Global System for Mobile communications

SOMMAIRE

I. INTRODUCTION

1°) Objectif des systèmes de télécommunications.

- Transmettre entre deux abonnés une communication voix ou donnée.
- Assurer ce service de façon permanente, fiable et d'accès rapide à tous les utilisateurs.
- Assurer la confidentialité des communications.
- Assurer l'authentification des utilisateurs de ces services sans ambiguïté afin d'établir les facturations afférentes.
- Proposer des services supplémentaires tels que :
  - renvoi d'appel,
  - conférence,
  - identification de l'appelant, ….

2°) Création d'un service supplémentaire permettant la mobilité de l'usagé.

Ce service était destiné à l'origine à certains professionnels (Police, Secours, Entreprises de transport …)

3°) Historique

1970 : création des premiers systèmes radio mobiles de 1ere génération (analogiques).

1979 : Bande 900 MHz réservé en Europe pour les communications mobiles

1982 : Création du Groupe Spécial Mobile pour la spécification d'un système à l'horizon 1990. Allocation des fréquences :

890-915 MHz : Mobile vers station de base

935-960 MHz : station de base vers mobile

1985 : Choix de la transmission numérique AMRT (choix du type de modulation, du codage de canal et du codage de la parole).

1986 : Ouverture du réseau Radiocom 2000 et Ligne SFR

1987 : Signature du MOU (Memorandum of Understanding) par 13 pays européens pour le déploiement simultané de système GSM.

1990 : Gel des spécifications GSM & Digital Cellular System dans la bande 1800 MHz

1991 : 1ère Communication GSM entre un Mobile et un Abonné RTC

1992 : Ouverture du réseau GSM de France Télécom ITINERIS

1994 : Apogée des réseaux analogiques Radiocom 2000 et Ligne SFR

1995 : Développement exponentiel du réseau GSM

2005 : GSM présent dans 120 pays (la norme numérique la plus utilisées), 45 millions d'abonnés en France, plus d'un milliard d'utilisateur sur

4°) Première génération de téléphonie mobile analogique

Grand nombre de standards incompatibles : R2000 (France Télécom), NMT (SFR).
Service limité aux territoires nationaux et pas d'économie d'échelle pour les constructeurs.

- Fonctionnement à 450 MHz en modulation de fréquence ou de phase.
- Grosse occupation spectrale.
- Un émetteur de forte puissance placé sur un point haut donc grosse zone de couverture.
- Faible trafic écoulé (répartition par multiplexage en fréquence).
- Pas de mobilité possible d'une zone de couverture à l'autre (pas de continuité de la communication).
- 460 000 abonnés max.

5°) Objectifs du GSM

Service de téléphonie mobile de voie et de données compatibles avec les réseaux fixes (Analogiques, RNIS et données par paquets) sur l'ensemble du territoire européen.

Efficacité ⇒ transmission numérique

Souplesse pour convenir aux zones rurales et urbaines

Protection (confidentialité pour usagers et sécurité pour les opérateurs).

Services compatibles avec le RNIS

Utilisation possible dans toute l'Europe.

II. Les Contraintes générées par la mobilité

1°) Le vecteur de transmission n'est plus filaire.

Solution :

Le seul vecteur de transmission permettant de transporter une information sans liaison filaire est un vecteur radiofréquence.

2°) Le territoire ou le service est proposé doit être parfaitement couvert.

Solution :

Définition d'un PLMN

PSTN : Public Switched Téléphone Network

PLMN : Public Land Mobile Network, réseau établi par un opérateur pour offrir un service de communication mobile sur un territoire national.

Un PLMN peut accueillir des abonnées d'autre PLMN Itinérances ou Roaming

Un PLMN s'appuie sur le réseau téléphonique classique pour recevoir et transmettre les appels relatifs à des abonnées fixes

3°) L'acheminement des communications doit être possible.

Solution :

Localisation et identification des utilisateurs des services.

L'abonné est identifié par son numéro de téléphone (MSISDN).

Grâce à ce numéro il est possible de connaître le central de rattachement du mobile (HLR).

Ce central connaît et met à jour de façon permanente la zone dans laquelle se trouve l'abonné. Cette zone est sous le contrôle d'un autre central (VLR).

Ce central peut communiquer avec le mobile via un émetteur récepteur radiofréquence (BTS).

La recherche de l'abonné est réalisée par une méthode similaire à de l'adressage indirect de mémoire

Vocabulaire :

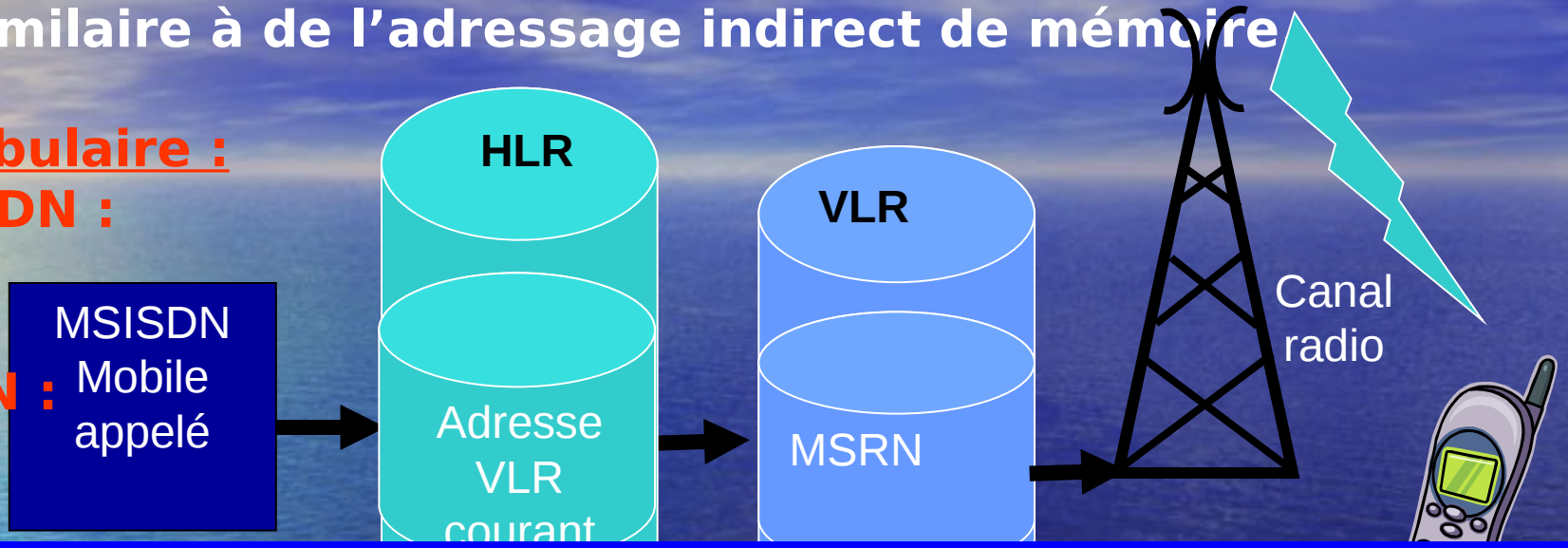
MSISDN :

HLR :

VLR :

MSRN :

BTS :



MSRN : (Mobile station roaming number)

C'est un numéro temporaire attribué par le VLR à l'abonné présent dans sa zone de couverture et transmis au HLR de l'abonné lors d'une demande de communication vers le mobile. C'est en fait le vrai numéro qui permettra le routage de l'appel vers le mobile.

Ce numéro est composé de 3 champs:

BTS : (base Transceiver station)

équipement composé des émetteurs récepteurs radio et constituant l'interface entre les mobiles et le réseau.

courant du mobile.

SN : numéro identifiant une ligne du VLR et réservé à l'abonné pour l'établissement de la communication

4°) L'accès à ce service doit être étendu à toutes les catégories d'usagés.

Solution :

4.1) Partage des ressources radios

Découpage du PLMN en cellule de taille plus ou moins grande permettant de réutiliser les canaux de transmission physiques sur des cellules non adjacentes.

Multiplexage fréquentiel de la ressource radio fréquence en canal de transmission radio fréquence (ARFC).

Multiplexage temporel (TDMA) du canal de transmission radio fréquence donnant un canal de transmission physique.

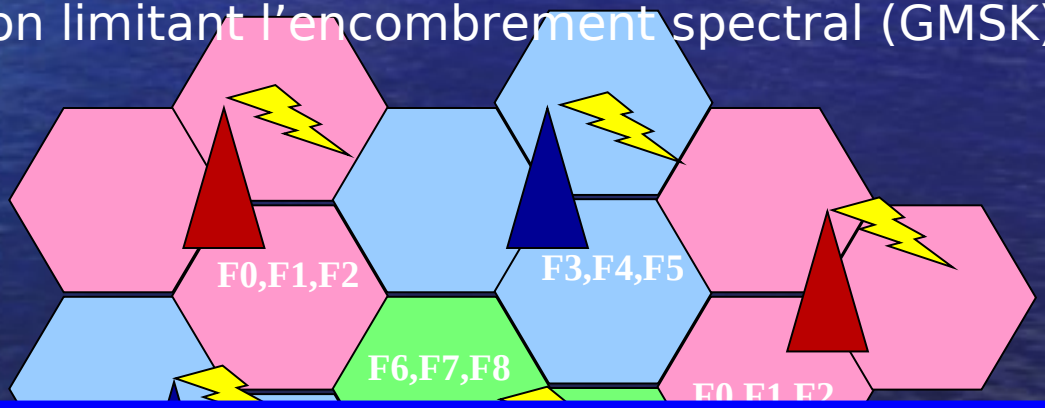
Utilisation d'une modulation limitant l'encombrement spectral (GMSK).

Vocabulaire :

ARFC :

TDMA

GMSK :



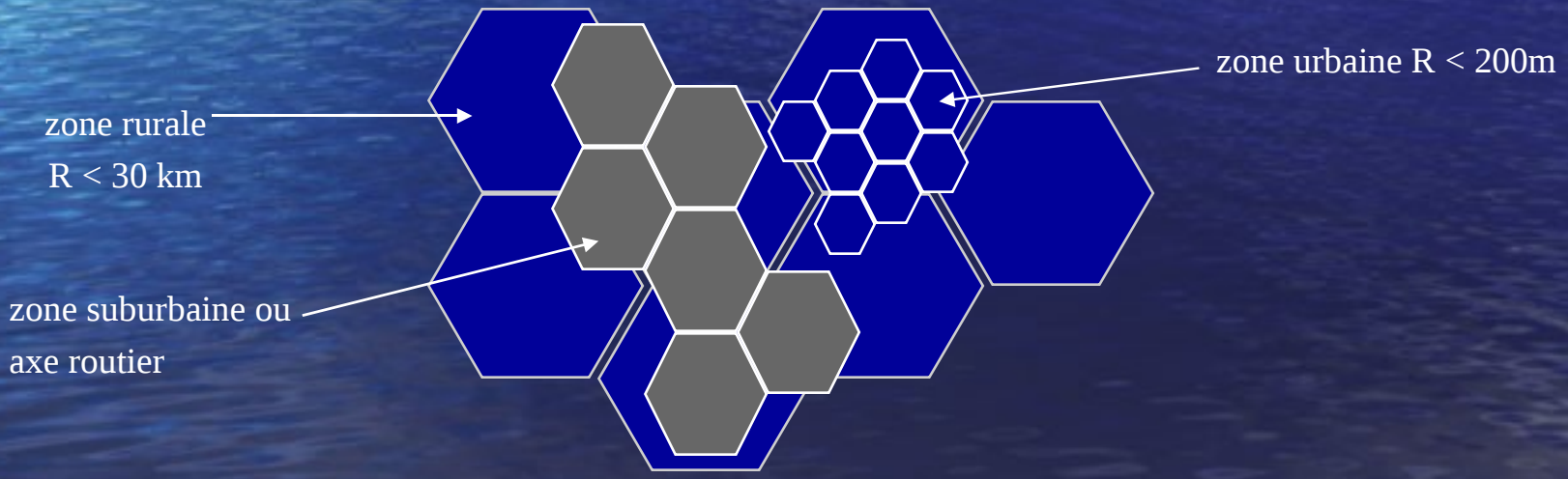
TDMA (Time Division Multiple Access ou AMRT) : La trame TDMA (4,6152ms) est découpée en 8 IT (0,5769ms) appelés slots.

GMSK (gaussian filtered Minimum shift keying) : modulation PM d'un signal numérique (BPSK) filtré par un filtre passe bas

4.2) Le principe cellulaire

émetteurs de faible puissance dont la portée est limitée (par cette faible puissance et par des gammes de fréquences plus élevées) à une zone appelée cellule ⇨ appellation "**Téléphone Cellulaire**".

les cellules adjacentes utilisent des fréquences différentes (limitations des interférences).



4.3) La réutilisation des fréquences

spectre de fréquences disponible (= ressource radio) et portée des sites sont limités ⇨ on réutilise les mêmes fréquences sur plusieurs cellules

cette réutilisation se fait de manière à minimiser les interférences

(co-canal et canal adjacent). Elle peut se faire suivant un motif ou non.

motif régulier

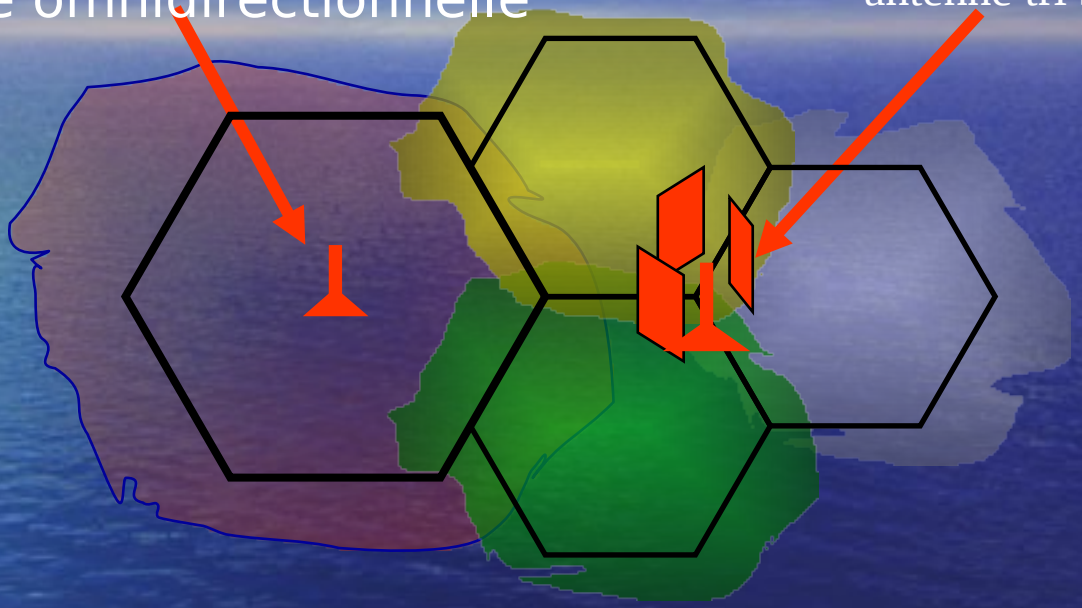
à 7 fréquences

4.4) Les antennes

- Les émetteurs sont généralement équipés d'antennes omnidirectionnelles ou tri sectorielles.

antenne omnidirectionnelle

antenne tri sectorielle

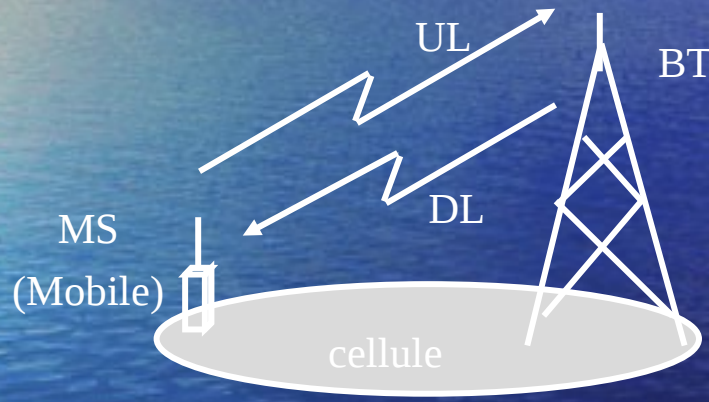


Environnement	Densité de BTS	Rayon de cellule
Grande Ville	1 pour 8 à 10000 habitants	200 m à 750 m
Ville moyenne et petite	1 pour 10 à 15000 habitants	750 m à 1500 m
Axe routier, Zone rurale	-	3 à 15 km

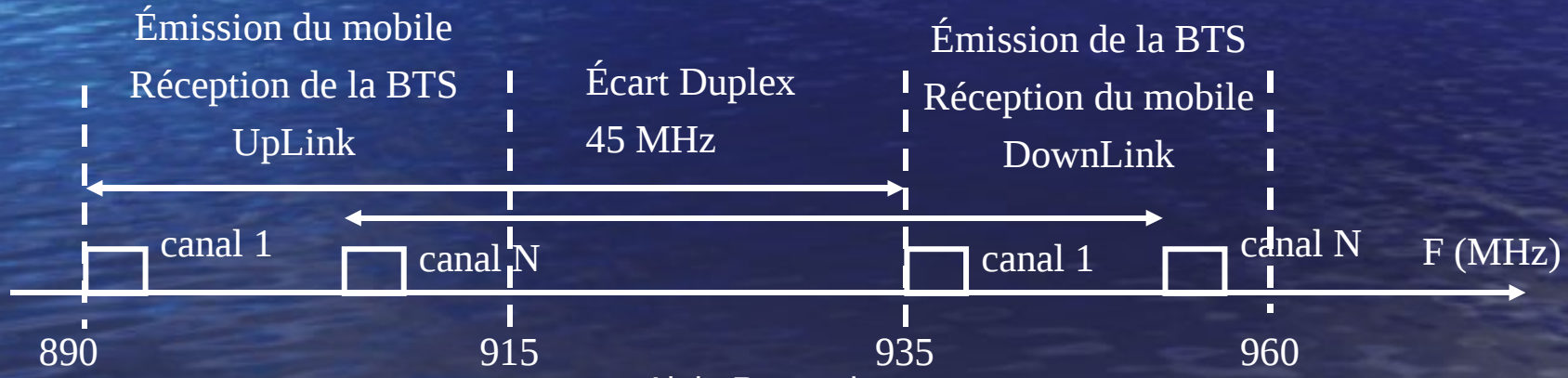
4.5) La liaison hertzienne

liaison hertzienne ou interface Air (interface Um) : entre le terminal mobile (ME – Mobile Equipment) et la station de base (BTS). Elle est basée sur :

Le duplexage fréquentiel : une partie de la bande de fréquence est réservée à la liaison mobile - BTS (Liaison montante - UpLink), l'autre à la liaison BTS - mobile (Liaison descendante - DownLink).



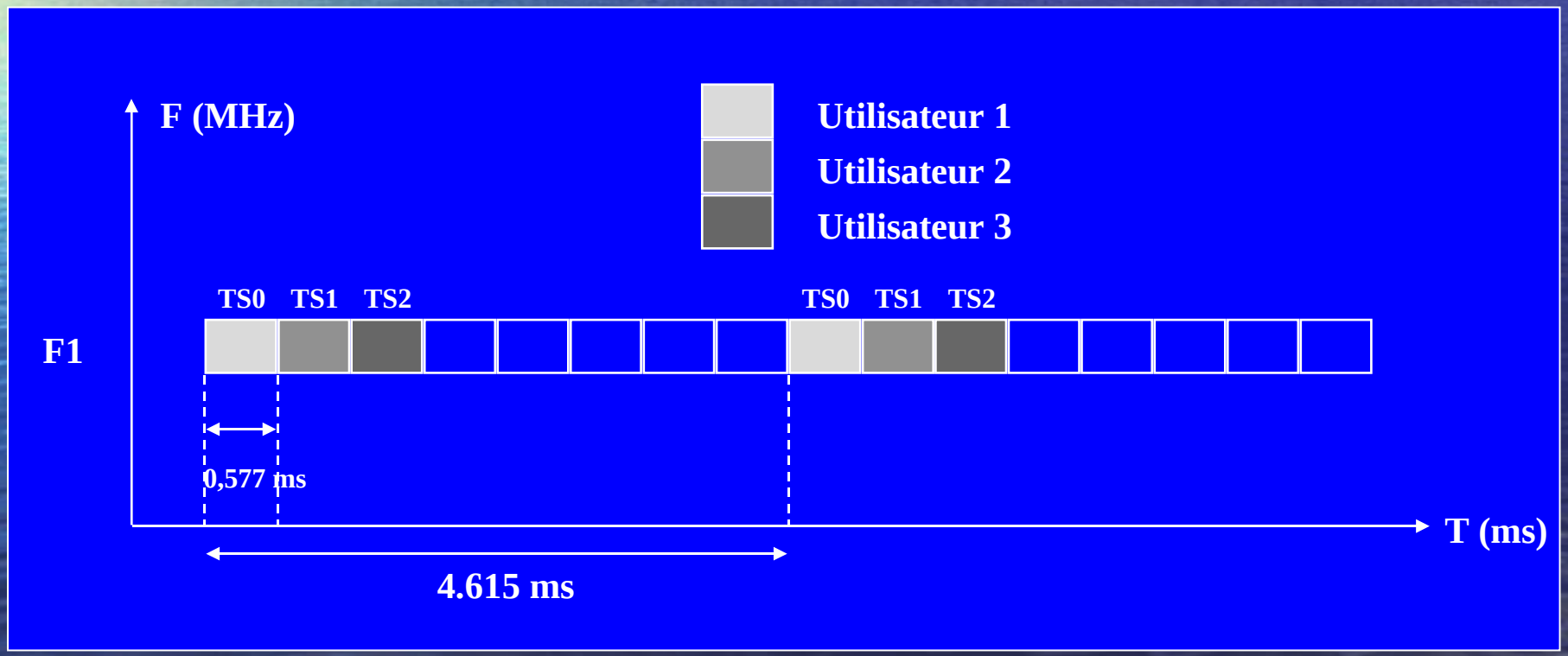
Chaque fréquence est appelée canal
et a une largeur de bande de 200 kHz



4.6) Le multiplexage temporel et fréquentiel

Le système TDMA (Time Division Multiple Access ou AMRT). Sur la trame TDMA, chaque utilisateur a un intervalle de temps (TS) parmi 8 sur une fréquence.

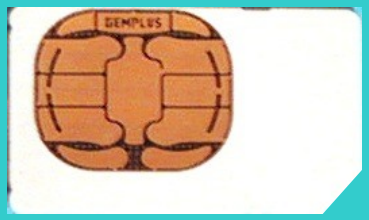
Pour augmenter la capacité, on ajoute des fréquences (à chaque fréquence ajoutée, on gagne 8 TS)



	E-GSM (depuis 99)	GSM	DCS
Bande de fréquence	880 - 890 MHz (↑ UL) 925 - 935 MHz (↓ DL)	890 - 915 MHz (↑ UL) 935 - 960 MHz (↓ DL)	1710 - 1785 MHz (↑ UL) 1805 - 1880 MHz (↓ DL)
Nombre d'intervalles de temps par trame TDMA	8		
Ecart Duplex	45 MHz	45 MHz	95 MHz
Débit de la parole	13 kbit/s		
Largeur de canal	200 kHz		
Puissances des terminaux	2 et 8 W		0.25 et 1 W
fréquence voie descendante (↓ DL) n = ARFCN	**935+0.2*(n-1024)** $975 \leq n \leq 1024$	935+0.2*n $1 \leq n \leq 124$	1805.2+0.2*(n-512) $512 \leq n \leq 885$
fréquence voie montante (↑ UL)	**UL=DL- 45MHz**		**UL=DL- 95MHz**

4.7) Coût non prohibitif

Standardisation des terminaux mobiles en dissociant l'abonnement à un service proposé par un opérateur du terminal de communication mobile.



Carte SIM

Abonné : SUBSCRIBER
Entité qui obtient un service auprès d'un opérateur et est responsable du paiement de l'ensemble des charges

SIM : Subscriber Idendity Module
Carte de crédit ou est stocké l'ensemble des données d'abonnement : identités (IMSI), mots de passe personnel, services souscrits, annuaire personnel

Vocabulaire :
IMSI :

IMSI : international mobile subscriber identity.

5°) L'accès à tous les services proposés par le réseau fixe doit être possible.

Solution :

5.1) Télé services vocaux

La téléphonie c'est à dire la transmission de la voie est le premier service offert par un PLMN.

Les tonalités DTMF (ou Q.23) afin de disposer des services des réseaux fixes (boite vocale, répondeur). Elles sont transmises en numérique au sein du PLMN et converties ensuite en analogiques

Appel d'urgence normalement unique au niveau européen «112 » Si opérateur l'autorise fonctionne même sans la carte SIM. Routage automatique vers un abonné fixe prédéterminé avec les autorités de régulations nationales.

5.2) Télé services de données [GSM 02.03]

La télécopie

Fax de groupe 3 (9600 bits/s)

5.3) Les Messages Courts [GSM 03.40]

Les Shorts Messages Service «sms » permettent de réaliser une messagerie bidirectionnelle avec acquittement. Les messages courts ont une longueur maximale de 140 octets (soit 160 caractères sur 7 bits en ASCII). (horodatage et acquittement)

Émis par le mobile (Mobile Originated SMS Point-to-Point).

Destiné au mobile (Mobile Terminated SMS Point-to-Point).

Diffusé par l'infrastructure (93 caractères) (cell Broadcast).

5.4) Service support [GSM 02.04]

Cela correspond à la fourniture d'une capacité de transmission

Deux catégories :

Continuité numérique : *Unrestricted Digital Information* (UDI)

Non-continuité numérique : *3,1 kHZ external to PLM* (le lien peut contenir une partie analogique).

Deux modes :

Transparent (T) : pas de protocole, délais moyen, Taux d'erreurs important

Non-Transparent (NT) : *Radio Link protocol* (RLP), délais non maîtrisés, taux d'erreurs faible

Type de service	Transfert	Débit (bits/s)	Type d'accès	Mode	Remarques
Circuit de données	3,1 kHz	Synchrone 300,1200 2400, 4800, 9600	Asynchrone	T ou NT	V21, V22$_{bis}$ V26$_{ter}$, V32
			Synchrone		
	UDI		Asynchrone		
			Synchrone		
Accès asynchrone Réseau de donnés	UDI	300,1200 2400,4800, 9600	Asynchrone	NT	
Accès synchrone Réseau de donnés			Synchrone		

5.5) Services supplémentaires [GSM 02.04]

Type de service	Norme	Abréviation
Identification de numéro	Calling Line Identification Présentation	CLIP
	Calling Line Identification Restriction	CLIR
Renvoi d'appel	Call Forwarding Unconditional	CFU
	Call Forwarding on Mobile Subscriber Busy	CFB
	Call Forwarding on No Reply	CFNRy
	Call Forwarding on Mobile Subscriber Not Reachable	CFNRc
Double appel	Call Waiting	CW
Conférence	Multi-Party Service	MPTY
Facturation	Advice of Charge	AoCI
Restriction d'appel	Barring of All Outgoing Calls	BAOC
	Barring of Outgoing International Calls	BOIC
	Barring of Outgoing Calls except the Home PLMN	BOIC-exHC
	Barring of All Incomming Calls	BAIC
	Barring of Incomming Calls except the Home PLMN	BIC-Roam

6°) Les communications doivent être sécurisées.

Solution :

6.1) Sécurité pour l'usager

Confidentialité des informations utilisateurs

Cryptage voix données et signalisation, allocation dynamique du canal de transmission.

6.2) Sécurité pour l'usager et l'opérateur

Confidentialité de l'identité de l'utilisateur

Allocation dynamique d'une identité temporaire transmise en mode crypté (TMSI, Temporary Mobile Subscriber Identity)

6.3) Sécurité pour l'opérateur

Authentification de l'abonné

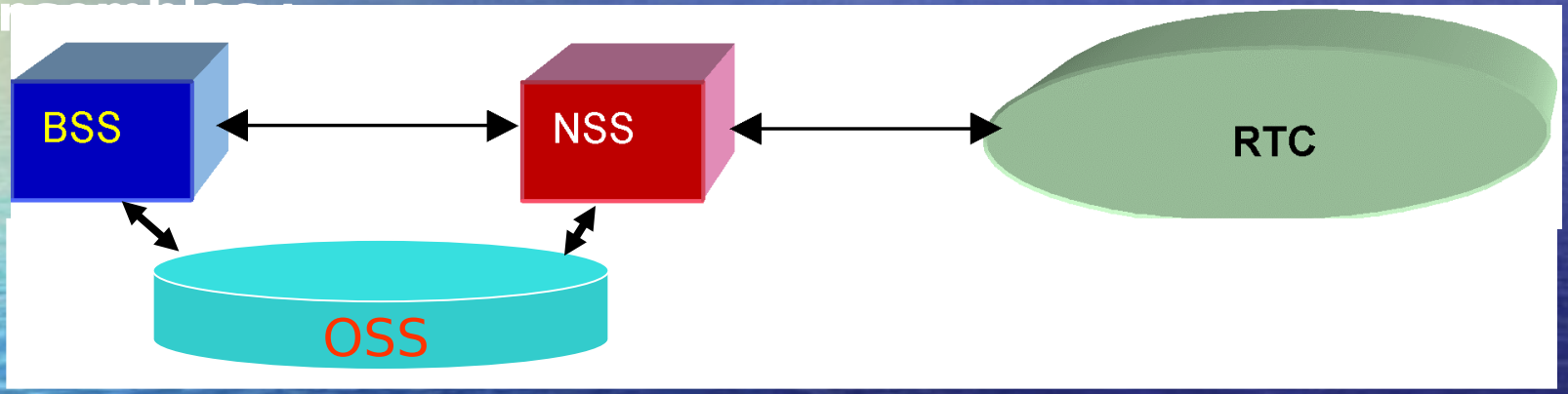
Clef secrète stockée dans la carte SIM et vérifiée à chaque appel.

III. Architecture du réseau GSM.

1°) Vue globale.

1.1) Sous systèmes dans le système GSM.

Un réseau de radiotéléphonie se décompose en trois sous-ensembles :

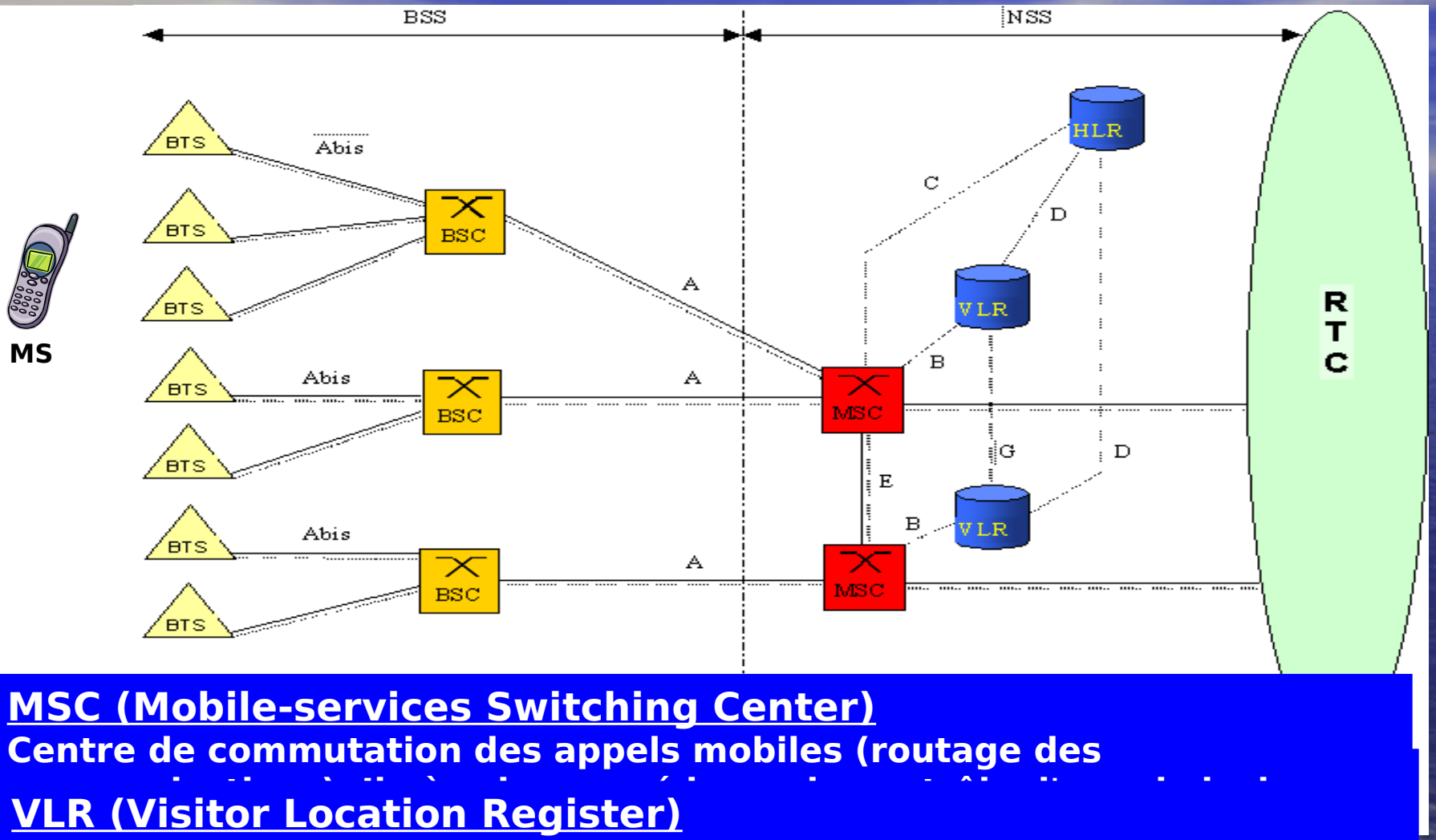


Le BSS (Base Station Sub-system) : sous-système radio qui assure les transmissions radioélectriques et gère la ressource radio.

Le NSS (Network Sub-System) : sous-système d'acheminement, aussi appelé réseau fixe, qui réalise les fonctions d'établissements des appels et de la mobilité.

L'OSS (Operation Sub-System) : sous-système d'exploitation et de maintenance qui permet à l'exploitant d'administrer son réseau.

1.2) Liste des interfaces dans le système GSM.



MSC (Mobile-services Switching Center)

Centre de commutation des appels mobiles (routage des

VLR (Visitor Location Register)

Enregistreur de localisation des visiteurs. Base de données temporaire qui "recopie" les données du HLR pour des mobiles présents dans une zone géographique considérée. En général situé dans un MSC

Nom	Localisation	Utilisation
Um	MS-BTS	Interface radio
Abis	BTS-BSC	Divers
A	BSC-MSC	Divers
C	GMSC-HLR	Interrogation HLR pour appel entrant
	SM/GMSC-HLR	Interrogation HLR pour message court entrant
D	VLR-HLR	Gestion des informations d'abonnés et de localisation
	VLR-HLR	Services supplémentaires
E	MSC-SM/GMSC	Transport des messages courts
	MSC-MSC	Exécution des handover
G	VLR-VLR	Gestion des informations d'abonnés
F	MSC-EIR	Vérification de l'identité du terminal
B	MSC-VLR	Divers
H	HLR-AUC	Echange des données d'authentification

2°) Sous-système radio (BSS)

2.1) Fonctions de la BTS

Un BSS est composé de plusieurs BTS (Base Transceiver Station) qui sont des émetteurs - récepteurs très simples. Les BTS réalisent l'ensemble des mesures radio pour vérifier qu'une communication en cours se déroule normalement.

Elles peuvent supporter au plus une centaine de communications simultanées. La capacité maximale d'une BTS est en théorie de 16 porteuses.

La BTS est un ensemble d'émetteurs - récepteurs appelés TRX.

Elle a à sa charge la transmission radio :
Modulation, démodulation, égalisation,
Codage correcteur d'erreur.
Elle gère donc toute la couche physique :
Multiplexage TDMA
Saut de fréquence lent
Chiffrement.

2.2) Classes des puissances des BTS :

Les BTS normales [GSM 05.05]

	GSM 900			DCS 1800	
Numéro de Classe	Puissance Maximale (W)	Limite de la puissance maximale (W)	Sensibilité	Puissance Maximale (W)	Limite de la puissance maximale (W)
1	320	640	-104 dBm	20	40
2	160	320		10	20
3	80	160		5	10
4	40	80		2,5	5
5	20	40			
6	10	20			
7	5	10			
8	2,5	5			

Les Micro-BTS [GSM 05.05]

	GSM 900		DCS 1800	
Numéro de Classe	Puissance Maximale (W)	Sensibilité	Puissance Maximale (W)	Sensibilité
M1	0,08	- 97 dBm	0,5	-102 dBm
M2	0,03	-92 dBm	0,16	-97 dBm
M3	0,01	-87 dBm	0,05	-92 dBm

2.3) Fonctions du BSC

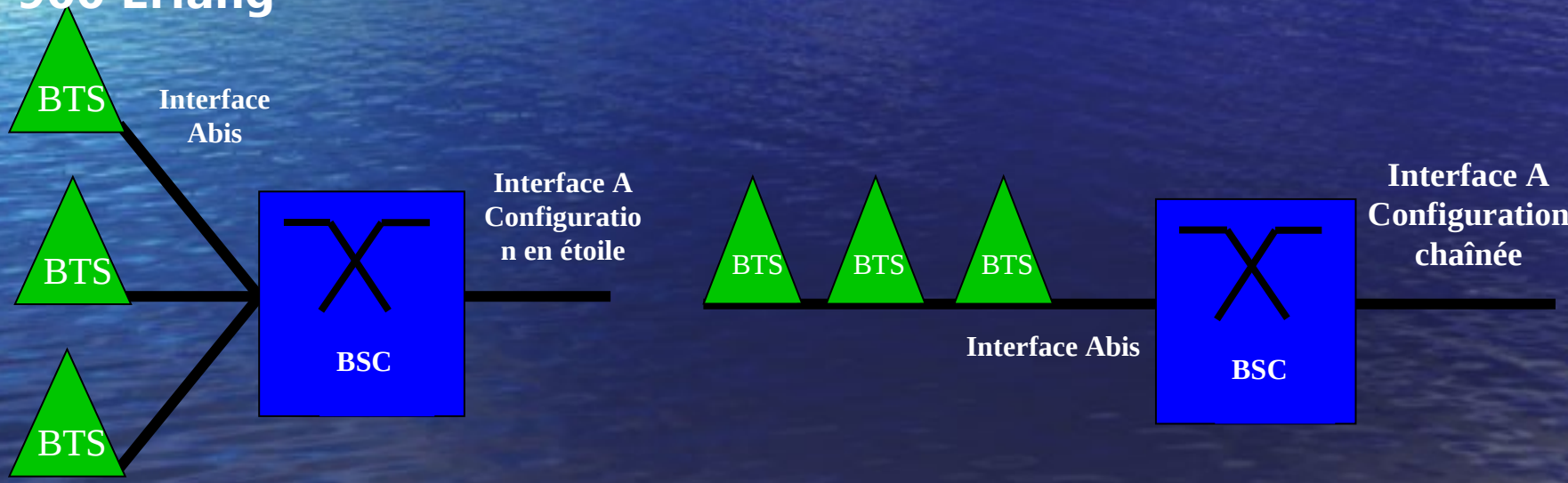
Le BSC (Base Station Controller) contrôle un ensemble de BTS et permet une première concentration des circuits.

Il gère la ressource radio :

Commande l'allocation des canaux

Utilise les mesures effectuées par les BTS pour contrôler la puissance d'émission des mobiles et/ou des BTS.

Le BSC est relié par une ou plusieurs liaison MIC avec la BTS et le MSC. Les capacités des BSC sont comprises entre 100 et 900 Erlang



3°) Sous-système fixe (NSS)

3.1) Fonctions du HLR

Le HLR (Home Location Register) est une base de données de localisation et de caractérisation des abonnés d'un PLMN. Il mémorise :

- l'identité internationale de l'abonné (IMSI)
- le numéro annuaire de l'abonné (MSISDN)
- le profil de l'abonnement.

Un HLR peut gérer plusieurs centaines de milliers d’abonnés. Le réseau identifie le HLR propre à chaque abonné à partir du numéro IMSI ou du MSISDN.

Le HLR est aussi une base de données de localisation. Il mémorise pour chaque abonné le numéro du VLR où il est enregistré, même dans le cas ou l’abonné se connecte sur un PLMN étranger.

3.2) Fonctions du MSC et du VLR

Le MSC (Mobile-services Switching Centre) est un commutateur qui gère l'établissement des communications entre un mobile et un autre MSC, la transmission des messages courts et l'exécution du handover.

Il dialogue avec le VLR (Visitor Location Register) pour gérer la mobilité des usagers.
Le MSC peut posséder une fonction passerelle, GMSC (Gateway MSC)

Le VLR (Visitor Location Register) est une base de données qui mémorise les données d'abonnement des clients présents dans la zone géographique qu'il contrôle.
Les données mémorisées par le VLR sont similaires aux données du HLR auquel vient se rajouter l'identité temporaire le TMSI

Un ensemble MSC/VLR peut gérer de l'ordre d'une centaine de milliers d'abonnés pour un trafic moyen par abonnée de 0,025 Erlang.

4°) Sous-système d'exploitation et de maintenance

4.1) Administration du réseau

L'administration de réseau comprend toutes les activités qui permettent de mémoriser et de contrôler les performances et l'utilisation des ressources.

Les différentes fonctions d'administration sont :

- **L'administration commerciale (déclaration des abonnés, des terminaux, facturations, statistiques).**
- **La gestion de la sécurité (détection d'intrusion, niveau d'habilitation).**
- **L'exploitation et la gestion des performances (observation du trafic, qualité, adaptation à la charge).**
- **Le contrôle de la configuration du système (mise à jour logiciel, introduction de nouveaux équipements et de nouvelles fonctionnalités)**
- **La maintenance (détection des défauts, tests d'équipements, ...)**

4.2) L'EIR

L'EIR (Equipment Identity Register) est une base de données annexe contenant les identités des terminaux (IMEISV : international mobile équipement identity).

Cette identité unique codée sur 17 digits est composée d'un numéro d'homologation commun à tous les terminaux d'une même série, d'un

Approval Code (TAC) 6 digits	*Final Assembly Code* (FAC) 2 digits	*Serial Number* (SNR) 6 digits	*SV* 2 digits	*Spare* 1 digits

Type Approval Code (TAC) : champ fourni au constructeur lorsque le matériel a passé l'agrément.
Final Assembly Code (FAC) : champ qui identifie l'usine de fabrication. Ce champ est égal à 00 pour tous les mobiles fabriqués depuis 2003 ;
Valeurs des codes FAC des constructeurs courants :
00 = mobile fabriqué après 2003 (champ non significatif)
01,02 =AEG 60 =Alcatel 07,40 =Motorola 10,20 =Nokia 65 =AEG 30,61 =Ericsson 70,82 =Sagem 40,41,44 =Siemens 75 =Dancall 50 =Bosch 80 =Philips 51 =Sony, Siemens, Ericsson 85 =Panasonic
Serial Number (SNR) : numéro librement affecté par le constructeur;
SV : numéro de version du logiciel du téléphone
Spare : digit réservé pour l'instant.

4.3) L'AUC

L'AUC (AUthentication Center) mémorise pour chaque abonné une clé secrète utilisée pour authentifier les demandes de services et pour chiffrer (coder) les communications.

Un AUC est en général associé à chaque HLR. L'ensemble peut être intégré dans un même équipement

Cliquez sur l'icône

IV. Gestion de l'itinérance et de la sécurité des appels.

L'introduction de la mobilité dans les réseaux a nécessité la définition de nouvelles fonctions par rapport aux réseaux fixes classiques.

Le système doit connaître à tout moment la localisation d'un abonné de façon plus ou moins précise. La fonction correspondante est appelée "gestion de l'itinérance" ou roaming.

1°) Présentation :

La gestion de l'itinérance doit répondre :

A la nécessité pour le système de connaître en permanence la localisation de chaque mobile pour pouvoir le joindre ;

Identification spécifique des usagers.

A la nécessité pour le mobile de rester "actif" c'est-à-dire en "état de veille", de façon à signaler ses mouvements au système et ce, même en l'absence de

L'utilisation d'un canal radio rend les communications vulnérables aux écoutes d'où des problèmes de confidentialité.

<u>Le système GSM a donc recours aux procédés suivants :</u>

Authentification de chaque abonné avant de lui autoriser l'accès à un services ;

Utilisation d'une identité temporaire ;

Chiffrement (ou cryptage) des communications.

2°) Numérotation liée à la mobilité

Le système GSM utilise quatre types d'adressages liés à l'abonné :

Le MSISDN est le numéro de l'abonné, c'est le seul identifiant de l'abonné mobile connu à l'extérieur du réseau GSM

L'IMSI (identité invariante de l'abonné) n'est connu qu'à l'intérieur du réseau GSM ; cette identité doit rester secrète autant que possible.

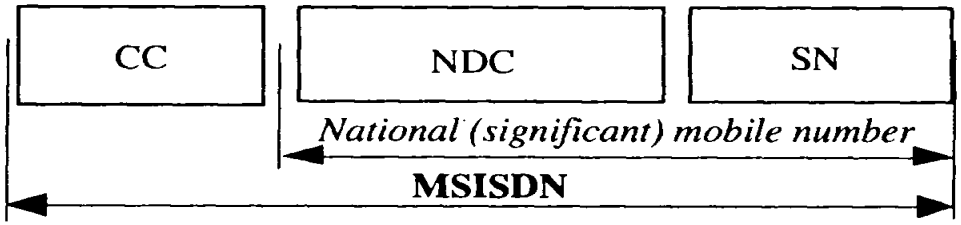
Le TMSI est une identité temporaire utilisée pour identifier le mobile lors des interactions Station Mobile-Réseau.

Le MSRN est un numéro attribué lors d'un établissement d'appel. Sa principale fonction est de permettre l'acheminement des appels par les commutateurs (MSC)

Du fait de la séparation entre l'équipement et l'abonnement, le réseau peut de plus contrôler l'identité IMEI de tout équipement qui désire un service.

2.1) MSISDN (Mobile Station ISDN Number)

Numéro public de l'abonné mobile

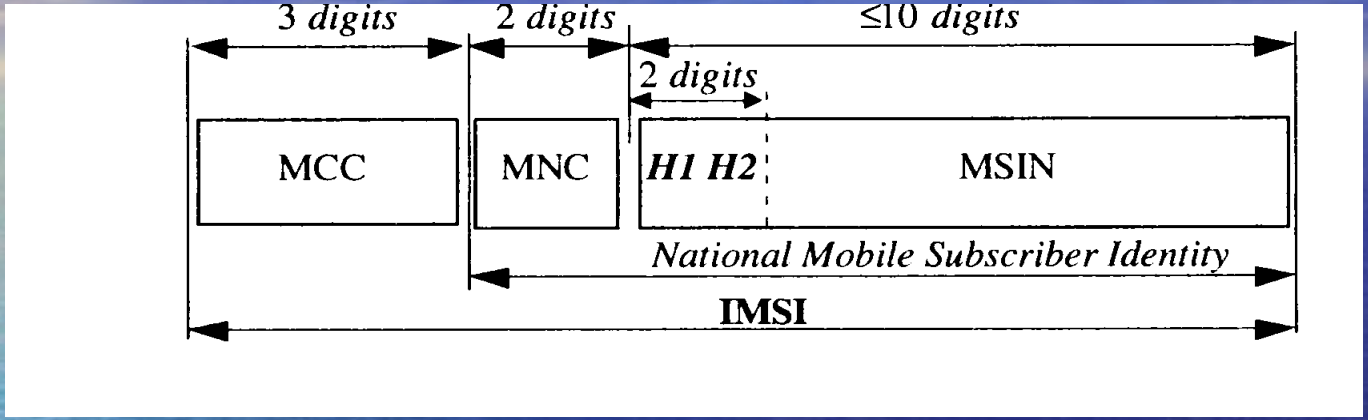


« CC » Country Code : indicatif du pays dans lequel est souscrit l'abonnement
« NSMC » National Significant Mobile Number : numéro national du mobile composé du :
« NDC » National destination Code déterminant le PLMN
« SN » attribué librement par l'opérateur.

Exemple : français 33 06 AB PQ MCDU
06 regroupe tous les abonnés mobiles
AB (07, 08 et 04 pour FT, 09 et 04 pour SFR, 60, 61 et 18 pour Bouygues Télécom).
PQ numéro de HLR du réseau GSM
MCDU numéro de l'abonné dans le HLR

2.2) L'IMSI (International Mobile Subscriber Identity)

Identité internationale de chaque abonné unique pour tous les réseaux GSM (N° abonnement opérateur)



MCC Mobile Country Code : indicatif du pays domicile de l'abonné mobile (208 pour la France)

MNC Mobile Network Code : Indicatif du PLMN nominal de l'abonné mobile (01 pour FT et 10 pour SFR)

MSIN Mobile Subscriber Identification Number : numéro de l'abonné dans son réseau GSM. Les 2 premiers chiffres du champ MSIN donnent l'indicatif du HLR de l'abonné au sein de son PLMN. Cette information permet à un MSC/VLR de connaître le HLR de rattachement de n'importe quel mobile qui entre en contact avec lui en transmettant son IMSI.

2.3) TMSI (Temporary Mobile Station Identity)

A l'intérieur d'une zone gérée par un VLR, un abonné dispose d'une identité temporaire, le TMSI, attribué au mobile de façon locale, c'est-à-dire uniquement pour la zone gérée par le VLR courant du mobile.

Le TMSI n'est connu que sur la partie Station Mobile - MSC/VLR et le HLR n'en a jamais connaissance.
Le TMSI est utilisé pour identifier le mobile appelé ou appelant lors d'un établissement de communication. Plusieurs mobiles dépendant de VLR différents peuvent avoir le même TMSI.
A chaque changement de VLR, un nouveau TMSI doit être attribué.

2.4) MSRN (Mobile Station Roaming Number)

Le MSRN a pour fonction de permettre le routage des appels entrants directement du commutateur passerelle (GMSC) vers le commutateur courant (MSC) de la station mobile.

Il est attribué par le VLR courant du mobile de façon temporaire et uniquement lors de l'établissement d'un appel à destination de la station mobile. Le MSRN a la même structure que le MSISDN

3°) Authentification et chiffrement.

3.1) Confidentialité de l'identité de l'abonné

Le meilleur moyen d'éviter l'interception de l'IMSI est de le transmettre le plus rarement possible sur la voie radio. C'est pourquoi le système GSM a recours au TMSI.

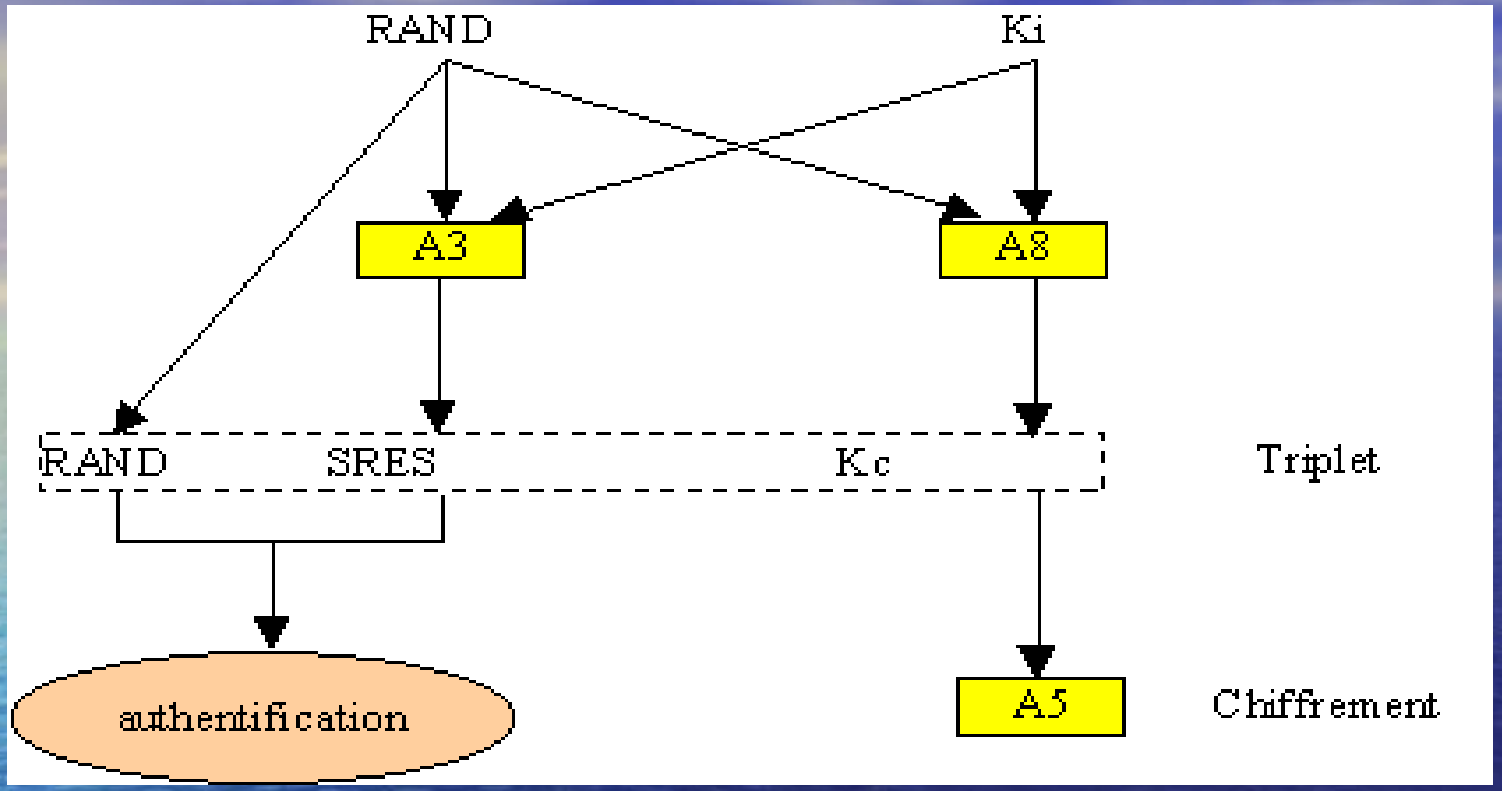
L'allocation d'un nouveau TMSI est faite au minimum à chaque changement de VLR et, suivant le choix de l'opérateur, éventuellement à chaque intervention du mobile. L'envoi du nouveau TMSI à la station mobile a lieu en mode chiffré dans le cas où le chiffrement serait mis en œuvre.

3.2) Principes généraux d'authentification et de chiffrement

Pour mettre en œuvre les fonctions d'authentification et de chiffrement des informations transmises sur la voie radio, GSM utilise les éléments suivants :

- Des nombres aléatoires RAND,
- Une clé Ki pour l'authentification et la détermination de la clé de chiffrement Kc,
- Un algorithme A3 fournissant un nombre SRES à partir de RAND et Ki,
- Un algorithme A8 pour déterminer la clé Kc à partir de RAND et Ki
- Un algorithme A5 pour le chiffrement/déchiffrement des données à partir de la clé Kc.

A chaque abonné est attribuée une clé Ki propre. Les algorithmes A3, A5 et A8 sont les mêmes pour tous les abonnés d'un même réseau.



L'algorithme A3 au niveau du HLR/AUC et de la Station Mobile permet de déterminer SRES à partir d'un nombre aléatoire RAND et de la clé d'authentification Ki.
L'algorithme A8 permet au niveau du HLR/AUC et la Station Mobile de déterminer la clé de chiffrement Kc à l'aide de RAND et Ki. Les triplets obtenus (RAND, SRES, Kc) permettent au réseau (au niveau MSC/VLR) d'authentifier un abonné et de chiffrer les communications.

3.3) Authentification de l'identité de l'abonné.

L'authentification permet de vérifier que l'identité transmise par le mobile (IMSI ou TMSI) sur la voie radio est correcte afin de protéger :

L'opérateur contre l'utilisation frauduleuse des ses ressources.

Les abonnés en interdisant à des tierces personnes d'utiliser leur compte.

L'authentification de l'abonné peut être exigée du mobile par le réseau à chaque mise à jour de localisation, établissement d'appel (sortant ou entrant) et avant d'activer ou de désactiver certains services supplémentaires.

Procédure d'authentification :

Le réseau transmet un nombre aléatoire RAND au mobile,
La carte SIM du mobile calcule la signature de RAND grâce à l'algorithme d'authentification A3 et à la clé d'authentification Ki (information secrète). Le résultat calculé, SRES, est envoyé par le mobile au réseau,
Le réseau compare SRES au résultat calculé de son côté. Si les deux résultats sont identiques, l'abonné est authentifié.

3.4) Confidentialité des données transmises sur la voie radio.

La confidentialité des données permet d'interdire l'interception et le décodage des informations usager et de signalisation, par des individus, entités ou processus non autorisés.
Elle sert plus particulièrement à protéger les éléments suivant : IMEI (identité du terminal), IMSI (Identité de l'abonné), numéro de l'abonné appelant ou appelé.
La confidentialité des informations usager est obtenue grâce au chiffrement de celles-ci. Elle ne concerne que les informations transmises sur l'interface Station Mobile-BTS.

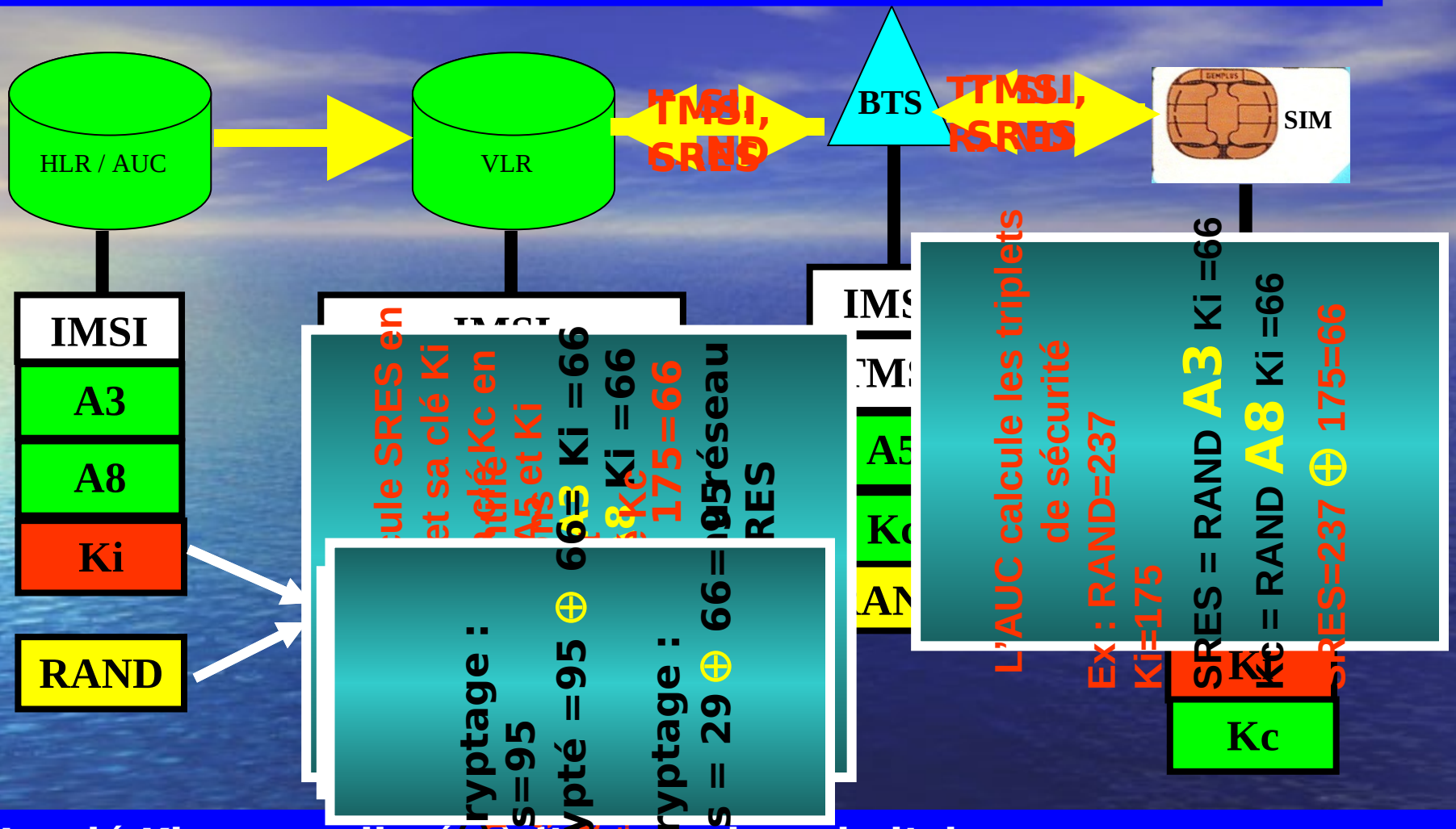
a) Etablissement de la clé Kc.

Les informations transmises sur les canaux dédiés sont chiffrées grâce à la clé de chiffrement Kc. Cette clé est calculée à partir du nombre aléatoire RAND et de l'algorithme A8. Le calcul utilise donc le même argument que l'authentification mais un algorithme différent.

b) Activation du chiffrement.

L'algorithme A5 de chiffrement/déchiffrement est implanté dans la BTS. L'activation se fait sur la demande du MSC.

Authentification Etude simplifiée A3=A5=A8= opération ⊕



La clé Ki est attribuée [illegible] lors de l'abonnement, avec

Les messages envoyés sont cryptés avec Kc : Mcrypté= Mess **A5** Kc

À la réception le mobile décrypte le message en utilisant sa clé Kc

Mess = Mcrypté **A5** Kc = (Mess **A5** Kc) **A5** Kc = Mess

4°) Gestion de l'itinérance.

Le rôle principal d'un mécanisme de gestion de la localisation ou de l'itinérance, est de permettre au système de connaître à tout moment la position d'un mobile et/ou d'un abonné. Cette fonction est nécessaire pour que le système puisse joindre un abonné.

Le mobile peut se trouver dans 3 modes :

Il est éteint. Le réseau ne peut pas le localiser . Tous les appels le concernant sont dirigés vers la boîte vocale.

Il est allumé mais hors communication. C'est le mode Idle.Le mobile est localisable et joignable.

Il est en communication.

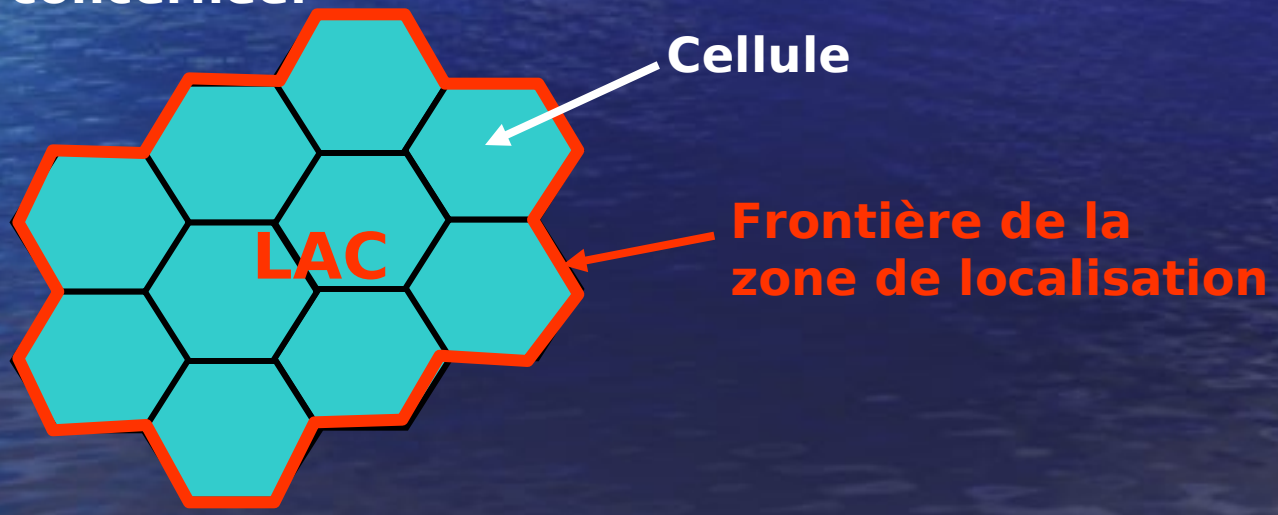
Dans la gestion de la localisation des mobiles, deux mécanismes de base interviennent :

La localisation qui consiste à savoir où se trouve un mobile et ce à tout moment,

La recherche d'abonné (ou paging) qui consiste à émettre des messages d'avis de recherche dans les cellules où le système a précédemment localisé l'abonné.

4.1) Présentation générale.

Des zones de localisation regroupant un certain nombre de cellules sont définies. Le système connaît la zone de localisation précise de l'abonné, c'est-à-dire la dernière dans laquelle le mobile s'est signalé mais ignore la cellule précise où se trouve le mobile à l'intérieur de la zone de localisation.
De cette manière, lorsque l'usager reçoit un appel, le système va le rechercher dans la zone de localisation courante en émettant un avis de recherche dans les cellules de cette zone. Et ainsi, la consommation de ressources (radio !) sera réduite à celle nécessaire à la recherche de l'abonné dans la zone de localisation concernée.



4.2) Localisation du mobile.

La mise à jour sur changement de zone de localisation est la méthode la plus utilisée par les systèmes cellulaires.

Chaque station de base diffuse périodiquement sur une voie balise (le BCCH) le numéro de la zone de localisation à laquelle elle appartient : l'adresse LAC (Localisation Area code).
Le mobile de son côté écoute périodiquement la voie balise et stocke en permanence le numéro de sa zone de localisation courante.

Si le mobile s'aperçoit que le numéro de la zone dans laquelle il se trouve est différent du numéro stocké, il signale sa nouvelle position au réseau. C'est le mécanisme de "mise à jour de localisation" (location updating procedure), appelé aussi "inscription" ou "enregistrement". Les bases de données de localisation vont ainsi être mises à jour au niveau du réseau.

Périodiquement, le réseau envoie une demande de mise à jour de localisation (Periodic Location Updating) au mobile

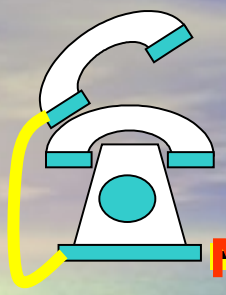
4.3) Recherche d'abonné.

Lorsque le mobile s'est déplacé éteint et qu'il a changé de LAC, le réseau fait une procédure de Paging sur toutes les LAC (augmentation de charge sur le réseau).

Pour éviter des paging inutiles sur tout le réseau lorsqu'un mobile est éteint, les procédures IMSI Attach & IMSI Detach permettent de savoir si le mobile est allumé ou éteint. S'il est éteint, le réseau renvoie directement sur la boite vocale.

4.4) Gestion des bases de données (HLR, VLR).

Un VLR peut gérer plusieurs zones de localisation. En revanche, une zone de localisation ne peut comprendre des cellules dépendant d'un autre VLR. Pour éviter les transferts inutiles de signalisations, 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.



MSISDN

068

Acheminer l'appel au : 0450095588

GMSC

MSRN

VMSC

BTS 32

TMSI

VLR N°27891

IMSI	LAC	MSRN	TMSI
2080170002000	2080120993	045009558	600423A
2080170892255	2080120993	8	685151F

MSRN

IMSI

HLR N°8850

MSISDN	IMSI	Dernier VLR de couverture
0688500049	208017000200	27891
0688500050	208017000225	52891

Appel pour L'IN 208 01 700020

Appel pour le TMSI 4227

Le VMSC va enfin appeler le mobile en utilisant l'identité temporaire, TMSI qui a été attribuée au mobile lors de la mise à jour de localisation ou lors de l'inscription du mobile.

V. Les canaux physiques :

La répétition périodique d'un slot dans les trames sur un couple de fréquence porteuses (Up/Down) particulière constitue un "canal physique".

Toutes les trames générées par la même BTS dans le sens descendant sont synchronisées et les trames du sens montant ont un retard de 3 slots par rapport aux descendantes. Cela permet aux mobiles d'émettre et de recevoir sur le même slot sans avoir à réaliser ces 2 actions simultanément. Le mobile utilise pour sa synchronisation les i

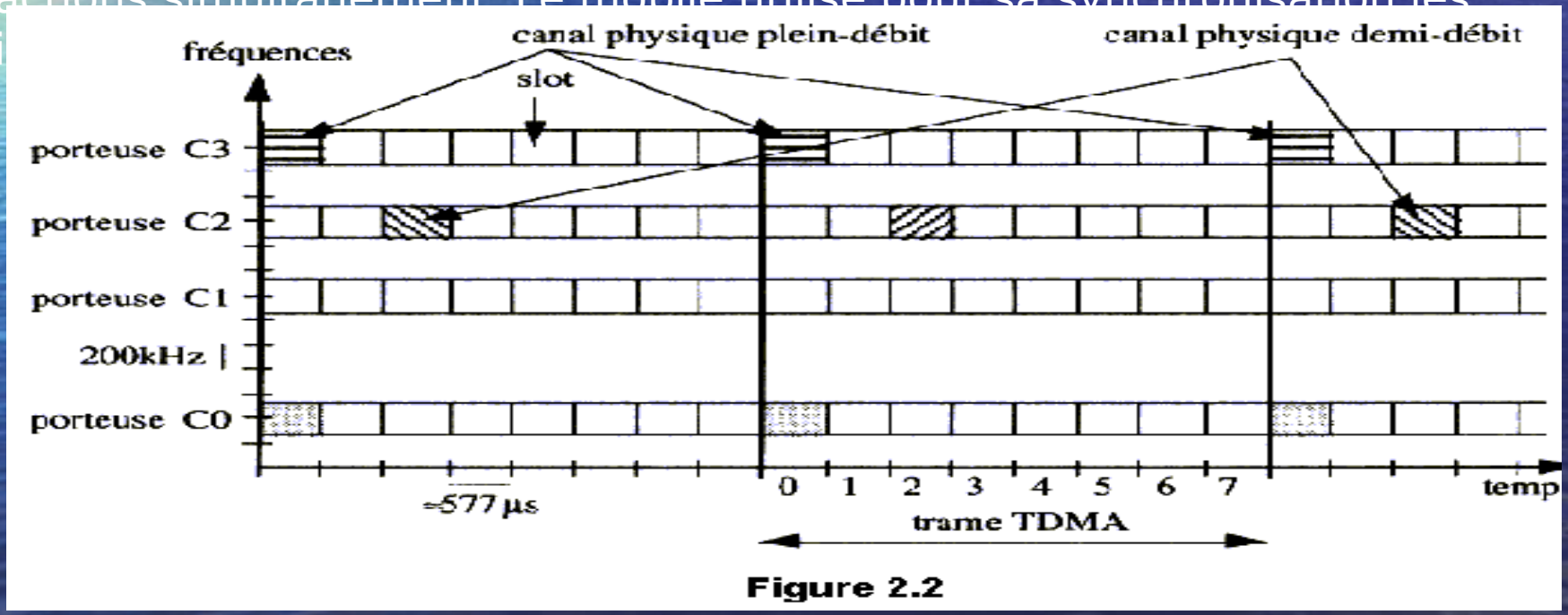


Figure 2.2

VI. Les canaux logiques :

Un canal « logique » est une suite de Time Slots de différentes trames

L'information transportée sur les canaux physiques est structurée en différents canaux logiques en fonction des débits souhaités, du mode de transmission (diffusion, liaison point à point, up-link, down-link...)

Les canaux logiques de signalisation et de communication

1°) Canaux de diffusion BCH (Broadcast CHannel - voie balise)

Ils diffusent des données relatives à une cellule permettant à chaque mobile d'accrocher au système local en acquérant les paramètres nécessaire.

Ils contiennent :

le FCCH (Frequency Correction CHannel) qui assure le calage du mobile sur la fréquence porteuse de la BTS.

le SCH (Synchronized CHannel) qui assure la synchronisation du mobile et l'identification de la cellule.

le BCCH (Broadcast Common CHannel) qui diffuse des informations locales du système (caractéristiques de la cellule).

Ils occupent généralement le TS(0) de la porteuse C0 (voie balise)

Ils occupent généralement le TS(0) de la porteuse C0 (voie balise)

CANAL	Nom Complet	Slot possible	Multitrame	Débit	Fonction
FCCH	Frequency Correction Channel	0	51	146bit toutes les 50 ms	Calage du mobile sur la fréquence porteuse
SCH	Synchronisation Channel	0	51	146bit toutes les 50 ms	Identification de la BTS et synchronisation du mobile sur celle-ci
BCCH	Broadcast Control Channel	0	51	782 bit/s	Canal de diffusion des informations spécifique de la BTS de la cellule et des BTS voisines.

2°) Canaux communs de contrôle CCCH

Ils sont réservés pour les opérations de gestion des communications (établissement, allocation de canaux de trafic).

Sens descendant :

le PCH (Paging CHannel) utilisé lors de la procédure de paging.
le AGCH (Access Grant CHannel). Allocation d'un canal physique dédié (fréquence + Time Slot) en réponse à une demande du mobile.
le CBCH (Cell Broadcast CHAnnel). Messages courts en diffusion vers les mobiles.

Sens montant :

Le RACH (Random Access CHannel). Accès aléatoire de la part des mobiles (demande d'allocation de canal).

Tous ces canaux de contrôle (UpLink ou DownLink) sont toujours diffusés sur un canal physique appelé voie balise. Il s'agit du Time Slot 0 (voire 2, 4 et 6 pour les grosses BTS) de la première fréquence de la cellule (fréquence BCCH). Coté BTS, la voie balise est diffusée en permanence et à pleine puissance.

CANAL	Nom Complet	Slot possible	Multitrame	Débit	Fonction
RACH	Random Access Channel	0,2,4,6	51	36 bit	Il permet au mobile de signaler à la BTS qu'il désire effectuer une opération sur le réseau
PCH	Paging Channel	0,2,4,6	51	456 bit	Il permet de diffuser l'identité d'un mobile. lorsque le réseau veut communiquer avec un mobile, il diffuse l'identité du mobile sur un ensemble de cellules.
AGCH	Access Grant Channel	0,2,4,6	51	456 bit	Il est utilisé pour l'allocation d'un canal dédié à un mobile. Il contient la description complète du canal utilisé: Numéro de porteuse et numéro du slot utilisé; il contient également le paramètre TA.
CBCH	Cell Broadcast Channel	0,1,2,3	51	variable	Il offre aux usagers présents dans la cellule des informations spécifiques (informations routières, météo).

3°) Canaux de signalisation dédiés (transmis sur un canal physique différent de la voie balise)

Ils fournissent une ressource réservée à un mobile. Le mobile se voit attribuer une paire de slots dans laquelle il est seul à émettre et recevoir.

Le SDCCH (Stand-alone Dedicated Control CHannel)
Le SDCCH, canal bas débit, transporte les données de signalisation (authentification, chiffrement puis établissement de la communication) dès la connexion mobile-BTS et jusqu'au basculement sur un canal de trafic TCH.
Le SACCH (Slow Associated Control CHannel).
Canal très bas débit associé à un TCH ou à un SDCCH pour superviser les liaisons radio et se localise sur le même canal physique. Il transporte des informations générales entre mobile et BTS, tels que les rapports de mesures sur cellule serveuse et voisines, le contrôle de puissance du mobile etc…
Le FACCH (Fast Associated Control CHannel).
Il est utilisé en cas de signalisation urgente, pour le HandOver en particulier (le SACCH est de débit trop lent). Son débit important remplace alors la transmission du canal TCH (rupture momentanée de la transmission de la voix).

Ils occupent un TS dédié attribué par le réseau

CANAL	Nom Complet	Slot possible	Multitrame	Débit	Fonction
TCH	Traffic channel	0 à 7	26	13 Kbit/s	Canal supportant le trafic voix ou data (DCH)
SACCH	Slow associated Control Channel	0 à 7	51 ou 26	304 bit/s	Canal de supervision d'une liaison : control de la puissance, qualité, remonté des mesures…
SDCCH	Stand Alone Dedicated control channel	0 à 7	51	782 bit/s	Canal alloué aux phases d'établissement de la communications : signalisation et mise à jour de la localisation….
FACCH	Fast Associated Control Channel	0 à 7	26	9,2 Kbit/s	Canal servant à exécuter les hand-over , il prend momentanément le slot réservé au canal TCH.

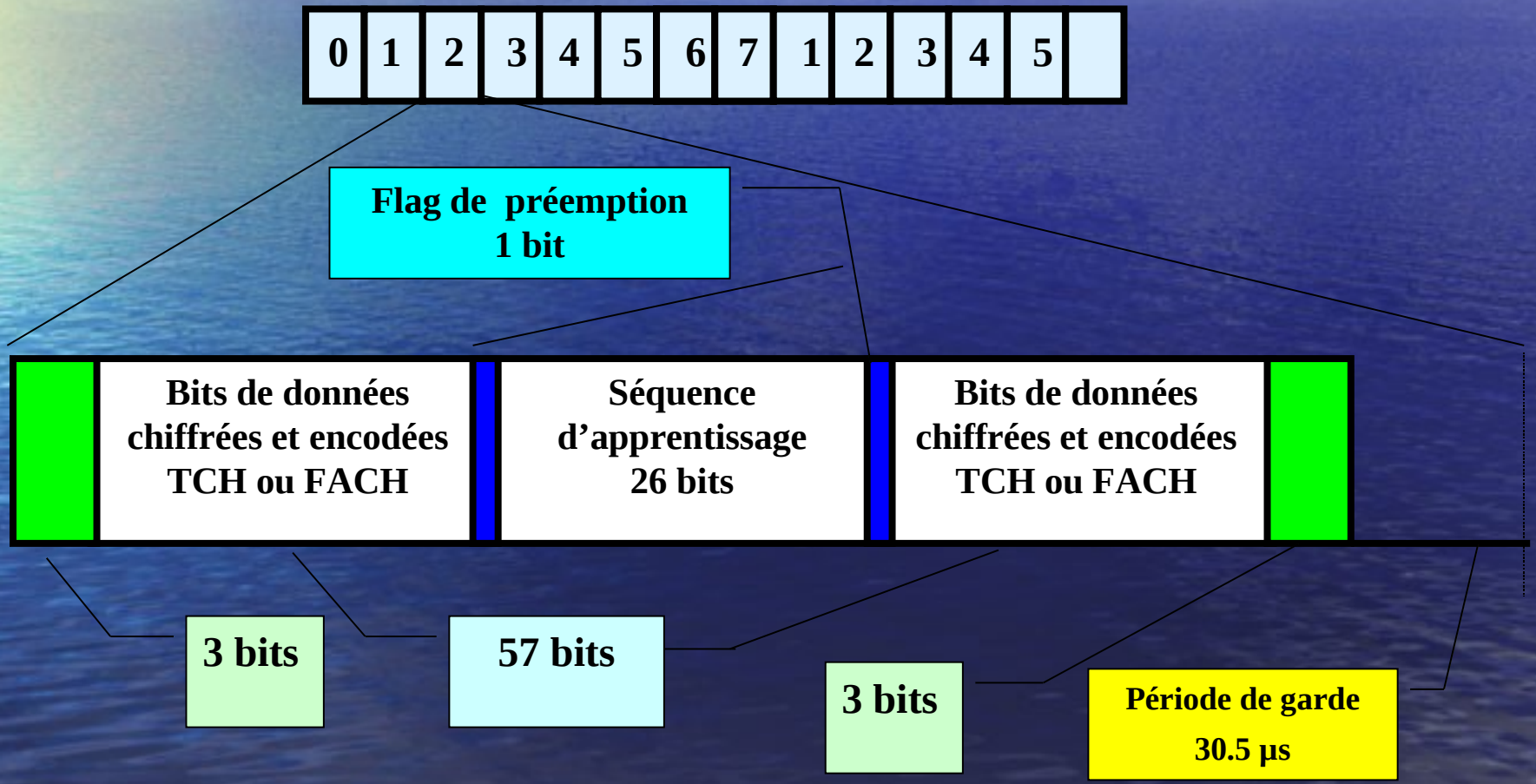
4°) Canaux de trafic

Le TCH (Traffic CHannel)
Lorsque la communication est établie, un canal TCH est alloué et sert au transfert de la parole ou éventuellement de données (émission en slot i à f2, réception en slot i à f2+45MHz).
Parallèlement à cette activité principale, il écoute périodiquement les voies balises de la cellule et des cellules voisines pour détecter une variation de niveau lui indiquant un changement de cellule (hand over)

5°) Constitution d'un slot normal:

Chaque slot sert au transport d'un canal logique. Le burst est le contenu physique du slot. L'information à transmettre est donc découpée en bursts.

Format du burst :

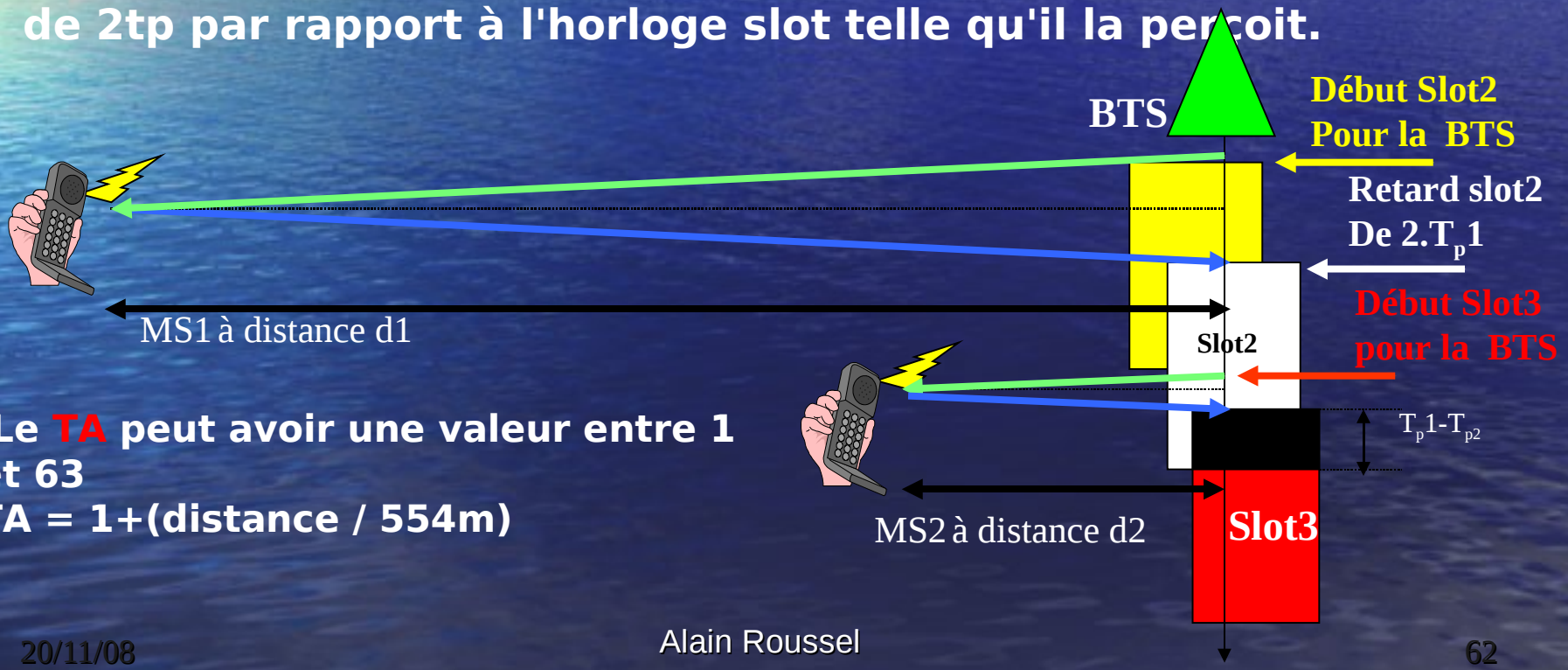


6°) Compensation des temps de propagation :

Soient 2 mobiles dans la même cellule mais ne se trouvant pas à la même distance de la BTS. Si ces 2 mobiles utilisent des slots consécutifs, il faut veiller à ce que les bursts qu'ils envoient ne se chevauchent pas au niveau de la BTS.

Compensation en gérant un paramètre TA (Time Advance) qui correspond au temps de propagation aller-retour. Ce paramètre est transmis par SACCH

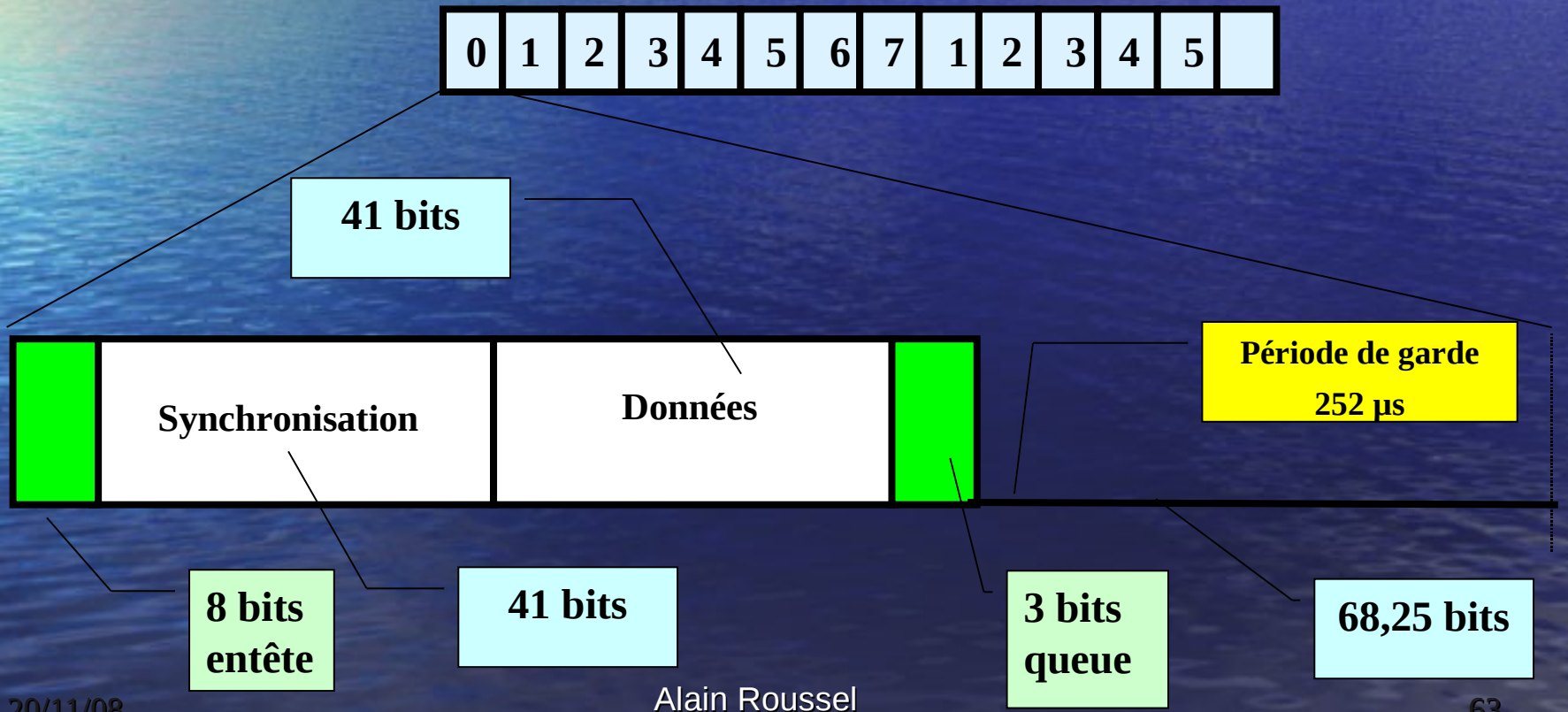
Le mobile MS1 doit avancer l'émission de chacun de ses slots de 2tp par rapport à l'horloge slot telle qu'il la perçoit.



Le TA peut avoir une valeur entre 1 et 63
TA = 1+(distance / 554m)

7°) Constitution d'un slot RACH:

Tout mobile désirant établir une communication fait une requête sur RACH afin qu'un TCH lui soit attribué. Le mobile faisant une requête d'appel ne dispose donc pas encore d'un SACCH et donc de l'information Time Advance. Ne pouvant être bien synchronisé, la durée de garde a été augmentée, dans le but d'éviter un débordement sur le burst suivant d'un autre mobile sur RACH



8°) Les interférences

Une interférence se caractérise par un signal parasite émis à la même fréquence que le signal utile. Ce signal parasite se superpose au signal utile et la résultante est un signal plus ou moins dégradé suivant la puissance de l'interféreur.

Les interféreurs peuvent être externes au réseau ou internes (dus à la réutilisation des fréquences).

Dans un réseau cellulaire, on trouve 2 types d'interférences dues à la réutilisation des fréquences :

Les interférences co-canal :

Interférence entre deux cellules utilisant la même fréquence. Gênant dès que la différence entre la serveuse et l'interféreuse atteint 9 dB.

Les interférences dues au canal adjacent :

Le gabarit fréquentiel d'un canal n'est pas à flancs raides donc il va "déborder" sur les canaux adjacents (le canal N va interférer les canaux N+1 et N-1). Gênant dès que la serveuse et l'interféreuse sont de même valeur.

Pour y remédier, corriger le plan de fréquences, baisser la puissance des cellules interféreuses.

9°) Le contrôle de puissance : Power Control

But :

Faire varier la puissance d'émission du mobile et de la BTS en cours de communication afin d'utiliser la puissance la plus faible possible sans altérer la qualité de la communication.

Intérêt :

Economie de batteries (mobiles).
Réduction du taux moyen d'interférence sur le réseau (BTS).

Remarque :

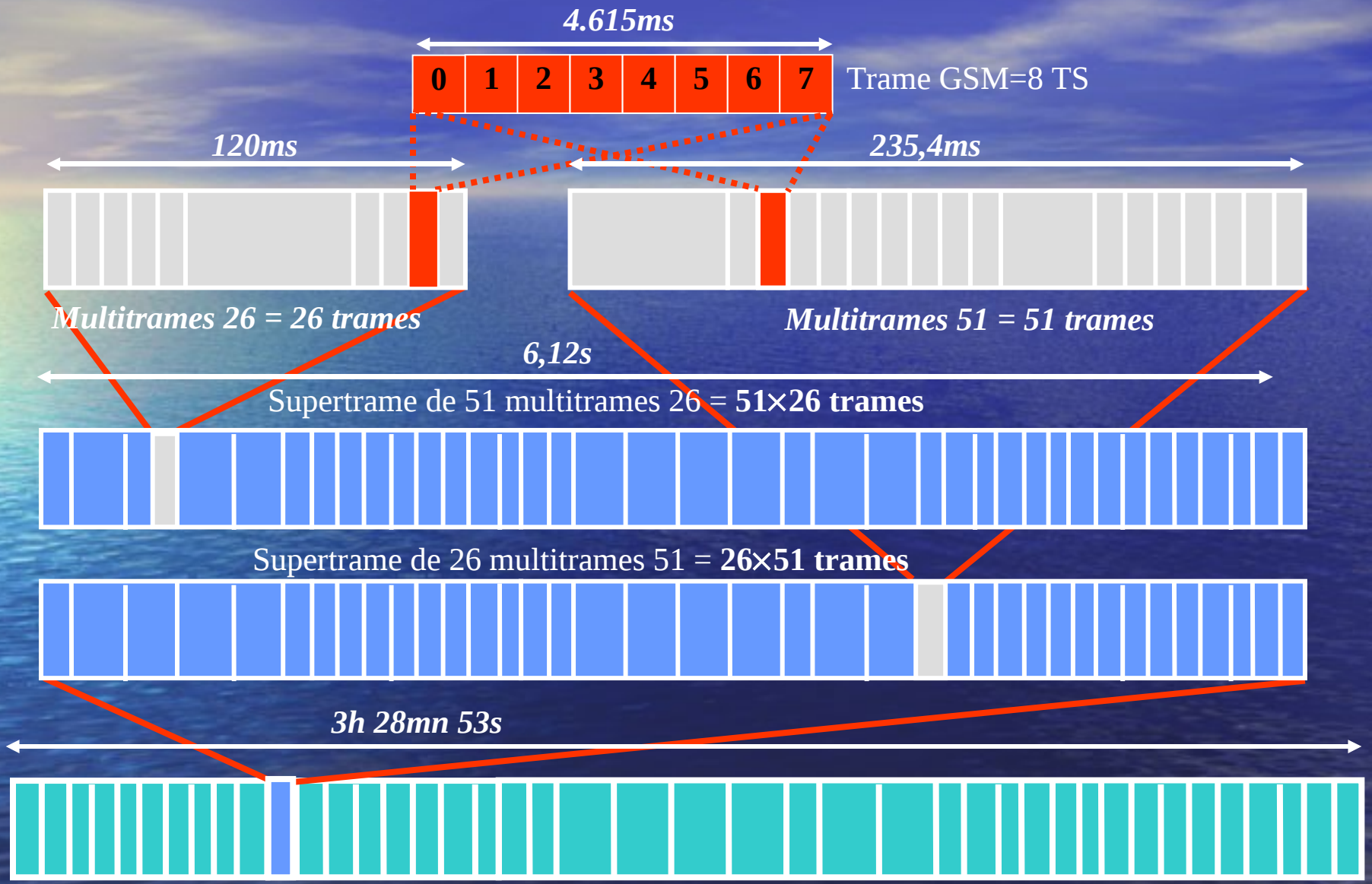
La fréquence BCCH (1er ARFC d'une cellule) ne fait pas de contrôle de puissance DownLink. Le power Control est désactivable par l'opérateur.

Principe et fonctionnement :

La gestion est entièrement réalisée par la BTS, le mobile exécute (contrôle tous les 60 ms)
A partir des mesures du mobile et de la BTS, la BTS réduit sa puissance ou réduit la puissance du mobile (ordre sur le SACCH) si les mesures dépassent certains seuils (paramétrables). Les pas d'incrémentation et de décrémentation sont de +4 dB et +2 dB (paramétrables).
Les algorithmes de Power Control UpLink et DownLink sont indépendants et peuvent être exécutés en parallèle.

Spectre fréquences descendantes

10°) Organisation des trames



11°) Organisation des canaux logiques dans les trames

Exemples de configuration de BTS

BTS avec une seule porteuse ARFC (CH):

8 TS sont donc disponibles, soit 6 communications

TS0 : FCCH,SCH,BCCH,PCH,AGCH,RACH, SDCCH-SACCH

TS1 : SDCCH-SACCH

TS2 à TS7 : TCH ,SACCH .

DOWNLINK		
FN	TS0	TS1
0	FCCH	SDCCH0
1	SCH	SDCCH0
2	BCCH1	SDCCH0
3	BCCH2	SDCCH0
4	BCCH3	SDCCH1
5	BCCH4	SDCCH1
6	AGCH/PCH	SDCCH1
7	AGCH/PCH	SDCCH1
8	AGCH/PCH	SDCCH2
9	AGCH/PCH	SDCCH2
10	FCCH	SDCCH2
11	SCH	SDCCH2
12	AGCH/PCH	SDCCH3
13	AGCH/PCH	SDCCH3
14	AGCH/PCH	SDCCH3
15	AGCH/PCH	SDCCH3
16	AGCH/PCH	SDCCH4
17	AGCH/PCH	SDCCH4
18	AGCH/PCH	SDCCH4
19	AGCH/PCH	SDCCH4
20	FCCH	SDCCH5
21	SCH	SDCCH5
22	SDCCH0	SDCCH5
23	SDCCH0	SDCCH5
24	SDCCH0	SDCCH6
25	SDCCH0	SDCCH6
26	SDCCH1	SDCCH6
27	SDCCH1	SDCCH6
28	SDCCH1	SDCCH7
29	SDCCH1	SDCCH7
30	FCCH	SDCCH7
31	SCH	SDCCH7
32	CBCH	SDCCH0
33	CBCH	SDCCH0
34	CBCH	SDCCH0
35	CBCH	SDCCH0
36	SDCCH3	SDCCH1
37	SDCCH3	SDCCH1
38	SDCCH3	SDCCH1
39	SDCCH3	SDCCH1
40	FCCH	SDCCH2
41	SCH	SDCCH2
42	SACCH0	SDCCH2
43	SACCH0	SDCCH2
44	SACCH0	SDCCH3
45	SACCH0	SDCCH3
46	SACCH1	SDCCH3
47	SACCH1	SDCCH3
48	SACCH1	
49	SACCH1	
50		

Multiplex des canaux de diffusion et de contrôle commun sur TS0 etTS1

(multitrame 51)

UPLINK		
FN	TS0	TS1
0	SDCCH2	SACCH1
1	SDCCH3	SACCH1
2	SDCCH3	SACCH1
3	SDCCH3	SACCH1
4	RACH	SACCH2
5	RACH	SACCH2
6	SACCH2	SACCH2
7	SACCH2	SACCH2
8	SACCH2	SACCH3
9	SACCH2	SACCH3
10	SACCH3	SACCH3
11	SACCH3	SACCH3
12	SACCH3	
13	SACCH3	
14	RACH	
15	RACH	SDCCH0
16	RACH	SDCCH0
17	RACH	SDCCH0
18	RACH	SDCCH0
19	RACH	SDCCH1
20	RACH	SDCCH1
21	RACH	SDCCH1
22	RACH	SDCCH1
23	RACH	SDCCH2
24	RACH	SDCCH2
25	RACH	SDCCH2
26	RACH	SDCCH2
27	RACH	SDCCH3
28	RACH	SDCCH3
29	RACH	SDCCH3
30	RACH	SDCCH3
31	RACH	SDCCH4
32	RACH	SDCCH4
33	RACH	SDCCH4
34	RACH	SDCCH4
35	RACH	SDCCH5
36	RACH	SDCCH5
37	SDCCH0	SDCCH5
38	SDCCH0	SDCCH5
39	SDCCH0	SDCCH6
40	SDCCH0	SDCCH6
41	SDCCH1	SDCCH6
42	SDCCH1	SDCCH6
43	SDCCH1	SDCCH7
44	SDCCH1	SDCCH7
45	RACH	SDCCH7
46	RACH	SDCCH7
47		SDCCH0
48		SDCCH0
49		SDCCH0
50		SDCCH0

DOWNLINK

FN	TS2	TS3	TS4	TS5	TS6	TS7
0	TCH	TCH	TCH	TCH	TCH	TCH
1	TCH	TCH	TCH	TCH	TCH	TCH
2	TCH	TCH	TCH	TCH	TCH	TCH
3	TCH	TCH	TCH	TCH	TCH	TCH
4	TCH	TCH	TCH	TCH	TCH	TCH
5	TCH	TCH	TCH	TCH	TCH	TCH
6	TCH	TCH	TCH	TCH	TCH	TCH
7	TCH	TCH	TCH	TCH	TCH	TCH
8	TCH	TCH	TCH	TCH	TCH	TCH
9	TCH	TCH	TCH	TCH	TCH	TCH
10	TCH	TCH	TCH	TCH	TCH	TCH
11	TCH	TCH	TCH	TCH	TCH	TCH
12	SACCH	SACCH	SACCH	SACCH	SACCH	SACCH
13	TCH	TCH	TCH	TCH	TCH	TCH
14	TCH	TCH	TCH	TCH	TCH	TCH
15	TCH	TCH	TCH	TCH	TCH	TCH
16	TCH	TCH	TCH	TCH	TCH	TCH
17	TCH	TCH	TCH	TCH	TCH	TCH
18	TCH	TCH	TCH	TCH	TCH	TCH
19	TCH	TCH	TCH	TCH	TCH	TCH
20	TCH	TCH	TCH	TCH	TCH	TCH
21	TCH	TCH	TCH	TCH	TCH	TCH
22	TCH	TCH	TCH	TCH	TCH	TCH
23	TCH	TCH	TCH	TCH	TCH	TCH
24	TCH	TCH	TCH	TCH	TCH	TCH
25						
0	TCH	TCH	TCH	TCH	TCH	TCH
1	TCH	TCH	TCH	TCH	TCH	TCH
2	TCH	TCH	TCH	TCH	TCH	TCH
3	TCH	TCH	TCH	TCH	TCH	TCH
4	TCH	TCH	TCH	TCH	TCH	TCH
5	TCH	TCH	TCH	TCH	TCH	TCH
6	TCH	TCH	TCH	TCH	TCH	TCH
7	TCH	TCH	TCH	TCH	TCH	TCH
8	TCH	TCH	TCH	TCH	TCH	TCH
9	TCH	TCH	TCH	TCH	TCH	TCH
10	TCH	TCH	TCH	TCH	TCH	TCH
11	TCH	TCH	TCH	TCH	TCH	TCH
12	SACCH	SACCH	SACCH	SACCH	SACCH	SACCH
13	TCH	TCH	TCH	TCH	TCH	TCH
14	TCH	TCH	TCH	TCH	TCH	TCH
15	TCH	TCH	TCH	TCH	TCH	TCH
16	TCH	TCH	TCH	TCH	TCH	TCH
17	TCH	TCH	TCH	TCH	TCH	TCH
18	TCH	TCH	TCH	TCH	TCH	TCH
19	TCH	TCH	TCH	TCH	TCH	TCH
20	TCH	TCH	TCH	TCH	TCH	TCH
21	TCH	TCH	TCH	TCH	TCH	TCH
22	TCH	TCH	TCH	TCH	TCH	TCH
23	TCH	TCH	TCH	TCH	TCH	TCH
24	TCH	TCH	TCH	TCH	TCH	TCH

Multiplex des canaux dédiés

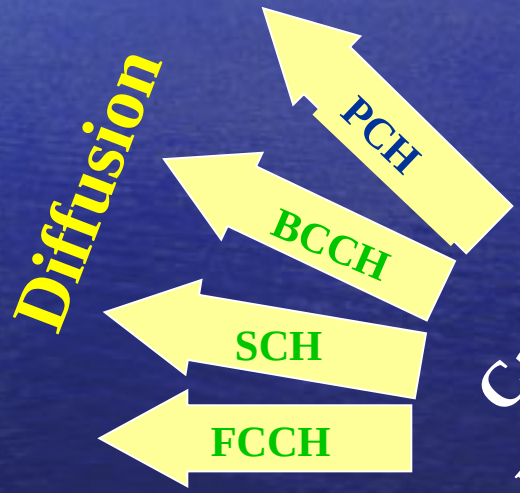
(multitrame 26)

UPLINK

FN	TS2	TS3	TS4	TS5	TS6	TS7
0	TCH	TCH	TCH	TCH	TCH	TCH
1	TCH	TCH	TCH	TCH	TCH	TCH
2	TCH	TCH	TCH	TCH	TCH	TCH
3	TCH	TCH	TCH	TCH	TCH	TCH
4	TCH	TCH	TCH	TCH	TCH	TCH
5	TCH	TCH	TCH	TCH	TCH	TCH
6	TCH	TCH	TCH	TCH	TCH	TCH
7	TCH	TCH	TCH	TCH	TCH	TCH
8	TCH	TCH	TCH	TCH	TCH	TCH
9	TCH	TCH	TCH	TCH	TCH	TCH
10	TCH	TCH	TCH	TCH	TCH	TCH
11	TCH	TCH	TCH	TCH	TCH	TCH
12	SACCH	SACCH	SACCH	SACCH	SACCH	SACCH
13	TCH	TCH	TCH	TCH	TCH	TCH
14	TCH	TCH	TCH	TCH	TCH	TCH
15	TCH	TCH	TCH	TCH	TCH	TCH
16	TCH	TCH	TCH	TCH	TCH	TCH
17	TCH	TCH	TCH	TCH	TCH	TCH
18	TCH	TCH	TCH	TCH	TCH	TCH
19	TCH	TCH	TCH	TCH	TCH	TCH
20	TCH	TCH	TCH	TCH	TCH	TCH
21	TCH	TCH	TCH	TCH	TCH	TCH
22	TCH	TCH	TCH	TCH	TCH	TCH
23	TCH	TCH	TCH	TCH	TCH	TCH
24	TCH	TCH	TCH	TCH	TCH	TCH
25						
0	TCH	TCH	TCH	TCH	TCH	TCH
1	TCH	TCH	TCH	TCH	TCH	TCH
2	TCH	TCH	TCH	TCH	TCH	TCH
3	TCH	TCH	TCH	TCH	TCH	TCH
4	TCH	TCH	TCH	TCH	TCH	TCH
5	TCH	TCH	TCH	TCH	TCH	TCH
6	TCH	TCH	TCH	TCH	TCH	TCH
7	TCH	TCH	TCH	TCH	TCH	TCH
8	TCH	TCH	TCH	TCH	TCH	TCH
9	TCH	TCH	TCH	TCH	TCH	TCH
10	TCH	TCH	TCH	TCH	TCH	TCH
11	TCH	TCH	TCH	TCH	TCH	TCH
12	SACCH	SACCH	SACCH	SACCH	SACCH	SACCH
13	TCH	TCH	TCH	TCH	TCH	TCH
14	TCH	TCH	TCH	TCH	TCH	TCH
15	TCH	TCH	TCH	TCH	TCH	TCH
16	TCH	TCH	TCH	TCH	TCH	TCH
17	TCH	TCH	TCH	TCH	TCH	TCH
18	TCH	TCH	TCH	TCH	TCH	TCH
19	TCH	TCH	TCH	TCH	TCH	TCH
20	TCH	TCH	TCH	TCH	TCH	TCH
21	TCH	TCH	TCH	TCH	TCH	TCH
22	TCH	TCH	TCH	TCH	TCH	TCH
23	TCH	TCH	TCH	TCH	TCH	TCH
24	TCH	TCH	TCH	TCH	TCH	TCH

12°) Les canaux logiques mis en œuvre pour l'état de veille

- En veille, le mobile échange avec sa base des signaux de contrôle sur la voie balise (émission en slot 0 à f1, réception en slot 0 à f1+45MHz) toutes les 15 secondes si le signal reçu est fort et toutes les secondes s'il est faible



BTS

13°) Les canaux logiques mis en œuvre lors de l'établissement dun appel

Contrôle

RACH

AGCH

Canaux non-dédiés

Canaux dédiés

BTS

14°) Les canaux logiques mis en œuvre en communication

Canaux dédiés

Diffusion

PCH
BCCH
SCH
FCCH

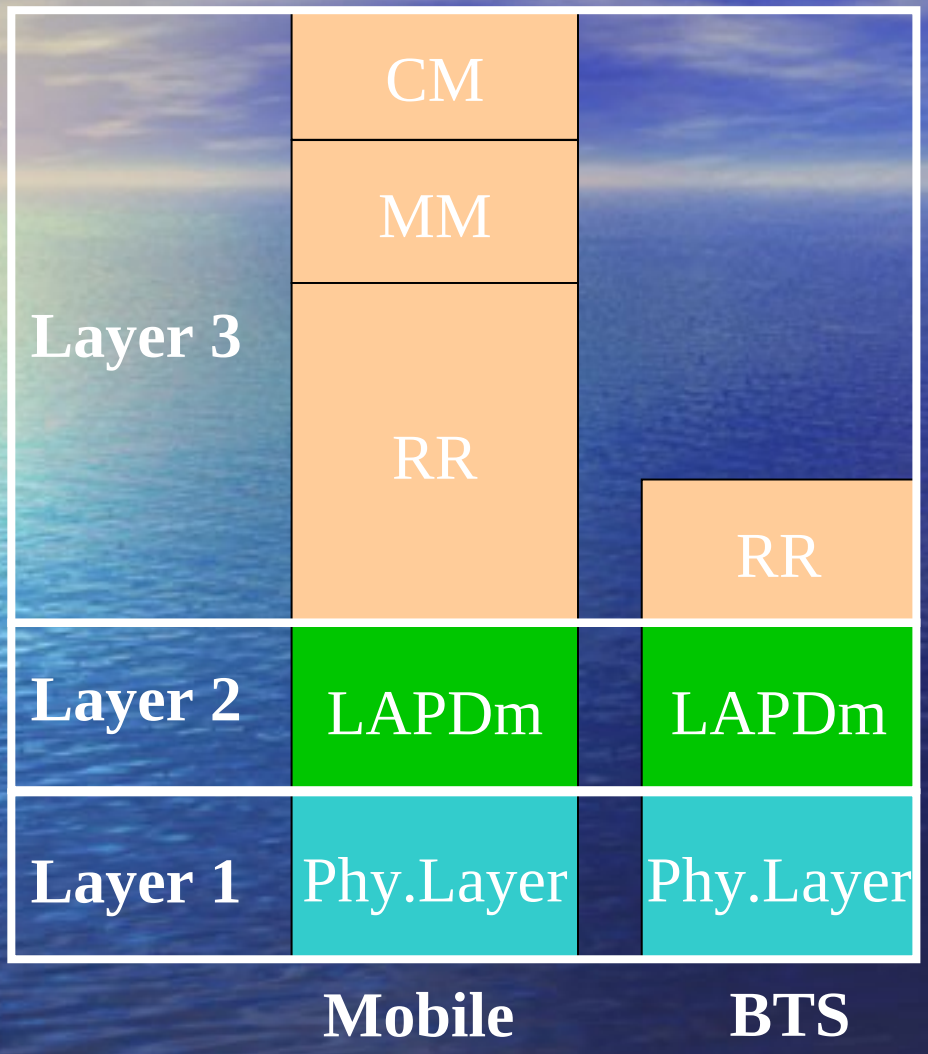
Canaux non-dédiés

BTS

VII. Architecture de protocoles

OSI GSM

1°) Les couches GSM



Layer 3 :

- **RR :** Radio Ressource Management : installation, maintenance et abandon d'une connexion radio. (Message type 06)
- **MM :** Mobility Management : Enregistrement auprès du réseaux, authentification, mise à jour de la localisation…(Message type 05)
- **CM :** Call Management : Etablissement, maintient et arrêt d 'une communication. (Message type X3)

Layer 2 : Link Access protocol D-Channel: Assure la gestion de la liaison de données.
Protocole X25 LAPDm

Layer 1 : Couche physique de transmission: C'est l 'interface Radio : création des burst, multiplexage, mesures….

2°) Les communications

Appel à l'initiative d'un mobile (appel sortant ou Mobile Originating MO) :

Emission d'un RACH du mobile à la BTS.
Demande d'affectation de canal de la BTS au BSC.
Allocation du canal au mobile par le BSC via la BTS (AGCH).
Authentification du mobile et chiffrement sur canal SDCCH.
Basculement sur le canal FACCH et TCH alloué.
Relâchement du canal SDCCH.
Transmission de la parole sur TCH.

Appel vers un mobile (appel entrant ou Mobile Terminating MT) :
La procédure est la même sauf que l'émission du RACH du mobile est précédée d'une procédure de paging (PCH) venant du réseau.

PCH RR Paging request type 1

PCH RR Paging request type 2

PCH RR Paging request type 3

Message de couche 3 en mode Idle

BCCH RR System information type 1

BCCH RR System information type 2

BCCH RR System information type 2 ter

BCCH RR System information type 3

BCCH RR System information type 4

MS

BTS

Parmis tous les paging Request le mobile peut identifier s'il en est le

System information type 3 (code 06 1B) : contient Les informations de la cellule serveuse : identé CI (cell identity), LAC, description du canal, gestion de la

System information type 2 ter (code 06 03) : contient les droits d'accès et les fréquences ARFC supplémentaires du DCS 1800 des BTS des cellules voisines.

Message de couche 3 périodiques pendant une communication

SACCH RR System information type 5

SACCH RR System information type 5ter

SACCH RR System information type 6

MS

BTS

SACCH RR Measurement report

Measurement report (code 06 15) : transfère les mesures courantes du mobile à la BTS. Il contient les niveaux de réception mesurées pour la cellule serveuse et les 6 voisines. Il est émis toutes les 480ms. Il sert à déclencher la commande de Hand Hover

Connect acknowledge (code 03 0F) : le mobile acquitte la connexion. On paye à partir de cet instant la communication.

RACH RR Channel Request

AGCH RR Immediat assignement

SDCCH MM CM service requested

SDCCH MM Authentification request

SDCCH MM Authentification response

SDCCH RR Ciphering mode command

SDCCH RR Ciphering mode complete

SDCCH CC Setup (*établissement*)

SDCCH CC Call proceeding

SDCCH RR Assignement command

FACCH RR Assignement complete

FACCH CC Alerting

FACCH CC Connect

FACCH CC Connect acknowledge

MS

Message de couche 3 lors de l'établissement d 'une communication (Mobile appelant)

BTS

Immediat assigment (code 06 3F) : ordre au mobile de commuter sur le canal SDCCH activé. Contient TA (time advance. TS (time slot sur le

Assignement complete (code 06 29) : Le mobile libère le SDCCH puis confirme son passage sur le canal TCH + FACCH alloué.
mobile.

Messages de couche 3 lors de l'établissement d 'une communication (Mobile appelé)

PCH RR Paging request

RACH RR Channel request

AGCH RR Immediat assignement

SDCCH RR Paging response

SDCCH Authentification request

SDCCH Authentification response

SDCCH Ciphering mode command

SDCCH Ciphering mode complete

SDCCH Setup

SDCCH Call confirmed

SDCCH Assignement command

FACCH Assignement complete

FACCH Alerting (*call confirmation*)

MS

BTS

Parmi tous les paging Request le mobile peut identifier s'il en est le destinataire en examinant le TMSI ou l'IMSI passé en paramètre.

Trois type de Paging request type 1 (code 06 21) : 1 seul mobile appelé

Paging response (code 06 27) : le mobile répond à la demande de paging

Le mobile demande l'allocation d'un canal SDCCH en réponse au paging des 6 cellules voisines.

3°) La mobilité : le HandOver

La mobilité est la possibilité qu'a le mobile de maintenir la communication lors de son déplacement.
Pour cela, le réseau effectue la procédure de HandOver (HO), c'est-à-dire le passage d'une cellule à l'autre afin d'assurer la meilleure qualité de la communication

Pour définir si la communication est de bonne ou mauvaise qualité, des paramètres ont été définit :

Le niveau de puissance du signal de la cellule **RxLev**. C'est un nombre entier. RxLev-110 = puissance en dBm.

La qualité du signal de la cellule **RxQual**. C'est un nombre entier compris entre 0 (bon) et 7 (mauvais) qui traduit le taux d'erreurs binaires (BER) dans les trames TDMA.

La distance entre Mobile et BTS : **le Timing Advance (TA).**
Décalage temporel des émissions des mobiles pour synchroniser les intervalles de temps dans la trame TDMA. C'est un nombre entier entre 0 et 63 (63 représentant la distance max 35 km).

Le HO se déclenche à l'initiative du réseau pour les raisons suivantes :

Si le niveau de champ (RxLev) de la cellule serveuse est insuffisant => HO sur niveau (RxLev UpLink ou DownLink).

Si le niveau de qualité (RxQual) de la cellule serveuse est insuffisant => HO sur Qualité (RxQual UpLink ou DownLink).

Si le mobile est trop loin de la BTS => HO sur Distance (la distance maximale entre Mobile et BTS est de 35 km).

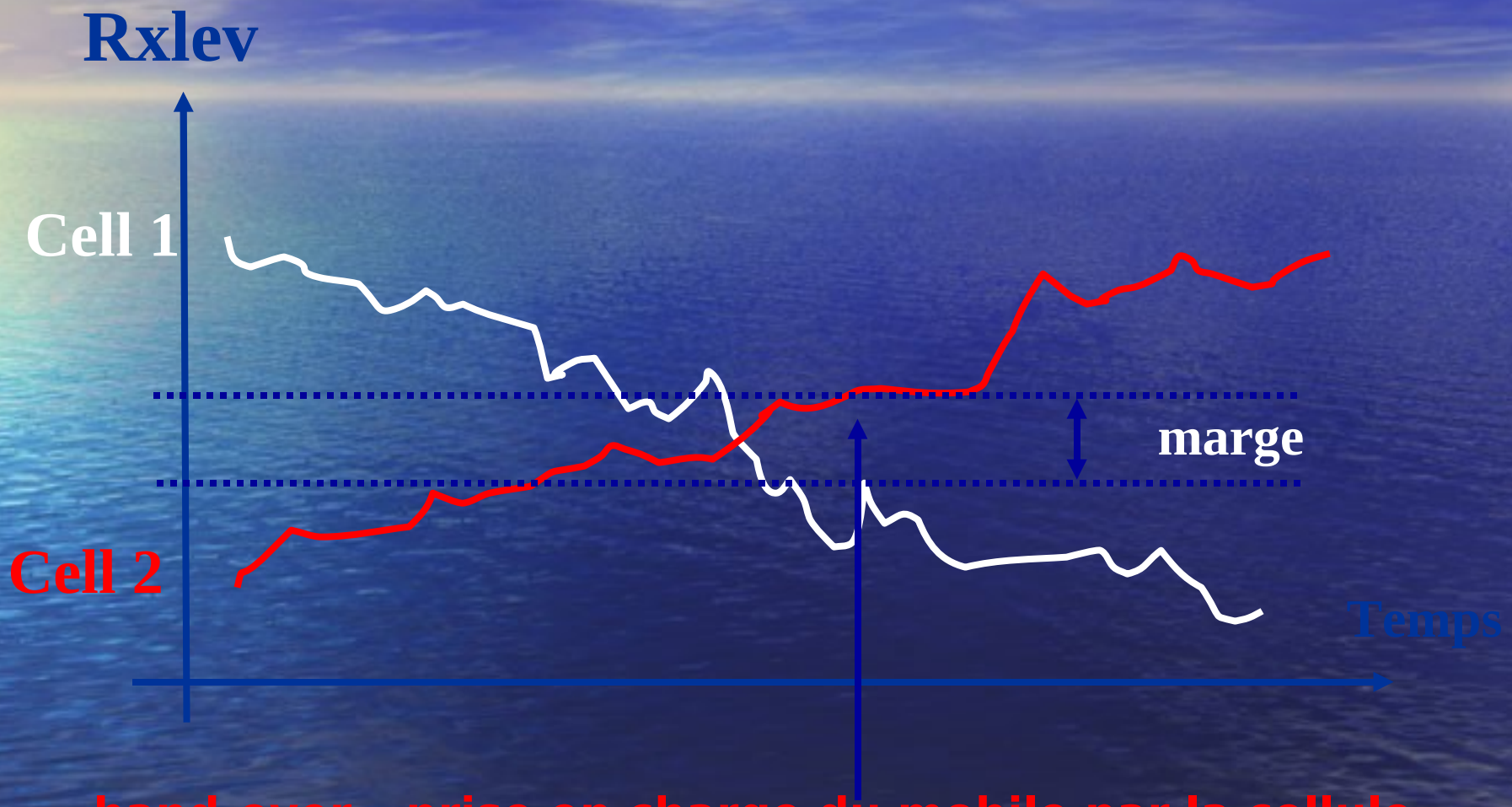
Si une cellule voisine est meilleure ou de qualité égale mais nécessitant une puissance plus faible sans que la cellule serveuse soit mauvaise => HO sur bilan de liaison (HO sur PBGT).

Pour savoir, en cas de HO, sur quelle cellule aller, le mobile est à l'écoute de diverses informations qui lui permettront d'établir une liste des cellules voisines possibles.

Il mesure :

le niveau de champ de la cellule serveuse et des cellules voisines.
la qualité de la cellule serveuse.
la distance par rapport à la cellule serveuse.
l'identité de la cellule serveuse et des cellules voisines.
la LAC sur laquelle il est connecté.

Ces informations servent au réseau à déclencher le HO et à savoir sur quelle cellule le mobile doit aller.



hand-over= prise en charge du mobile par la cellule 2

En veille :

le mobile scrute le canal de signalisation BCCH (Broadband Control Channel) de 7 cellules proches lui.

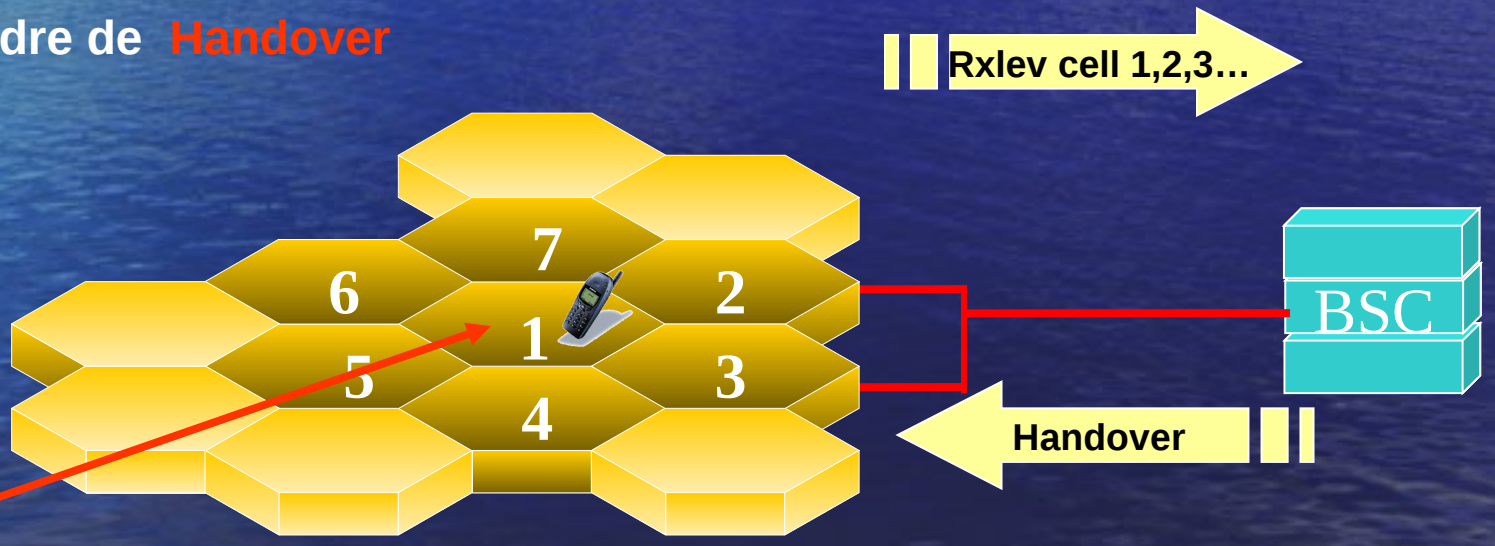
Le mobile mesure sur les 7 cellules le niveau du signal BCCH reçu noté RXLev, et la qualité du signal noté RXQual.

En communication:

Des rapports de mesures de puissance et de qualité sont envoyées au BSC afin d'y être analysées.

C'est le BSC qui décide de changer de cellule serveuse.

C'est un ordre de Handover



La cellule reçue la plus puissante est appelée : La « cellule serveuse » (Serving cell)

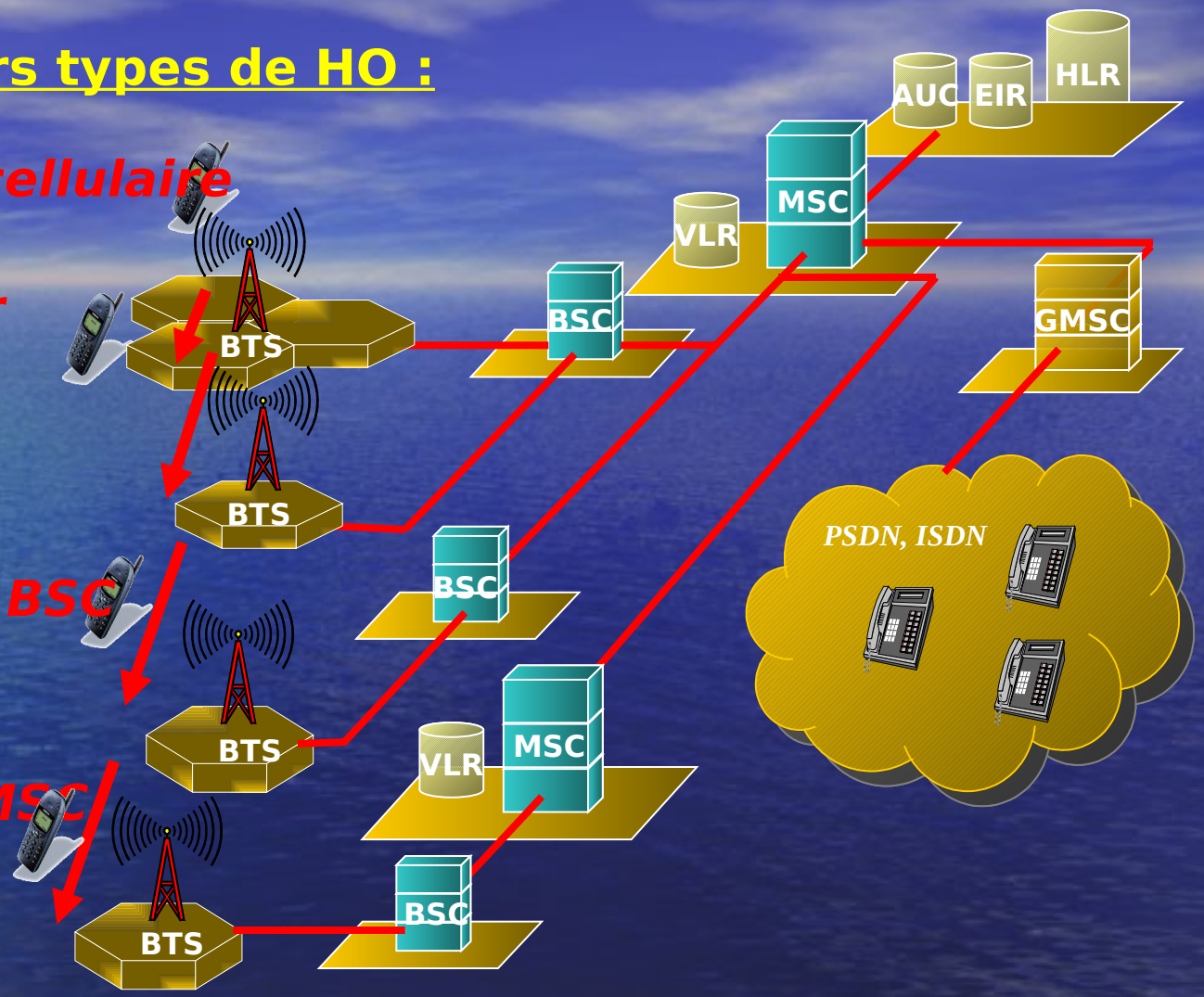
Il existe plusieurs types de HO :

Hand-over intra cellulaire

Hand-over inter cellulaire ou intra BSC

Hand-over inter BSC

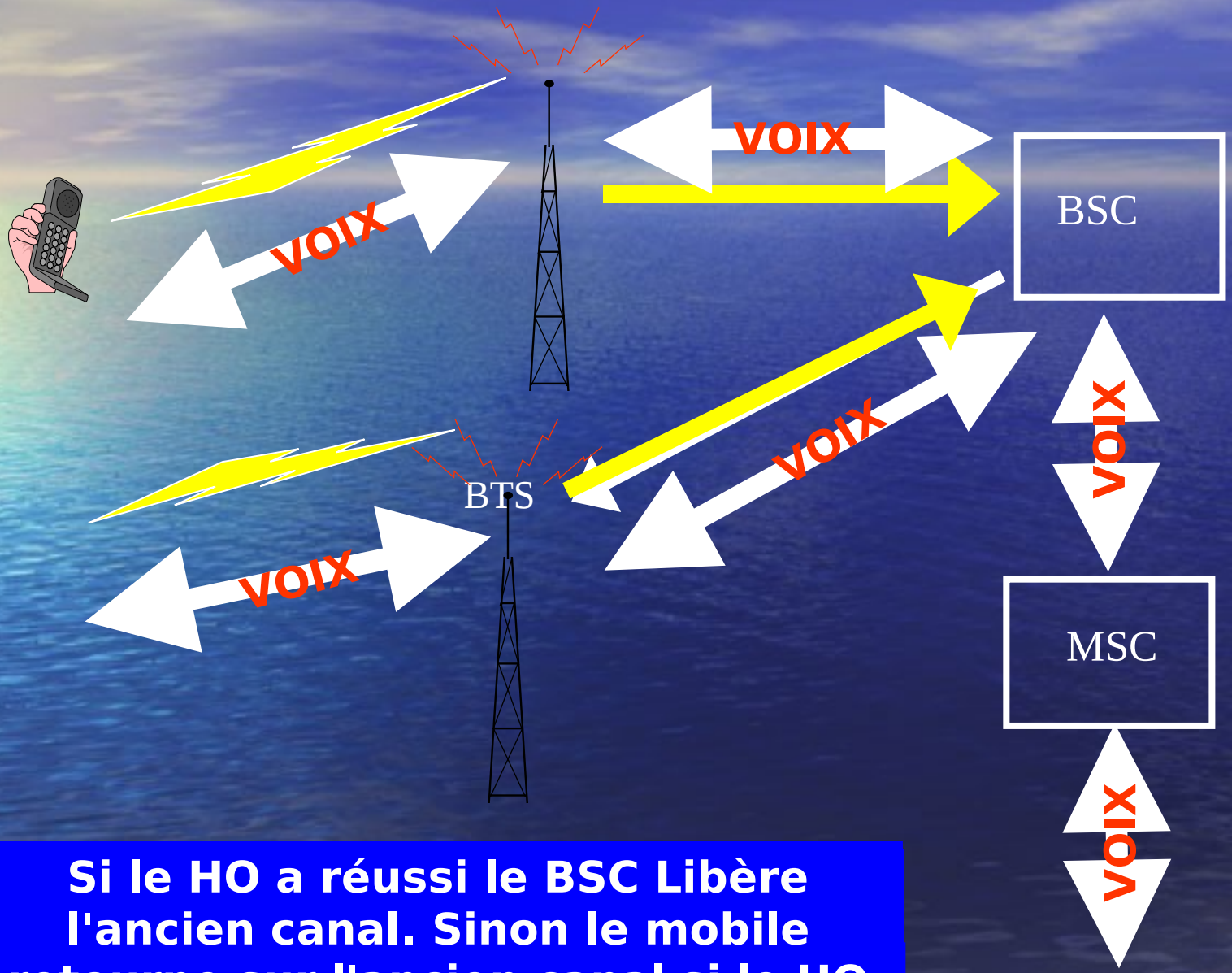
Hand-over inter MSC



HO interMSC.

Passage d'une cellule gérée par un BSC d'un MSC à une cellule gérée par un autre BSC dépendant d'un autre MSC. Ce type de HO est le plus critique car les temps de transfert des informations pendant la procédure pénalise le HO.

HO intercellulaire.



Si le HO a réussi le BSC Libère l'ancien canal. Sinon le mobile retourne sur l'ancien canal si le HO (HO-FAILURE)

Hand-over

MS

SACCH RR Measurement report

FACCH Hand Over command

FACCH Hand Over access

FACCH Hand Over complete

FACCH Physical Information

BTS1

Measurement report (code 06 15) : transfère les mesures courantes du mobile à la BTS. Il contient les niveaux de réception mesurées pour la cellule serveuse et les 6 voisines. Il est émis toutes les 480ms. Au cas ou ces niveaux deviennent insuffisant le réseau décidera de réaliser un Hand Over sur une des cellules voisines dont le BSIC est fournit par le mobile avec les mesures de sa puissance de réception.

Le mobile à trace pouvant forcer le Hand Over il ne transmet que les valeurs d'une

4°) Analyse de trace

L'analyse de trace permet de suivre tous les messages de couche 2 et 3 transmis entre le mobile et la BTS. Il permet aussi de connaître la configuration et le paramétrage du mobile.

Pour réaliser ces mesures il faut utiliser un mobile spécial appelé mobile à trace. Ces appareils sont très couteux et difficile à se procurer.

La trace d'une communication complète réalisée à partir de mon domicile, à été enregistrée. Vous pouvez l'examiner tout à loisir comme s'il s'agissait d'une communication en temps réel. Vous y trouverez :

Une trace en mode idle (0<compteur<300),

Un appel sortant ou Mobile Originating MO (300<compteur<800),

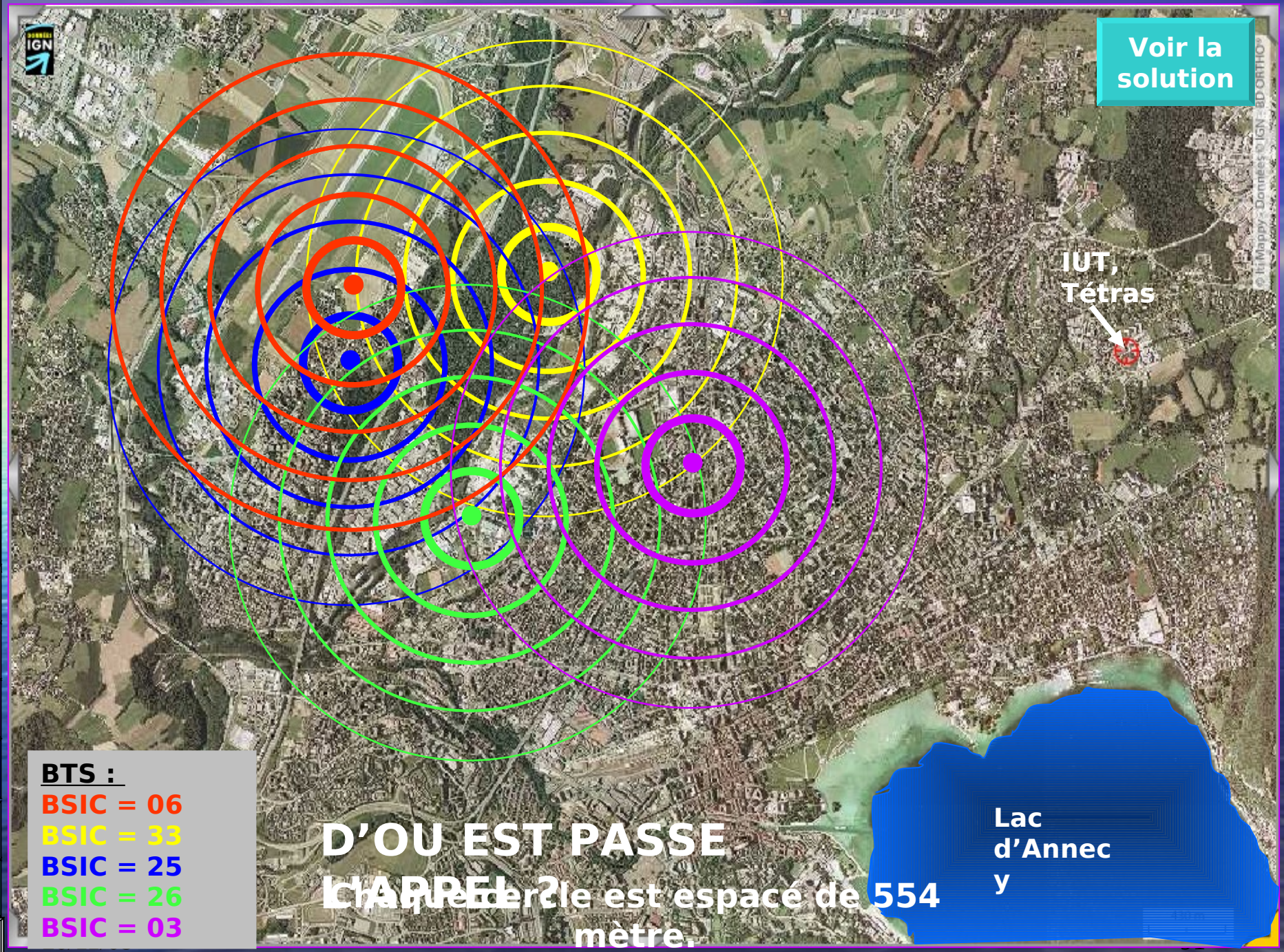
Un premier Hand over (800<compteur<1150) puis un second Hand over (1150<compteur<1450). Ces hand over ont étés forcés grâce au mobile à trace. Il n'y a donc pas eu de déplacement réel.

Une fin d'appel (1450<compteur) .

A partir des informations présentes dans cette trace
Déterminer :

- Mon opérateur de téléphonie mobile
- La marque de mon mobile
- Mon pays
- Mon TMSI
- Le numéro de référence de ma demande d'attribution d'un canal TCH
- Le code de ma zone de localisation
- L'identifiant de la 1ere cellule serveuse
- Le code d'identification de la BTS de cette cellule
- La fréquence de sa voie balise
- Le time slot attribué sur SDCCH pour réaliser mon authentification
- La distance entre le mobile et cette BTS
- La valeur du nombre RAND qui m'a été envoyé pour vérifier mon identité
- La valeur du résultat SRES que le mobile à retourné
- L'algorithme de chiffrement que le mobile à activé
- Le numéro que j'ai composé. Vous savez, c'est celui que vous pouvez faire pour vous inscrire à Tétras en licence pro R&T en alternance.
- L'identifiant de la cellule serveuse suite au 1er Hand Over
- Le code d'identification de la BTS de cette cellule
- La fréquence de sa voie balise
- Le time slot attribué sur SDCCH pour réaliser mon authentification
- La distance entre le mobile et cette BTS
- L'identifiant de la cellule serveuse suite au 2eme Hand Over
- Le code d'identification de la BTS de cette cellule
- La fréquence de sa voie balise
- Le time slot attribué sur SDCCH pour réaliser mon authentification
- La distance entre le mobile et cette BTS
- Repérer sur la carte, page suivante l'endroit d'où je passe cet appel. Vous avez tous les éléments pour y parvenir, et avec un peu de chance essayez de calculer l'age du capitaine ….

Exécuter le logiciel de trace GSM


Voir la solution
IUT, Tétras
Lac d'Annecy
BTS :
BSIC = 06
BSIC = 33
BSIC = 25
BSIC = 26
BSIC = 03
D'OU EST PASSE L'APPEL ?
Chaque cercle est espacé de 554 mètre.

VIII. Les évolutions du GSM

Le mode circuit :

Le GSM s'oriente de plus en plus vers la transmission de données et principalement vers de l'internet.
Problème : le débit sur GSM est actuellement de 9,6 à 14,4 kbit/s.

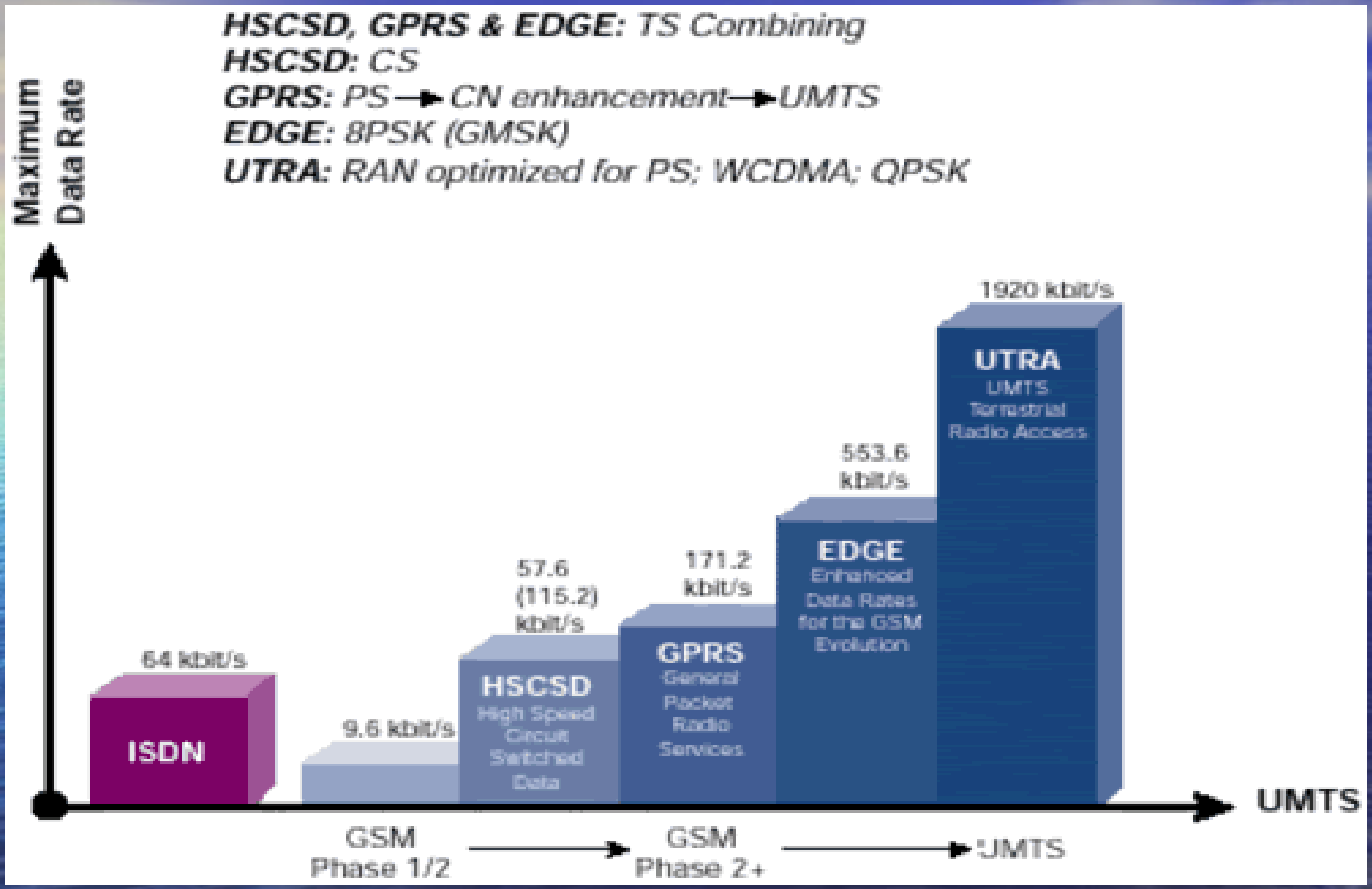
1°) Le Mode Circuit

On utilise un ou plusieurs canaux privés pour transmettre les données.

pour le service data/fax du GSM actuel on obtient un débit de 9,6 à 14,4 kbit/s

En utilisant plusieurs canaux on peut obtenir un débit jusqu'à 64 kbit/s. (HSCSD High Speed Circuit Switched Data).

Inconvénient : L'utilisation en continu d'un ou plusieurs canaux pour des émissions sporadiques de données engendre de grosses pertes de capacité donc un gaspillage.


HSCSD, GPRS & EDGE: TS Combining
HSCSD: CS
GPRS: PS → CN enhancement → UMTS
EDGE: 8PSK (GMSK)
UTRA: RAN optimized for PS; WCDMA; QPSK
Maximum Data Rate
64 kbit/s
ISDN
9.6 kbit/s
57.6 (115.2) kbit/s
HSCSD
High Speed Circuit Switched Data
171.2 kbit/s
GPRS
General Packet Radio Services
553.6 kbit/s
EDGE
Enhanced Data Rates for the GSM Evolution
1920 kbit/s
UTRA
UMTS Terrestrial Radio Access
UMTS
GSM Phase 1/2
GSM Phase 2+
UMTS

2°) Le Mode Paquet

Le principe du mode paquet est de découper l'information et de transmettre les données par paquet lorsque les canaux ne sont pas utilisés pour la phonie.

Le mode paquet permet la facturation à la quantité de données transportée

Le mode paquet optimise les ressources radio par gestion de priorité, mise en attente et affectation de ressources radio uniquement en cas de transfert.

Un canal radio peut être utilisé par plusieurs utilisateurs. Les Time Slots sont partagés entrainant moins de blocage.

Un utilisateur peut utiliser plusieurs canaux radio. Les Time Slots sont agrégés les débits sont plus importants.

Mode circuit :

Mode paquet :

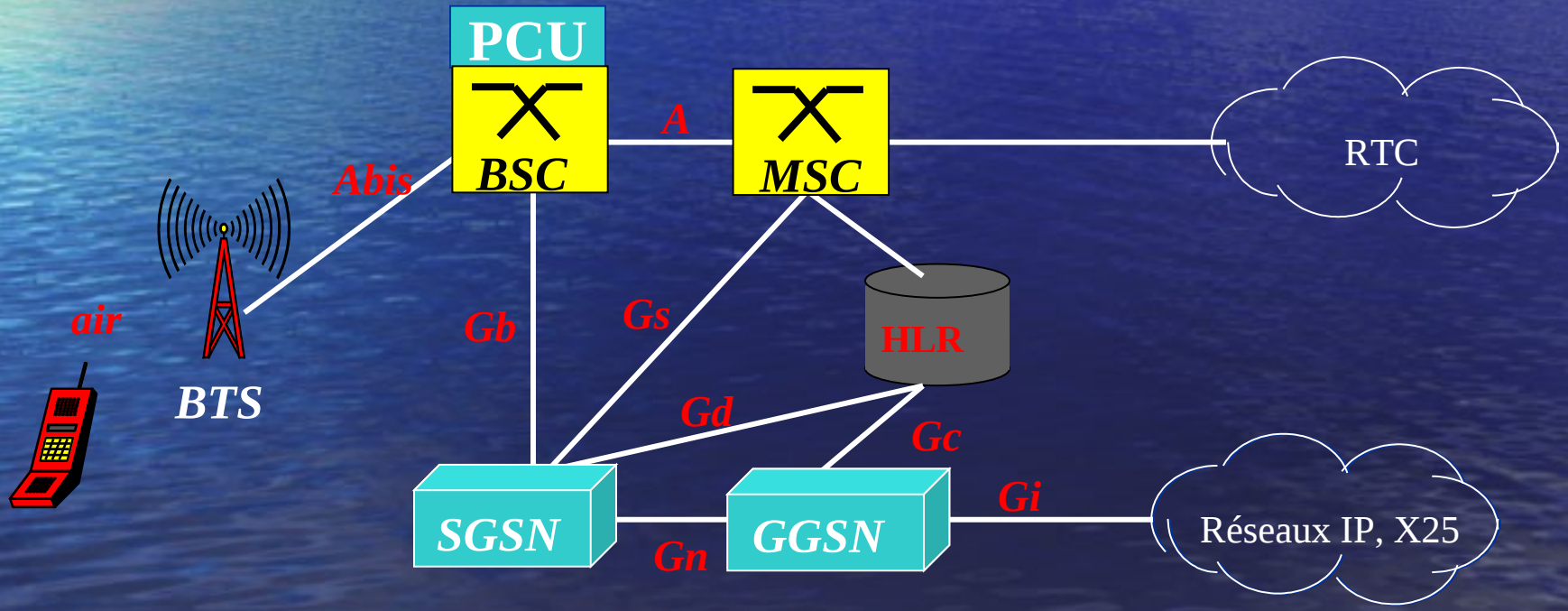
En-tête, contient l'adresse du destinataire.

« payload », contient les données utilisateur

3°) Le GPRS (General Packet Radio Service)

Le ***GPRS*** est un service de transmission de données en mode ***paquet*** qui exploite la radio GSM pour la transmission des paquets sur l'interface air.

Le déploiement du GPRS nécessite la mise en place d'une ***infrastructure réseau basée sur la commutation de paquets*** et l'introduction de passerelles pour s'adosser aux réseaux GSM existants.



Le nœud de service (*SGSN*, Serving GPRS Support Node) est relié au BSS de l'opérateur. Il permet la gestion des données d'abonnés, la gestion de sa mobilité ainsi que la phase d'établissement d'une session et du contrôle de la qualité de service lié à l'établissement de cette session.

Le nœud passerelle (*GGSN*, Gateway GPRS Support Node) est relié aux divers réseaux de données qui lui sont raccordés. Le GGSN est un *routeur* permettant de transiter les paquets de données entrants/sortants entre le réseau GPRS et les réseaux externes.

Afin de contrôler l'allocation de canaux logiques spécifiques (canaux PDCH) et de gérer les types de codage qu'offre GPRS, l'élément complémentaire PCU est ajouté au niveau du BSC.

4°) L'EDGE (Enhanced Data rate for GSM Evolution) ou EGPRS

Le débit max du GPRS n'est valable que pour des C/I importants (utilisation du CS-4), ce qui n'est pas toujours le cas.
On va donc changer de modulation la GMSK devient 8-PSK. La vitesse de modulation est la même que pour le GMSK mais permet un débit instantané 3 fois plus élevé, chaque état de modulation transmettant l'information relative à 3 bits.

Débits du EDGE

6 débits sont normalisés de PCS-1 à PCS-6 variant de 22,8 kbit/s à 69,2 kbit/s par Time Slot.
Le débit max instantané sera donc de 553 kbit/s (moy # 300 kbit/s).

5°) L ’UMTS

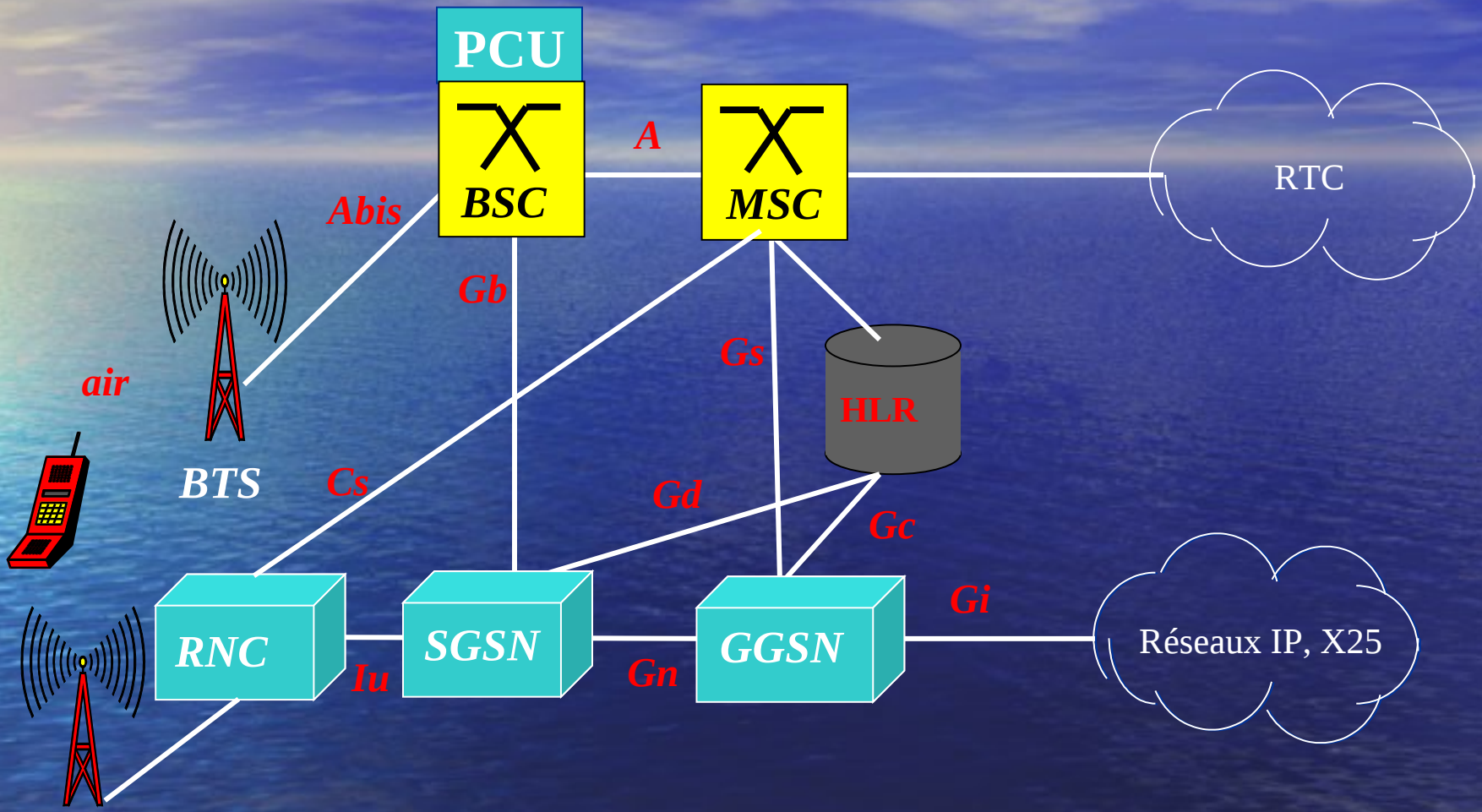
L'UMTS (Universal Mobile Telecommunication System) **est la version européenne définie par l'ETSI (Institut Européen de Normalisation des Télécommunications) de la troisième génération des services mobiles (3G). Il devrait délivrer des débits compris entre 384 kb/s et 2 Mb/s.**

Cette norme est un membre de famille du projet IMT-2000 (International Mobile Telecommunication System 2000) défini par l'UIT (Union Internationale des Télécommunications). Celui-ci a pour but de normaliser les systèmes de télécommunications mobiles de troisième génération qui assureront l'accès à l'infrastructure mondiale des télécoms, dans un contexte mondial d'itinérance.

Cette nouvelle norme repose sur les technologies W-CDMA (combinaison de CDMA et FDMA) et TD-CDMA (combinaison de TDMA, CDMA et FDMA).

Le principe de transmission repose sur l’étalement de spectre et la modulation QPSK. Les fréquences utilisées sont 2 bandes appairées (1920-1980 MHz et 2110-2170 MHz) et 2 bandes non appairées (1900-1920 MHz et 2010-2025 MHz).

Cette technologie permet la transmission de données en mode paquet (et en mode circuit) à des débits d’environ 2 Mbit/s,


PCU
BSC
MSC
A
RTC
Abis
Gb
Gs
HLR
air
BTS
Cs
Gd
Gc
RNC
SGSN
GGSN
Gi
Iu
Gn
Réseaux IP, X25

FIN

SOMMAIRE

II. Les Contraintes générées par la mobilité.

1°) Le vecteur de transmission n'est plus filaire.

2°) Le territoire ou le service est proposé doit être parfaitement couvert.

3°) L'acheminement des communications doit être possible.

4°) L'accès à ce service doit être étendu à toutes les catégories d'usagés.

- 4.1) Partage des ressources radios
- 4.2) Le principe cellulaire
- 4.3) La réutilisation des fréquences
- 4.4) Les antennes
- 4.5) La liaison hertzienne
- 4.6) Le multiplexage temporel et fréquentiel
- 4.7) Coût non prohibitif

5°) L'accès à tous les services proposés par le réseau fixe doit être possible.

- 5.1) Télé services vocaux
- 5.2) Télé services de données
- 5.3) Les Messages Courts
- 5.4) Service support
- 5.5) Services supplémentaires

6°) Les communications doivent être sécurisées.

- 6.1) Sécurité pour l'usager
- 6.2) Sécurité pour l'usager et l'opérateur
- 6.3) Sécurité pour l'opérateur

III.Architecture du réseau GSM.

IV.Gestion de l'itinérance et de la sécurité des appels.

V. Les canaux physiques :

VI. Les canaux logiques :

1°) Canaux de diffusion BCH

2°) Canaux communs de contrôle CCCH

3°) Canaux de signalisation dédiés

4°) Canaux de trafic

5°) Constitution d'un slot normal

6°) Compensation des temps de propagation

7°) Constitution d'un slot RACH

8°) Les interférences

9°) Le contrôle de puissance : Power Control

10°) Organisation des trames

11°) Organisation des canaux logiques dans les trames

12°) Les canaux logiques mis en œuvre pour l'état de veille

13°) Les canaux logiques mis en œuvre lors de l'établissement dun appel

14°) Les canaux logiques mis en œuvre en communication

VII.Architecture de protocoles

1°) Les couches GSM

2°) Les communications

3°) La mobilité : le HandOver

4°) Analyse de trace

VIII.Les évolutions du GSM

1°) Le Mode Circuit

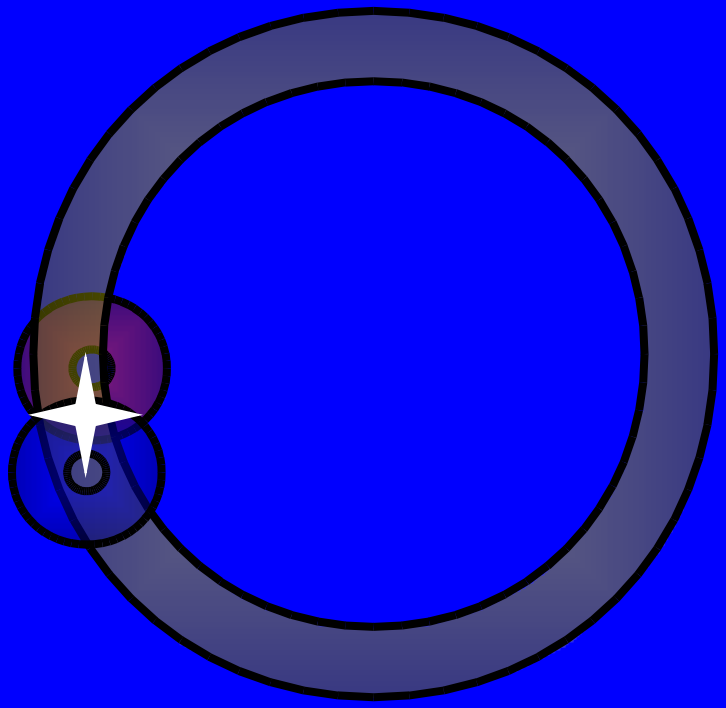
2°) Le Mode Paquet

3°) Le GPRS (General Packet Radio Service)

4°) L'EDGE

5°) L 'UMTS

FIN



VOICI LA SOLUTION