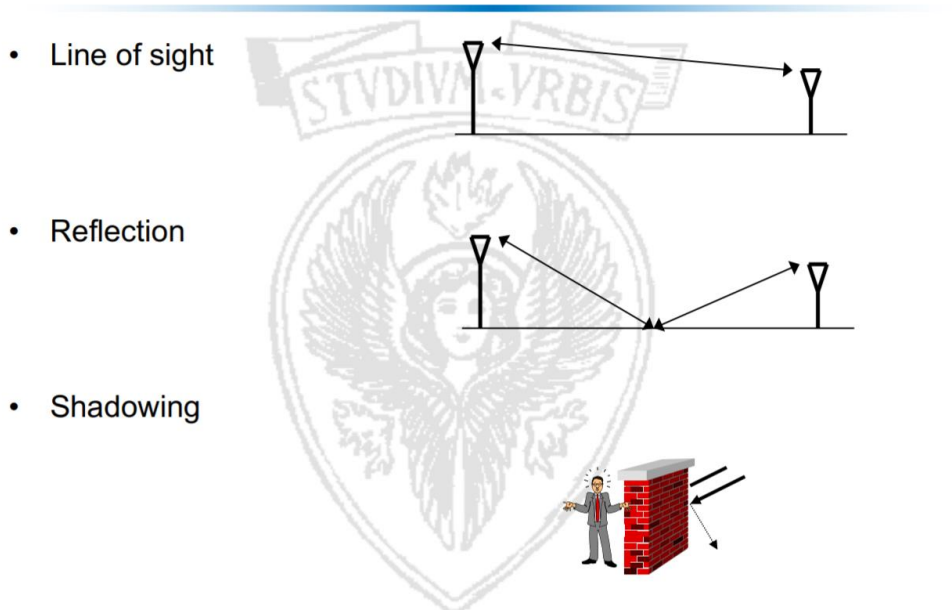
Internet of things notes

Author : Mario Tobia Vendrame

Wireless System Models

- Infrastructure networks (mobile users and station/access points)
- Ad Hoc Wireless NW (Peer to per communication)
    - They are affected by BER (Bit error rate)

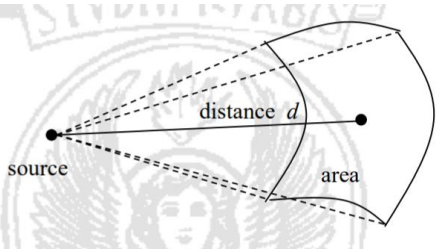
Wireless channels are much less reliable that wired ones, it can be attenuated due obstacles, and propagation will be multipath.



Difraction : When wave encountered sharp edges

Scattering: When wavelength encounters smaller objects (vegetation, clouds etc)

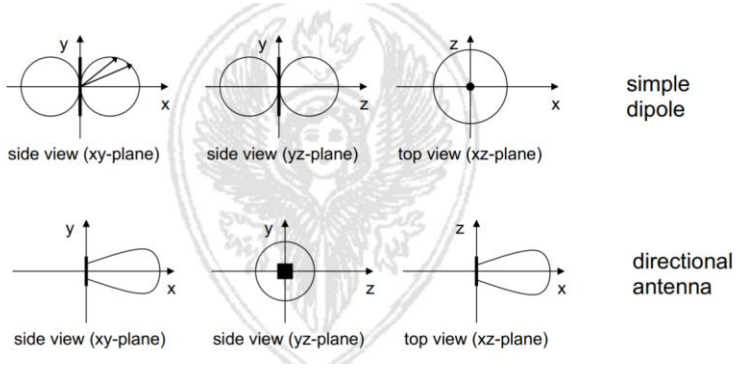
Radio signal attenuation :



$$F = \frac{P_T}{4\pi d^2} \quad [\mathrm{W/m^2}]$$

The power density at distance d is equal to the ratio between the transmission power and the surface area of a sphere cetered in the source and with radius d.

Antenna types:



Isotropic antenna: Radiates power equally in all directions (it is an ideal one, not real)

Antenna gain: Power output, in a particular direction, compared to a perfect omni-directional antenna (isotropic)

$$\text{Directivity D} = \frac{\text{power density at a distance d in the direction of maximum radiation}}{\text{mean power density at a distance d}}$$

$$\text{Gain G} = \frac{\text{power density at a distance d in the direction of maximum radiation}}{P_T / 4\pi d^2} \quad k$$

K = antenna efficiency factor <=1

$$F = \frac{P_T g_T}{4\pi d^2} \quad [\mathrm{W/m^2}]$$

Gt = max transmission gain

Pt*Gt = power at which an isotropic radiator should transmit to reach the same power dentary of the directional antenna at dist = d

$$P_R = P_T g_T g_R \left(\frac{\lambda}{4\pi d}\right)^2 \frac{1}{L}$$

$$A_{eff} = \frac{\lambda^2}{4\pi}$$

Power received by a receiver at distance d from source in case of no obstacles.

Gt and Gr are the gains of the transmitter and receiver, lambda is the wavelength(c/f) and d the distance t-r

L is a parameter to track HW losses.

dBm = ratio between the power and a nominal power of 1mW

- Power in dBm = 10 log(power/1mW)
- Power in dBW = 10 log(power/1W)

Path loss

$$PL = \left(\frac{\lambda}{4\pi d}\right)^{-2}$$ That's equal to Pt/Pr

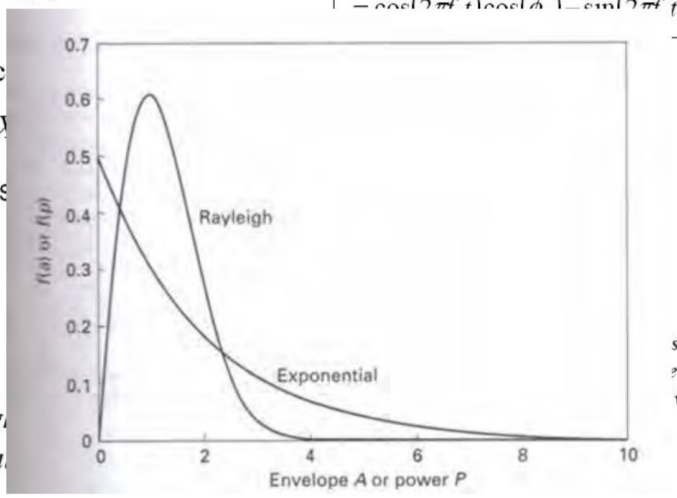
Real uses case formula

$$P_R = P_T g_T g_R \left(\frac{\lambda}{4\pi}\right)^2 \frac{1}{d^\eta}$$

N between 2 and 5

Rayleight fading

$$e_r(t) = \sum_{k=1}^{N} a_k \cos(2\pi f_0 t + \phi_k) =$$ | recall that : $\cos(2\pi f_0 t + \phi_k) =$



In the assumptions:

- N large (many paths)
- ϕ_k uniformly distributed in $(0,2\pi)$
- a_k comparable (no privileged path such as LOS)

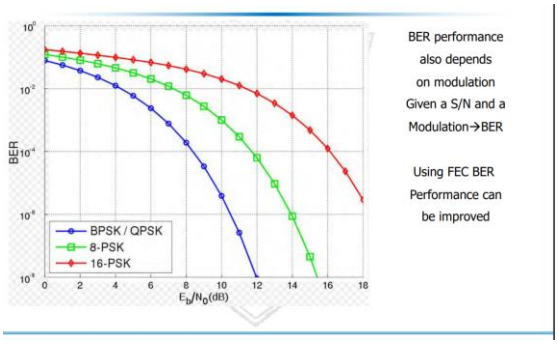
X,Y are gaussian, identically distributed random variables

Sigma² is the Variance of The X,Y variables

Rayleigh fading power distribution

$$f_p(x) = \frac{1}{2\sigma^2} e^{-x/2\sigma^2}$$

BER performance



Multipath fading

$$\tau_{RMS} = \sqrt{\frac{1}{\sum_{i=1}^{n} P_i}\sum_{i=1}^{n}\left(\tau_i^2 P_i\right) - \tau_d^2} \qquad \tau_d = \frac{\sum_{i=1}^{n}\left(\tau_i P_i\right)}{\sum_{i=1}^{n} P_i}$$

- τ_{RMS}
- τ_i
- P_i
- n

I'm coming into

Techniques for energy efficient communication

Portable devices rely on portable on portable energy sources, for that reason we have to use it as best as we can.

Network lifetime :

- Time till the first node of the network dies (low battery)
- Time till the network gets disconnected or fails

Energy efficiency :

- Energy spent by the network per bit correctly delivered to the final destination.
- E2E metrics (throughput/latency)

Laptop most energy consuming devices are :

- LCD
- Wireless card
- CPU/GPU

Network-related energy consumption:

- Computing: data processing
- Communications : wireless communication (transmit and receive)

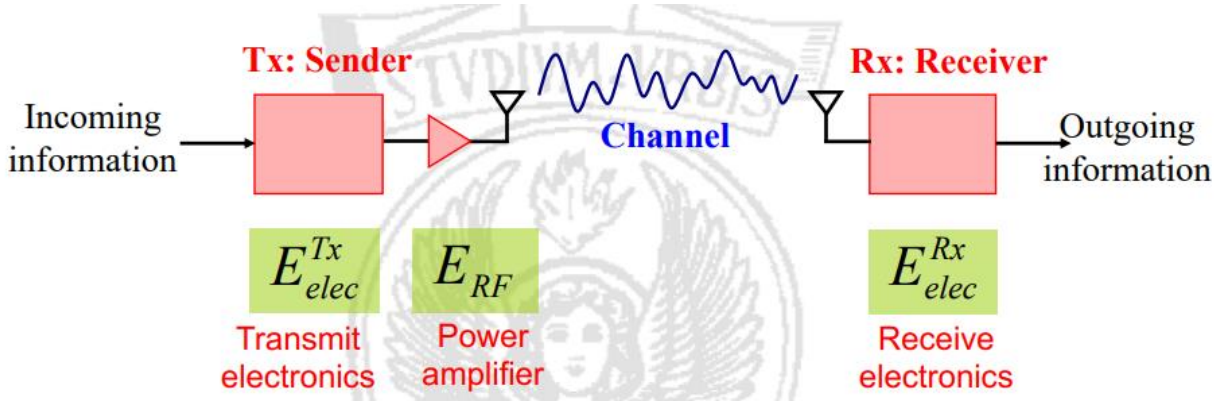
We need a trade-off between these two, that is the objective of the energy efficient communication.

Techniques:

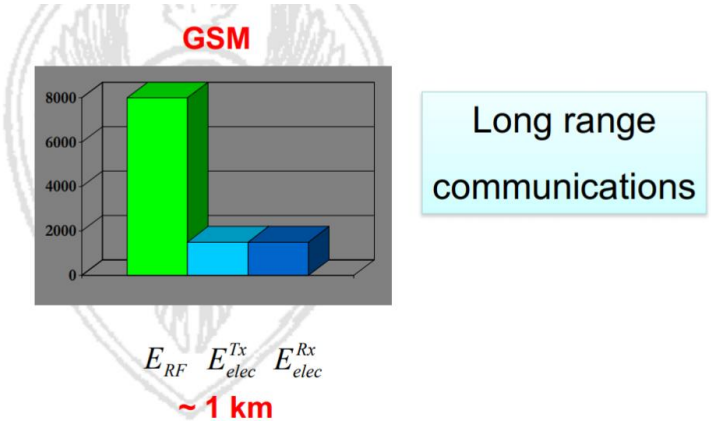
- Power control to minimize transmission energy : Minimize the energy needed to activate the transceiver circuitry and emit power, also wireless technologies can dynamically change the modulation scheme used over the time , high data rate reduce the time needed to transmit.
- HW selection could significantly impact overall system energy consumption.

Promiscous mode(force card to stay idle for long period of time) → high energy consumption , to perform a significant increase of power, we can set our devices in “sleep state”, low power state.

Device has to stay in low power state until it will not involved in communication.



Transmission range is very important on that schema.

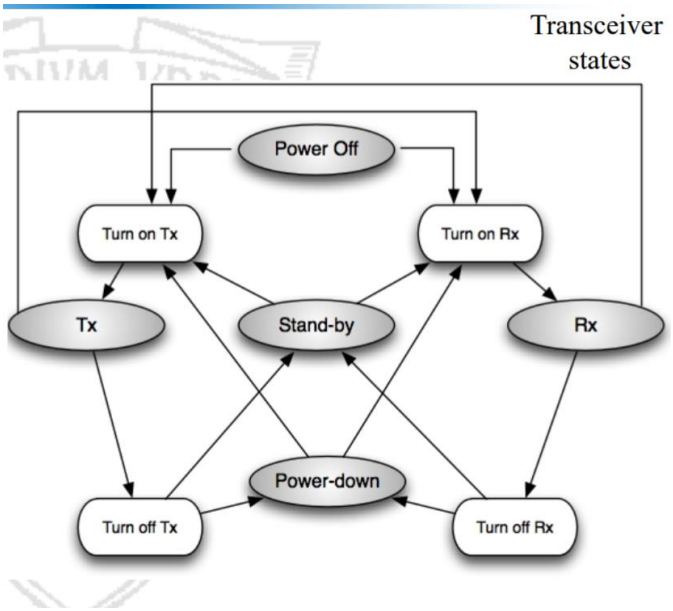


General guidelines :

- Awake/asleep schedule:
  - High energy consuming states when the transceiver is ON and packets can be transmitted / received
  - Low energy consuming states → transceiver OFF and cannot receive packets
  - Duty Cycle = Ton/(Ton+/Toff)
  - There are two different type of protocols to consider :
    - Synchronous

        - Nodes exchange info on when to wake up
        - Periodic control message to know when neighbors will wake up
    - Asynchronous
        - Awake/Asleep time is unknown
        - No control messages
        - Exchanging info has to be done when nodes are alive (ON)
- Nodes not involved has to go to sleep till info exchanging completes
- Nodes should minimize collisions
- Header compressions → to deliver less bits and transceiver is ON for less time
- If channel is in a bad state, is convenient to delay transmissions because is very likely that packets will not received
- Minimize overhead associated o route discovery and maintenance
- Avoid passing through critical nodes (with low energy)

Transceiver states :



- TX : Awake and transmitting
- RX : Awake and receiving
- Idle : Awake, neither transmitting nor receiving
- Asleep : Energy consumption is low

Protocol energy usage:

Ramp : low state → high state

Tail: high state → low state

New energy model

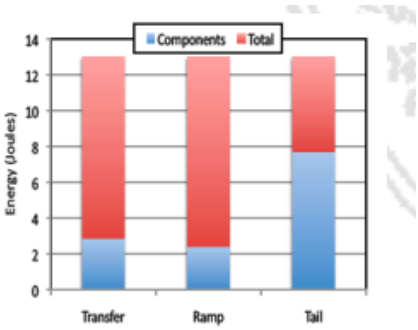
$$\mathbf{P} = \rho_{id} + P_{tx} + P_{xg}(\lambda_g)$$

ρ_{id} is the platform specific baseline power consumption

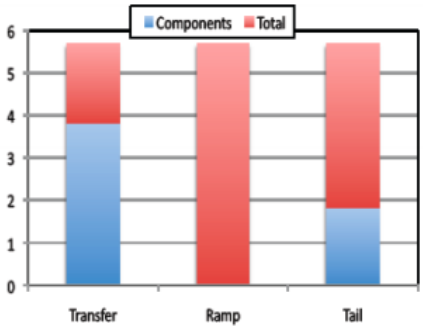
P_{tx} is the power consumption Associated to transmission (depends on airtime, tx power Modulation)

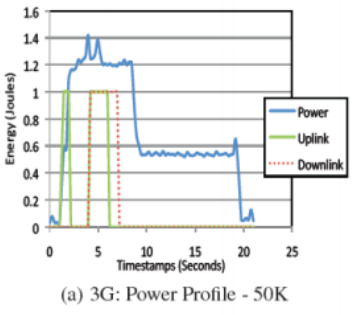
$P_{xg}(\lambda g)$ is the new cross factor

3g

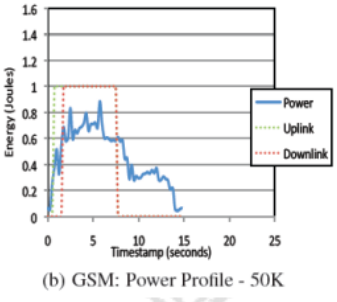


GSM

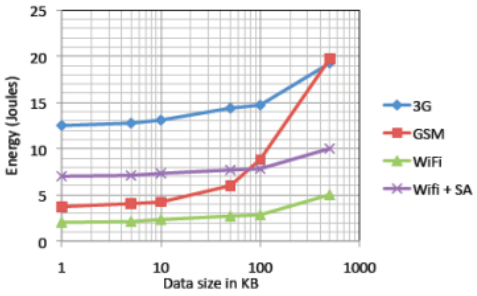




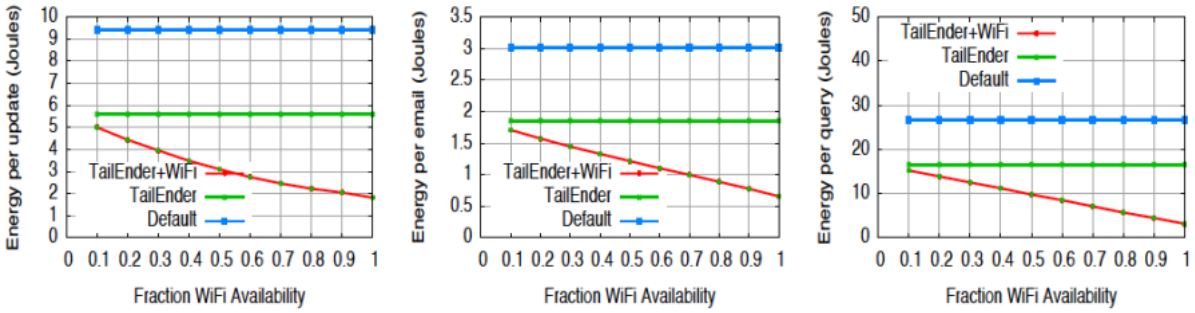
(a) 3G: Power Profile - 50K



(b) GSM: Power Profile - 50K



Solution : Combine 3g with WiFi (with prediction WiFi availability)

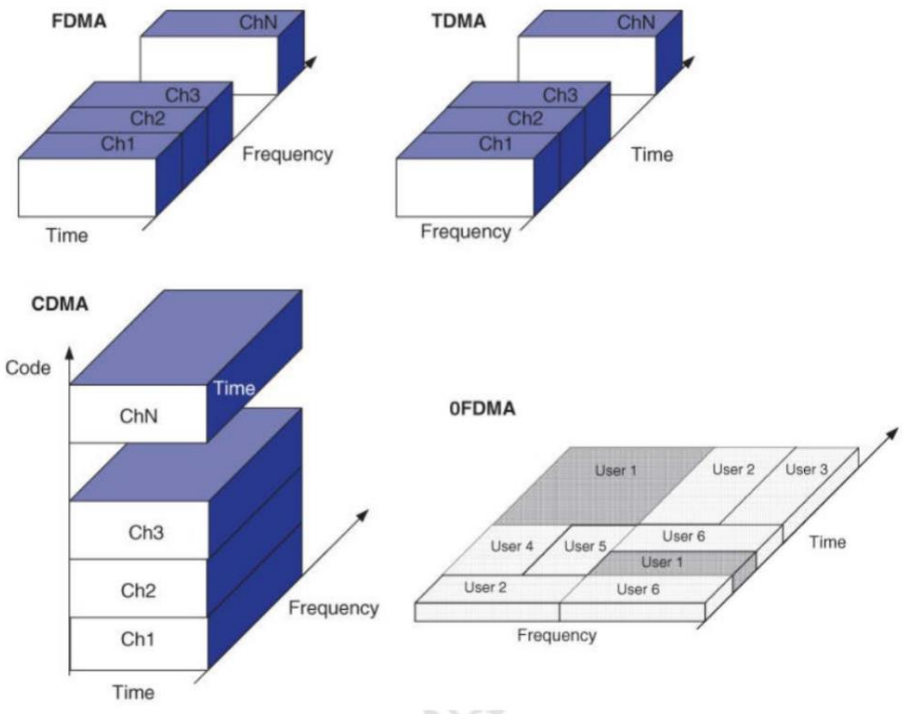


Someone has experimentally tried to send data without ack, that “obviously” lower the energy consumption.

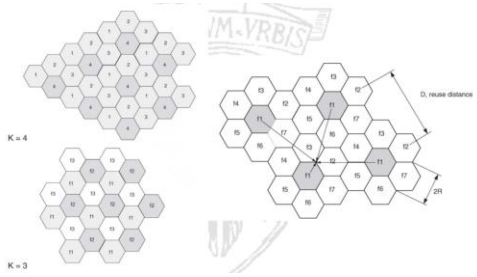
Physical sharing of resources

We have low physical resources availability so we have to think about a method to share info in a better way, so there are different allocation techniques:

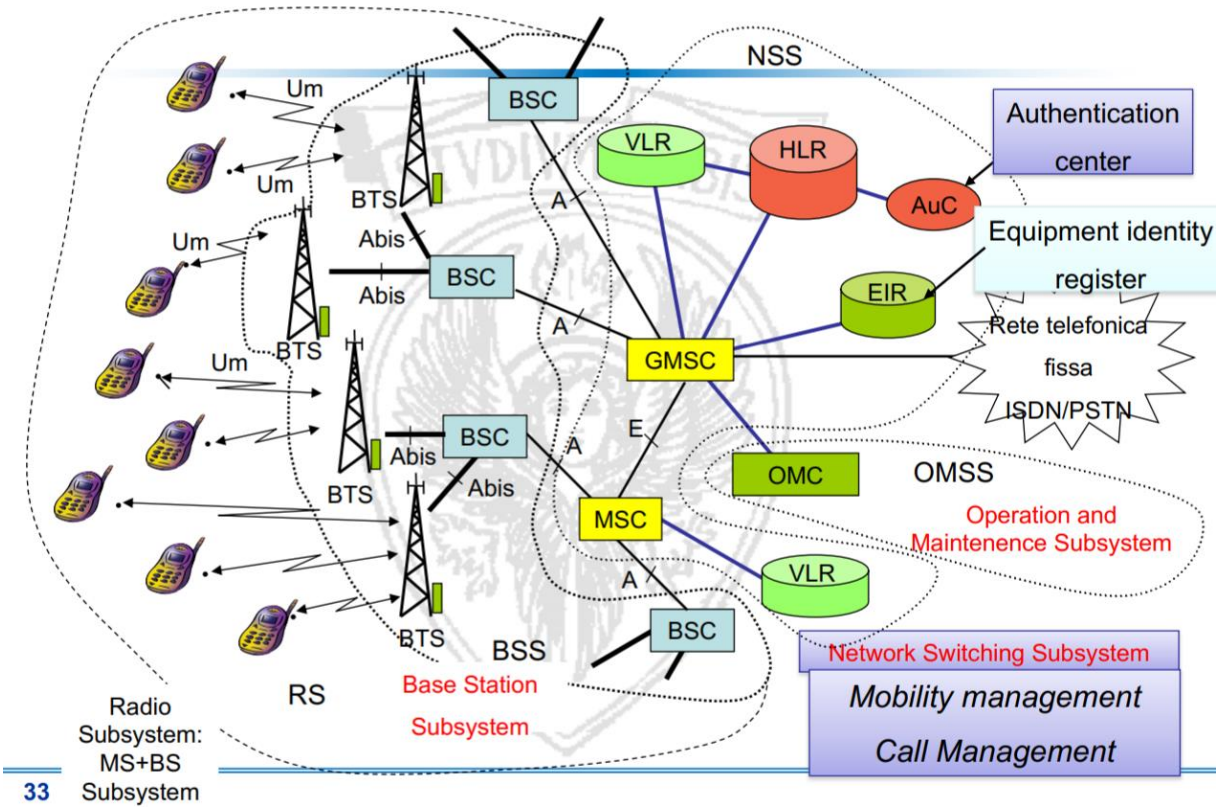
- TDMA : Time division multiple access
- FDMA : Frequency division multiple access
- CDMA : Ortogonal codes that allow to use simultaneously the channel without collision
- 0FDMA : More flexible way to allocate dynamically users



Base station is on the center of that exagon, and that is the visual explaination on how users are allocated in frequency, users can be served by the same frequency only if they are far enough to not have interference.



GSM :



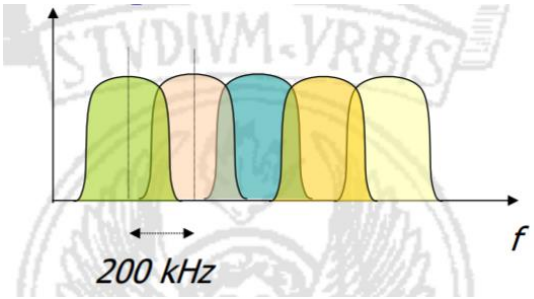
- BTS: Base transceiver station
- BSC: Base station controller
- BSS: Base station subsystem
- PLMN (Public Land mobile network) : Service area of a cellular nw
- MSC/VLR area : Area managed by an MSC, data regarding users in the area are stored temporally in a database called VLR.
- Location area :If users changes area (LA) she has to perform location update (LAI location area identifier) transmitted over the broadcast control channel.
- Cell: Area covered by the BTS (it is identified by BSIC (Base station identity code transmitted in broadcast)
- MS: Mobile station: terminal owned by the user, they can operate on different frequency bands (900,1800,1900), they can operate over different channels and slots.
    - Vehicular: antenna can emit 20W max
    - Laptops : antenna can emit 8W max
    - Personal: antenna can emit 2W max

MS is divided in : ME (Mobile Equipment) identified by the IMEI and SIM (Subscriber identity module).

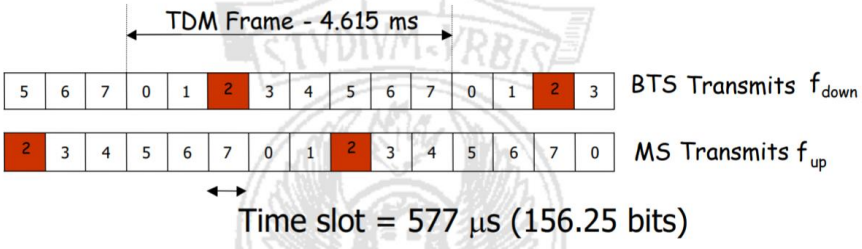
Information stored in SIM:

- Serial number : uniquely identifies the user on the network
- Security auth and cyphering information (A3 and A8 algo for auth and encrypt, Ki,Kc (keys for auth and encryption))
- Temporary network info :
    - LAI (location area identifier)
    - TMSI (Temporary mobile subscriber Identity)
- List of services offered
- PIN and PUK
- Access rights, prohibited networks, call messages,phone number

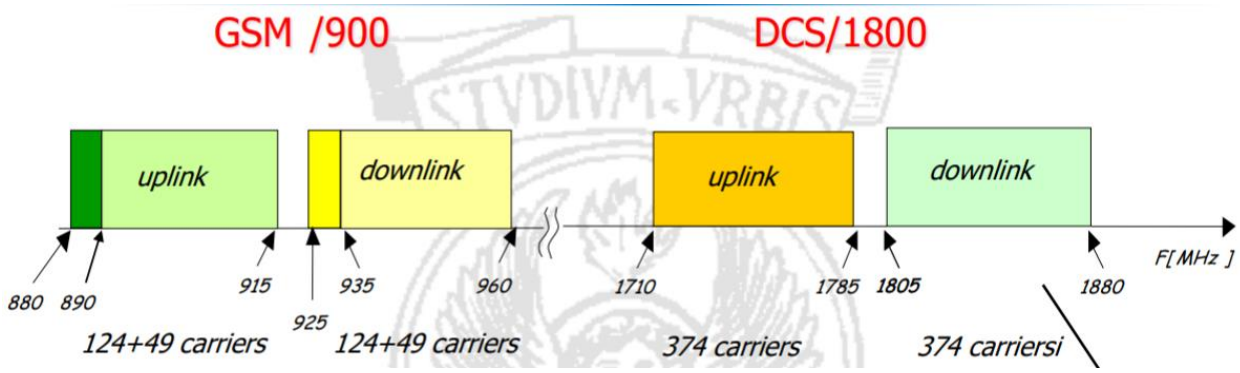
- Bandwidth = 200KHz



- TDMA (8 slots per carrier / 8 channels per carrier) →FDMA



- Full-duplex
- Modulation : GMSK
- 13Kbps full rate coder every TDM slot
- Frequency reuse, power control, discontinuous transmission, adaptive equalization
- Power control : power emitted is adjusted according to the conditions of propagation
- Discontinous Trasmission: during speech pauses, coded voice transmission is interrupted to reduce interference and energy consumption



Lower frequency requires less power to tx to a given distance

Base station system (BSS) : It deals with radio aspects of the system, like communication with the MS, BSS also performs radio resource management.

BSS includes:

- BTS (base transceiver station)
- HW/SW components that enable the transmission and reception of info through the radio interface, it also perform encryption,modulation,coding.
- BSC (Base station controller) : Monitors and manages the resources of a group of BTS

BTS (Base transceiver station) :

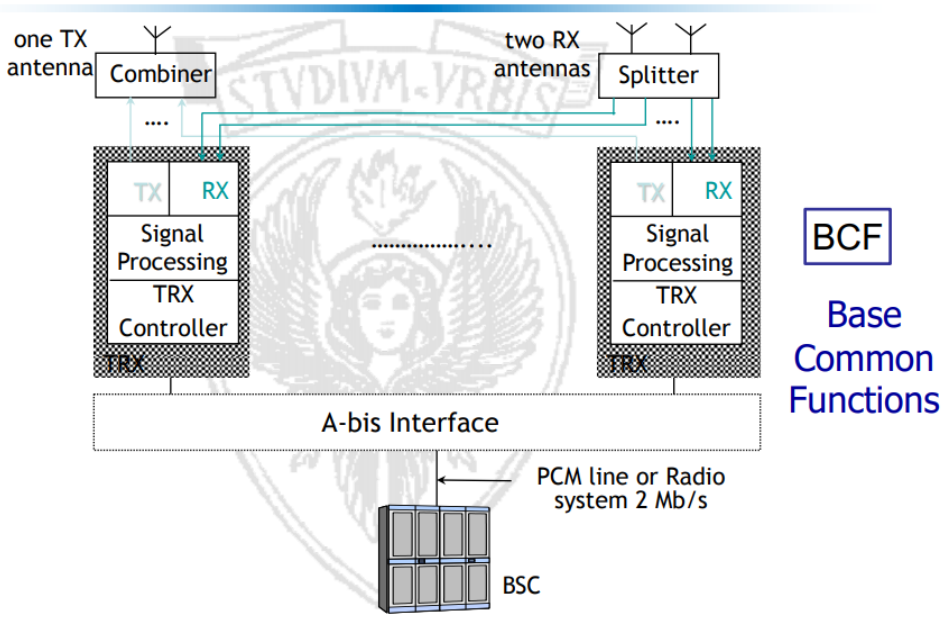
Implement low level protocols of the radio interface, and then receive and transmit signals, it perform modulation, coding ,multiplexing, frequency hopping and encryption.

That station perform quality measurements on the physical channel and those made by MS (to know when and where handoff)

It is also in charge of sending paging messages to locate the current position of a user.

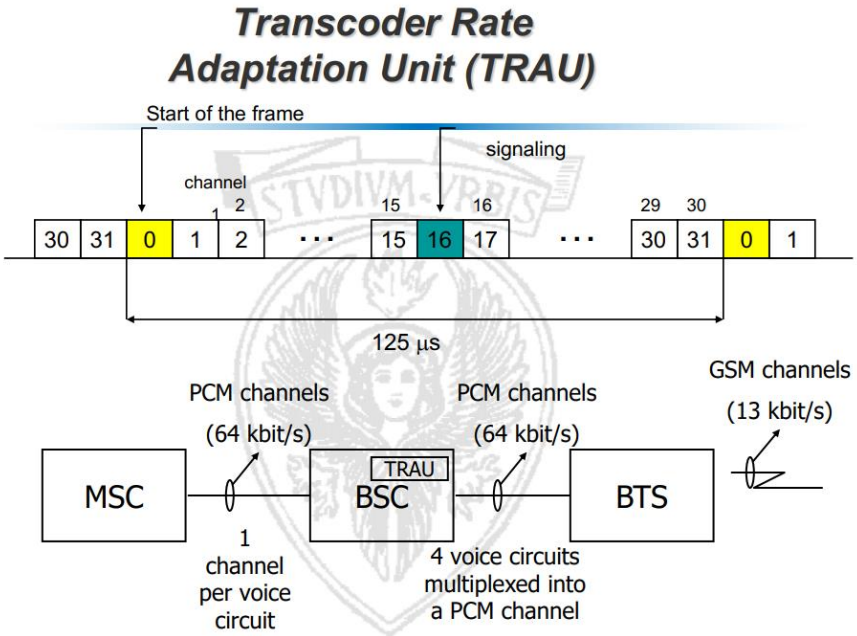
BTS is divided in :

- TRX (Transceiver) :
    - Radio elements responsible for reception and transmission of a single radio carrier
        - Trasmitter : modulation, power amplifier
        - Receiver: diversity,demodulation
        - Signal processing
        - TRX controller
- BCF (Common base function) :
    - Control element of TRX that perform the common functions: sync,frequency hopping computation
    - Interface with BSC



Transcoder rate adaptation unit (TRAU) :

- GSM voice coding is 13 kbps while the PCM provides 64kbps
- Transcoding provided by the TRAU
- TRAU could be on the BTS but often is in BSC
- For each GSM carrier (8 channels at 13kbps) we need 3 PCM channels at 64kbps



Base station controller (BSC): it is like a switching node, but do not perform routing tasks

- The BSC controls a large number go BTS (tens to hundreds)
- Configuration of each cell by assigning traffic and control channels
- Set up and release of connections between channels
- Management of handovers between controlled BTS
- Management of the paging messages
- Analysis of the link quality and power measurements

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

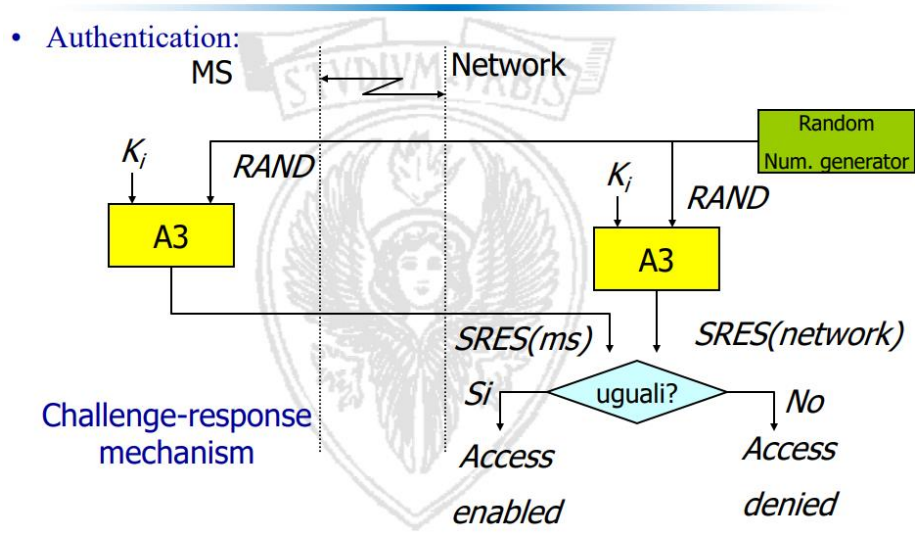
Network switching subsystem (NSS) : (Subsystem that is responsible for circuit switching to the mobile users, managing mobility)

- MSC (Mobile switching center)
    - It is connected with VLR and BSC (via PCM channels)
    - It can be reached by fixed users via phone number (MSISDN)
    - Provides originating call,terminating call,gateway
    - Location updating, periodic registration and auth
    - It includes protocols to exchange info with others elements on the nw
        - DTAP (Direct transfer application part) : protocol to exchange info over logical channel
        - BSSMAP (BSS management application part) protocol to exchange info with the BSC

        - MAP (Mobile application part) protocol to exchange info with other nw elements
- VLR (Visitor location register) : Database that contains info about users registered in the area managed by the MSC
    - Authentication : task of verifying the user identity and protect fraud use of identification
    - Encryption: Encryption algorithms and frequency hopping
- HLR (Home location register) : Database that store info of mobile users, it can identify the VLR of each subscribed user.
    - It provide MSRN (Mobile station roaming number) associated to the MSC/VLR query
    - Persistent database uniquely associated to a GMSC
    - Stores IMSI (international mobile subscriber identity), and additional info
    - Manage localization, store VLR number
    - Send routing info to the GMSC
    - Storage and supply to the VLR
    - Management of user data
- AuC (Authentication center) : It contains keys and procedure to identify mobile users (related to HLR)
    - Stores the secret keys Ki for each user
    - Generate random numbers and calculates SRES and the encryption key Kc
    - Provides the triplets to the nw elements
- EIR (equipment identity register) : Contains all IMEIs of all devices authorized to access the service

MSISDN –(reach)-->MS—(routed)-->GMSC(that identify HLR that contains users info and queries to determine how to route to thee mobile user current MSC) : HLR returns MSRN –(allow)-->GMSC (to route call)

Security procedures :



Ki : user auth key of 128 bits stored in SIM and AUC

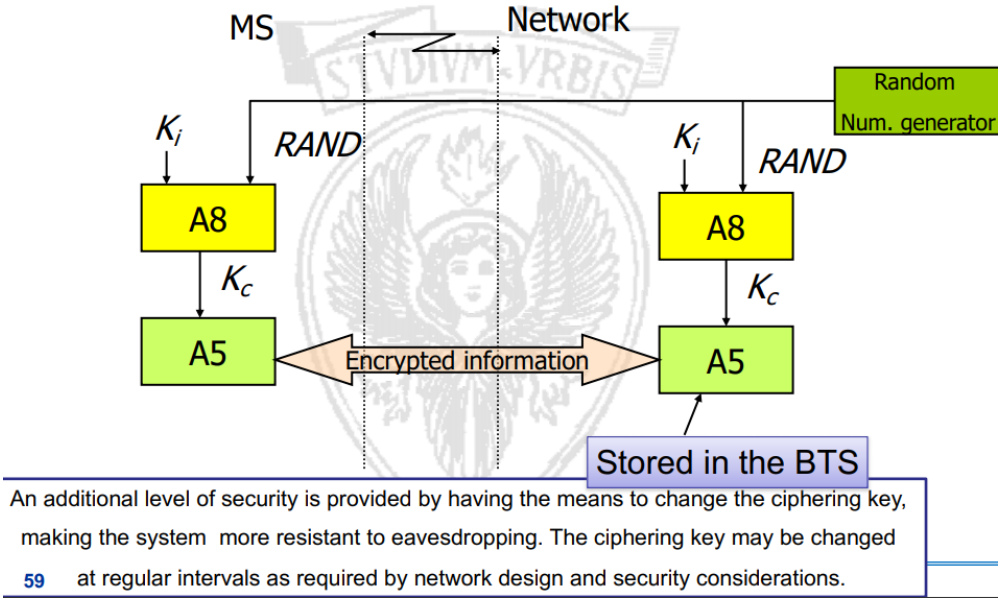
RAND: 128bit random nuber generated by the AuC and sent to the MSC

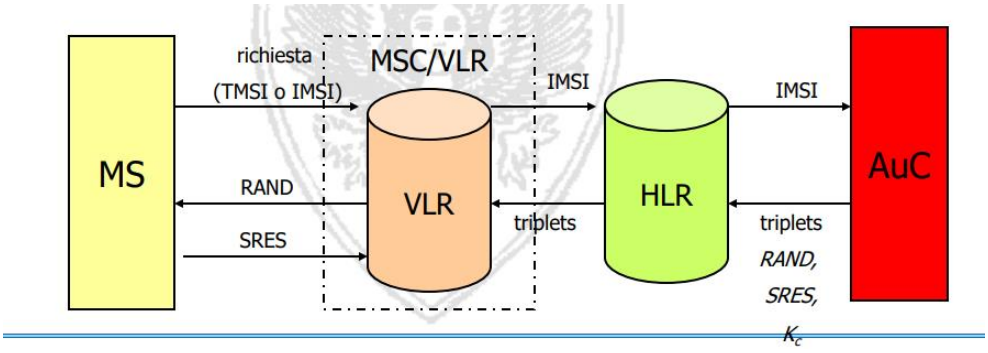
A3: auth algo

A8: encrypt algo

Kc : Encryption key

SRES: output of auth algo

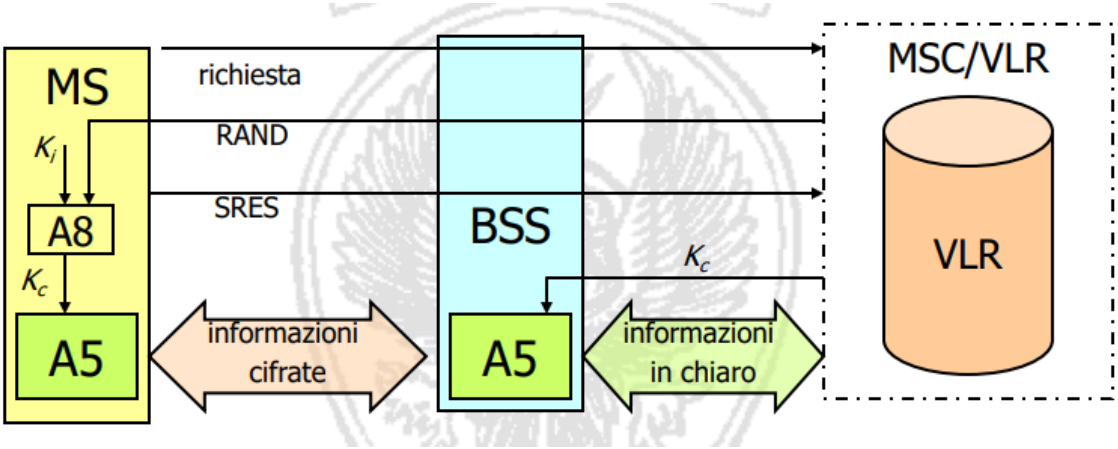




To initiate a communication the MS send its ID (IMSI) to identify itself before starting the auth procedure, to minimize the risk of spoofing, the VLR generate an TMSI (Temporary mobile subscriber Identity), every time a location update is performed, VLR generate another TMSI to the MS.

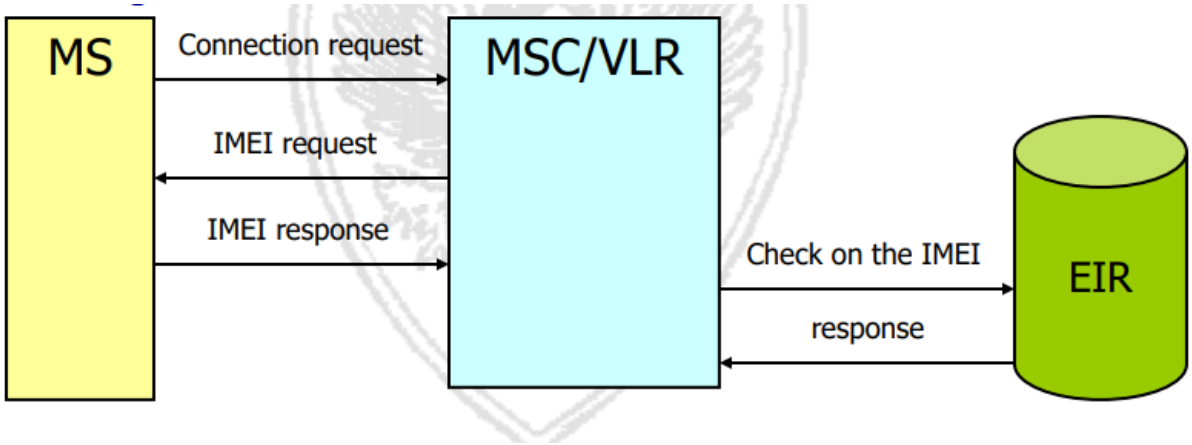
IMSI : Identification number on the network, divided in :

- MCC :Mobile country code
- MNC: Mobile network code
- MSIC: Mobile subscriber identification number (identify the SIM)



EIR (Equipment identity register) :

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

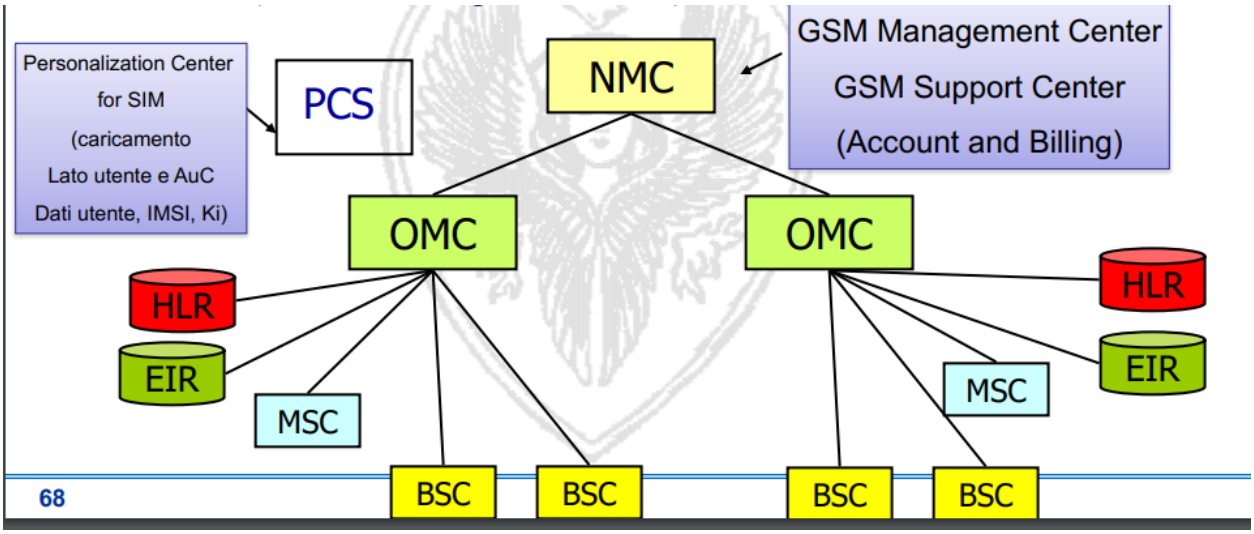


IMEI management

- White list : valid IMEIs
- Black list: Can't use GSM nw exception for emergency calls, that list is exchanged among operators
- Gray list: IMEIs that need to be tracked for some reason, a call from gray IMEI is reported

Operation and maintenance subsystem (OMSS)

- Units responsible for monitoring the network
- It configure the functionality of all network devices, display alarms, show stats on data traffics
- Commercial and operation service
- Security management



Number and IDs in GSM:

- MSISDN : user mobile number
- MSRN : It is assigned to by the current VLR, to communicate with GMSC, and GMSC with mobile user
- Handover number : it allows reroute the call till the target MSC
- IMSI : Permanetly stored In SIM and HLR
- TMSI : Temporary ID assigned by a VLR to an MS (it avoid to transmit IMSI in clear)
- IMEI: Uniquely identifies a terminal equipment
- LAI : uniquely identify the location area with MS is under control
- CGI : it identifies the cell within it's location area
- RSZI: Regions where the user can roam
- BSIC: It allows to distinguish among signals received

- 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)

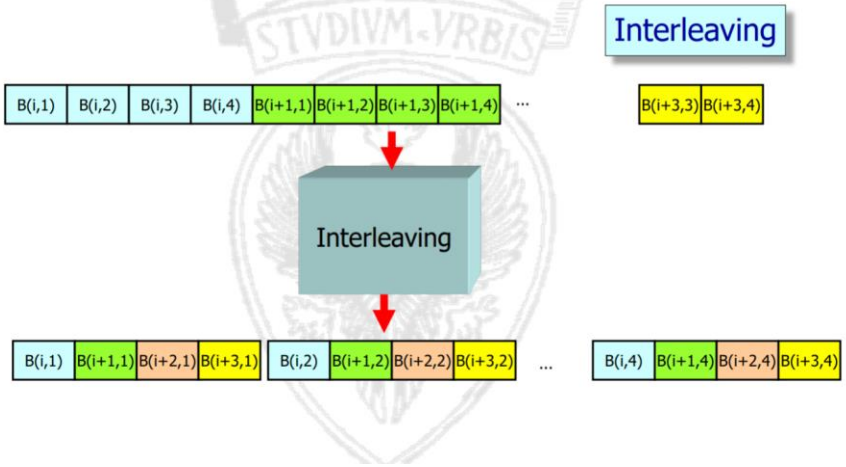
Radio interface

Band of 200kHz divided in uplink and downlink, every user has his amount of frame (Time slot =577 microseconds, 1 frame = 44,615ms), between every frame there are 3 slots to divide transmission and time to receive.

On frequency we use a FEC that is a bit to permit correction of the communication in case of needed (before a limit threshold) .

Frequency hopping is a technique that allow a communication to hop on another frequency if the channel is enough disturbed, the frequency will hop to predefined pseudorandom sequence, that allow the channel to serve as good it can.

Interleaving is another technique that send different block of packets in different time, to prevent a completely retrasmission of the packet at the destination if a problem income.

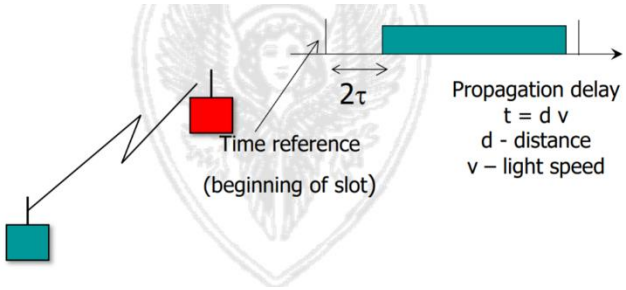


Power control :

Output power of the MS is controlled by the BTS (sending commands to the MS), The step to increase/decrease is 2db, that mechanism allow the MS to prevent not needed use of the power.

GSM Sync :

- Carrier frequency sync (MS ha to retrieve precisely the frequency of the radio carrier)
    - That frequency of the radio carrier is obtained by the MS listening to the broadcast BTS's common control channel. Every regular intervals a special fixed sequence of bits are transmitted to select carrier frequency , and adjust the local oscillator.
- Slot sync (MS must have info about current slot)
    - The sequence of frequency hopping depends on the multiframe structure, BTS in fact transmits on the broadcast channel the info to reconstruct the current time slot and frame.
    - To sync slot we have to keep in mind that propagation could be delayed (depends on distance between MS and BTS) in fact each slot needs to have a guard period to compensate.



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

To limit the guard time : The BTS estimates the delay and sends the info to the MS wich can then compensate by anticipating the transmission. (GSM → 9bits (33,3ms))

- Frame sync (MS must know the current frame number)
- BS sync (Sync frame number and clocks)

Best way to manage power control is to have many BS, really low power consumption , unlimited capacity, but it has some disadvantages like mobility management and additional infrastructure costs.

Mobility management : That problem is encountered when an MS what to change position and so BS.

MS could be in some different situation :

- Call out
- Be called
- Converse

When user is in active mode, the call need to be rerouted after every change of cell (handover)

If IDLE →location must be updated

Every terminal select his BS in base of the signal strength , periodically it perform a scan to know if better BS are spawned to make a reselection.

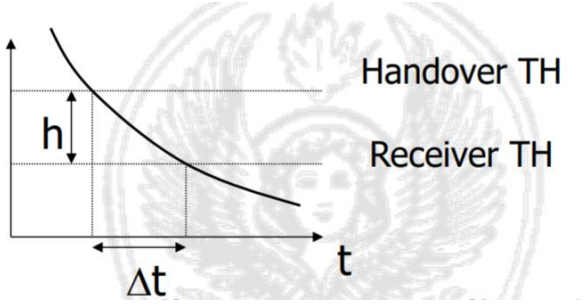
Location update :

Location area is a group of several cells, every IDLE MS is tracked by a system based on location area, and the last area location of each user is stored in a operator database.

When a user change location area it triggers a location update procedure. When a call arrives for the MS the network initiate a paging procedure to know where the MS is, when the MS answers the networks knows the cell and the routes till the mobile user.

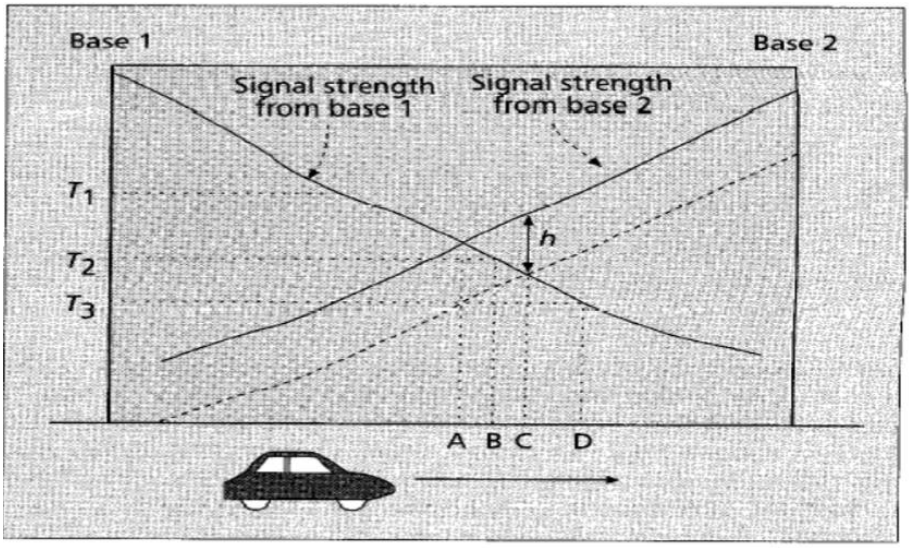
Handover:

Handover is triggered due to a threshold, if h is too small the risk is to loose the connection, if h is high the number of handover increase so also the signaling traffic.



When to trigger an handover?

- Strongest signal (Point A)
- Strongest signal with threshold (Point B)
- Stronges signal with hysteresis (if the power of the other BS is stronger than a value h the handover accurs at the point C)



Could be that the new channel where the MS will handover is not available, in that case we deifce Pdrop the probability that a handover request can not be met and the blocking probability Pblock as the probability to rejecting a new call (it's better to block an incoming call that loosing one active).

Guard channels :

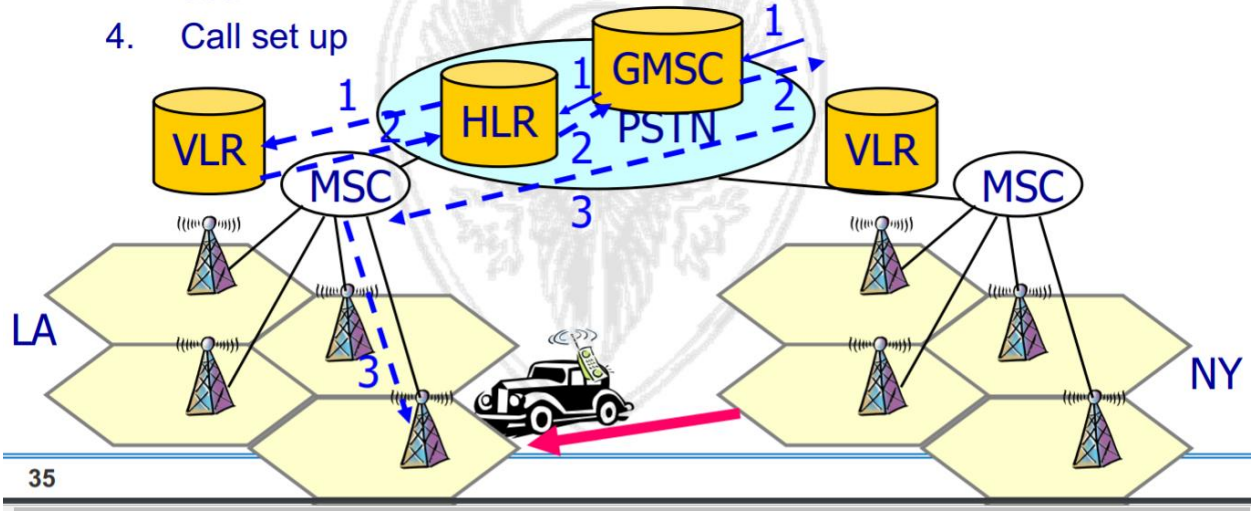
- A number of channels is reserved to handover requests(Pdrop becomes lower but the capacity of the system is lower)
- Queuing priority scheme (if the new BS is full, the MS remain connected to the same BS as before until the channel will be free)
- Subrating scheme(if there are no channel available, the channel previously allocated to a call is divided in two channel half of rate)

Hard handover : Removal and establishment of a new radio link

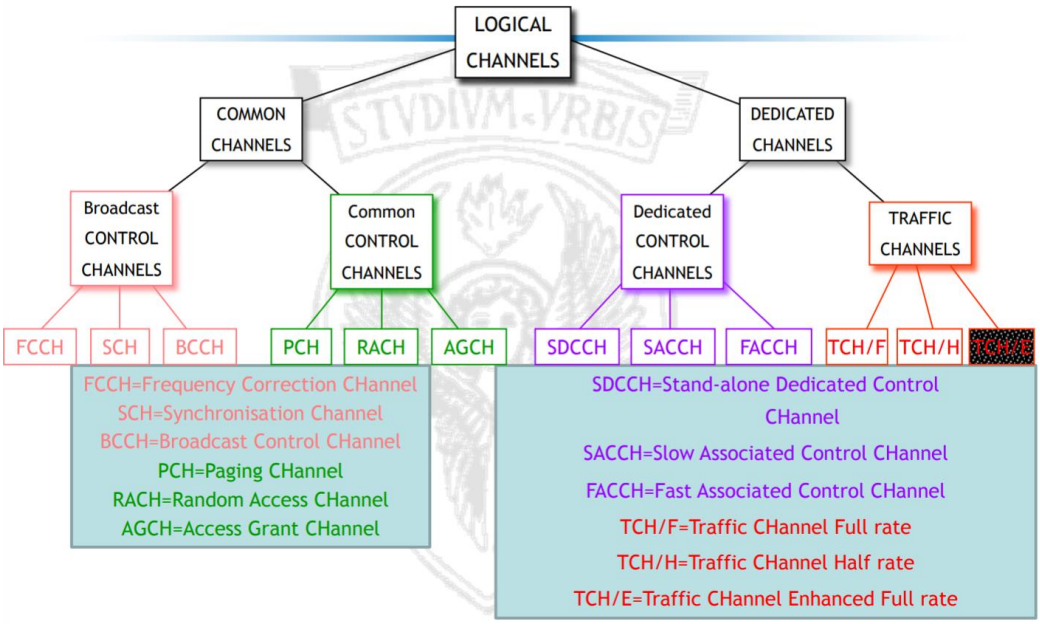
Soft handover: for some period of time MS is connected to multiple BS

Call set up : example

1. MS→fixed phone through the VLR of the MS
2. Fixed phone→MS:through the gateway MSC of the MS the caller contacts the HLR and , throught it, the VLR currently managing the user
3. VLR provides information such as a routing number, LA of the user
4. Call set up



Logical channels :



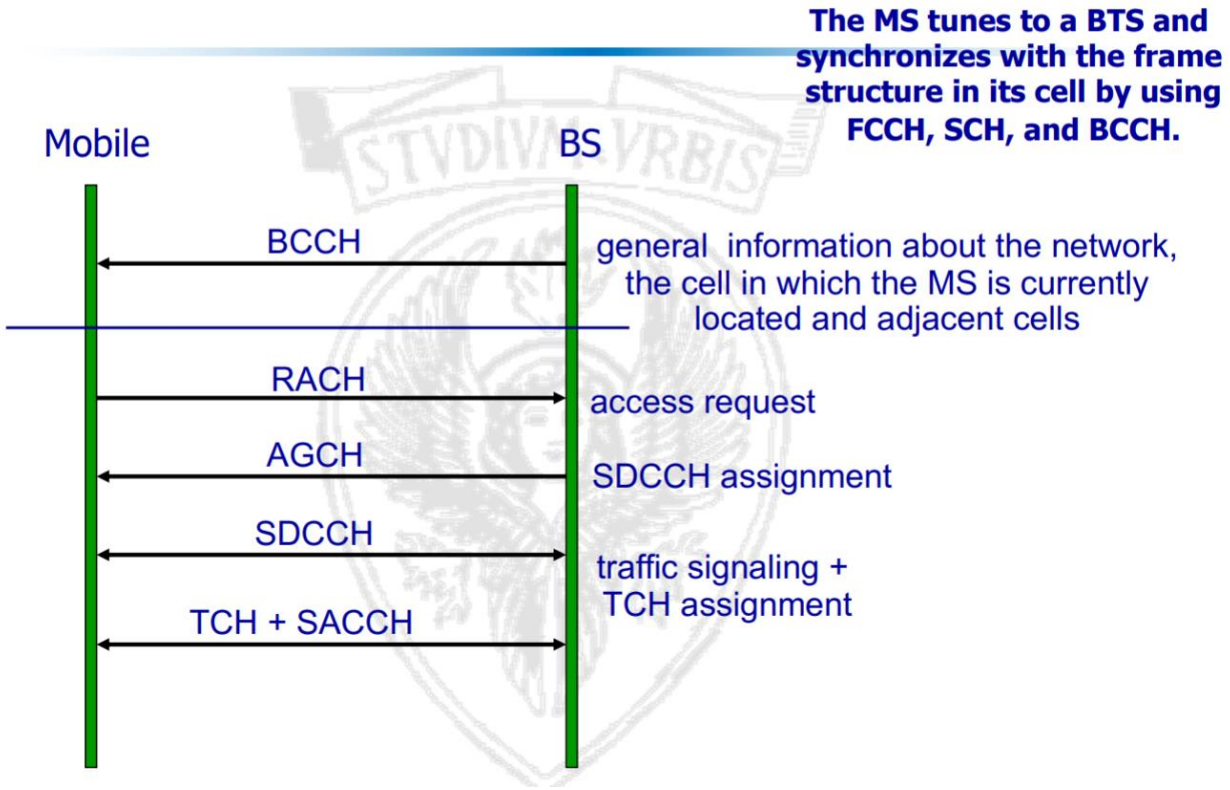
Control channels : carry signaling information (14 types), them are divided in three categories of CCH:

- Broadcast channel (BCH) : unidirectional downlink channels providing general info about network.
    - FCCH(frequency correction channel) : downlink channel used to correct MS frequency (148bits without coding)
    - SCH (Sync channel) : carry the BS identity code (BSIC) and the frame number (FN), 25+ channel coding
    - BCCH (Broadcast control channel) : carry general info that are broadcasted to all user of a BS (184 bytes after coding) like frequency hopping algo etc..

- Common control channels (CCCH) : carry info for initiating a connection (shared between multiple connections)
    - PCH(paging channel) : downlink channel used by the BTS to notify an incoming call to MS, broadcasted over the LA
    - RACH (Random access channel) : uplink channel used by a MS to request access to the network (location update, call request), prone to collision
    - AGCH(Access grant channel): downlink channel carrying reply to RACH request
        - RACH channels is prone to collisions
        - Access messages that are correctly received by the BS are ack on the AGCH channel
        - RACH messages include temporary pseudo-random sequence that is included on the acknowledgment sent on the AGCH channel
        - Slotted-ALOHA protocol for transmission on that channel

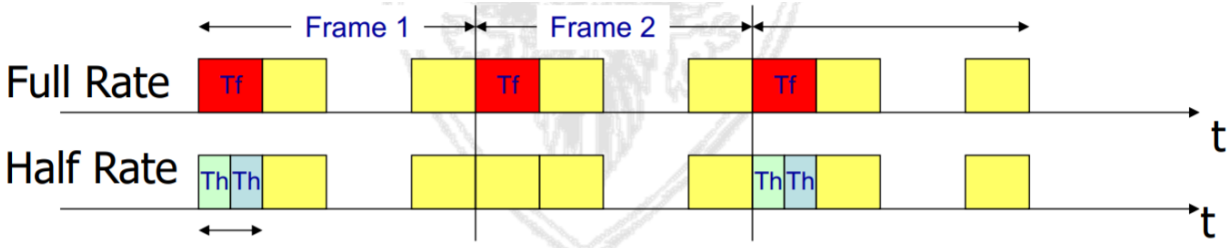
- Dedicated control channels(DCCH) : carry signaling information specific for a single connection
    - SACCH(slow associated control channel): bidirectional channel used to exchange connection metrics between MS/BS and vice versa (signal strength , quality and so on) (184bits)
        - Downlink
            - Power control commands
            - BCCH info
        - Uplink
            - MS measurement report (signal strength for own BTS, downlink BER signal strength from adjacent cells, BCCH carrier of adjacent cells, BSIC of adjacent cells)
    - FACCH (fast associated control channel) : used to exchange of time critical information (urgent handover request)
    - SDCCH (standalone dedicated channel): after RACH request for auth messages and call set-up

Set-up traffic channel :



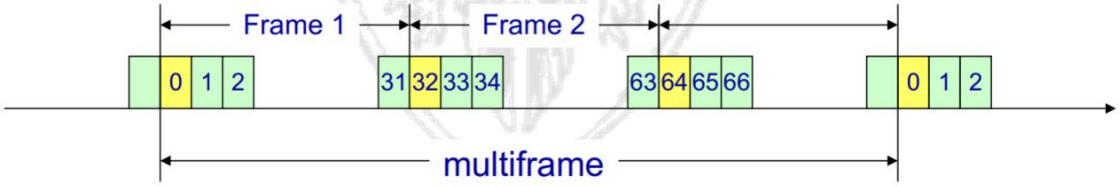
TCH : Carry speech and data there are two types of TCH

- Full rate channels(22,8 Kb/s)
- Half rate channels(11,4Kb/s)
- Voice channel(13Kb/s)

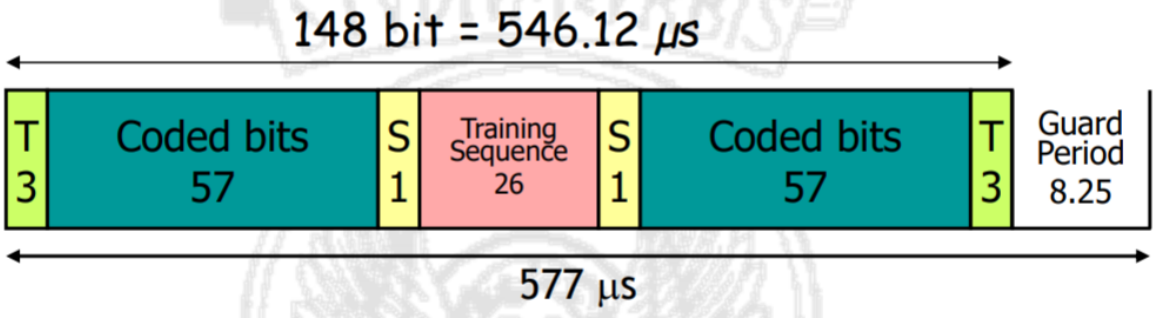


Mapping of logical channels onto physical channel :

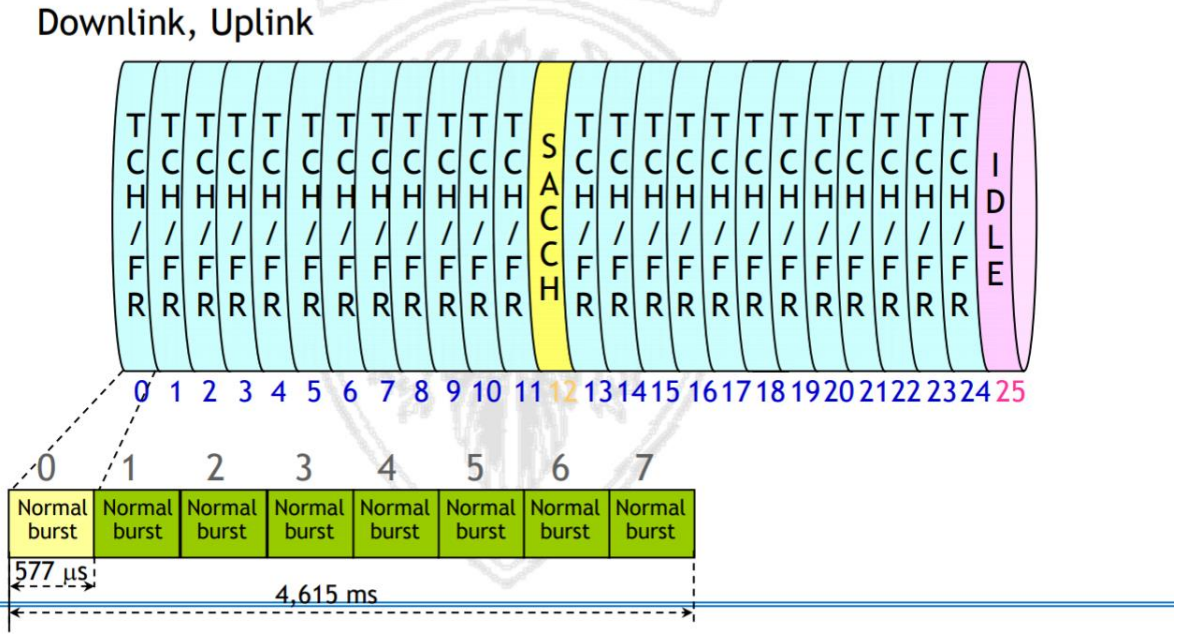
To reduce transmission rate we can use a multiframe technique :



A normal burst carries 114 bits of data (24,7Kb/s) → coded speech is transmitted at a rate of 22,8Kb/s

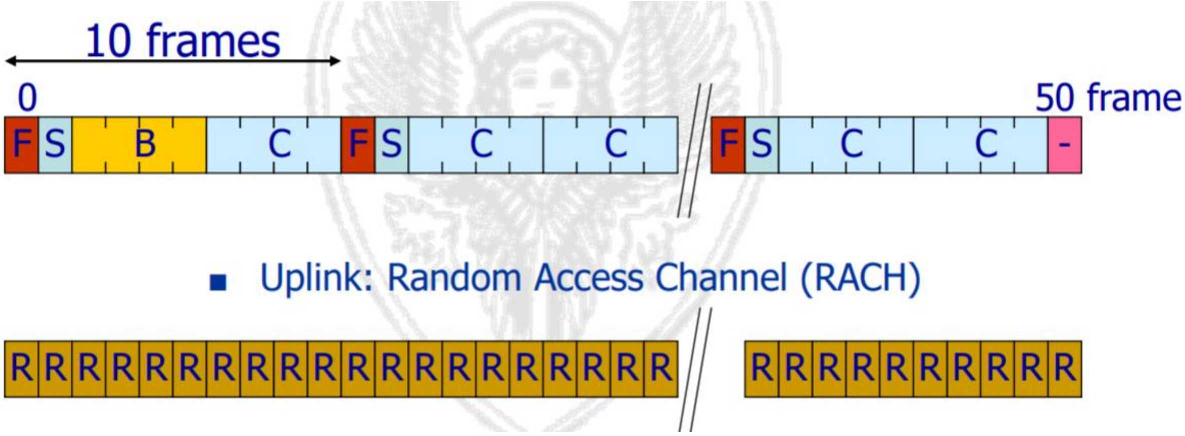


That is a temporal diagram for the sequence of slots of the same traffic channel, SACCH (Control channel)



A given slot 0 over the main carrier is used to obtain one or multiple channels that use a multiframe containing 51 frame, the downlink is always transmitted at a power higher that the other carriers that allows the MS to sync with the main carrier and receive the info for tuning to the BS.

Common signaling channels



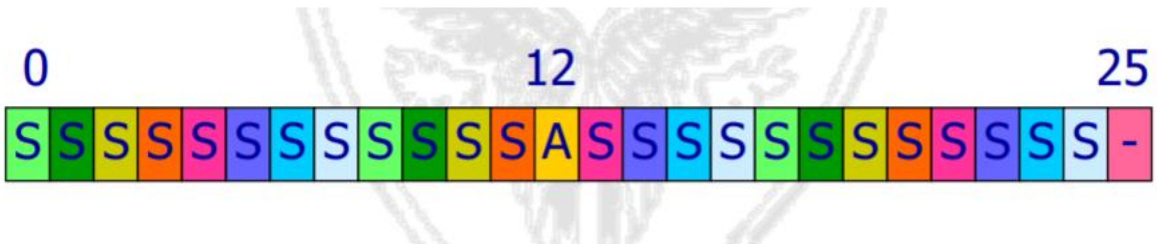
F : frequency channel (FCH)

S: Sync channel (SCH)

B: Broadcast channel (BCCH)

C: Common control channel (PCH, AGCH in downlik)

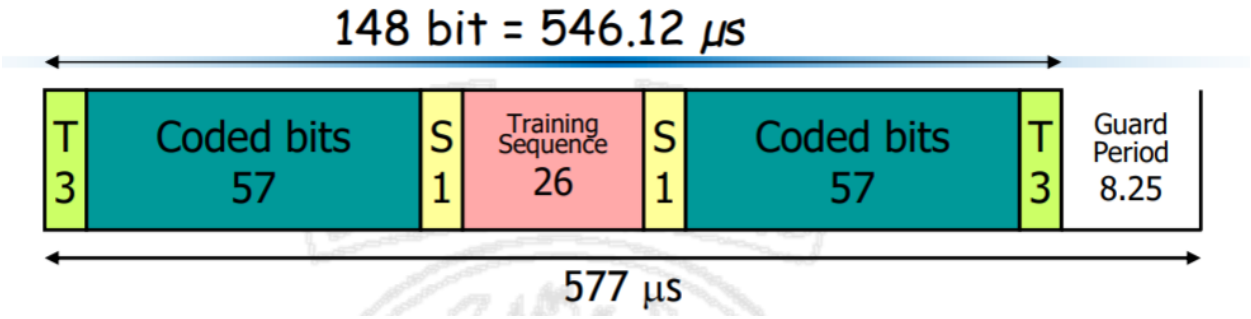
SDCCH channel: Used to setuo and other messages (SMS), the 8 channels are obtained by using 3 slots each within the super-frame of 26 slots, the last frame is idle (serch frame), the last frame can monitor the BCCH of this and neighbor cell, it allow to scan all BCCH slots during superframe.



The physical block is the info transmitted during a slot, due to TDMA each block is an autonomous transmission entity, which should be transmitted at the appropriate power level to avoid interface with adjacent slots.

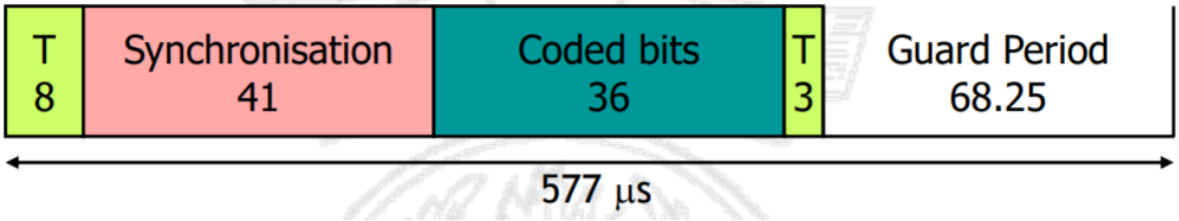
Burst classification :

- Normal Burst : used to user transmissions (speech or data) over traffic channel



- Tails bits always set to 0
- Stealing bits indicate whether the burst contains user data or signaling info (SACCH or FACCH channels)
- Coded data: user bits (speech, data etc) 114 bit with channel coding, corresponding to 13kbits for speech and to 9.6kbits or lower for data (due to the channel coding using more bits)
- Training sequence : control bits used for the equalization and tuning of the transmitters

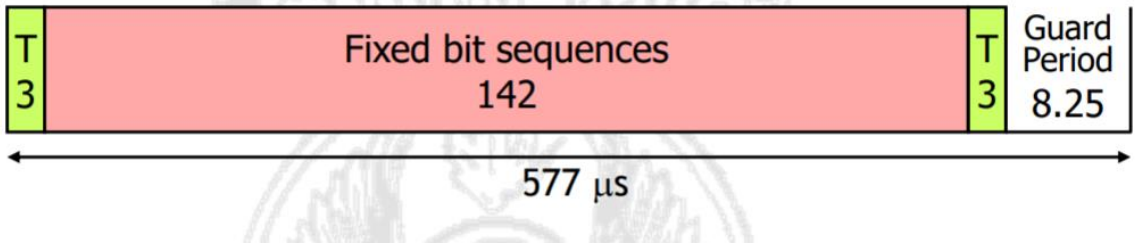
- Access Burst : Used to transmit info over the random access Channel – RACH, first time access
    - Longer guard period (68,25) to avoid overlapping, the guard period is computed assuming a mac cell size of 35Km.



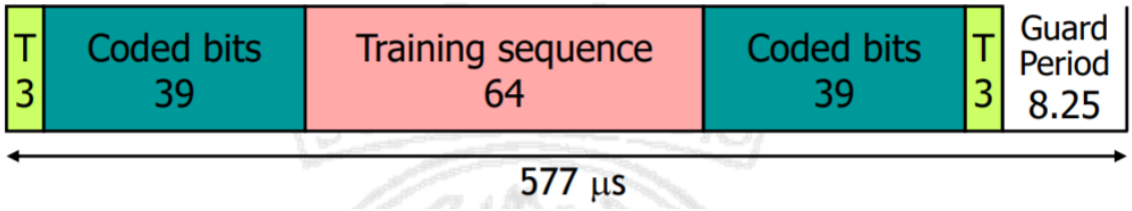
Used by the MS on the random access channel at the first access (async access, no timing advance check), it contains 156.25bits :

- 8 tailing bits
- 41 sync sequence
- 36 coded bits
- 3 tailing bits
- 68.25 bits guard period

- Frequency correction burst :
    - Used over the frequency correction channel (FCCH)
    - 142 bits set to 0
    - Correct the frequency of the MS's local oscillator, effectively locking it to that of the BTS

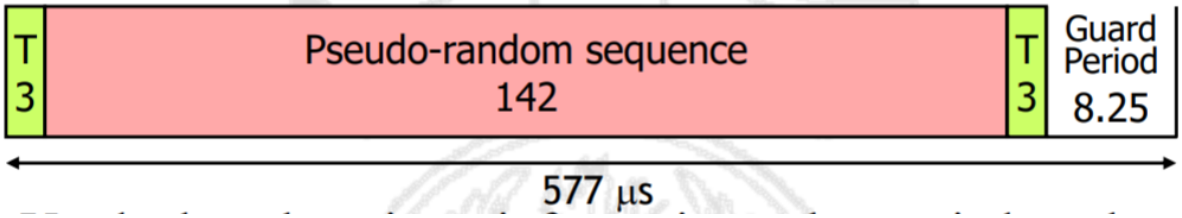


- Sync burst :
    - Used to transmit info about sync for slots and frame

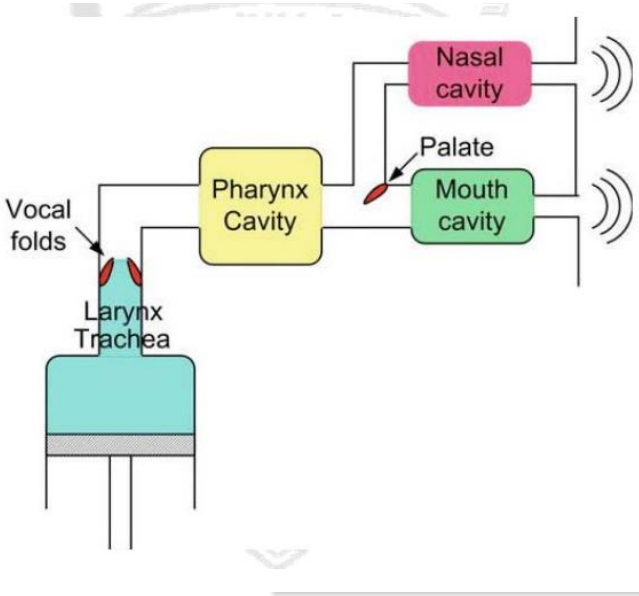


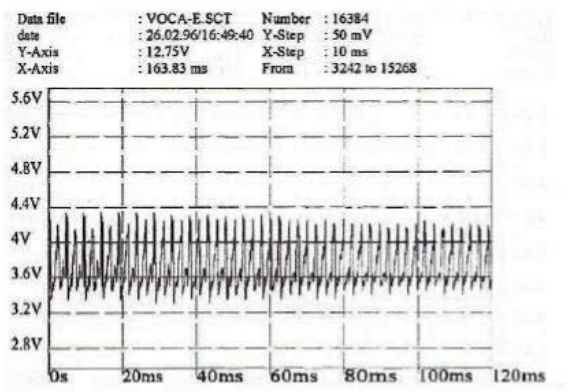
Coded bits must be protected and correctly decoded.

- Dummy Burst:
    - It contains no info, only padding bits
    - Used when there is no info to be carried on the unused timeslots of the BCCH carrier (downlink only)

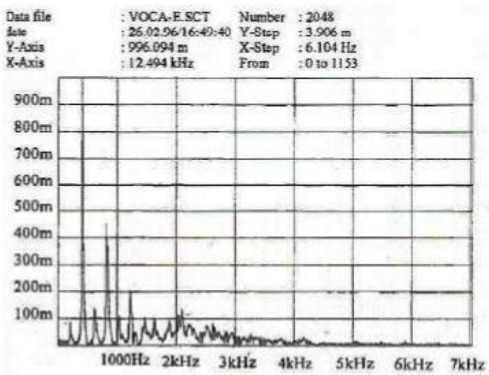


Voice recording :





Signal in time



Signal spectrum (frequency components)

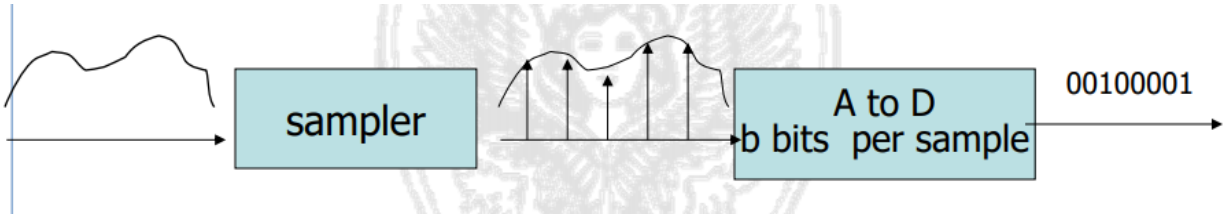
Signal in time and signal in spectrum of the vowel “e”.

Sound produces by the vocal folds has some features :

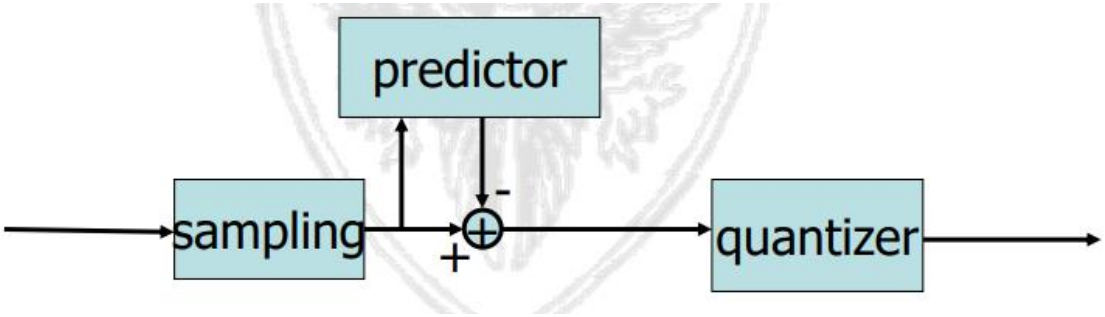
- Periodic (Pitch period)
- High amplitude
- Slow variation of the signal
- Low number of frequency around which the energy is concentrated (formant frequencies)
- Formant frequencies are low frequencies

Most significant frequency components are located between 300Hz and 3400Hz with small spectral components till 7kHz.

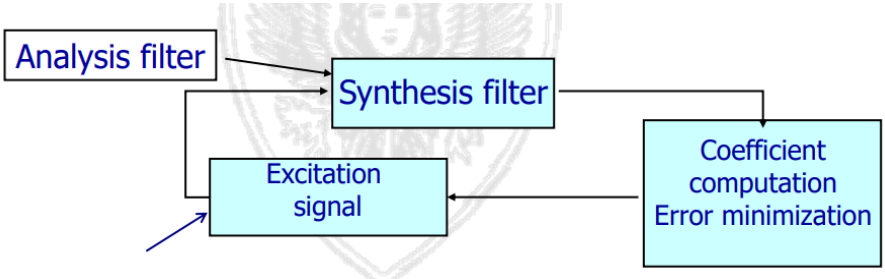
There are more way to code voice :



- Waveform codecs (high quality, low complexity, low delay, robustness to errors and background noise)
    - No a priori knowledge of how the signal was generated
    - Info needed
        - Signal bandwidth (speech signal < 4KHz)
        - Maximum tolerable quantization noise
    - In waveform codecs, the subsequent voice samples are correlated, so we can use a prediction methods for evaluating the next sample known previous, transmitting only the difference between the predicted value and the actual value, because of the correlation the variance of the difference is smaller and it is possible to encode it with a smaller number of bits.



    - Performance improves if predictor and quantizer are adaptive (equal quality but 32Kbps)
- Source codecs (vocoders)
    - They are based on models for the generation of the human voice, they allows to remove redundancy from the vocal segments to obtain an information base to reproduce the original voice signal (so if we know the structure of the signal and little info about features we have enough to rebuild it)
    - High complexity
    - Delays and average higher, sensitive to errors , noise and non-human sounds



- Vocoders instead of trying to encode the waveform itself, try to determine some parameters about how the signal was created to reconstruct it later
- Transfer function : H(z)=A(z)/B(z)
- Example linear vocoder (LPC) :
  - they encode the synthesis filter and the excitation sequence
  - The voice sample is approximated by a linear combination of a number of past samples
  - It has high delays due to segmentation, analysis and synthesis, quality is not natural (problems with background noise)
  - Low bit rate <2,4kbit/s

Coding	Year	Bit rate (kbit/s)	Frame size (ms)	Look ahead (ms)
G.711 PCM	1972	64	0.125	0
G.726 ADPCM	1990	32	1	0
G.722 Subband ADPCM	1988	48-64	0.125	1.5
G.728 LD-CELP	1992-94	16	0.625	0
G.729 CS-ACELP	1995	8	10	5
G.723.1 MP-MLQ	1995	6.3	30	7.5
G.723.1 ACELP	1996	5.3	30	5
RPE-LTP (GSM)	1987	13	20	0

Codebook Excited Linear prediction

LTP= Long term prediction

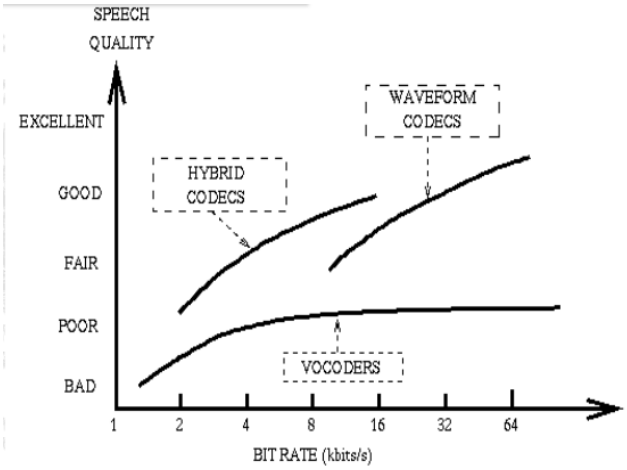
Hybrid

Regular pulse excitation-residual signal is undersampled

The sequence of departure from which the decoder must start to rebuild the speech signal is not a pseudorandom sequence but is representative of the "real signal"

- Codebook excited linear prediction
  - Tries to overcome the synthetic sound of vocoders by allowing a wide variety of excitation signals, all captured in CELP codebook.
  - To determine which excitation signal to use the coder performs an exhaustive search (for each entry in the codebook, the resulting speech signal is synthesized and will be chosen the one with smallest error)

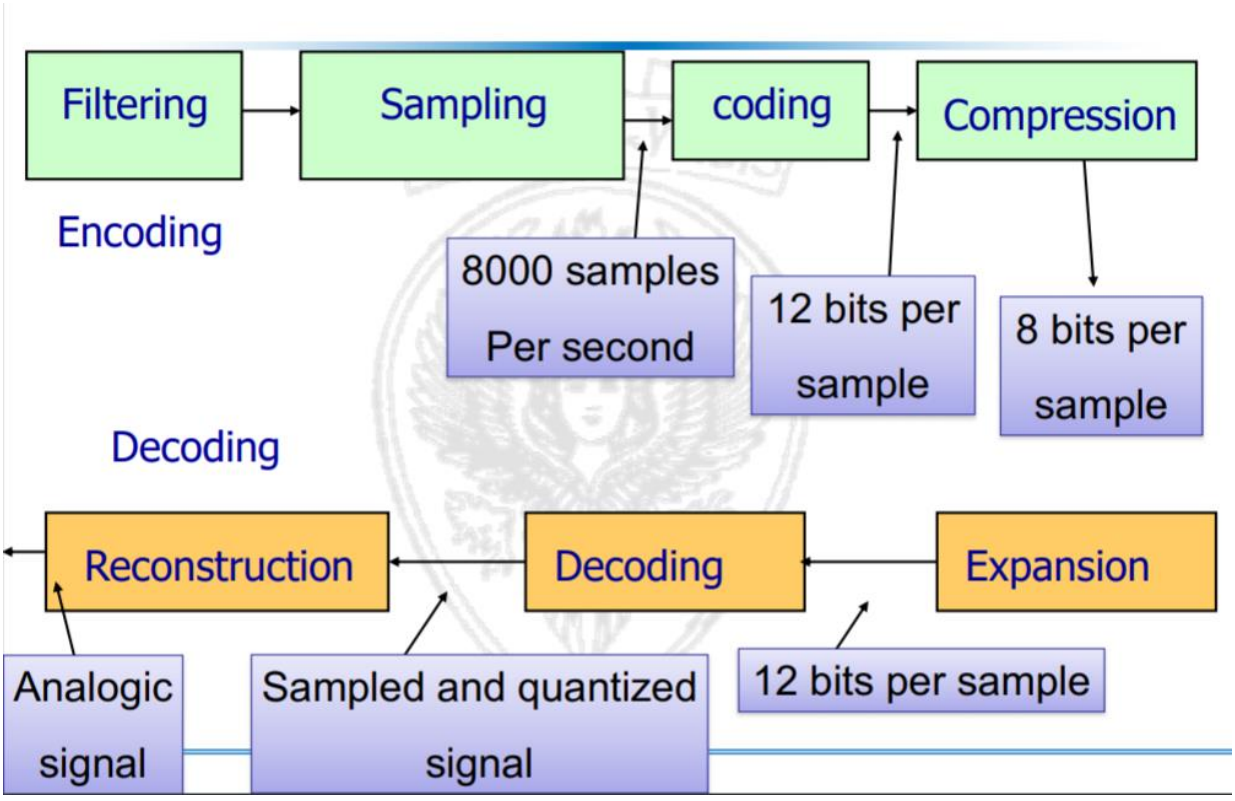
- Hybrid codecs



Uniform quantization :

The problem with the stream is that we have to module and quantize a signal that is uniform on a discrete distribution. Quantization error is fixed and it is < q/2 where q is the quantization step, so the number of bits) , 12 bits per sample are needed to achieve a quantization error low enough also for small values.

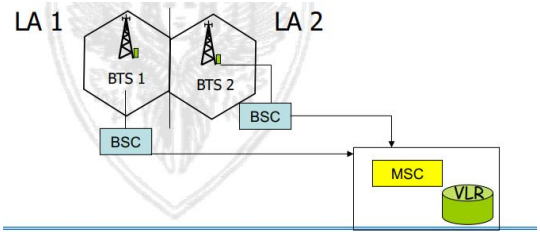
Non-uniform quantization : Many relatively small values, with higher quantization errors can be tolerated in case of high values, 8 bits per sample results in an excellent perceived quality.



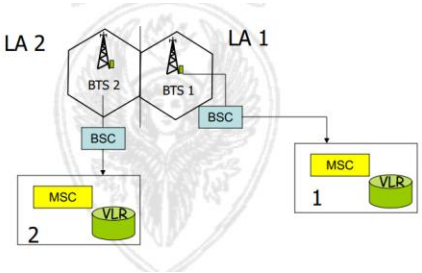
MS procedures:

- Cell selection : MS select the BTS to which tune to
    - MS scans all RF carriers operating in the cells :
        - Scans c0 carrier over which the BCCH is transmitted (these carrier are transmitted ad higher power that other carriers)
    - MS will connects to the RF carrier from which the strongest signal is received
    - Through the FCCH channel the MS sync to the BTC carrier
    - Through the SCH the MS sync to the slot and frame and receives the BSIC (Base station identity code)
    - MS can now decode the BCCH which includes :
        - Location area code
        - Cell local identity
        - Mobile country code
        - Mobile network code

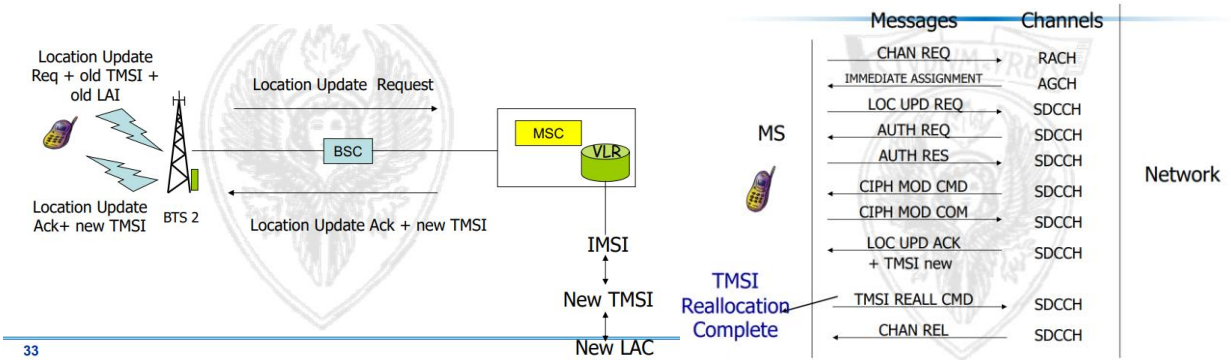
- Registration (Location update procedures) : the MS notifies the MSC of its presence in the location area, two cases are possible :
    - It is the same of that stored in the SIM (same LA of switched off phone)
        - The IMSI attach procedure is invoked → MS activates its IMSI stored in the current VLR
    - NO LAI stored or received, LAI different from the stored one (it is also performed periodically (every 30 min for ex) to know if device is already in the LA (implicit detach)
        - Location updating procedure is invoked
            - There are two types of location update :
                - Two LAs of the same MSC/VLR



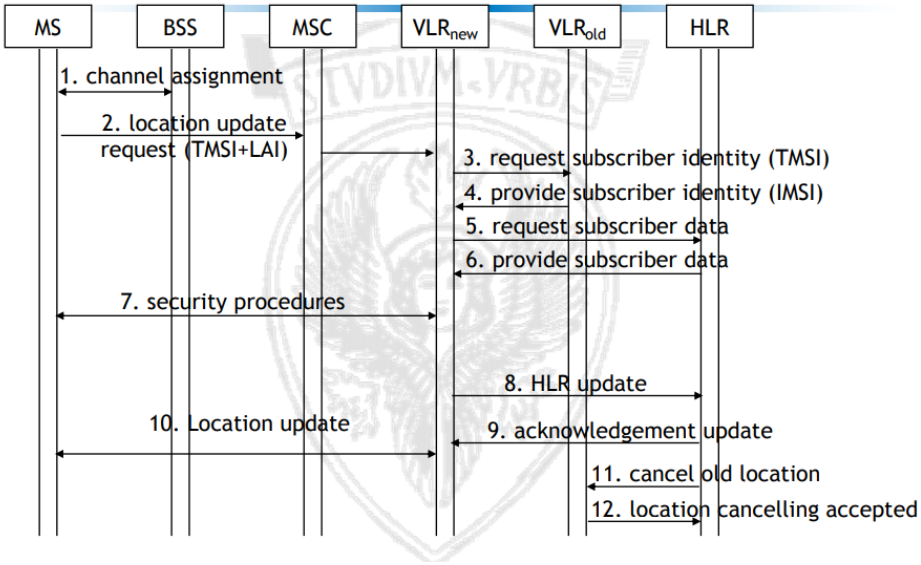
                - Roaming between Las of different MSC/VLRs



LOCATION UPDATING INTRA-MSC



LOCATION UPDATING INTER-MSC



Set up of a call originated via PSTN/ISDN

PSTN/ISDN –call→ MSISDN

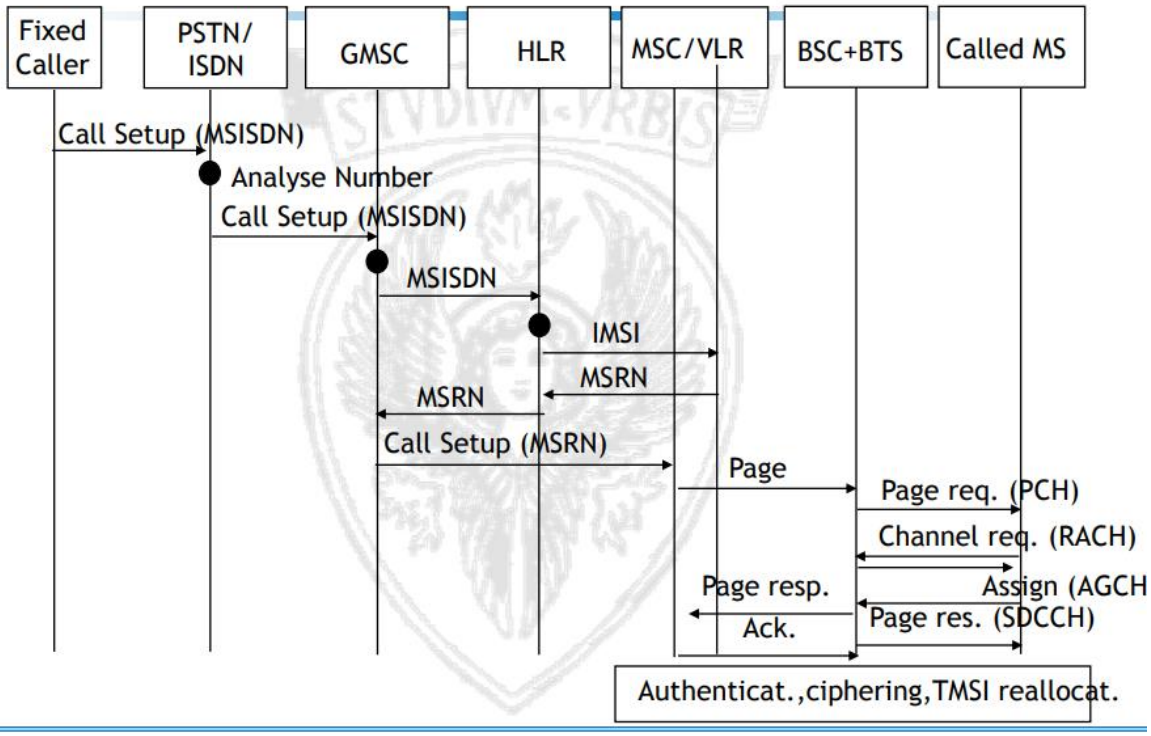
MSISDN : +39 347 6527268

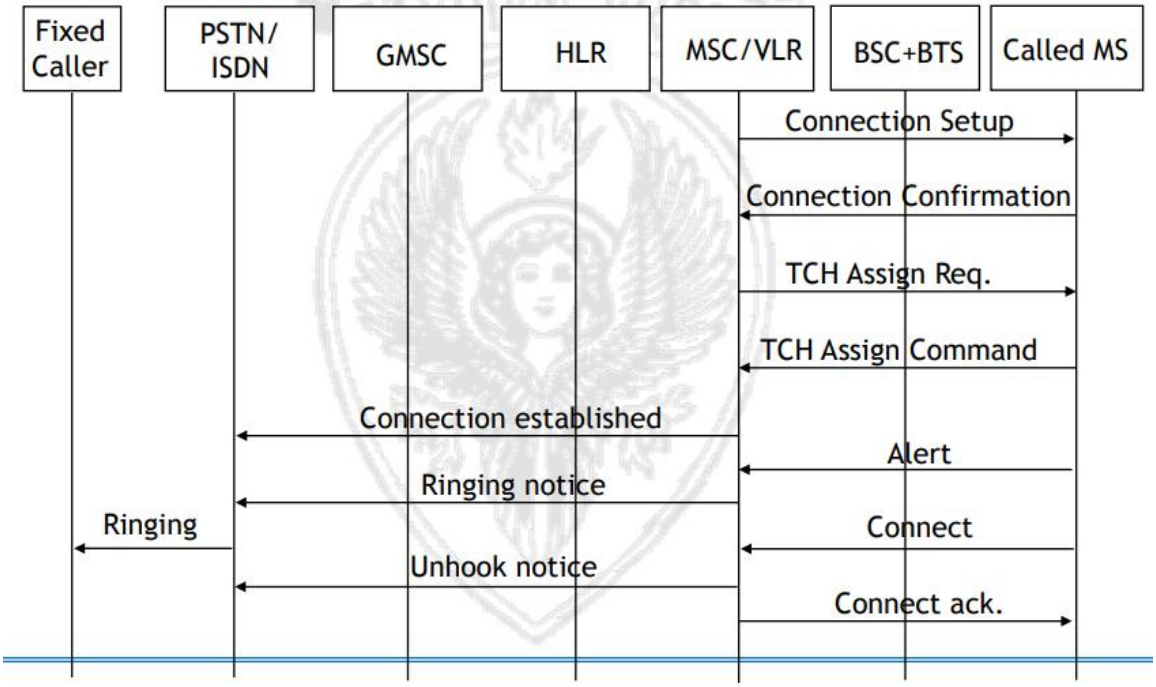
39 = country code

347 = National Destination code

6527268 = subscribe number

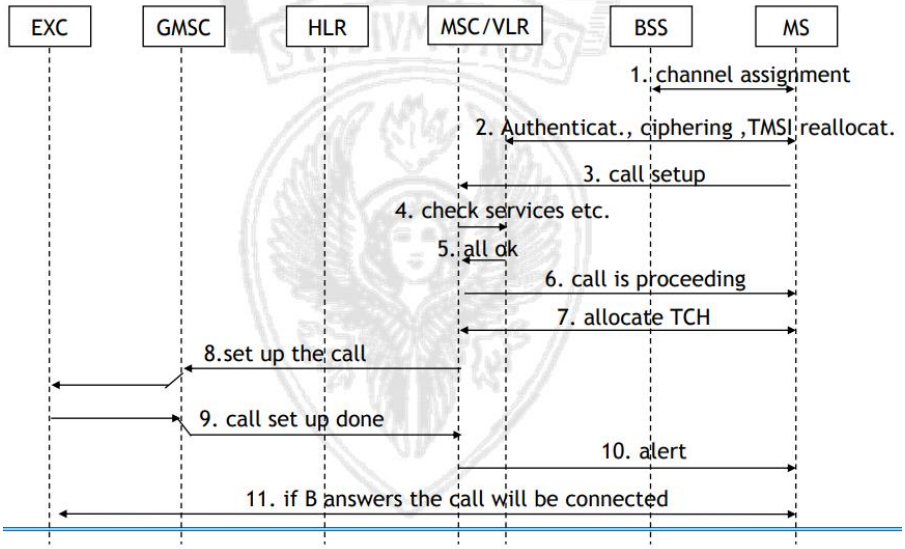
1) The PSTN/ISDN network routes the call to the GMSC of the called user by the National destination code, the GMSC receivers the messages requesting to set-up a call through the SS7 nw which contains the MSISDN of the user called.
2) The GMSC identifies the HLR containing the data of the called user (not aware of the MS position)
3) GMSC sends a message requiring to send routing info to the HLR.
4) The HLR identifies the address of the VLR in which the called MS is currently registered
5) The HLR sends a provide roaming number message to the MSC/VLR
6) The MSC/VLR temporarily allocates a mobile station roaming number to be used for the call
7) MSRN is forwarded by the MSC o the HLR
8) The GMSC routes the call towards the MSC/VLR of the LA in which the MS is currently located
9) MSC/VLR activates the paging procedure
    a. It identifies the currently-visited LA thanks to the IMSI
    b. It sends a paging command to all BSC of the location area
10) BSC requires the BTSs to sed paging message destined to the MS over the paging channel (PCH), this message contains the TMSI assigned to the MS
11) The MS replies to the paging message by requiring a stand alone dedicated control channel (SDCCH) through the random access channel (RACH)
12) The MSC/VLR activates the auth and the ciphering procedures
13) A traffic channel (TCH) is allocated for the communication
14) The MSC/VLR notifies the caller that the called phone is ringing
15) The called user answers the call
16) The connection between the two users is established





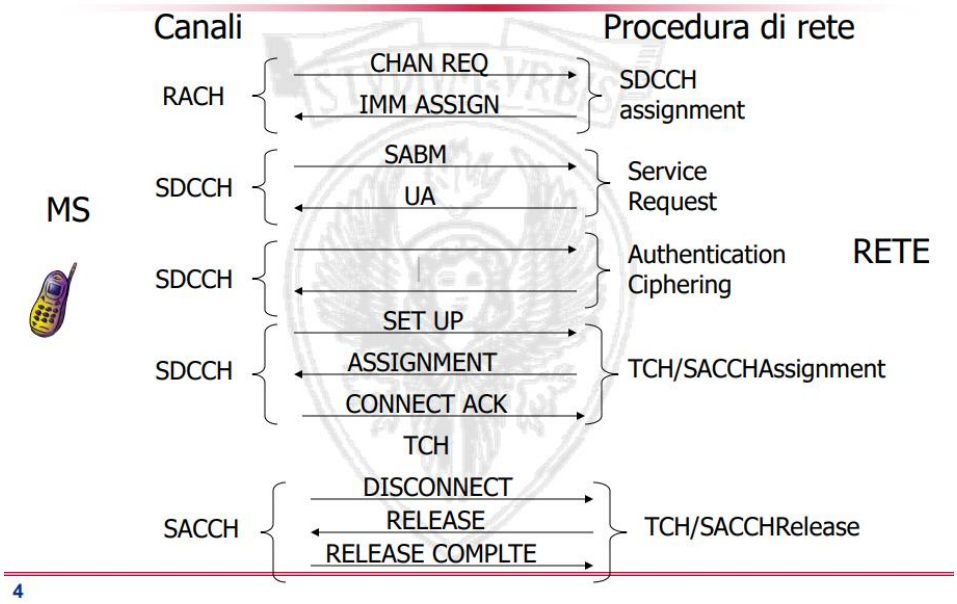
Otherwise if the call is originated by the MS :

- The current MSC analyses the caller data and authorize or deny the call, if authorized 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
    - If the called number is in another GSM network the call is routed to GMSC (Gateway mobile switching center)



Mobile originated call for PSTN :

- Access request, resource allocation for signaling
- Authentication and ciphering, caller id is transmitted, traffic channel is allocated
- Call routing



HANDOVER PROCEDURE

When the MS connects to a cell, the BSC sends to it a list of “alternative channels” (the BCCH of 6 adjacent cells) whose signal strength should be monitored by the MS, those result of measurement are transmitted to the BSC by the MS using the SACCH channel every 480 ms, the handover procedure may be started based on measurements performed by both the MS and BTS.

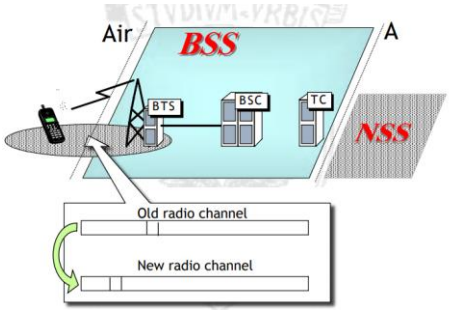
The procedure requires :

- A set of rules to determine whether an handover is necessary
    - Parameters to handover (MS side) :
        - Signal strength on the BCCH carrier of adjacent cells (RXLEVNCELLn)
        - Signal strength on the active TCH channel (RXLEV)
        - Quality of the active TCH channel (RXQUAL)
    - Parameters to handover (BTS side) :
        - Signal strength from the MS on the traffic channel (RXLEV)
        - Quality of the traffic channel from the MS (RXQUAL)
        - Distance of the MS (Timing Advance)
    - Reason for handovers:
        - Low quality transmissions (RXLEV and/or RXQUAL below a given threshold)
        - Distance between the MS and the BTS is above a given threshold

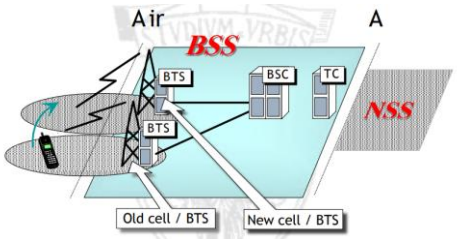
        - Traffic motivation (high load on a cell)
        - Control and maintenance
- Dedicated procedures to commute the communication from the original radio channel to the new channel.
- It has to be transparent to the user.

There are 4 types of handovers :

- Intra cell – intra BSC

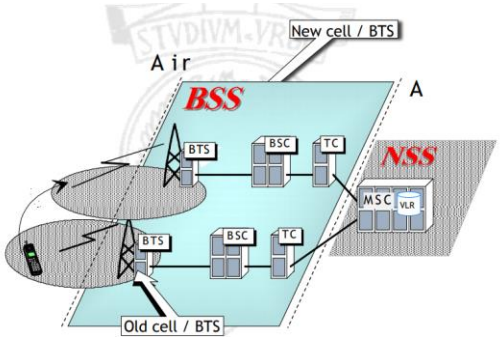


    - Simple handover decided by BSC only
    - A new traffic channel is allocated, usually the frequency within the BTS is modified as well
    - That type of handover is triggered by :
        - Low quality TCH, high received signal strength
        - No adjacent BTS can provide better quality
- Inter cell – Intra BSC



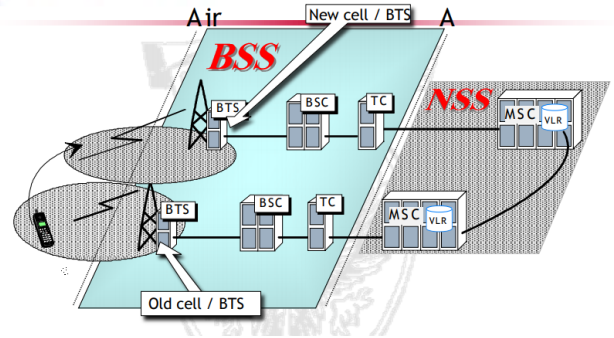
    - The BSC identify the best BTS and the best TCH for the MS based on both MS and BTS measurements.
    - BSC connects to the new BTS and requires the allocation of a new TCH
    - The MS starts sending traffic on the new TCH
    - The old connection is released
    - The BSC notifies the handover to the MSC/VLR
    - After the handover the MS must acquire info about new adjacent cells (via SACCH)
        - If the LA is changed by the handover a location procedure must be triggered by MS

- Inter cell – inter BSC



  - The BSC identifies the best BTS and the best TCH for the MS
  - The current BSC sends a message to the MSC/VLR, as the new BTS is controlled by another BSC
  - The new BSC reserves a radio channel for the MS, which should now use the new radio channel (TCH)
  - The MS starts sending traffic on the new channel. The connection is routed by the MSC toward the new BSC
  - The old connection is released

- Inter MSC



  - The current BSC decides an handover towards a BTS controlled by another MSC/VLR
  - The current BSC sends an handover command to the initial MSC/VLR
  - The initial MSC/VLR sends a request to the final MSC/VLR
  - The final MSC/VLR allocates an HandOver number (HON), which is transmitted to the initial MSC/VLR
    - The HON handover number :
      - HON : CC + NDC + SN
        - Country code
        - National destination code
        - Subscriber number (it is located in HLR if MSISDN otherwise if located in VLR Is HON and MSRN)

        - HON contains enough info to allow the GMSC to route the call towards the destination MSC
    - The destination MSC/VLR starts a connection to the new BSC
    - A traffic channel is reserved to the MS by the new BSC
    - The initial MSC/VLR sends an handover command to the MS by using the FACCH channel of the old BSC and BTS
    - The MS switches to the new channel and starts sending traffic over the new TCH
    - The old connection is released

Widespread of internet usage raises demand for data communication, so the technology has to win some challenges :

- Packet switching
- Data rates must increase
- Data encoding quality must increase
- Need to extend the functionalities of a mobile operator system allow to provide more complex services.

<u>2G + innovation:</u>

- Enhanced full rate codec bahased on ACELP (13kbit/s)
- Adaptive multirate (these channels changes rate depending on channel propagation conditions)
- Tandem free operation (limit use of transcoding that implies degradation of voice quality) allowing multiplexing of flows of coded speech signal.
- Enhanced data rates achieved through improvements of phy layer, and allocation of multiple slots to the same MS.
- Location services granted by triangolarization (100m precision)
- User can maintain the same number even when he changes the operator
- Cordless telephony system
- SIM application toolkit, and can ask for :
    - Set up of a call to a number in the SIM
    - Send telephone numbers the ME is dialing to the SIM that can analyze
    - Pass to the SIM info
    - Execute a command sent by the SIM
    - Launch the microbrowser in the ME redirecting it to a particular WEB address
- Mobile execution environment

<u>EDGE:</u>

That technology show improvements on the radio interfaces increasing gross data range from 22,8Kbit/s to 59,2Kbit/s, without changing the mobile cellular system architecture.

- 3/8 shifted 8PSK modulation → 3 times more bits per symbol

- Carrier bandwdith : 200kHz
- Time slot per frame : 8 , frame saturation 4,615 ms
- Radio interface symbol rate 270ksymbols/s
- Normal burst : 384 payload bits

Adaptive modulation :

- Limits of the high rate modulation at low SNR results in high BER
- A dynamic section of the channel coding and modulation is implemented, which is based on the SNR of the radio channel.
- The net transmission data rate is reduced or increased depending on the quality of the radio channel

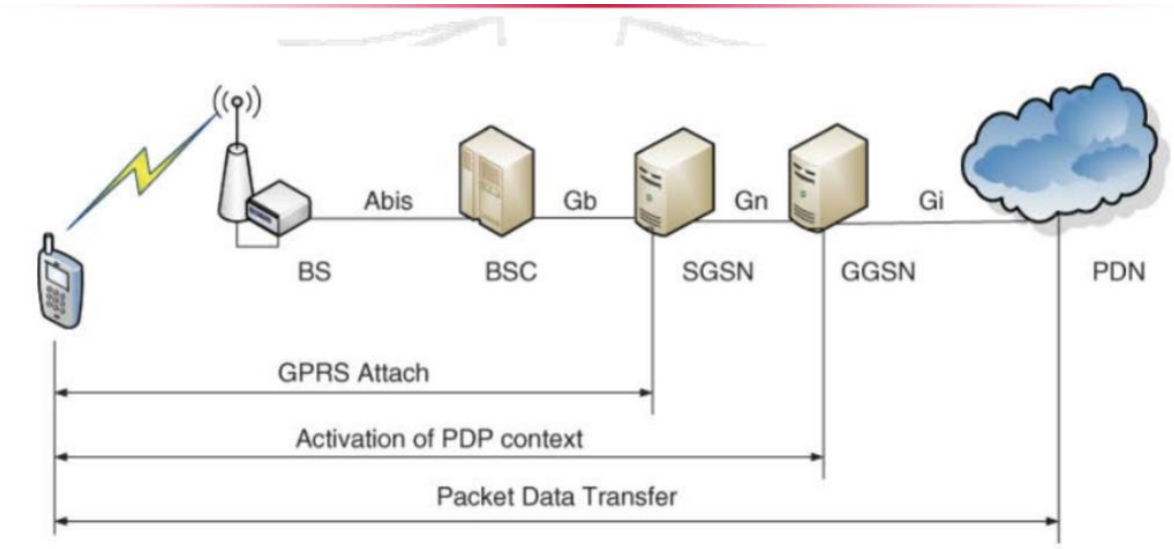
The first technology to support not only voice transmission is GPRS (general packet radio service), IP backbone used for packet switching and It is integrated with the circuit switching networks

- SGSN (GPRS support node) are IP routers supporting mobility management, area is splitted in finer grain routing areas.
- GGSN (gateway , GGSN support node) interfaces cellular network with external packet data networks
- These two (SGSN and GGSN) are connected through an IP backbone
- Network elements must be associated IP addresses
- At the BSSS level a new entity is added denoted PCU (Packet control unit) to manage transmssion over the radio links.
    - The packet control unit (PCU)
        - Deals with dynamic resource allocation between GSM CS and GPRS and to interconnect MS and SGSN for packet data exchange
        - It performs :
            - Segmentation and reassembly
            - Physical channel scheduling
            - Error detection and management (ACK/NAK, buffering, retrasmission)
            - Access request management and resource allocation
            - Channel management (Power control,congestion management, broadcasting of control messages)

    - SGNS-serving GPRS support node
        - Handles user authentication and checks it is entitled to access the service, coordinates encryption
        - Performs mobility management
        - With the BSS radio resource management it reserves radio resources needed to support the requested QoS
        - Gathers information useful for biling

- Routes info flows from/to the MS
- Performs encapsulation and tunneling of the packets
- Performs logical connections management to/from the MS

- GGSN .gateway GPRS support node
  - It interfaces the cellular operator network with external packet data networks
  - Performs routing tasks, encapsulation/decapsulation, analyzes and filters arriving messages, and gather info needed for accounting and billing
  - Stores in its location register the address of the SGSN who are serving the different MS, MS user profiles, and active/standby MS PDP context
    - Upon context it creates PDP context



PDP context activation : (can be requested only after a static IP address is allocated to the MS)

PDP context contains : (it is stored in all SGSN and GGSN)

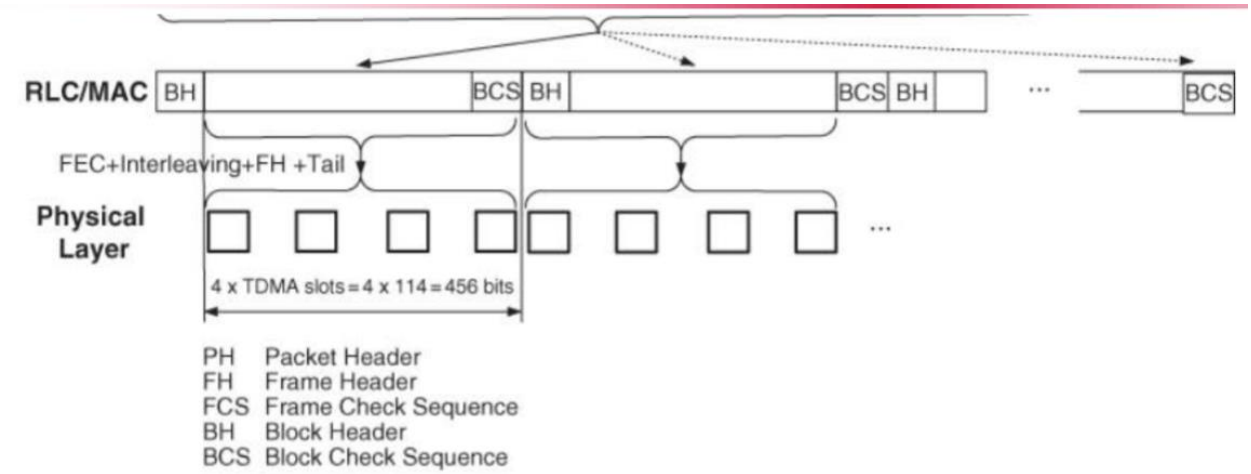
- PDP Type (e.g IPv4)
- Requested Qos class
- The address of the GGSN that servers

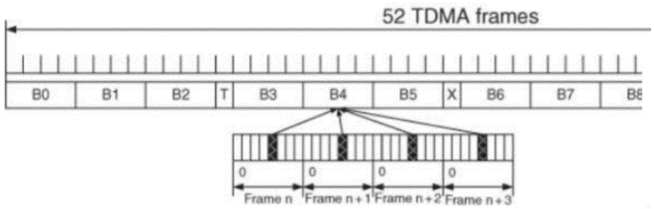
Physical and logical channels

PDCH : Packet data channel, that is a physical channels allocated for data transmission

- Same FDMA/TDMA structure as in GSM

- This physical channel is allocated only for the time needed to transmit data and then released.
- More info (up to 8) can be multiplexed over the same PDCH
- PDCH supports transmission of radio blocks
    - RLC/MAC block + block check sequence
    - 456 bits transmitted in 4 normal bursts → 4 slots in consecutive frames
    - More slots can be allocated in parallel to the same MS



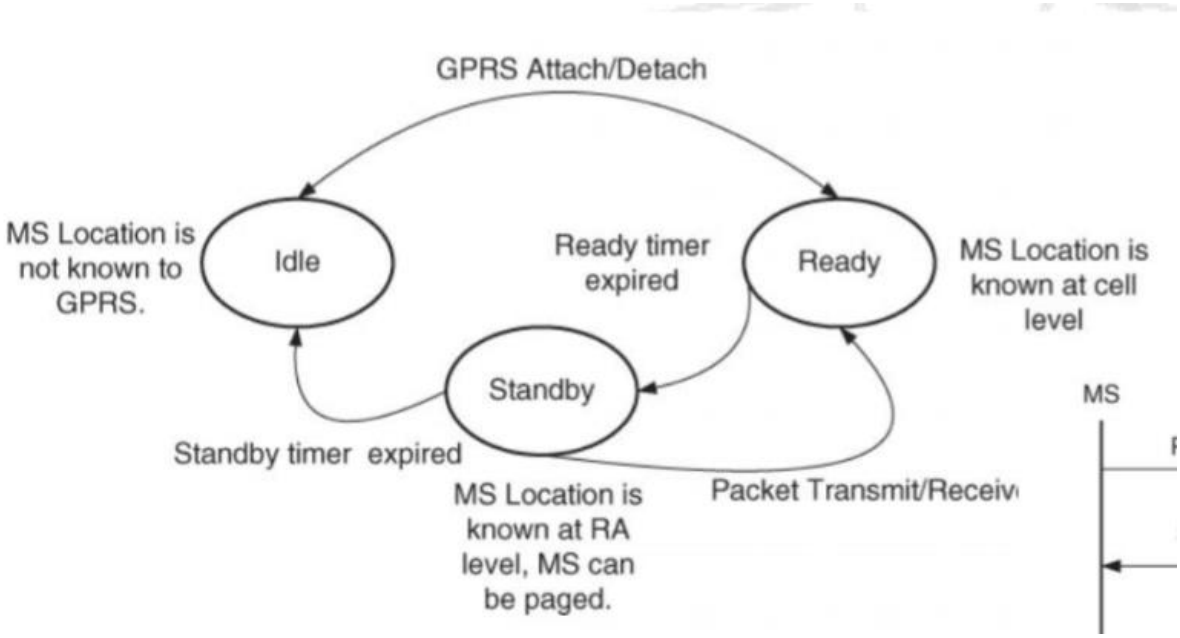


One radio block is allocated four slots in successive frames 4 x 114 = 456 bits.

- Resource allocation:
    - The network allocates resources as a temporary flow block (TBF), which has associated an identity (identity-TFI)
    - Before an MS can communicate it has to request a TBF
    - Once PDU have been transmitted the TBF is released
    - Statistical multiplexing : the network must allocate resources so that different flows can be multiplexed over the same physical channel
        - When communicating in downlink the network give backs the info or which MS should communicate in uplink in the next frame
        - Scheduling

- Control channels :
    - Packet common control channels
        - PPCH (packet paging channel)
        - PRACH (packet random access)
        - PACGH (packet notification channel → downlink channel used to notify a group of MS that there is a traffic for them (point to multipoint)
        - Packet broadcast control channel (PBCCH)
        - Dedicated control channels
            - PACCH (packet associated control channel, bidirectional channel)
                - Info transmitted : power control, ACK/NAK, reassignment of resources, assignment of a downlink PDTCH for MS using an uplink PDTCH.
            - Packet timing advance control channel

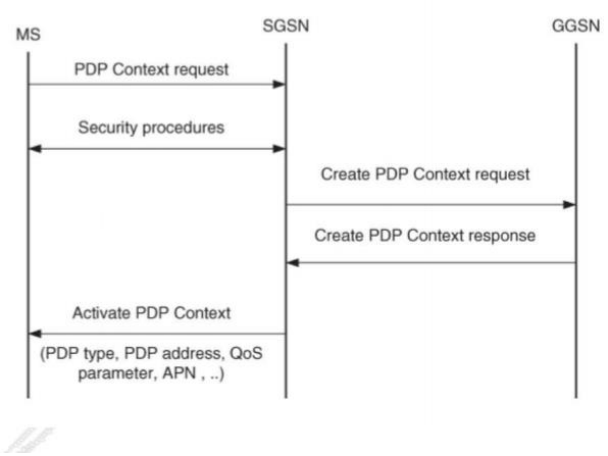
<u>PDP context activation</u>



Ready : Location of an MS known at cell level, data exchange without paging

Standby : State entered after some inactive period, in that state is probably that info about it are maintained at the level of routing area.

Idle : After an MS detach or after a timer expires in standby (no exchange of data in standby) MS move to idle.

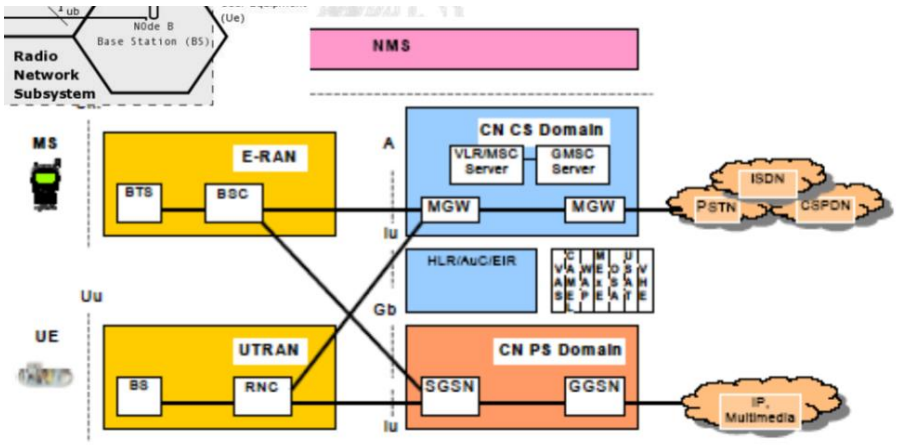


3G systems

These systems has a object a full support of a variety of services and multimedia applications, so different classes of traffic, heterogeneous QoS demands.

Now cells come from Macrocell →Microcell → Picocell and the bandwidth 1885-2025Mhz; 2110-2200Mhz (144Mhz for terrestrial and 75Mhz for satellite networks)

- Them are splitted in 5Mhz channels
- TDD and FDD to divide resources among uplink and downlink
- Support asymmetric services
- Increase of bandwidth to 500MHz



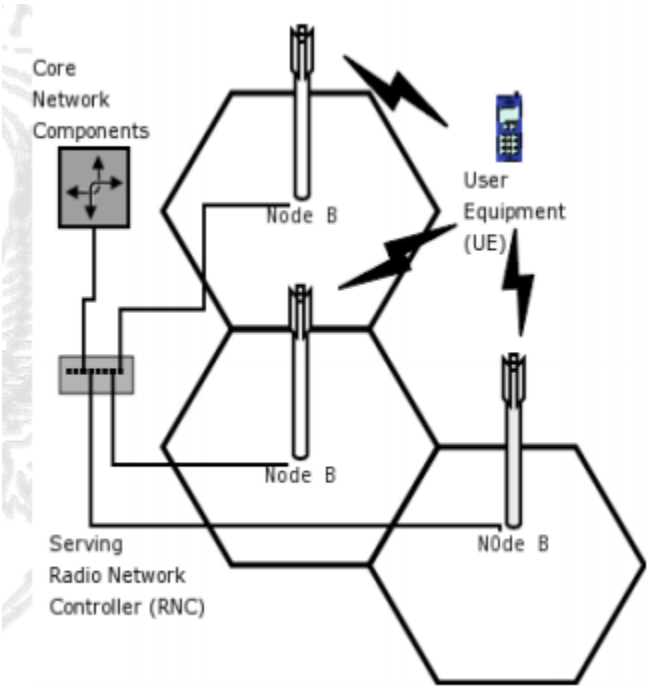
- UTRAN functions
    - Controls cell capacity and interference in order to provide an optimal utilization of the wireless interface resources

- Includes algorithms for power control, handover,packet scheduling, call admission control and load control
- Encryption of the radio channel
- Congestion control to handle situations of the network overload
- System information broadcasting
- Micro and macro diversity

- Network functions of UTRAN
  - Packet scheduling
    - Controls the UMTS packet access
    - Handles all non real time traffic
    - Decides when a packet transmission is initiated and the bit rate to be used
  - Load control
    - Ensures system stability and that the network does not enter an overload state
      - Decides whether or not a call is allowed to generate traffic in the network

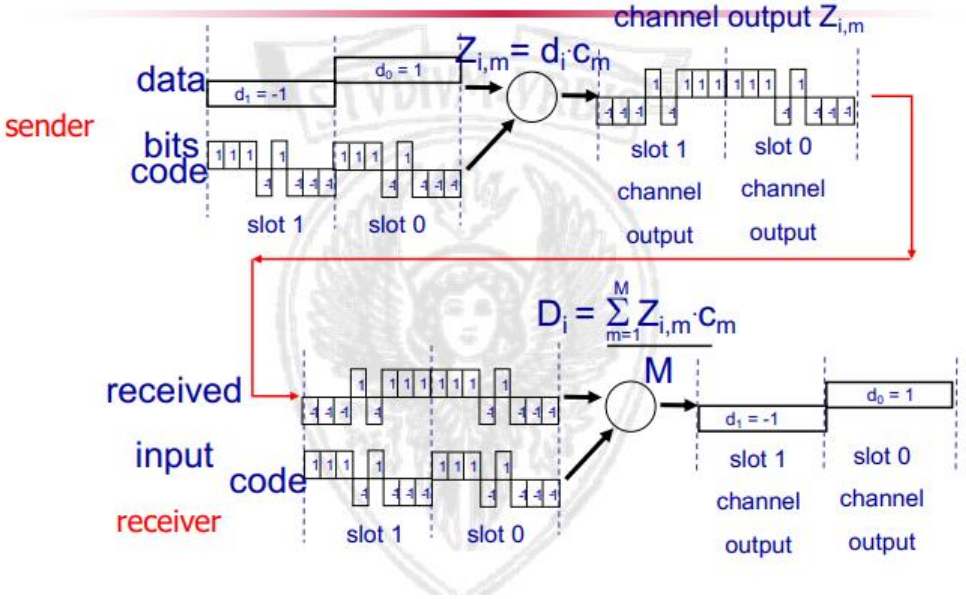
Macrodiversity :

- Same data stream is sent over different physical channels
  - Uplink – UE sends its data to different node B
    - Data stream is reassembled, reconstructed in Node B, SRNC or NC
  - Downlink – receiving same data from different cells on different spread codes



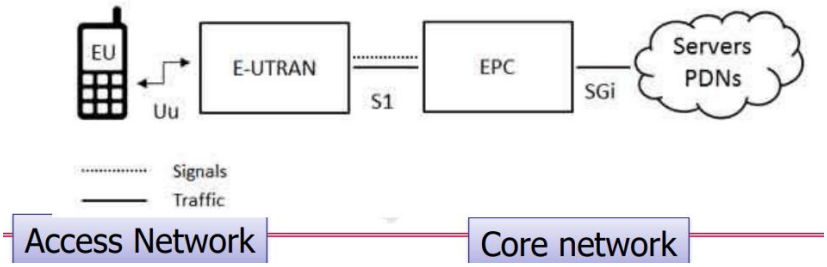
CDMA

- Unique code assigned to each user
- All users share same frequency, but each user has own “chipping” sequence to encode data
- Encoded signal = (original data) x (chipping sequence), so for decode is the inner-product between encoded signal and chipping sequence
- Signals are orthogonal, so allows more users to transmit with low interference

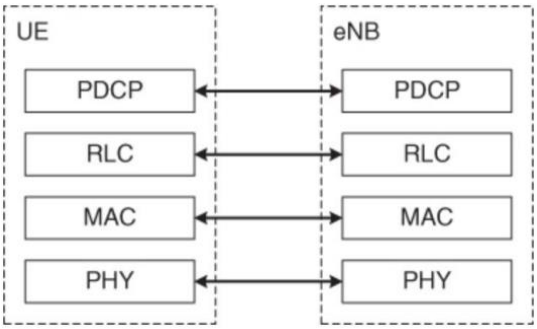


4G – LTE

It is the system we use nowadays, even if scientists started to think about it in 2005. Here, data rate is increased even more than previous system. But there are also other news such as improved spectral efficiency, reduced delays, low energy and power consumption, a lot of active users per cell and many others. Extending the bandwith and improving the spectral efficiency (increase the bit send for Hz unity) are two way used to increase the data rate.
New technologies have been introduced: Muticarrier technology (OFDMA), Multiantenna technology and a new system of packet switching (bearer concept).
Network elements are callled in another way: radio interface (E-UTRAN) and the backbone (EPC).
Nodes B became eNode Band some elements were introduced in the core network (EPC):



RAN architecture :

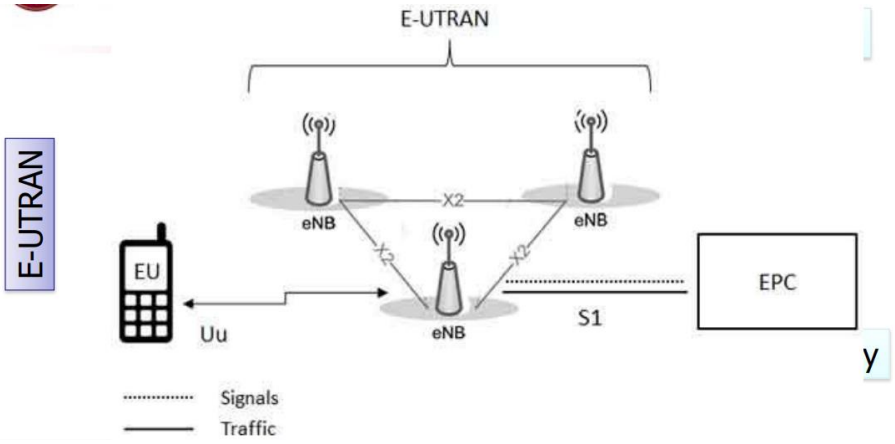


-PDCP performs IP heard compressions and produces output PDCP-PDU.
-RLC protocol is responsible for segmenting of the PDCP-PDU for radio interface transmissions and performs error correction.
-MAC is responsible for scheduling the data according to priorities
-PHY coding and modulation, antenna and resource mapping

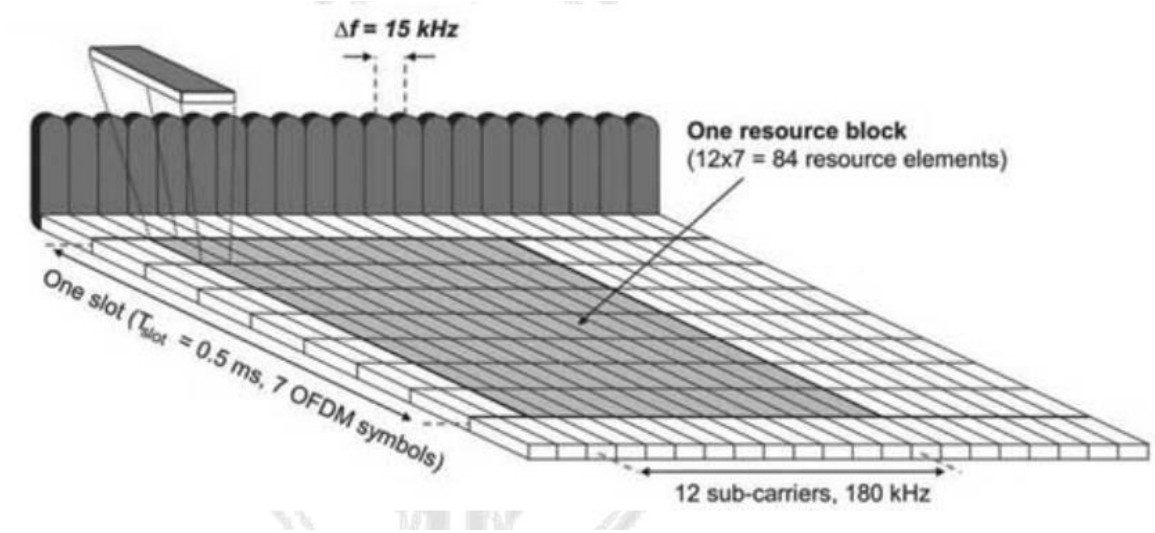
- Home Subscriber Server (HSS): User subscription data, identity of the MME the user is connected to, authetication center
- P-GW: address allocation to UE and QoS enforcement in downlink
- S-GW: transport the IP data traffic between the UE and the external network
- MME (Mobility Management Entity): connection set up including paging within a tracking area and security tasks

Bearers guarantees the minimum bit rate. The eNodeB in the access network ensures the necessary QoS for a bearer over the radio interface. Each one of them has an associated QoS Class Identifier and an Allocation and Retention Priority.
The scheduler in the eNodeB distributes the available radio resources in one cell among all different UEs. Each eNodeB allocates downlink and uplink radio resources to each UE basing on channel quality indicator reports.

- Dynamic scheduling : assignment of downlink transmission resources and uplink grant messages for the allocation of uplink transmission resources
- Persistent scheduling : resources are semi-statically configured and allocated to a UE for a long period.



LTE is based on orthogonal frequency-division multiplexing (OFDM), the OFDM symbols are grouped into resources blocks(180kHZ in frequency and 0.5ms in time domain). The resources blocks are allocated for different users in the timefrequency grid. The more resource blocks a user gets, the higher the Bit-Rate is.



- LTE brings up to 50 times performance improvement
- 300Mbps peak downlink and 75 Mbps peak uplink
- LTE supports flexible carrier bandwidths (from 1,4MHz up to 20 MHz, both FDD and TDD)
- LTE devices have to support MIMO transmissions, allowing BS to transmit several data streams over the carrier simultaneously
- All interfaces are IP based
- QoS mechanism have been standardized on all interfaces
- Works with previous technology and allow new spectrum, supports hand-over and roaming to existing mobile networks

5G

The large amount of data we exchange nowadays (mobile and IoT devices) requires a new infrastructure and a new technology, which increase all the features we have seen until now, such as data rate and so on. We need new technologies which support connectivity at high speed and high computing power also for cheap devices. This bring us to introduce a new technology, which is discussed in nowadays and it is not full developed yet: it is 5G. Lets see some features of this new technology which have been already standardized:

- Throughput: provide 1000x more available throughput in aggregate, as weel as 10x more speed to individual end users
- Latency: down to 1ms when needed for tactile internet

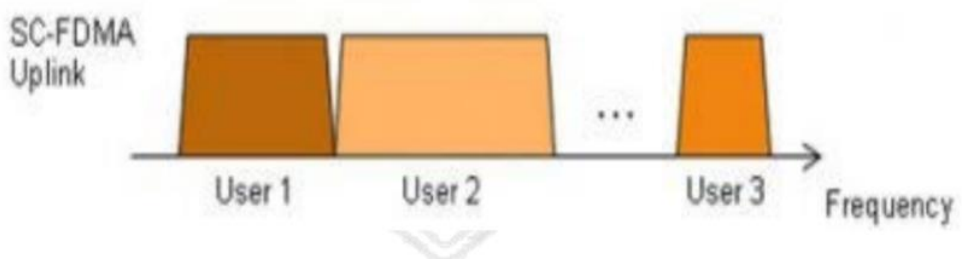
• Energy efficiency: 90% increase in energy efficiency and 10x battery lifetime for low power devices
• Large coverage

There are also some challenge that 5G wants to win, lets see some of them:

• Diversity Challenge: support the increasing diversity of wireless solutions, traffic and devices connected
• Multi-tenancy Challenge: provide services across different infrastructures ownership, with different network coexisting and providing an integrated efficient interaction between mobile systems
• Density Challenge: billions of devices, increased even more by the coming of IoT devices
• Security Challenge: making communication systems robust to attack and natural disasters
• Mobility Challenge: seamless mobility across networks/technologies
• Harvesting Challenge: exploit energy harvesting to improve lifetime
• Flexibility Challenge: devices truly flexible control mechanism no protocol for relocating functions, protocol entities and states relying on technologies such as SDN and NFV
• Identity Challenge: provide identity management or any type of device with access agnostic authentication mechanism.

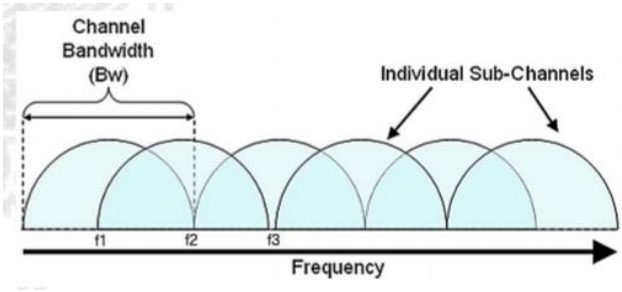
All these objectives can be achieved only introducing some new communication techonogies developed in these years, such as: MIMO, antenna arrays, Beamforming, novel modulations and so on.

Single carrier FDMA (SC-FDMA)



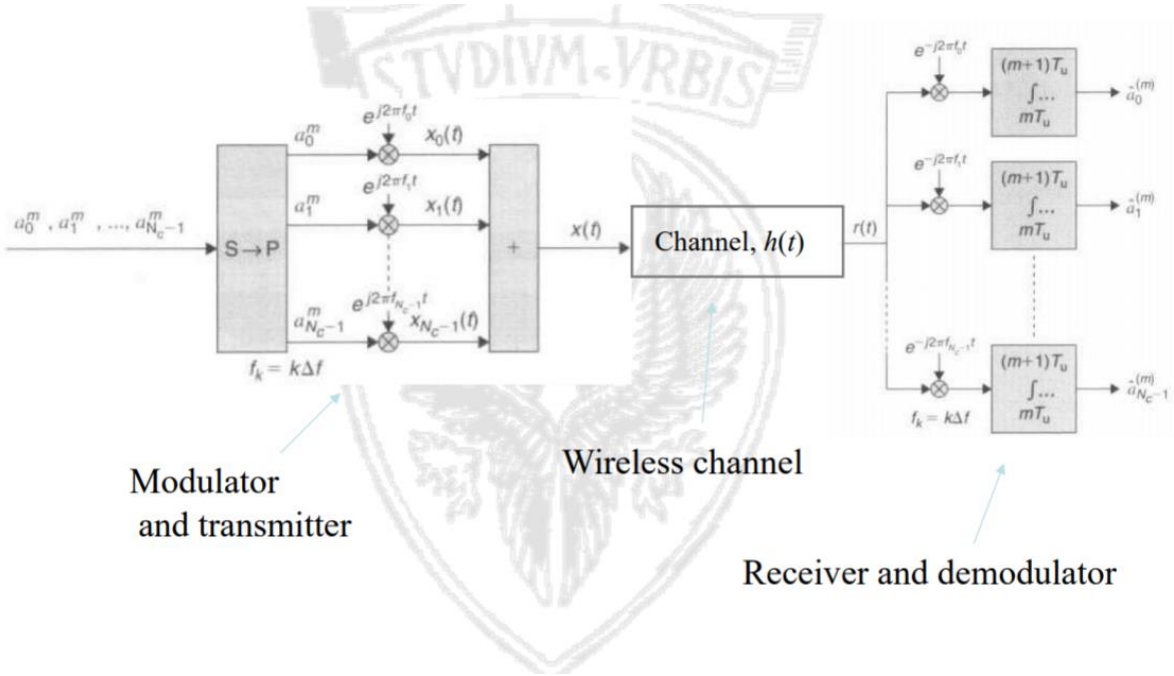
- Linearly pre-coded OFDMA
- Single carrier modulation and orthogonal frequency multiplexing using DTF-spreading in the transmitter and frequency domain equalization in the receiver
- Low PAPR respect to OFDMA

What is OFDM(A)? :



OFDM is a special case of frequency division multiplexing, carriers are orthogonal to each other and can be packed tight, there is a strict relation between carriers : $f_k = k \cdot \Delta f$ where $\Delta f = 1/T_U$ (T_U is the symbol period)

- Sub-band spectral interface, with 64 adjacent sub-bands (WiFi), there is clearly a danger of inter spectrum interference or inter-carrier interference, also danger of spectrum leaking outside the OFDM band.
- That modulation is highly efficient because sub carriers are as close as they can possibly be
- The bit-rate using N sub-channels is 1/N of the total bit-rate
- Zero-crossing of sinc spectra, so the sinc spectra die away must faster



$$\frac{1}{T_U}\int_0^{T_U}\underbrace{\left(\sum_{q=0}^{N_c-1} a_q \cdot e^{j2\pi q\Delta f t}\right)}_{\text{Received signal, } r(t)} \cdot e^{-j2\pi k\Delta f t}dt = \sum_{q=0}^{N_c-1}\frac{a_q}{T_U}\int_0^{T_U} e^{j2\pi(q-k)\frac{1}{T_U}\cdot t}dt = \begin{cases} a_k, & k=q \\ 0, & k\neq q \end{cases}$$

$T_u = 1/\Delta f$ gives subcarrier orthogonality over one T_u
=> possible to separate subcarriers in receiver

There are more modulation for the sub-carriers :

- BPSK = 2 phase shifts, 1 amplitude level, 1 bit/symbol
- QPSK = 4 phase shifts, 1 amplitude level, 2 bits/symbol
- QAM-16 = 4 phase shifts, 4 amplitude levels, 4 bits/symbol
- QAM-64 = 4 phase shifts, 16 amplitude levels, 6 bits/symbol

Example of OFDM

- Lets we have following information bits
  1, 1, -1, -1, 1, 1, 1, -1, 1, -1, -1, -1, -1, 1, -1, -1, ...
- Just converts the serials bits to parallel bits

C1	C2	C3	C4
1	1	-1	-1
1	1	1	-1
1	-1	-1	-1
-1	1	-1	-1
-1	1	1	-1
-1	-1	1	1

Cyclic prefix length:

Tcp should cover the maximum length of the time dispersion (If Tcp = 0,8 microsec) and speed of radio waves is circa 300x10^6 m/s this allows for a path length difference of 00.8x300 = 250m

Increasing Tcp implies increased overhead in power and bandwidth

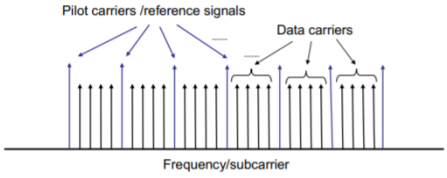
For large transmission distances there is a trade-off between power loss and time dispersion

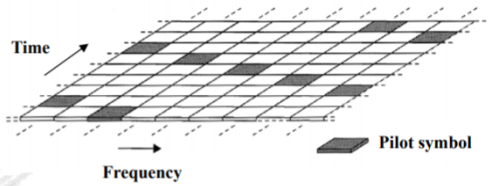
The OFDM symbol can be exposed to a frequency selective channel, the attenuation for each subcarrier can be viewed as flat due to the cyclic prefix there is no need for a complex equalizer

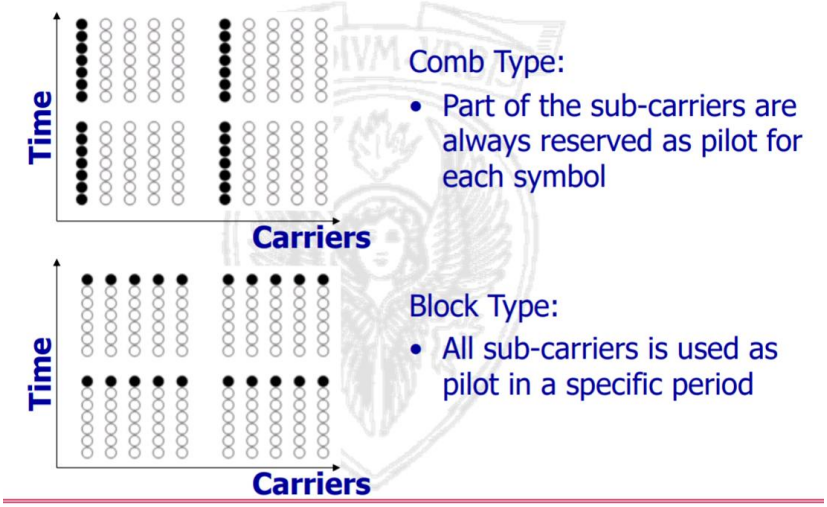
- Transmission techniques :
    - FEC over the frequency band
    - Adaptive coding and modulation per carrier

On a multipath channel :

- The channel parameters can be estimated based on known symbols(pilot symbols)
- The pilot symbols should have sufficient density to provide estimates with good quality (tradeoff with efficiency), estimation methods :
    - Averaging combined with interpolation
    - Minimum mean square error





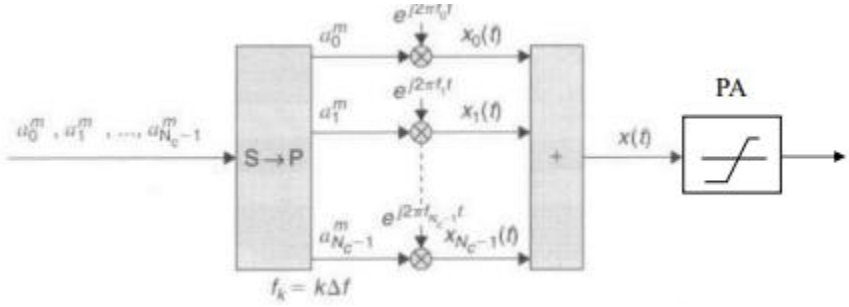


Problems with OFDMA

- Peak to average power ratio (PAPR) : when a sub-carriers are added coherently, the instantaneous power will be more that the average power.
    - The sum of independently modulated subcarriers can have large amplitude variations

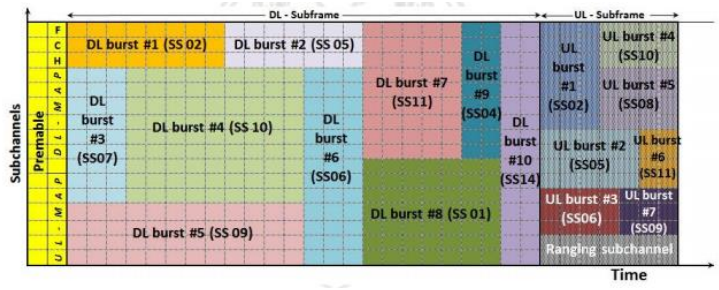
$$x(t) = \sum_{k=0}^{N_c - 1} a_k \cdot e^{j2\pi k \Delta f t}$$

        - High efficiency power amplifiers are desirable for handset (long battery life) and for base station (reduced operating costs)
        - A large PAPR is negative for the power amplifier efficiency
        - Non linearity results in inter-modulation
            - Degrades BER performance
            - Out of band radiation
    - There are more tools to deal with PAPR problem :
        - Signal distortion techniques (tradeoff with respect to reduced backoff)
        - Coding techniques: FEC codes excludes OFDM symbols with a large PAPR, tone reservation and pre-coding are other examples.
        - Scrambling techniques (Different scrambling sequences are applied and the smallest PAPR is chosen
    - Signal goes into nonlinear region of operation of the power amplifier (PA) at the transmitter

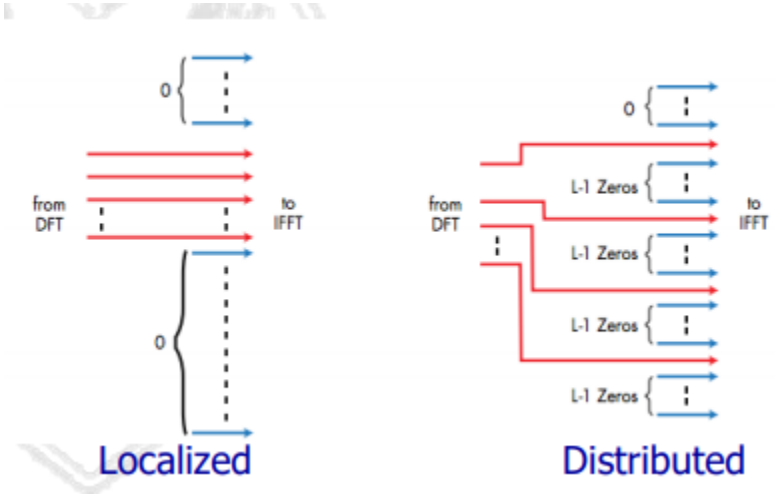


- Carrier frequency offset : Necessity of accurate frequency sync between the receiver and the transmitter. With frequency deviation, the sub-carriers will no longer be orthogonal causing ICI

OFDMA Structure



- Flexible bandwidth from 1.4 to 20 MHz
- Transmitters inserts null sub-carriers at position assigned to other users, there are two types :



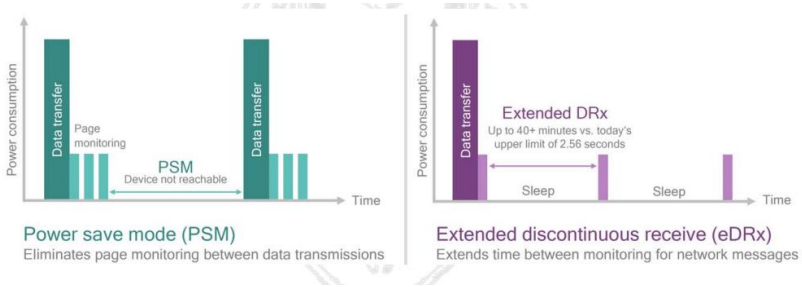
OFDM summary :

- Splitting the channel into narrowband channels (enable significant simplification of equalizer design)
- Effective implementation applying FFT
- Flexible bandwidths enable through scalable number of sub-channels
- Possible to exploit both frequency and time domain
- It is used in TVB,DSL,WLANs, 4/5G

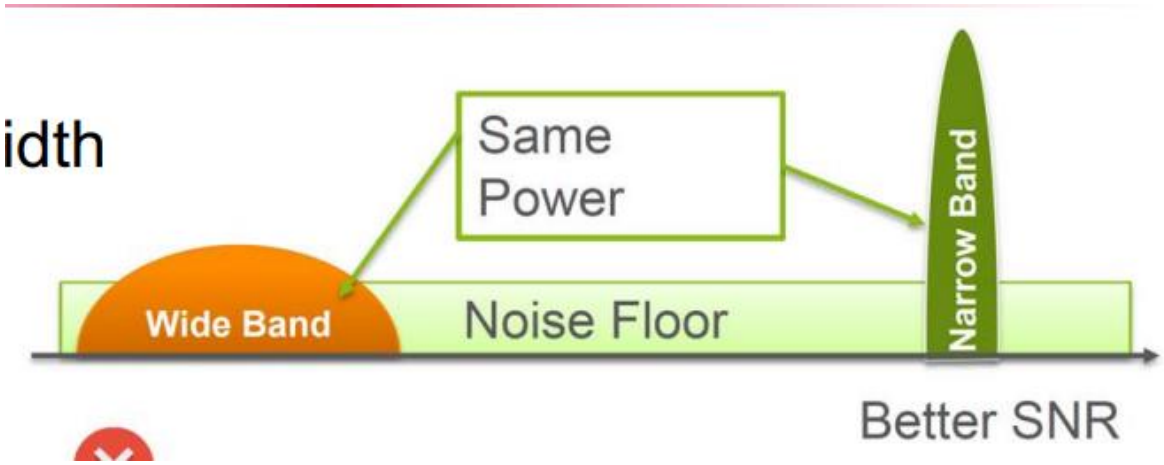
IoT utilization of OFDM

- Low power wide area (LPWA) networks
    - Battery duration (10y)
        - UEs with lower transmission power

- Sleep/idle/ready states



  - Optimized for the transmission of brief messages
  - Low cost module
    - Allowed by already created spectrum for cellular
  - Coverage I the order of 10s of km for a cell
  - Every environment coverage (outdoor, indoor …)
    - Smaller bandwidth, repetitions
  - Narrowband modulation



  - Short time to market
  - Massive use of devices
  - End to end secure connectivity

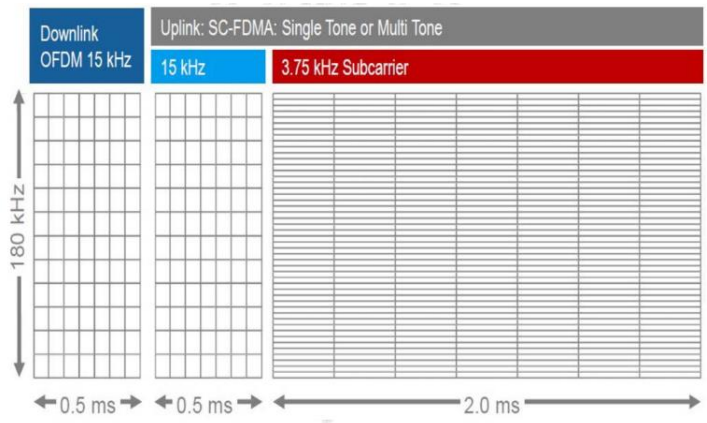
LPWA are divided in 2 main fields :

- ISM Band
  - LoRa
  - SigFox
  - RPMS
- Licensed spectrum
  - 3GPP LTE
    - LTE-M
    - NB-IOT

Feature	LORAWAN	SIGFOX	LTE Cat 1	LTE M	NB - LTE
Modulation	SS chip	UNB / GFSK / BPSK	OFDMA	OFDMA	OFDMA
Rx Bandwith	500 – 125 KHz	100 Hz	20 MHz	20 – 1.4 MHz	200 KHz
Data Rate	290bps – 50Kbps	100 bit / sec 12 / 8 bytes Max	10 Mbit /sec	200 kbps – 1 Mbps	Average 20K bit / sec
Max. # Msgs/day	Unlimited	UL: 140 msgs / day	Unlimited	Unlimited	Unlimited

IoT networks are supposed to provide connectivity over cellular networks, so reutilization of the core network and already cellular coverage.

- EC-GSM-IoT (enhanced GSM)
- LTE-M (enhanced LTE with power saving)
- NB-IoT (low end market radio frequency)
    - Very narrowband 180kHz (in-band, guard-band, stand-alone)
    - Extended coverage : 164 dB link (144dB GPRS , 142,7 dB LTE)
    - Long battery life 10y
    - Massive number of devices 50.000/cell
    - Reuses the LTE design extensively
    - HW for existing LTE
    - It supports two modes for Uplink
        - Single tone (15kHz and/or 3.75 kHz tone spacing)
        - Multiple tone (15kHz tone spacing)



    - Repetitions have different coverage classes
        - Variable number of repetitions : 1,2,4,8 ,..
            - Them achieve extra coverage (up to 20db compared to GPRS)
        - Up to 128 (UL) and 2048 (DL)
        - Normal (outdoor MCL 144db)
        - Robust (outdoor MCL 154db)

- Extreme (deep indoor/underground MCL 164db)
- MTU size 1500B
- Maximum transport block size : 680DL 1000UL

	eMTC (LTE Cat M1)	NB-IOT
Deployment	In-band LTE	In-band & Guard-band LTE, standalone
Coverage*	155.7 dB	164 dB for standalone, FFS others
Downlink	OFDMA, 15 KHz tone spacing, Turbo Code, 16 QAM, 1 Rx	OFDMA, 15 KHz tone spacing, TBCC, 1 Rx
Uplink	SC-FDMA, 15 KHz tone spacing Turbo code, 16 QAM	Single tone, 15 KHz and 3.75 KHz spacing SC-FDMA, 15 KHz tone spacing, Turbo code
Bandwidth	1.08 MHz	180 KHz
Peak rate (DL/UL)	1 Mbps for DL and UL	DL: ~250 kbps UL: ~250 for multi-tone, ~20 kbps for single tone
Duplexing	FD & HD (type B), FDD & TDD	HD (type B), FDD
Power saving	PSM, ext. I-DRX, C-DRX	PSM, ext. I-DRX, C-DRX
Power class	23 dBm, 20 dBm	23 dBm, others TBD

IoT ad hoc network

It is a wireless nw multi-hop infrastructure-les whose devices act as source/destination of messages and as a relay for packets, so it has no need for infrastructure (low cost), but must be sef-organizied,self-configurated and self-maintained.

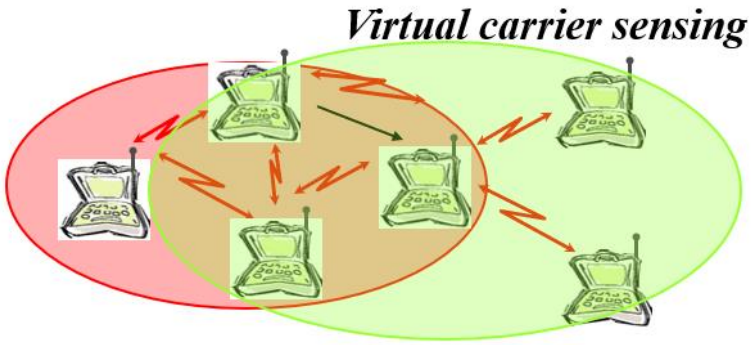
These networks are used :

- Disaster recovery applications
- Military nw
- Personal area nw
- Home nw
- Wireless sensors nw and IoT
- Inter vehicular communication
- Mesh nw

Must be highly dynamic nw → device mobility, awake/sleep modes, low power consumption(that is the real bottleneck, memory also is bottleneck), low overhead and simple protocols(code must be simple), usually 10-100 nodes.

Medium access control to that nw type : CSMA/CA

- Before transmitting a frame the sender node x performs carrier sensing
- If the channel is free for a DIFS time node x transmits the packet
    - Otherwise (if channel in use) node x waits for the end of current transmissions + random backoff time (the count of the backoff timer is frozen until the channel is busy)
        - When backoff timer is 0, the device transmit the packet
        - The backoff timer value is randomly picked within a window interval of CW slots (initially 16slots then doubled to max 1024 slots)
        - Packet is successfully received after ACK and SIFS<DIFS
- To mitigate hidden terminal phenomenon DCF uses virtual carrier sensing (Red – RTS , GREEN – CTS)



    - Before transmitting the sender performs carrier sensing waiting for DIFS (distributed interframe space) and then transmit a packet towards the destination(RTS, request to send)
        - RTS includes :
            - NAV (network allocation vector) = time of RTS exception – end of handshake (ACK reception) , looking at that value ,the devices can estimate when they not to transmit
    - After CTS (clear to send)
        - All destination neighbors will know that the channel is busy and for how long
        - So now the sender transmit the DATA packet (after SIFS)
        - Upon receiving the DATA packet, the destination waits for a SIFS and then sends the ACK
    - If handshake is not correctly completed the node performs a retransmission attempt after an exponential backoff.

Routing approach

- Intra-AS (OSPF routing protocol)
- Link state approaches
    - Each node periodically send info on its neighbors (flooding)
    - Updates can be sent also in case of changes

    - Running Dijkstra
- Distance vector approaches (RIP)
    - With this approach every router calculate distance from the neighbors, usually with bellman-ford algorithm, every router has a table with every known destination:distance:first step to do to reach it
- Bellman-ford
    - Given a graph G=(N,A) and node s find the shortest path from s to every node in N
    - In real world is used distributed bellman-ford (I need to know the best routes among each pair of nodes)

$$D^{h+1}_i = \min_k [c_{i,k} + D^h_k]$$

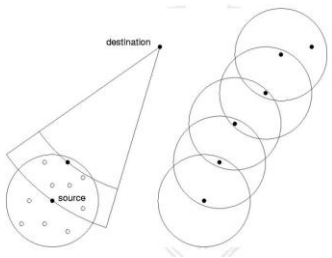
Some of the routing problem are affected by count to infinity, these are some solutions :

- Bounded network diameter (RIP)
    - TTL to discard all packets that have traversed more that x hops
- Split horizon with poison reverse
    - Limit transmitted info
    - Broadcast cannot be used to send updates
    - Does not solve all loop situation
- Trigger updates (to fast converge)
    - Updates are transmitted immediately to fast converge (flooding)

<u>Ad-hoc network routing:</u>

GeRaF:

- Geographic routing
    - Each nodes needs to know its location, the destination and the location of whom is transmitting
    - Greedy approach : tries to select relays so to advance as much as possible toward the destination



    - Example of GeRaF operation
        - RTS invites all awake neighbors to become a relay
        - Nodes in best position should win
            - Nodes within tx range are divided in areas depending on how close they are to destination
            - These nodes sends RTS with the identity of the area → each nodes upon receiving the RTS, decides whether it belongs to the polled area or not.
            - Only nodes in the polled area answer with a CTS
                - No answer → no nodes in the area or sleeping
                - One answer → CTS correctly received → send DATA
                - Multiple answers → Collision (MAC needed to resolve)
                    - LOOP CTS (with probability p) until only one node answer
        - That algorithm introduce a jitter to know how good the potentially relay is (best relay answer first)
    - Dead-ends problem (can't reach my destination)
        - We can set a maximum number of attempts to find a relay
- Awake/asleep schedule
- MAC

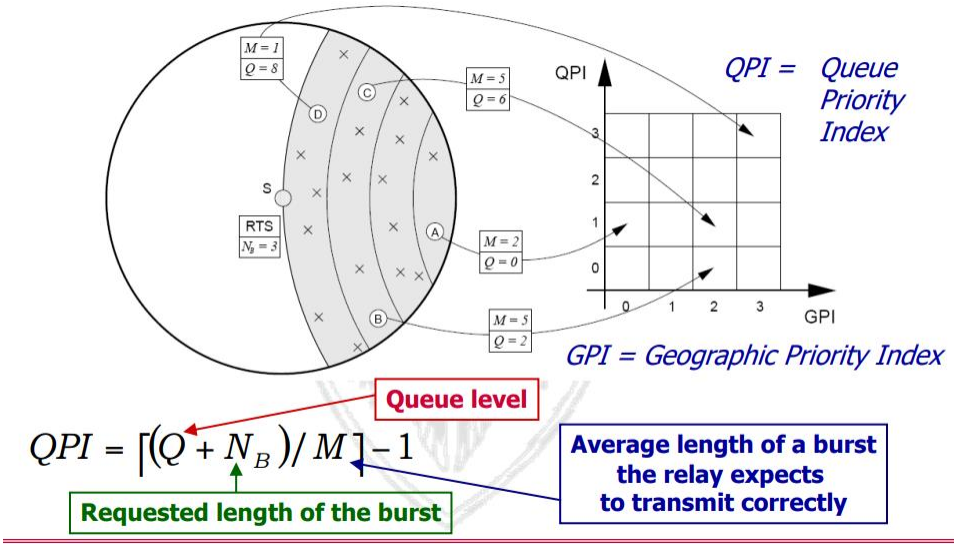
<u>ALBA (cross-layer integrated protocol stack for medium-large scale wireless sensor networks)</u>

- Geographic routing paradigm (forward the packet to a node that offers geo advancement toward the destination)
    - PRO : virtually stateless (need only knowledge of the source's and the destination's locations)
    - CONS:
        - Position estimation
        - Need to resolve dead ends
            - Planarizing the network graph
                - PROS : guarantee delivery
                - CONS: planarization overhead prone to location and channel errors

ALBA is adaptive so :

- Nodes forward packets in burst (adapted burst)
- Forwarder are elected based on :
    - The ability to receive and correctly forward packets
        - The used metrics involves :

- Queue level, past transmission history and # of packets that render needs to transmit
- Geographic proximity to the destination



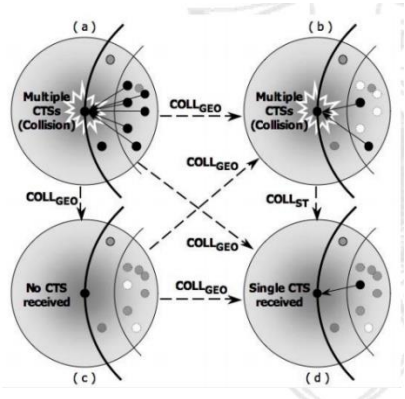
Metrics used to the choice of the relay ensures load balancing as it chooses relays with :

- Low queue
- Good forwarding history
- Nodes emloy duty-cycling to enforce energy saving

That relay selection works in phases :

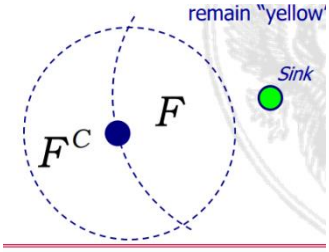
- 1 Selection of the best QPI
  - Awaking nodes can participate in this selection phase
- 2 Selection of the best GPI
  - Performed if more than one node with the same QPI was found

<u>Collision resolution algorithm :</u>



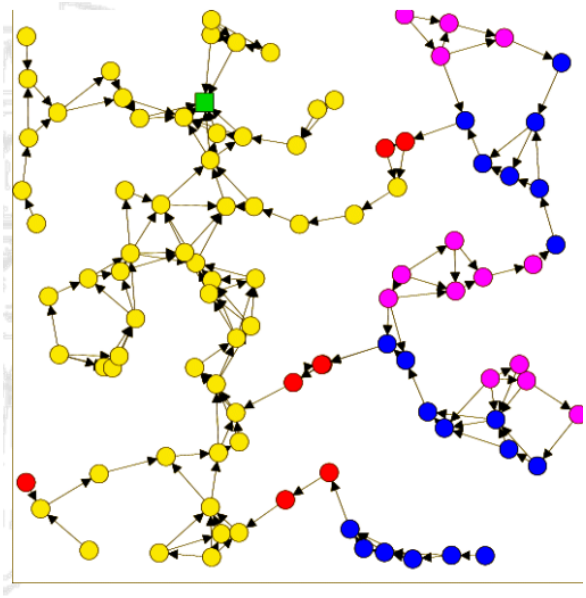
a) Upon receiving a COLLgeo msg nodes reply based on their GPI
b) Upon receiving a COLLgeo msg nodes persist in sending CTSs with p=0.5
c) If all silent → COLLgeo enables further decision
d) Eventually the process ends with a single valid relay

Rainbow node coloring scheme



F and F^C are positive and negative advancement areas.

1) Initially all nodes are yellow → all nodes exhibit a greedy path to the sink remain yellow.
2) If a yellow nodes cannot forward packets further, it switches to red



3) If red nodes cannot advance packets turn to blue
4) If blue nodes still have problems finding relays they switch color again to violet

More in general, given h labels (C1,C1,C3,..,Ch), the nodes switch from a label to the following one evey time they perceive to be a dead end, so Ck will always look for Ck or Ck-1 nodes.

Localization in sensor networks:

- Basic step : evaluate distance between two nodes (ranging), different techniques depending on the HW
    - AoA
    - RSS
    - ToA

    - Simple geometric relationship finding intersections of the lines
    - Radiolocation based on angle of arrival
        - Directive antennas + compass
    - Distance via received signal strength
        - Each measurement gives a circle on which the MS must lie
    - Distance via time of arrival
        - Distance = time * c
        - Each measurement gives a circle on which the MS must lie

Iterative multilateration:

- Nodes that estimates their locations can become beacons and help other nodes discover their locations.

- Range free approaches (number of hops are used to estimate the distance between them)
    - Anchors know their position according to a common coordinate system
    - All nodes compute shortest path between them and anchors, also anchors computer distance in hops
    - Triangolarization.