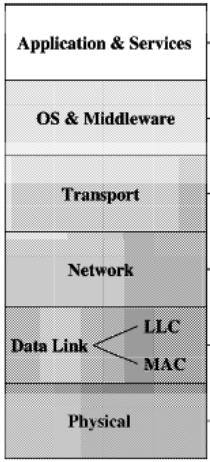
IoT, Course introduction

Internet of Things a.a. 2019/2020

Un. of Rome “La Sapienza”

Chiara Petrioli

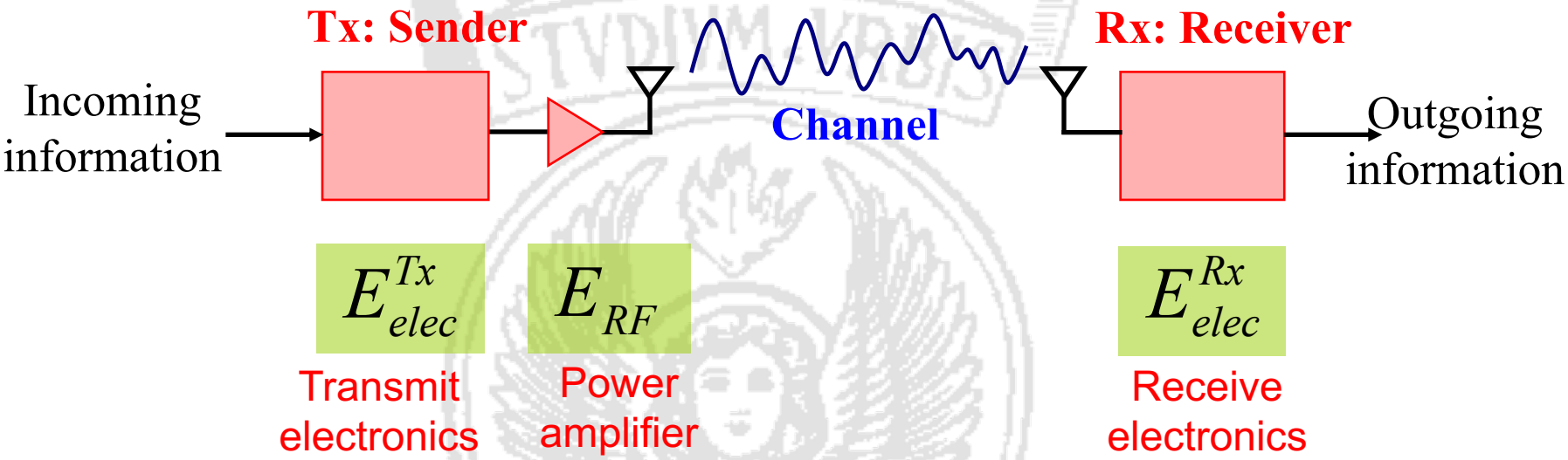
Department of Computer Science – University of Rome “Sapienza” – Italy



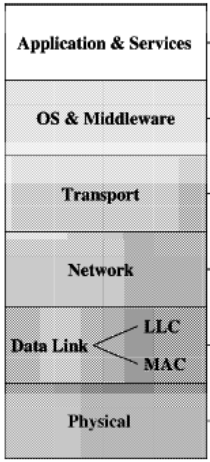
Energy-efficient techniques

- General guidelines
  - PHY:
    - ✓ Power consumption is a function of the energy needed to activate the transceiver circuitry and of the emitted power → we can significantly decrease overall energy consumption in case of long range communication by **applying power control** (Objective: minimizing transmission energy)
    - ✓ Wireless technologies can dynamically change the modulation scheme used over time. **Use of high data rate modulations reduce the time needed to transmit packets, thus the associated transmission energy consumption** (Objective: minimizing transmission energy)
    - ✓ HW-dependent optimization and selection of HW: due to design choices standard compliant transceivers can have quite different performance in terms of energy consumption, BER and PER (Bit and Packet Error Rates). **HW selection can thus significantly impact the overall system energy consumption**.
    - ✓ Promiscous mode: several protocols proposed for ad hoc network routing exploit the idea of operating the wireless interface card in promiscous mode (→received packets are passed to higher layers and processed even if not addressed to the node) in order to gather information over the wireless broadcast channel which can be used to optimize the protocol operations.
    - ✓ **Operating the wireless interface card in promiscous mode** forces the interface card to stay in idle (instead of low power modes) for long periods of time, and leads to significant energy consumption due to processing of packets. Therefore, its use typically **is a killer in terms of overall energy consumption**.

Energy in Radio: the Deeper Story….

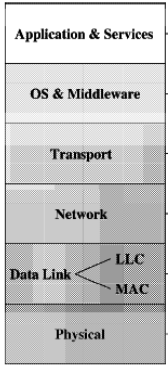


- Wireless communication subsystem consists of three components with substantially different characteristics
- Their relative importance depends on the **transmission range** of the radio



Energy-efficient techniques

- General guidelines
  - PHY:
    - ✓ Power consumption is a function of the energy needed to activate the transceiver circuitry and of the emitted power → we can significantly decrease overall energy consumption in case of long range communication by applying power control (Objective: minimizing transmission energy)
    - ✓ Wireless technologies can dynamically change the modulation scheme used over time. Use of high data rate modulations reduce the time needed to transmit packets, thus the associated transmission energy consumption (Objective: minimizing transmission energy)
    - ✓ HW-dependent optimization and selection of HW: due to design choices standard compliant transceivers can have quite different performance in terms of energy consumption, BER and PER (Bit and Packet Error Rates). HW selection can thus significantly impact the overall system energy consumption.
    - ✓ **Wireless transceiver should instead be switched to a low power 'sleep state'** (where it cannot receive or transmit packets but the energy consumption is orders of magnitude lower) whenever a packet is not addressed to the node or whenever information exchanged during a handshake make the node aware that the channel will be busy for the next future for transmitting packets not addressed to it
    - ✓ The transceiver should switch to low power mode for the whole time interval when it knows it will not be involved in communications.
      - This is also why destination address is the first field of the header
      - This is also why NAV field is part of RTS/CTS handshake in IEEE 802.11



Energy-efficient techniques

- General guidelines
  - MAC
    - ✓ **<u>Awake/asleep schedule:</u>** Nodes alternate between
      - high energy consuming states (awake:transmit/receive/idle) in which the transceiver is ON and packets can be transmitted/received AND
      - states in which the transceiver is OFF, packets cannot be received or transmitted but the energy consumption is much lower.
      - **Duty cycle=$T_{ON}/(T_{ON}+T_{OFF})$**
      - Two possible classes of protocols:
        - » Synchronous:
        - nodes exchange information to coordinate on when to wake up;
        - periodic control message exchange ensures they know when their neighbors will wake up;
        - a packet is transmitted to a neighbor when it is ON.
        - » Asynchronous:
        - Awake/asleep schedule of neighbors is unknown;
        - No control overhead is needed to keep information updated;
        - To ensure reliable communications a sequence of packets must be sent until the destination node wakes up and answers (overhead when a packet has to be sent)
        - OR nodes must follow a cross-layering approach selecting one neighbors among the awake neighbors as relay.
    - ✓ **Nodes not involved in communication should go to sleep till current information exchange completes** (Objective: avoid energy waste).

Tends to increase latency

Transceiver states

- Transceiver can be in one of the following states

tx Awake and transmitting

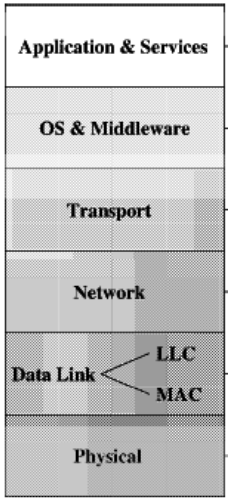
rx Awake and receiving

idle Awake, neither transmitting nor receiving

asleep Asleep: the transceiver is not operational but energy consumption is low. There can be several asleep states with different subsets of the circuitery switched OFF →different time to switch to such states, but also different energy consumption.

There is a time and energy consumption associated to the switch whish should be accounted for when designing energy efficient protocols

Energy efficient techniques



- General guidelines
  - Data Link and Routing
    - ✓ Avoid energy waste as much as possible in protocol design: minimize collisions, avoid tx in bad channel conditions, header compression, data aggregation to reduce in network data transmission
    - ✓ Minimize overall energy consumption when tx/rx on a route, also accounting for retransmissions (ETX metric); avoid passing through critical nodes (with few energy resources); Energy aware routing solutions which account for residual energy (and expected future availability of energy in case harvesting is an option) when selecting the best next hop relay.
    - ✓ All what listed as ultimately low power design is applied when performing HW design, selecting solutions at each layer of the protocol stack.

Energy efficient techniques

- In the last few years there has been a change of devices used to access the Internet
  - From PC to smartphone
  - Novel Phy layer and more advanced transceiver features
  - How has the energy model been affected by changes in the device technology?
  - Can we still make the same assumptions or are there additional components to account for?

  In the following the outcomes of:

  N. Balasubramanian, A. Balasubramanian, A. Venkataramani “Energy consumption in mobile phones: A Measurement Study and Implications for Network Applications”, ACM IMC 2009. Observation: Workload impacts energy consumption of typical devices (cellular-GSM/3G; WiFi)

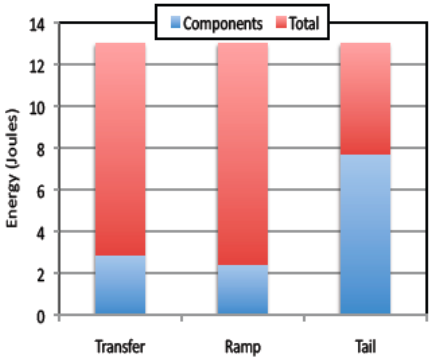
  A. Garcia Saavedra, P. Serrano, A. Banchs, G. Bianchi “Energy Consumption Anatomy of 802.11 Devices and Its Implication on Modeling and Design” in Proceedings of Co-NEXT 2012 (on WiFi)

Device and standard-dependent optimizations

- Implementations and choices made for implementing standards make the difference:
  - N. Balasubramanian, A. Balasubramanian, A. Venkataramani "Energy consumption in mobile phones: A Measurement Study and Implications for Network Applications", ACM IMC 2009. Observation: Workload impacts energy consumption of typical devices (cellular-GSM/3G; WiFi)
    - ✓ In 3G, a large fraction (nearly 60%) of the energy, referred to as the *tail energy,* is wasted in high-power states after the completion of a typical transfer.
      - Switching back from an active state is handled by means of inactivity timers often set to a few seconds.
    - ✓ Tail and ramp energies (more limited) are constants that amortize over larger transfer sizes or frequent successive transfers.

Device and standard-dependent optimizations

- Implementations and choices made for implementing standards make the difference:
  - N. Balasubramanian, A. Balasubramanian, A. Venkataramani "Energy consumption in mobile phones: A Measurement Study and Implications for Network Applications", ACM IMC 2009. Observation: Workload impacts energy consumption of typical devices (cellular-GSM/3G; WiFi)
    - ✓ In 3G, a large fraction (nearly 60%) of the energy, referred to as the *tail energy,* is wasted in high-power states after the completion of a typical transfer.



Typical 3G transfer

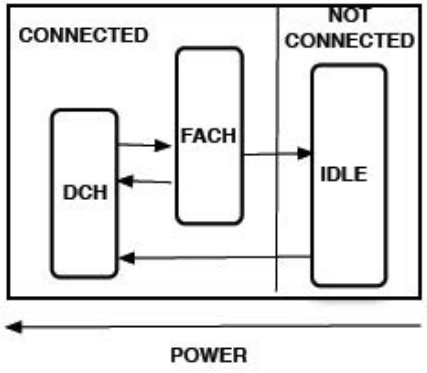
HTTP request issued to a remote server

50KB download

Nokia N95

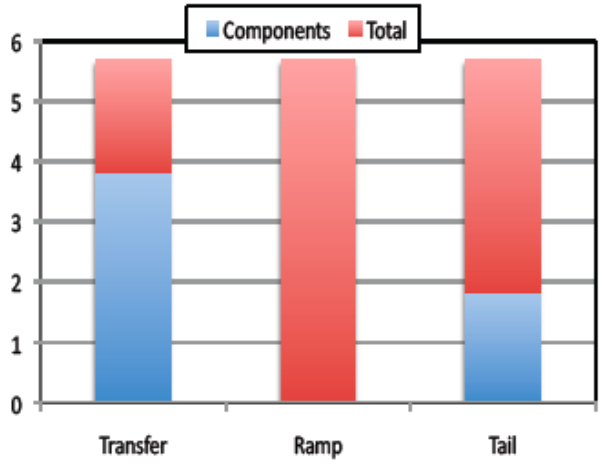
Device and standard-dependent optimizations

- Implementations and choices made for implementing standards



  - N. Balas … nkataramani "Energy … rement Study and Imp… IMC 2009. Observa… ion of typical devices
    - ✓ In 3G, a large fraction (nearly 60%) of the energy, referred to as the *tail energy,* is wasted in high-power states after the completion of a typical transfer.
      - Switching back from an active state is handled by means of inactivity timers often set to a few seconds.
    - ✓ Tail and ramp energies (more limited) are constants that amortize over larger transfer sizes or frequent successive transfers.

Device and standard-dependent optimizations

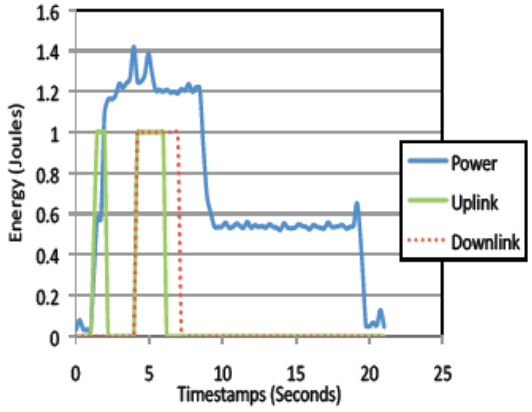


GSM shows a different trend

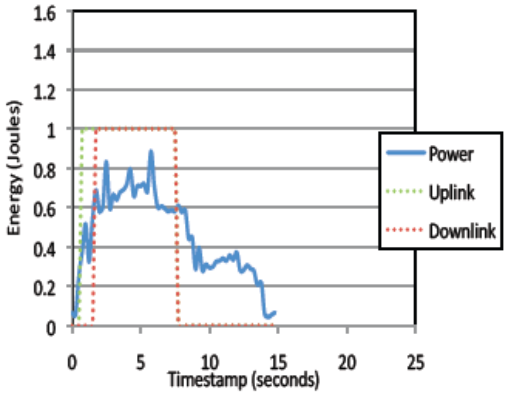
Lower power

More significant transmission energy

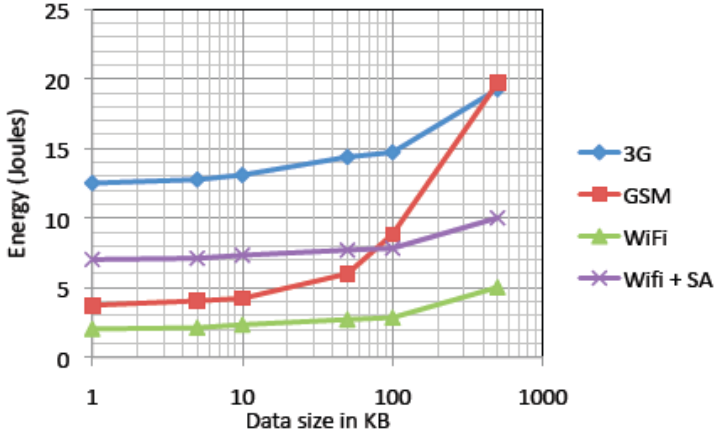
Less significant (even if present) tail energy effect



(a) 3G: Power Profile - 50K



(b) GSM: Power Profile - 50K



Solution:TailEnder

- Three ideas:
  - Combine use of 3G and WiFi (with prediction of WiFi availability)
  - For delay tolerant applications (news, emails) delay transfer if tolerable delay so to transfer batches
  - For web surfing applications design of energy-optimized prefechting techniques

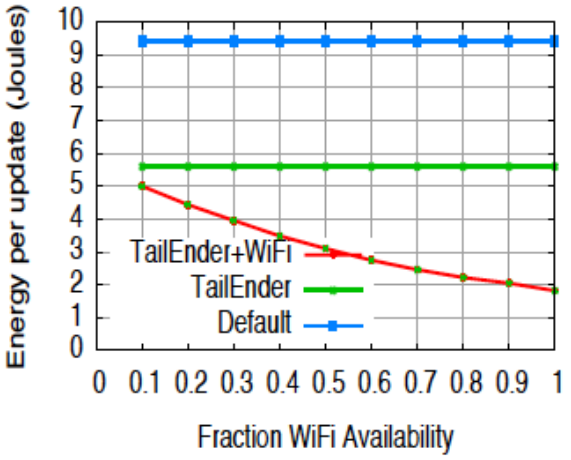


Figure 22: News feed. Average energy improvement when switching between

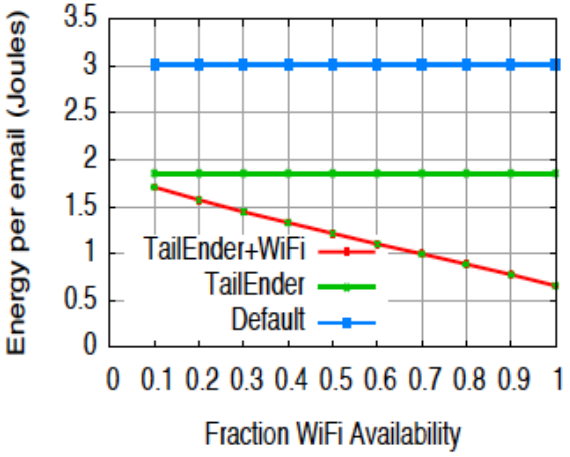


Figure 23: E-mail. Average energy improvement when switching between

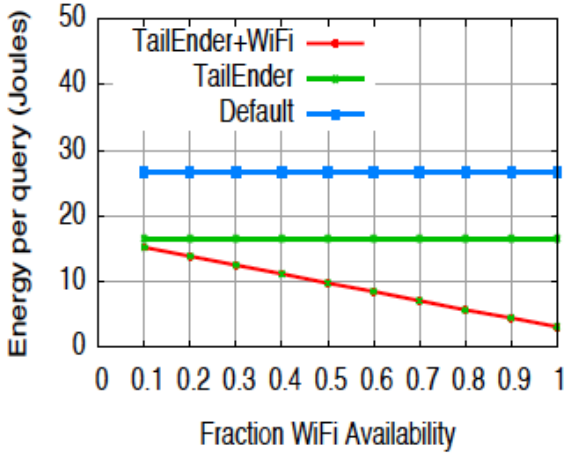


Figure 24: Web Search. Average energy improvement when switching between

Energy Consumption Anatomy- IEEE 802.11

- Experiments and measurements on multiple commercial devices
  - Soekris net 4826-48 + Atheros 802.11a/b/g Mini-PCI card, configured to use the 802.11a PHY
  - Alix2d2 + Broadcom BCM4319 802.11b/g Mini-PCI card
  - Linksys WRT54GL + Broadcom BCM4320 802.11b/g Mini-PCI card
- Checking no interference (sniffers)
- Measuring energy consumption with high accuracy power meters
- Controlled traffic generation (mgen generates UDP packets)

A. Garcia Saavedra, P. Serrano, A. Banchs, G. Bianchi "Energy Consumption Anatomy of 802.11 Devices and Its Implication on Modeling and Design" in Proceedings of Co-NEXT 2012

Energy Consumption Anatomy- IEEE 802.11

- Baseline energy consumption has been measured

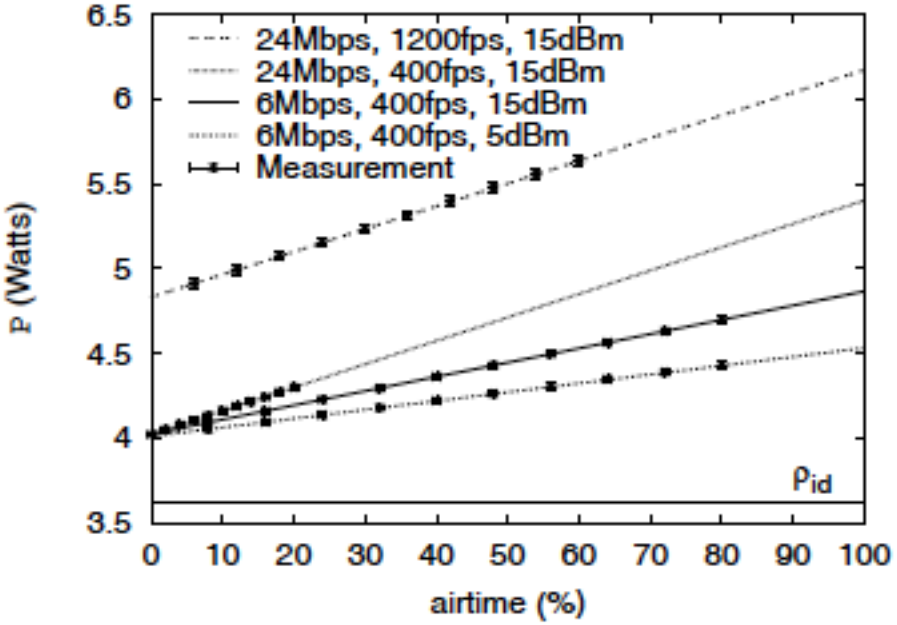
Table 2: Soekris Baseline consumption profile

Config.	Description	Cons. (W)
w/o card	no NIC connected	$2.29 \pm 2.2\%$
WiFi off	NIC connected driver not loaded	$2.58 \pm 2.0\%$ (+0.29)
Idle (ρ_{id})	NIC activated+associated to AP no RX/TX besides beacons	$3.56 \pm 1.7\%$ (+0.98)

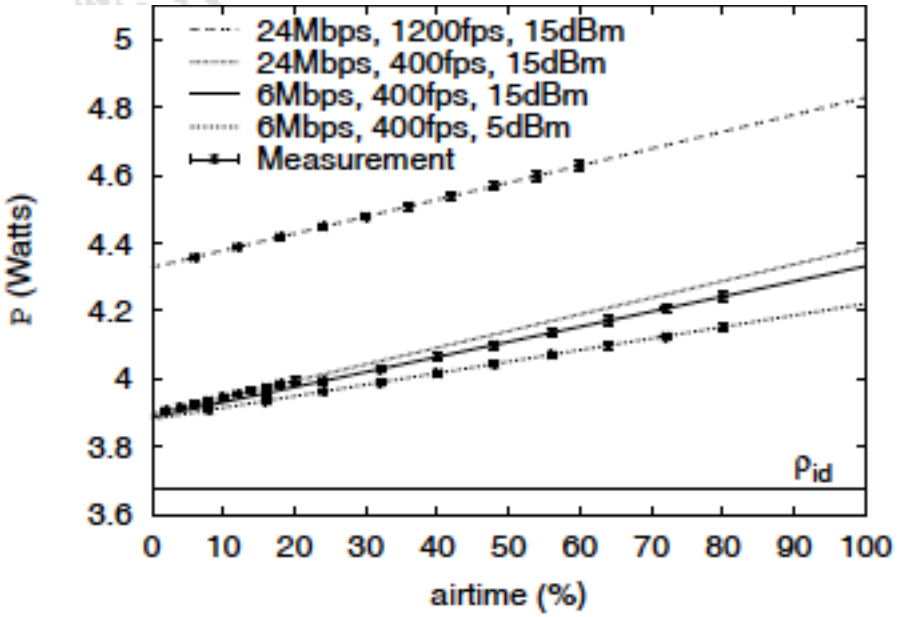
- Eenergy consumption of transmitting one packect without ACKs has been studied
- Impact on energy consumption of varying transmission power, packet length, type of modulation has been quantitatively studied

Energy Consumption IEEE 802.11

- Experimental results: Total power consumed by (unacknowledged) transmissions vs. airtime percentage



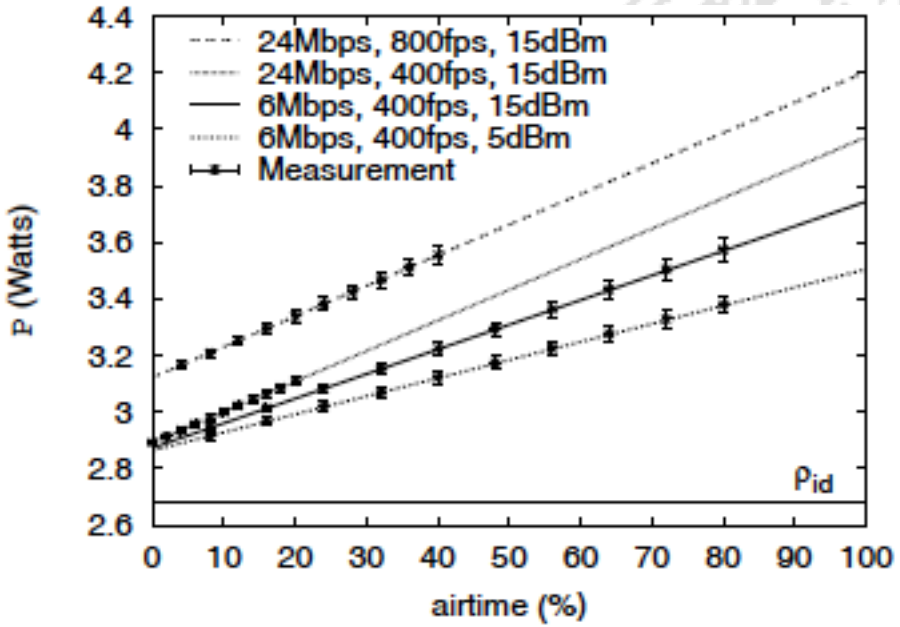
(a) Soekris



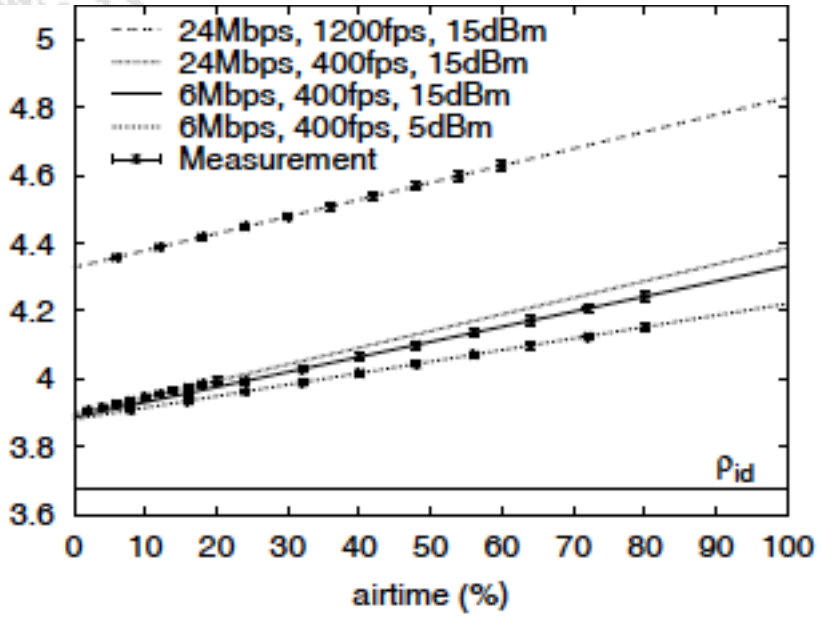
(b) Alix

Energy Consumption IEEE 802.11

- Experimental results: Total power consumed by (unacknowledged) transmissions vs. airyime percentage



(c) Linksys



(b) Alix

Energy Consumption IEEE 802.11

- Experimental results: Relationship between cross factor and traffic intensity

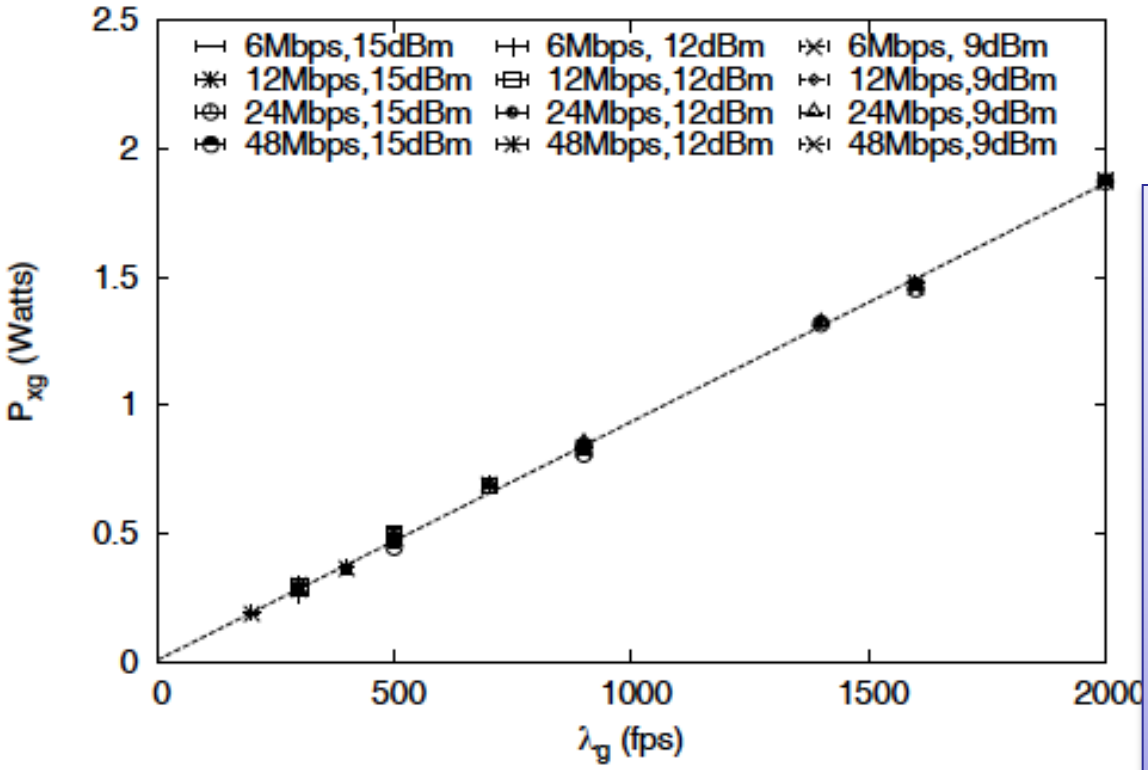


Figure 2: Relation between $P_{xg}(\lambda_g)$ and λ_g.

New energy model

$$\mathbf{P} = \rho_{id} + P_{tx} + P_{xg}(\lambda_g)$$

ρ_{id} is the platform specific baseline power consumption

P_{tx} is the power consumption Associated to transmission (depends on airtime, tx power Modulation)

$P_{xg}(\lambda g)$ is the new cross factor

Cross factor analysis

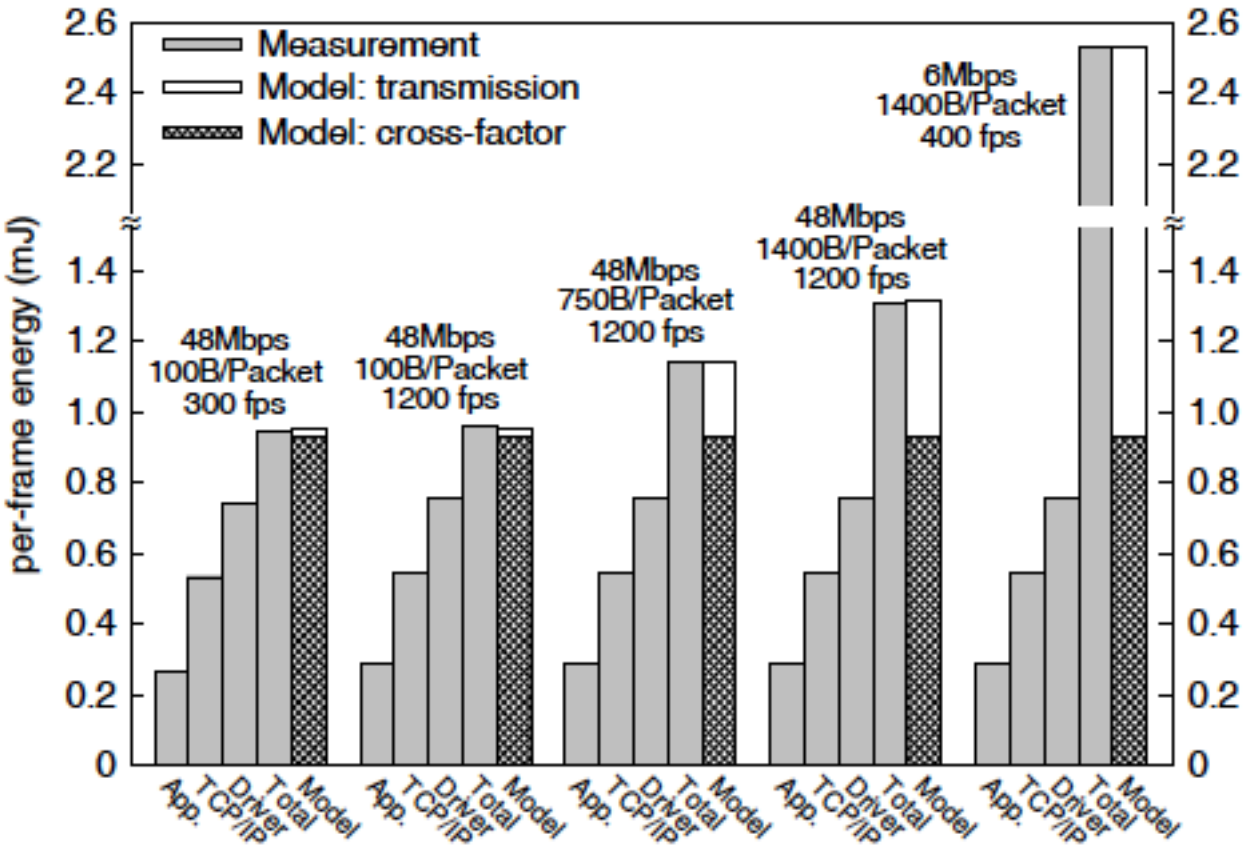


Figure 4: Per-frame energy cost in transmission.

New approaches are proposed for

- Packet relay selection
- Data compression
- Data transmission (back to back)
- Stack implementation

Introduction to cellular systems

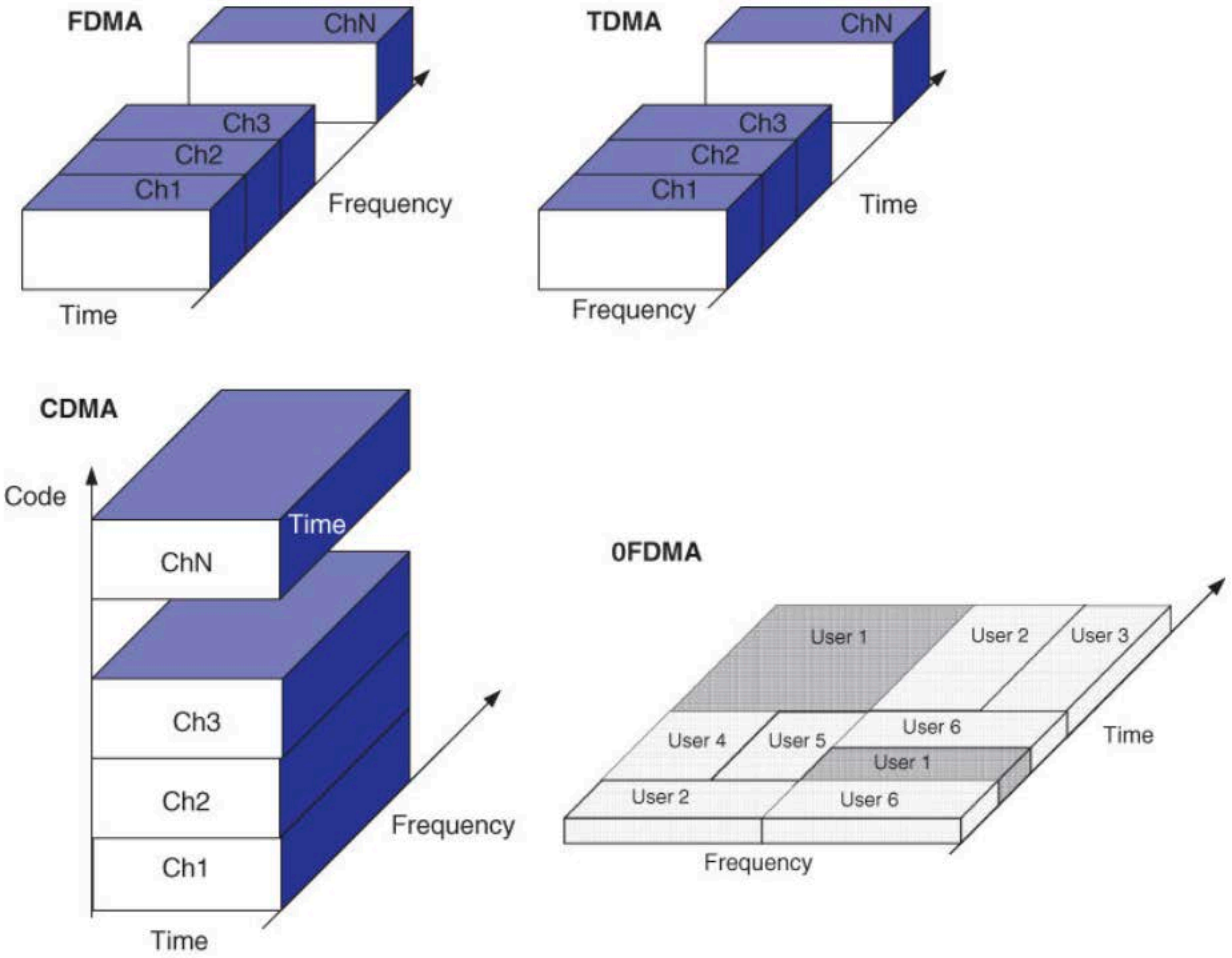
IoT, a.a. 2019/2020

Un. of Rome "La Sapienza"

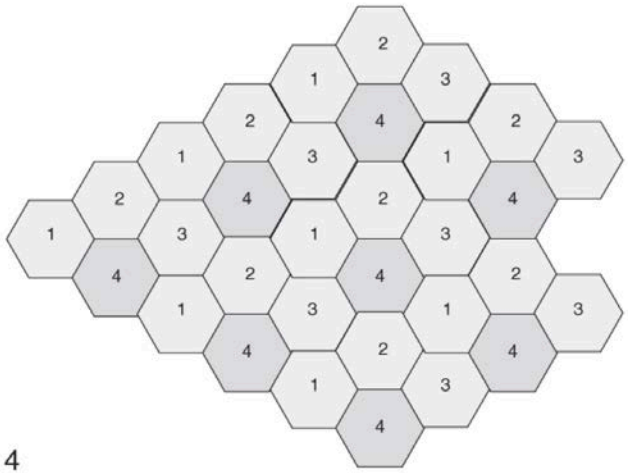
Chiara Petrioli[†]

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

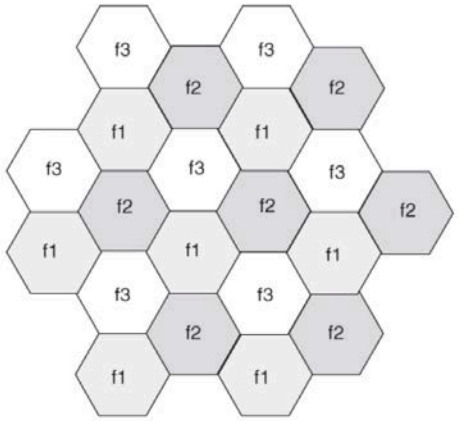
How physical resources are shared among users



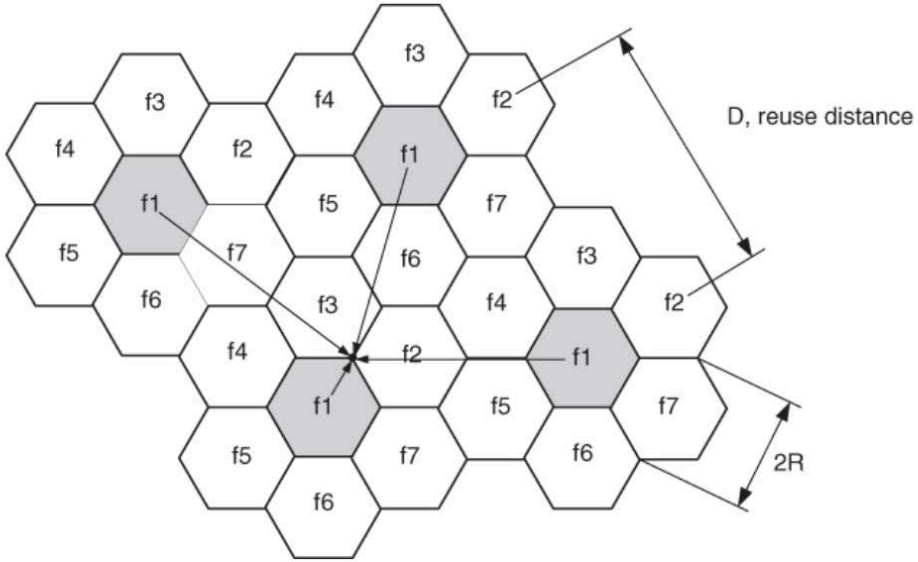
How frequencies are reused



K = 4



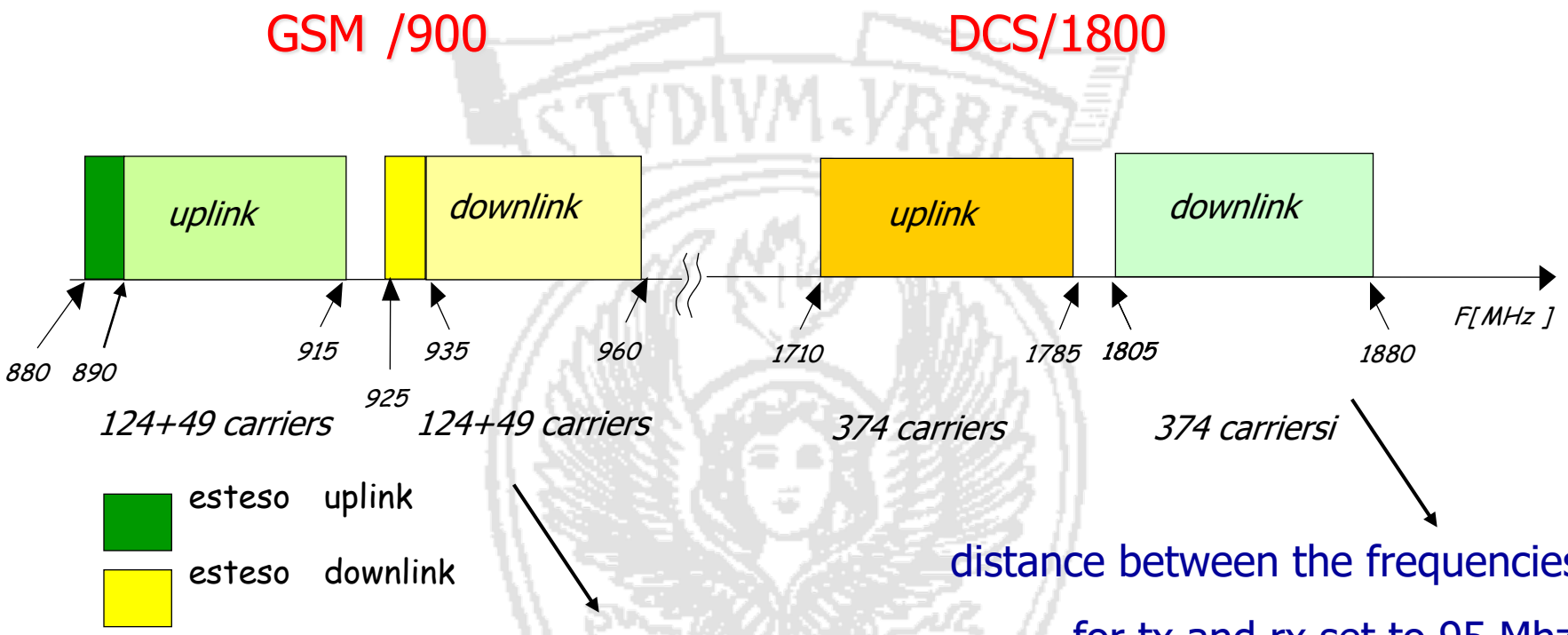
K = 3



GSM General features

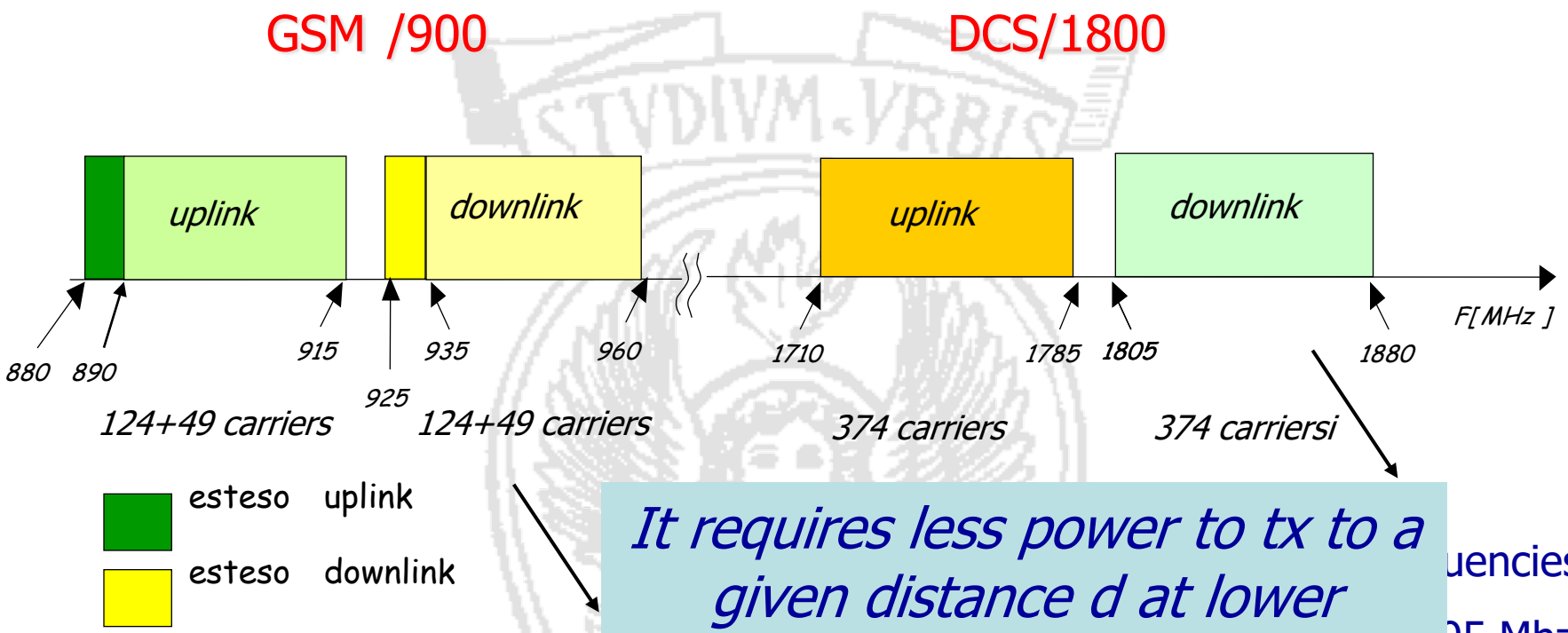
- 2ª Generation (2G) cellular system
- Carrier bandwidth=200KHz
- Multicarrier TDMA multiple access (8 slots per carrier, thus 8 channels per carrier)→ TDMA/FDMA
- Full Duplex: Frequency Division Duplex (FDD)
- Modulation: GMSK; Spectrum efficiency: 1,35bps/Hz; Gross bit rate per carrier: 270,822 kbit/s
- 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

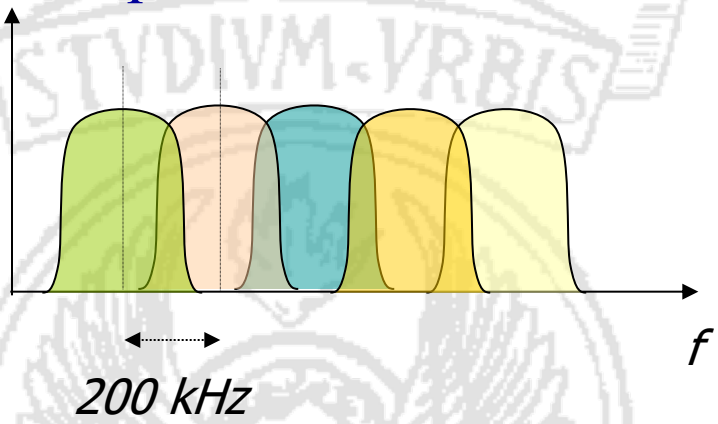
distance between the

for tx and rx s

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

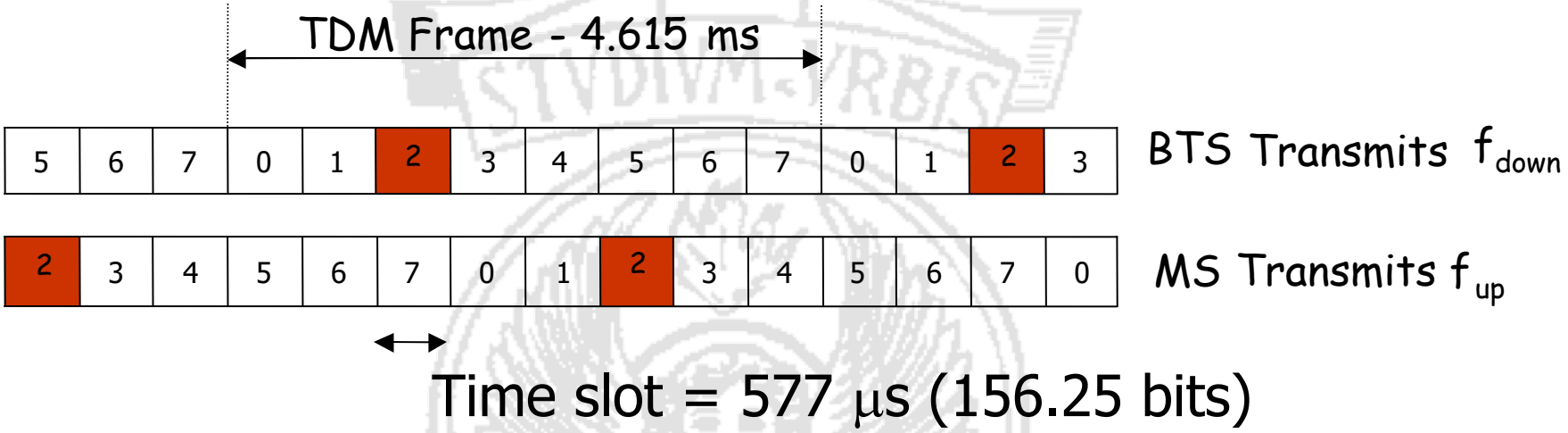
Carriers and channels

- 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

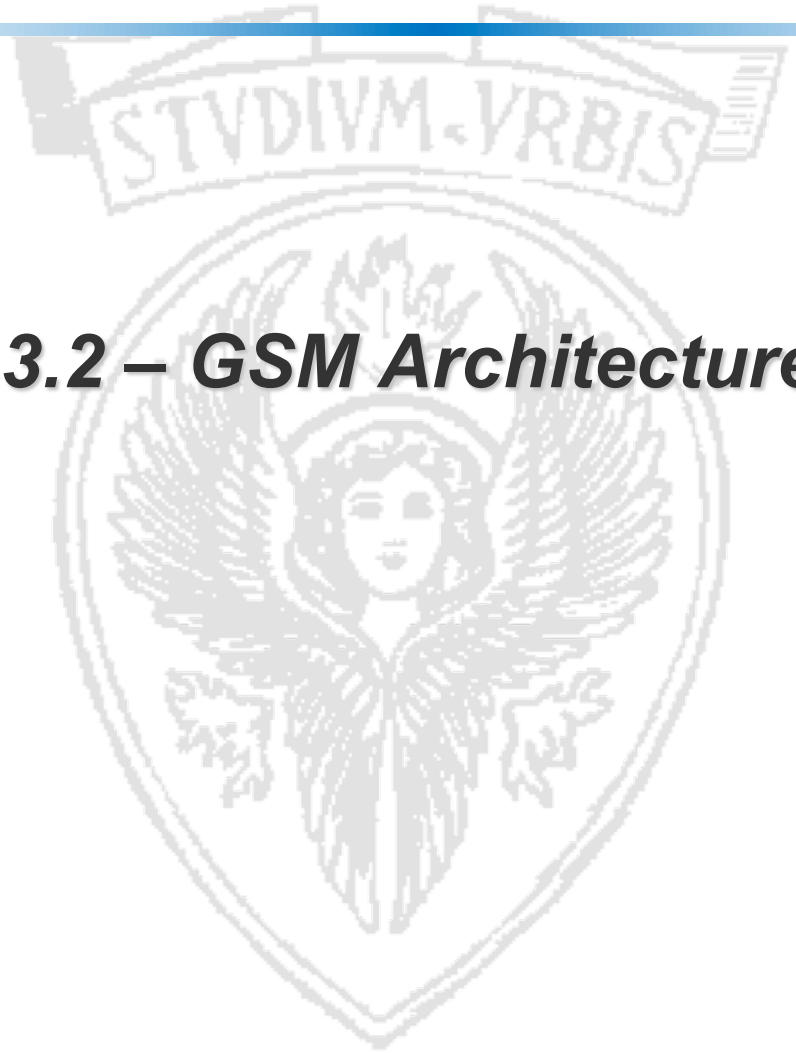
TDMA Frame



- 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

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)

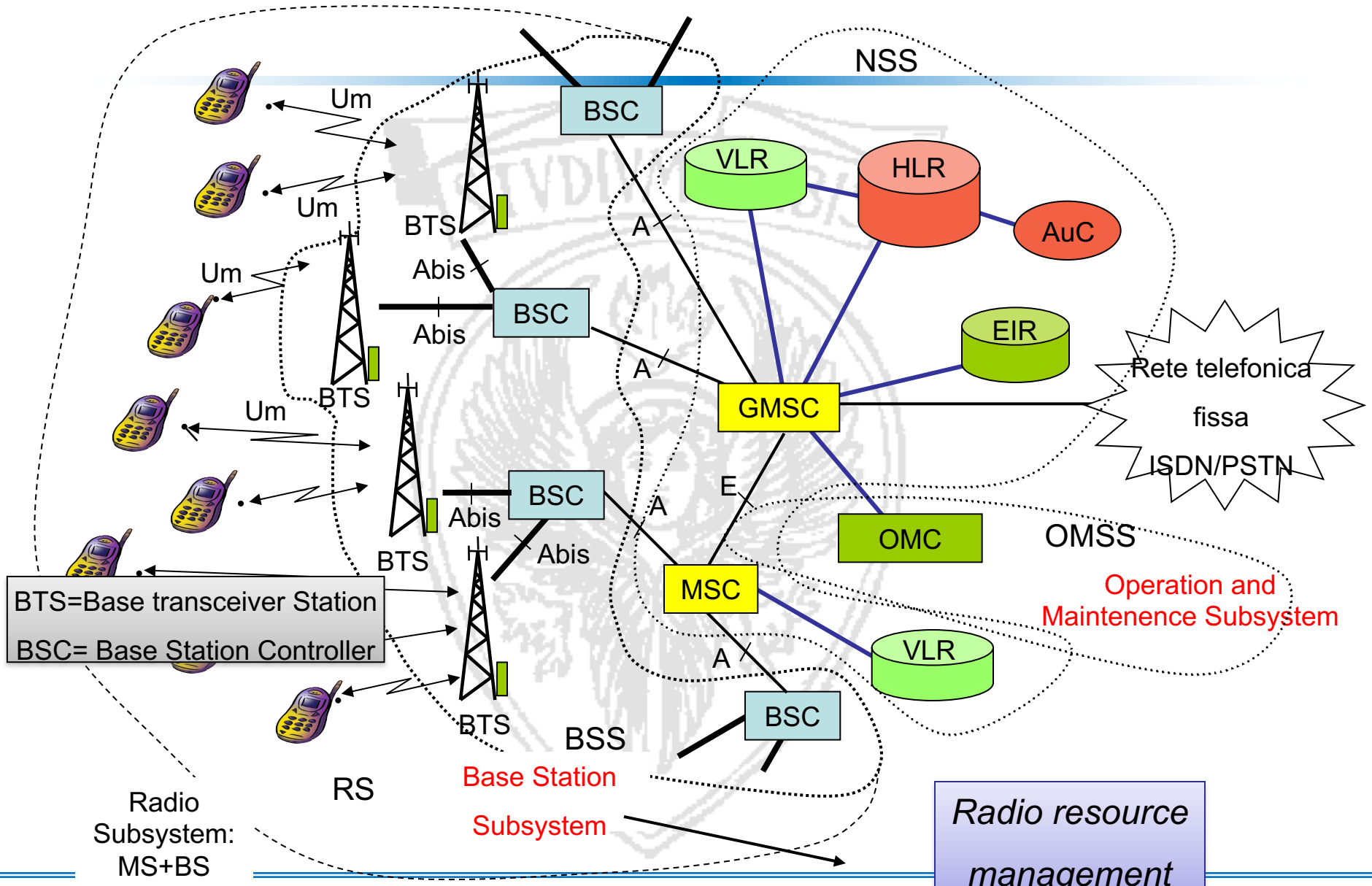
Core Network (CN)

Ext. network

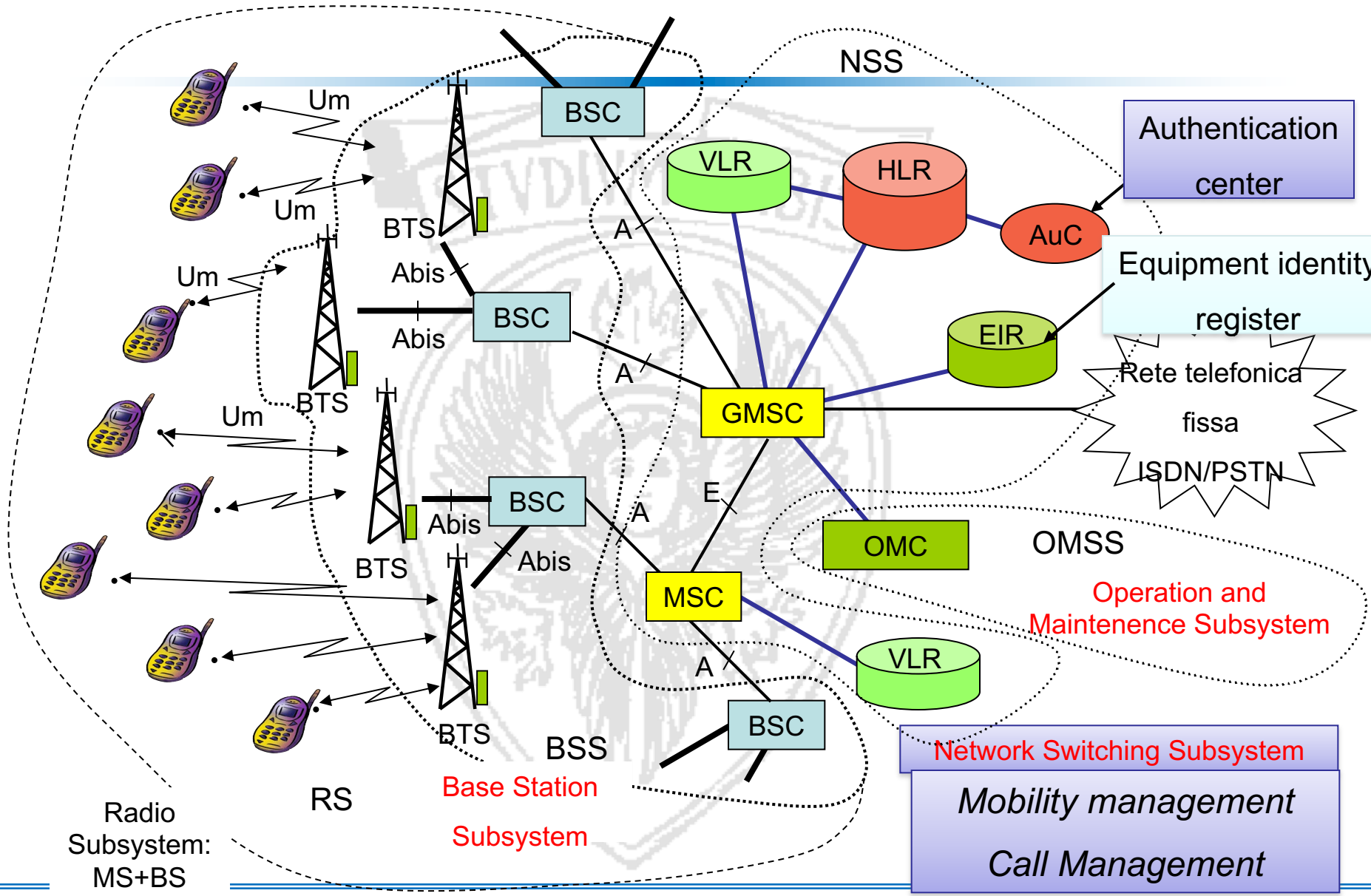
High level network architecture (2/2)

- 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"

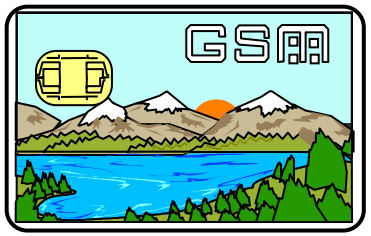
(Mobile Station - MS)

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	.

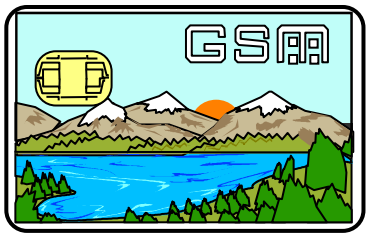
- Features
  - MS multi-band: can operate on different frequency bands (900, 1800, 1900, …)
  - MS multi-slot: can operate over different channels, in different slots (only for GPRS)
- MS is composed of an ME (Mobile Equipment) and a SIM (Subscriber Identity Module)
  - ME is the terminal through which 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)



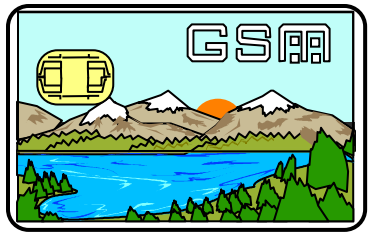
Information stored in the SIM



- *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



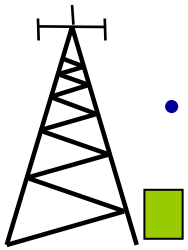
A Mobile Equipment without SIM is enabled to make only emergency calls

A Mobile Equipmentis 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)

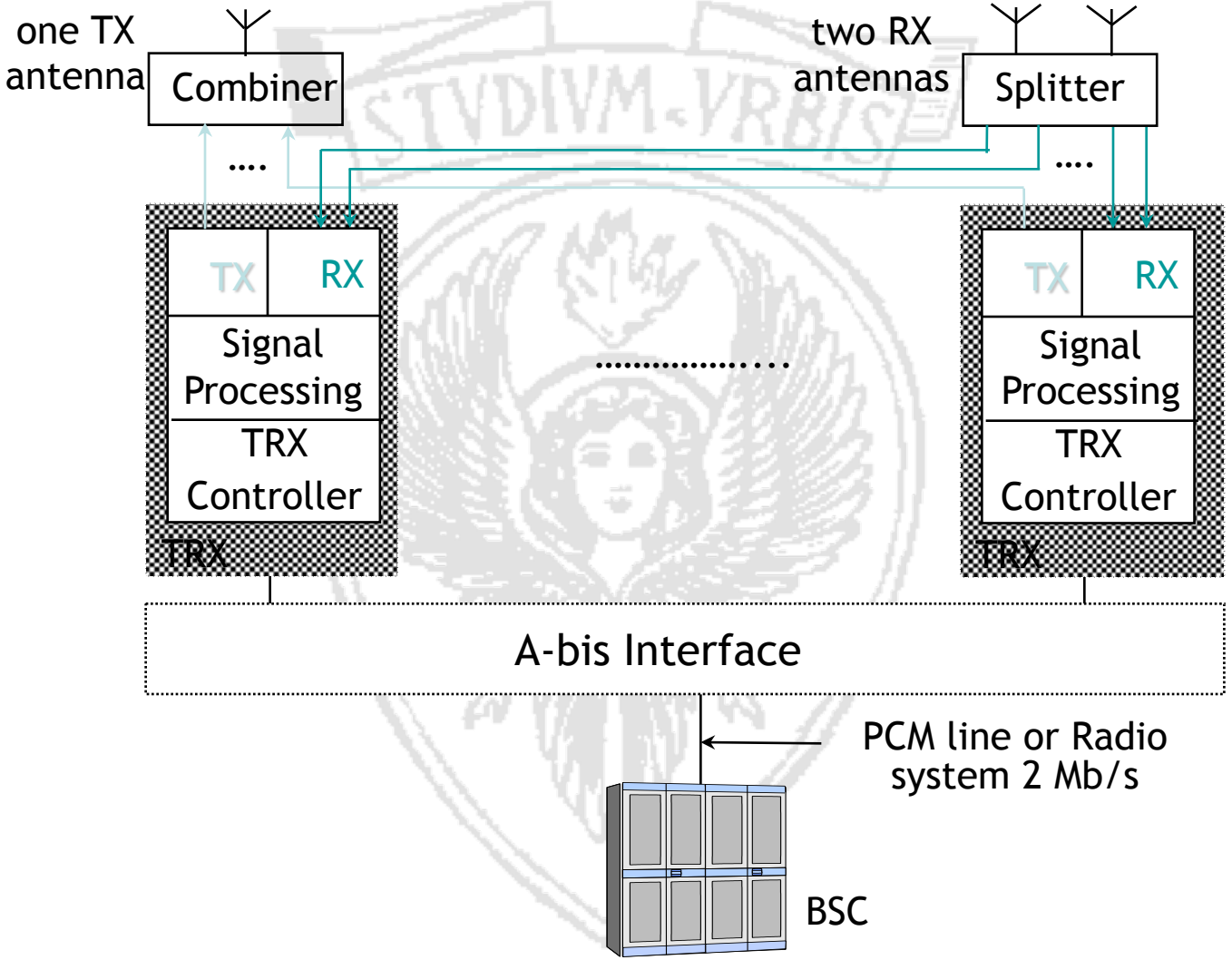


- The BTS is the element that has the task of implementing the low-level protocols of the radio interface
- And then to transmit and receive signals from MS implementing the functionality of modulation, coding and multiplexing of physical channels. It performs frequency hopping (if enabled) and encryption.
- 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



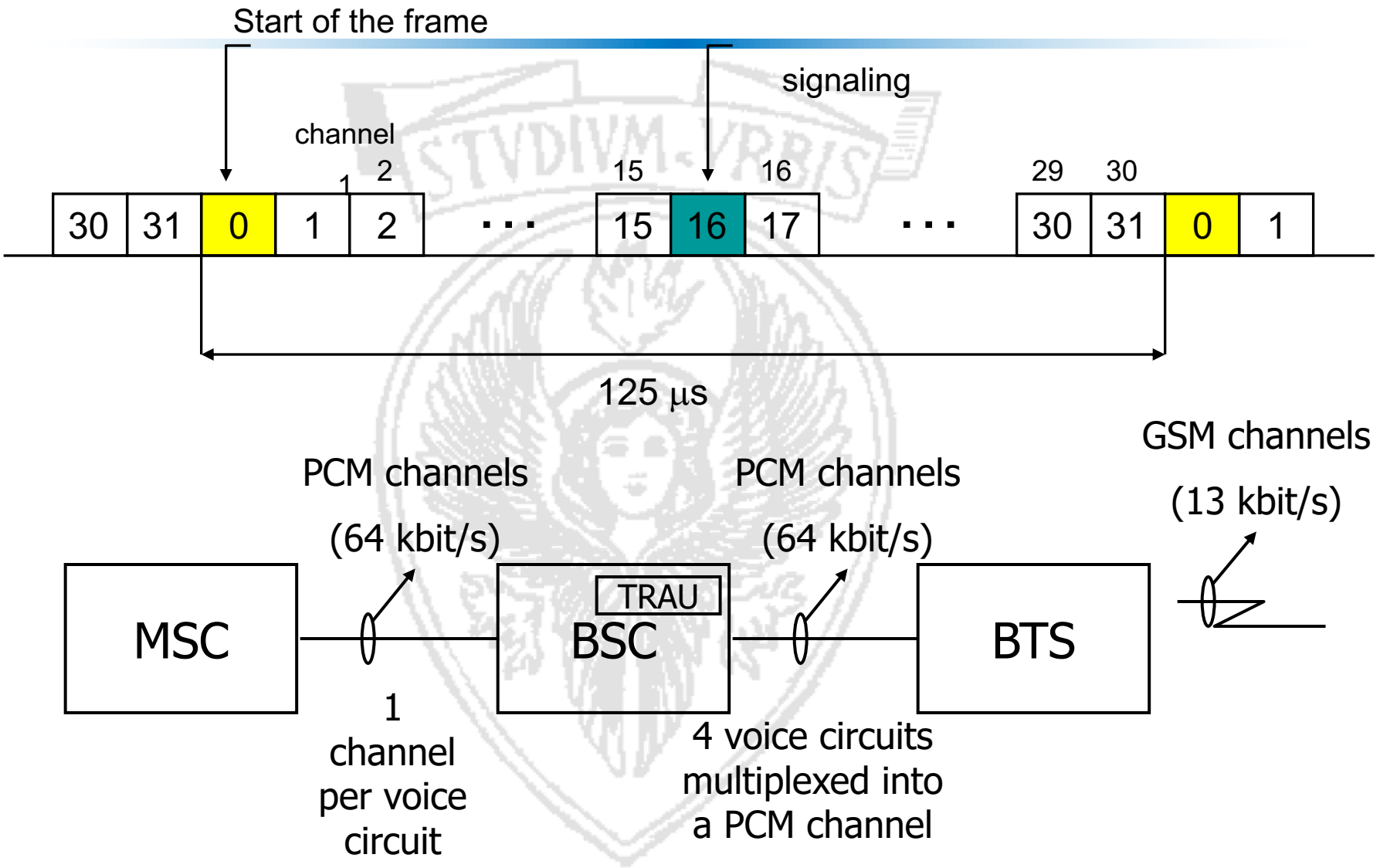
BCF

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 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.

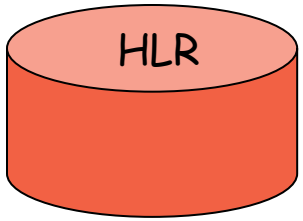
Mobile Switching Centre (MSC)

- 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)

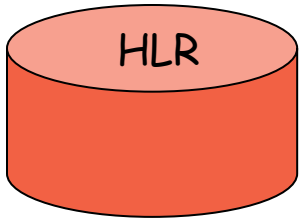
- The MSC provides the following functionalities
  - CM (Connection Management)
    - ✓originating call, terminating call, gateway
  - MM (Mobility Management)
    - ✓location updating, periodic registration, authentication, ecc.
- The MSC is the core entity in charge of signaling; It implements protocols 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)



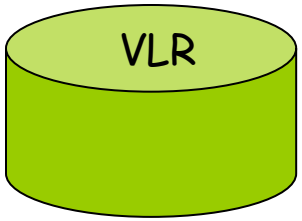
- It is a permanent database uniquely associated to a GMSC
- It stores information about all MS whose default location is at the considered GMSC
- HLR stores permanent information such as the IMSI (International Mobile Subscriber Identity), the identifier of the SIM card and its associated authentication 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

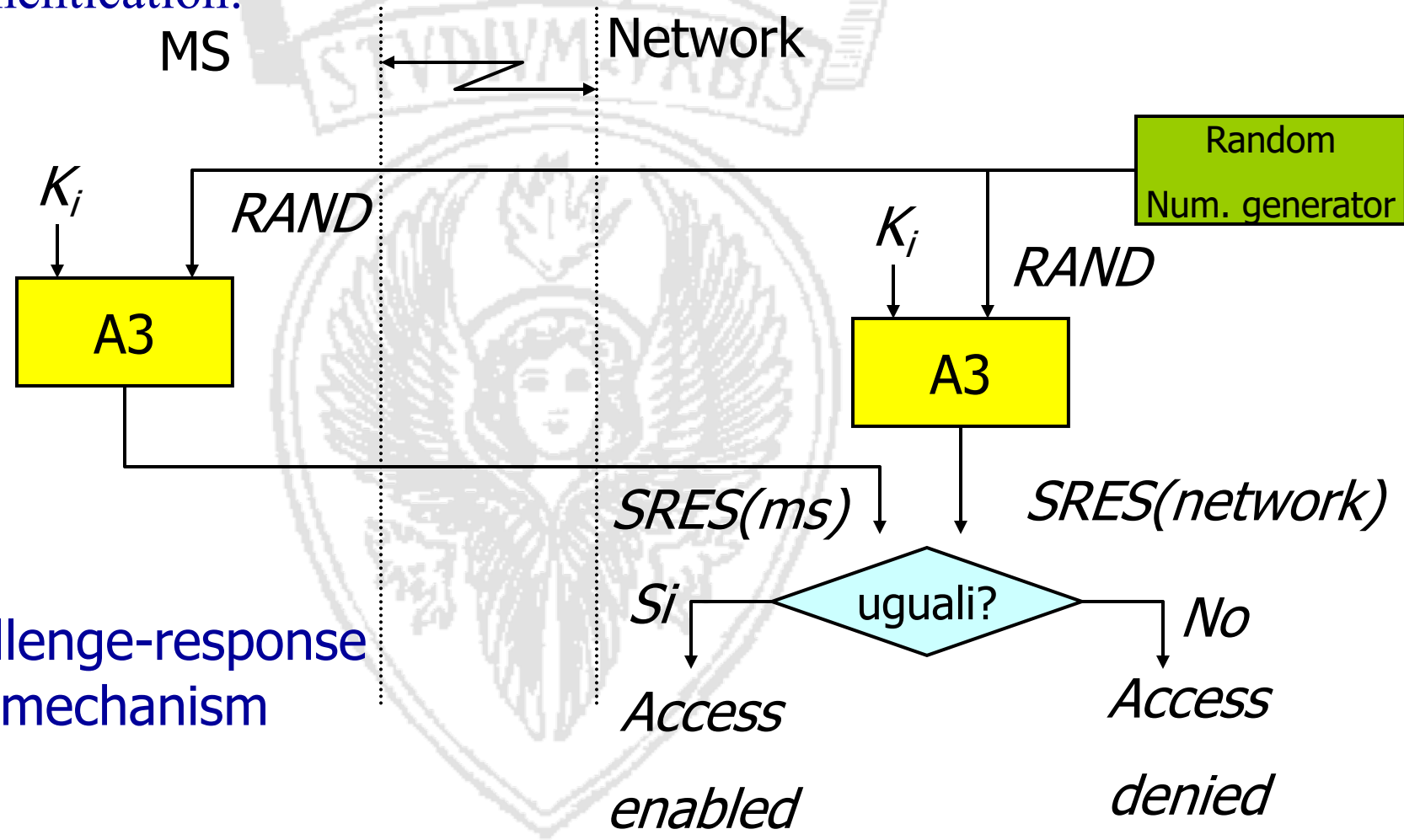
Triplets

(*RAND, SRES,* K_c)

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

Security procedures

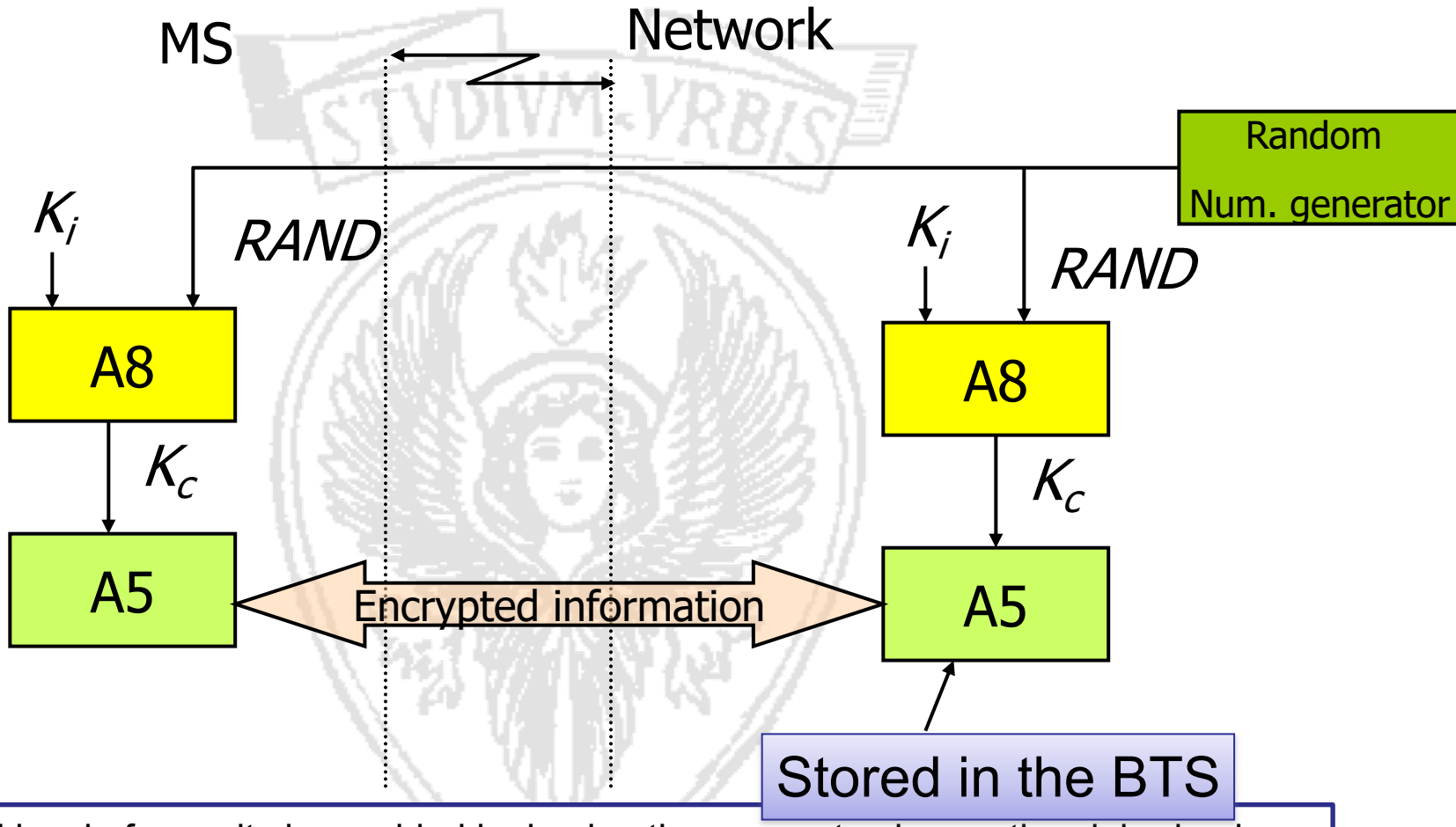
- Authentication:



Challenge-response mechanism

Security procedures

- Encryption

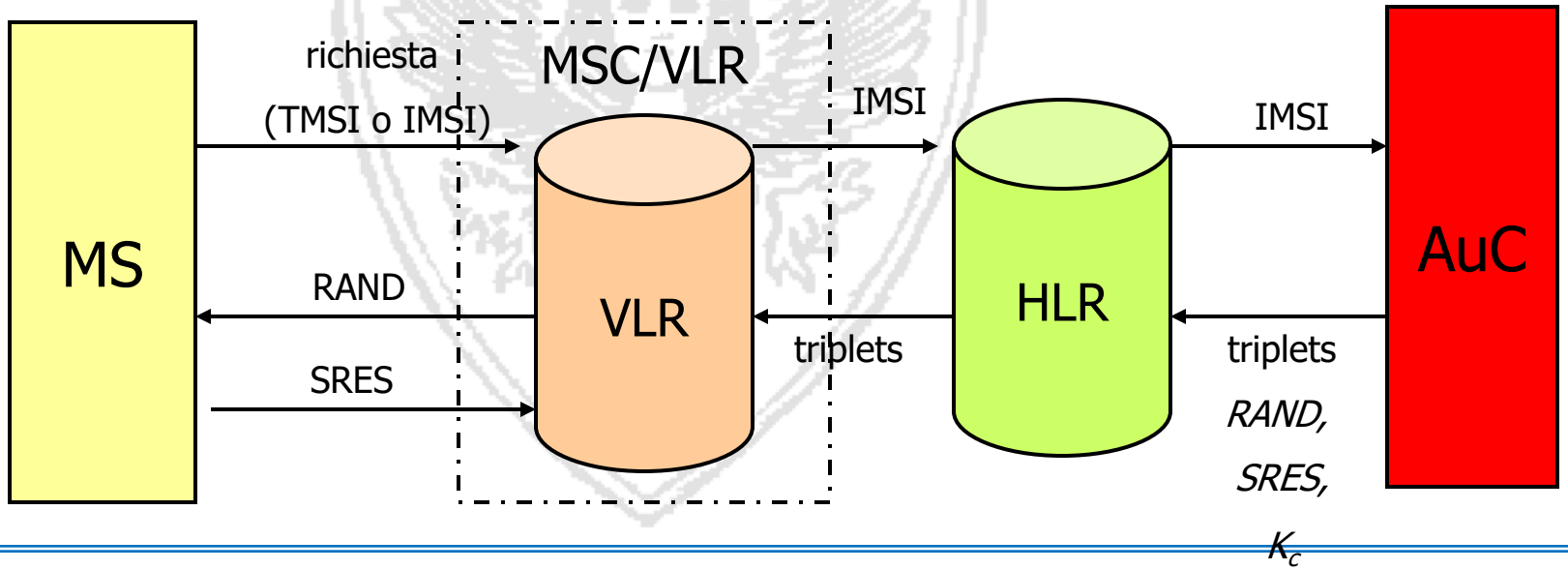


An additional level of security is provided by having the means to change the ciphering key, making the system more resistant to eavesdropping. The ciphering key may be changed at regular intervals as required by network design and security considerations.

Security procedure: network elements involved

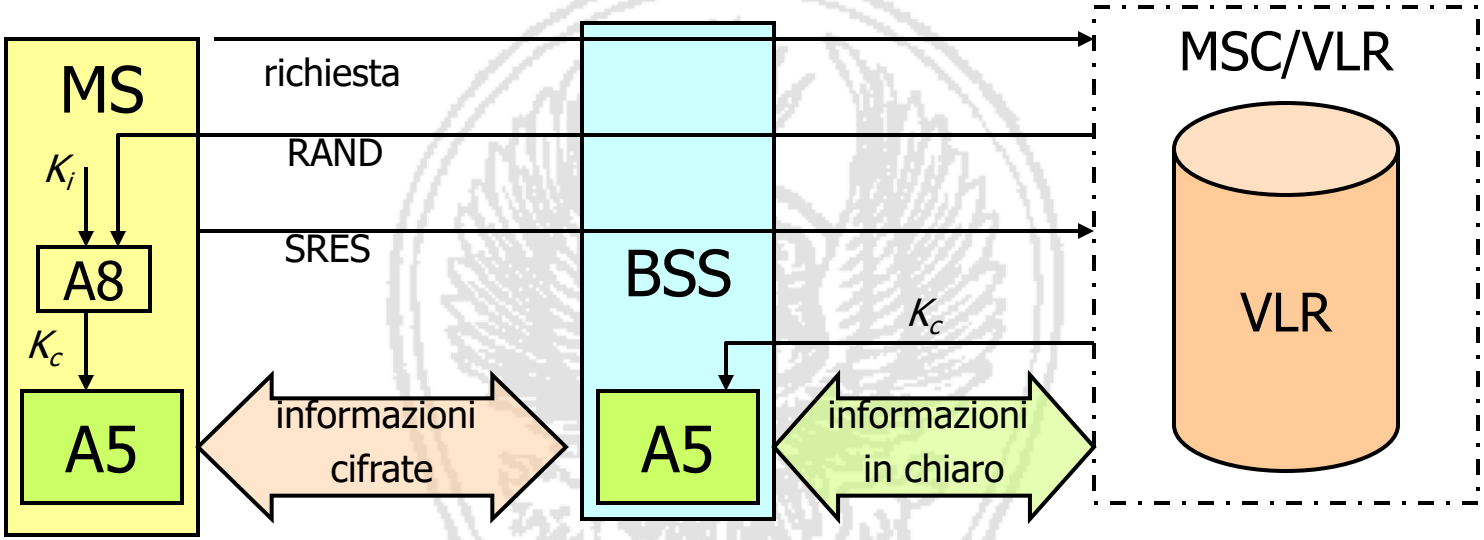
- Autentication Centre (AuC)
  - stores the secret keys K_i for each user
  - generates random numbers and calculates SRES and the encryption key K_c
  - Provides the triplets to the other network elements

AuC



Security procedure: network elements involved

- BSS/NSS elements involved in data encryption



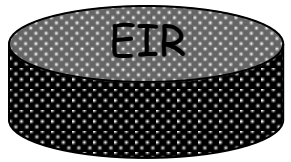
Security procedures: TMSI allocation

- 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.

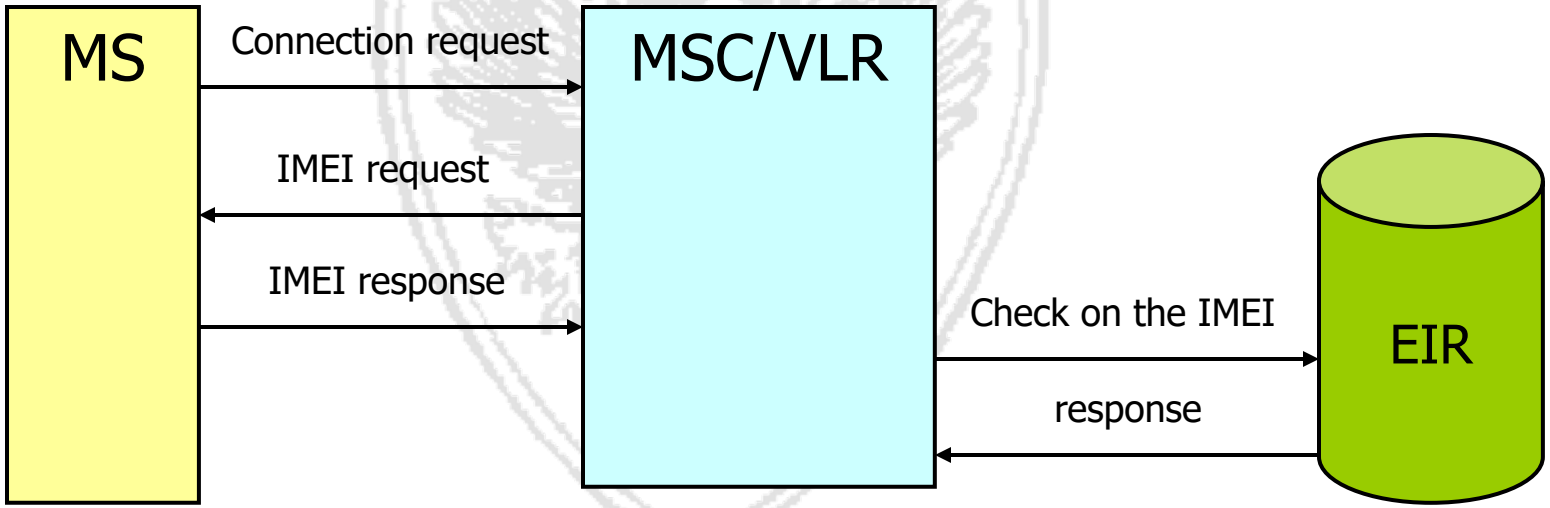
IMSI

- 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

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



IMEI management

- 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

Operation and Maintenence Subsystem (OMSS)

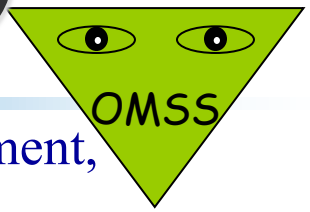
- Include the functional units responsible for monitoring the network, its maintenance and remote management
- It deals with:
  - configuring the functionality of all network devices
  - displayed alarms on malfunctioning elements
  - shows the statistics on data traffic
- etc..

Operation & Maintenance Sub-system (OSS)

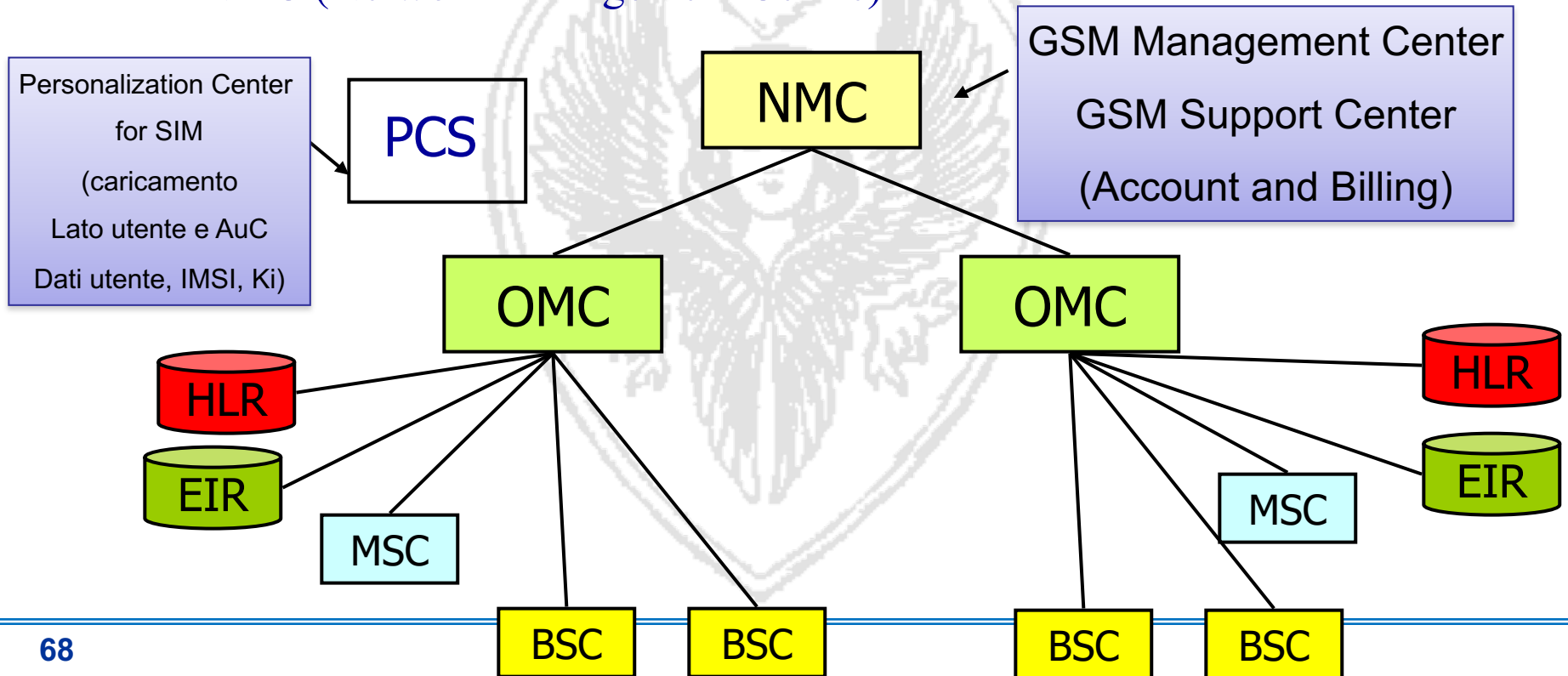
- Network measurement and control functions
- Monitored and initiated from the OMC (Operation and Maintenance Center)
- Basic functions
  - Network Administration
    - ✓ configuration, operation, performance management, statistics collection and analysis, network maintenance
  - Commercial operation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

ID associated to a mobile entity

- 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

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)