

# Introduction to cellular systems

IoT, a.a. 2018/2019

Un. of Rome "La Sapienza"

Chiara Petrioli<sup>†</sup>

<sup>†</sup> *Department of Computer Science – University of Rome "Sapienza" – Italy*



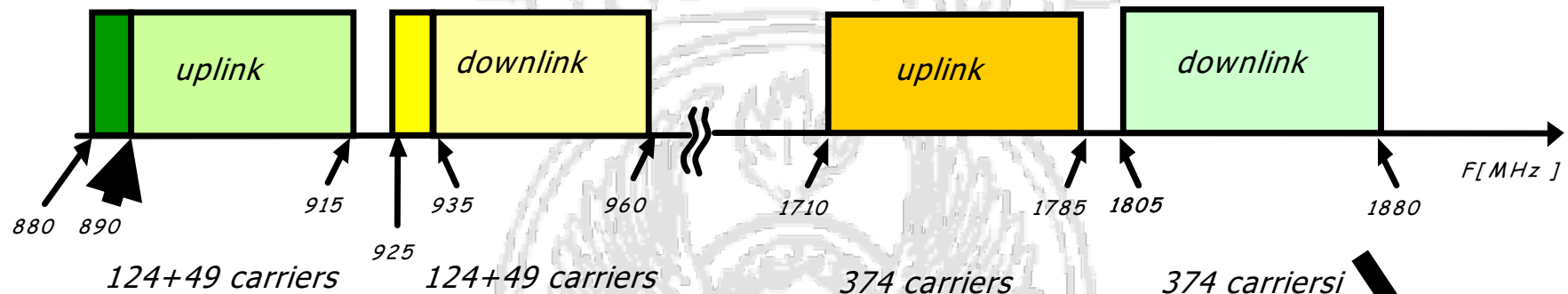
- 2<sup>nd</sup> Generation (2G) cellular system
- Carrier bandwidth=200KHz
- Multicarrier TDMA multiple access (8 slots per carrier, thus 8 channels per carrier)→ TDMA/FDMA
- Full Duplex: Frequency Division Duplex (FDD)
- Modulation: GMSK; Spectrum efficiency: 1,35bps/Hz; Gross bit rate per carrier: 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, discontinuous transmission
- Adaptive equalization
- Services
  - telephony with many additional services
  - circuit switching data network (single-channel or multi-channel)
  - packet switching data network (GPRS - General Packet Radio Service)



# Allocated frequencies

GSM /900

DCS/1800



esteso uplink  
esteso downlink

distance between the frequencies used

for tx and rx set to 45 Mhz

distance between the frequencies used

for tx and rx set to 95 Mhz

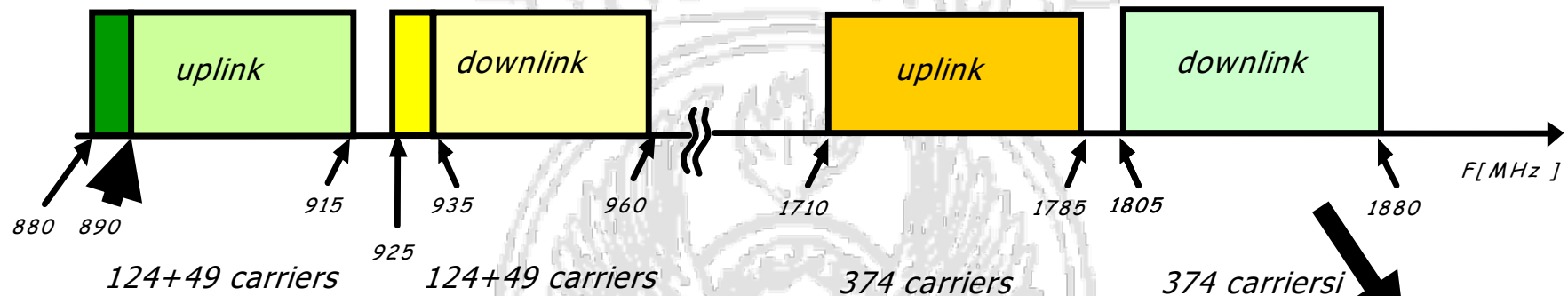
- In UK and USA it uses bands around 1900 MHz instead of around 1800 MHz (1850÷1910 uplink, 1930÷1990 downlink).



# Allocated frequencies

GSM /900

DCS/1800



esteso uplink  
esteso downlink

distance between the

for tx and rx s

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

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

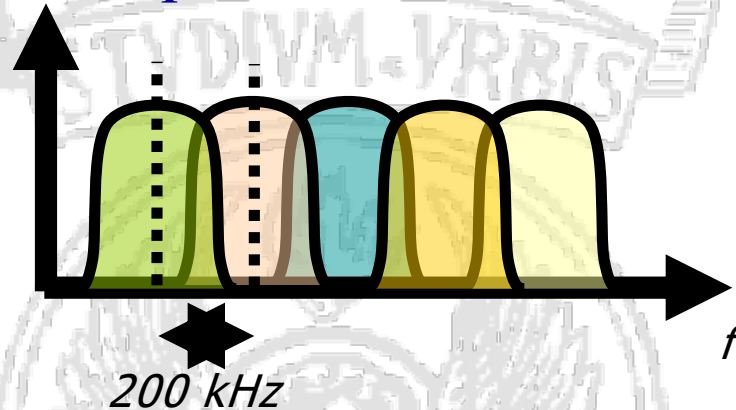
*The lower portion of the spectrum is allocated to uplink channels, saving MS consumed power*

frequencies used

95 Mhz

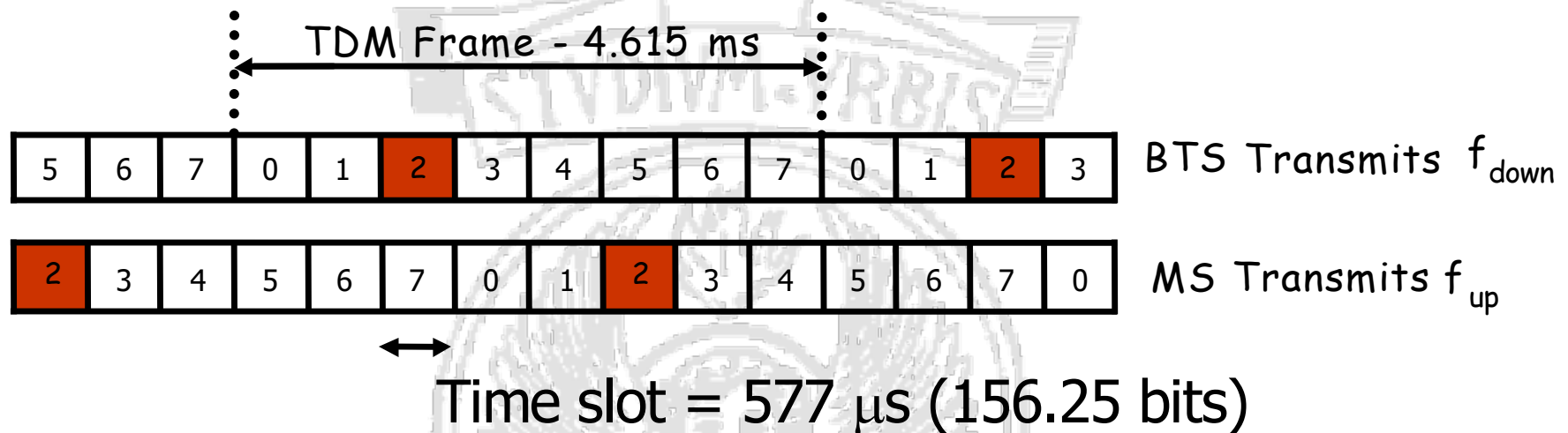
of

- 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

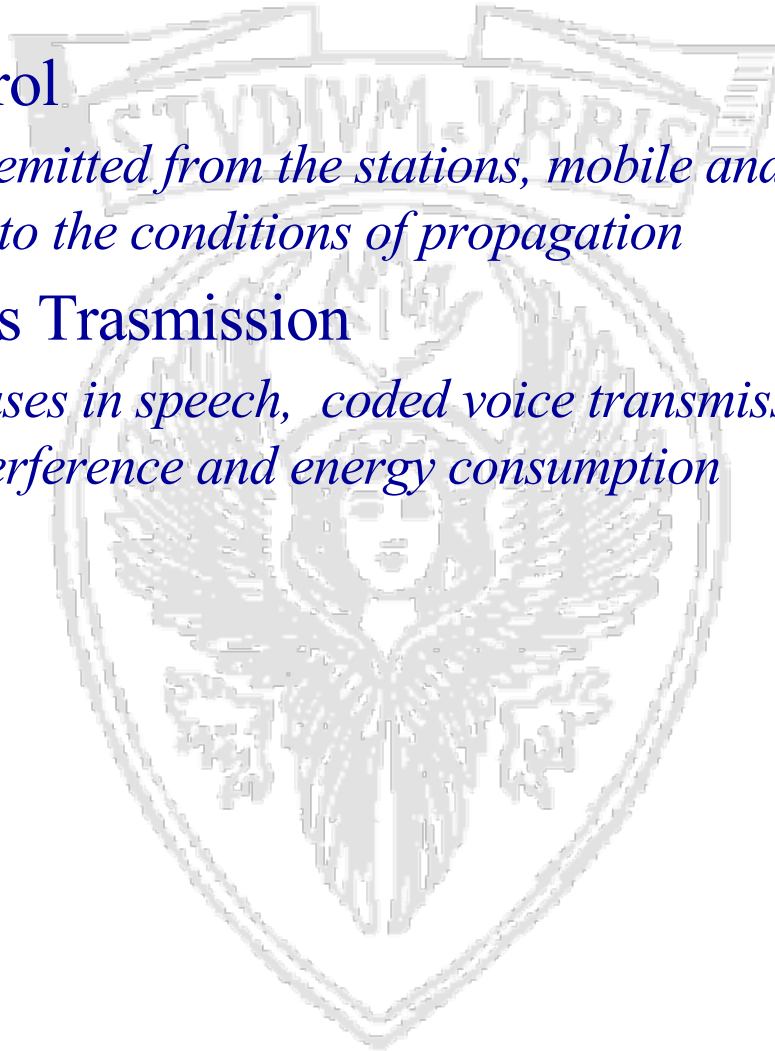




- On each radio carrier the TDMA structure allows us to create up to 8 channels for the transmission of voice encoded at 13 Kb / s



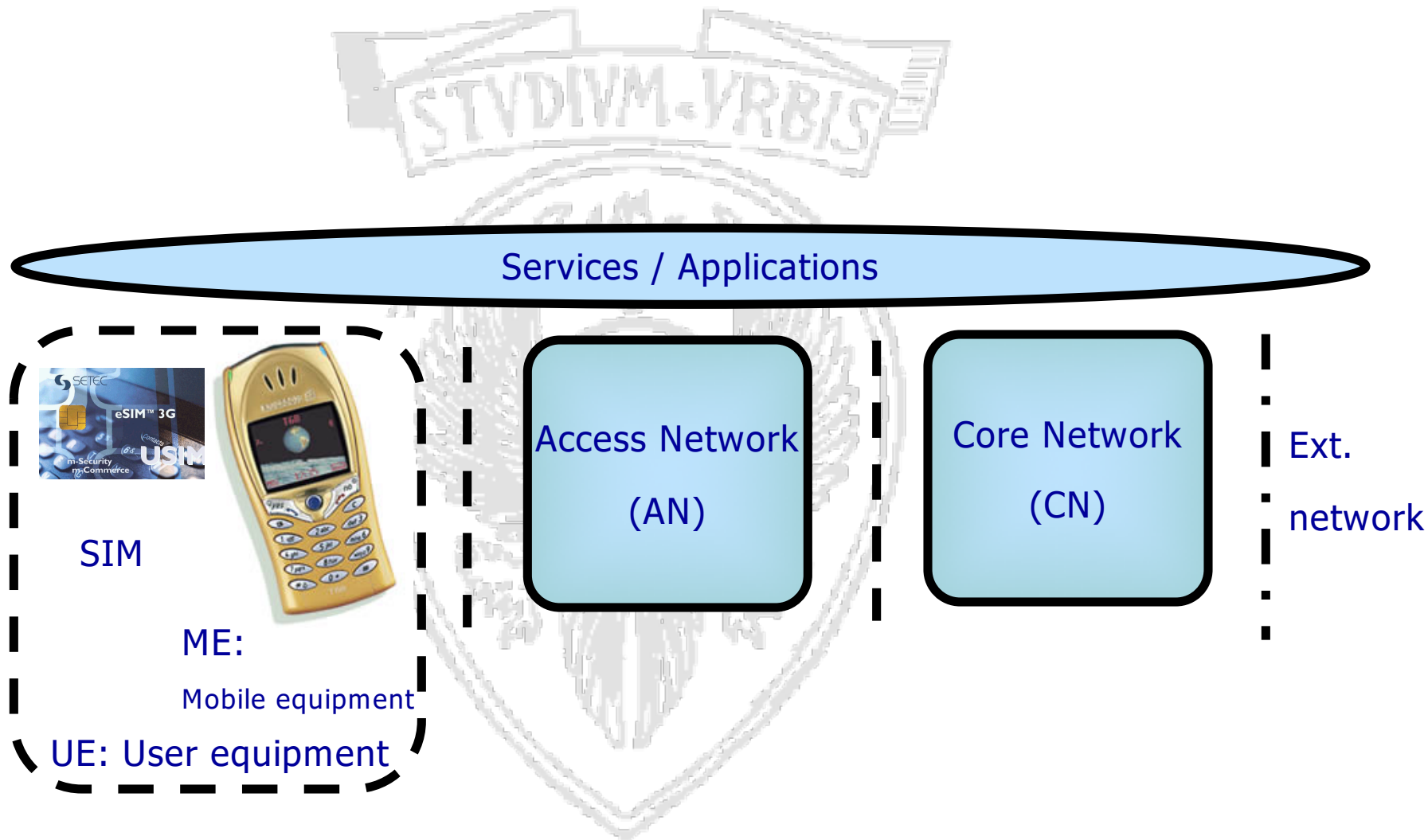
- Power Control
  - *the power emitted from the stations, mobile and base, is adjusted according to the conditions of propagation*
- Discontinuous Transmission
  - *during pauses in speech, coded voice transmission is interrupted to reduce interference and energy consumption*



A large, faint, light-gray watermark of the University of Rome seal is centered in the background. It features a shield with an eagle and a banner above it that reads "STVDIVM-VRBIS".

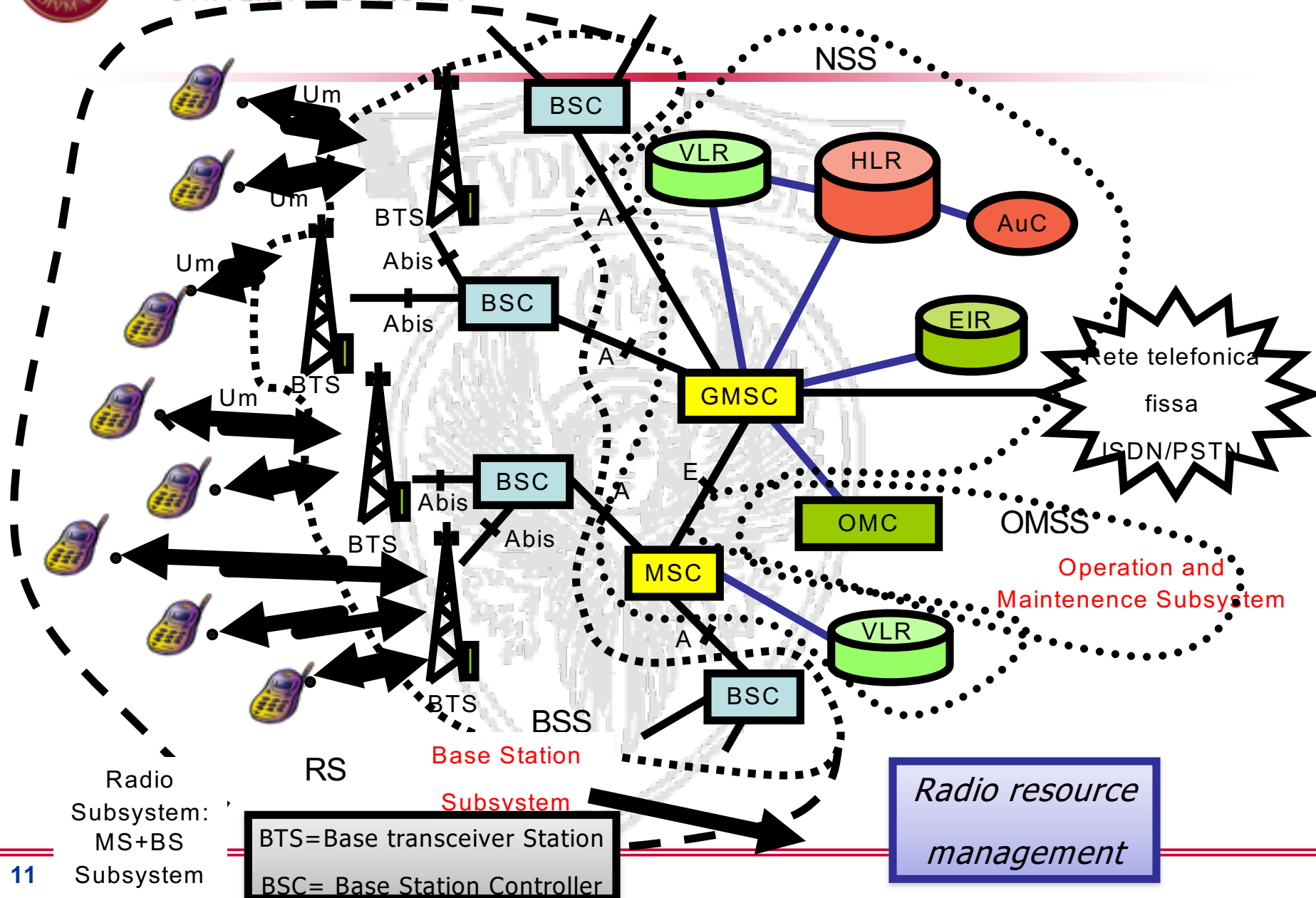
## ***3.2 – GSM Architecture***

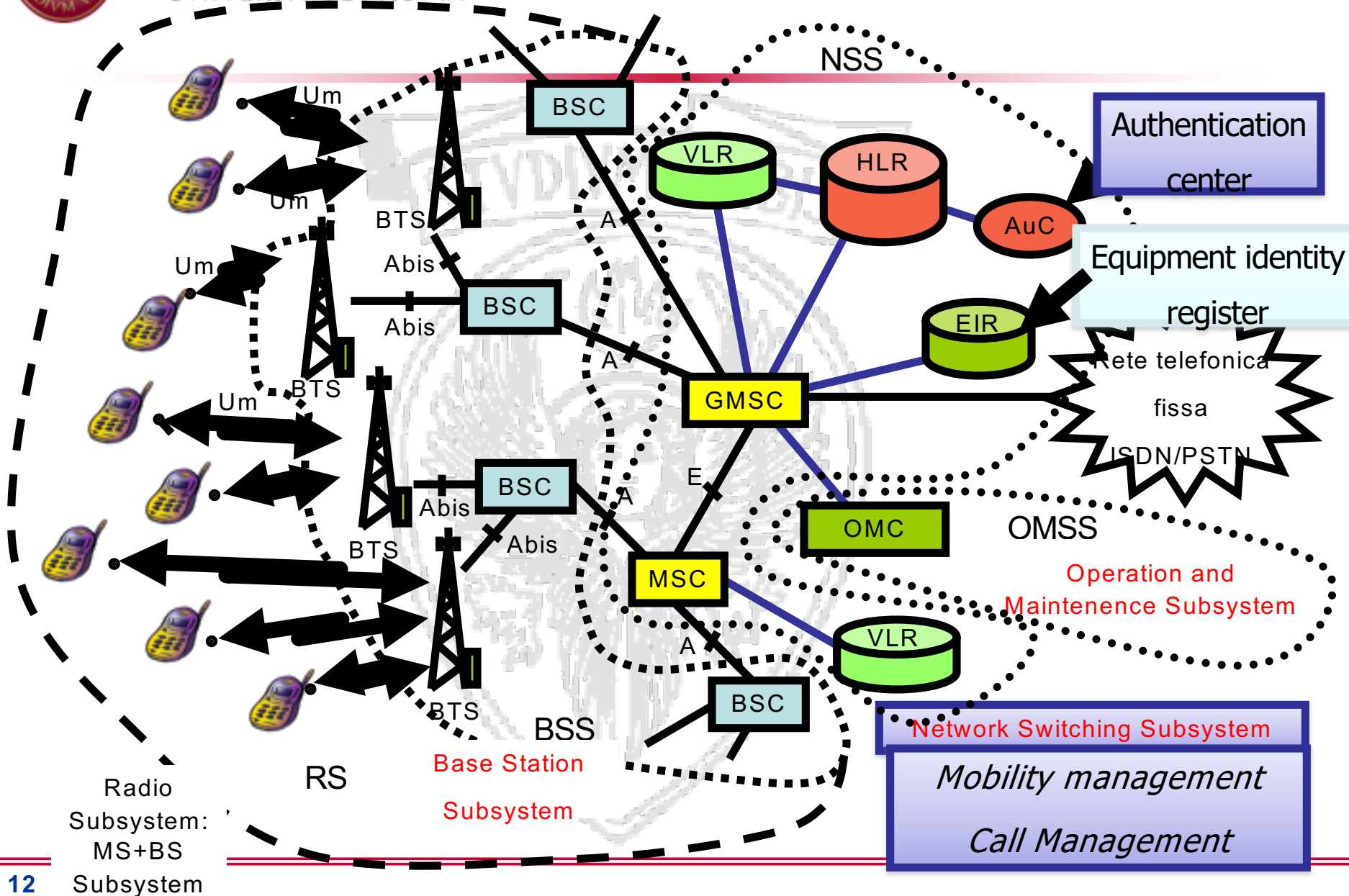






- The network contains functionally of: User Equipment (UE), Access Network (AN), and Core Network (CN)
  - User equipment: Interfaces the user, handles radio functionality
  - Access network: Communication to and from the user equipment, handles all radio related functionality in the network
  - Core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









- *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 temporarily 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)

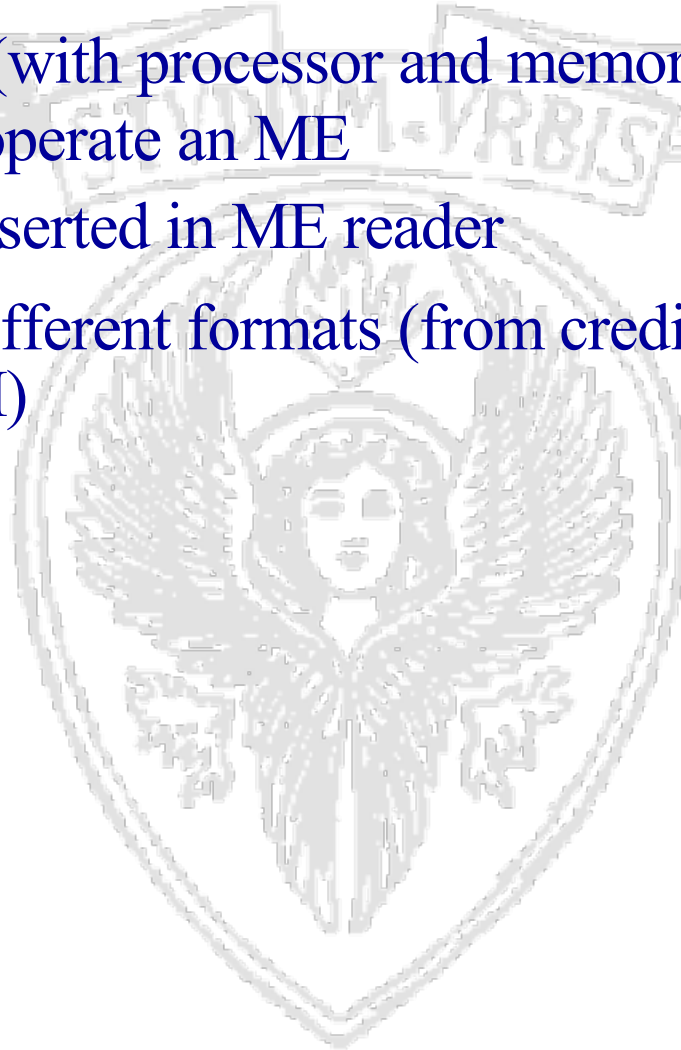


Classe	Potenza massima nominale [W]		Potenza media nominale [mW]	
	GSM 900 MHz	DCS 1800 MHz	GSM 900 MHz	DCS 1800 MHz
1	.	1	.	120
2	8	0,25	960	30
3	5	4	600	480
4	2	.	240	.
5	0,8	.	96	.

- 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



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







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



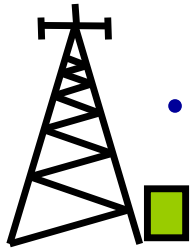
A Mobile Equipment without SIM is enabled to make only emergency calls

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





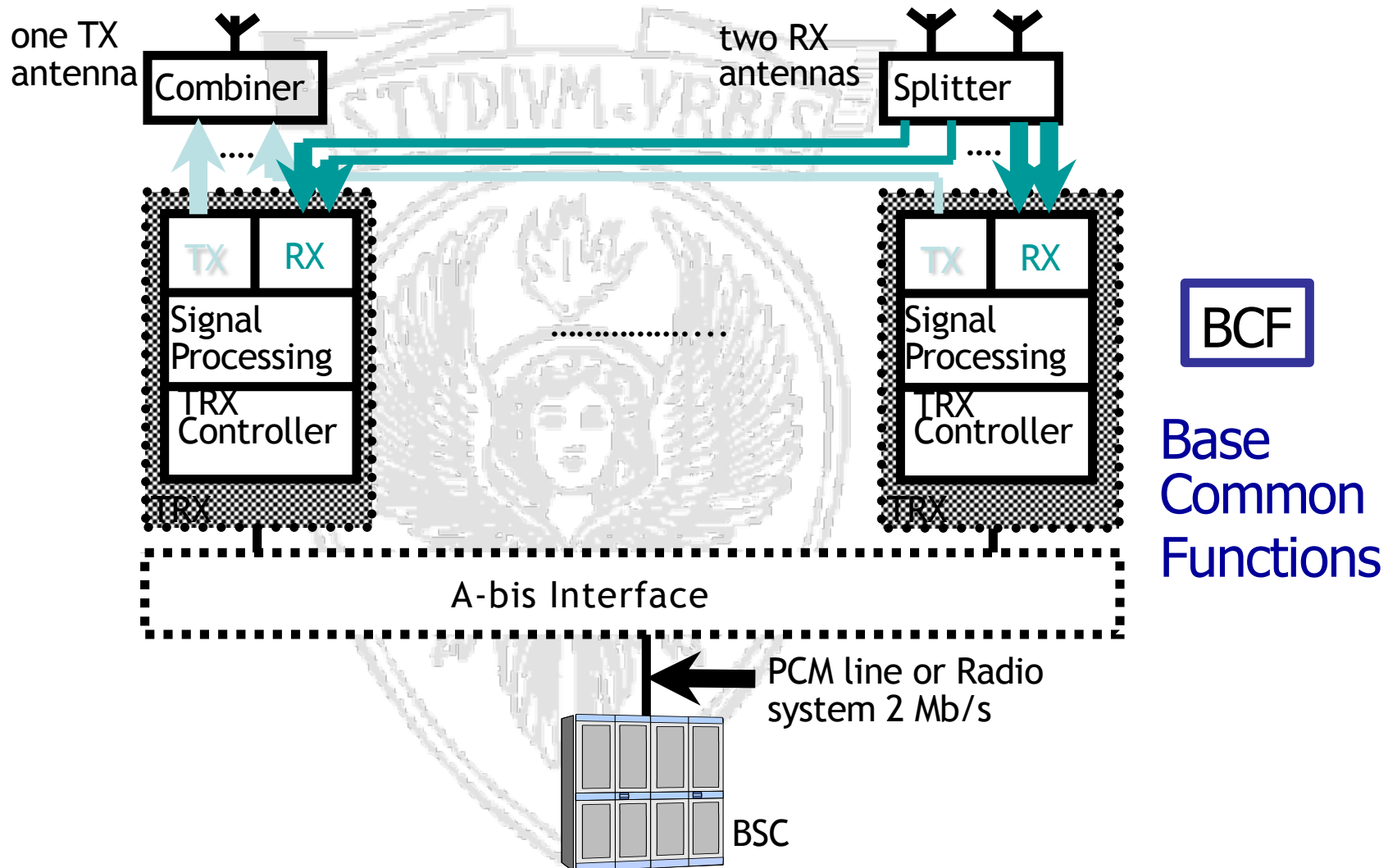
- BSS includes the functional units that deal with aspects of the radio system related to coverage and radio communication via a radio interface with the MS. The BSS also performs radio resource management
- BSS includes:
  - Base Transceiver Station (BTS)
  - HW / SW components that enable the transmission 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 ....



- 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 broadcasts 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)



- 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





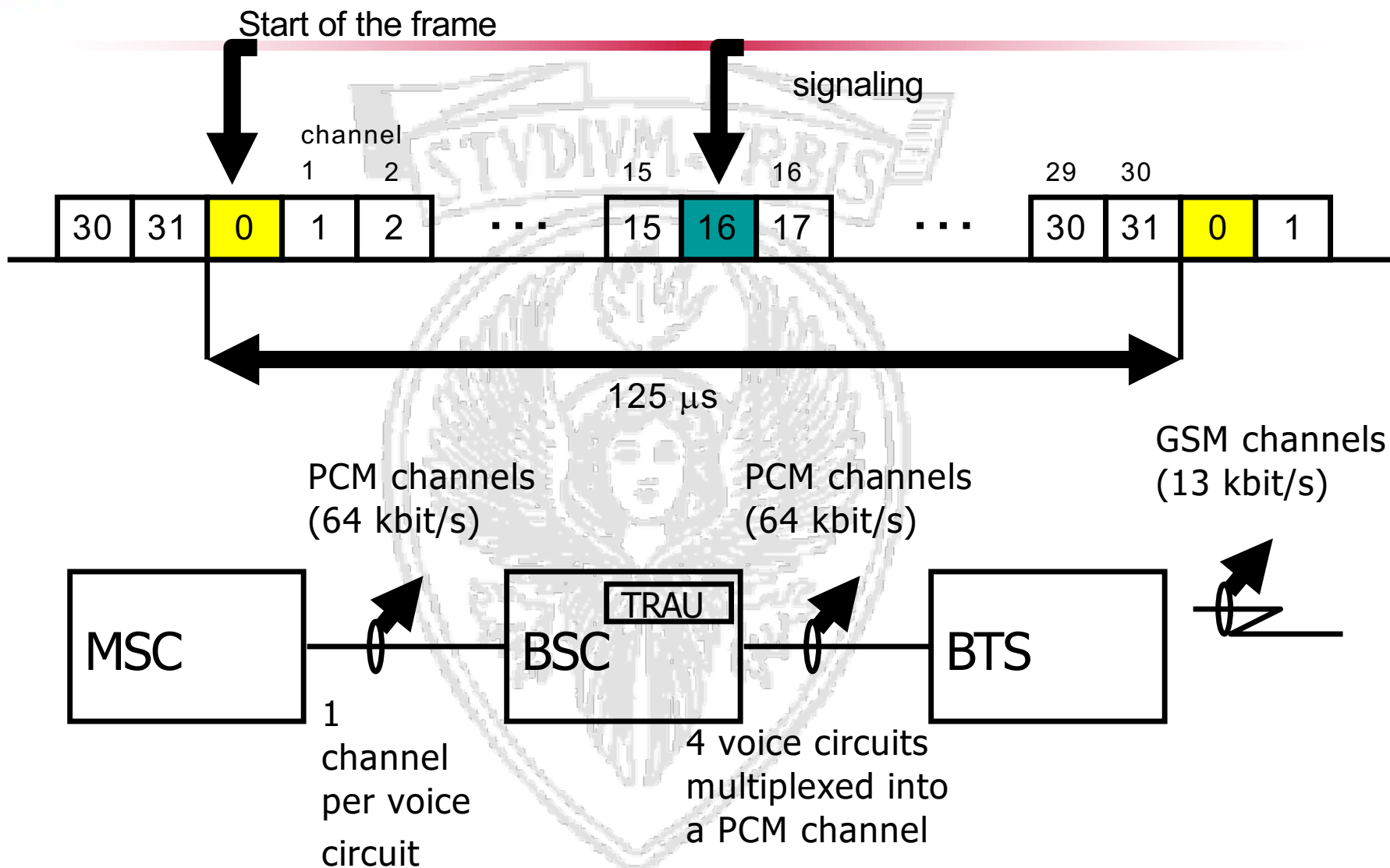


- GSM voice coding is 13 kbps while the PCM provides 64 kbps
- The transcoding is performed by the TRAU
- The TRAU may be in the BTS, but more often it is in the BSC
- In this case, the 13 kbps flows must be transported without coding in the channels at 64 kbps
- On each PCM channel 4 13Kbps flows are 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)





- 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



- 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



- It is the subsystem that is responsible for circuit switching to the mobile users, managing also 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.
  - Equipment 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 is interfaced to the fixed telephone network for routing to and from fixed users.

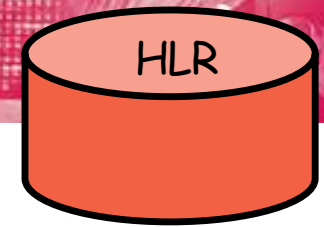




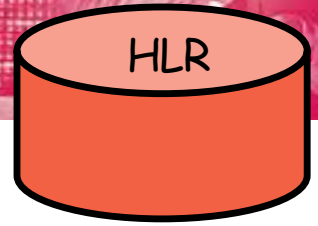
- An MS can be reached by fixed users using the phone number (MSISDN)
- The call is routed to the GMSC, which identifies the HLR that contains user information associated with the MSISDN and queries it to determine how to route to the mobile user current MSC
- the HLR returns the MSRN (Mobile Station 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



- 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 Transfer 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)



- 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..

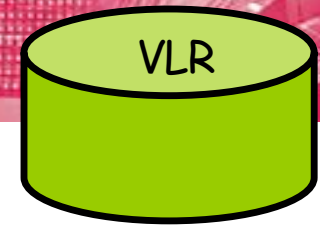


- Main tasks:
  - Managing localization, store the VLR number of each registered user
  - Sending routing information (MSRN) to the GMSC
  - Registration, Cancellation and activation/deactivation of additional services
  - storage and supply to the VLR of the parameters of authentication and encryption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



- 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.



- $K_i$ 
  - ✓ 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  $K_c$ , which is stored in the SIM and AuC

## Output of the procedures:

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

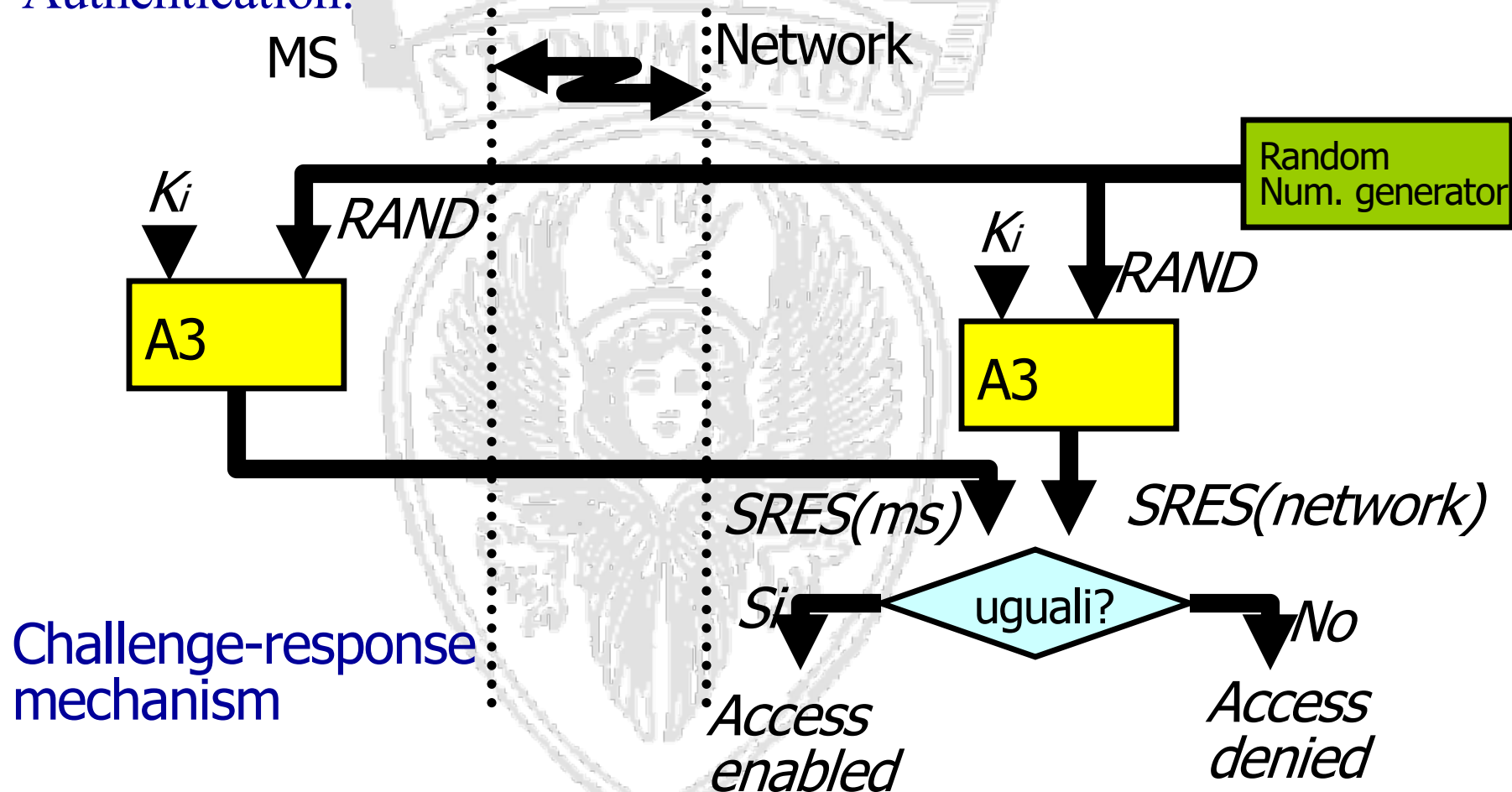
## Triplets

$(RAND, SRES, K_c)$

are generated sequentially for each IMSI and stored in the HLR



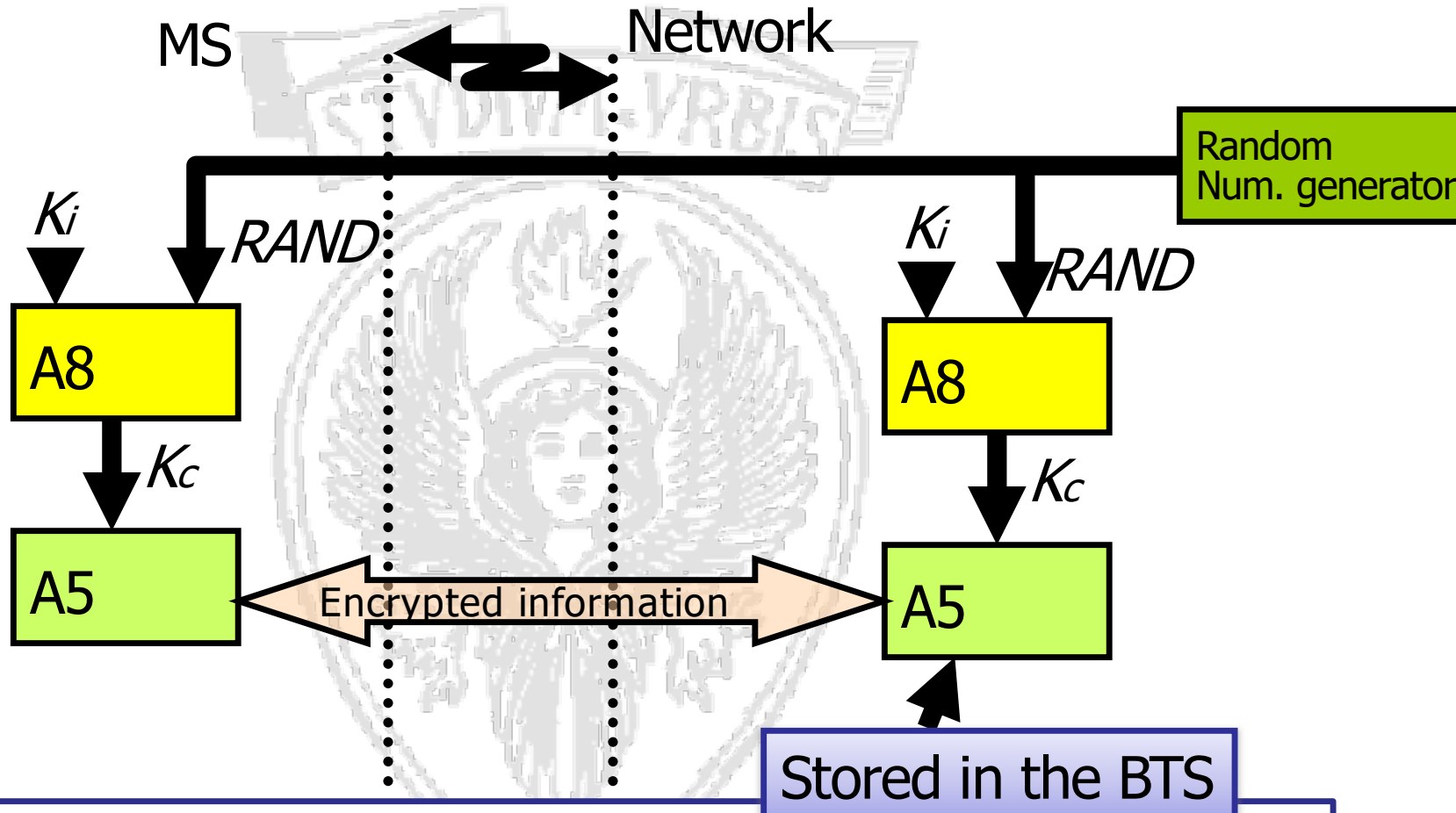
- Authentication:







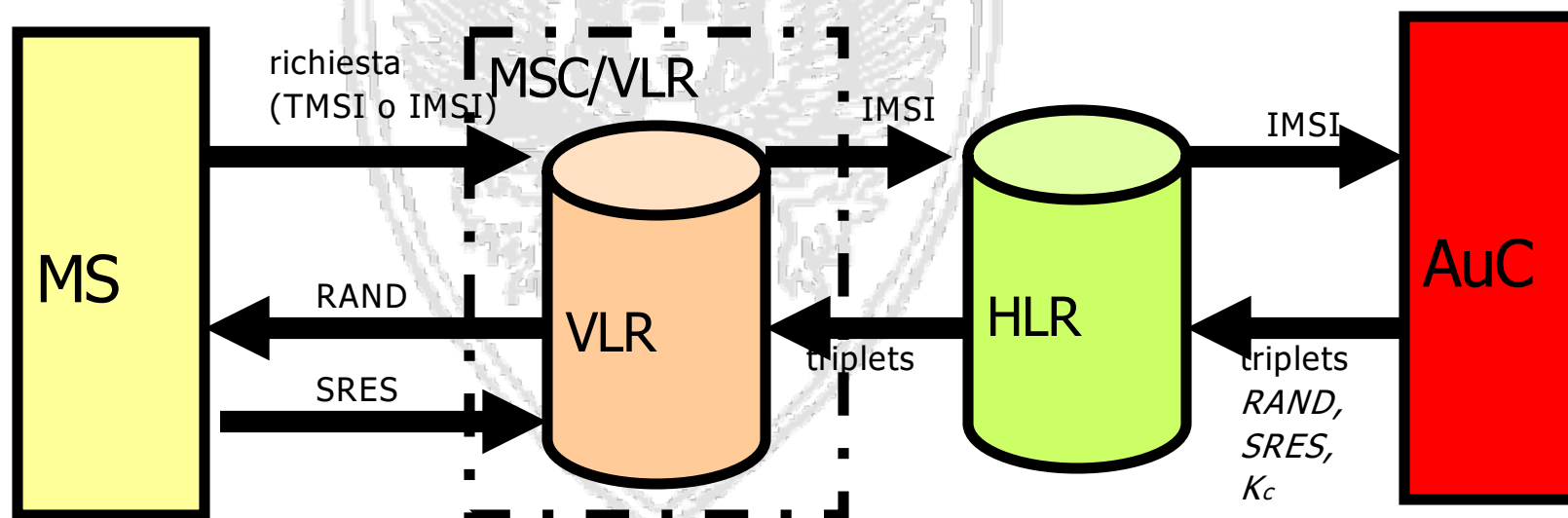
- Encryption



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.

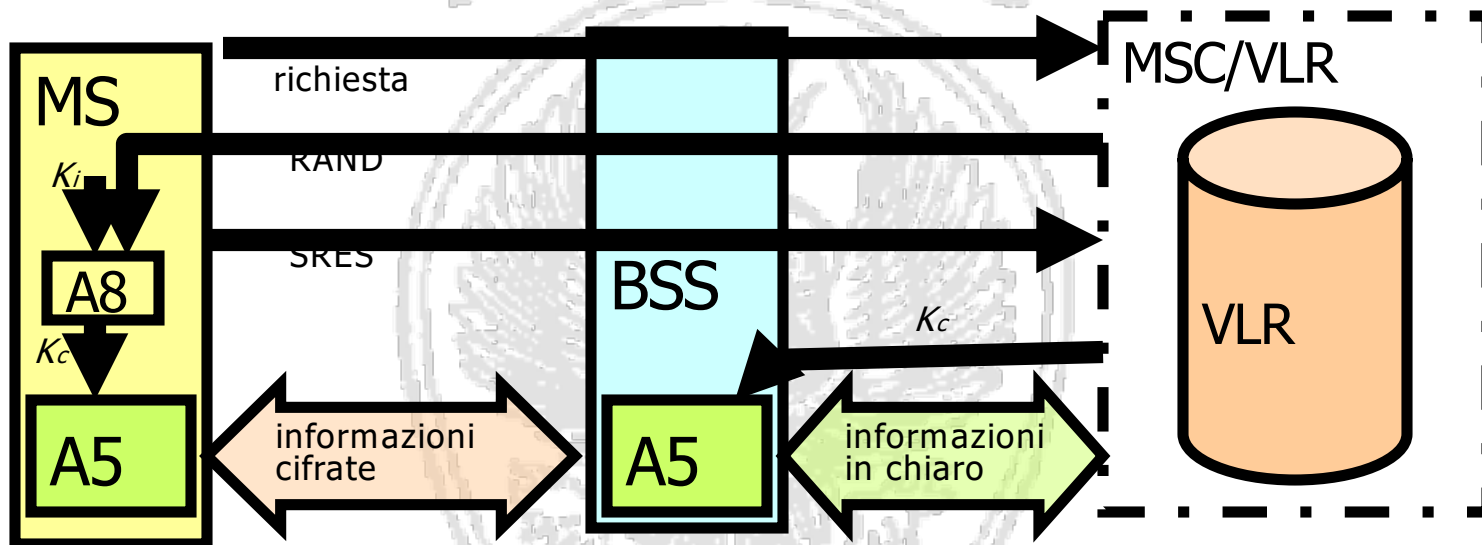
- Authentication Centre (AuC)
  - stores the secret keys  $K_i$  for each user
  - generates random numbers and calculates SRES and the encryption key  $K_c$
  - Provides the triplets to the other network elements

AuC





- BSS/NSS elements involved in data encryption





- 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.

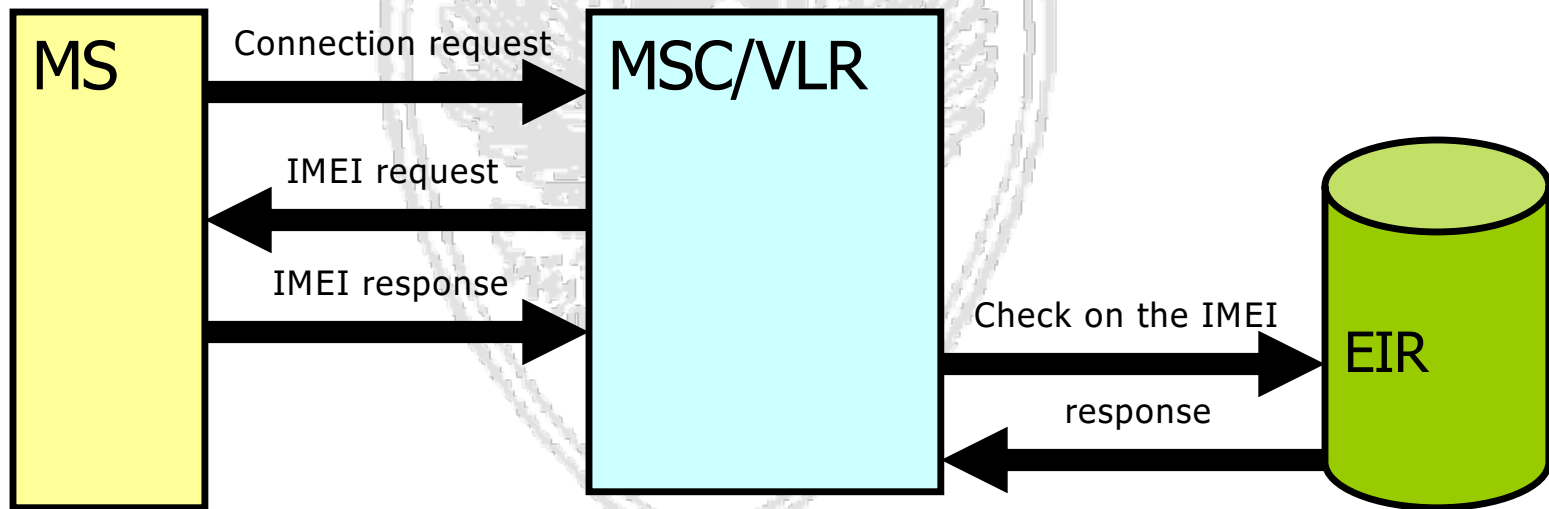




- It is the identification number for use in the network
- It consists of 3 fields:
  - MCC: Mobile Country Code (3 digits)
  - MNC: Mobile Network Code, which identifies the operator that provides the service (2 digits)
  - MSIC: Mobile Subscriber Identification Number, which identifies the SIM (up to 10 digits)
- For example, the number 222 01 4572228769, identifies an Italian SIM (222) of the operator TIM (01)
- The telephone number of the apparatus in question (MSISDN) is completely independent from the IMSI; the digits of the prefix (for ex. 0330 or 0347) identify the HLR and then the GMSC which the device is connected



- 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





- Protection against stolen and malfunctioning terminals
- Equipment Identity Register (EIR): 1 DataBase for each operator; keeps:
  - WHITE LIST:
    - ✓ valid IMEIs
    - ✓ Corresponding MEs may be used in the GSM network
  - BLACK LIST:
    - ✓ IMEIs of all MEs that must be barred from using the GSM network
    - ✓ Exception: emergency calls (to a set of emergency numbers)
    - ✓ Black list periodically exchanged among different operators
  - GRAY LIST:
    - ✓ IMEIs that correspond to MEs that can be used, but that, for some reason (malfunctioning, obsolete SW, evaluation terminals, etc), need to be tracked by the operator
    - ✓ A call from a “gray” IMEI is reported to the operator personnel



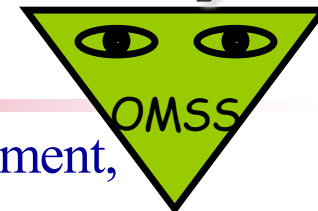
- Include the functional units responsible for monitoring the network, its maintenance and remote management
- It deals with:
  - configuring the functionality of all network devices
  - displayed alarms on malfunctioning elements
  - shows the statistics on data traffic
- etc..



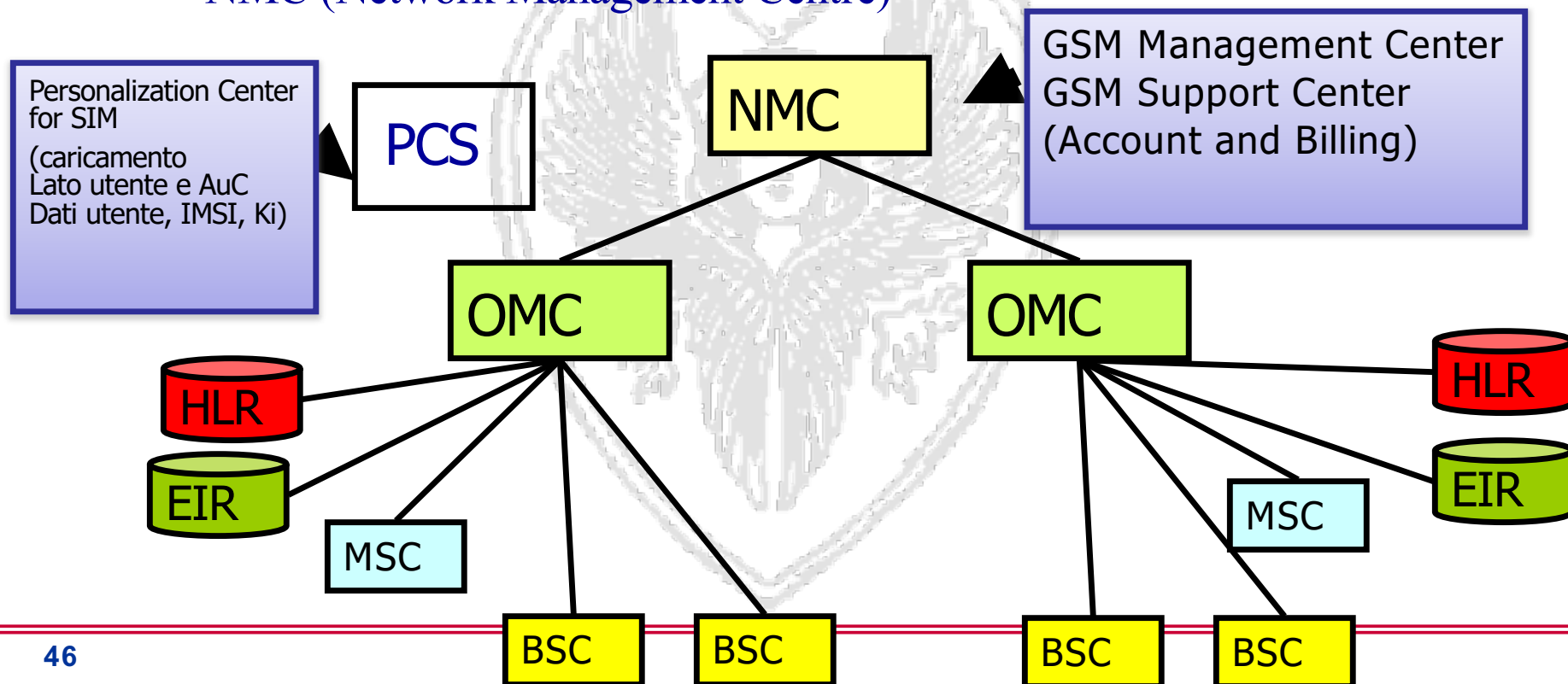


- Network measurement and control functions
- Monitored and initiated from the OMC (Operation and Maintenance Center)
- Basic functions
  - Network Administration
    - ✓ configuration, operation, performance management, statistics collection and analysis, network maintenance
  - Commercial operation & 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*



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





- Mobile Station ISDN Number (MSISDN)

It is the user mobile telephone number( $\leq 15$  cifre)

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)



- International Mobile Subscriber Identity (IMSI)

Permanently stored in the SIM and HLR, temporarily in the VLR; uniquely identifies the subscriber

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

- Temporary Mobile Subscriber 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 octets.

- 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





- 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 (operator), 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 regions users can roam.
- Base Station Identity Code (BSIC)

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



- IMSI (→HLR,VLR)
- MSISDN (→HLR, VLR)
- TMSI (→VLR)
- MS category (→HLR,VLR)
- RAND,SRES,Kc (→HLR, provided upon request to the VLR)
- Cyphering Key Sequence Number (→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)



### ***3.3 – Radio Interface***

Wireless systems

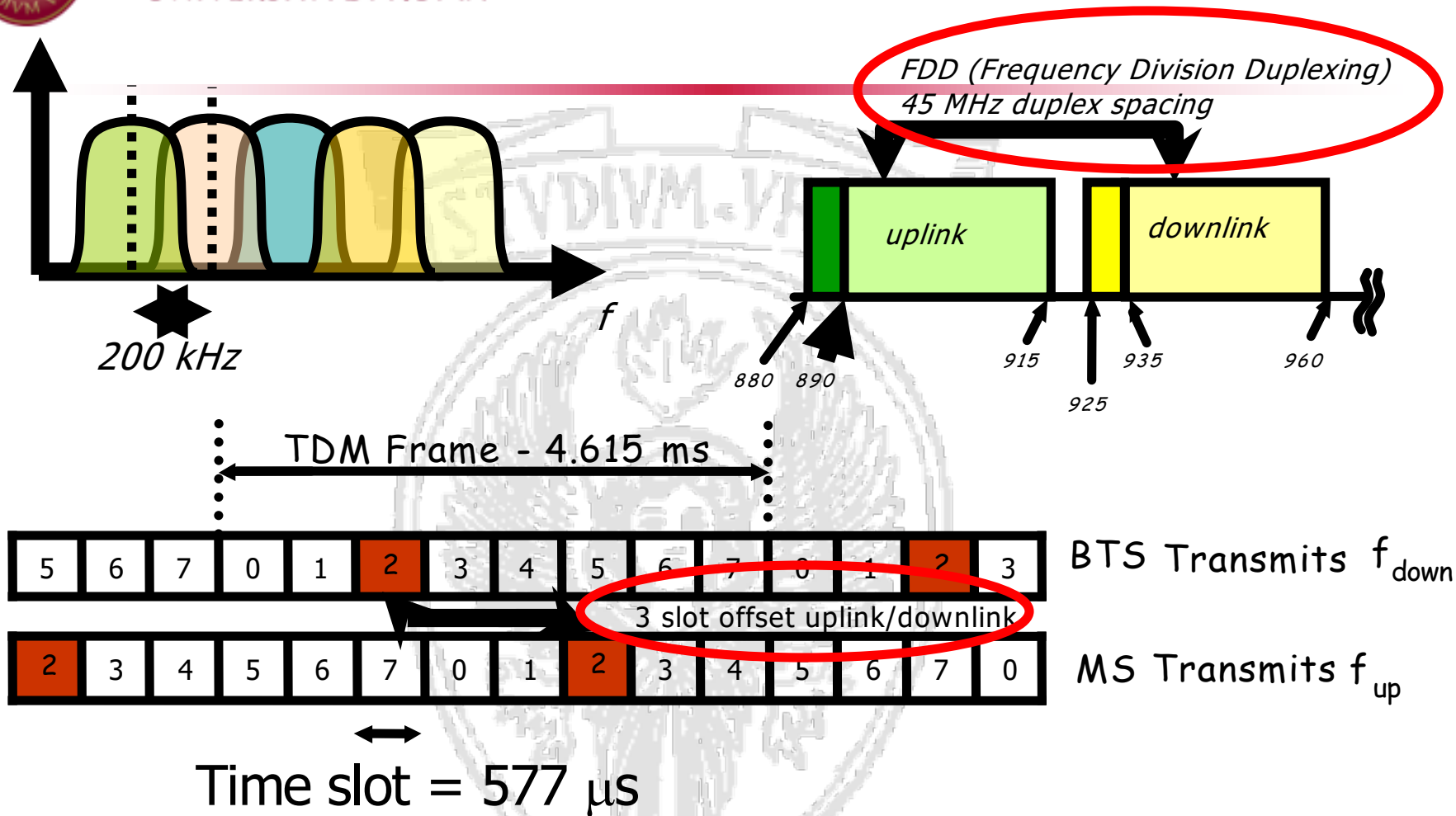


si veda

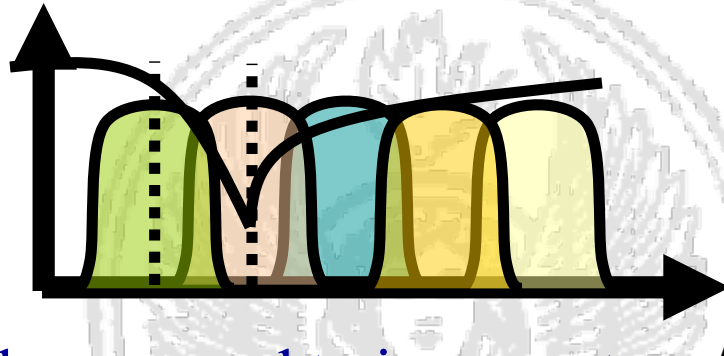
- ☒ O. Bertazioli, L. Favalli, *GSM-GPRS*, Hoepli Informatica 2002  
*Capitolo 6*







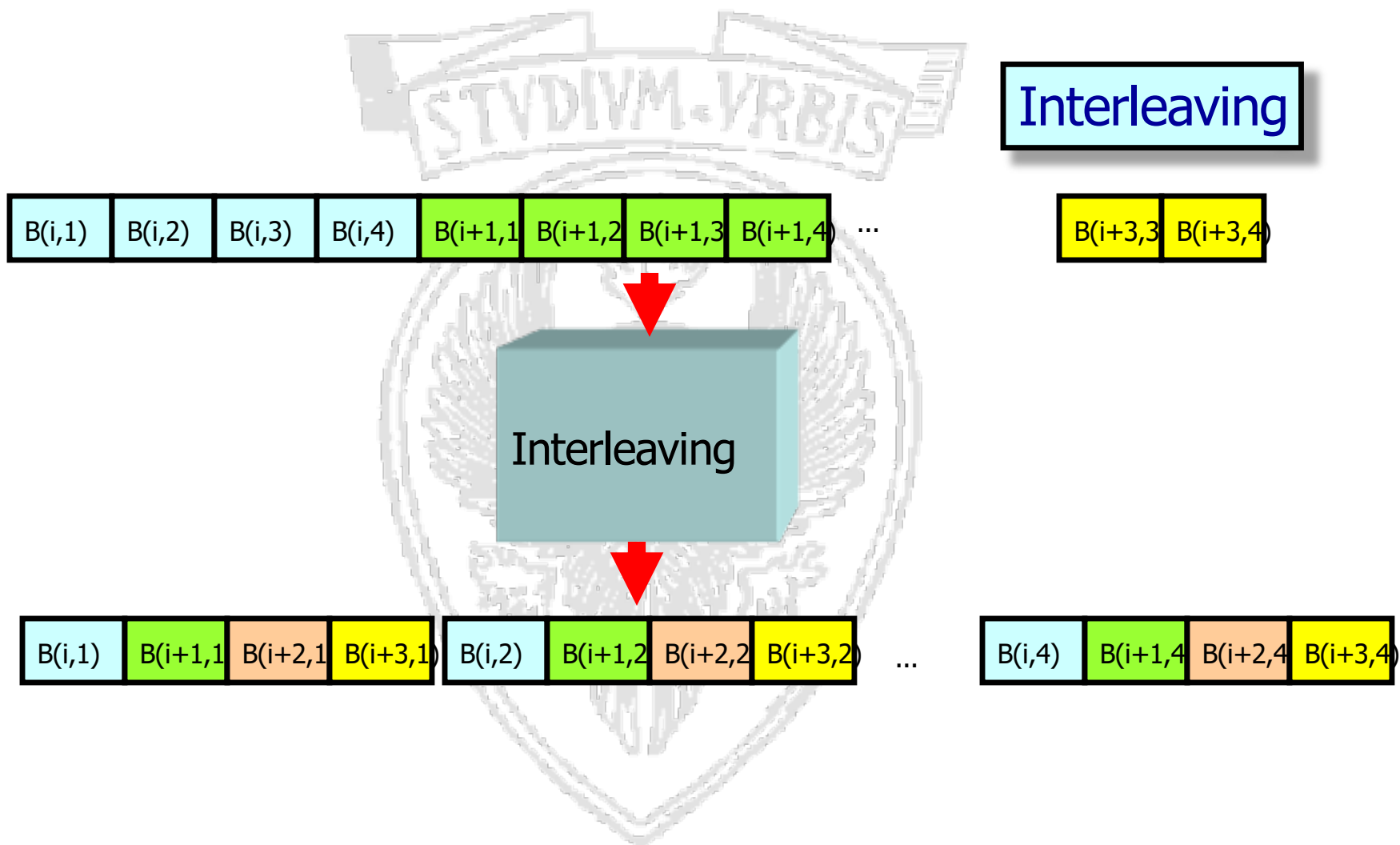
- Multipath fading depends on the carrier used for transmission
- At a given time, when transmitting to a user some carriers may suffer high attenuation while others low attenuation



- 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





- 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





- 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



- 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

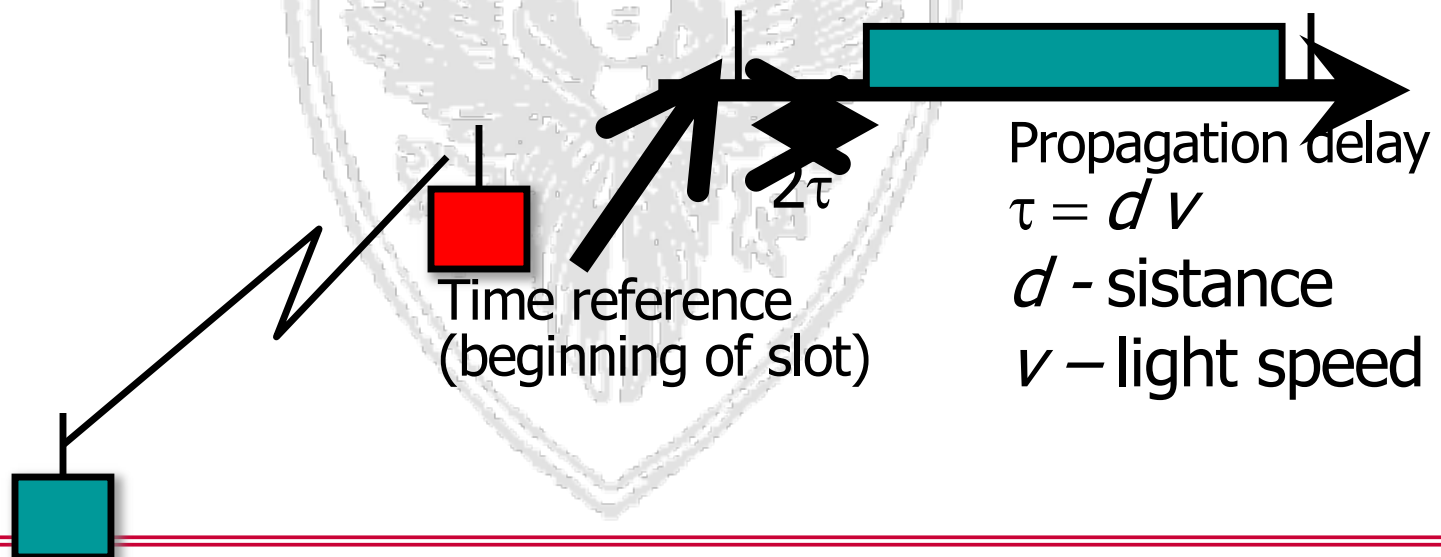


- Many channels in GSM follow a multiframe structure (for example, the broadcast channel is broadcast every  $x$  frames)
- The sequence of frequency hopping depends on the multiframe structure
- Each MS must therefore know the number of the current frame to correctly interpret the information
- The 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



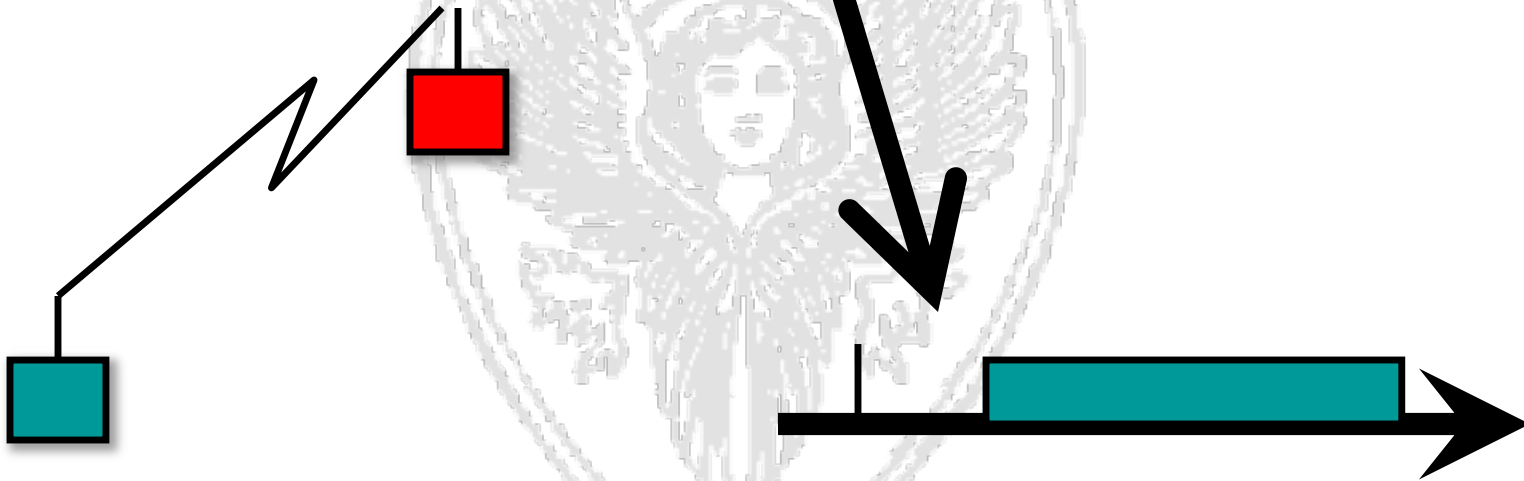




# Slot synchronization

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

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



- 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  $33,3 \mu\text{sec}$ )

2) Propagation delay estimation      4) Following transmissions

