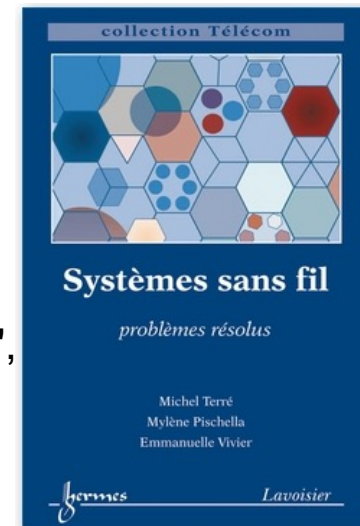


Références

- X. Lagrange, P. Godlewski, S. Tabbane, "Réseaux GSM", Hermès – Lavoisier, 978-2-7462-0153-8
- J.G.Remy, J.Cueugnet, C.Siben, "Systèmes de Radiocommunications avec les Mobiles", Eyrolles
- A. Goldsmith, "Wireless Communications", Cambridge University Press , 978-0-5218-3716-3
- J. G. Proakis, "Digital Communications", Mc Graw-Hill, 978-0-0711-3814-5
- H. Holma, A. Toskala, "WCDMA for UMTS", Wiley, 978-0-470-84467-1
- X. Lagrange, "Principes et évolutions de l'UMTS", Lavoisier (Hermes science), 978-2-7462-1040-1
- J. Sanchez, M. Thioune, "UMTS", Hermes, 978-2-7462-0856-8
- [VIT 94] VITERBI A.J., VITERBI A.M., ZEHAVI E., "Other-cell interference in celular power-controlled CDMA", IEEE Trans. On Com. Vol. 42, n°2-4, 1994
- <http://www.3gpp.org/>
- H. Holma, A. Toskala, "HSDPA/HSUPA for UMTS", Wiley, 978-0-470-01884-2
- M. Terré, M. Pischella, E. Vivier, "Systèmes sans fil, Problèmes résolus", Hermès – Lavoisier, 978-2-7462-3906-7



2 G – 2.5 G : GSM / GPRS / EDGE



Histoire

- Groupe Spécial Mobile ⇒ **Global System for Mobile** communications
 - Système novateur, conçu par deux laboratoires de R&D publics (France, Allemagne) :
 - Commutation de circuits
 - Système cellulaire numérique + Modulation radio robuste
 - Roaming automatique
 - Séparation de la fonction téléphonique du mobile de la fonction « identification », placée dans une carte à puce (SIM)
 - Cryptage des communications; protection de l'identité de l'abonné
- Normalisation (1987- 1995) : par l'organisme de normalisation européen ETSI
 - Réservation d'un espace suffisant dans le spectre radioélectrique (dès 1979 dans la bande des 900 MHz)
 - Etablissement de normes très détaillées et précises, sans options
- Ouverture des réseaux :
 - 1992 : Orange France & SFR
 - 1996 : Bouygues Telecom
 - Taux de pénétration (fin 2006) : 82.5 % en France
- Réseau concurrent : IS-95 (< 10% parts de marché)

Technologie mondiale!



Organisation fréquentielle

- Deux bandes de fréquences, aux alentours de :
 - 900 MHz (GSM historique)
 - 1800 MHz (DCS)
- Bande unitaire : 200 kHz
- En France, les opérateurs ont désormais une sous-bande dans chacune des bandes
 - 10 MHz dans la bande 900 MHz
 - ~25 Mhz dans la bande 1800 MHz
 - \Rightarrow couverture des zones rurales et des zones urbaines

1/



Architecture du réseau GSM

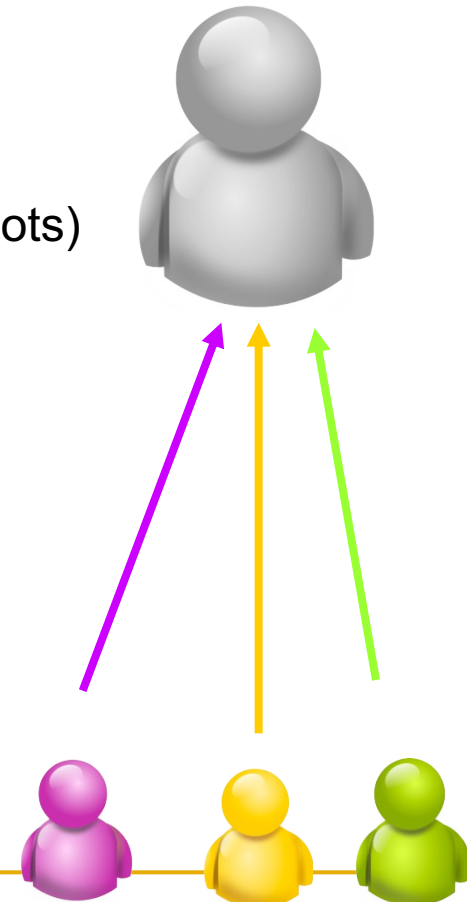
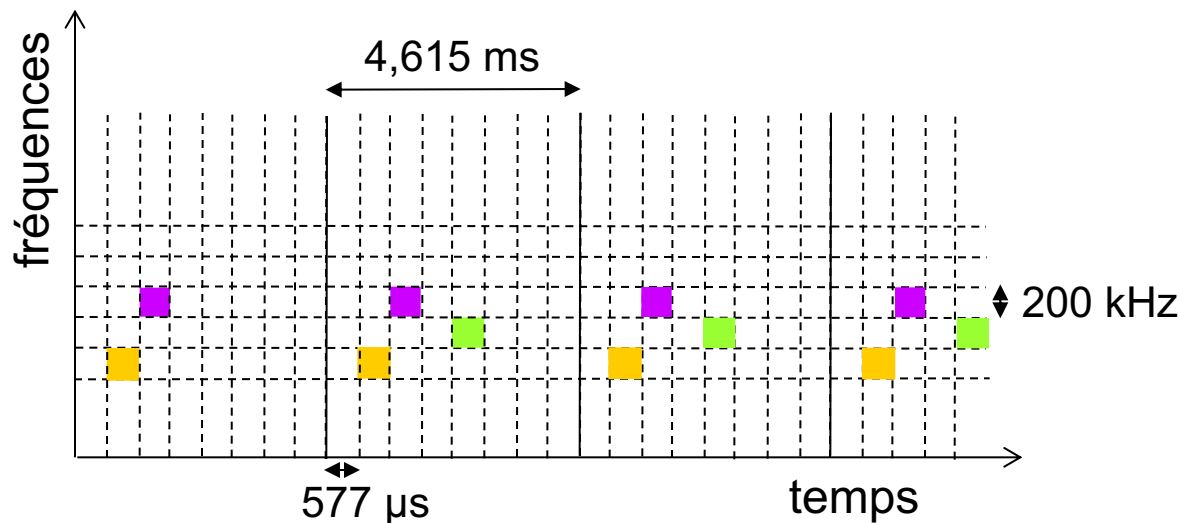
2/

- Mobiles : puissance max d'émission : 1 W (2W)
- Réseau d'accès :
 - BTS : points d'accès au réseau
 - BSC : contrôle des BTS
- Réseau cœur :
 - MSC : commutateur
 - G-MSC : passerelle vers les autres réseaux : fixe ou mobile.
 - d'autres éléments de réseau assurent :
 - l'authentification, le chiffrement :
 - AuC,
 - la vérification des services souscrits par l'abonné :
 - HLR, VLR
 - la supervision & la maintenance du réseau :
 - OMC, NMC

Multiplexage des utilisateurs GSM

- Rappel : RA CH=Random Access Chance
répartition des différents utilisateurs sur la voie radio, entre le mobile et le point d'accès au réseau

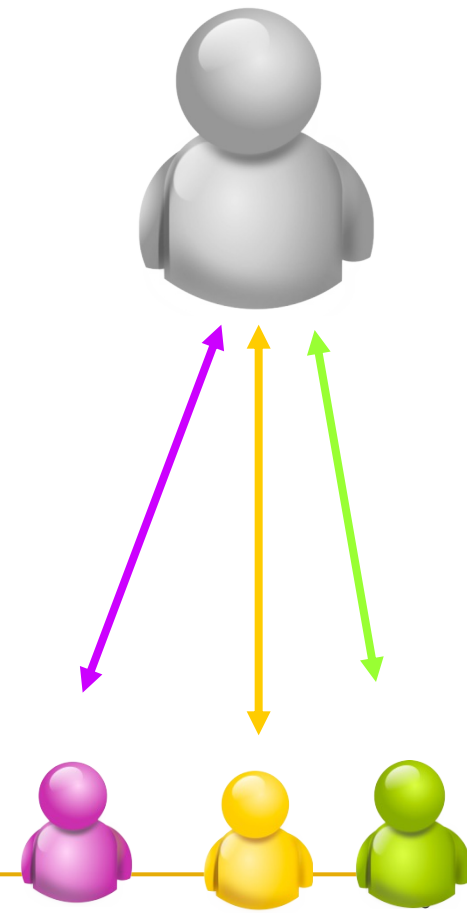
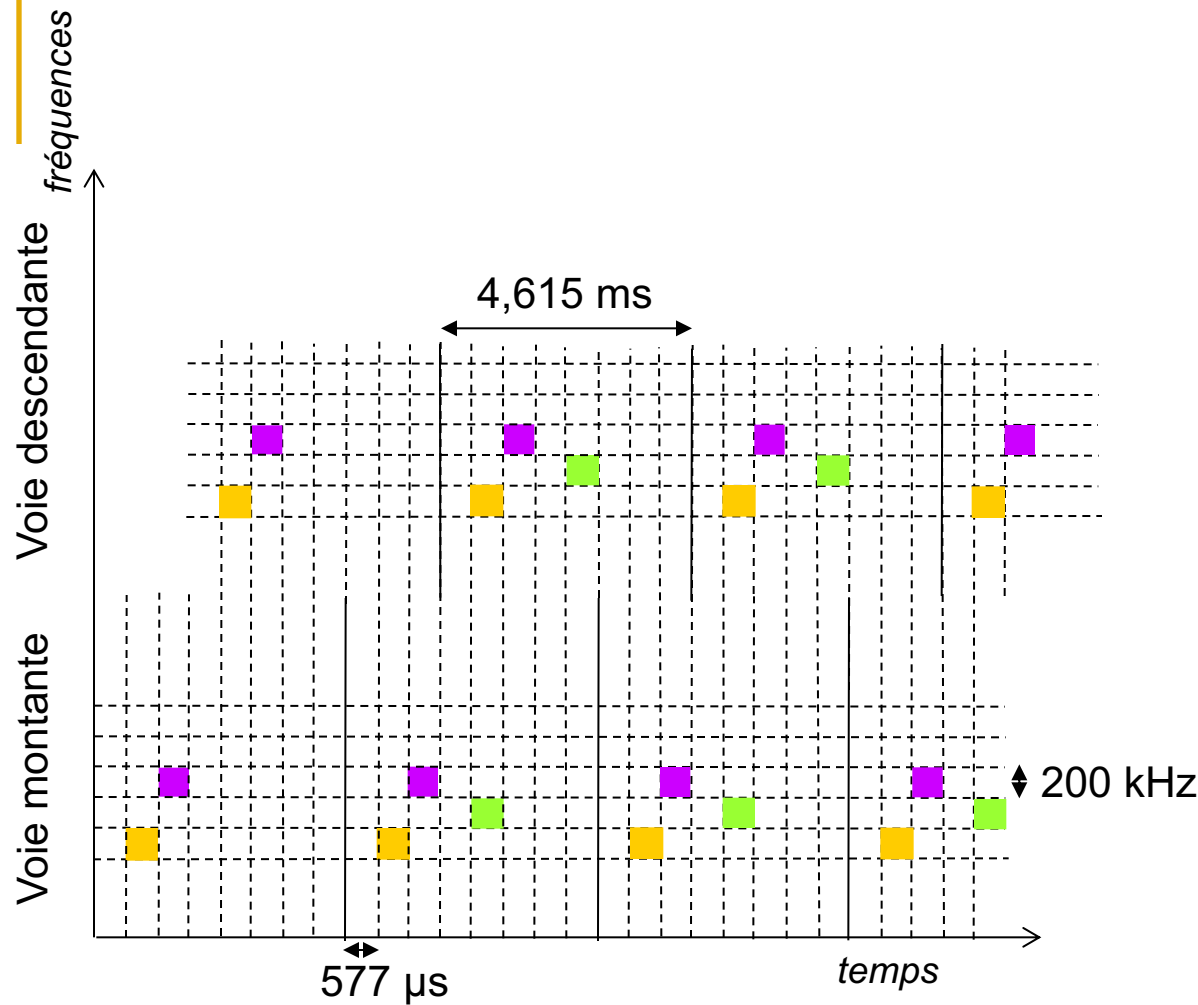
- **F/TDMA : multiplexage en fréquence et en temps**
 - Largeur des canaux radios : 200 kHz
 - Durée de la trame radio : 4,615 ms, 8 IT (slots, timeslots)



Duplexage des comm. 2G – 2,5G

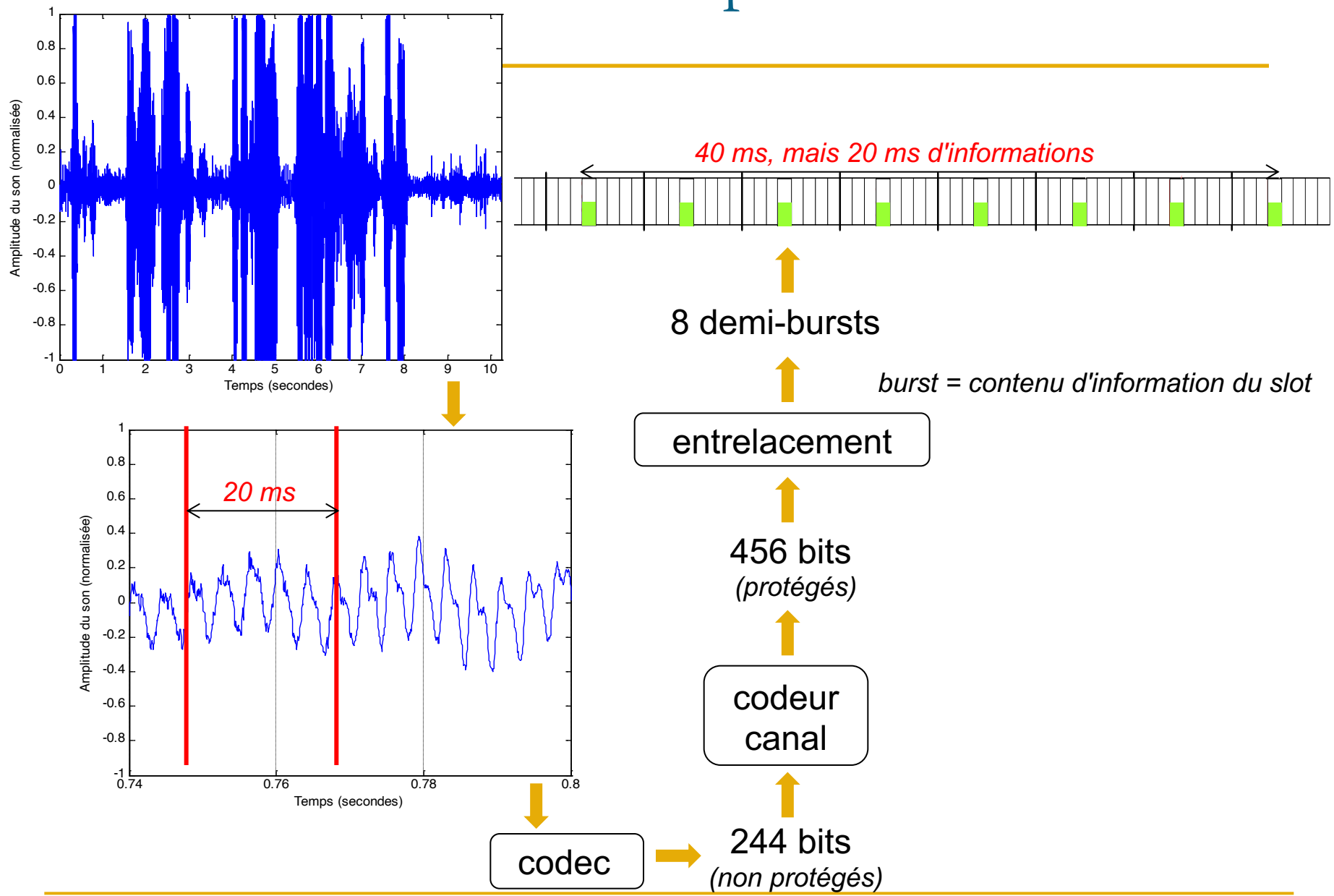
- Duplexage FDD, écart duplex :
 - 45 MHz dans la bande 900 MHz
 - 95 MHz dans la bande 1800 MHz
- Organisation fréquentielle/temporelle :
 - Les données d'un utilisateur ne sont transmises qu'1/8 du temps!
 - Décalage voie \uparrow / voie \downarrow : 3 timeslots

Organisation Fréq./Temp. en GSM



Ressources radios utilisées pour une comm. GSM

ISEP – Domaine Réseaux & Télécommunications – Emmanuelle Vivier



Capacité d'une cellule GSM

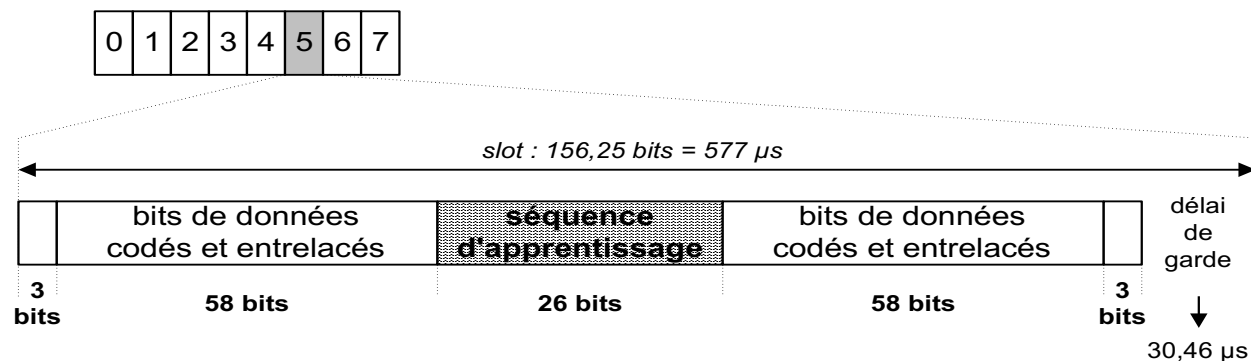
- 1 « TRX » = 1 bande de fréquence duplex parmi celles allouées à l'opérateur :
 - 200 kHz ↓
 - 200 kHz ↑
- Suivant le motif de réutilisation des fréquences adopté, chaque cellule comporte un certain nombre de TRX :

⇒ elle peut donc écouler une certaine capacité de trafic, que l'on peut exprimer sous diverses formes, dont :

 - le nb de communications simultanées par cellule : $8 \times N_{TRX}$
 - l'efficacité spectrale utile (en bits utiles/sec/Hz) : $\frac{8 \times 12.2}{200} = 0.49 \text{ bits / s / Hz}$
 - le nombre d'Erlangs écoulés par la cellule pour une probabilité de blocage donnée
- Attention à prévoir une partie de la capacité pour la signalisation (voie balise, signalisation de début/fin de communication, supervision de la communication, etc)

Structure d'un slot en GSM

- Un slot = timeslot = IT = 577 μ s, contient :
 - un burst :
 - élément d'information contenu dans le slot : 156,25 bits au max.
 - 4 types de burst (Normal, Frequency, Synchronization, Access)
 - structure générale :
 - bits de tête permettant la montée en puissance de l'émetteur
 - bits d'information
 - séquence d'apprentissage permettant d'évaluer la qualité du canal radio
 - bits de queue permettant le retour au repos de l'émetteur
 - Un délai de garde: pour tenir compte des aléas du temps de transmission
- Exemple: « normal burst » :



Canaux logiques GSM

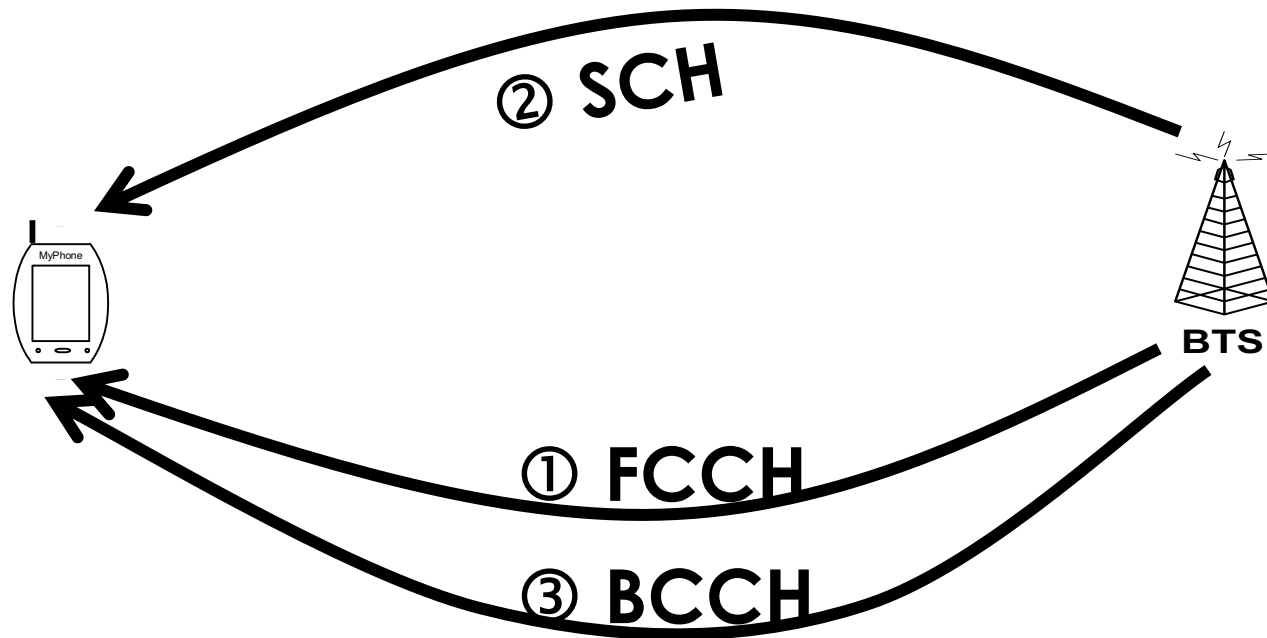
1/

- Fonctions des différents canaux logiques :
 - diffusion des informations systèmes
 - Broadcast Control Channel, BCCH – diffusion ↓ (simplex): information système
 - Frequency Correction Channel, FCCH – diffusion ↓ (simplex): calage de fréquence
 - Synchronization Channel, SCH – diffusion ↓ (simplex)
 - appel des mobiles, accès au réseau
 - Paging Channel, PCH – diffusion ↓ (simplex),
 - Random Access Channel: RACH – accès multiple ↑ (simplex),
 - Access Grant Channel: AGCH – diffusion ↓ (simplex),
 - Cell Broadcast Channel, CBCH – diffusion ↓ (simplex)
 - communication
 - Trafic Channel, TCH – dédié ↓↑ (duplex)
 - contrôle des paramètres durant la communication
 - Slow Associated Control CHannel SACCH – dédié ↓↑ (duplex): Gestion de liaison
 - Fast Associated Control CHannel FACCH – dédié ↓↑ (duplex): Exécution du Handover
 - signalisation
 - Stand-alone Dedicated Control Channel SDCCH – dédié ↓↑ (duplex)

Canaux logiques GSM

2/

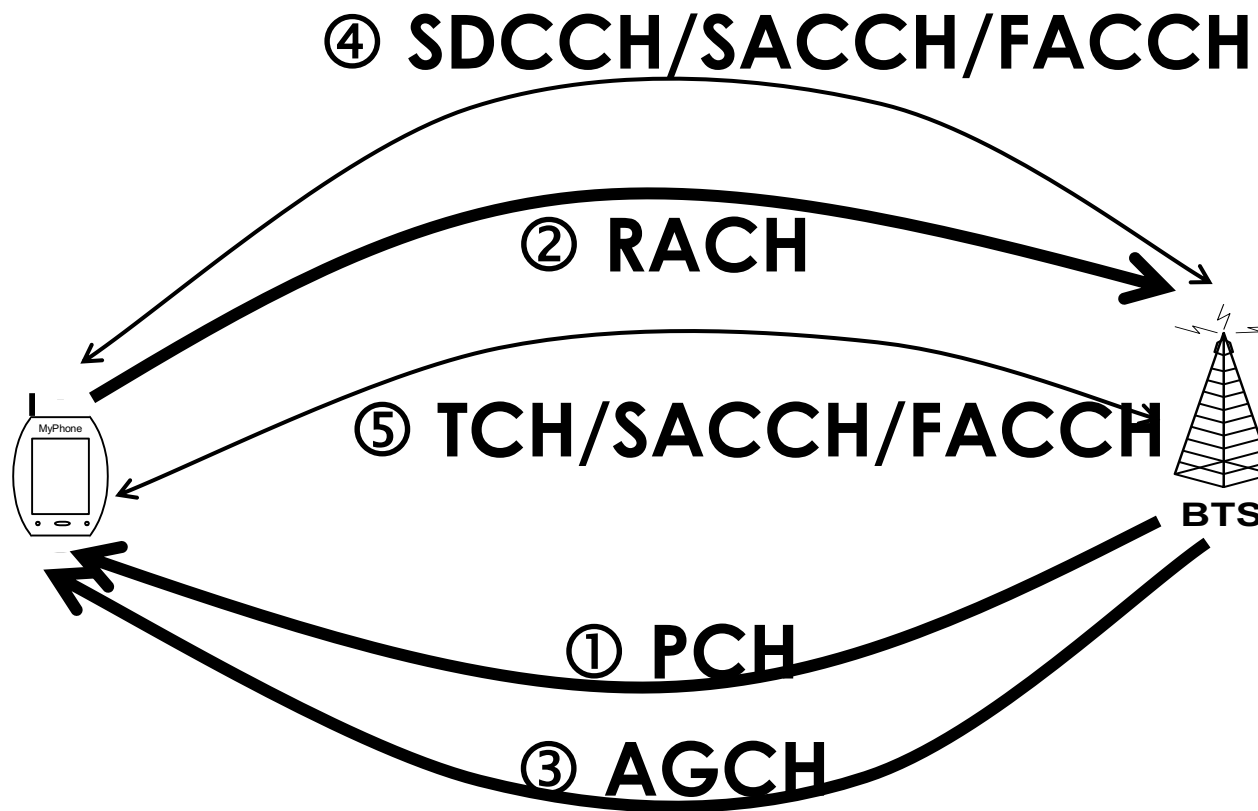
- Mise sous tension du mobile :



Canaux logiques GSM

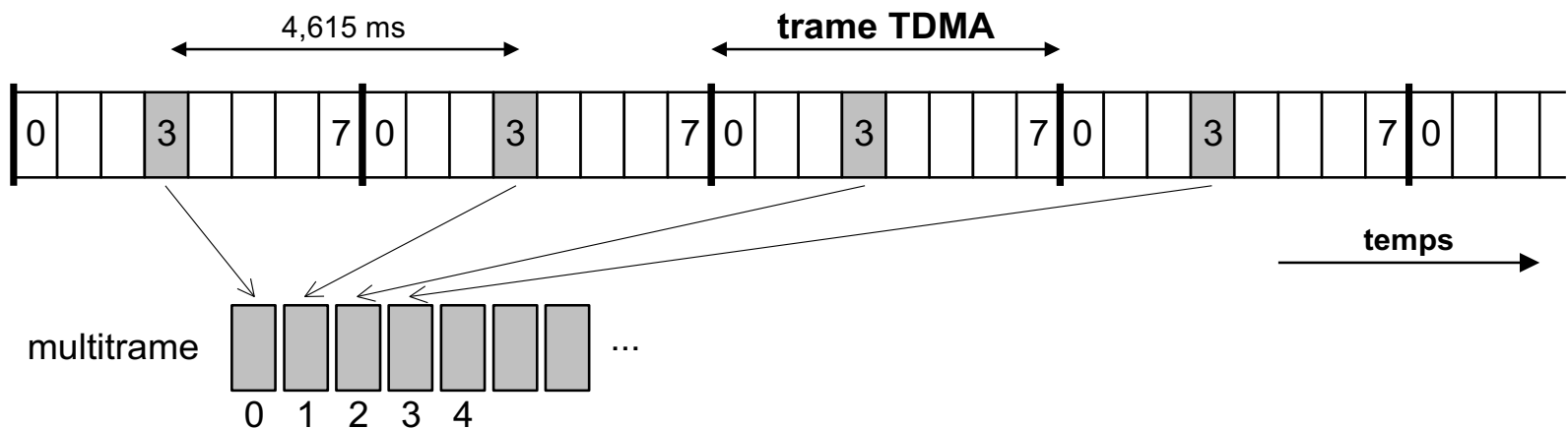
3/

- Réponse à un appel entrant :



1/

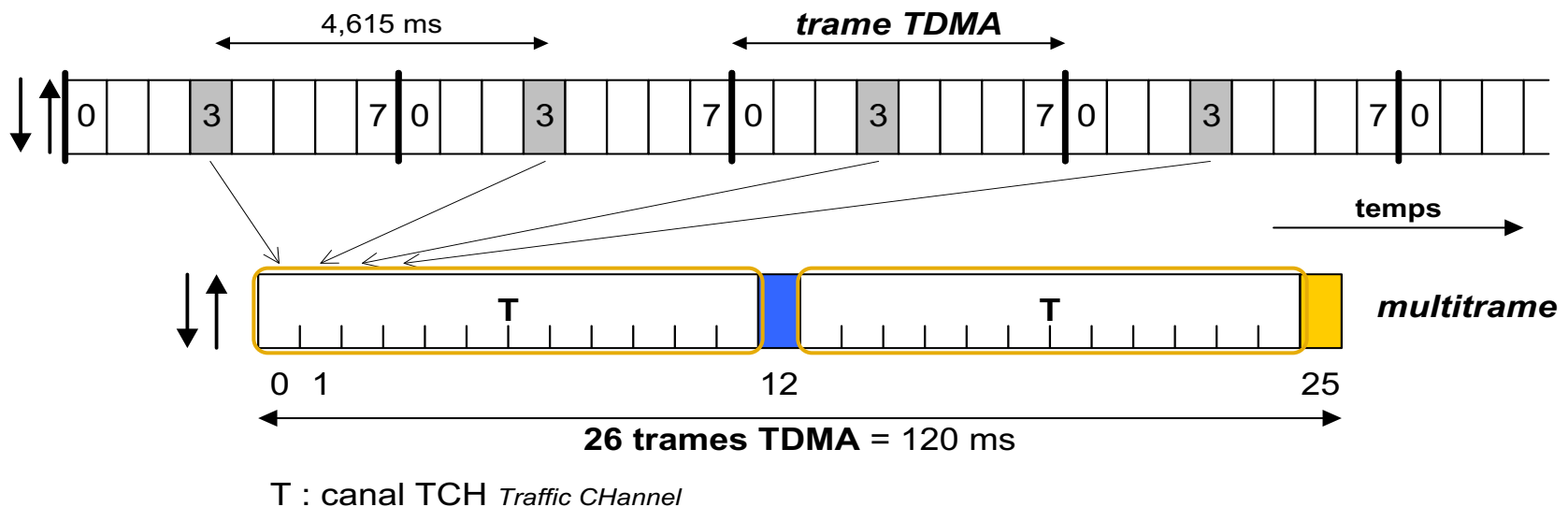
- multiplexage de plusieurs canaux logiques sur un même canal physique
- multiframe TDMA :
 - succession de plusieurs (26 ou 51) trames TDMA consécutives
 - définit la période de transmission de chacune des infos véhiculées sur les canaux logiques



Multiframe GSM à 26 trames

2/

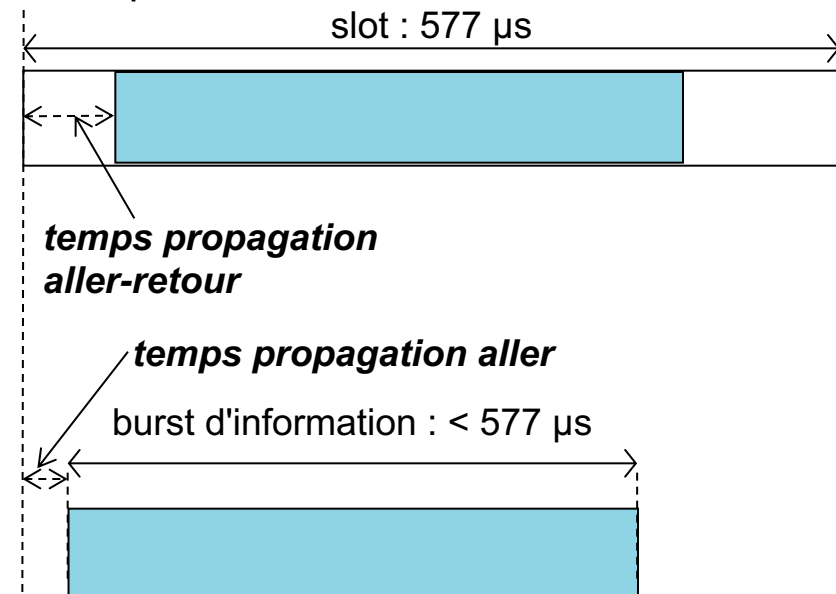
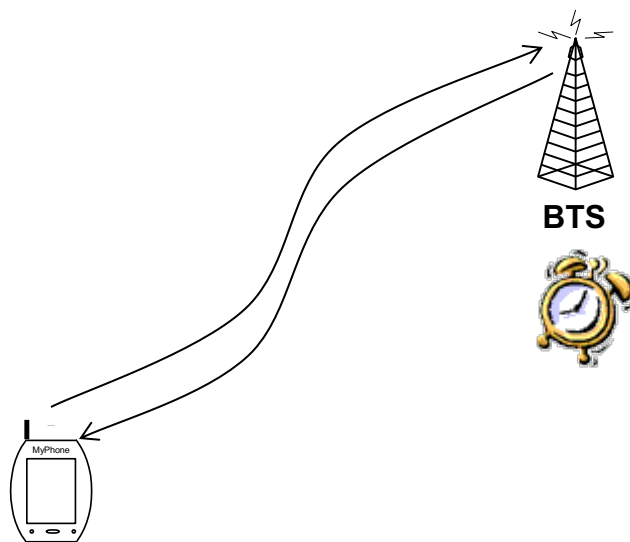
- informations :
 - parole (13 kbits/s, 5,6 kbits/s, 12,2 kbits/s)
 - données (9,6 kbits/s, 14,4 kbits/s)
- multiplexage :
 - 24 trames / multiframe à 26 (6 x 4 bursts / 120 ms)



Mobilité 2G – 2,5G : Timing Advance

■ Timing Advance :

- Sur le lien uplink, la BTS estime la distance MS-BTS en fonction du TA et de la position de l'access burst dans le slot.
- Sur le lien downlink, la BTS envoie toutes les 480 ms la valeur mise à jour du Timing Advance (1 unité = 553m ~ 600 m)
- Imprécision du TA : Fluctuation possible
 - burst d'accès au réseau (RACH) : 252 μ s \leftrightarrow 37.8 km A/R
 - en cours de com. : délai de garde : 30.46 μ s \leftrightarrow 4.5 km A/R



Mobilité 2G – 2,5G : Handover

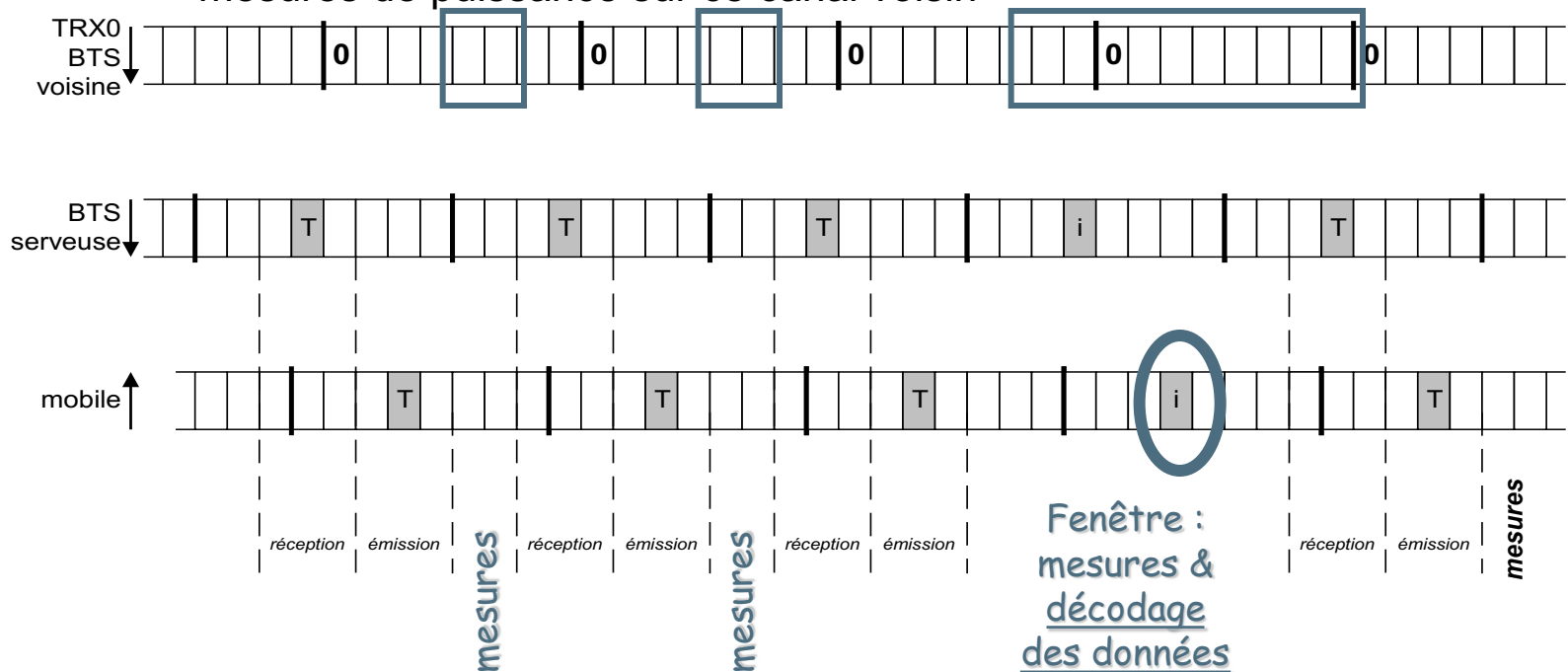
1/

- Préparation d'un HO sur la cellule courante :
 - Remontées des mesures vers le BSC, toutes les 480 ms des moyennes de :
 - Rxleveldown
 - Rxqualdown
 - Rxlevelup
 - Rxqualup
 - RXlevel est codé sur 6 bits, de :
 - '0' : niveau de champ inférieur à -110 dBm à
 - '63' : niveau de champ supérieur à -48 dBm
 - par pas de 1 dB.
 - RXqual est codé sur 3 bits

RXqual	TEB correspondant
'0'	TEB < 0,2 %
'1'	0,2 % < TEB < 0,4 %
'2'	0,4 % < TEB < 0,8 %
'3'	0,8 % < TEB < 1,6 %
'4'	1,6 % < TEB < 3,2 %
'5'	3,2 % < TEB < 6,4 %
'6'	6,4 % < TEB < 12,8 %
'7'	12,4 % < TEB

2/

- Préparation d'un HO : synchronisation sur les cellules voisines :
 - à chaque trame idle, le mobile est sûr de décoder le slot 0 d'une BTS voisine, *i.e.* sa voie balise :
 - au bout d'un moment, il va tomber sur son canal FCCH, puis sur son canal SCH et enfin son canal BCCH (droits d'entrée, ...).
 - il saura donc qui elle est exactement et fera ensuite régulièrement des mesures de puissance sur ce canal voisin

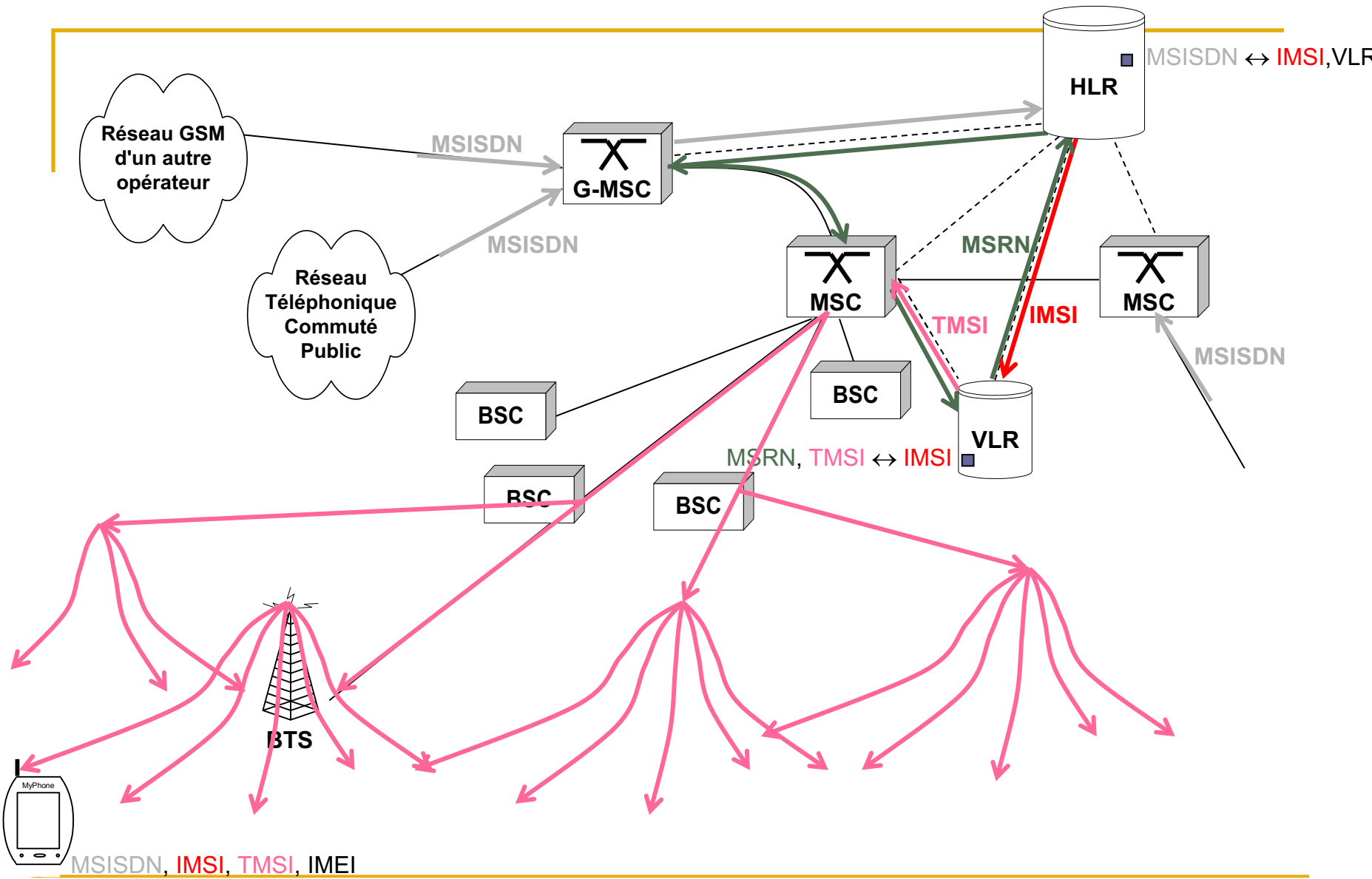


Mobilité 2G – 2,5G : Handover

3/

- Décision de HO prise par le BSC, à partir des paramètres :
 - RXlevelup, RXqualup
 - RXleveldown, RXqualdown
 - RXleveldown_voisine_k
 - timing advance
 - et d'un algorithme propre à l'opérateur
- déclenché par le MSC ou par le BSC
- type de handovers :
 - HARD HO
 - Suivant la situation de l'abonné et la topologie du réseau :
 - intra-cellulaire (interférences)
 - inter-cellulaire,
 - inter-BSC,
 - inter-MSC...

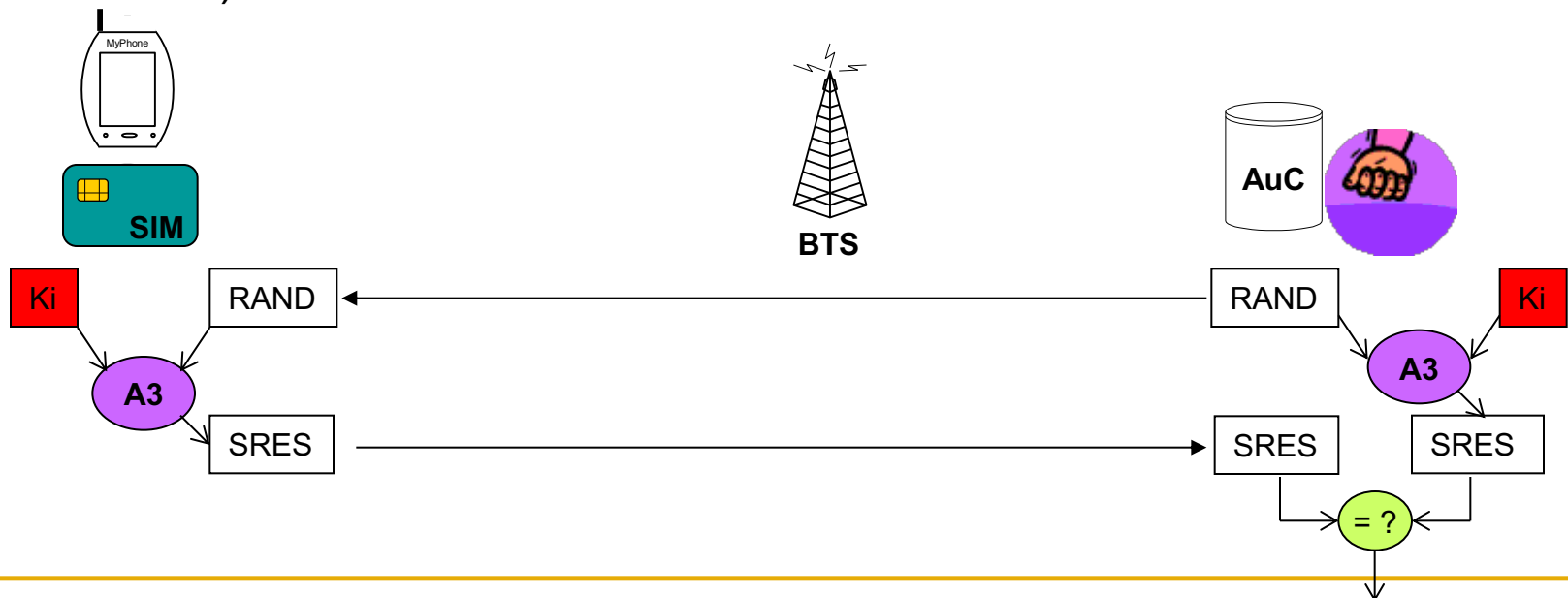
Sécurité 2G – 2,5G



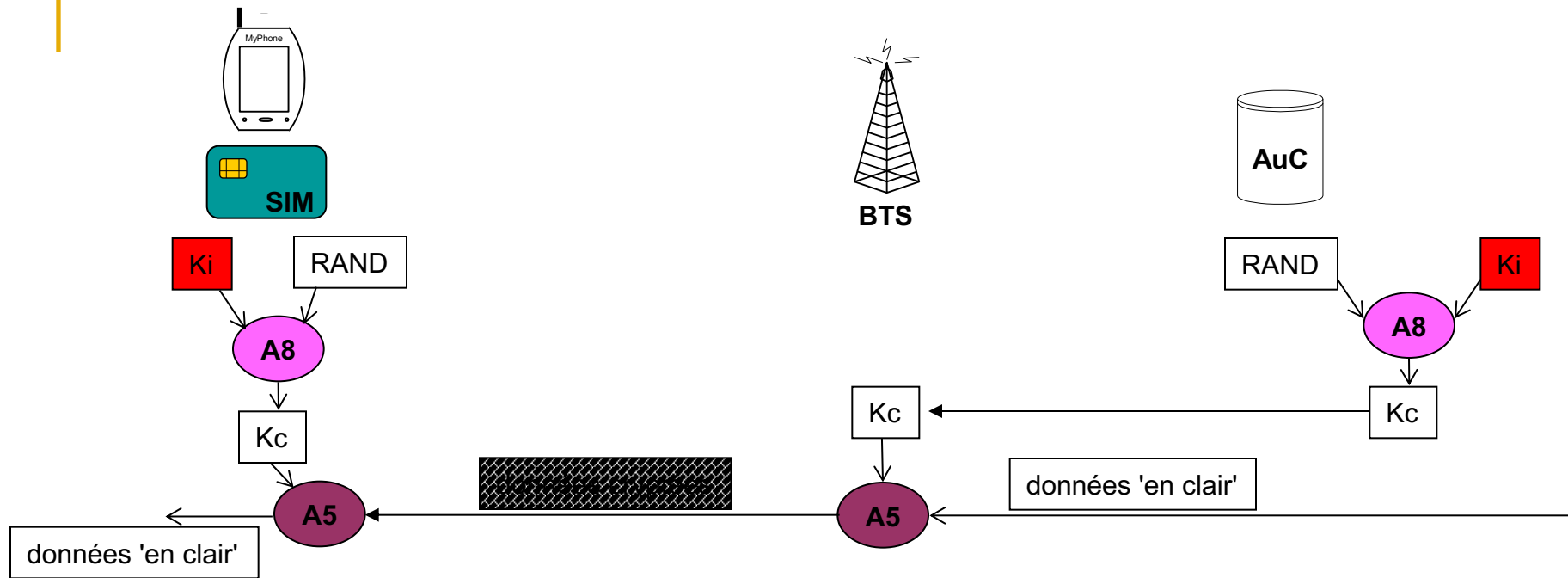
ISEP – Domaine Réseaux & Télécommunications – Emmanuelle Vivier

Sécurité 2G – 2,5G : authentification

- L'authentification de l'abonné :
 - protège le réseau de l'utilisation frauduleuse de ses ressources
 - protège l'abonné de l'utilisation frauduleuse de son compte
 - exigible lors :
 - des MAJ localisation
 - des établissements d'appels (entrants/sortants)
 - La clé Ki (128 bits) n'est jamais transmise à travers le réseau (fixe ou radio)



Sécurité 2G – 2,5G : chiffrement



- En 1999, l'algorithme A5 est cassé...

Short Message Services

- coût très faible pour l'opérateur :

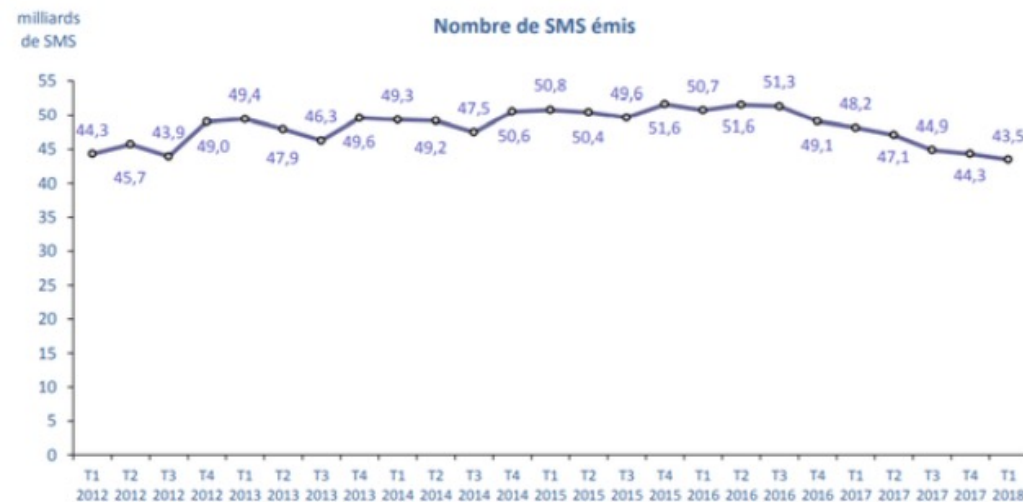
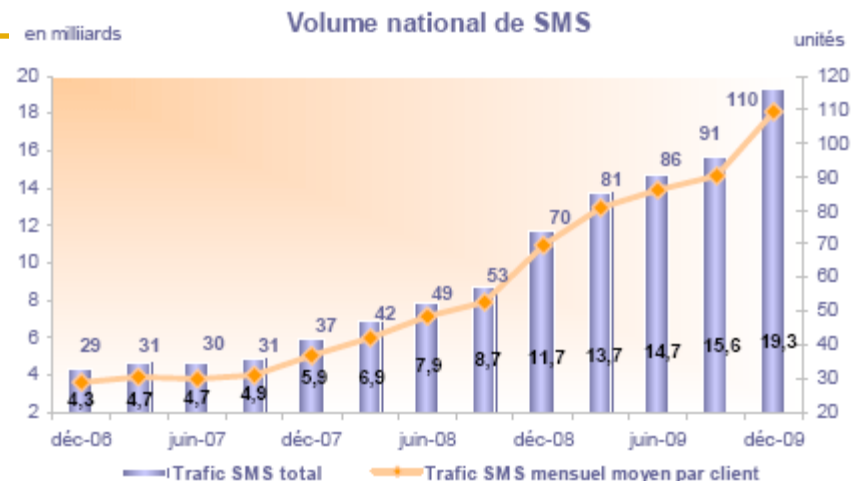
- messages courts (160 caractères / SMS)
- débit très faible : < 1kb/s
- transmission sur des voies de signalisation :
 - SACCH
 - SDCCH

- 2012 :

- 40 milliards de SMS / trimestre en France
- 242 SMS / abonné / mois (> 800 pour les 16-25 ans)

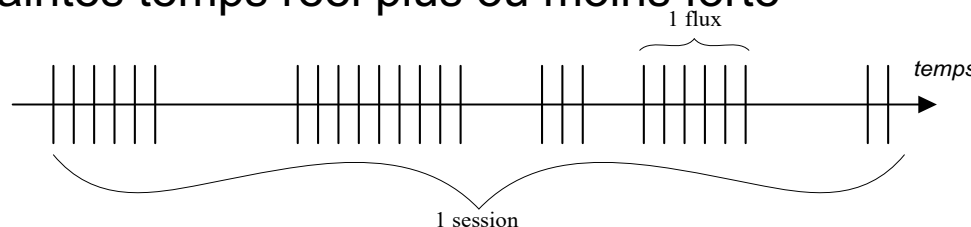
- 2014 :

1,5 milliards de SMS échangés en France (30 000 / sec. à minuit chez Orange) pour le nouvel an... 25 milliards en Chine...



Conclusion 2G

- GSM est un/le réseau cellulaire numérique mondial :
- Qualité des communications vocales :
~ identique à celle des communications sur réseau fixe
- Limitations : Transfert de données :
 - ❑ à très bas débit (14,4 kbits/s)
 - ❑ en mode circuit, ie canal réservé (et payé) même en cas d'inactivité
- Caractéristiques essentielles des données / voix :
 - ❑ Flux de données en rafales (« bursty »)
 - ❑ Taux d'erreur nécessairement très bas (\neq voix)
 - ❑ Contraintes temps réel plus ou moins forte

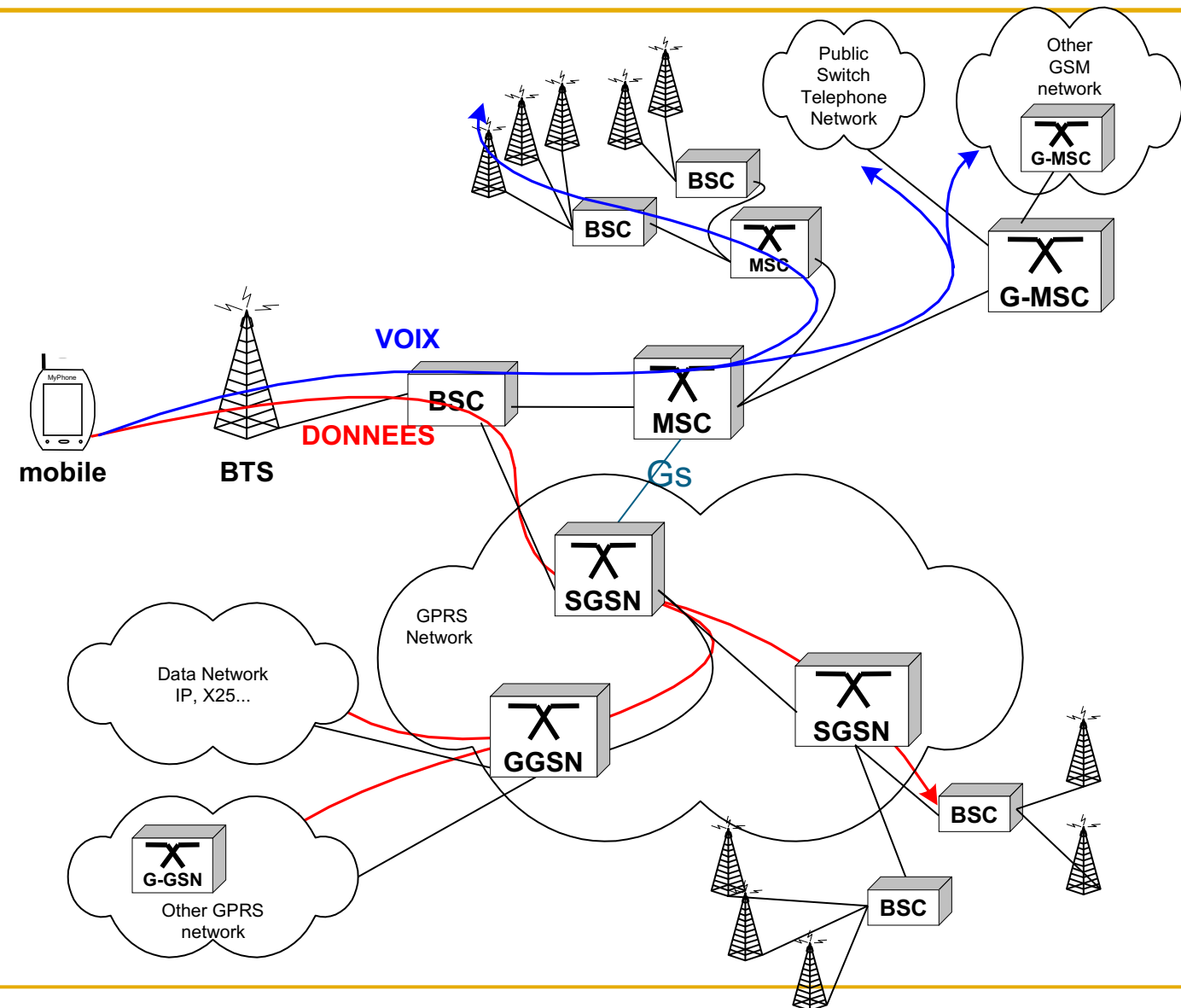


⇒ nécessité d'une évolution dans le réseau : 2.5G :

General Packet Radio Services, disponible en France à partir de 2001/2002

GPRS network architecture

1/



GPRS network architecture

2/

- SGSN (Serving GPRS Support Node) :
 - Manages GPRS services in a geographical area :
 - for the mobile: Access Point to GPRS network
 - Security (in collaboration with HLR): authentication, encryption
 - Mobility: paging, location update
 - Billing
 - Transfers packets :
 - Switch
 - Compression / Decompression

- GGSN (Gateway GPRS Support Node) :
 - Serves as gateway towards other data networks
 - Allocates IP @ to mobile
 - Switches packets
 - Bills

GPRS network architecture

3/

- Impact on existing GSM network's elements:
 - BTS & BSC reuse, with:
 - Radio re-dimensioning
 - New devices :
 - PCU (Packet Control Unit) in BSC
 - Segmentation, Re-assembly, Acknowledgement of packets,
 - Radio access (arbitration)
 - CCU (Channel Control Unit) in BTS
 - Packet processing (coding, interleaving)
 - HLR reuse, and in addition (similarly to GSM), for each subscriber:
 - settings to allow the access to packet services: subscribed QoS
 - current Location (SGSN)
 - mobile state : on/off
 - increased capacity

GPRS main characteristics

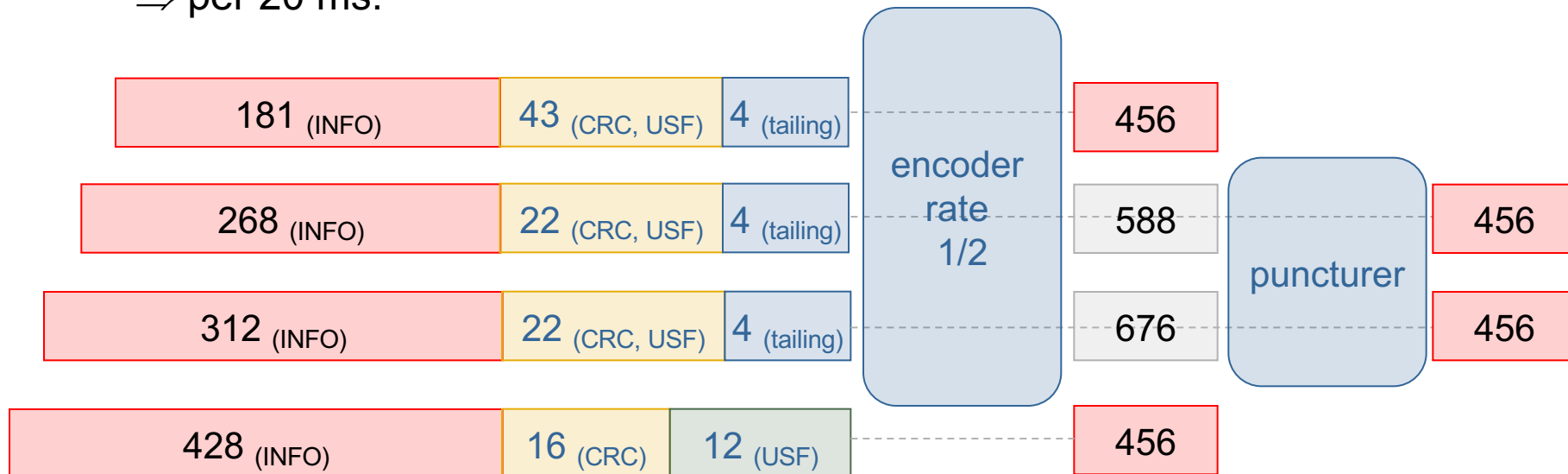
- Packet switching
 - new network elements
 - new user equipments
- up to 8 slots can be allocated to each user.
 - All must belong to the same TRX.
- a slot can be shared by up to 8 users.
- data throughput on each slot :
 - 9.05 , 13.4 , 15.6 or 21.4 kbits/s
- data networks (IP, X25...) connection
- 29 multislot classes handsets determining the maximum achievable data rates in uplink and downlink directions:
 - total number of slots that can be used simultaneously for both uplink and downlink communications,
 - amount of uplink & downlink timeslots that can be used for transmission.

GPRS coding scheme

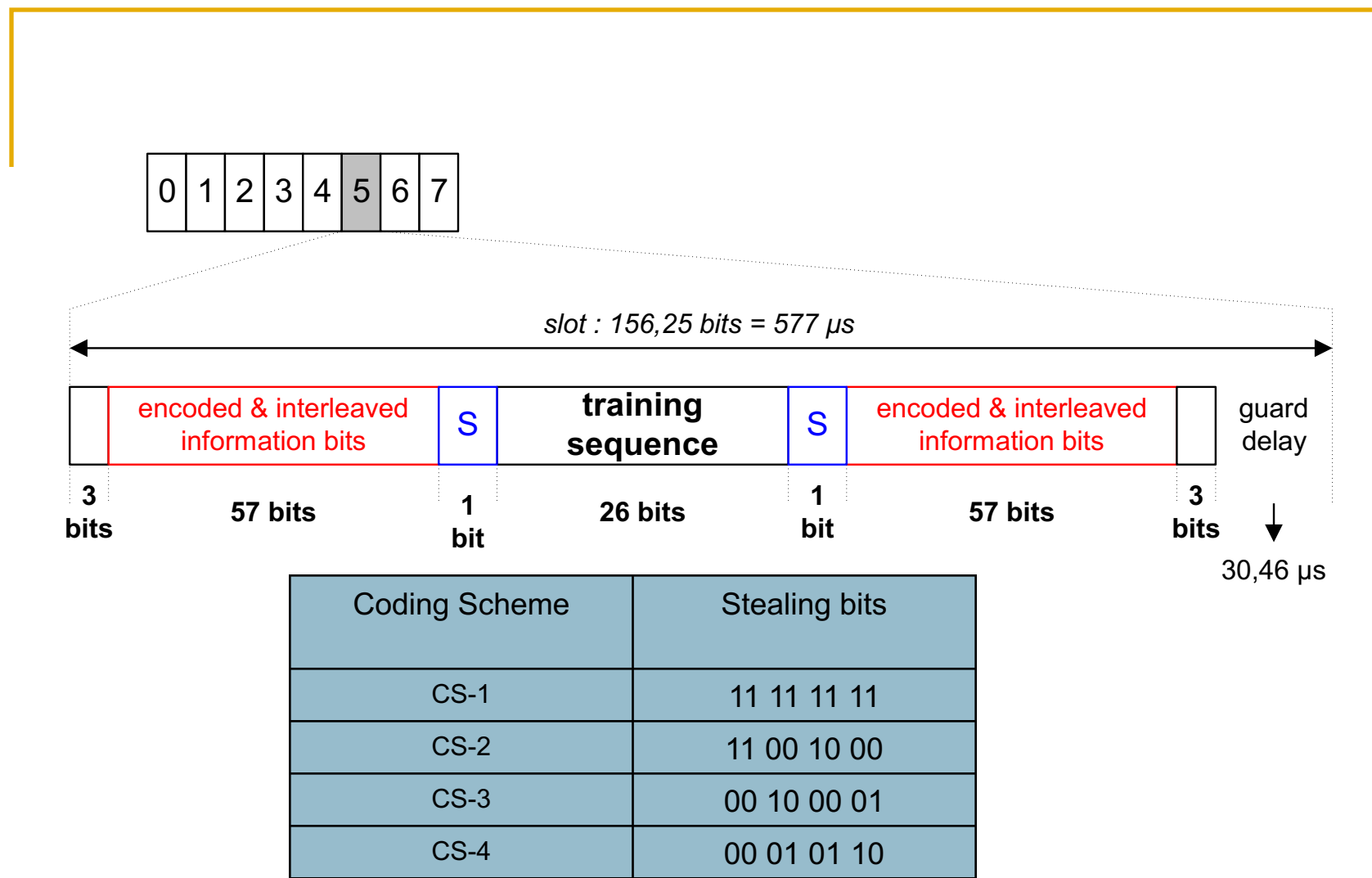
■ Four coding schemes:

- ❑ CS1: 9.05 kbits/s
- ❑ CS2: 13.4 kbits/s
- ❑ CS3: 15.6 kbits/s
- ❑ CS4: 21.4 kbits/s

⇒ per 20 ms:

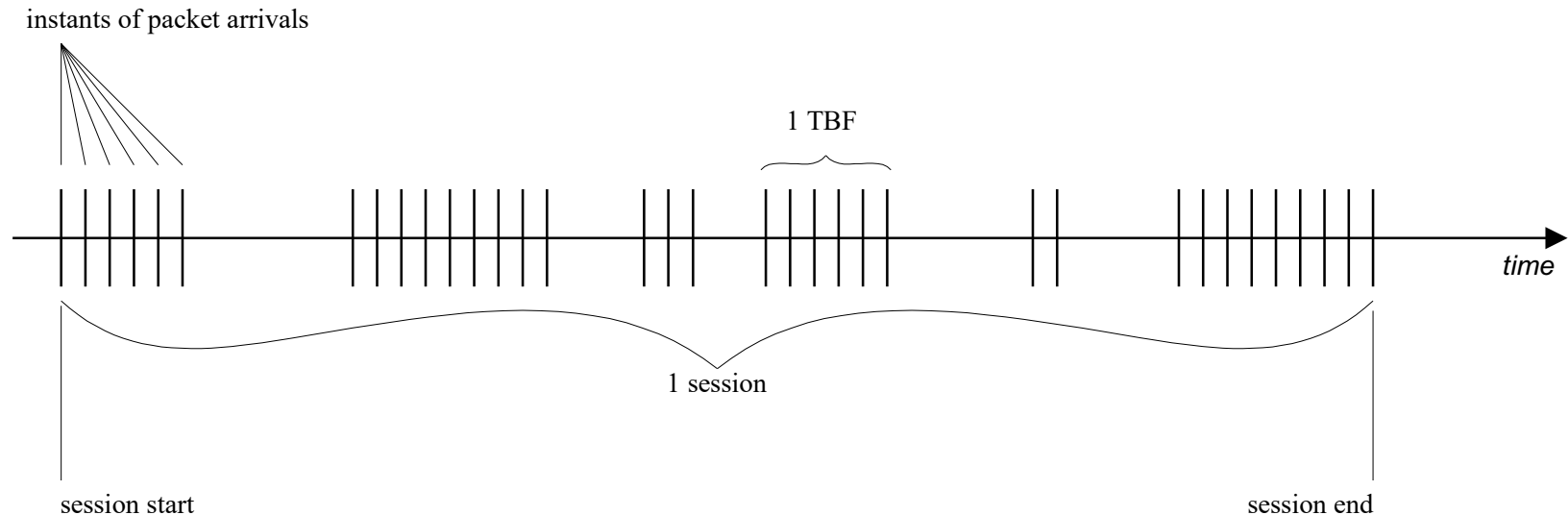


GPRS slot structure

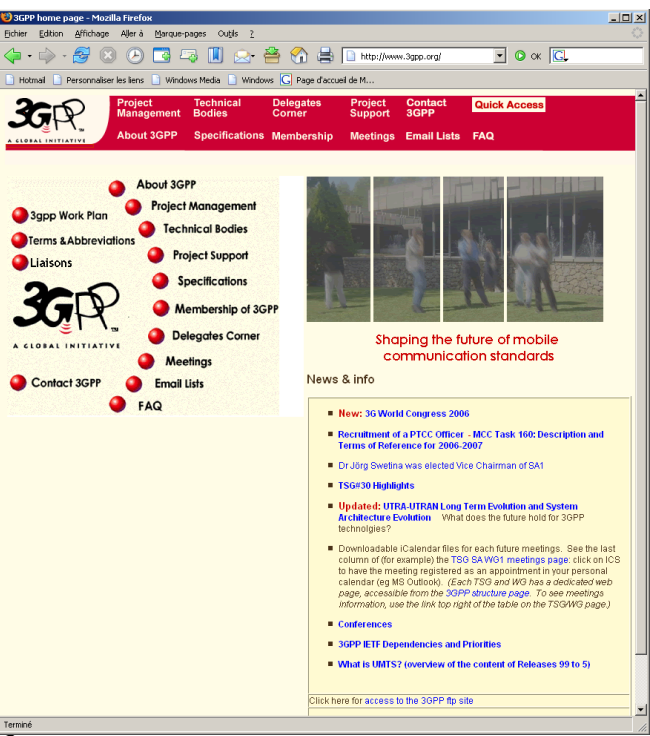


GPRS data flow

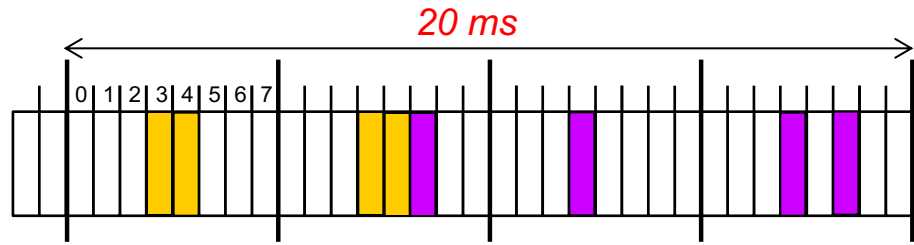
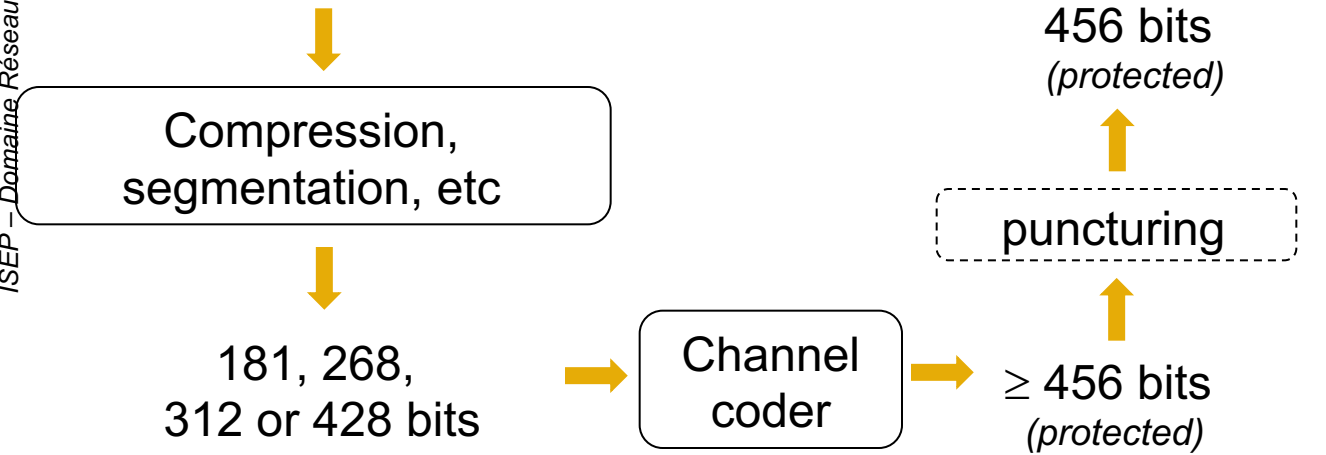
- one GPRS data flow = one Temporary Block Flow TBF
- one Web session = several TBF and reading intervals:



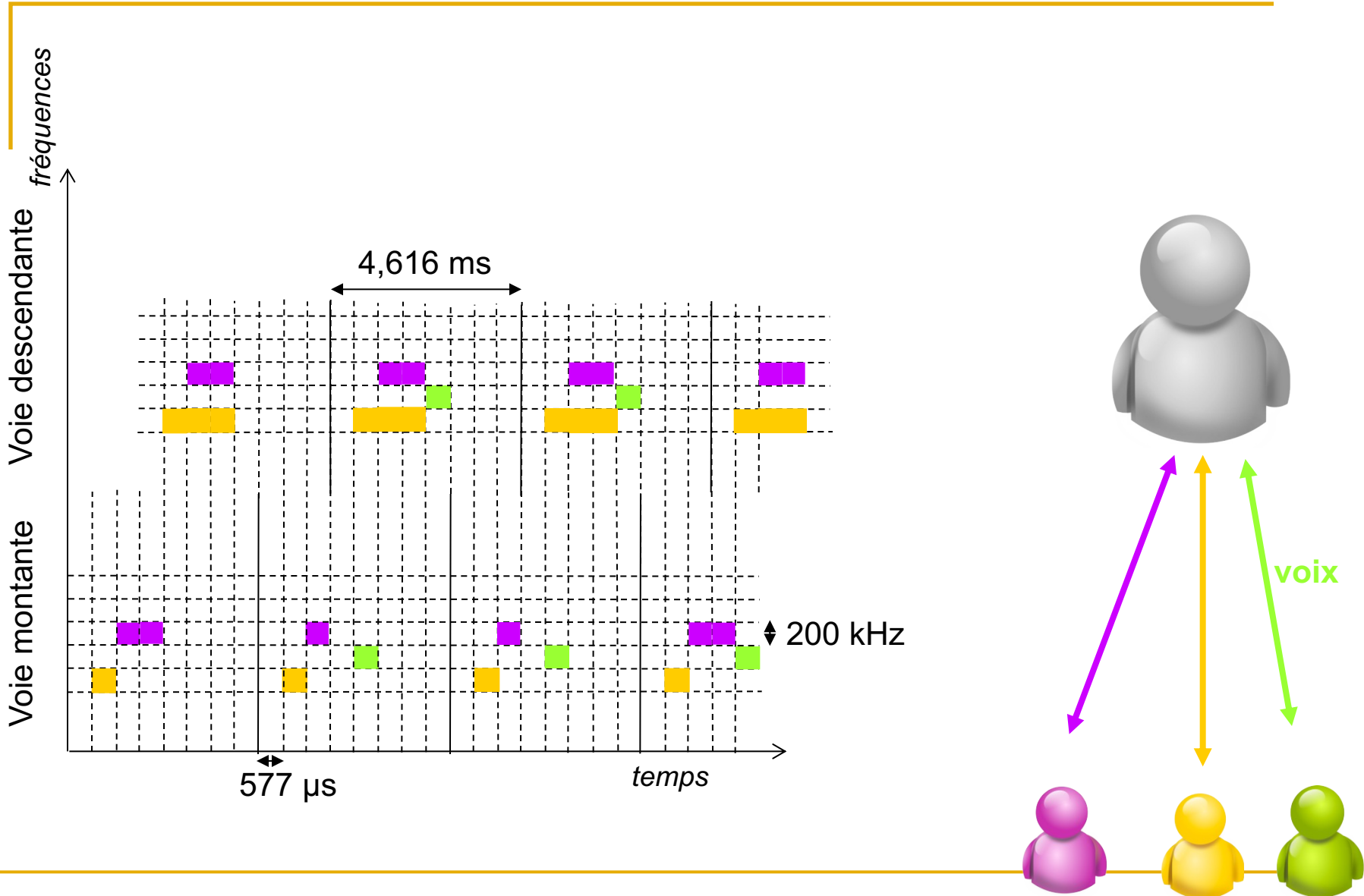
Radio resources for a TBF



ISEP – Domaine Réseau



Frequency/Time grid for a TBF



PDP context activation

1/

- 'Packet Data Protocol context'
 - *set of information stored in MS, SGSN and GGSN in order to enable a data transfer.*
 - preliminary activation before data transfer:
 - On radio interface:
 - TLLI (Temporary Link Layer Identity) : ~ P-TMSI
 - External data network (X25, IP...)
 - Terminal PDP @ (dynamically allocated by GGSN)
 - Subscriber's current SGSN IP @
 - Negotiated QoS
 - In the network :
 - IMSI (recovered by SGSN from TLLI)
 - APN (Access Point Name) : GGSN selected by SGSN to access the external data network.

PDP context activation

2/

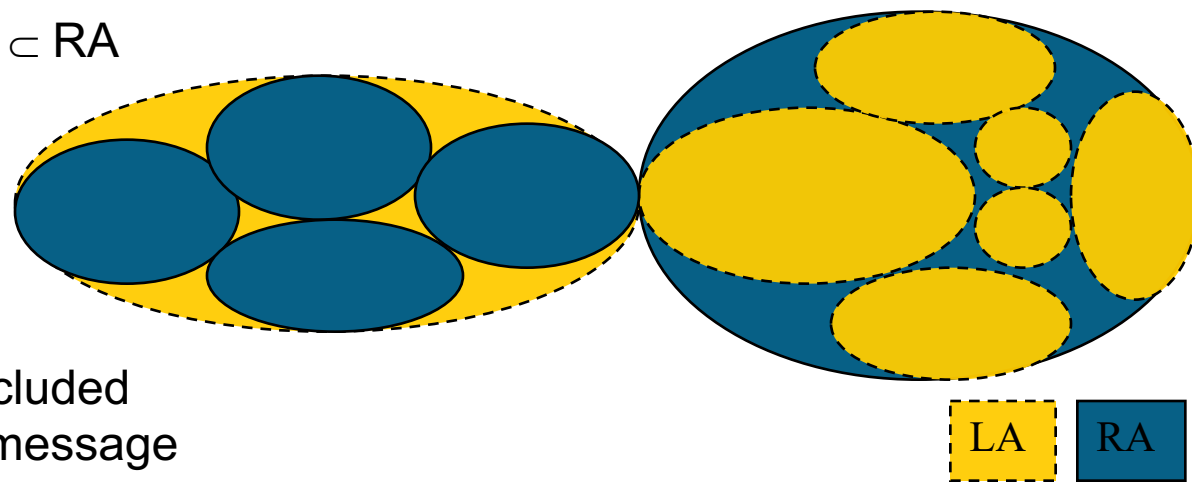
■ PDP Quality of Service

- can be renegotiated in case of PDP update
- is described with several parameters :
 - precedence:
 - 3 classes (priority vs other services)
 - reliability:
 - 3 classes (packet loss/out of sequence/corrupted rate)
 - variations from 10^{-9} to 10^{-2}
 - delay in the GPRS core network:
 - 4 classes
 - variations from 0,5 sec to >250 sec
 - mean throughput: 19 classes
 - variations from 100 bytes/h to 50 Mbytes/h
 - peak throughput: 9 classes
 - variations from 1 kbytes/s to 256 kbytes/s

GPRS Mobility Management

- Information broadcasting on BCCH :
 - Cell identity
 - Location Area (GSM)
 - Routing Area (GPRS)
- Cell Location Update (in ready state)
- Combined LA-RA Location Update (in standby state) via Gs MSC – SGSN interface:

- $RA \subset LA$ or $LA \subset RA$



- Former RA / LA included in the LU request message (for update in HLR connection with former SGSN/MSC)
- New (P)-TMSI allocation, if necessary

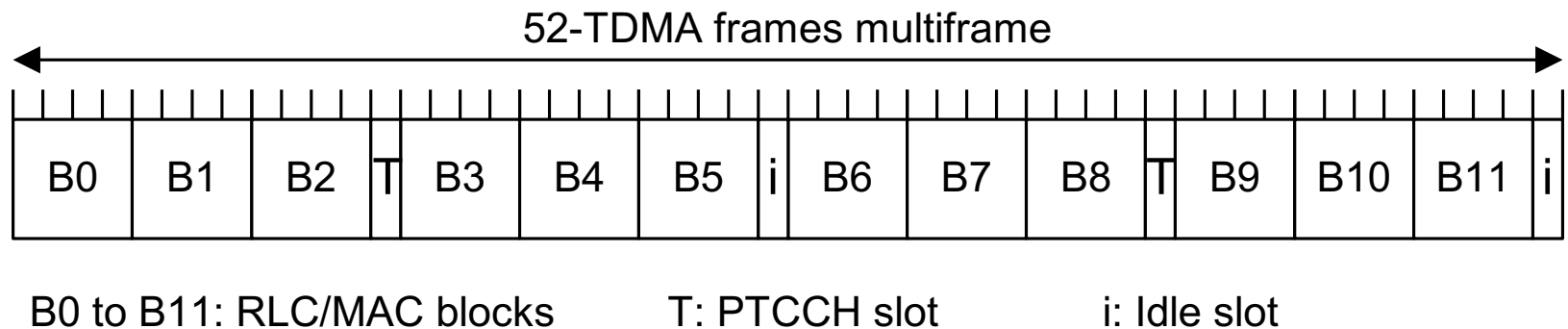
GPRS Logical channels

- GSM Beacon channel reuse:
 - ↓ : FCCH, SCH, BCCH, PCH, AGCH
 - ↑ : RACH

- specific GPRS logical channels addition:
 - Traffic channels ↓ ↑:
 - PDTCH (Packet Data Traffic Channel)
 - Control channels ↓ ↑:
 - PACCH (Packet Associated Control Channel):
 - during a session : packets Ack/Nack, radio measurements, handover...
 - session start/end
 - PTCCH (Packet Timing Control Channel):
 - Timing advance control
 - Extra (if mentionned on BCCH SYSTEM INFO 13 message):
 - ↓ : **PBCCH**, **PPCH**, **PAGCH**
 - ↑ : **PRACH**

GPRS multiframe structure

- A 52-frames multiframe is divided into:
 - $12 \times 4 = 48$ PDTCH or PACCH frames,
 - 2 PTCCH frames,
 - 2 Idle frames.
- PDTCH or PACCH **dynamic** multiplexing (\neq GSM)

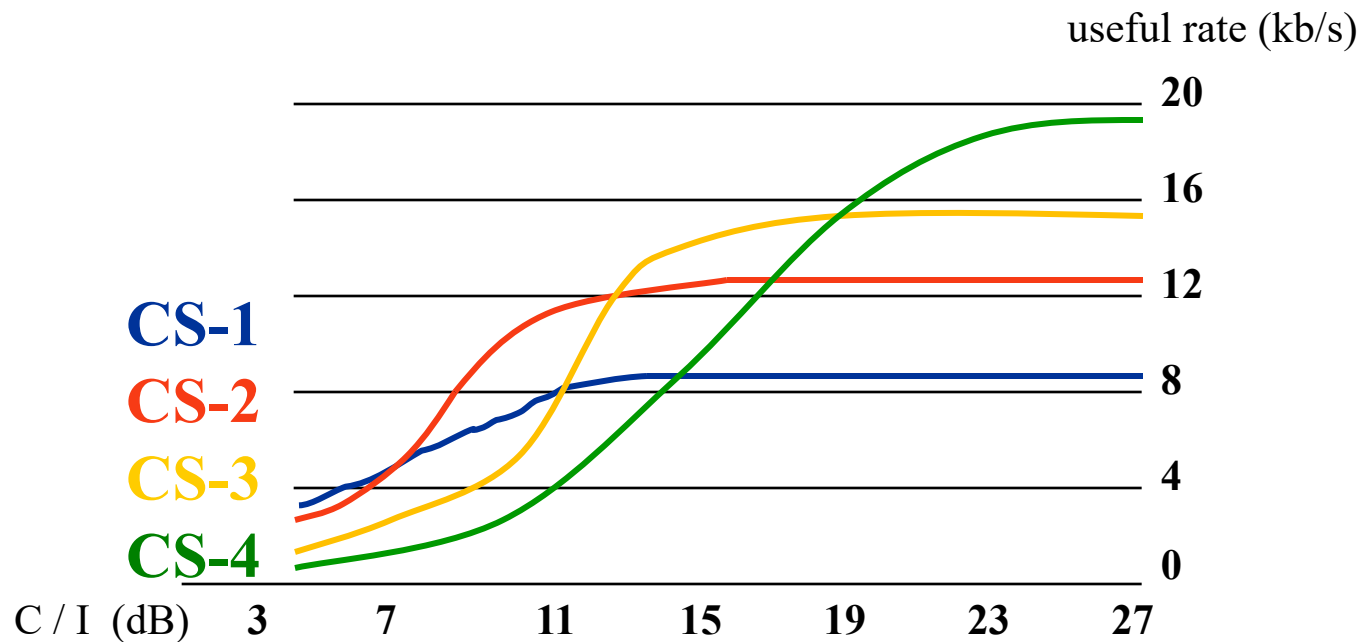


GPRS Radio Resource Management

- Downlink TBF: The mobile decodes the overhead of each downlink RLC/MAC block transmitted on the slots that are or could be allocated to the user:
 - the overhead identifies the block recipient.
 - the message of the block contains either data or control information.
- Uplink TBF: Two types of allocation resources:
 - fixed allocation:
 - at the beginning of its TBF, the mobile exactly knows when its data will be transmitted.
 - dynamic allocation:
 - the network informs the mobile about the transfer of a packet, one after the other.
 - The mobile decodes the overhead of each downlink RLC/MAC block transmitted on the slots that are or could be allocated to the user, in order to detect:
 - either a downlink signalling message from the network,
 - or an “invitation” to transfer a packet (only for dynamic allocation)

GPRS Abis interface re-dimensioning

- CS-1 & CS-2 : OK (16 kbits/s)
- CS-3 & CS-4 : NOK (32 kbits/s)



Conclusion 2.5G

- No resource monopolization
- GPRS/GSM management based on "Capacity on demand"
 - but preemption is still allocated to voice services
- Simultaneous Trans./Rec. Handsets
- ~identical logical channels
 - but dynamic multiplexing
- CS-1 & CS-2 deployment (3+1 and 4+1)
- Limitations :
 - Throughputs: 171.2 kbits/s...
 - blocks retransmission with original CS

⇒ a new evolution is necessary in the network: 2.75G:

Enhanced Data for GSM Evolution, available in France since 2002/2003

EDGE main characteristics

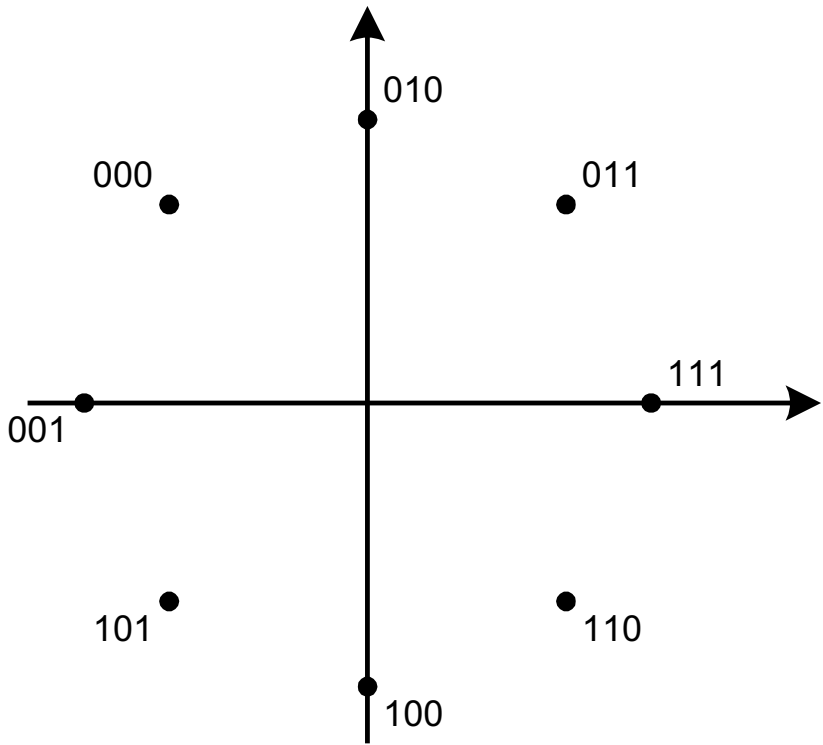
- GSM :
 - GMSK modulation
- EDGE :
 - 8PSK modulation
- data rate increased
 - $\times 3$
- new pulse shaping filter
 - 8PSK spectrum \approx GMSK spectrum

EDGE modulation 1/

- EDGE pth symbol to be transmitted:

$$s_p = e^{j k \pi / 4} \times e^{j p 3 \pi / 8}$$

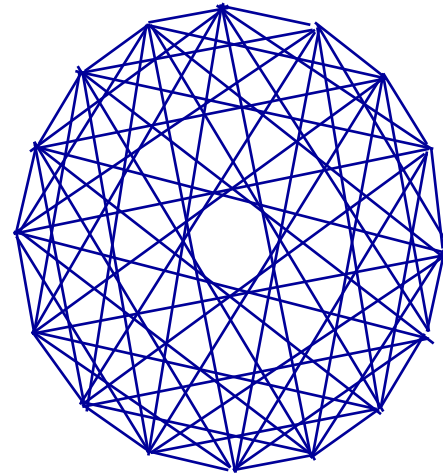
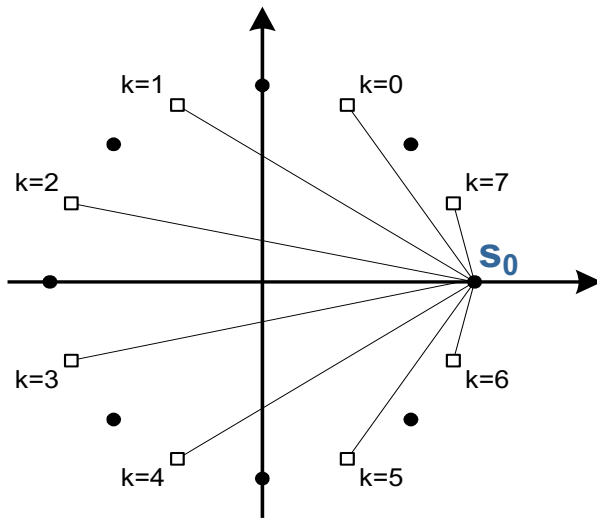
Bits to be modulated (b _{3p} b _{3p+1} b _{3p+2})	Associated symbol k
1 1 1	0
0 1 1	1
0 1 0	2
0 0 0	3
0 0 1	4
1 0 1	5
1 0 0	6
1 1 0	7



EDGE modulation

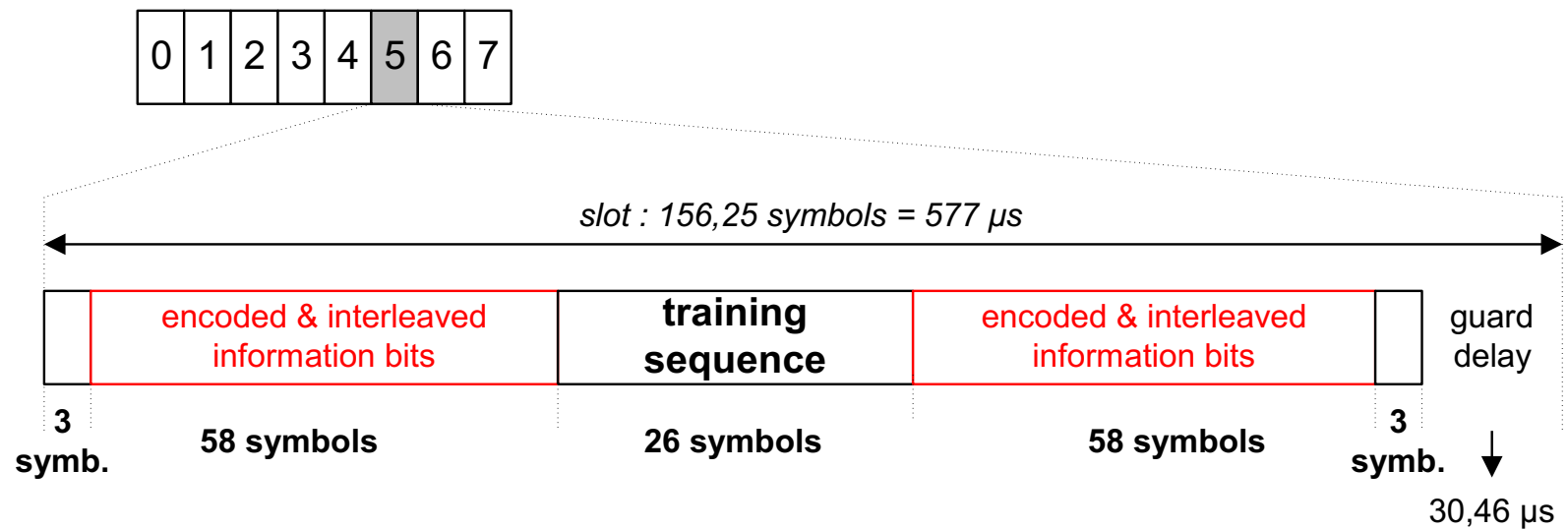
2/

- Example: $b_0 = b_1 = b_2 = 1 \Rightarrow s_0 = 1$, and s_1 symbol can take one of the 8 positions below, depending on b_3, b_4 and b_5 values:



EDGE slot structure

- one symbol = 3 bits
- data rate:
 - $116 \times 3 \text{ bits} / 5 \text{ ms} = 69,6 \text{ kbits/s}$



EDGE Throughputs

- **Circuits** services (8PSK) **ECSD** :
28.8 kbits/s, 32 kbits/s, 43.2 kbits/s

- **Packets** services **EGPRS**:

GMSK : MCS-1 to MCS-4 :

- ❑ 8.8 kbits/s ,
 - ❑ 11.2 kbits/s ,
 - ❑ 14.8 kbits/s ,
 - ❑ 17.6 kbits/s
- Bad radio conditions : ~ GPRS

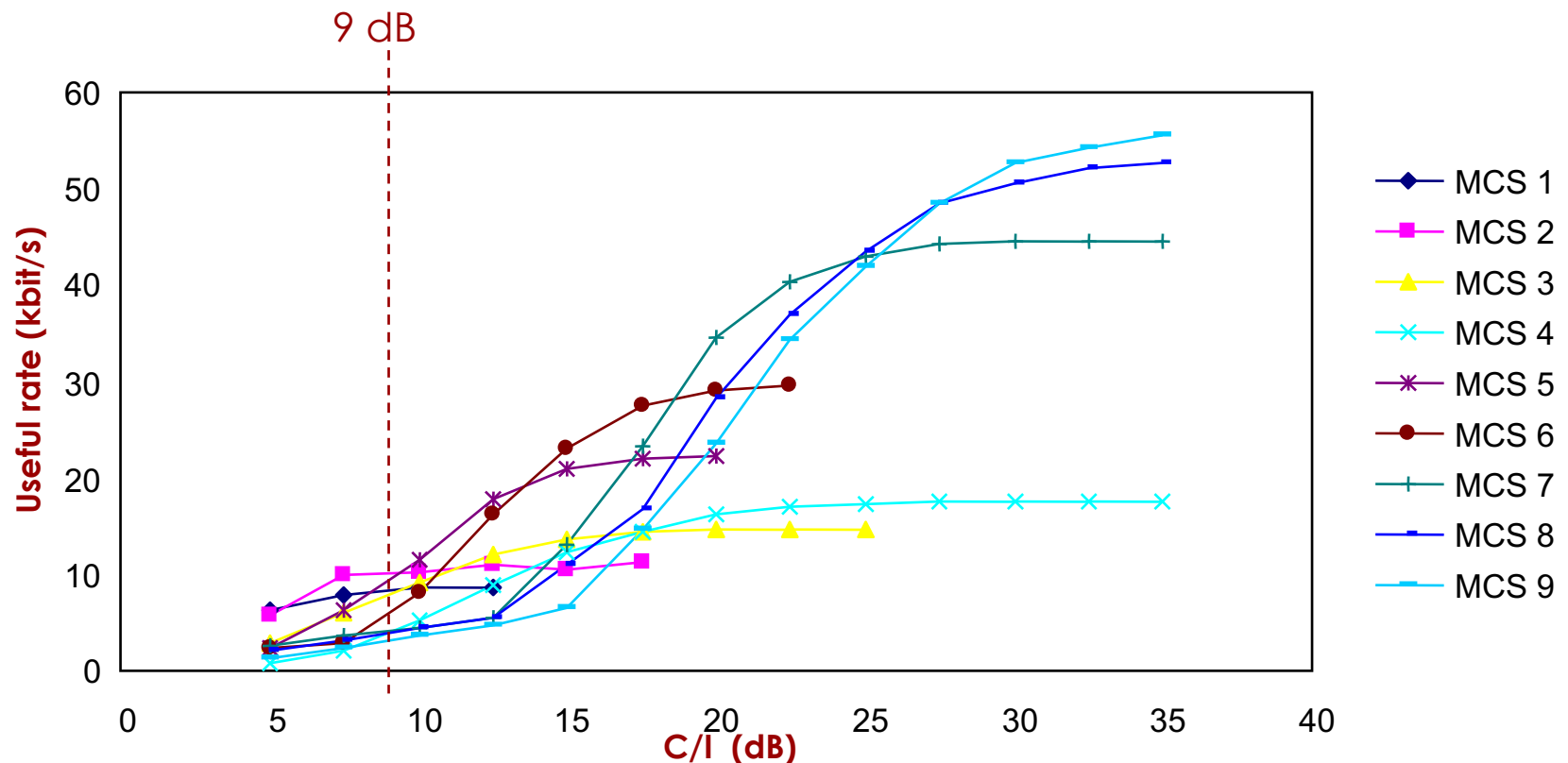
8PSK : MCS-5 to MCS-9 :

- ❑ 22.4 kbits/s,
 - ❑ 29.6 kbits/s,
 - ❑ 44.8 kbits/s,
 - ❑ 54.4 kbits/s,
 - ❑ 59.2 kbit/s
- Good radio conditions : > GPRS

Coding	Family
MCS-1	C
MCS-2	B
MCS-3	A
MCS-4	C
MCS-5	B
MCS-6	A
MCS-7	B
MCS 8	~A
MCS9	A

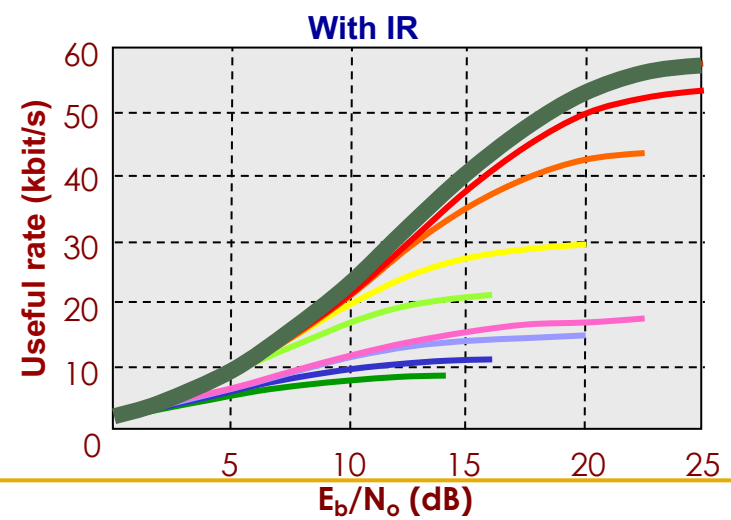
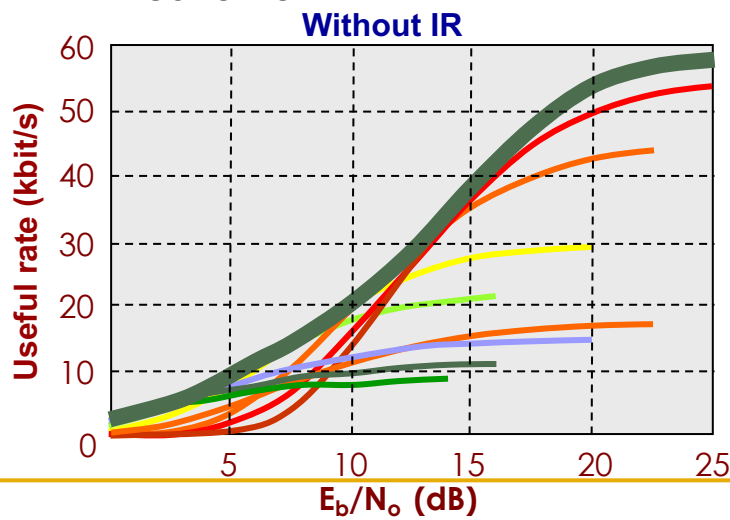
Link Adaptation in EDGE

- Link Adaptation :
 - DURING THE SESSION, selects automatically the most appropriate Modulation Coding Scheme (MCS) for transmission of the next packet
 - parameters : channel quality (Packet Error Rate)



ARQ Mechanisms in EDGE

- Automatic ReQuest for repetition:
 - When a corrupted block is received, the block is retransmitted using:
 - Type I ARQ retransmission:
 - the same MCS, or
 - a more robust MSC, issued from the same family
 - Type II ARQ (Incremental Redundancy) retransmission: retransmitted data are combined until the block is successfully decoded:
 - successive erroneous blocks are not discarded, but stored and combined
 - the block is retransmitted, using the same MCS and a different puncturing scheme



Conclusion 2,75G

- Significant and « cheap » GPRS evolution
- effective throughput:
 - ~120 kbits/s (4+1 handsets)
- market :
 - operators with no UMTS licence
- network capacity redimensionning
- additional features in BTS & new handsets
- GSM / EDGE Radio Access Network GERAN :
 - existing {GSM/GPRS + EDGE} network 'migration' for integration into 3rd generation european network: UMTS