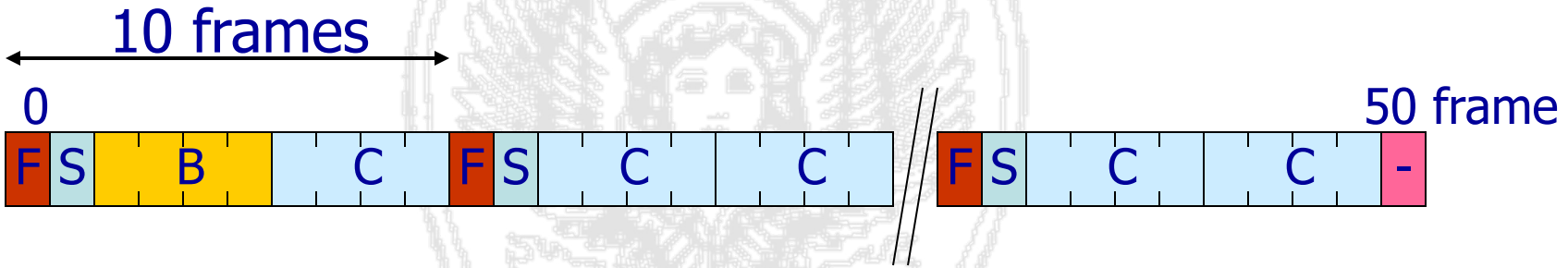
Common signaling channels

- A given slot (slot 0) over a given carrier (C0 or main carrier) among those associated to the cell is used to obtain one or multiple channels that use a multiframe containing 51 frames (235.38 ms).
- In downlink, the main carrier is always transmitted at a power higher than the other carriers, which allows a MS to synchronize with the main carrier and to receive the information it needs for tuning to the BS.

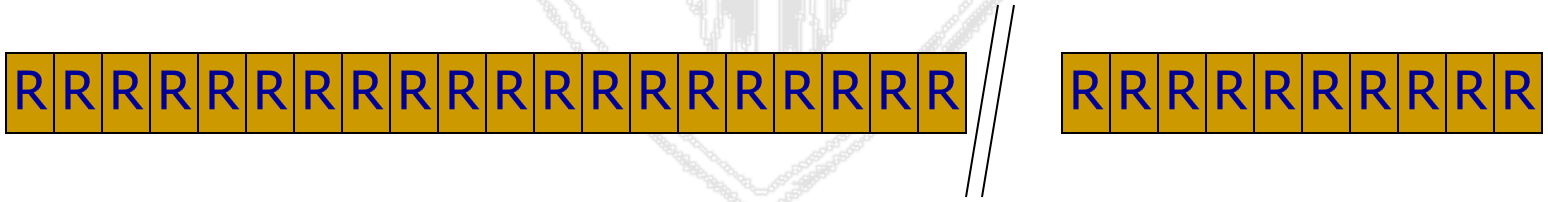


Common signalling channels

- Downlink channels:
  - Frequency Channel (FCH)
  - Synchronization Channel (SCH)
  - Broadcast Control Channel (BCCH)
  - Common Control Channel (PCH, AGCH in downlink)

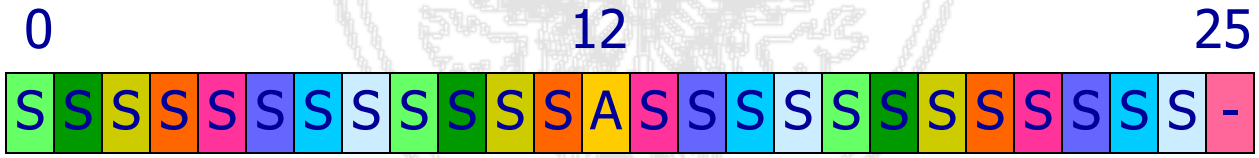


- Uplink: Random Access Channel (RACH)



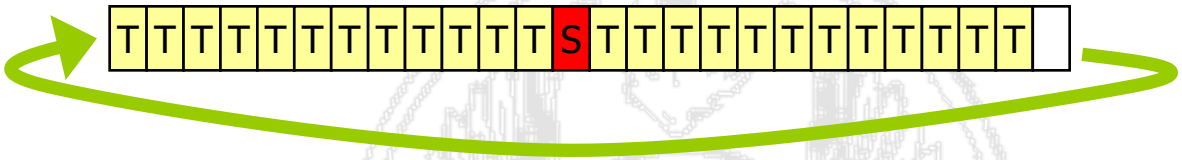
SDCCH channel

- Another slot is used to obtain 8 Stand-Alone Dedicated Control Channel (SDCCH) (S)
- Used for setup and other messages (SMS)
- The 8 channels are obtained by using 3 slots each within the super-frame of 26 slots



Why 26 and 51?

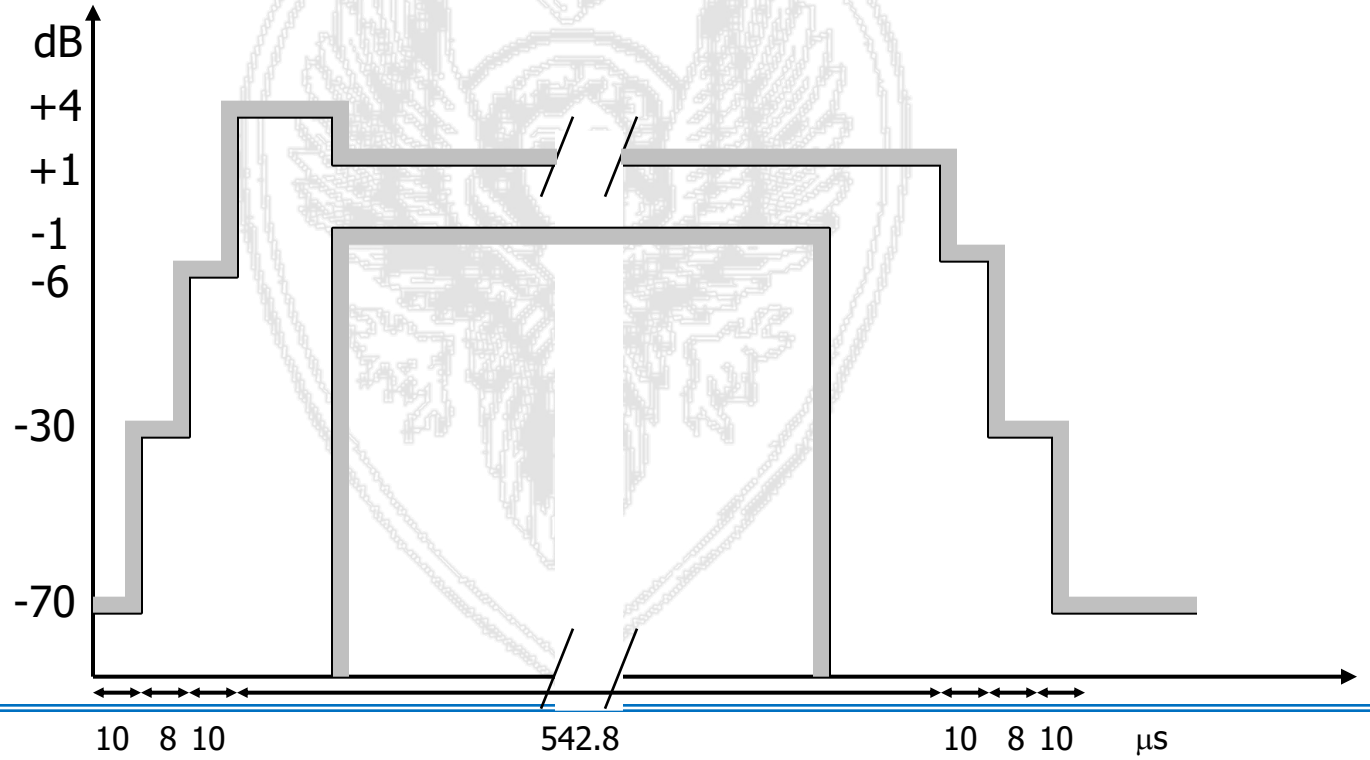
Last frame (idle) in TCH multiframe (Frame #25) used as “search frame”!



- An active call transmits/receive in 25 frames, except the last one.
- in this last frame, it can monitor the BCCH of this (and neighbor) cell
- this particular numbering allows to scan all BCCH slots during a superframe

Physical blocks (Bursts)

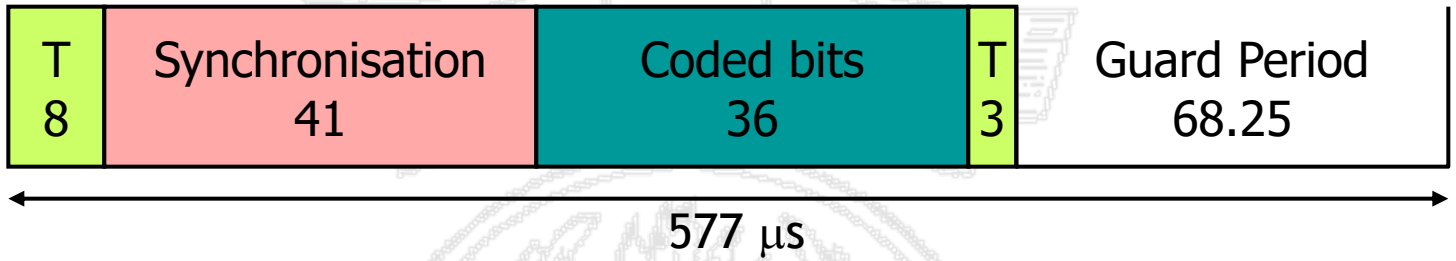
- The physical block is the information transmitted during a slot
- Due to TDMA, each block is an autonomous transmission entity, which should be transmitted at the appropriate power level to avoid interference with adjacent slots



Bursts Classification

- Normal Burst
  - Used for user transmissions (speech or data) over traffic channels
- Access Burst
  - Used to transmit information over the Random Access CHannel - RACH
  - First-time access
- Longer guard period (68,25 bit durations) to avoid overlapping of the the transmission from different mobiles; remember that mobile users do not know the timing advance at the first access (or after handover). The guard period is computed assuming a maximum cell size of 35Km.

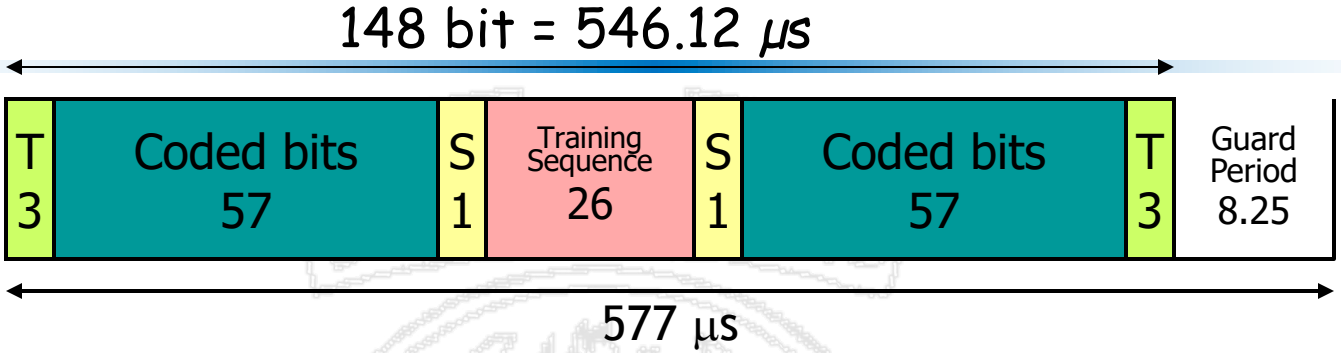
Access Burst



- Used by the MS on the random access channel at the first access
- Asynchronous access, no timing advance check
- It contains 156.25 bits
  - 8 tailing bits
  - 41 synchronisation sequence
  - 36 coded bits
  - 3 tailing bits
  - 68.25 bits guard period

To estimate timing advance

Normal Burst

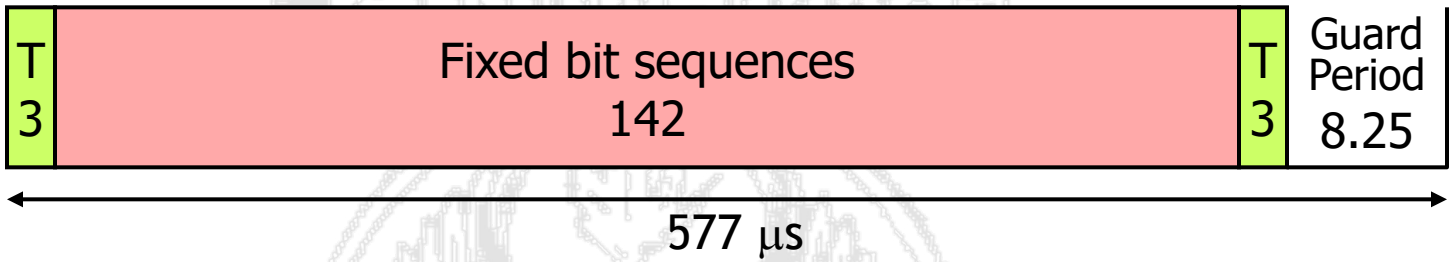


- T-bits: tail bits always set to 0
- S-bits: (stealing bits) indicate whether the burst contains user data or signaling information (SACCH or FACCH channels, only one of the two blocks may contain signaling information in case of FACCH)
- Coded Data: user bits (speech, data, etc.), 114 bit with channel coding, corresponding to 13 kbit/s for speech and to 9.6 kbit/s or lower for data (due to the channel coding using more bits)
- Training Sequence: control bits used for the equalization and tuning of the transmitters
- GP: guard period

Bursts Types

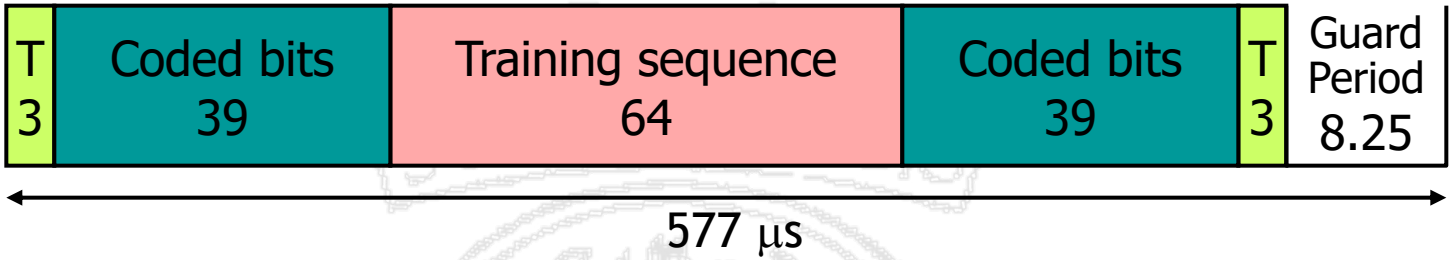
- Frequency Correction Burst
  - Used over the Frequency Correction Channel - FCCH
  - 142 bits set to “0”
  - Correct the frequency of the MS’s local oscillator, effectively locking it to that of the BTS
- Synchronisation Burst
  - Used to transmit information about synchronization for slots and frames
- Dummy Burst
  - It contains no information, only padding bits
  - Used when there is no information to be carried on the unused timeslots of the BCCH Carrier (downlink only)

Frequency Correction Burst



- 148 + 8.25 bits
  - 2 x 3 tail control bits
  - 142 fixed bit sequences
    - ✓ All bits set to 0
    - ✓ a pure sine wave is transmitted, which is the frequency with which the MS has to tune with
  - 8,25 bits guard period

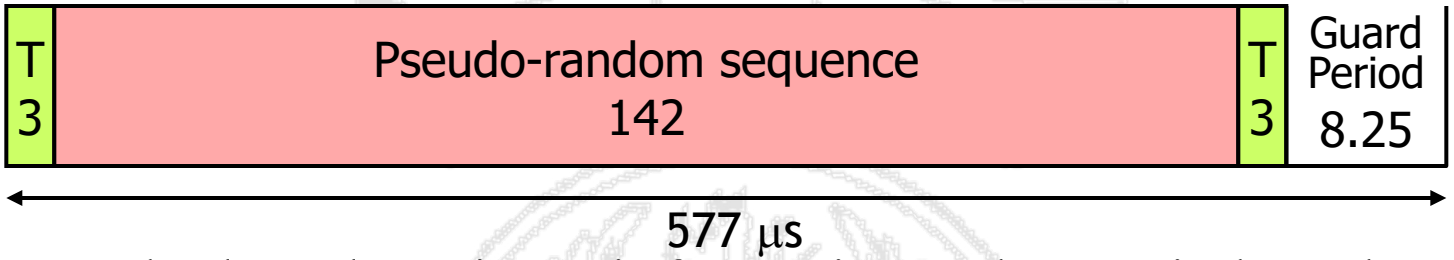
Synchronisation Burst



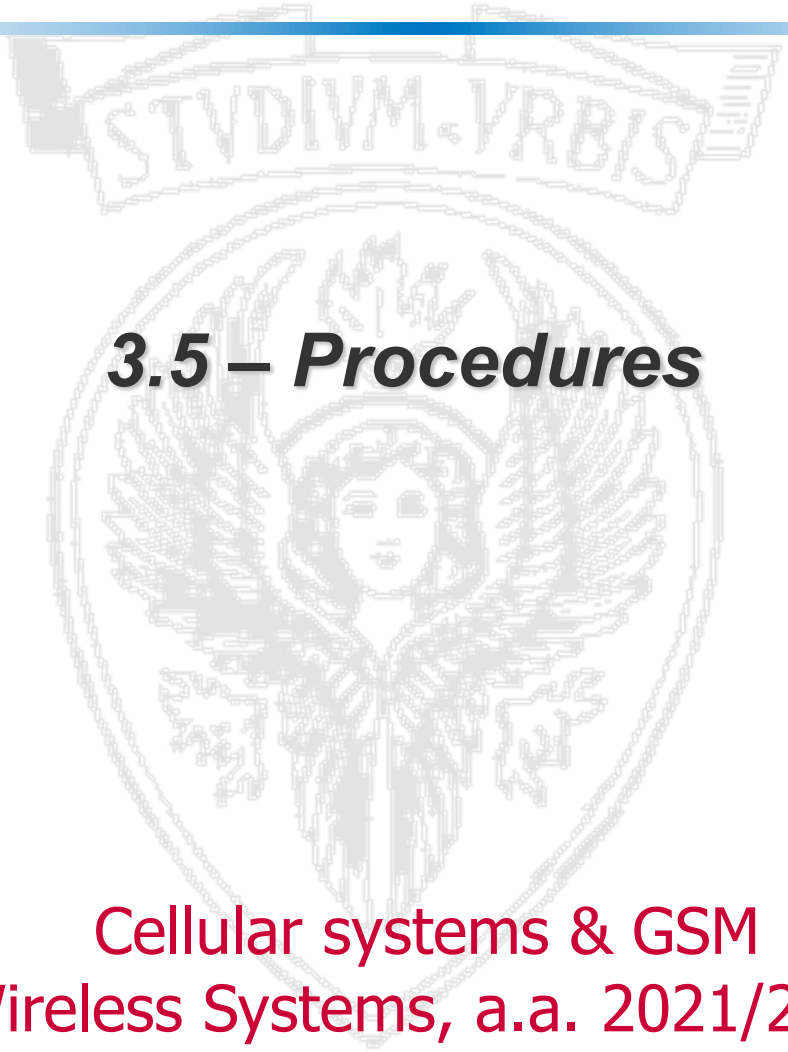
- 148 + 8.25 bits
  - 2 x 3 tail control bits
  - 2 x 39 coded bits
    - ✓25 bit information
    - ✓78 bit with coding
    - ✓Split into two pieces of 39 bit
  - 64 bit di training sequence
  - 8.25 bit guard period

Critical information, must be protected and correctly decoded

Dummy Burst



- Used when there is no information to be carried on the unused timeslots of the BCCH Carrier (downlink only).
- Measurements on signal strength must be carried out independently of whether there are data to transmit.
- Contains 148 + 8.25 bits
  - 2 x 3 tail control bits
  - 142 pseudo-random sequence
  - 8.25 bits guard period



3.5 – Procedures

Cellular systems & GSM
Wireless Systems, a.a. 2021/2022

Procedures

☑ O. Bertazioli, L. Favalli, *GSM-GPRS*, Hoepli Informatica 2002

Capitolo 11

GSM procedures

- Network Access
- Mobility
- Call Set Up
- Handover
- Paging

IMSI attach and Location Update

IMSI attach

- When a MS is switched ON:
  - **Cell selection**: the MS selects the BTS to which tune to
  - **Registration** (Location Update procedure): the MS notifies the MSC of its presence in the Location Area

Cell Selection

- The MS scans all RF carriers operating in the cell:
  - Scans c0 carrier over which the BCCH is transmitted
  - Such carriers are transmitted ad higher power than other carriers (dummy bursts are used when necessary), and frequency hopping is disabled
- The MS connects to the RF carrier from which the strongest signal is received
- Through the FCCH channel the MS synchronizes to the BTS carrier
- Through the SCH the MS synchronizes to the slot and frame and receives the BSIC – Base Station Identity Code
- The MS can now decode the BCCH, which includes
  - ✓LAC (Location Area Code)
  - ✓CGI (Cell Glocal Identity)
  - ✓MCC (Mobile Country Code)
  - ✓MNC (Mobile Network Code)

Registration

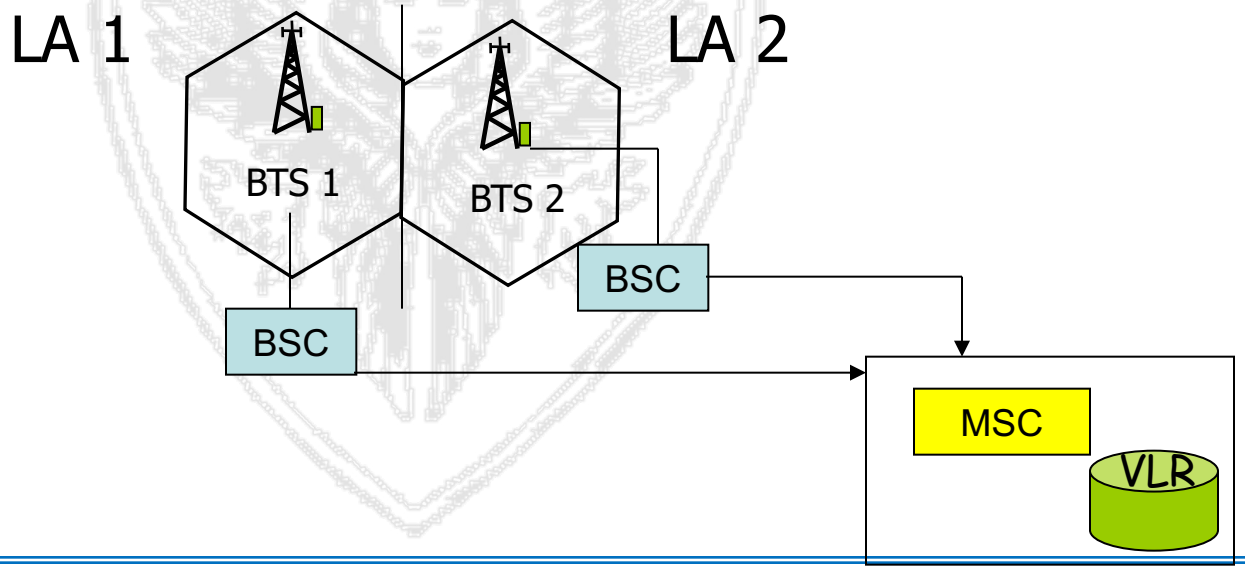
Two cases are possible, based on the **received LAI**:

1)<u>It is the same of that stored in the SIM</u> (which happens when the phone is turned off and on in the same LA). The ***IMSI attach*** procedure is invoked, with which the MS activates its IMSI stored in the current VLR (it means the MS was previously registered with the VLR, and that the detached flag was set when the MS was switched off – paging is not performed towards detached users)

1)<u>No LAI stored, o received LAI different from the stored one</u> (which happens when the phone is turned off and on in different LAs). The ***Location Update*** procedure is invoked.

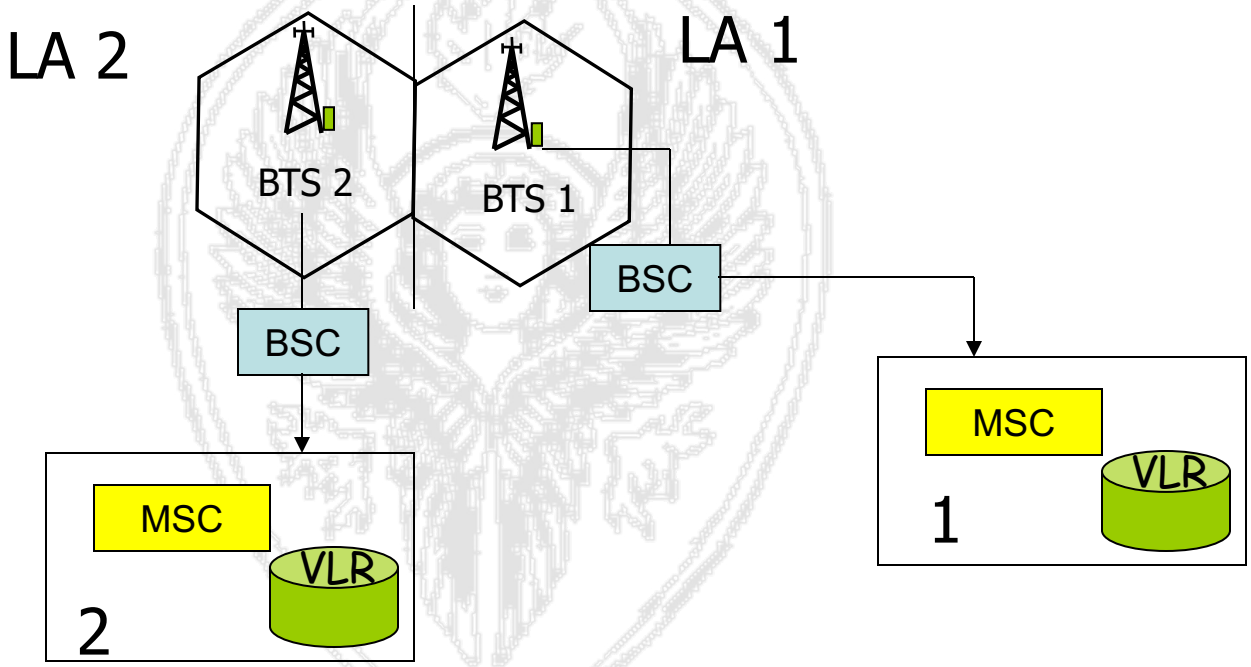
Location Update (1)

- When is it performed?
  - When a MS is switched on (if needed);
  - Periodically (e.g. every 30 min). If the periodic location update is not received, the VLR flags the user as detached -- *implicit detach*;
  - When the Location Area changes due to MS movements (roaming);
- Two types of Location Update:
  - Two LAs of the same MSC/VLR (the simplest case)



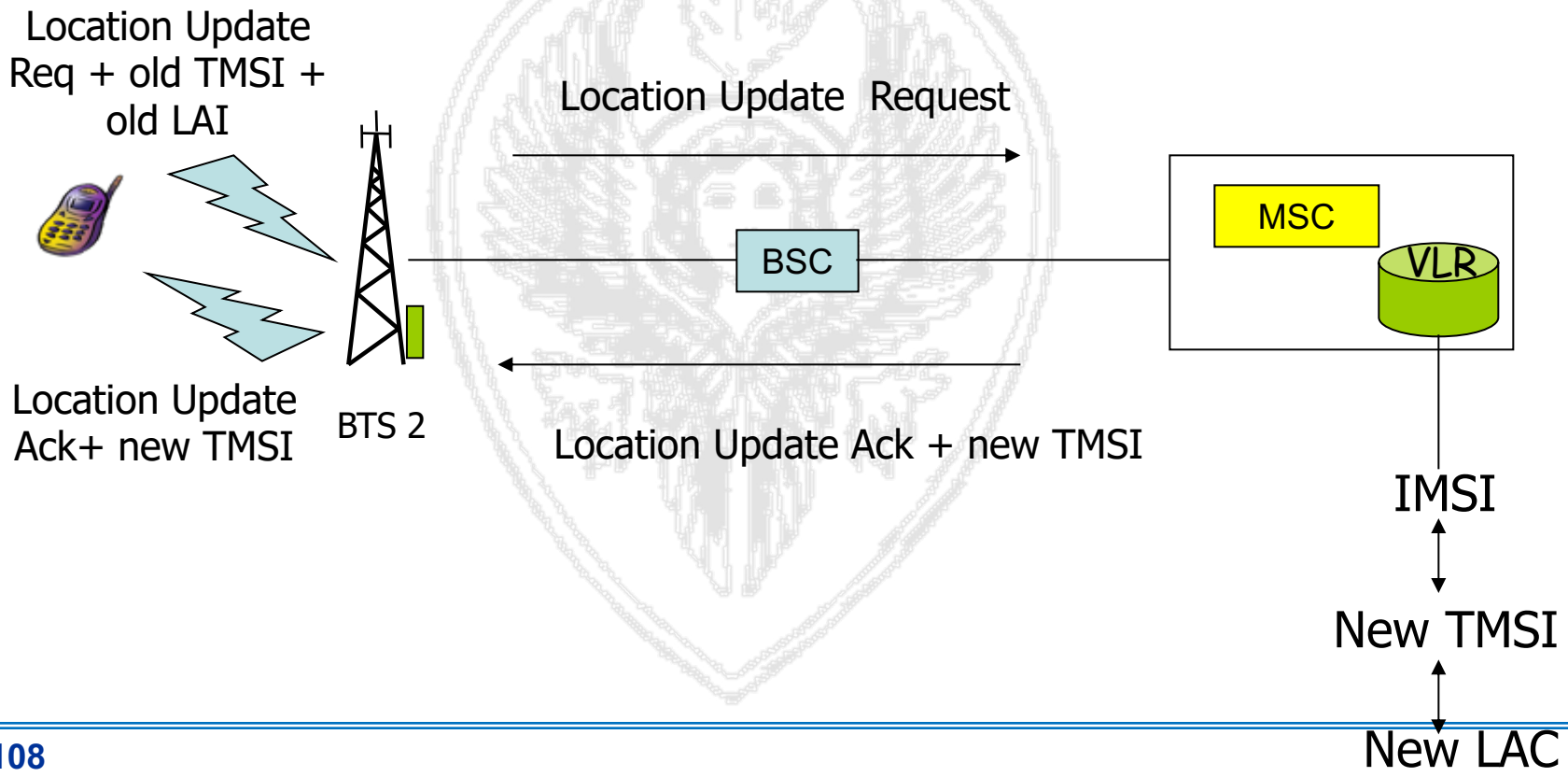
Location Update (2)

- Roaming between LAs of different MSC/VLRs

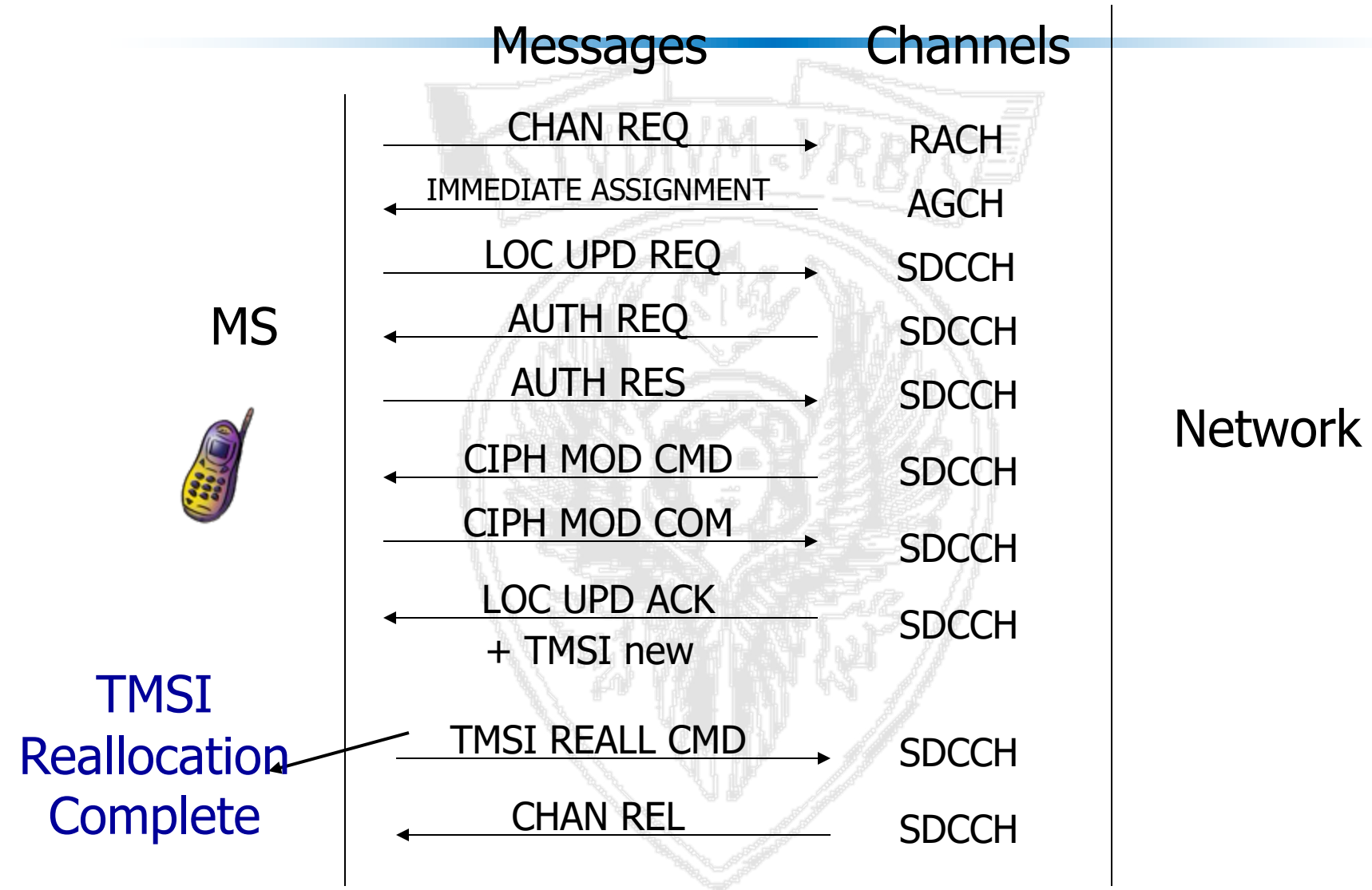


Location Update - Intra MSC

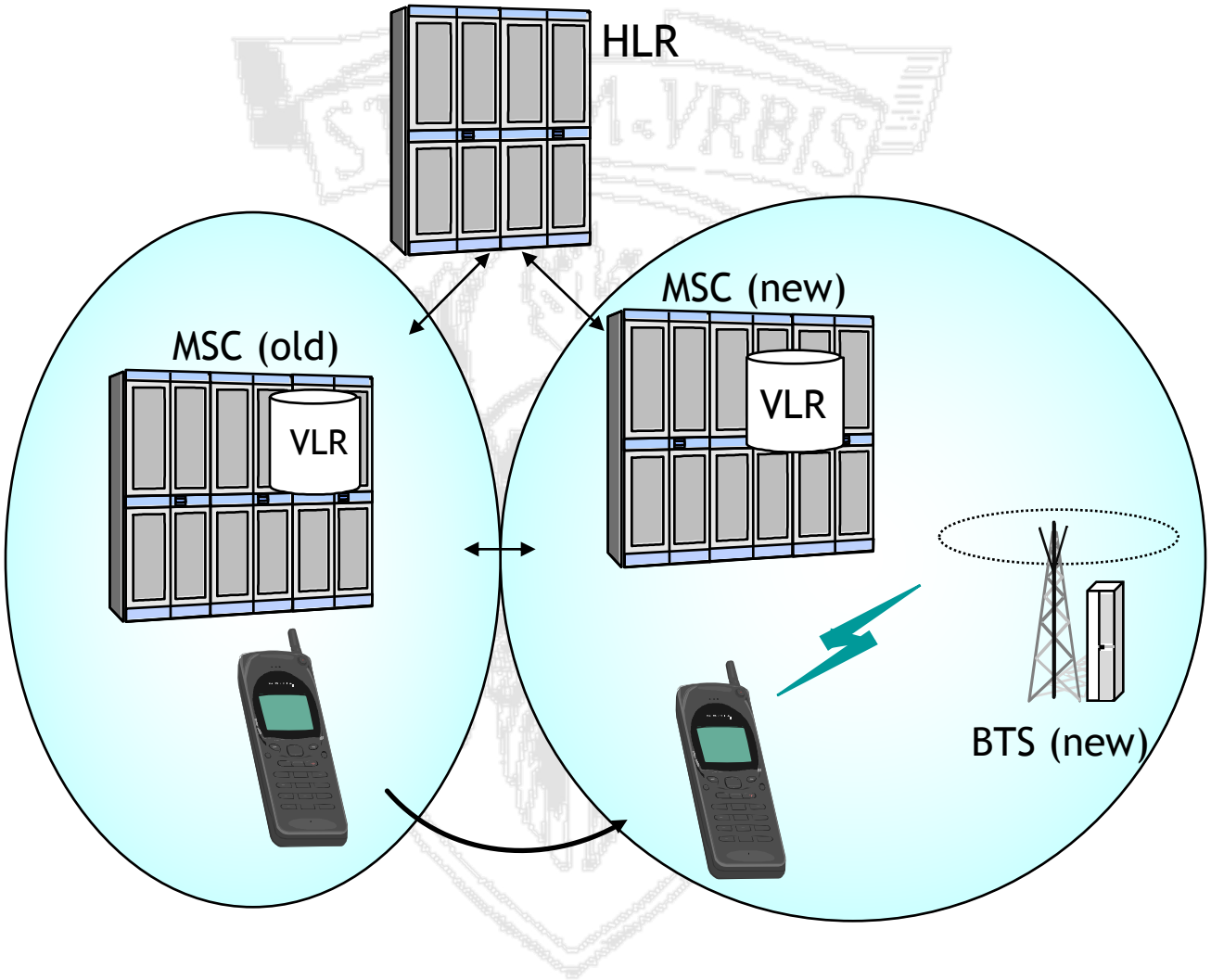
The System Information Message sent over the BCCH contains the location area identifier (LAI). Once tuned to a new BTS, the MS thus can determine if a location update is needed.



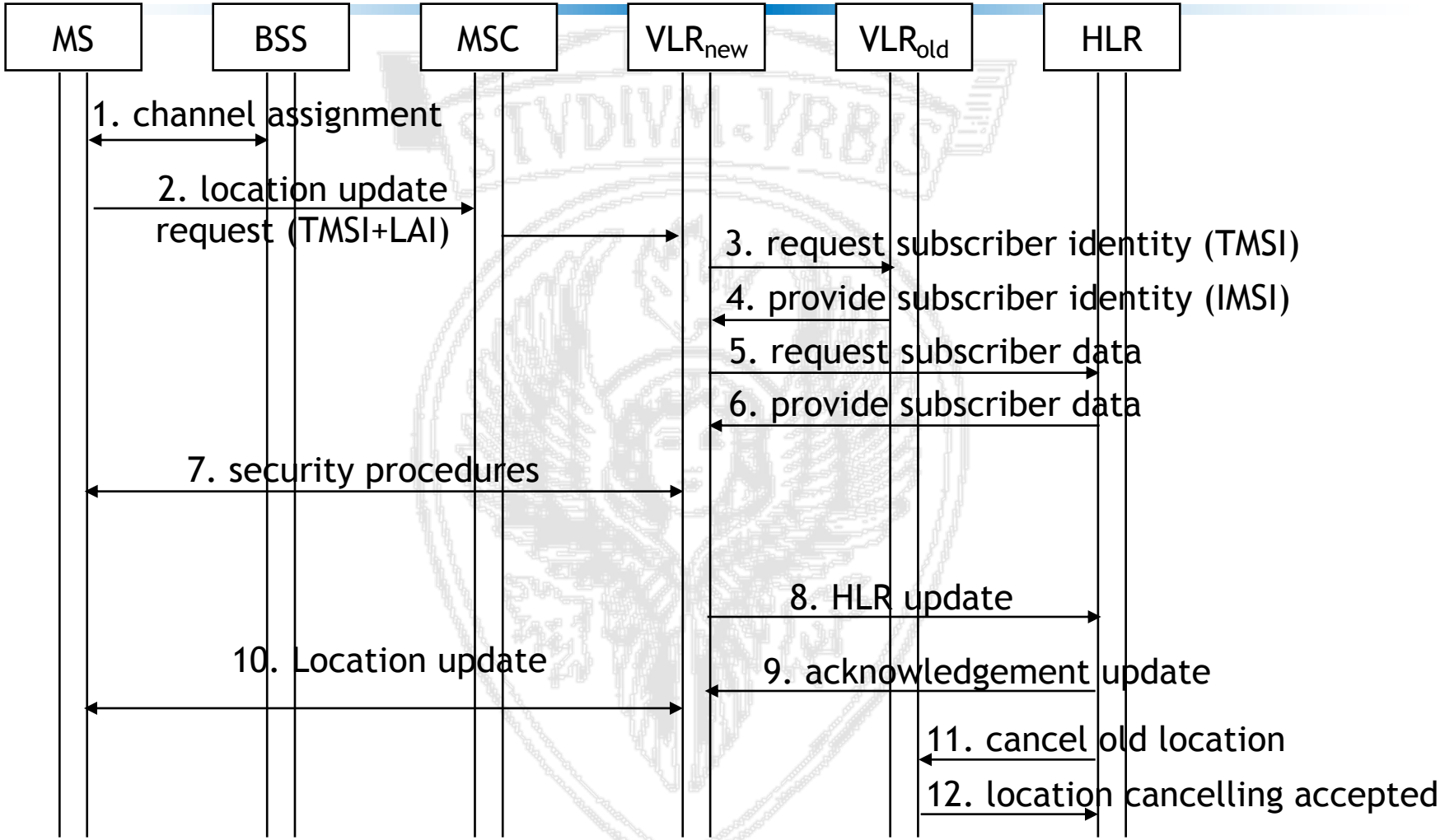
Location Update - Intra MSC



Location Update inter MSC

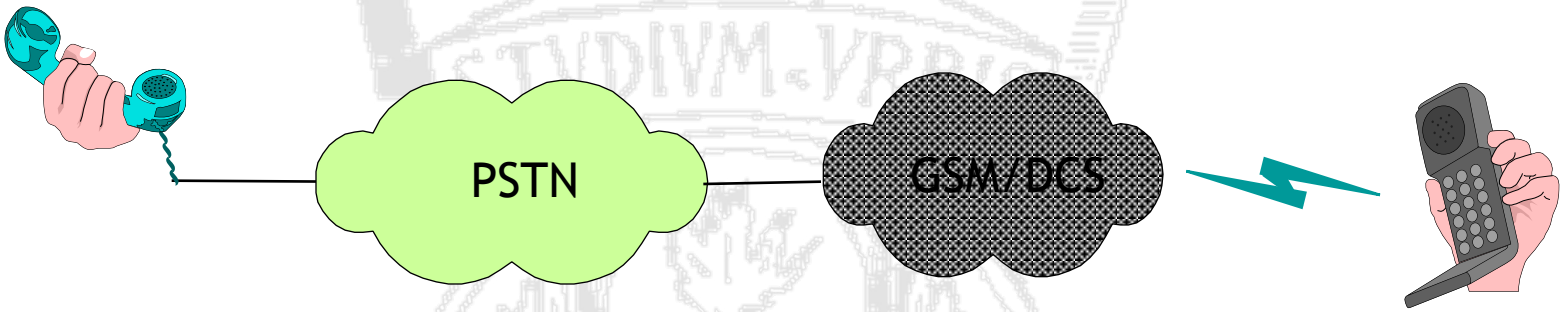


Location Update inter MSC



Call Set Up

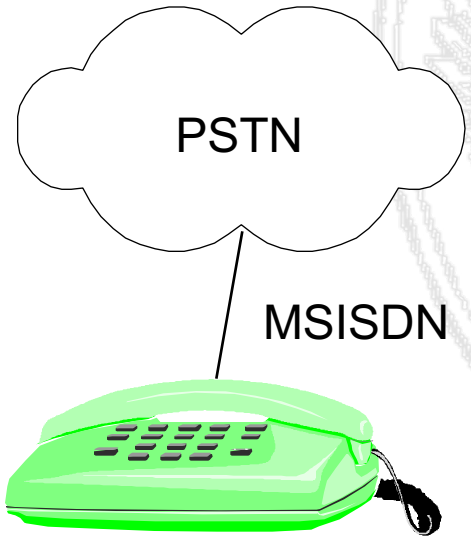
Call originated from PSTN



- Setting up a call terminated on a mobile user is more involved that setting up calls between PSTN users

Call Set-up Step by Step (1)

A The PSTN/ISDN user dials the Mobile Subscriber International ISDN Number (MSISDN) of the user she wants to call



MSISDN: +39 347 6527268

39 = Country Code (Italy)

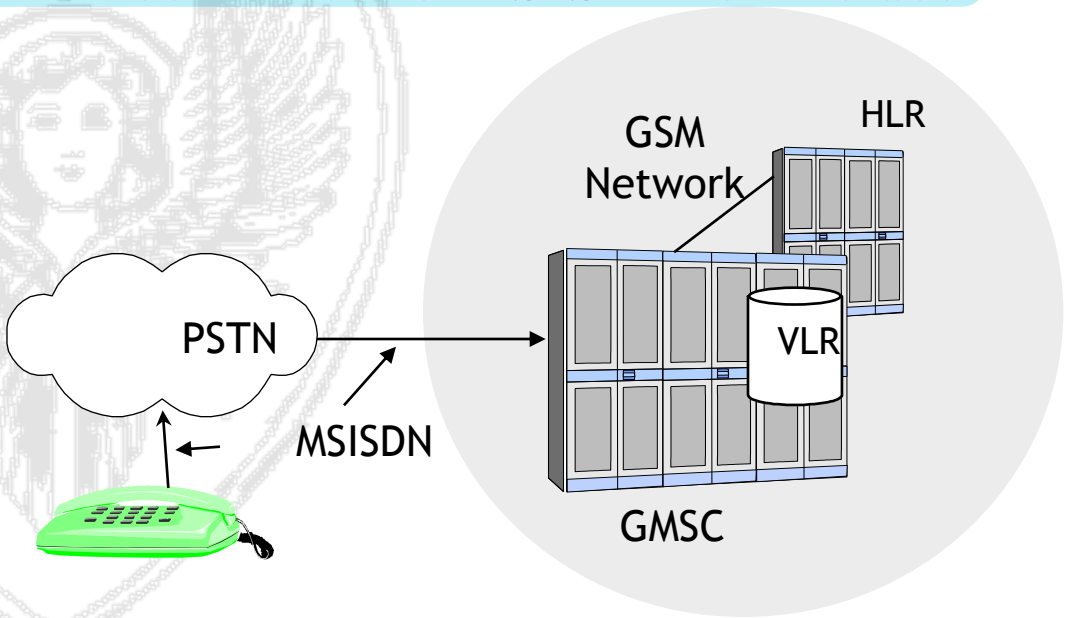
347 = National Destination code

6527268 = Subscriber Number

Call Set-up Step by Step (2)

B The dialled number is analysed by the PSTN/ISDN network, which routes the call to the GMSC of the PLMN of the called user by making use of the National Destination Code (NDC)

C The GMSC receives the message requesting to set-up a call through the SS7 network, which contains the MSISDN of the user called

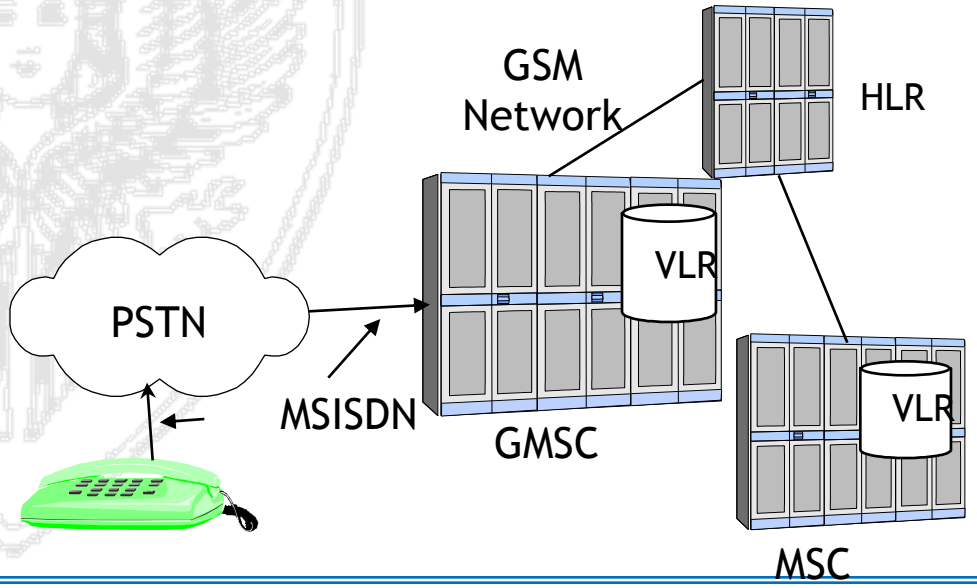


Call Set-up Step by Step (3)

D The GMSC identifies the HLR containing the data of the called user (it is not aware of the position of the MS!!)

E The GMSC sends a message requiring to "send routing information" to the HLR

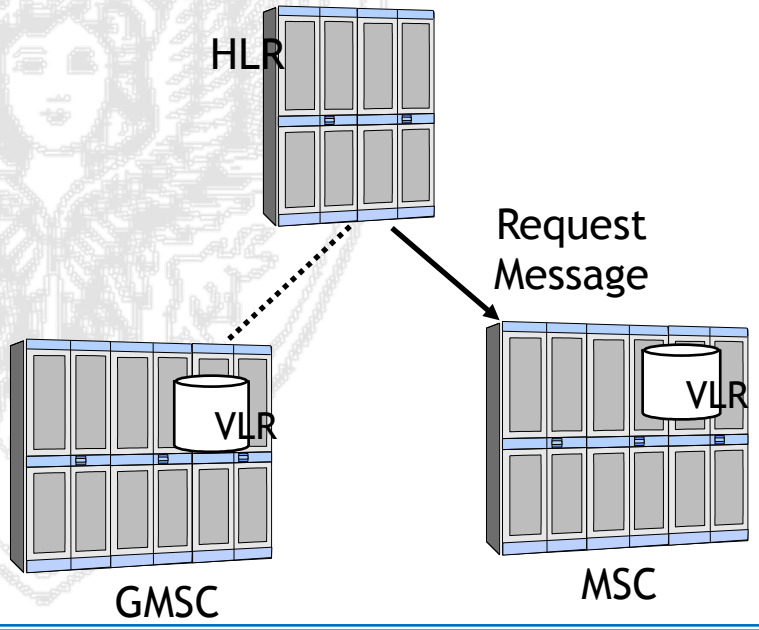
F The HLR identifies the address of the VLR in which the called MS is currently registered



Call Set-up Step by Step (4)

G The HLR sends a “provide roaming number” message to the MSC/VLR

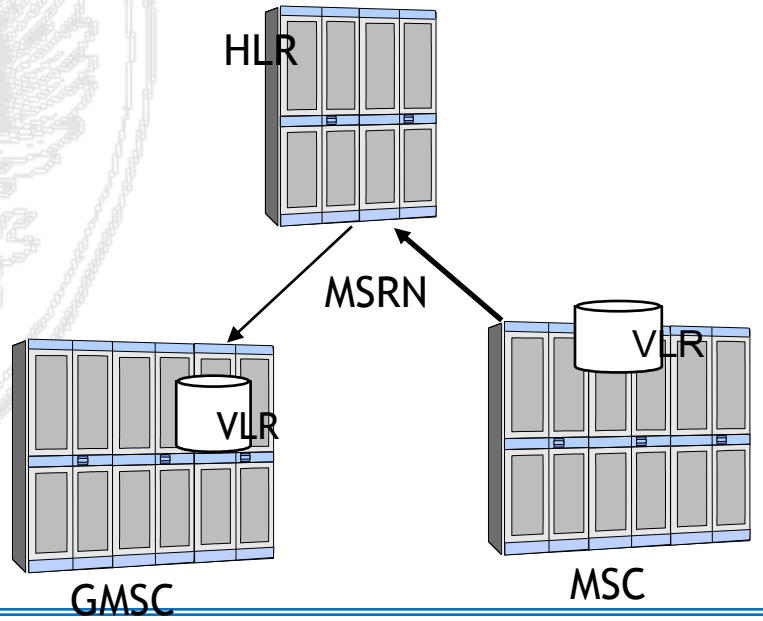
H The MSC/VLR temporarily allocates a Mobile Station Roaming Number (MSRN) to be used for the call



Call Set-up Step by Step (5)

I The MSRN is forwarded by the MSC to the HLR

J The GMSC routes the call towards the MSC/VLR of the LA in which the MS is currently located



Call Set-up Step by Step (6)

K The MSC/VLR activates the **paging** procedure:
- It identifies the currently-visited LA thanks to the IMSI
- It sends a paging command to all BSC of the location area

L BSC requires the BTSs to send the paging message destined to the MS over the paging channel (PCH) -- this message contains the TMSI assigned to the MS

M The MS replies to the paging message by requiring a Stand alone Dedicated Control CHannel (SDCCH) through the Random Access CHannel (RACH)

Call Set-up Step by Step (7)

N The MSC/VLR activates the authentication and the ciphering procedures

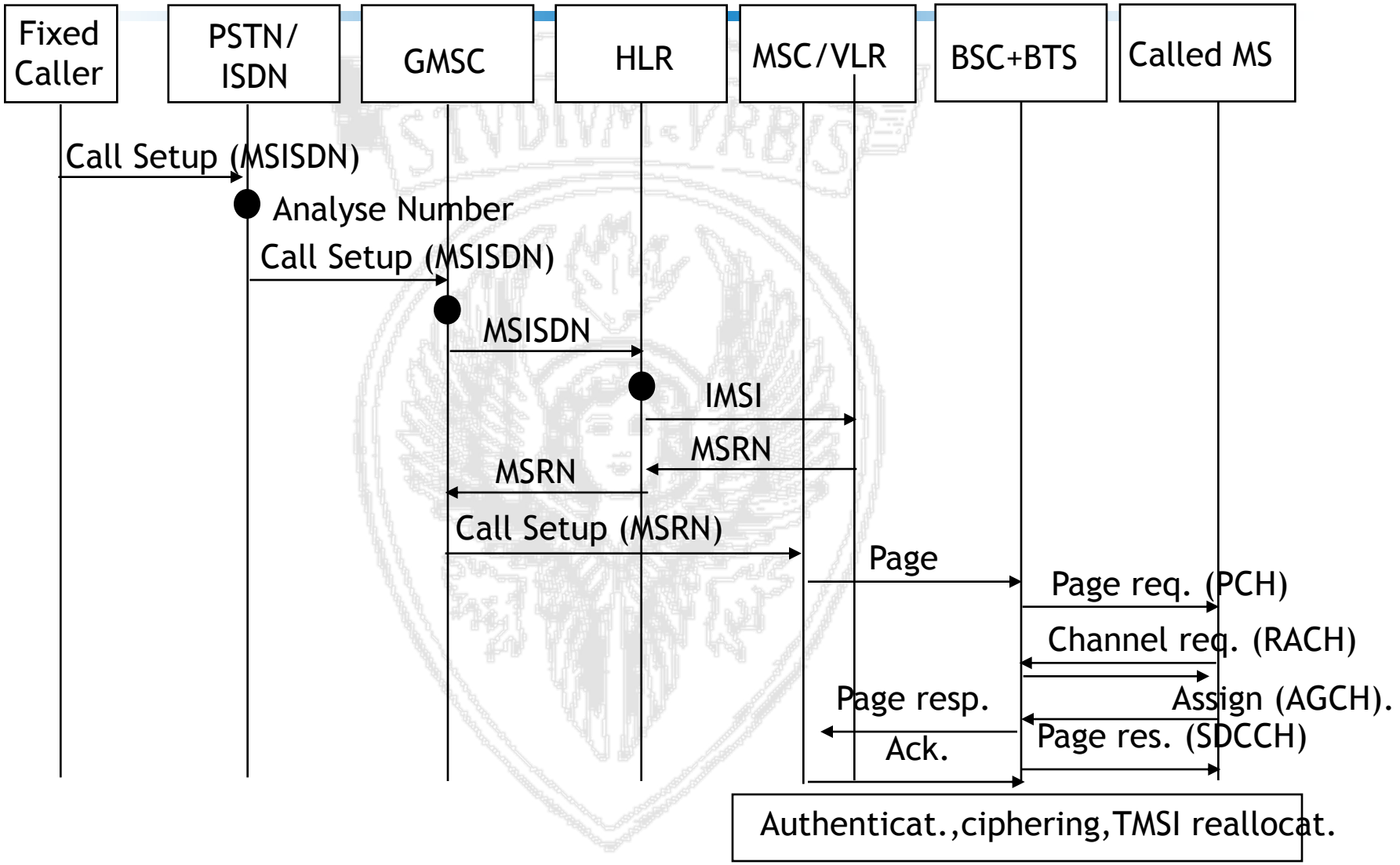
P A traffic channel (TCH) is allocated for the communication

Q The MSC/VLR notifies the caller that the called phone is ringing

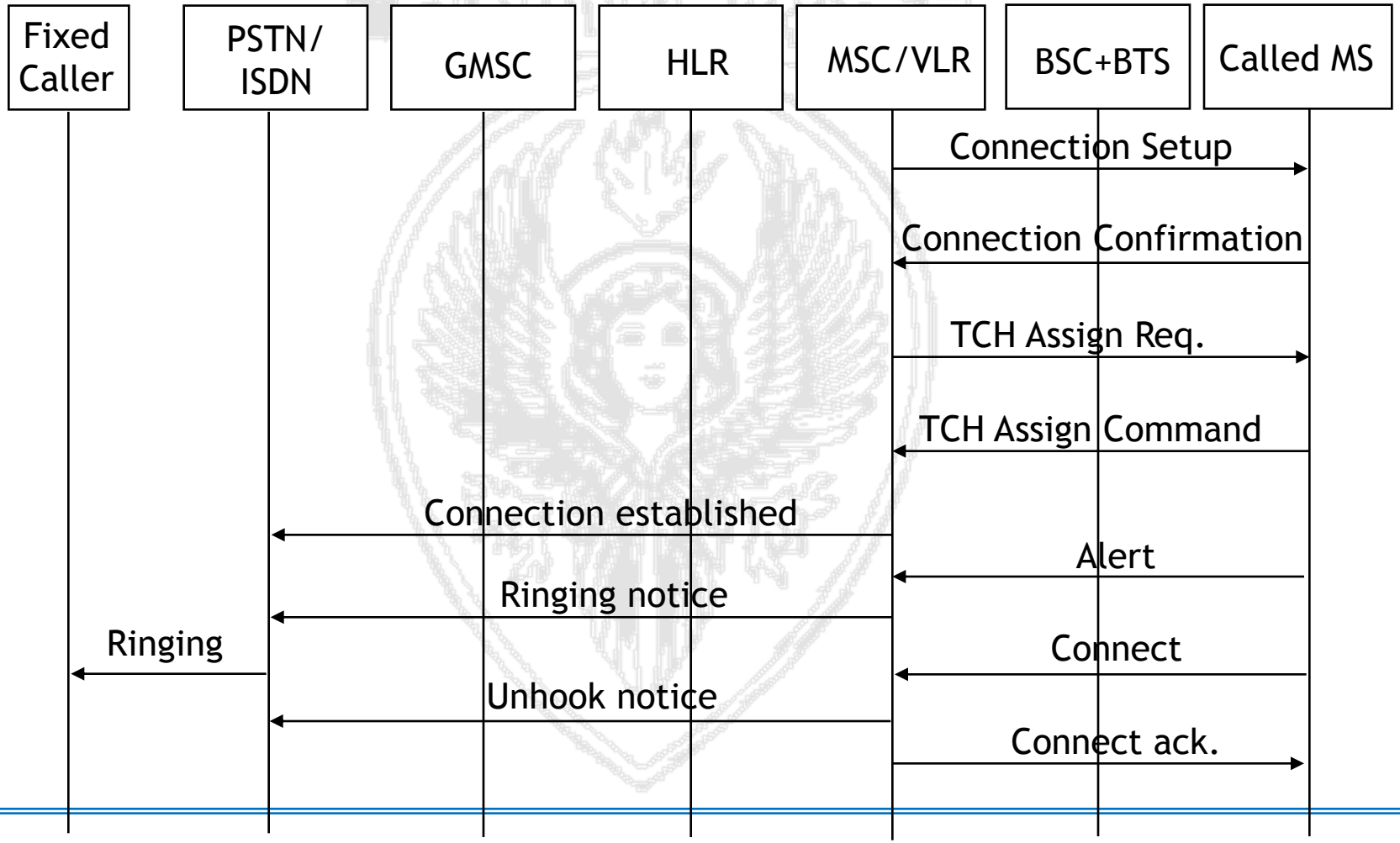
R The called user answers the call

S The connection between the two users is established

Summary of the Call Set-up Steps (1)



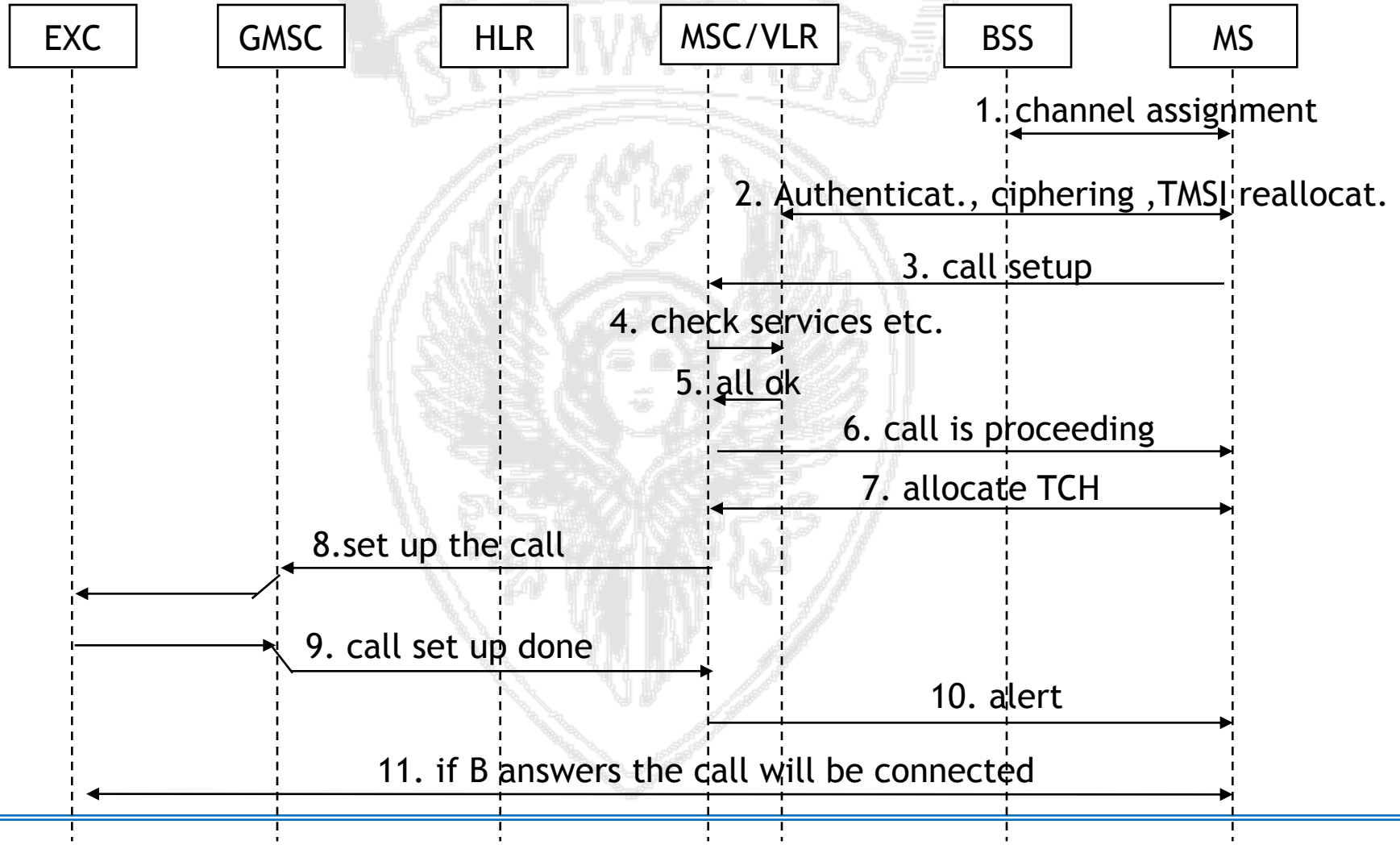
Summary of the Call Set-up Steps (2)



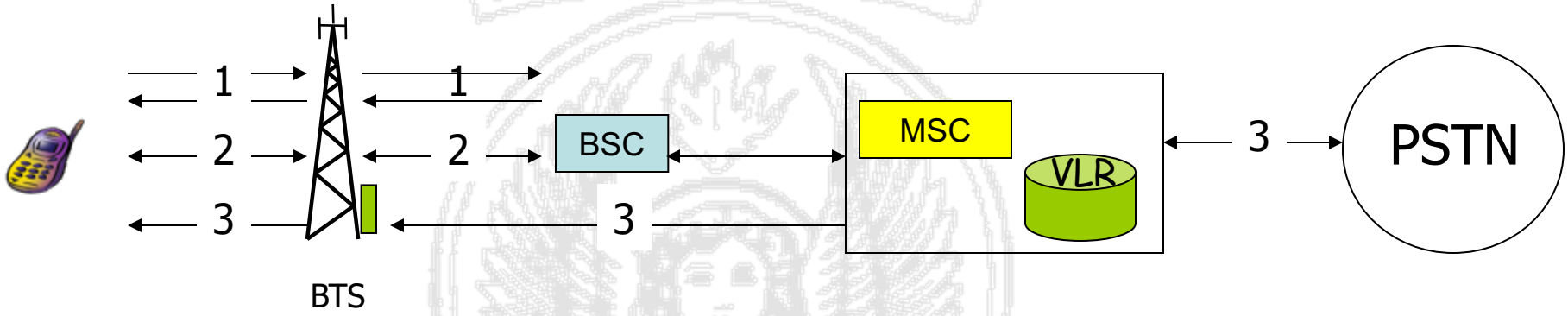
MS-originated call

- The called number is dialled by the MS
- The current MSC analyses the caller data and:
  - It either authorizes or deny the call
  - The call routing procedure is started
- If the called number is in the same GSM network, a “send routing info” procedure is started to obtain the MSRN
  - Same procedure as PSTN-originated calls
- If the called number is in another GSM network, the call is routed to the GMSC.

Summary of the Call Set-up Steps



Mobile-originated call (1)



1- Access request, resource allocation for signaling

2 – Authentication and ciphering, caller id is transmitted, traffic channel is allocated

3 –Call routing

Mobile-originated calls (2)