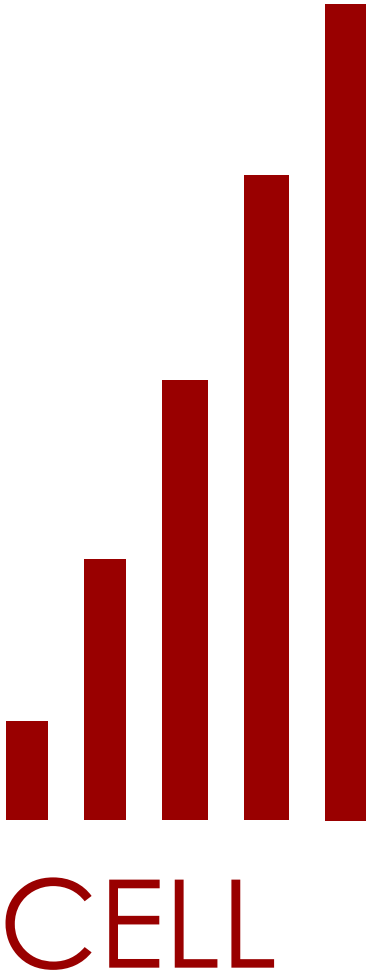


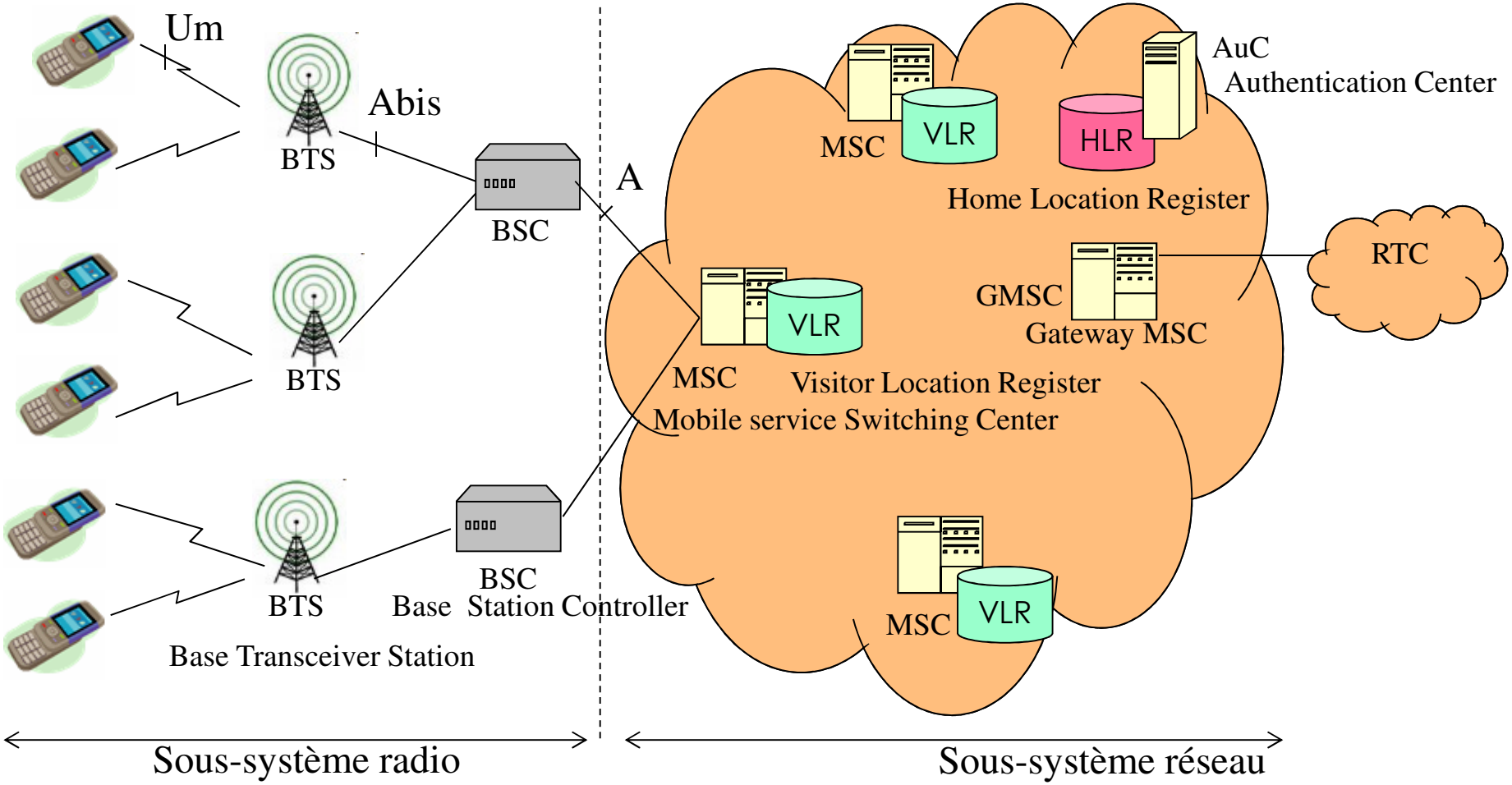
GSM

Thi-Mai-Trang Nguyen
LIP6-UPMC

Plan

- Architecture GSM
- Gestion de la sécurité
- Gestion d'itinérance
- Interface radio
- Canaux logiques

Architecture GSM (1)



Architecture GSM (2)

- Sous-système radio
  - BTS (Base Transceiver Station)
  - BSC (Base Station Controller)
- Sous-système réseau
  - MSC (Mobile service Switching Center)
  - Deux bases de données
    - HLR (Home Location Register)
    - VLR (Visitor Location Register)
  - AuC (Authentication Center)
- Terminal mobile
  - Carte SIM (Subscriber Identity Module)

Sous-système radio

- Assurer les transmissions sur l'interface air et gérer la ressource radio
- Station de base (BTS)
  - Responsable de la transmission radio
  - Modulation, démodulation, égalisation, codage correcteur erreur
  - Multiplexage TDMA, saut de fréquence lent, chiffrement, mesures radio
- Contrôleur de station de base (BSC)
  - Gérer la ressource radio
  - Allocation des canaux
  - Analyse des mesures effectués par les BTSs pour contrôler les puissances des mobiles ou BTSs
  - Décision de l'exécution d'un handover

Sous-système réseau (1)

- Commutateur du service mobile(MSC)
  - Fonction de matrice de commutation
  - Établissement des communications entre un mobile et un autre MSC
  - Exécution du handover au niveau MSC
  - Gestion de la mobilité des usagers (consulter le VLR lors d'un appel départ, transfert des informations de localisation)
  - Fonction de passerelle pour les appels avec un abonné fixe

Sous-système réseau (2)

- Deux bases de données pour la gestion des abonnés
  - Enregistreur de localisation nominal (HLR)
    - La base de données qui gère les abonnées d'un opérateur
    - Information: identité de l'abonné (IMSI), numéro d'annuaire de l'abonné (NSISDN), profil de l'abonné (services supplémentaires, autorisation d'appel international), le numéro de VLR où le mobile est enregistré
  - Enregistreur de localisation des visiteurs (VLR)
    - Une base de données des abonnés présents dans une zone géographique
    - Information: les numéros IMSI, MSISDN comme le HLR, et en plus, le numéro TMSI
- Centre d'authentification (AuC) associé au HLR
  - Détient la clé secrète de chaque abonné pour l'authentification et le chiffrement des communications

Terminal mobile

- Contient une carte à puce (carte SIM) qui comporte l'identité de l'abonné
- Authentification de l'identité de l'abonné s'effectue entre la carte SIM et le centre d'authentification (AuC)

Carte SIM
Numéro IMSI
(International Mobile Subscriber Identity)
Ex: 208 01 314159

Terminal
Numéro IMEI
(International Mobile Equipement Identity)

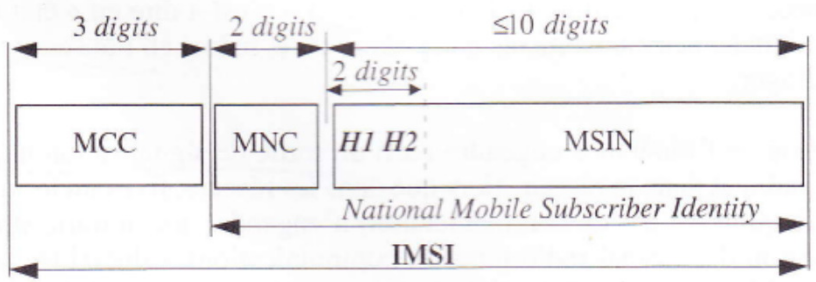
Utilisateur
Numéro MSISDN
(Mobile Station ISDN Number)
Ex: 33 6 07 62 17 73

Adressage

- IMSI
  - Identité invariante de l'abonné qui n'est connu qu'à l'intérieur du réseau GSM
- TMSI
  - Identité temporaire utilisée pour identifier le mobile lors des interactions MS – Réseau
- MSISDN
  - Le numéro d'appel de l'abonné

IMSI

- Chaque usager dispose d'une identité internationale IMSI
  - MCC (Mobile Country Code)
    - Indicatif du pays domicile de l'abonné
    - Ex: 208 pour la France
  - MNC (Mobile Network Code)
    - Indicatif du réseau nominal de l'abonné
    - Ex: 01 pour France Télécom, 10 pour SFR
  - MSIN (Mobile Subscriber Identification Number)
    - Numéro de l'abonné à l'intérieur du réseau GSM
    - Deux premiers chiffres (H1 H2) donne l'indicatif du HLR au sein de son réseau

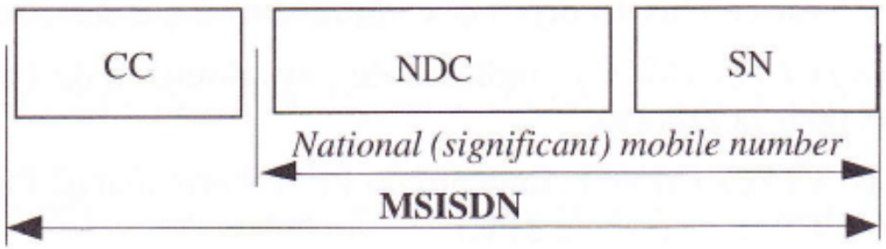


TMSI

- Temporary Mobile Subscriber Identity
- Attribuée au mobile de façon locale pour la zone gérée par le VLR courant du mobile
- N'est connu que sur la partie MS-MSC/VLR, pas au niveau d'HLR
- Utilisé pour identifier le mobile appelé ou appelant lors d'un établissement de communication
- A chaque changement de VLR, un nouveau TMSI doit être attribué
- La structure du TMSI est laissée libre à l'opérateur (codé sur 4 octets)
- Utilisation du TMSI est optionnelle (dépend de l'opérateur)

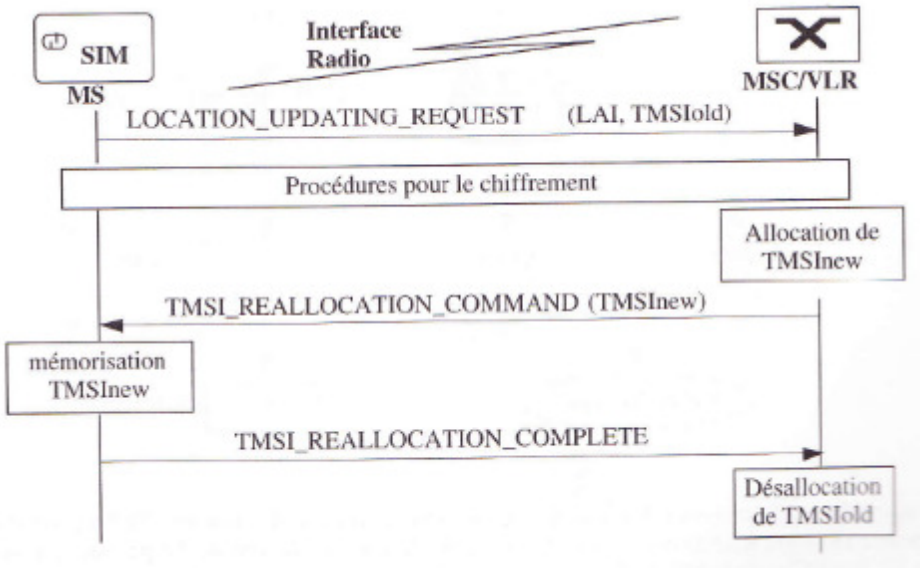
MSISDN

- Mobile Station ISDN Number
- Conforme au plan de numérotation téléphonique international E.164
- CC (Country Code)
  - Indicatif du pays de du réseau nominal de l'abonné
  - Ex: 33 pour la France
- NDC (National Destination Code)
  - Déterminer le réseau particulier dans le pays
- SN (Subscriber Number)
  - Attribué librement par l'opérateur



Confidentialité de l'identité de l'abonné

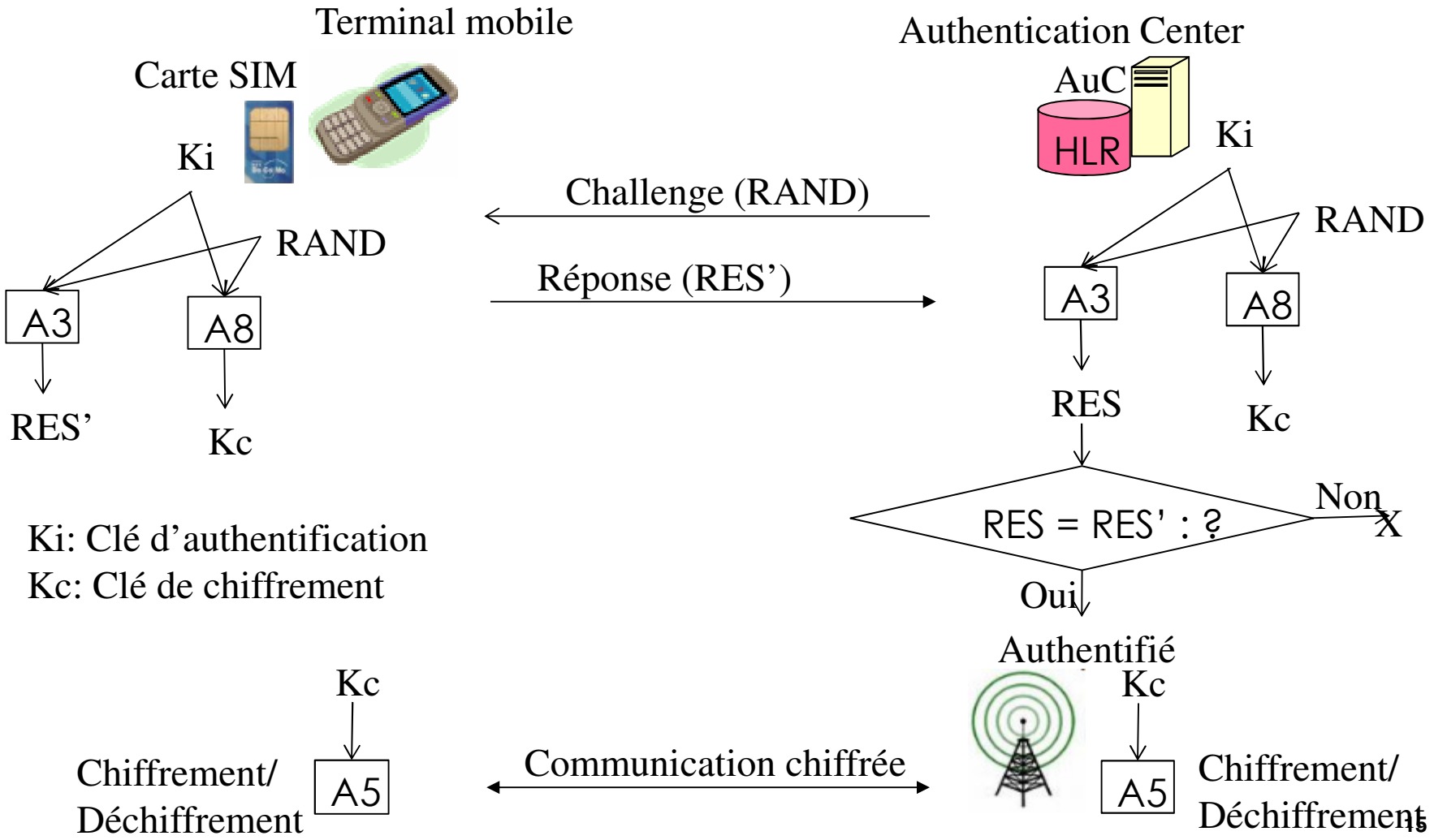
- Limiter la transmission de l'IMSI sur la voie radio
  - Utiliser le TMSI
  - La correspondance TMSI et IMSI est gérée au niveau VLR
  - TMSI est envoyé au mobile en mode chiffré



Authentification et chiffrement (1)

- Éléments
  - Deux clés: clé d'authentification Ki, clé de chiffrement Kc
  - Trois algorithmes: A3, A5, A8
  - Nombre aléatoire RAND
- Principes
  - Chaque abonné est attribuée une clé Ki propre stockée dans la carte SIM, avec l'IMSI, et dans l'AuC du réseau d'opérateur
  - Pour le chiffrement
    - La clé de chiffrement Kc est générée par l'algorithme A8 à partir de la clé Ki et le nombre aléatoire RAND
    - L'algorithme A5 utilise la clé Kc pour le chiffrement des données
  - Pour l'authentification
    - L'algorithme A3 génère un nombre SRES à partir de la clé Ki et le nombre aléatoire RAND
  - L'ensemble des trois valeurs (RAND, SRES, Kc) forme un triplet

Authentification et chiffrement (2)

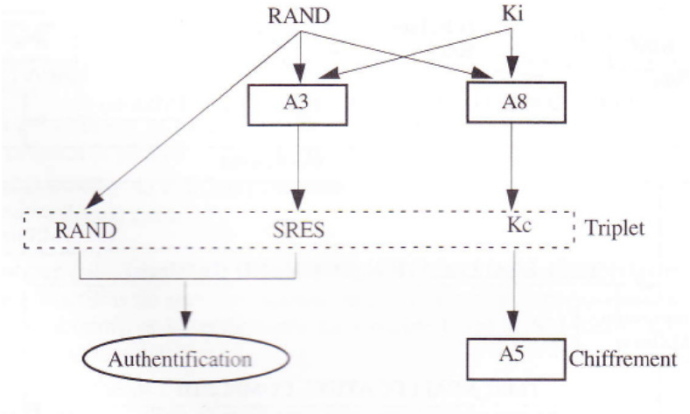


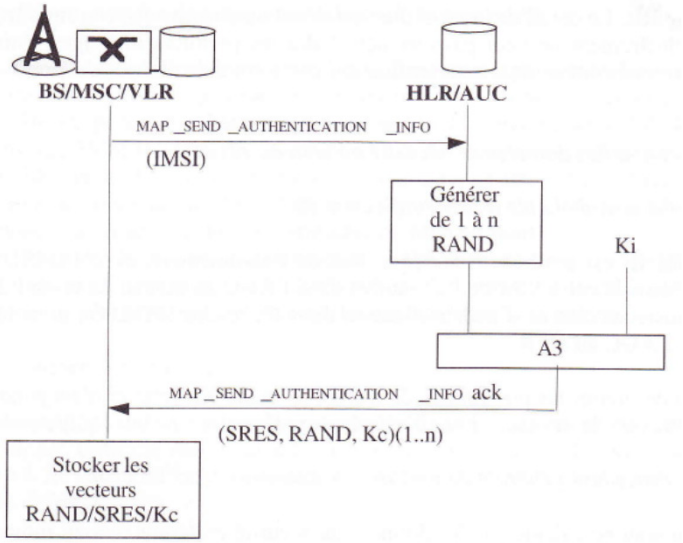
Authentification et chiffrement (3)

- Authentification
  - Permettre de vérifier que l'identité transmise par le mobile (IMSI ou TMSI) est correcte
  - A chaque mise à jours de localisation, établissement d'appel, activer/désactiver un service
- Chiffrement
  - L'algorithme de chiffrement/déchiffrement est implanté dans la BTS
  - L'activation du chiffrement se fait sur la demande du MSC

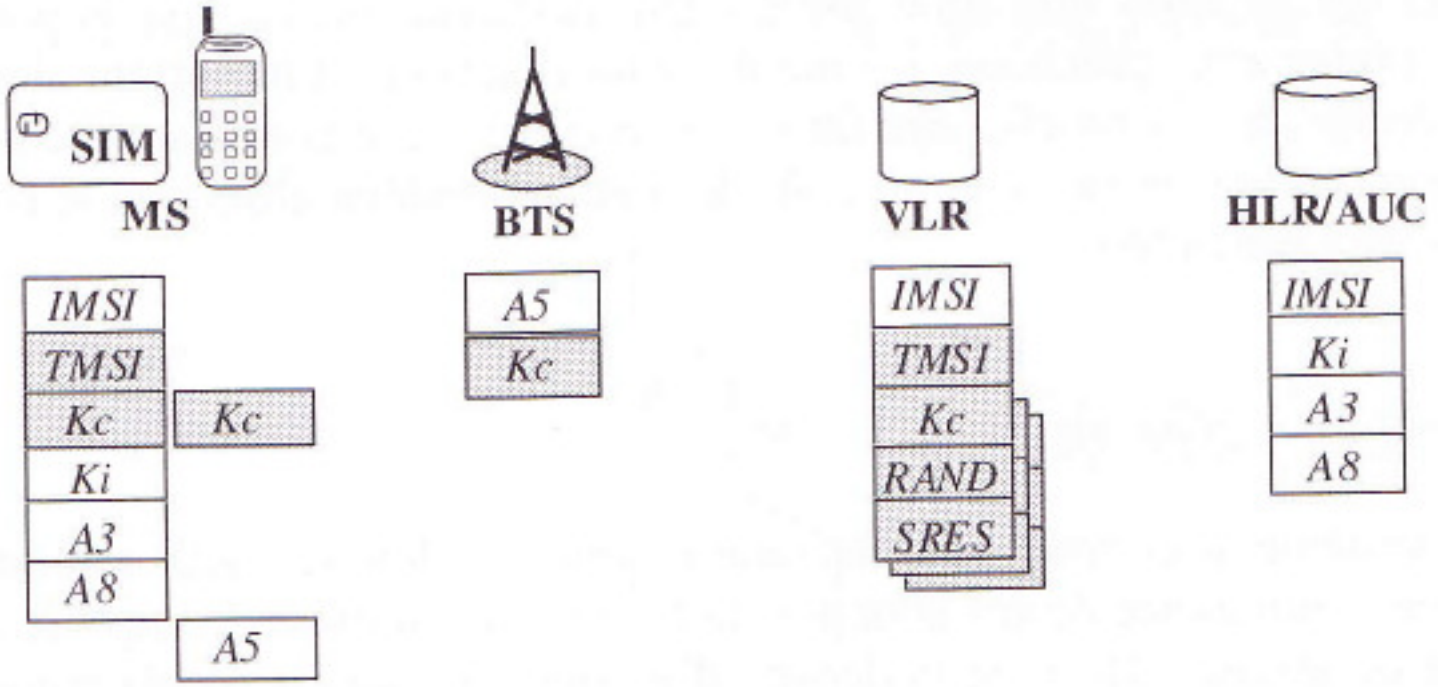
Triplet

- Le réseau qui utilise les triplets pour l'authentifier et activer le chiffrement n'a pas besoin de connaître les algorithmes A3, A8
- Les triplets sont calculés par l'AuC et envoyés au MSC/VLR
- Chaque opérateur peut avoir ses propres algorithmes A3 et A8
- L'abonné est toujours authentifié à partir des algorithmes de son réseau nominal





Vue globale de sécurité

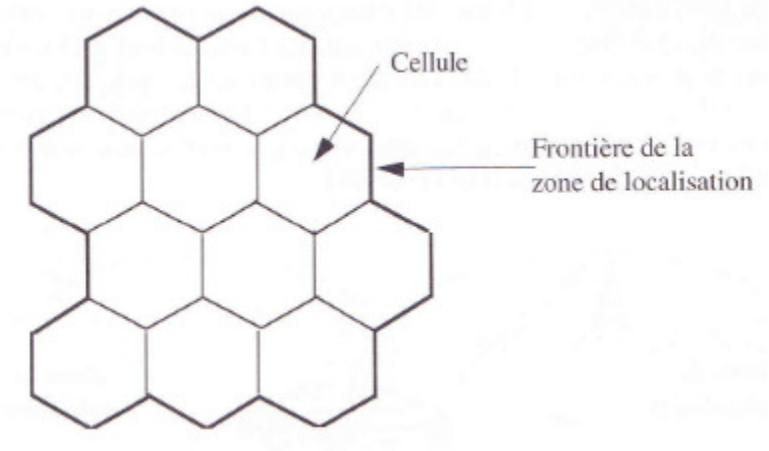


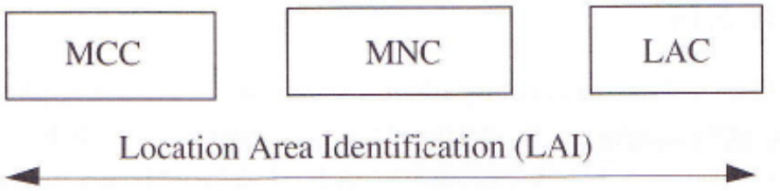
Gestion de l'itinérance

- Le système doit connaître à tout moment la localisation de chaque mobile pour pouvoir le joindre
- Le mobile doit rester actif (i.e. en état de veille), même en l'absence de communications usager, pour signaler ses mouvements au système
- La localisation de l'utilisateur est gérée par le concept de zone de localisation (LAI – Location Area identification)

Identité d'une zone de localisation

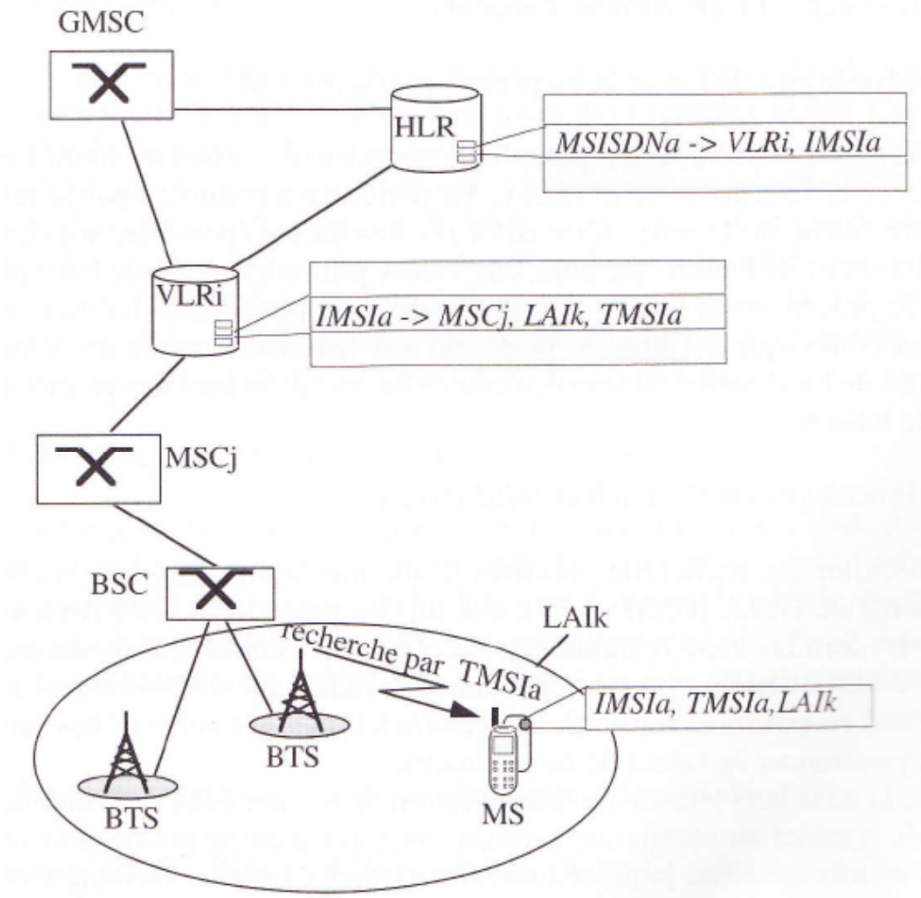
- Une zone de localisation regroupe un certain nombre de cellules
- Une zone de localisation est identifiée par l'adresse LAI (Location Area Identification)
  - MCC: indicatif du pays (comme dans l'IMSI)
  - MNC: indicatif du réseau (comme dans l'IMSI)
  - LAC (Location Area Code) (<= 2 octets): librement affecté par l'opérateur





Gestion de localisation

- Un VLR peut gérer plusieurs zones de localisation
- Une zone de localisation ne peut pas comprendre des cellules dépendant de VLR différents
- Seul le VLR mémorise la zone de localisation courante de l'ensemble des mobiles qu'il gère
- Le HLR mémorise l'identité du VLR courant de chaque abonné et non pas sa zone de localisation
- La mise à jour de localisation est initiée par les mobiles lors d'un changement de zone de localisation
- Il est possible d'avoir une mise à jour de localisation périodique avec une période contrôlée par le réseau



Procédures IMSI Attach/Detach

- Afin d'éviter les recherches inutiles d'abonnés ayant mis leur mobile hors tension
- Un paramètre dans le MSC/VLR indique si le mobile est joignable ou pas
- Lorsqu'un mobile est mis sous tension, la procédure IMSI Attach est destinée à « rattacher » ce mobile à sa zone de localisation
- Si le VLR contient des informations concernant le mobile, aucun message ne remonte jusqu'au HLR équivalent à une mise à jour sans changement de VLR
- Lors de la mise hors tension, ou lorsque le VLR n'a pas eu de contacts avec un mobile pendant une certaine période, le réseau peut le « détacher » lui-même

Procédure de paging

- Pour la recherche d'abonné lors d'un appel entrant
- Le MSC diffuse un message de paging contenant le TMSI (ou l'IMSI en cas d'absence du TMSI) de l'appelé dans les cellules de sa zone de localisation
- Le mobile répond au message de paging, réalise l'authentification et le chiffrement
- La durée d'établissement d'appel est d'environ 8 seconds

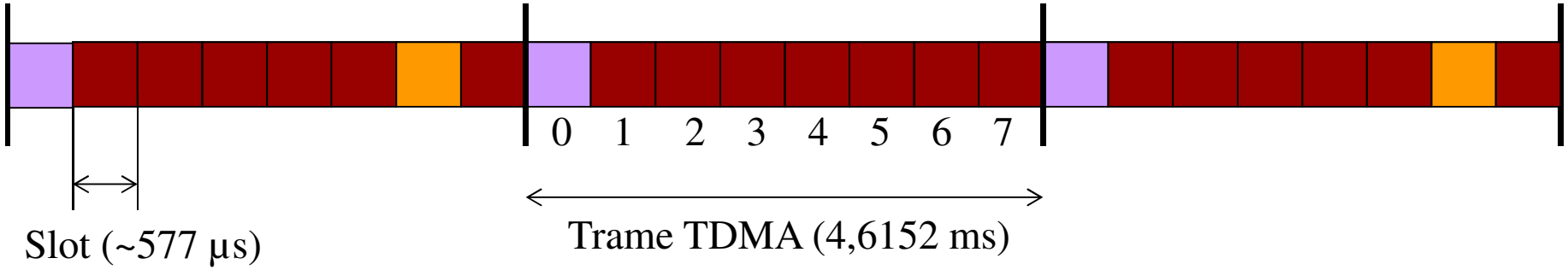
Interface radio

- Bandes de fréquences
  - Sens montant: 890 – 915 MHz
  - Sens descendant: 935 – 960 MHz
- Les bandes de fréquences sont subdivisées en canaux fréquentiels de largeur 200 KHz
  - Sur un canal, les signaux sont modulés et émis autour d'une fréquence porteuse qui siège au centre de la bande du canal
  - Dans GSM 900
    - 124 porteuses disponibles pour chaque bande de fréquences montante ou descendante

TDMA dans GSM

- Chaque porteuse est divisée en intervalles de temps appelés slots
  - T_{slot} = 0,5769 ms
- Sur une même porteuse, les slots sont regroupés par paquets de 8 pour former une trame TDMA
  - T_{TDMA} = 8 * Tslot = 4,6152 ms
- Chaque utilisateur utilise un slot par trame TDMA
- Un « canal physique » est constitué par la répétition périodique d'un slot dans la trame TDMA sur une fréquence particulière

Trame TDMA



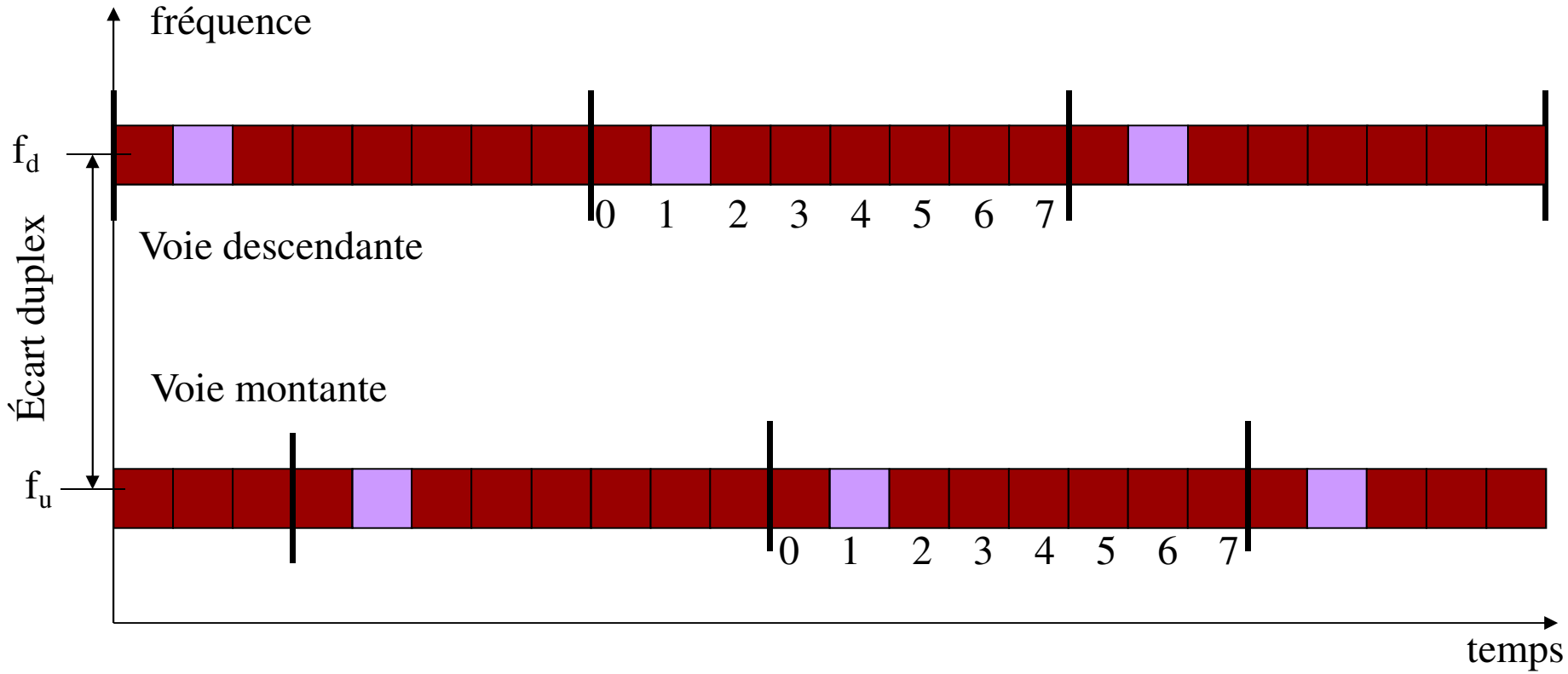
Un canal physique simplex plein débit sans saut de fréquence

Un canal physique simplex demi-débit sans saut de fréquence

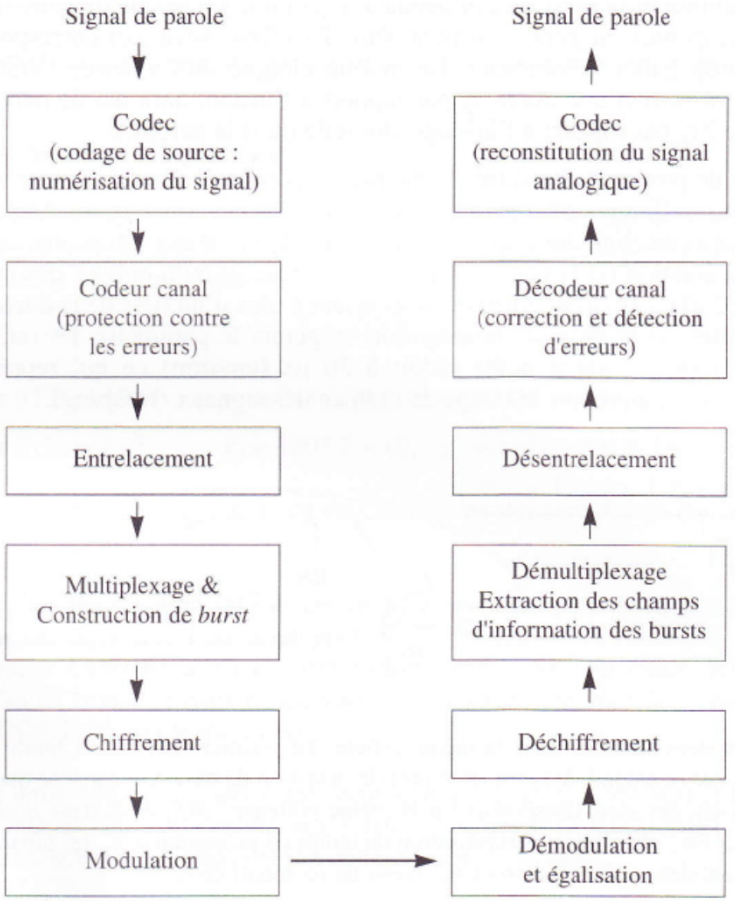
Duplexage

- Un canal physique duplex correspond à deux canaux physiques simplex
  - $f_{u(i)} = f_{d(i)} - \Delta W_{duplex}$
    - $f_{d(i)}$: la fréquence de la voie descendante
    - $f_{u(i)}$: la fréquence de la voie montante
    - ΔW_{duplex} est l'écart duplex (45 MHz en GSM)
- Les fréquences des voies descendantes en GSM 900
  - $f_d = 935 + (0,2 * n)$, $1 \leq n \leq 124$
- Un mobile émet et reçoit à des instants différents de trois slots

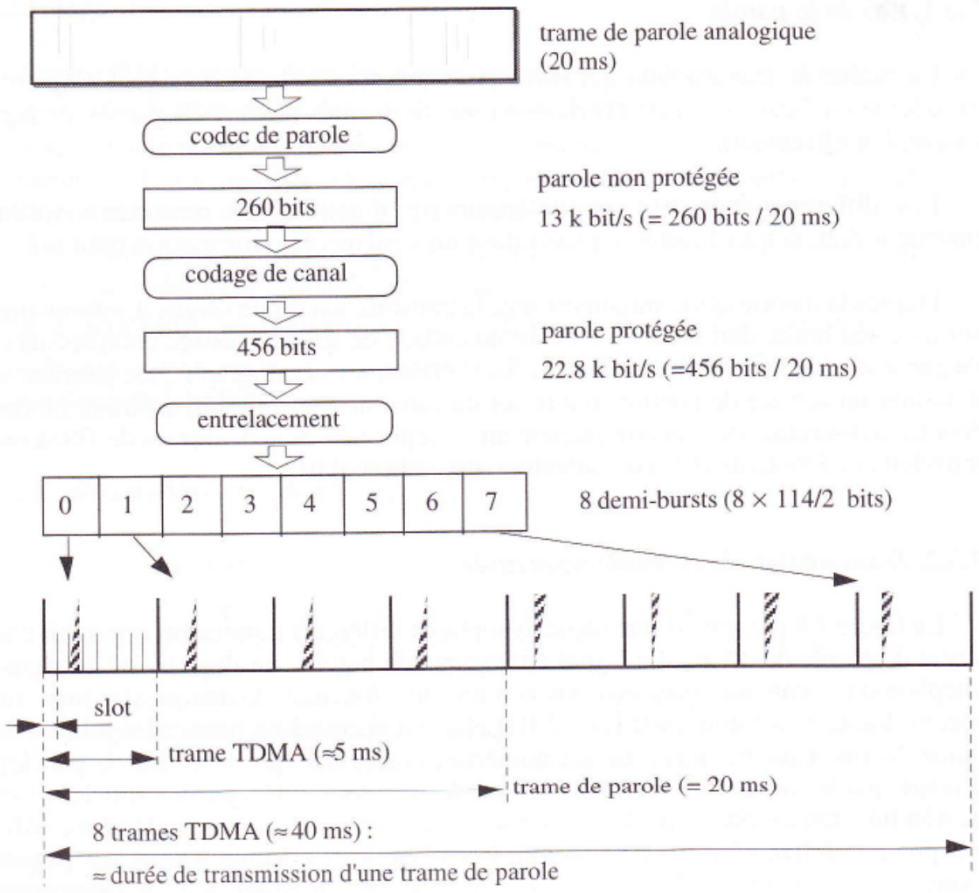
Canal physique duplex



Transmission de la voix (1)



Transmission de la voix (2)

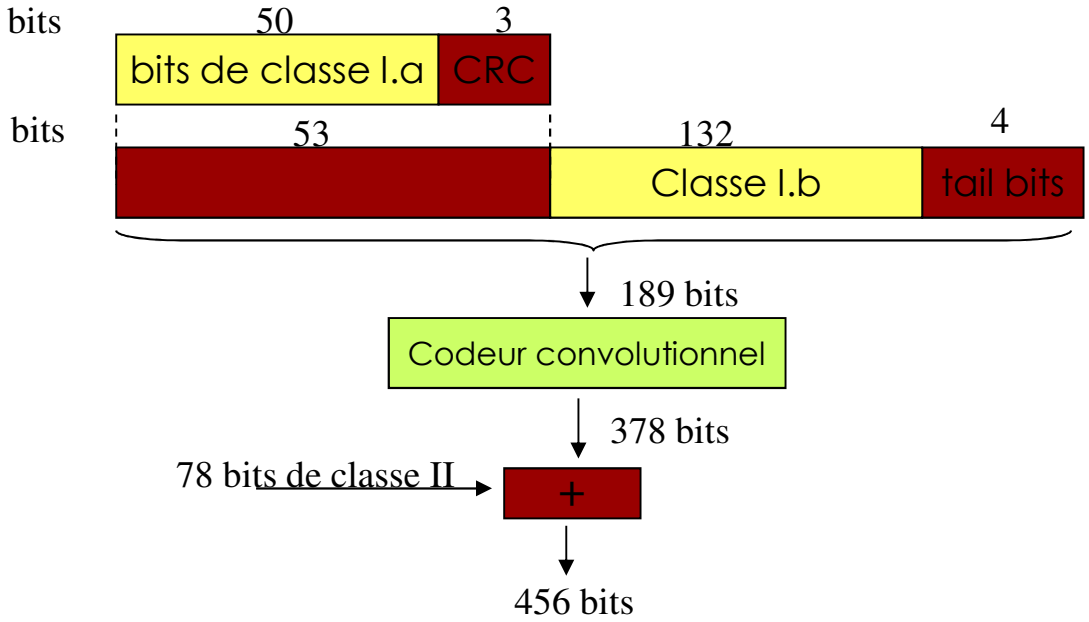


Codage de parole

- Plein débit
  - 13 Kbit/s
  - La voix est échantillonnée à 8 kHz et formée en trames de 20 ms
  - Le codec RPE-LTP (Regular Pulse Excitation – Long Term Prediction) transforme des segments de 20 ms de parole en blocs de 260 bits
- Demi-débit
  - 5,6 Kbit/s

Codage de canal (1)

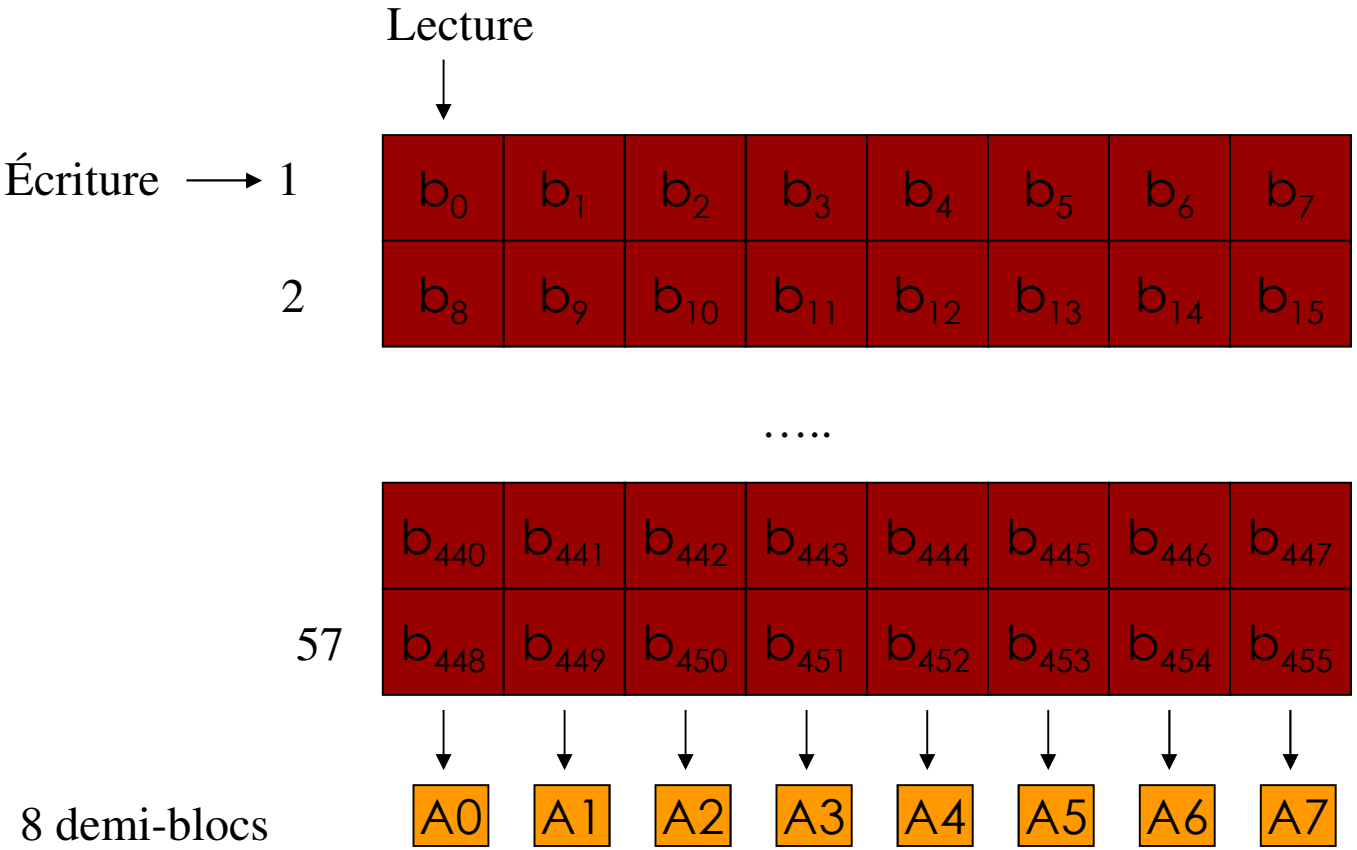
- Les 260 bits de parole n'ont pas tous la même importance
  - Classe I.a – 50 bits très sensibles aux erreurs
  - Classe I.b – 132 bits sensibles aux erreurs
  - Classe II – 78 bits moins sensibles aux erreurs



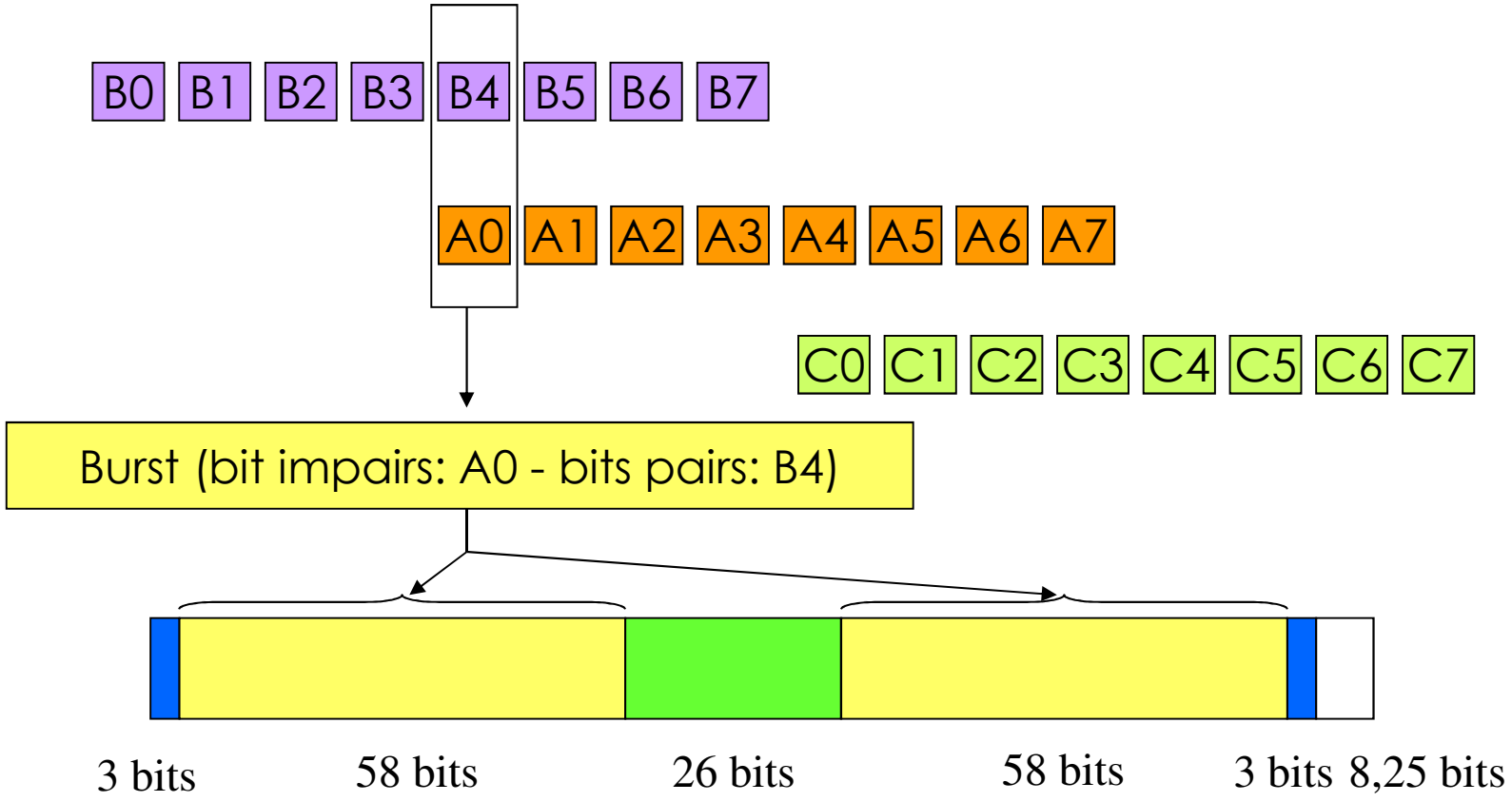
Entrelacement (1)

- Entrelacement est utilisé pour rendre plus aléatoire les positions des erreurs qui arrivent en salves dans le contexte radio
- Les symboles codés sont permutés avant leur transmission pour rendre la correction d'erreur en réception plus facile
- Entrelacement comporte
  - Un mélange des bits constituant un bloc codé
  - Une répartition des symboles brassés sur un certain nombre de bursts

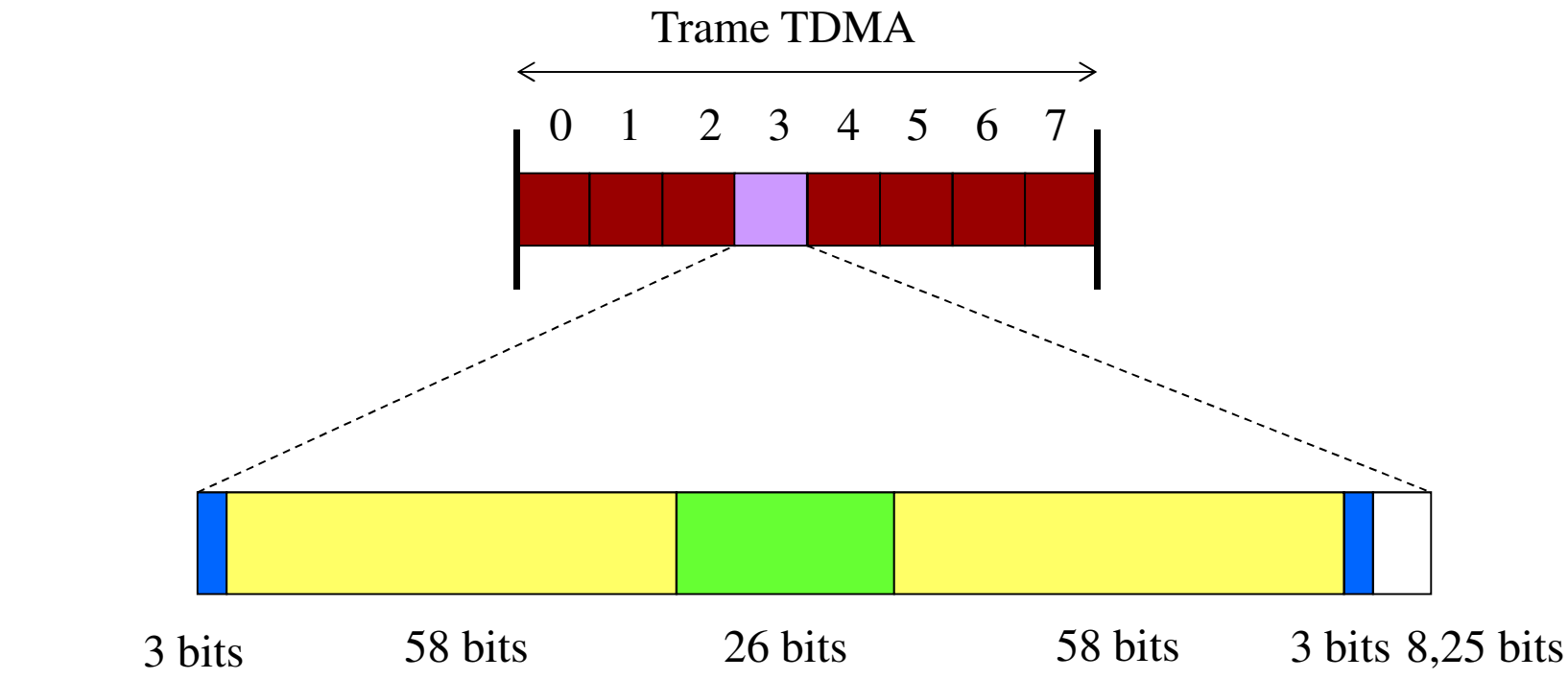
Entrelacement (2)



Entrelacement (3)



Formation du burst



Canaux logiques (1)

- Sur les canaux physiques, plusieurs canaux logiques ont été définis pour les différents types de fonction
  - Transport des données utilisateurs
  - Les fonctions de contrôle
    - Le mobile se rattache à une station de base favorable
    - Établir d'une communication
    - Surveiller le déroulement d'une communication
    - Assurer les handovers

Canaux logiques (2)

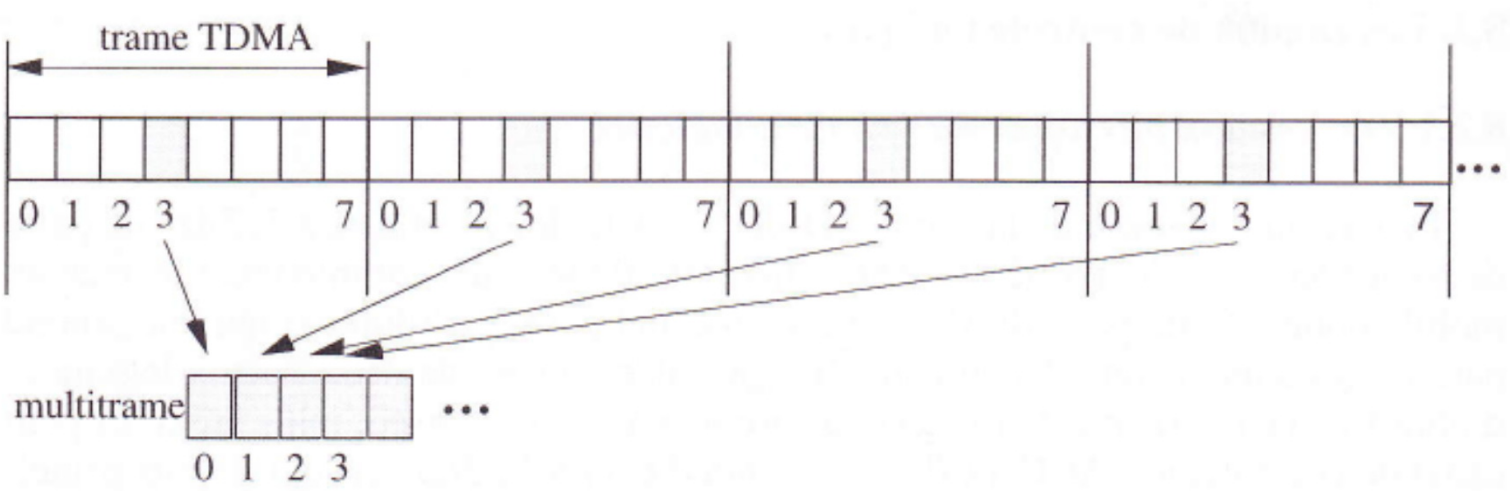
Broadcast Channel (BCH) ↓ unidirectionnel en diffusion (voie balise)	Frequency Correction Channel (FCCH) ↓	Calage sur fréquence porteuse
	Synchronization Channel (SCH) ↓	Synchronisation + Identification
	Broadcast Control Channel (BCCH) ↓	Information système
Common Control Channel (CCCH) (↓) (↑) accès partagé	Paging Channel (PCH) ↓	Appel du mobile
	Random Access Channel (RACH) ↑	Accès aléatoire du mobile
	Access Grant Channel (AGCH) ↓	Allocation de ressource
	Cell Broadcast Channel (CBCH) ↓	Messages courts diffusés

Canaux logiques (3)

Dedicated Control Channel	Stand-Alone Dedicated Control Channel (SDCCH) ↓↑	Signalisation
	Slow Associated Control Channel (SACCH) ↓↑	Supervision de la liaison
	Fast Associated Control Channel (FACCH) ↓↑	Exécution du handover
Traffic Channel (TCH)	Traffic Channel for coded speech (TCH/FS) et (TCH/HS) ↓↑	Voix plein/demi débit
	Traffic Channel for data ↓↑ (user rate) 9,6 kbit/s, 4,8 kbit/s, < 2,4 kbit/s	Données utilisateur

Multitrame

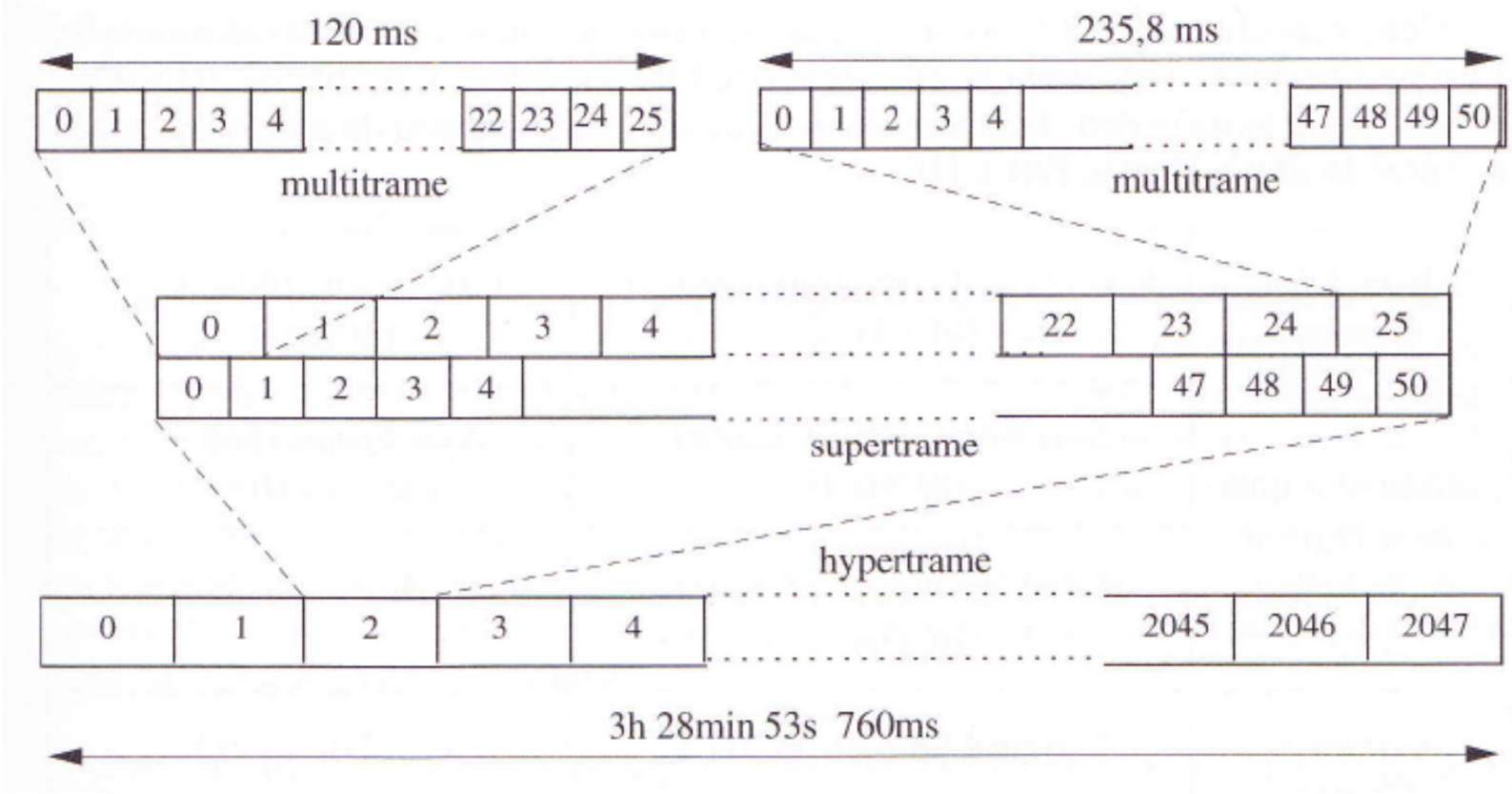
- Une multitrame est une succession d'un slot donné
- Entre deux slots d'une multitrame, il s'écoule 4,615 ms



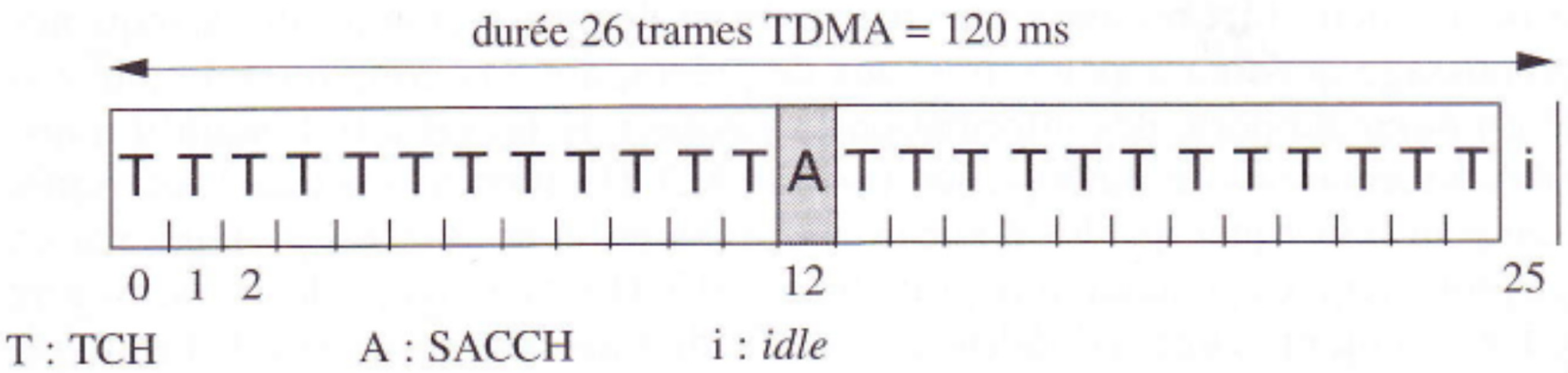
Multitrame, supertrame et hypertrame (1)

- Deux structures de multitrame sont définies
  - Multitrame à 26 trames
    - Durée de 120 ms
  - Multitrame à 51 trames
    - Durée de 235,8 ms
- Supertrame
  - Pour avoir une structure commune à deux types de multitrame
  - Composée de [26 multitrames à 51] ou [51 multitrames à 26]
- Hypertrame
  - Composée de 2048 supertrames
  - Durée de 3h 28min 53s 760ms
  - Chaque trame TDMA est repérée dans l'hypertrame par un compteur FN (Frame Number) qui est transmis régulièrement par le BTS

Multitrame, supertrame et hypertrame (2)



Multiplexage TCH-SACCH (1)



Multiplexage TCH-SACCH (2)

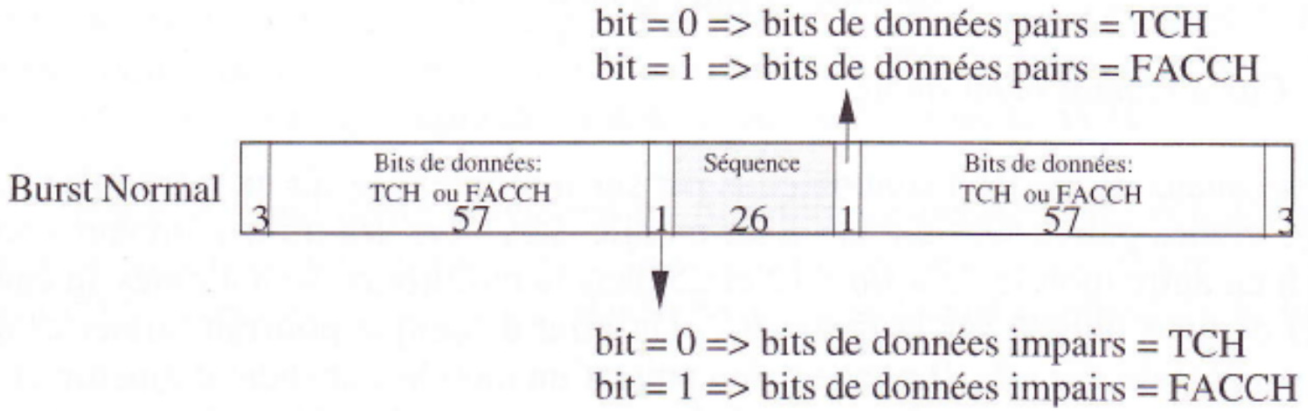
- 1 bloc de parole est de 20 ms
  - 260 bits à transmettre dans 8 demi-bursts (4 bursts)
  - 1 burst de parole tous les 5 ms est requis
- Une multitrame à 26 dure 120 ms
  - 6 blocs de parole (24 bursts) à transmettre
  - Le mobile dispose 26 slots
  - 2 slots sont libres
    - 1 slot pour le canal SACCH
    - 1 slot de repos (le mobile scrute les voies balise des cellules voisines)

SACCH

- Slow Associated Control Channel
  - Contrôle des paramètres physiques de la liaison
  - Compensation du délai de propagation aller-retour
  - Contrôle de la puissance d'émission du terminal mobile
  - Contrôle de la qualité du lien radio
  - Gestion des mesures effectuées sur les stations voisines

FACCH

- Fast Associated Control Channel
- Le débit faible du canal SACCH (380 bit/s) ne convient pas à l'exécution du handover
- Le canal TCH est temporairement volé pour écouler la signalisation



Voie balise (1)

- Beacon channel
- Propre à chaque station de base
- Permettre aux mobiles de se raccorder en permanence à la station de base la plus favorable
- Jouer le rôle essentiel pour réaliser l'itinérance et le handover
- Correspondre à une fréquence particulière appartenant à l'ensemble des fréquences allouées à la station de base
- Un mobile du voisinage mesure périodiquement sur cette voie le niveau de signal
- Permettre à un mobile de déterminer s'il est à la portée de la station, proche ou éloigné de la station

Voie balise (2)

- Informations
  - Signaux de forme spécifique
    - Permettre aux mobiles de détecter la présence de la station de base et de se caler en fréquence et en temps
  - Informations systèmes
    - Identité du réseau et les caractéristiques d'accès
- Terminal mobile
  - A la mise sous tension
    - Chercher à se caler sur la voie balise de la BTS la plus favorable
  - En état de veille
    - Surveiller constamment les voies de balises de la cellule courante et des cellules avoisinantes pour changer la cellule si nécessaire
  - En communication
    - Ecouter périodiquement les voies balises des cellules avoisinantes pour réaliser un handover si nécessaire

RACH – AGCH – PCH

- Random Access CHannel
  - Lorsque les mobiles veulent effectuer une opération sur le réseau (localisation, appel, etc.), ils doivent le signaler au réseau par une requête envoyée sur le canal RACH
- Access Grant CHannel
  - Lorsque l'infrastructure reçoit une requête venant d'un mobile, il faut allouer un canal de signalisation dédié par un message d'allocation sur le canal AGCH contenant le numéro de porteuse et le numéro de slot
- Paging CHannel
  - Lorsque l'infrastructure désire communiquer avec un mobile (pour un appel, une authentification, etc.), elle diffuse l'identité du mobile sur un ensemble de cellules grâce au canal PCH