IoT, Course introduction

Internet of Things a.a. 2021/2022

Un. of Rome “La Sapienza”

Chiara Petrioli

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

3.3 – Radio Interface

Wireless systems

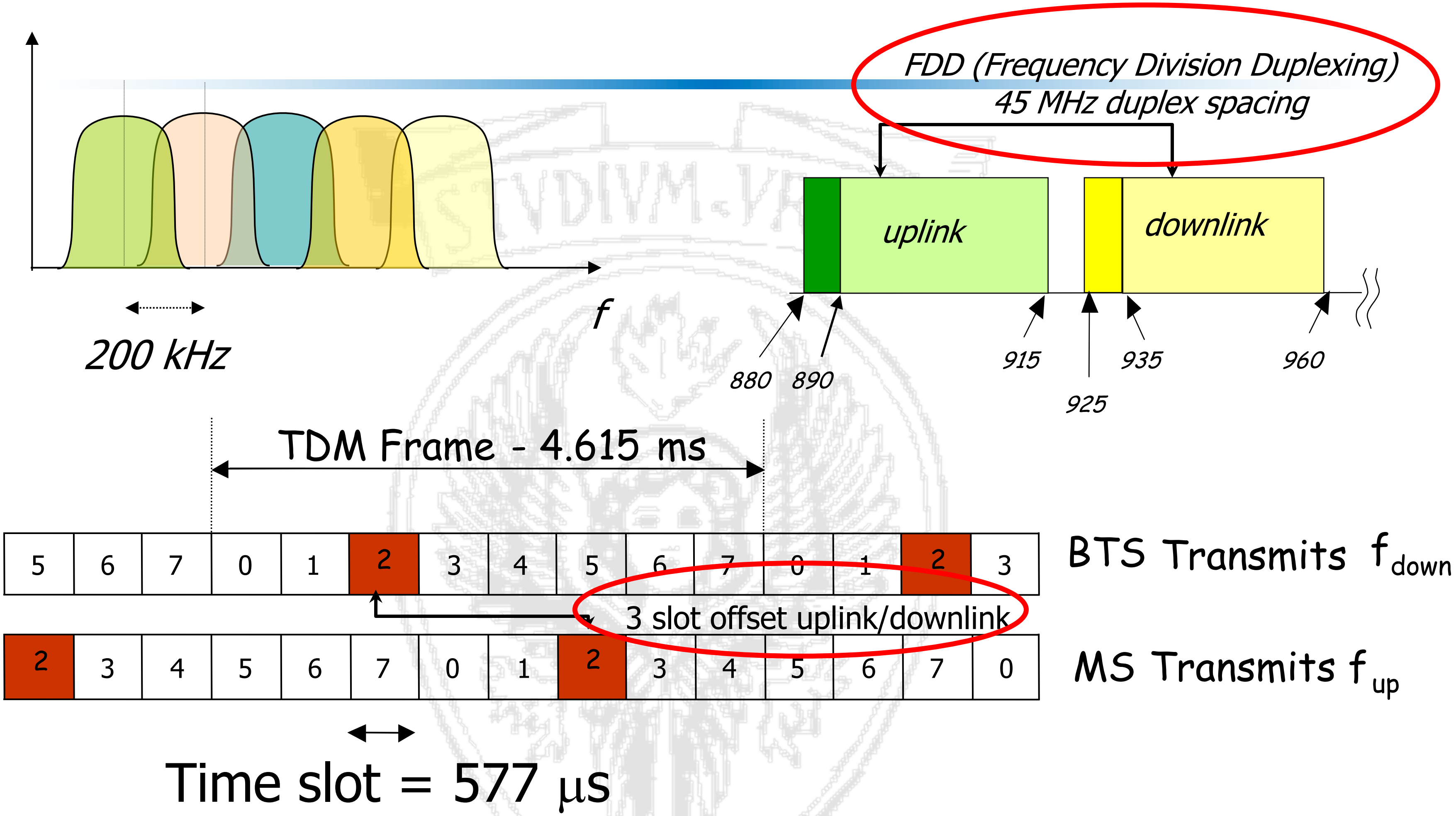
Radio Interface

<u>si veda</u>

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

Capitolo 6

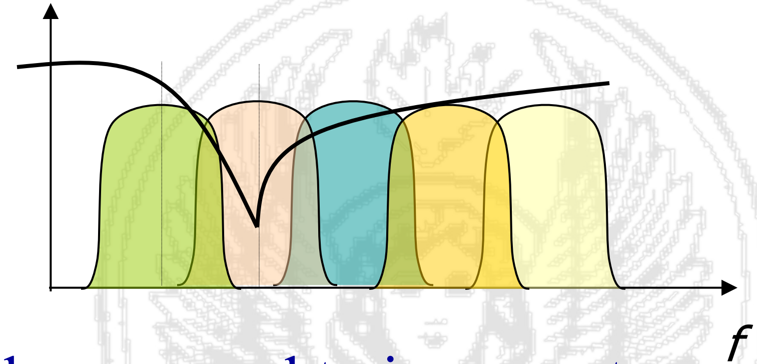
Radio Interface



5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	BTS Transmits f_{down}
2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	MS Transmits f_{up}

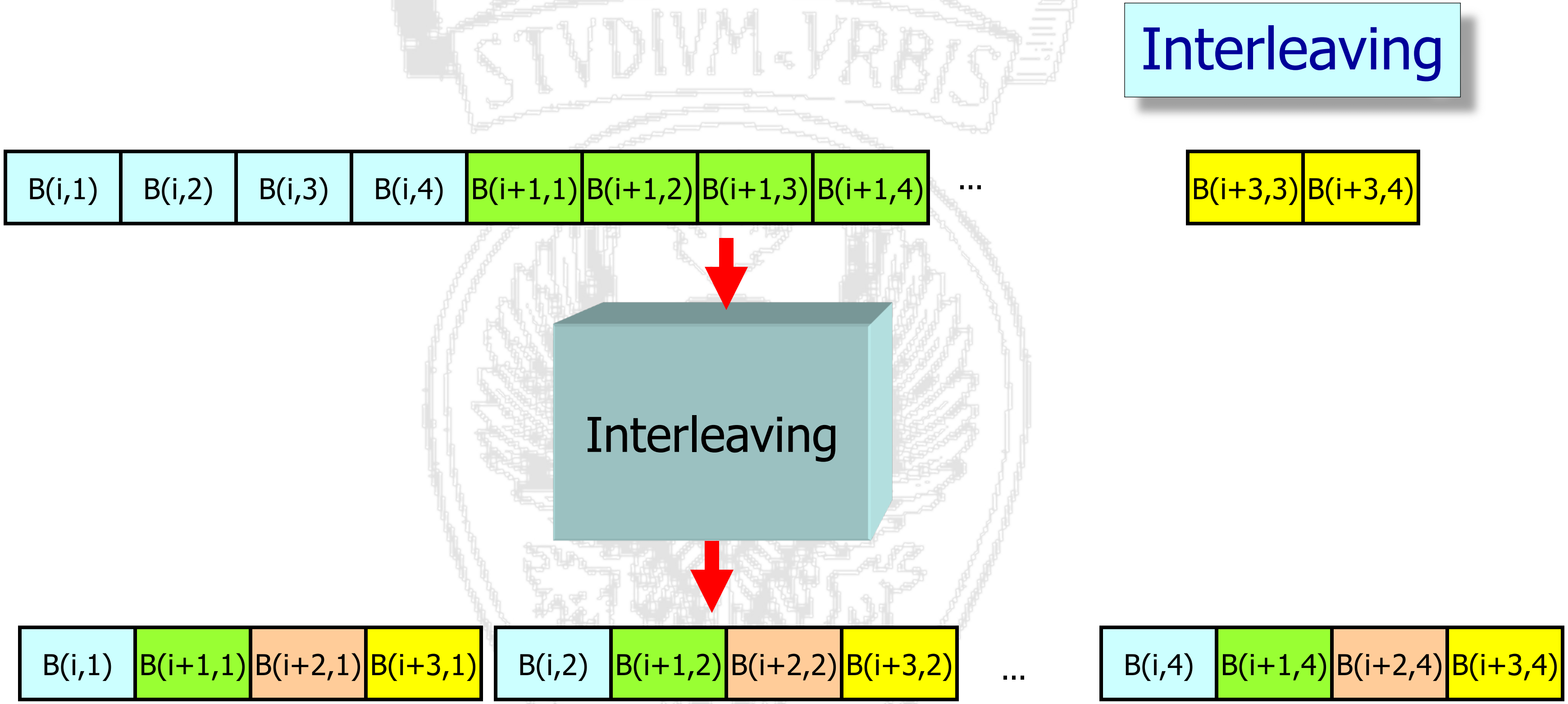
Frequency Hopping

- 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



Interleaving

B(i,1) B(i,2) B(i,3) B(i,4) B(i+1,1) B(i+1,2) B(i+1,3) B(i+1,4) ··· B(i+3,3) B(i+3,4)

Interleaving

B(i,1) B(i+1,1) B(i+2,1) B(i+3,1) B(i,2) B(i+1,2) B(i+2,2) B(i+3,2) … B(i,4) B(i+1,4) B(i+2,4) B(i+3,4)

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 Synchronization

- 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

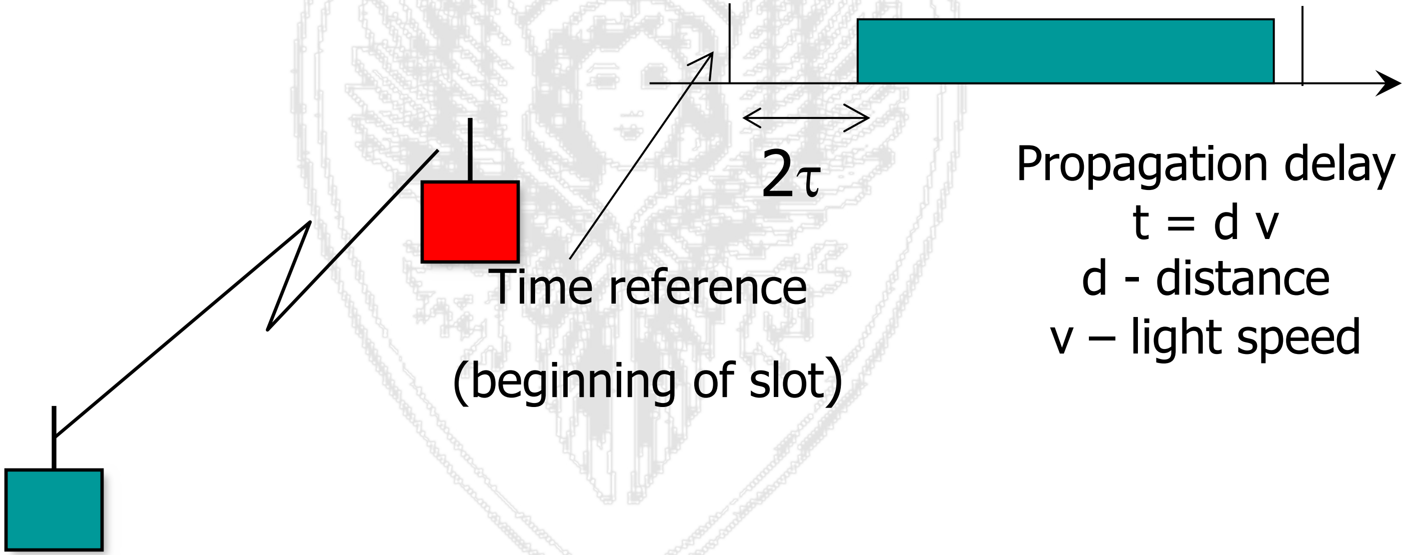
- The frequency of the radio carrier is obtained by the MS listening to the broadcast common control channel transmitted by the BTS
- On this channel, at regular intervals, a special fixed sequence of bits is transmitted at high power that is used to select the carrier frequency, and then adjust the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



2τ

Time reference

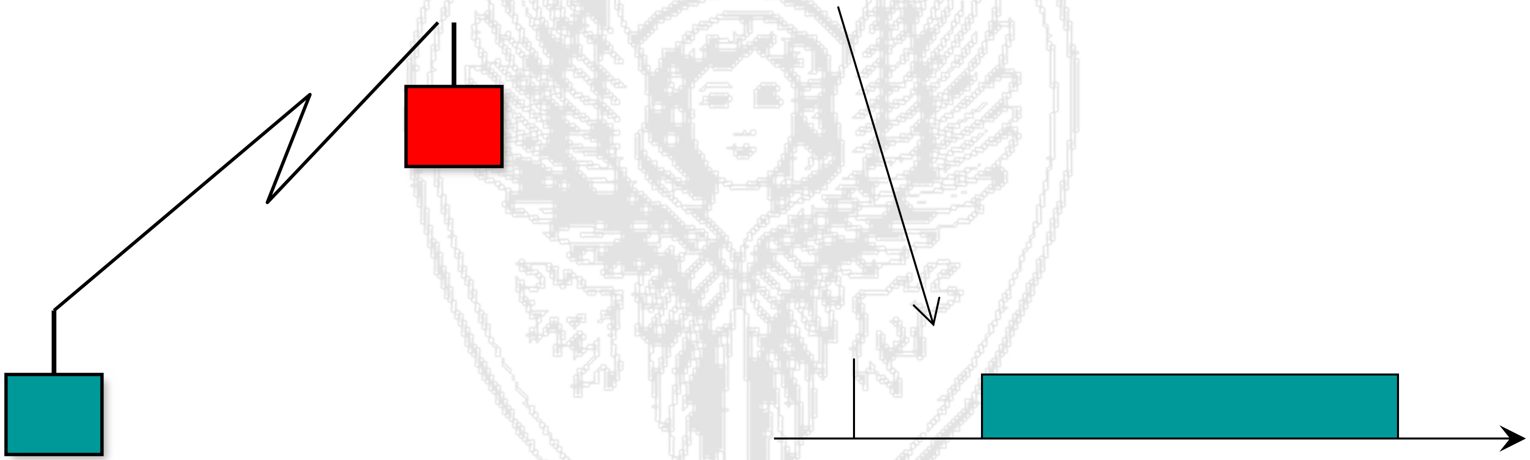
(beginning of slot)

Propagation delay
t = d v
d - distance
v – light speed

Slot synchronization

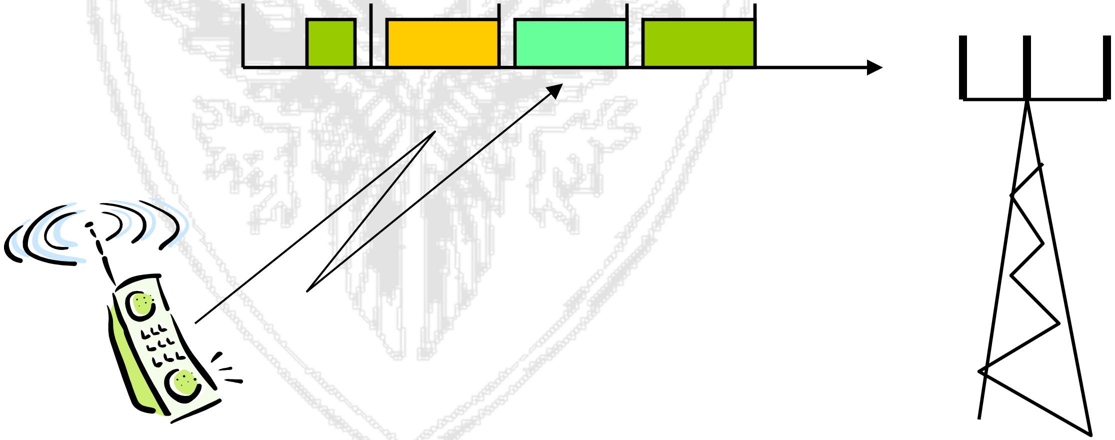
- We could make a conservative selection, setting the guard time to

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



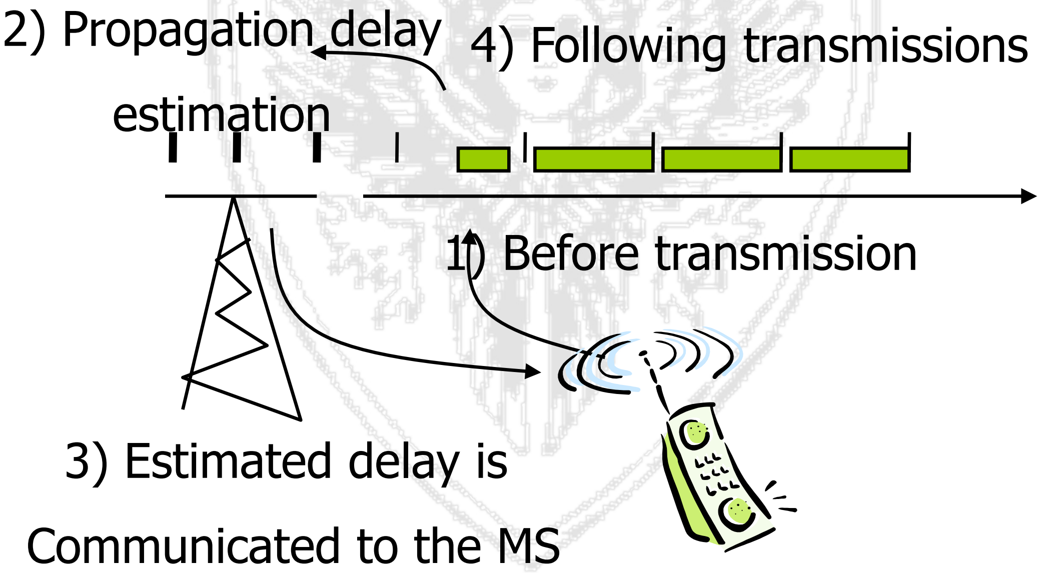
Slot synchronization

- 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 $2\tau = 2 \times 35 / 3 \times 10^8 = 233$ µs
- 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)



2) Propagation delay estimation

4) Following transmissions

1) Before transmission

3) Estimated delay is Communicated to the MS

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

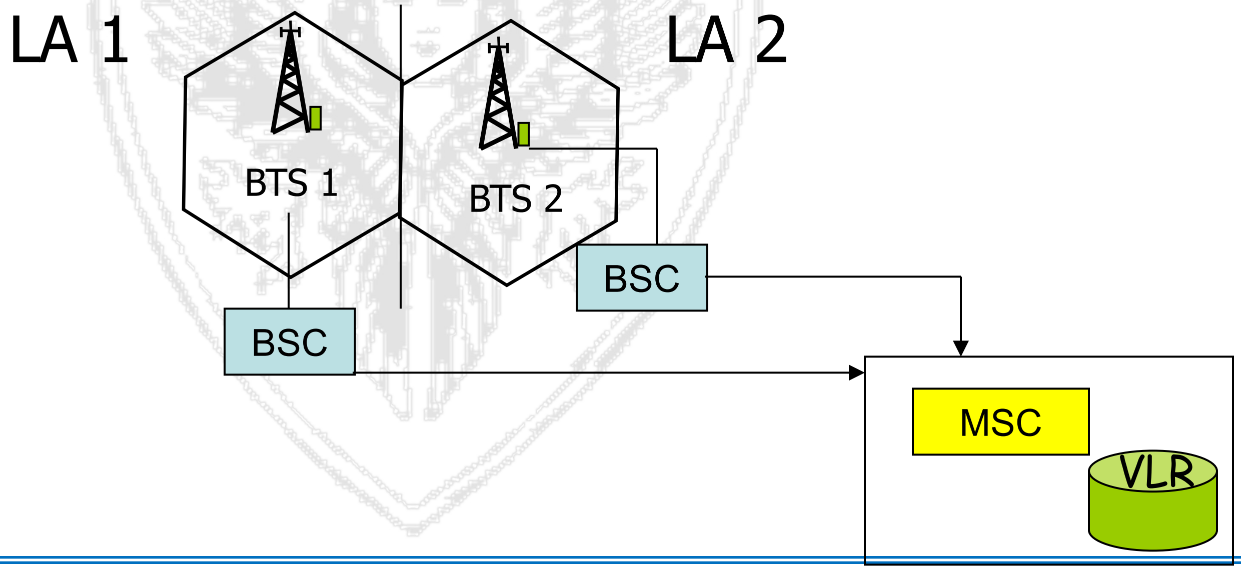
Two cases are possible, based on the **received LAI**:

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.

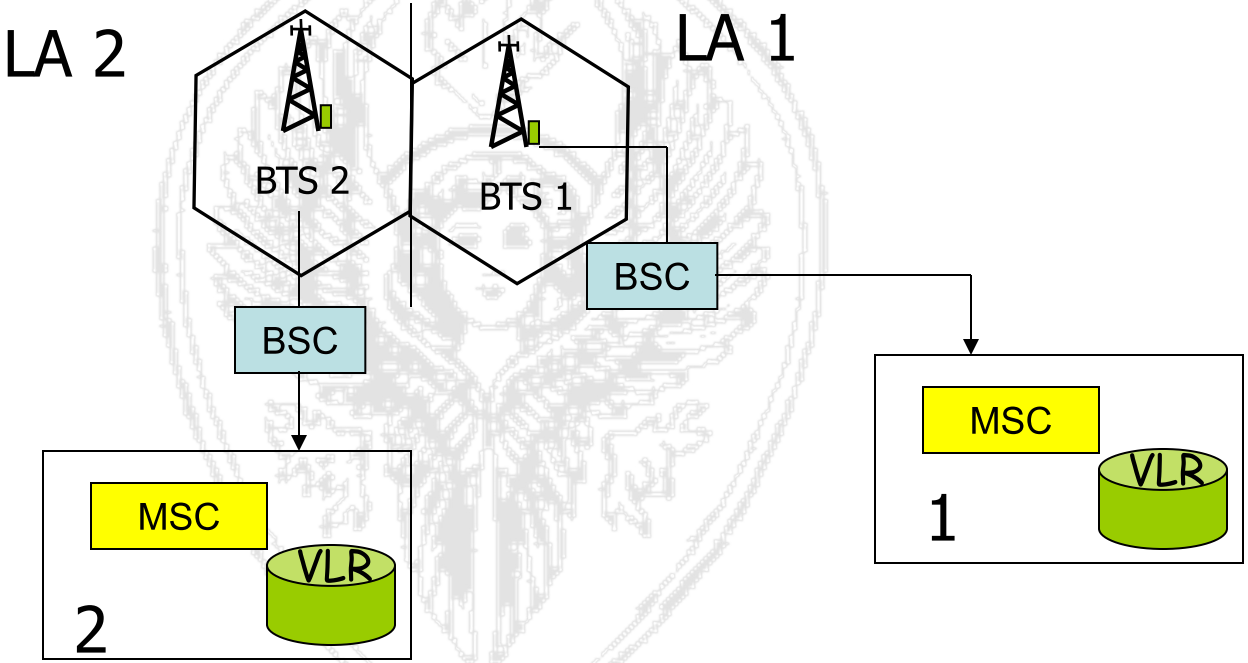
Location Update (1)

- 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)



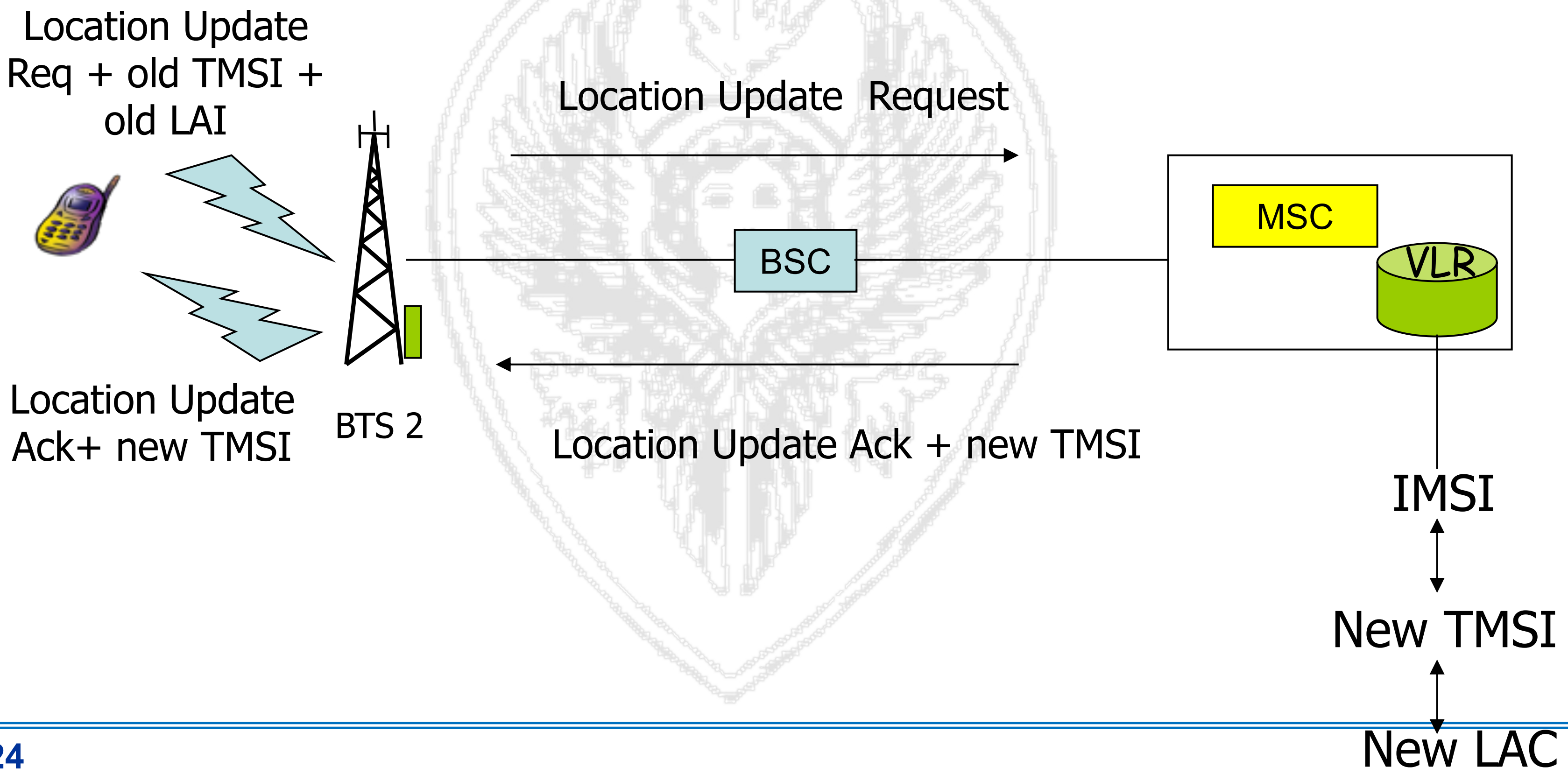
Location Update (2)

- Roaming between LAs of different MSC/VLRs

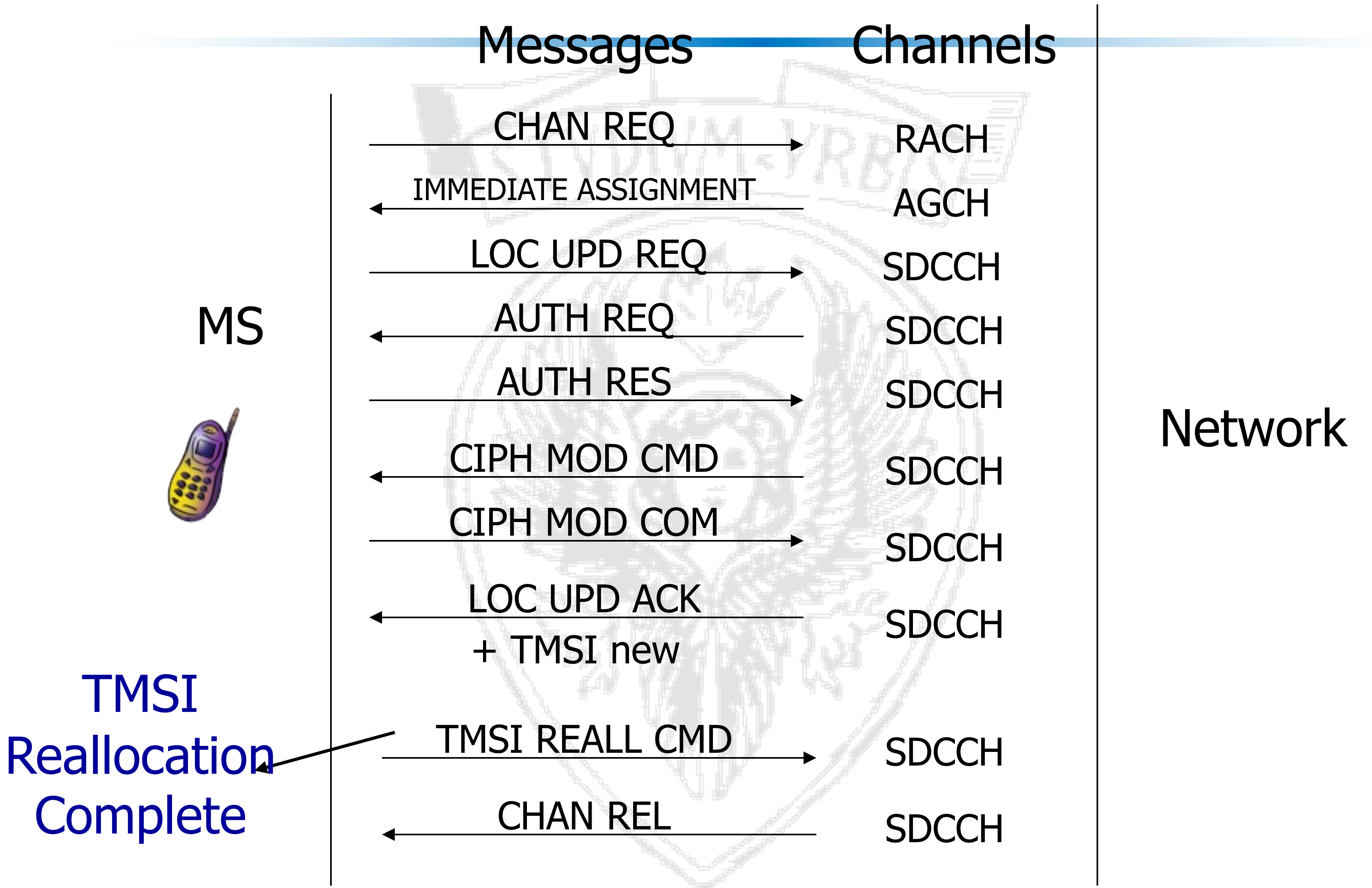


Location Update - Intra MSC

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 Req + old TMSI + old LAI
Location Update Request
MSC
BSC
VLR
Location Update Ack+ new TMSI
BTS 2
Location Update Ack + new TMSI
IMSI
New TMSI
New LAC

Location Update - Intra MSC



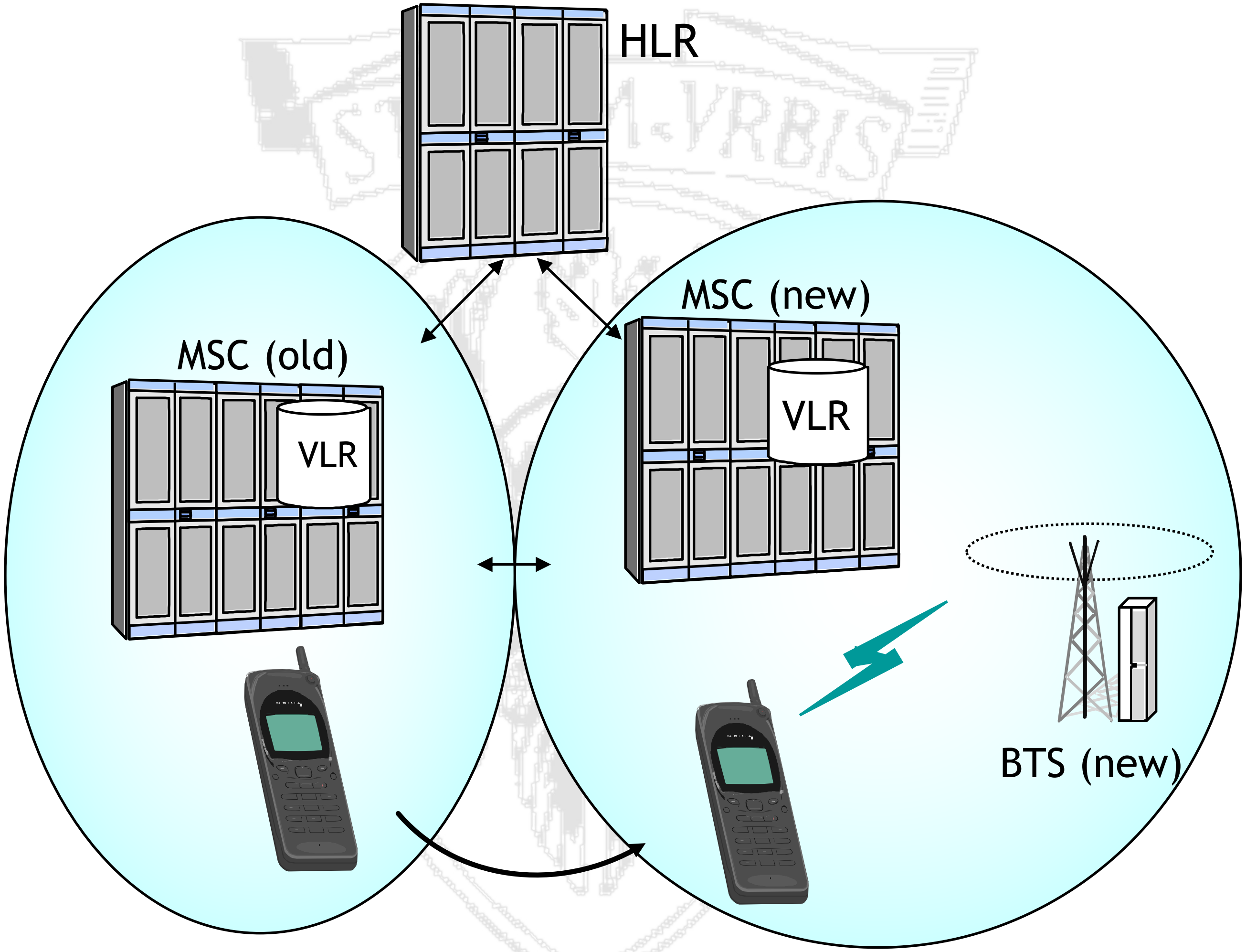
MS

Network

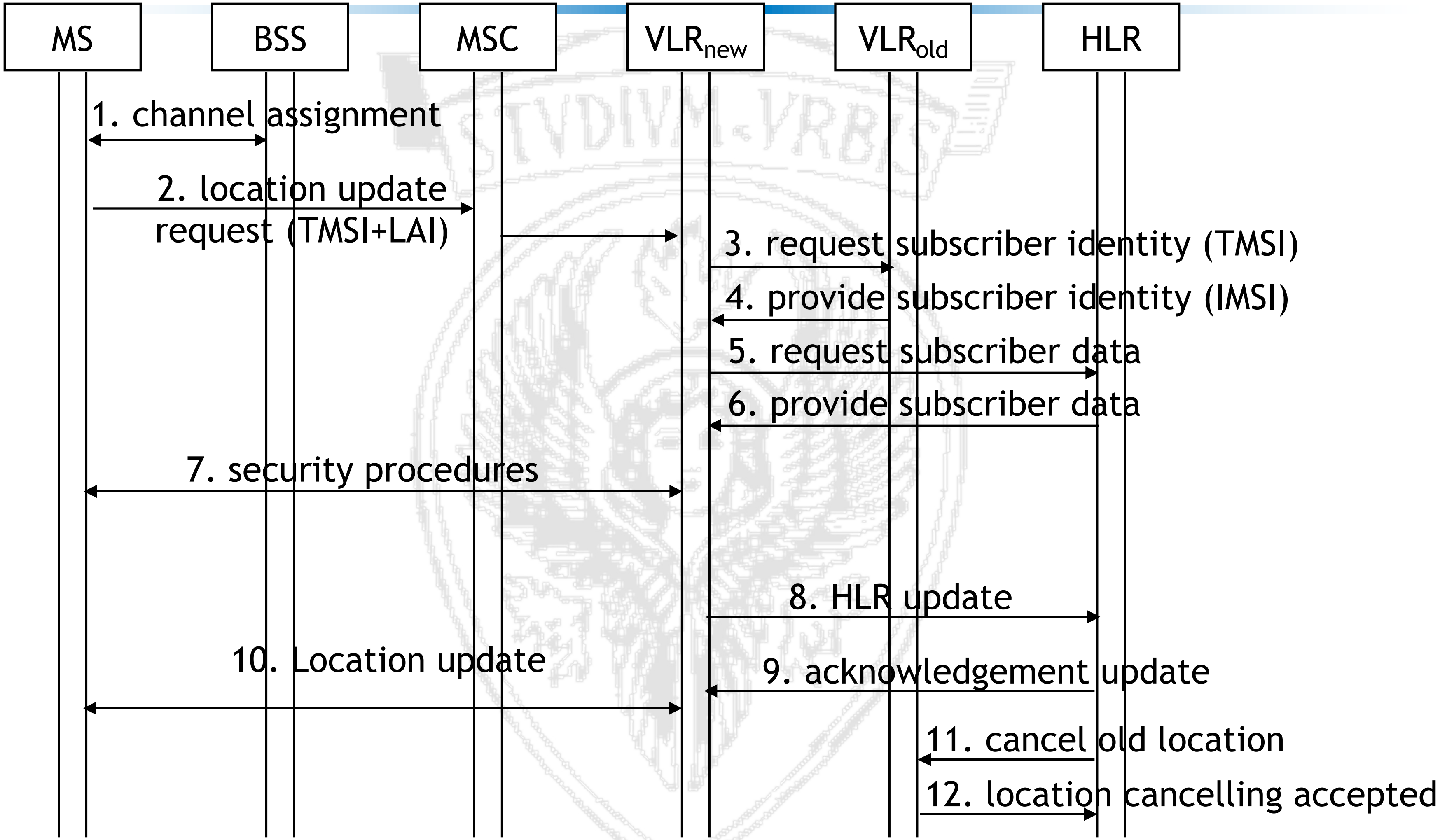
Messages	Channels
CHAN REQ →	RACH
← IMMEDIATE ASSIGNMENT	AGCH
LOC UPD REQ →	SDCCH
← AUTH REQ	SDCCH
AUTH RES →	SDCCH
← CIPH MOD CMD	SDCCH
CIPH MOD COM →	SDCCH
← LOC UPD ACK + TMSI new	SDCCH
TMSI REALL CMD →	SDCCH
← CHAN REL	SDCCH

TMSI Reallocation Complete

Location Update inter MSC

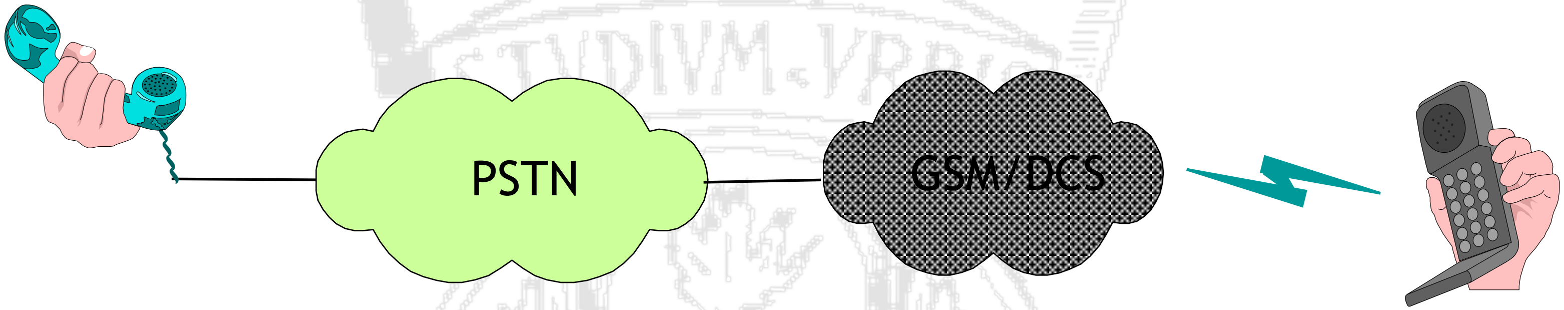


Location Update inter MSC


MS
BSS
MSC
VLRnew
VLRold
HLR
1. channel assignment
2. location update request (TMSI+LAI)
3. request subscriber identity (TMSI)
4. provide subscriber identity (IMSI)
5. request subscriber data
6. provide subscriber data
7. security procedures
8. HLR update
9. acknowledgement update
10. Location update
11. cancel old location
12. location cancelling accepted

Call Set Up

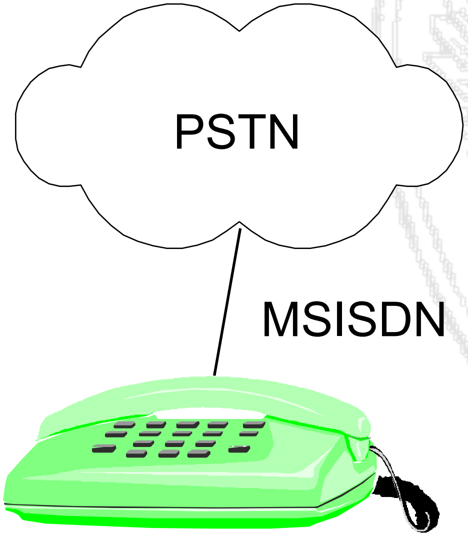
Call originated from PSTN



- 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)

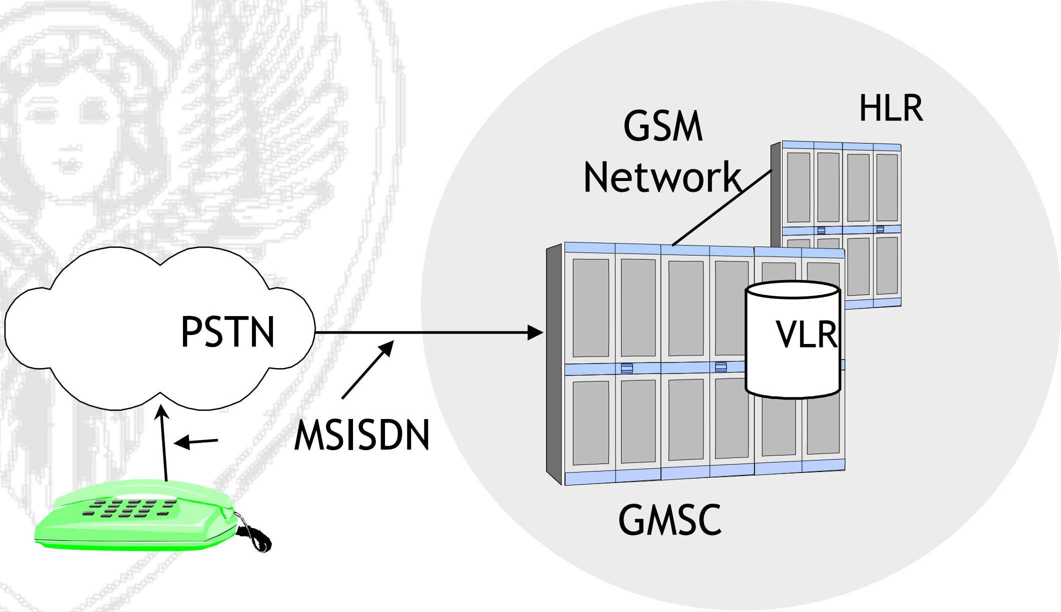
347 = National Destination code

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

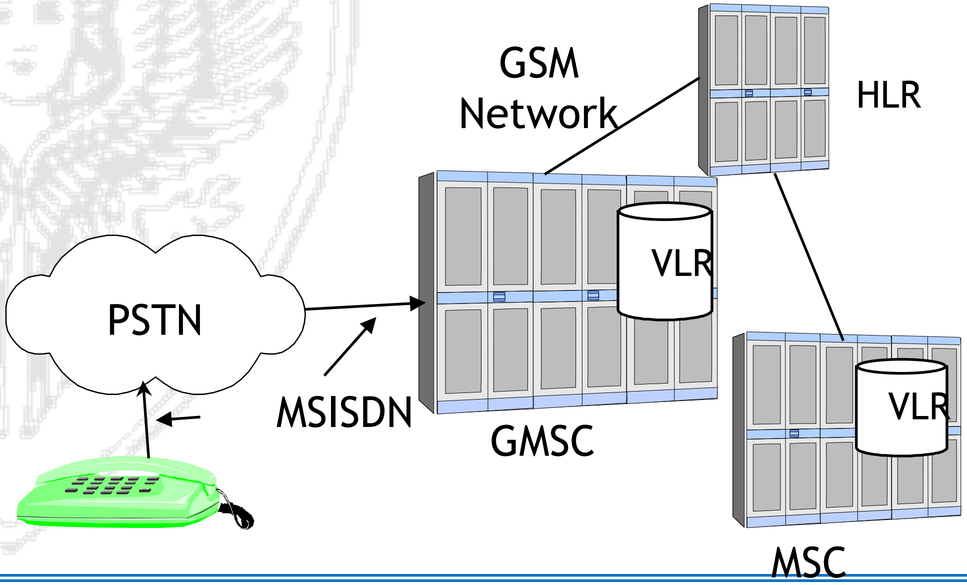


Call Set-up Step by Step (3)

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

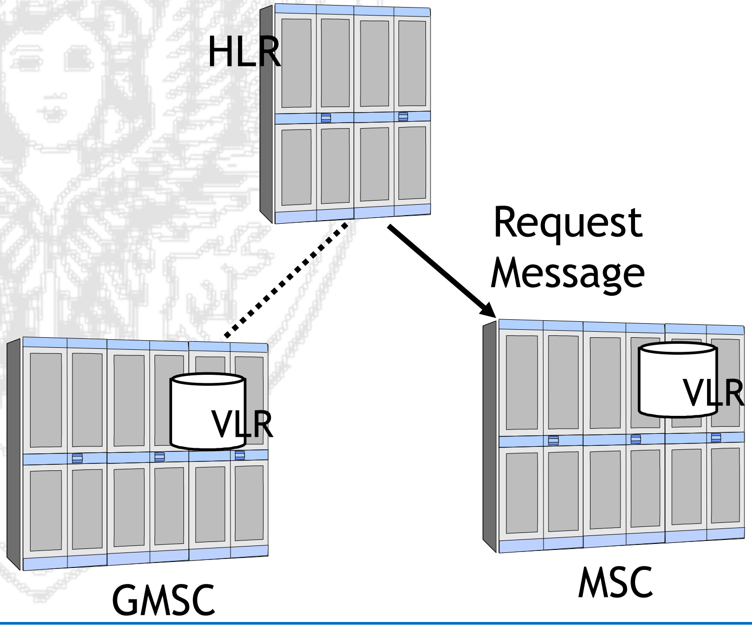
F The HLR identifies the address of the VLR in which the called MS is currently registered



Call Set-up Step by Step (4)

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

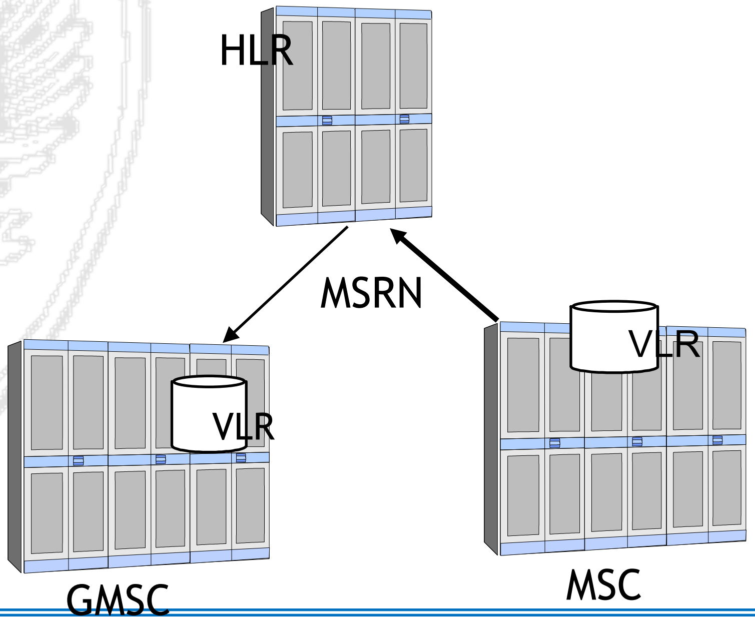
H The MSC/VLR temporarily allocates a Mobile Station Roaming Number (MSRN) to be used for the call



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

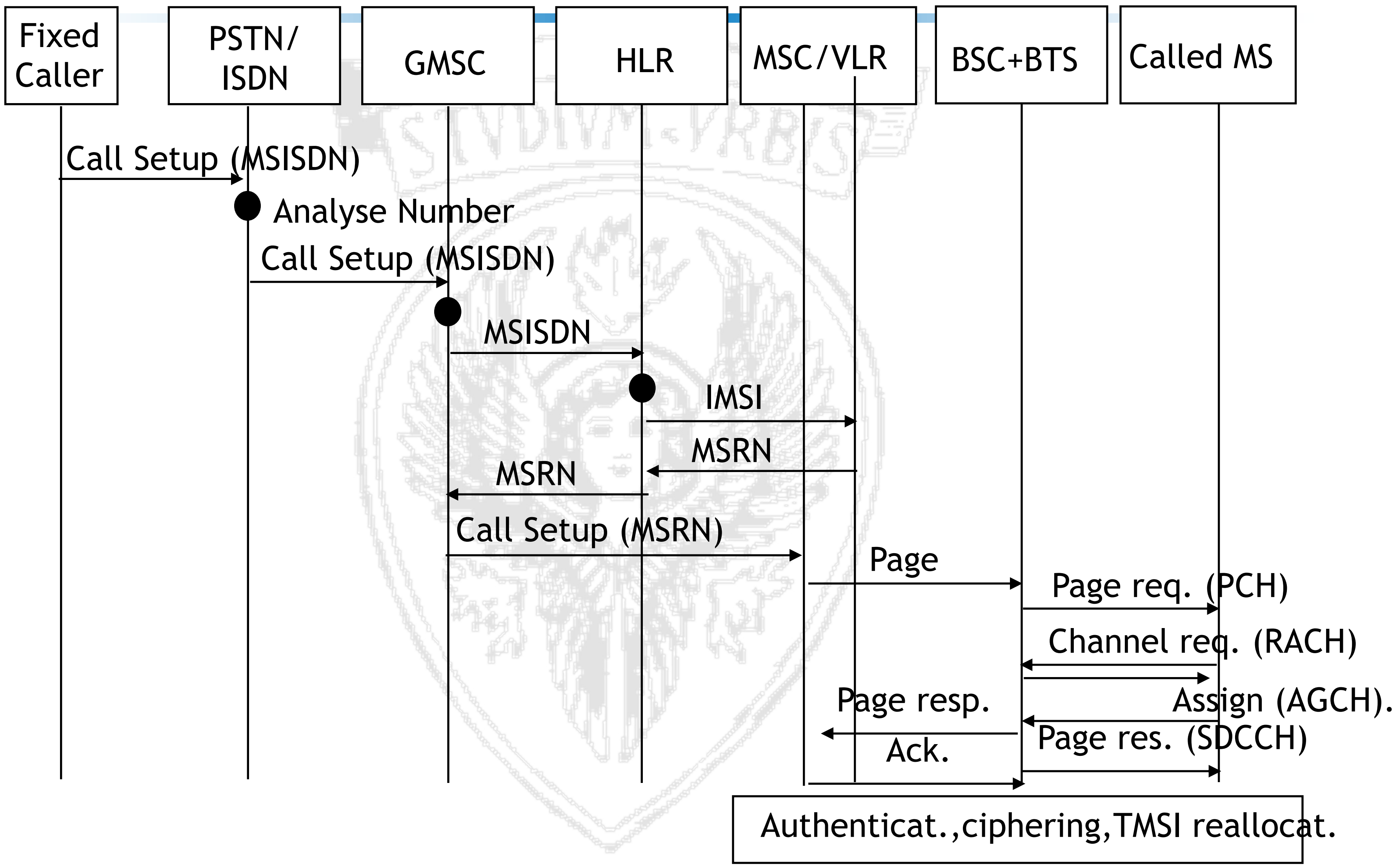
P A traffic channel (TCH) is allocated for the communication

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

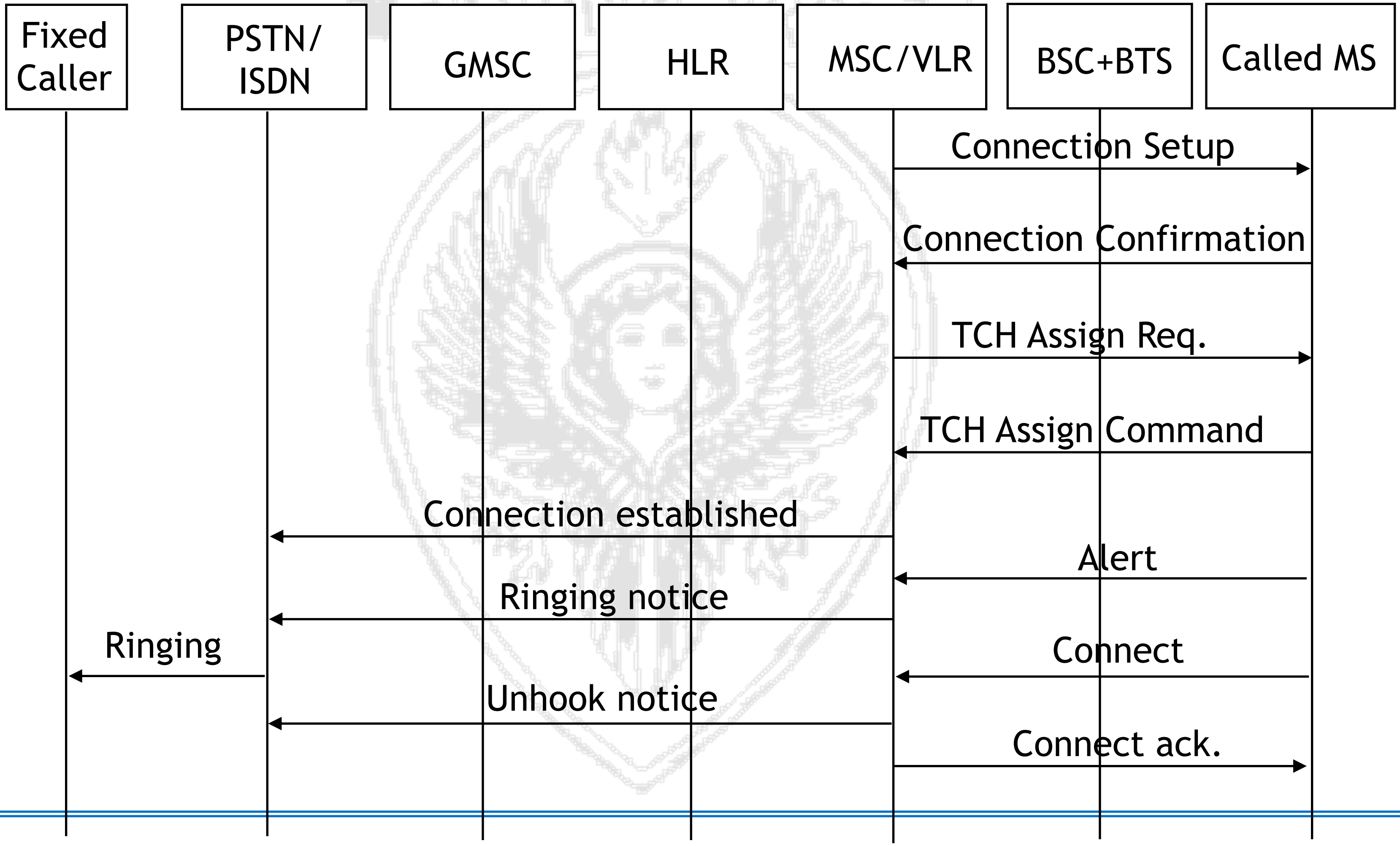
R The called user answers the call

S The connection between the two users is established

Summary of the Call Set-up Steps (1)



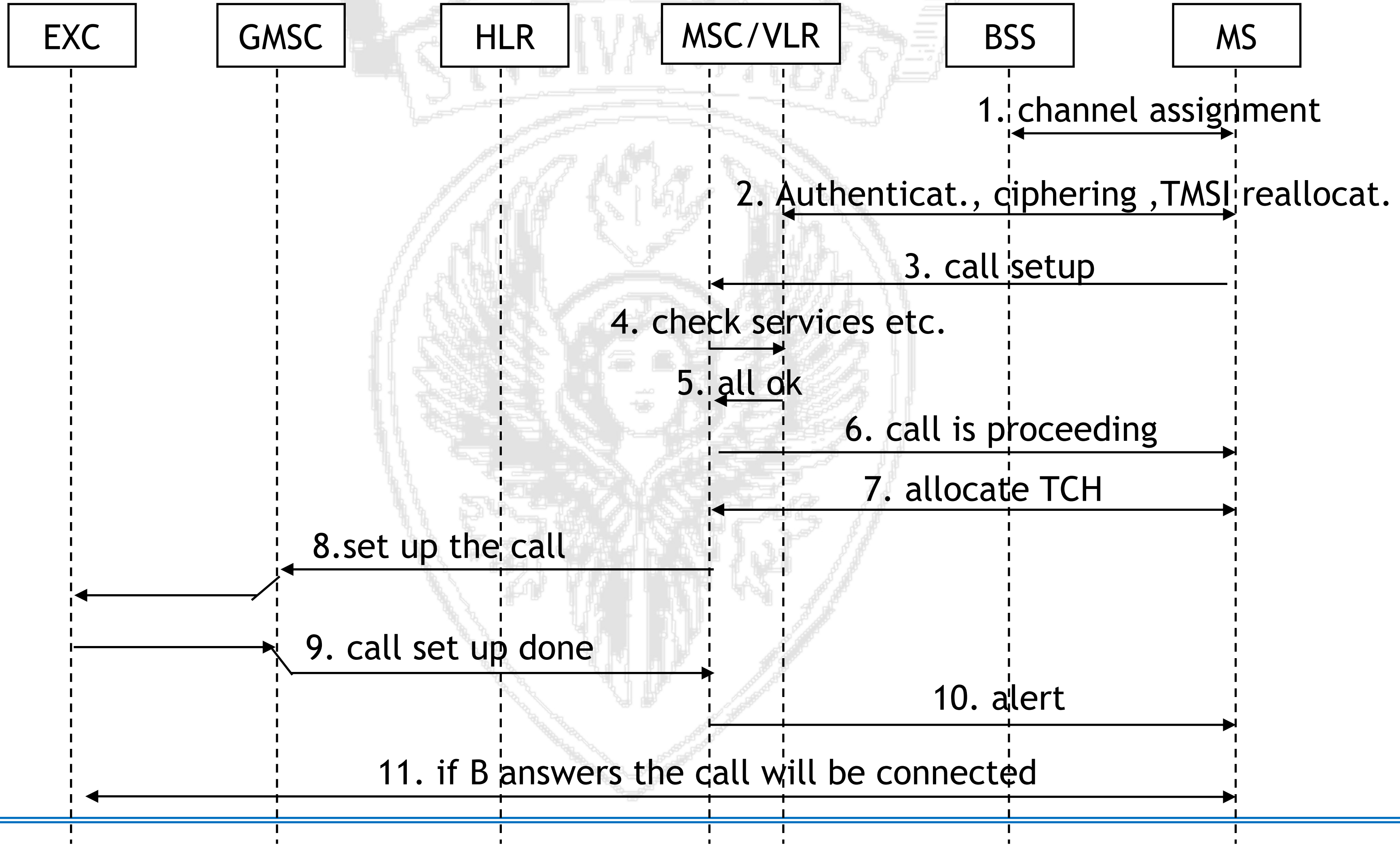
Summary of the Call Set-up Steps (2)



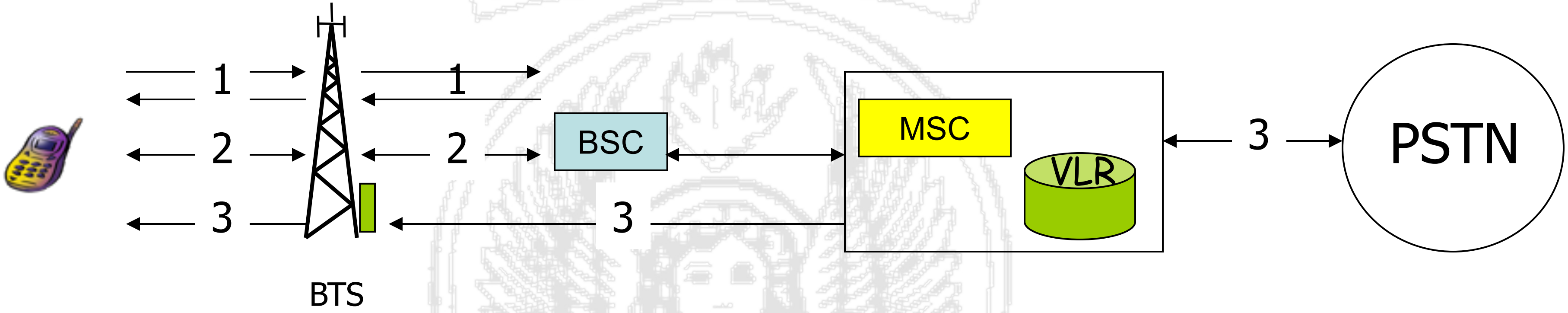
MS-originated call

- 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)

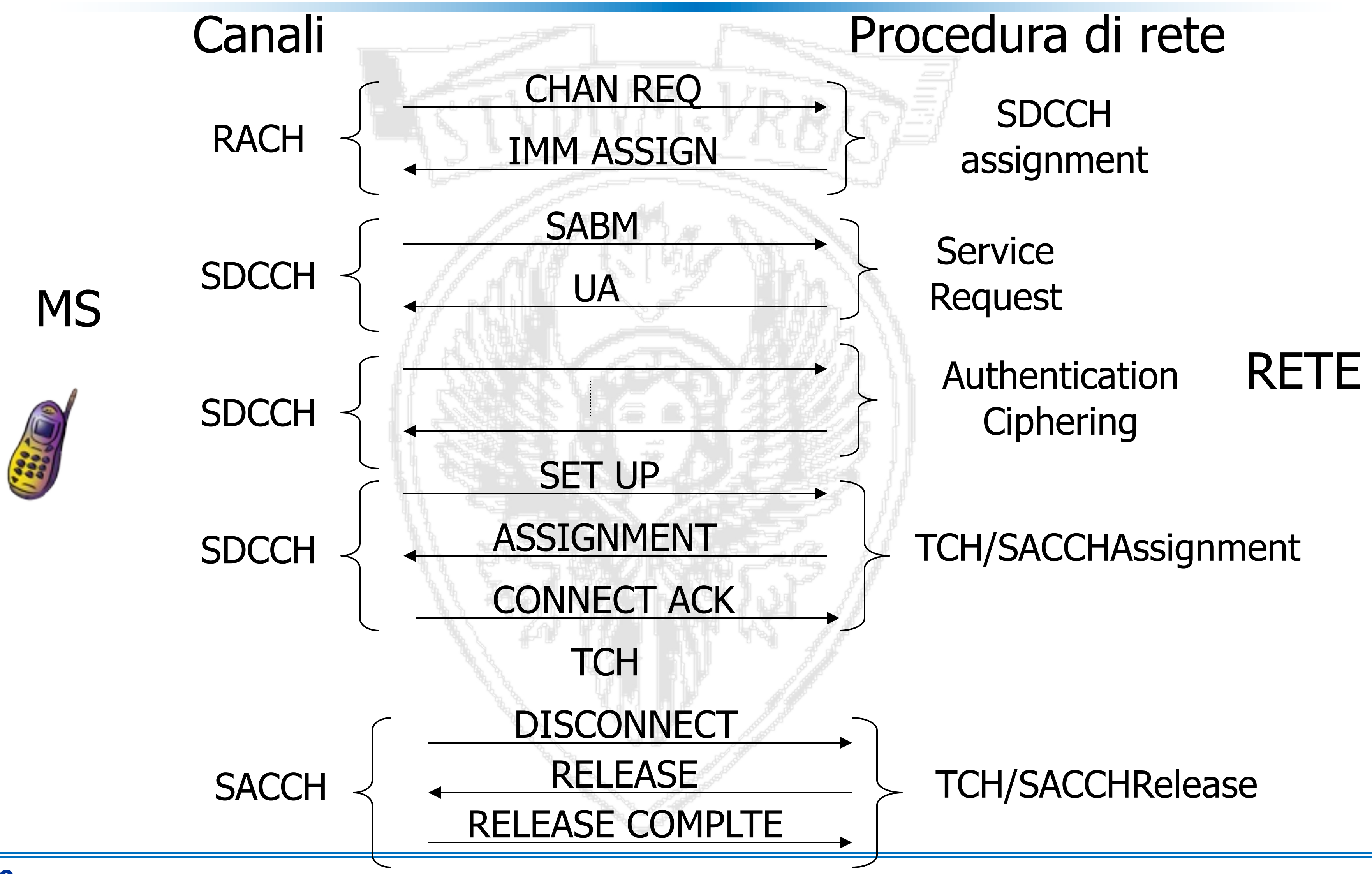


1- Access request, resource allocation for signaling

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

3 –Call routing

Mobile-originated calls (2)



Canali

Procedura di rete

MS

RETE

RACH

CHAN REQ

IMM ASSIGN

SDCCH assignment

SDCCH

SABM

UA

Service Request

SDCCH

Authentication Ciphering

SDCCH

SET UP

ASSIGNMENT

CONNECT ACK

TCH/SACCHAssignment

TCH

SACCH

DISCONNECT

RELEASE

RELEASE COMPLTE

TCH/SACCHRelease