

PRINCIPES DE BASE DU FONCTIONNEMENT DU RÉSEAU GSM

Cédric DEMOULIN, Marc VAN DROOGENBROECK
Département d'Électricité, Électronique et Informatique (Institut Montefiore)
Sart Tilman, B-4000 Liège, Belgique
<http://www.ulg.ac.be/telecom>

Résumé

Si la téléphonie mobile se banalise aujourd'hui, on le doit à la conjonction de l'avènement du numérique, à l'accroissement des performances des semi-conducteurs et à différentes avancées technologiques. Mais le facteur déterminant fut sans doute la cristallisation autour de la norme GSM issue d'un effort soutenu de standardisation mené à l'ETSI¹ (Organe européen de normalisation en télécommunications, créé à l'initiative du Conseil des ministres).

Dans cet article, nous passerons en revue différents aspects de la technologie GSM : éléments de la couche physique, caractérisation de la partie radio, architecture du réseau, etc. Pour faciliter la lecture –il faut concéder que les acronymes abondent dans ce domaine–, un glossaire est fourni en fin d'article.

1 Introduction

1.1 Historique

L'histoire de la téléphonie mobile (numérique) débute réellement en 1982. En effet, à cette date, le *Groupe Spécial Mobile*, appelé GSM², est créé par la Conférence Européenne des administrations des Postes et Télécommunications (CEPT) afin d'élaborer les normes de communications mobiles pour l'Europe dans la bande de fréquences de 890 à 915 [MHz] pour l'émission à partir des stations mobiles³ et 935 à 960 [MHz] pour l'émission à partir de stations fixes. Il y eut bien des systèmes de mobilophonie analogique (MOB1 et MOB2, arrêté en 1999), mais le succès de ce réseau ne fut pas au rendez-vous.

Les années 80 voient le développement du numérique tant au niveau de la transmission qu'au niveau du traitement des signaux, avec pour dérivés des techniques de transmission fiables, grâce à un encodage particulier des signaux préalablement à l'envoi dans un canal, et l'obtention de débits de transmission raisonnables pour les signaux (par exemple 9,6 kilobits par seconde, noté [kb/s], pour un signal de parole).

Ainsi, en 1987, le groupe GSM fixe les choix technologiques relatifs à l'usage des télécommunications mobiles : transmission numérique, multiplexage temporel des canaux radio, chiffrement des informations ainsi qu'un nouveau codage de la parole. Il faut attendre 1991 pour que la première communication expérimentale par GSM ait lieu. Au passage, le sigle GSM change de signification et devient *Global System for Mobile communications* et les spécifications sont adaptées pour des systèmes fonctionnant dans la bande des 1800 [MHz].

En Belgique, c'est en 1994 que le premier réseau GSM (proximus) est déployé ; Mobistar et Orange (rebaptisé Base) viendront plus tard. Aujourd'hui, le nombre de numéros attribués pour des communications GSM dépasse largement le nombre de numéros dédiés à des lignes fixes et cette tendance se poursuit.

1.2 Évolution technologique

Tel quel, le réseau GSM est adéquat pour les communications téléphoniques de parole. En effet, il s'agit principalement d'un réseau commuté, à l'instar des lignes "fixes" et constitués de circuits, c'est-à-dire de ressources allouées pour la totalité de la durée de la conversation. Rien ne fut mis en place pour les services de transmission de données. Or, parallèlement au déploiement du GSM en Belgique, en 1994, la société Netscape allait donner un tour spectaculaire à un réseau de transmission de données, appelé Internet, en diffusant le premier logiciel de navigation grand public, articulé sur le protocole http et communément appelé web.

¹<http://www.etsi.org>

²C'est en fait la première définition de l'acronyme GSM.

³Pour des raisons d'économie de puissance et en vertu de la loi de FRIIS, on privilégie toujours les basses fréquences pour les émissions omnidirectionnelles.

Comme le réseau GSM ne convenait guère pour la transmission de données, les évolutions récentes ont visé à accroître la capacité des réseaux en termes de débit mais à élargir les fonctionnalités en permettant par exemple l'établissement de communications ne nécessitant pas l'établissement préalable d'un circuit.

Pour dépasser la borne des $14,4 [kb/s]$, débit nominal d'un canal téléphonique basculé en mode de transmission de données, l'ETSI a défini un nouveau service de données en mode paquet : le *General Packet Radio Service (GPRS)* qui permet l'envoi de données à un débit de $115 [kb/s]$ par mise en commun de plusieurs canaux. D'une certaine manière, le GPRS prépare l'arrivée de la téléphonie de troisième génération, appelée *Universal Mobile Telecommunications System (UMTS)*, qui permettra d'atteindre un débit de $2 [Mb/s]$. Mais le chemin est long car les applications nécessitant l'UMTS se font attendre, sans perdre de vue que tous les éléments du réseau UMTS sont incompatibles avec ceux du GSM. Pourquoi les investisseurs devraient-ils donc mettre la main au portefeuille ?

2 La technologie GSM

2.1 Le concept cellulaire

Les réseaux de première génération possédaient des cellules de grande taille ($50 [km]$ de rayon) au centre desquelles se situait une station de base (antenne d'émission). Au tout début, ce système allouait une bande de fréquences de manière statique à chaque utilisateur qui se trouvait dans la cellule qu'il en ait besoin ou non. Ce système ne permettait donc de fournir un service qu'à un nombre d'utilisateurs égal au nombre de bandes de fréquences disponibles. La première amélioration consista à allouer un canal à un utilisateur uniquement à partir du moment où celui-ci en avait besoin permettant ainsi d'augmenter "statistiquement" le nombre d'abonnés, étant entendu que tout le monde ne téléphone pas en même temps. Mais ce système nécessitait toujours des stations mobiles de puissance d'émission importante ($8 [W]$) et donc des appareils mobiles de taille et de poids conséquents. De plus, afin d'éviter les interférences, deux cellules adjacentes ne peuvent pas utiliser les mêmes fréquences. Cette organisation du réseau utilise donc le spectre fréquentiel d'une manière sous-optimale.

C'est pour résoudre ces différents problèmes qu'est apparu le concept de *cellule*. Le principe de ce système est de diviser le territoire en de petites zones, appelées *cellules*, et de partager les fréquences radio entre celles-ci. Ainsi, chaque cellule est constituée d'une station de base (reliée au Réseau Téléphonique Commuté, *RTC*) à laquelle on associe un certain nombre de canaux de fréquences à bande étroite, sommairement nommés *fréquences*. Comme précédemment, ces fréquences ne peuvent pas être utilisées dans les cellules adjacentes afin d'éviter les interférences⁴. Ainsi, on définit des *motifs*, aussi appelés *clusters*, constitués de plusieurs cellules, dans lesquels chaque fréquence est utilisée une seule fois. La figure 1 montre un tel motif, en guise d'exemple.

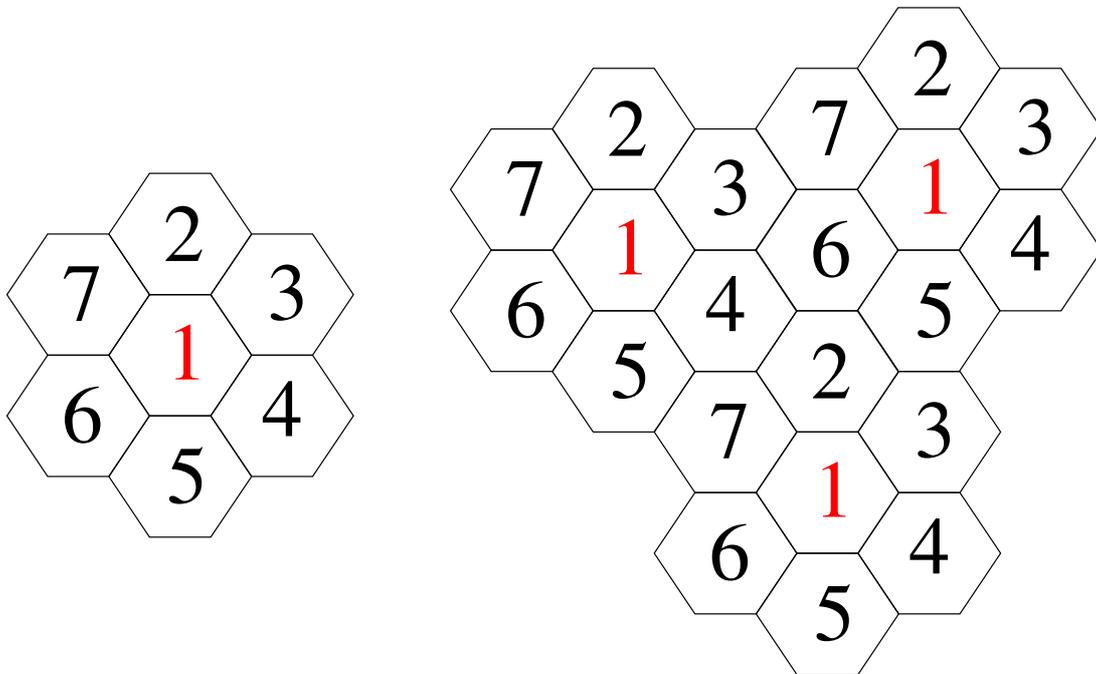


FIG. 1 – Figure représentant un motif élémentaire (à gauche) et un ensemble de motifs dans un réseau (à droite).

⁴En pratique, une distance minimale de deux cellules sépare deux cellules utilisant la même fréquence.

Graphiquement, on représente une cellule par un hexagone car cette forme approche celle d'un cercle. Cependant, en fonction de la nature du terrain et des constructions, les cellules n'ont pas une forme circulaire. De plus, afin de permettre à un utilisateur passant d'une cellule à une autre de garder sa communication, il est nécessaire que les zones de couverture se recouvrent de 10 à 15%, ce qui renforce la contrainte de ne pas avoir une même bande de fréquences dans deux cellules voisines.

Pour éviter les interférences à plus grande distance entre cellules utilisant les mêmes fréquences, il est également possible d'asservir la puissance d'émission de la station de base en fonction de la distance qui la sépare de l'utilisateur. Le même processus du contrôle de la puissance d'émission est également appliqué en sens inverse. En effet, pour diminuer la consommation d'énergie des mobiles et ainsi augmenter leur autonomie, leur puissance d'émission est calculée en fonction de leur distance à la station de base. Grâce à des mesures permanentes entre un téléphone mobile et une station de base, les puissances d'émission sont régulées en permanence pour garantir une qualité adéquate pour une puissance minimale.

En résumé, une cellule se caractérise :

- par sa *puissance d'émission nominale*⁵ –ce qui se traduit par une zone de couverture à l'intérieur de laquelle le niveau du champ électrique est supérieur à un seuil déterminé–,
- par la *fréquence de porteuse* utilisée pour l'émission radio-électrique et
- par le *réseau* auquel elle est interconnectée.

Il faut noter que la taille des cellules n'est pas la même sur tout le territoire. En effet, celle-ci dépend :

- du nombre d'utilisateurs potentiels dans la zone,
- de la configuration du terrain (relief géographique, présence d'immeubles, ...),
- de la nature des constructions (maisons, buildings, immeubles en béton, ...) et
- de la localisation (rurale, suburbaine ou urbaine) et donc de la densité des constructions.

Ainsi, dans une zone rurale où le nombre d'abonnés est faible et le terrain relativement plat, les cellules seront plus grandes qu'en ville où le nombre d'utilisateurs est très important sur une petite zone et où l'atténuation due aux bâtiments est forte. Un opérateur devra donc tenir compte des contraintes du relief topographique et des contraintes urbanistiques pour dimensionner les cellules de son réseau. On distingue pour cela quatre services principaux :

1. Le service "*Outdoor*" qui indique les conditions nécessaires pour le bon déroulement d'une communication en extérieur.
2. Le service "*Incar*" qui tient compte des utilisateurs se trouvant dans une voiture. On ajoute typiquement une marge supplémentaire de 6 **décibel** Watt, notée 6 [dB], dans le bilan de puissance pour en tenir compte.
3. Le service "*Indoor*" qui permet le bon déroulement des communications à l'intérieur des bâtiments. Cette catégorie de service se subdivise à son tour en deux :
 - (a) le "*Soft Indoor*" lorsque l'utilisateur se trouve juste derrière la façade d'un bâtiment et
 - (b) le "*Deep Indoor*" lorsqu'il se trouve plus à l'intérieur.

Typiquement, on considère que, lors de l'établissement du bilan de puissance, c'est-à-dire de l'analyse du rapport de la puissance émise à la puissance reçue au droit du récepteur, il faut tenir compte de 10 [dB] d'atténuation supplémentaire pour le *Soft Indoor* et de 20 [dB] pour *Deep Indoor* à 900 [MHz]. Quand on sait que 10 [dB] représente un facteur de 10 en puissance, on comprend qu'il est crucial pour un opérateur de dimensionner au mieux son réseau, quitte à effectuer des mesures sur le terrain.

2.1.1 Réutilisation des ressources

Par rapport au système de première génération, les cellules étant de taille plus petite, la puissance d'émission est plus faible et le nombre d'utilisateurs peut être augmenté pour une même zone géographique. C'est grâce au principe de réutilisation des fréquences qu'un opérateur peut augmenter la *capacité* de son réseau. En effet, il lui suffit de découper une cellule en plusieurs cellules plus petites et de gérer son plan de fréquences pour éviter toute interférence. Il y a ainsi toute une nomenclature spécifique pour classer les cellules en fonction de leur taille (macro, micro, pico, etc).

Définition 1 [Capacité] *La capacité est le trafic maximum que peut écouler une cellule en fonction du nombre de fréquences qui lui sont attribuées, le trafic étant fonction du nombre moyen de personnes qui communiquent et de la durée moyenne d'une communication.*

⁵Cette puissance est typiquement de l'ordre de la centaine de Watts.

2.1.2 Estimation du rapport de puissance porteuse à bruit

Étant donné que, dans un réseau, une même fréquence est réutilisée plusieurs fois, il est nécessaire d'évaluer la distance minimum qui doit séparer deux cellules utilisant la même fréquence pour qu'aucun phénomène perturbateur n'intervienne. En calculant le rapport entre la puissance de la porteuse et celle du bruit, il est possible d'estimer cette distance.

Pratiquement, dans une cellule, un mobile reçoit à la fois le message utile (dont la puissance vaut C) qui lui est destiné et un certain nombre de signaux perturbateurs. La connaissance du rapport entre ces puissances, nous permettra de connaître la qualité de la communication.

Pour commencer, il est nécessaire d'identifier les différents signaux perturbateurs. On peut les subdiviser en deux classes :

1. Les interférences de puissance totale I qui sont dues aux signaux émis par les autres stations. On peut distinguer :
 - (a) Les interférences *co-canal* qui sont dues aux signaux émis par les autres stations de base utilisant la même fréquence.
 - (b) Les interférences de canaux adjacents dues aux signaux émis par les stations de base utilisant des fréquences voisines.
2. Le bruit, de puissance N , provenant principalement du bruit de fond du récepteur.

Dès lors, c'est le rapport

$$\frac{C}{N + I} \quad (1)$$

qui permet d'évaluer la qualité de la communication ainsi que la distance de réutilisation des fréquences.

2.2 Synthèse des principales caractéristiques du GSM

La norme **GSM** prévoit que la téléphonie mobile par GSM occupe deux bandes de fréquences aux alentours des 900 [MHz] :

1. la bande de fréquence 890 – 915 [MHz] pour les communications montantes (du mobile vers la station de base) et
2. la bande de fréquence 935 – 960 [MHz] pour les communications descendantes (de la station de base vers le mobile).

Comme chaque canal fréquentiel utilisé pour une communication a une largeur de bande de 200 [kHz], cela laisse la place pour 124 canaux fréquentiels à répartir entre les différents opérateurs. Mais, le nombre d'utilisateurs augmentant, il s'est avéré nécessaire d'attribuer une bande supplémentaire aux alentours des 1800 [MHz]. On a donc porté la technologie GSM 900 [MHz] vers une bande ouverte à plus haute fréquence. C'est le système **DCS-1800** (*Digital Communication System*) dont les caractéristiques sont quasi identiques au GSM en termes de protocoles et de service. Les communications montantes se faisant alors entre 1710 et 1785 [MHz] et les communications descendantes entre 1805 et 1880 [MHz].

Connaissant les différents canaux disponibles, il est alors possible d'effectuer un multiplexage fréquentiel, appelé *Frequency Division Multiple Access* (**FDMA**), en attribuant un certain nombre de fréquences porteuses par station de base. Un opérateur ne dédie pas pour autant une bande de fréquences par utilisateur, car cela conduirait à un gaspillage de ressources radio étant donné qu'un utilisateur émet par intermittence. De plus, avec un tel système, si une source parasite émet un bruit à une fréquence bien déterminée, le signal qui se trouve dans la bande de fréquence contenant le parasite sera perturbé. Pour résoudre ces problèmes, on combine le multiplexage en fréquence à un multiplexage temporel (appelé *Time Division Multiple Access* ou **TDMA**) consistant à diviser chaque canal de communication en trames de 8 intervalles de temps (dans le cas du GSM). Pour être complet, signalons qu'il existe encore une autre technique de multiplexage appelé *Code Division Multiple Access* (**CDMA**), utilisée dans la norme américaine **IS-95** ou promue pour l'**UMTS**.

Ainsi, avec le TDMA, il est par exemple possible de faire parler huit utilisateurs l'un après l'autre dans le même canal. On multiplie donc le nombre de canaux disponibles par unité de temps par huit.

Le tableau 1 montre les caractéristiques des réseaux à technologie GSM et il compare les normes.

Tous les terminaux mobiles fabriqués actuellement sont compatibles avec les 2 normes ; ces terminaux sont appelés *bi-bandes* ou *dual-band*. Sur le territoire des États-Unis, aucune des bandes de fréquences pré-citées n'étaient encore disponibles. C'est pourquoi le réseau à technologie GSM américain utilise des bandes autour des 1900 [MHz]. Des terminaux capables d'opérer dans les trois bandes sont appelés *tri-bandes*.

3 Architecture du réseau

L'architecture d'un réseau GSM peut être divisée en *trois* sous-systèmes :

1. Le sous-système radio contenant la station mobile, la station de base et son contrôleur.
2. Le sous-système réseau ou d'acheminement.
3. Le sous-système opérationnel ou d'exploitation et de maintenance.

Les éléments de l'architecture d'un réseau GSM sont repris sur le schéma de la figure 2.

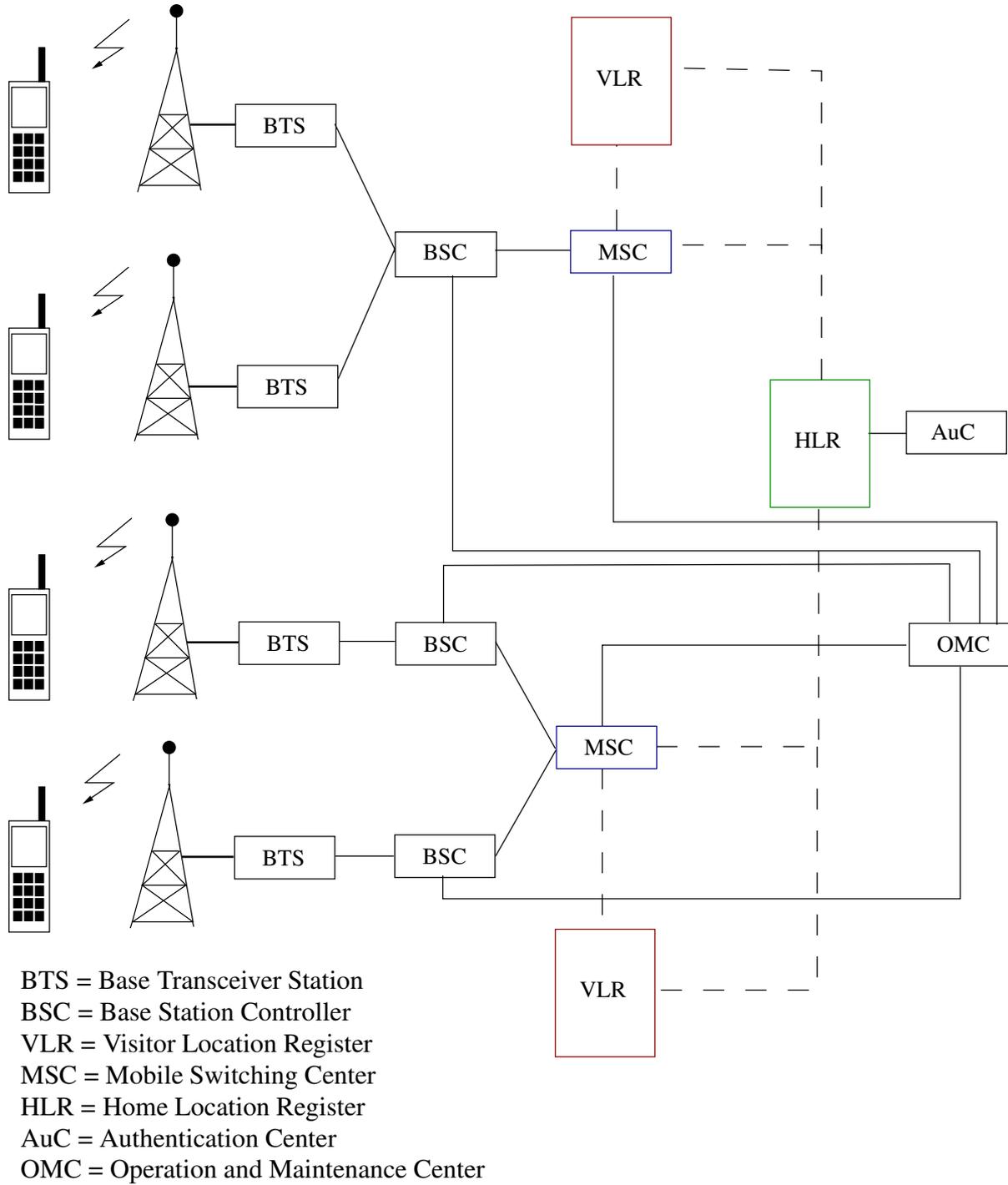


FIG. 2 – Architecture du réseau GSM.

	GSM	DCS-1800
Bande de fréquences (↑)	890,2 – 915 [MHz]	1710 – 1785 [MHz]
Bande de fréquences (↓)	935,2 – 960 [MHz]	1805 – 1880 [MHz]
Nombre d'intervalles de temps par trame TDMA	8	8
Débit total par canal	271 [kb/s]	271 [kb/s]
Débit de la parole	13 [kb/s]	13 [kb/s]
Débit maximal de données	12 [kb/s]	12 [kb/s]
Technique de multiplexage	Multiplexage fréquentiel et temporel	Multiplexage fréquentiel et temporel
Rayon de cellules	0,3 à 30 [km]	0,1 à 4 [km]
Puissance des terminaux	2 à 8 [W]	0,25 et 1 [W]
Sensibilité des terminaux	–102 [dB]	
Sensibilité de la station de base	–104 [dB]	

TAB. 1 – Comparaison des systèmes GSM et DCS-1800.

3.1 Le sous-système radio

Le sous-système radio gère la transmission radio. Il est constitué de plusieurs entités dont le *mobile*, la *station de base* (**BTS**, *Base Transceiver Station*) et un *contrôleur de station de base* (**BSC**, *Base Station Controller*).

3.1.1 Le mobile

Le téléphone et la carte **SIM** (*Subscriber Identity Module*) sont les deux seuls éléments auxquels un utilisateur a directement accès. Ces deux éléments suffisent à réaliser l'ensemble des fonctionnalités nécessaires à la transmission et à la gestion des déplacements.

La principale fonction de la carte SIM est de contenir et de gérer une série d'informations. Elle se comporte donc comme une mini-base de données dont les principaux champs sont fournis dans le tableau 2.

Paramètres	Commentaires
<i>Données administratives</i>	
PIN /PIN2	Mot de passe demandé à chaque connexion
PUK /PUK2	Code pour débloquer une carte
Language	Langue choisie par l'utilisateur
<i>Données liées à la sécurité</i>	
Clé K_i	Valeur unique, connue de la seule carte SIM et du HLR
CKSN	Séquence de chiffrement
<i>Données relatives à l'utilisateur</i>	
IMSI	Numéro international de l'abonné
MSISDN	Numéro d'appel d'un téléphone GSM
<i>Données de "roaming"</i>	
TMSI	Numéro attribué temporairement par le réseau à un abonné
Location updating status	Indique si une mise à jour de la localisation est nécessaire
<i>Données relatives au réseau</i>	
Mobile Country Code (MCC), Mobile Network Code (MNC), etc	Identifiants du réseau mobile de l'abonné
Numéros de fréquence absolus	Fréquences utilisées par le PLMN

TAB. 2 – Liste partielle des informations contenues dans une carte SIM (voir [1, page 13] pour la liste complète).

L'identification d'un mobile s'effectue exclusivement au moyen de la carte SIM. En effet, elle contient des données spécifiques comme le code **PIN** (*Personal Identification Number*) et d'autres caractéristiques de l'abonné, de l'environnement radio et de l'environnement de l'utilisateur.

L'identification d'un utilisateur est réalisée par un numéro unique (**IMSI**, *International Mobile Subscriber Identity*) différent du numéro de téléphone connu de l'utilisateur (**MSISDN**, *Mobile Station ISDN Number*), tous deux étant incrustés dans la carte SIM.

3.1.2 La station de base (BTS)

La station de base est l'élément central, que l'on pourrait définir comme un ensemble émetteur/récepteur pilotant une ou plusieurs cellules. Dans le réseau GSM, chaque cellule principale au centre de laquelle se situe une station base peut-être divisée, grâce à des antennes directionnelles, en plus petites cellules qui sont des portions de celle de départ et qui utilisent des fréquences porteuses différentes. En Belgique, il est fréquent d'avoir des antennes tri-sectorielles, qui couvrent un peu plus de 120 degrés. Ces antennes ont l'allure de paires de segments verticaux, disposées en triangle (cf. figure 3).

C'est la station de base qui fait le relais entre le mobile et le sous-système réseau. Comme le multiplexage temporel est limité à 8 intervalles de temps, une station de base peut gérer tout au plus huit connections simultanées par cellule. Elle réalise les fonctions de la couche physique et de la couche liaison de données.

En cas de besoin, on peut exploiter une station de base localement ou par télécommande à travers son contrôleur de station de base.

3.1.3 Le contrôleur de station de base (BSC)

Le contrôleur de station de base gère une ou plusieurs stations de base et communique avec elles par le biais de l'interface A-bis. Ce contrôleur remplit différentes fonctions tant au niveau de la communication qu'au niveau de l'exploitation.

Pour les fonctions des communications des signaux en provenance des stations de base, le BSC agit comme un **concentrateur** puisqu'il transfère les communications provenant des différentes stations de base vers une sortie unique. Dans l'autre sens, le contrôleur commute les données en les dirigeant vers la bonne station de base.

Dans le même temps, le BSC remplit le rôle de relais pour les différents signaux d'alarme destinés au centre d'exploitation et de maintenance. Il alimente aussi la base de données des stations de base. Enfin, une dernière fonctionnalité importante est la gestion des ressources radio pour la zone couverte par les différentes stations de base qui y sont connectées. En effet, le contrôleur gère les transferts inter-cellulaires des utilisateurs dans sa zone de couverture, c'est-à-dire quand une station mobile passe d'une cellule dans une autre. Il doit alors communiquer avec la station de base qui va prendre en charge l'abonné et lui communiquer les informations nécessaires tout en avertissant la base de données locale **VLR** (*Visitor Location Register*) de la nouvelle localisation de l'abonné.

C'est donc un maillon très important de la chaîne de communication et il est, de plus, le seul équipement de ce sous-système à être directement gérable (via l'interface **X25** qui le relie au sous-système d'exploitation et de maintenance).

3.2 Le sous-système réseau

Le sous-système réseau, appelé *Network Switching Center* (**NSS**), joue un rôle essentiel dans un réseau mobile. Alors que le sous-réseau radio gère l'accès radio, les éléments du *NSS* prennent en charge toutes les fonctions de contrôle et d'analyse d'informations contenues dans des bases de données nécessaires à l'établissement de connexions utilisant une ou plusieurs des fonctions suivantes : **chiffrement**, **authentification** ou **roaming**.

Le *NSS* est constitué de :

- *Mobile Switching Center* (**MSC**)
- *Home Location Register* (**HLR**) / *Authentication Center* (**AuC**)
- *Visitor Location Register* (**VLR**)
- *Equipment Identity Register* (**EIR**)

3.2.1 Le centre de commutation mobile (MSC)

Le centre de commutation mobile est relié au sous-système radio via l'interface A. Son rôle principal est d'assurer la commutation entre les abonnés du réseau mobile et ceux du réseau commuté public (RTC) ou de son équivalent numérique, le réseau **RNIS** (**ISDN** en anglais). D'un point de vue fonctionnel, il est semblable à un commutateur de réseau ISDN, mis à part quelques modifications nécessaires pour un réseau mobile.

De plus, il participe à la fourniture des différents services aux abonnés tels que la téléphonie, les services supplémentaires et les services de messagerie. Il permet encore de mettre à jour les différentes bases de données (HLR et VLR) qui donnent toutes les informations concernant les abonnés et leur localisation dans le réseau.

Les commutateurs MSC d'un opérateur sont reliés entre eux pour la commutation interne des informations. Des MSC servant de passerelle (*Gateway Mobile Switching Center*, **GMSC**) sont placées en périphérie du réseau d'un opérateur de manière à assurer une inter-opérabilité entre réseaux d'opérateurs.



FIG. 3 – Exemple d'antennes GSM (ROCKHAMPTON, QUEENSLAND, AUSTRALIE).

3.2.2 L'enregistreur de localisation nominale (HLR)

Il existe au moins un enregistreur de localisation (HLR) par réseau (PLMN). Il s'agit d'une base de données avec des informations essentielles pour les services de téléphonie mobile et avec un accès rapide de manière à garantir un temps d'établissement de connexion aussi court que possible.

Le HLR contient :

- toutes les informations relatives aux abonnés : le type d'abonnement, la clé d'authentification K_i –cette clé est connue d'un seul HLR et d'une seule carte SIM–, les services souscrits, le numéro de l'abonné (**IMSI**), etc
- ainsi qu'un certain nombre de données dynamiques telles que la position de l'abonné dans le réseau –en fait, son **VLR**– et l'état de son terminal (allumé, éteint, en communication, libre, ...).

Les données dynamiques sont mises à jour par le MSC. Cette base de données est souvent unique pour un réseau GSM et seules quelques personnes y ont accès directement.

Le centre d'authentification (AuC). Lorsqu'un abonné passe une communication, l'opérateur doit pouvoir s'assurer qu'il ne s'agit pas d'un usurpateur. Le centre d'authentification remplit cette fonction de protection des communications. Pour ce faire, les normes GSM prévoient deux mécanismes :

1. Le chiffrement des transmissions radio. Remarquons qu'il s'agit d'un chiffrement faible, qui ne résiste pas longtemps à la crypto-analyse ! Ceci explique sans doute pourquoi, en Belgique, de nombreux toits de bâtiments de puissance étrangère sont équipés d'antennes servant exclusivement à la réception de signaux GSM...
2. L'authentification des utilisateurs du réseau au moyen d'une clé K_i , qui est à la fois présente dans la station mobile et dans le centre d'authentification.

L'authentification s'effectue par résolution d'un défi sur base d'un nombre M généré aléatoirement et envoyé au mobile. À partir de ce nombre, un algorithme identique (algorithme A_3) qui se trouve à la fois dans la carte SIM et dans l'AuC produit un résultat sur base de la clé K_i et du nombre M .

Dès lors, lorsqu'un VLR obtient l'identifiant d'un abonné, il demande, au HLR du réseau de l'abonné, le nombre M servant au défi et le résultat du calcul afin de le comparer à celui qui sera produit et envoyé par le mobile. Si les résultats concordent, l'utilisateur est reconnu et accepté par le réseau.

Grâce à ce mécanisme d'authentification, un VLR peut accueillir un mobile appartenant à un autre réseau (moyennant un accord préalable entre opérateurs de réseau !) sans qu'il ne soit nécessaire de divulguer la clé de chiffrement du mobile.

On peut dès lors distinguer trois niveaux de protection :

1. La carte SIM qui interdit à un utilisateur non enregistré d'avoir accès au réseau.
2. Le chiffrement des communications destiné à empêcher l'écoute de celles-ci.
3. La protection de l'identité de l'abonné.

3.2.3 L'enregistreur de localisation des visiteurs (VLR)

Cette base de données ne contient que des informations dynamiques et est liée à un MSC. Il y en a donc plusieurs dans un réseau GSM. Elle contient des données dynamiques qui lui sont transmises par le HLR avec lequel elle communique lorsqu'un abonné entre dans la zone de couverture du centre de commutation mobile auquel elle est rattaché. Lorsque l'abonné quitte cette zone de couverture, ses données sont transmises à un autre VLR ; les données suivent l'abonné en quelque sorte.

3.2.4 L'enregistreur des identités des équipements (EIR)

Malgré les mécanismes introduits pour sécuriser l'accès au réseau et le contenu des communications, le téléphone mobile doit potentiellement pouvoir accueillir n'importe quelle carte SIM de n'importe quel réseau. Il est donc imaginable qu'un terminal puisse être utilisé par un voleur sans qu'il ne puisse être repéré.

Pour combattre ce risque, chaque terminal reçoit un identifiant unique (*International Mobile Station Equipment Identity*, **IMEI**) qui ne peut pas être modifié sans altérer le terminal. En fonction de données au sujet d'un terminal, un opérateur peut décider de refuser l'accès au réseau. Tous les opérateurs n'implémentent pas une telle base de données.

3.3 Le centre d'exploitation et de maintenance

Cette partie du réseau regroupe trois activités principales de gestion : la gestion administrative, la gestion commerciale et la gestion technique.

Le réseau de maintenance technique s'intéresse au fonctionnement des éléments du réseau. Il gère notamment les alarmes, les pannes, la sécurité, ... Ce réseau s'appuie sur un réseau de transfert de données, totalement dissocié du réseau de communication GSM.

3.4 L'acheminement des appels entre le réseau fixe et le réseau GSM : deux scénarios en guise d'exemple

Illustrons brièvement le fonctionnement des entités d'un réseau en traitant deux scénarios typiques simplifiés entre un réseau mobile et un réseau fixe :

1. *Un abonné GSM compose le numéro de téléphone d'un abonné du réseau fixe.*

Sa demande arrive d'abord au BTS de la cellule puis passe à travers le BSC et arrive enfin au MSC qui vérifie les droits de l'abonné (autorisation d'accéder à ce service, état de l'abonnement, ...). Si l'abonné remplit les conditions, le MSC transmet l'appel au réseau public et demande au BSC de réserver un canal pour la communication. Il ne reste alors plus qu'à attendre que le poste fixe soit décroché pour que la communication soit établie.

2. *Supposons au contraire qu'un abonné du réseau fixe veuille joindre un abonné du réseau GSM.*

Le fonctionnement est un peu plus complexe car l'opérateur GSM n'alloue des ressources à un abonné que lorsque celui reçoit ou émet un appel.

Le numéro composé sur le poste fixe est tout d'abord aiguillé vers le réseau de l'abonné GSM. La demande de connexion est interprétée par un commutateur passerelle entrant du réseau GSM –il s'agit d'un GMSC. Le numéro formé par l'abonné du réseau fixe n'est pas utilisé tel quel pour commuter la communication. À l'instar des numéros verts ou des numéros d'urgence, il y a un mécanisme qui, au droit du GMSC, va convertir le numéro de l'abonné en un autre numéro attribué dynamiquement en fonction de la position de l'utilisateur. C'est sur base de ce numéro dynamique que l'appel sera re-dirigé dans le réseau GSM. Concrètement, le HLR est interrogé afin de connaître la position de l'utilisateur du réseau mobile ainsi que son état (libre, occupé, éteint). Si le mobile est dans l'état "libre", le réseau interroge alors le VLR de la zone pour savoir dans quelle cellule le mobile se situe. Ainsi, le BSC de la zone demande aux différentes stations de base de sa zone de diffuser un avis d'appel. Comme le mobile est "libre", le destinataire écoute le réseau et s'aperçoit qu'on tente de le joindre et la sonnerie du terminal est activée. Une fois que l'utilisateur a décroché, un canal de communication est alloué à l'appel et les bases de données VLR et HLR sont mises à jour.

4 Description du canal physique

Dans un réseau GSM, deux techniques de multiplexage sont mises en œuvre : le multiplexage *fréquentiel* (FDMA) et le multiplexage *temporel* (TDMA).

4.1 Multiplexage fréquentiel

Dans sa version à 900 [MHz], la norme GSM occupe deux bandes de 25 [MHz]; l'une est utilisée pour la voie montante (890,2 – 915 [MHz]), l'autre pour la voie descendante (935,2 – 960 [MHz]). Il est également défini que chaque porteuse de cellule possède une densité spectrale confinée dans une bande de 200 [kHz] ce qui signifie que, théoriquement, on peut disposer de 124 canaux. Notons au passage que la bande de fréquences du DCS-1800 étant plus large, elle peut contenir 374 canaux.

Aussi, si on indique par F_u les fréquences porteuses montantes et par F_d les fréquences porteuses descendantes, les valeurs de fréquence porteuse valent

$$F_u(n) = 890,2 + 0,2 \times (n - 1) \text{ [MHz]} \quad (2)$$

$$F_d(n) = 935,2 + 0,2 \times (n - 1) \text{ [MHz]} \quad (3)$$

où $1 \leq n \leq 124$. Connaissant les canaux disponibles, il est alors possible d'effectuer un multiplexage fréquentiel en attribuant un certain ensemble de fréquences porteuses par opérateur GSM –c'est le rôle du régulateur, l'IBPT⁶ en Belgique– et l'opérateur choisit son plan de fréquences en allouant une ou plusieurs fréquences par station de base. Proximus utilise les canaux 1 à 30 et 61 à 90, Mobistar s'est vu attribuer les canaux 31 à 60 et 91 à 120; quant aux canaux restants (121 à 124), ils ont été réservés pour les téléphones sans fil. Base (nommé Orange auparavant) n'opère pas dans la bande des 900 [MHz]. Par contre, la bande DCS-1800 est utilisée par les 3 opérateurs (Base, Mobistar et Proximus).

⁶<http://www.ibpt.be>

4.2 La modulation

En raison de la forte variabilité de l'amplitude des signaux dans un environnement mobile, on préfère recourir à un technique de modulation angulaire pour ce type d'environnement. La technique de modulation utilisée pour porter le signal à haute fréquence est la modulation **GMSK** (*Gaussian Minimum Shift Keying*). Comme le suggère son nom, il s'agit d'une variante d'une modulation **MSK** appartenant à la famille des modulations de fréquence (**FM**) numériques. On utilise la **GMSK** car, en raison de la transition rapide entre 2 fréquences ($f_c - \Delta f$ et $f_c + \Delta f$), la modulation par **MSK** aurait nécessité une trop large bande de fréquences.

La modulation **GMSK** consiste en une modulation de fréquence à deux états portant non pas sur la séquence originale mais sur une nouvelle séquence dont le bit n est produit comme le résultat de la fonction du OU exclusif (**XOR**) entre le bit courant et le bit précédent. Après application du XOR, le signal est filtré. La figure 4 montre la création d'un signal modulé par **GMSK**.

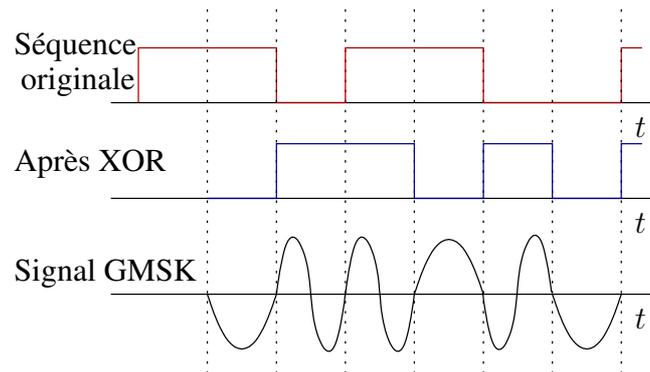


FIG. 4 – Création d'un signal modulé par **GMSK** au départ d'un train binaire.

Au bout du compte, il faut une largeur de $200 [kHz]$ par fréquence porteuse. Sachant que le débit atteint $270 [kb/s]$, on atteint un rapport du débit à largeur de bande, appelé *efficacité spectrale*, proche de 1. Cette valeur est typique pour des environnements mobiles, ce qui signifie que, pour doubler le débit, il n'y a d'autre solution que de doubler la largeur de bande.

4.3 Multiplexage temporel

Tant pour des questions d'interférences électromagnétiques que pour des raisons d'augmentation de capacité, le multiplexage fréquentiel se double d'un multiplexage temporel. Le multiplexage temporel consiste à diviser chaque canal de communication en 8 intervalles de temps de $0,577 [ms]$ chacun.

Définition 2 [Trame] On définit dès lors une *trame* élémentaire de 8 intervalles pour une durée de $8 \times 0,577 = 4,615 [ms]$.

Comme il est exclu de transmettre toutes les informations en une fois, il faut découper l'information et la transmettre au moyen de plusieurs trames consécutives. La norme **GSM** prévoit une organisation spécifique de structure hiérarchique de trames. Cette hiérarchie est dessinée à la figure 5. Les trames sont regroupées comme suit :

- 1 *multitrame* de type 26 = 26 trames TDMA élémentaires et 1 *multitrame* de type 51 = 51 trames TDMA élémentaires,
- 1 *supertrame* de type 26 = 26 multitrames et 1 *supertrame* de type 51 = 51 multitrames
- 1 *hyperttrame* = 2048 supertrames = 2.715.648 trames.

La structure en trames est à mettre en relation avec la typologie des informations véhiculées, dont il est question dans cet article à la section 5.3.

4.4 Mécanismes de protection contre les interférences radio-électriques

Le canal d'une communication avec un mobile est changeant et sujet à perturbations. Plusieurs mécanismes sont donc mis en œuvre pour réduire l'impact des interférences.

4.4.1 Le saut de fréquences ou Frequency Hopping

Pour protéger les canaux d'une source radio parasite, la fréquence porteuse utilisée pour transmettre une salve de données fluctue au cours du temps. C'est le principe du saut de fréquence ou du *Frequency Hopping* (**FH**) ; il est illustré à la figure 6.

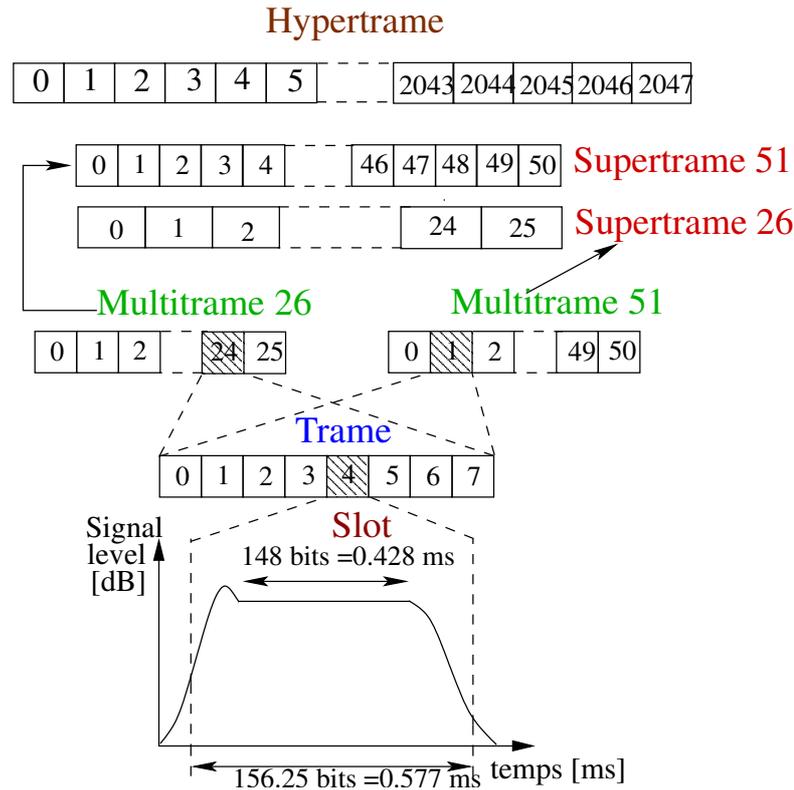


FIG. 5 – Organisation des multiples de trames.

Ainsi, si à un moment déterminé, une bande de fréquences est sujette à fortes perturbations, seule une petite quantité de données sera perturbée.

La norme GSM définit un parcours de fréquence cyclique ou pseudo-aléatoire, comprenant au plus 64 fréquences porteuses. Habituellement, un algorithme standardisé génère une suite pseudo-aléatoire de nombres s_i compris dans une liste de N fréquences disponibles pour les sauts.

La configuration des sauts se fait au moyen de paramètres tels que :

- le *Cell Allocation (CA)*, la liste des numéros des fréquences utilisées dans une cellule,
- le *Mobile Allocation (MA)*, la liste des numéros des fréquences disponibles pour les sauts⁷,
- le *Hopping Sequence Number (HSN)*, une valeur comprise entre 0 et 63, servant à initialiser le générateur pseudo-aléatoire, et
- le *Mobile Allocation Index Offset (MAIO)*, une valeur comprise entre 0 et 63 qui indique quel décalage doit être utilisé.

Cette valeur de décalage est convenue à l'initialisation de l'appel et elle diffère d'un mobile à l'autre.

L'opérateur choisit le nombre de fréquences à prendre pour chaque numéro de trame élémentaire (appelée *slot*). Néanmoins, il doit tenir compte de la nécessité d'un mobile entrant dans le réseau de pouvoir communiquer. Pour cela, on fixe la fréquence porteuse de certains *slots* dans le sens de la station de base vers le mobile. Ce canal a pour fonction essentielle de permettre au mobile de se rattacher à la station de base la plus favorable. Il s'agit par exemple du *slot* 0 pour lequel on fixe une fréquence et on n'autorise le saut que sur 3 fréquences (pour les appels en cours sur le *slot* 0) au lieu de 4 pour les autres *slots*.

Signalons qu'il n'est pas possible de passer de la bande 900 [MHz] à la bande 1800 [MHz] pour effectuer le saut de fréquence. Autrement dit, les ressources radio des bandes GSM et DCS-1800 ne sont jamais mélangées.

4.4.2 Décalage temporel des envois

Pour permettre le basculement d'un mobile du mode réception en mode émission, la norme GSM prévoit un décalage de 3 slots. Plus précisément, le mobile émet des informations 3 slots après réception des signaux envoyés par la station de base.

Malgré tout, les informations envoyées par les différents mobiles autour d'une même fréquence porteuse entre en collision au droit de la station de base si la distance entre les mobiles et l'antenne est fort différente d'un mobile à l'autre. Pour éviter des collisions, certains mobiles (les plus distants) doivent avancer le moment de l'envoi. La durée de l'avance temporelle de l'envoi est appelée *Timing Advance (TA)*. Elle est fournie dynamiquement par la station de base.

⁷Il y en a au maximum 64.

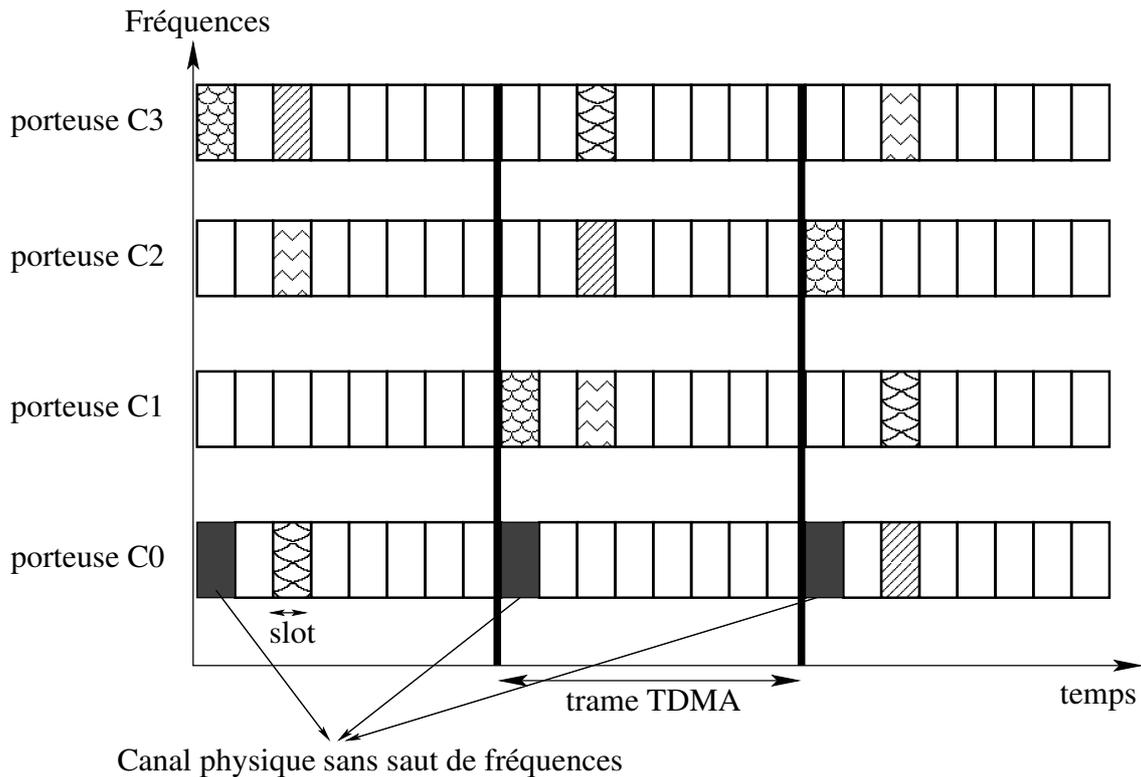


FIG. 6 – Principe du saut de fréquence (d'après [2, page 169]).

4.4.3 Le codage

Pour protéger les informations des erreurs qui peuvent se produire lors des communications radio et ainsi réduire le taux d'erreur sur bit, trois techniques de codage sont appliqués :

1. Un *codage en bloc* qui ajoute un bit de parité au bloc et qui permet la détection d'un nombre impair d'erreurs.
2. Un *codage récurrent* (algorithme de VITERBI). L'information n'est plus sectionnée en parties indépendantes mais certains bits de redondance sont placés régulièrement dans le code.
3. On effectue également un entrelacement par blocs de 464 bits. Cet entrelacement consiste à répartir les blocs selon une méthode définie. Ainsi, si le canal perturbe une suite de bits consécutifs, l'altération sera diffusée sur un grand nombre de blocs plutôt que sur la totalité d'un bloc ; les blocs affectés pourront alors être corrigés grâce aux bits redondants.

5 Protocoles

5.1 Pile de protocoles

La figure 7 représente l'architecture des protocoles GSM des différents éléments du réseau. Au niveau applicatif, on distingue les protocoles suivants qui, au travers de différents éléments du réseau, relient un mobile à un centre de communication (MSC) :

1. Le protocole *Call Control* (CC) prend en charge le traitement des appels tels que l'établissement, la terminaison et la supervision.
2. Le protocole *Short Message Service* (SMS) qui permet l'envoi de courts messages au départ d'un mobile. La longueur d'un SMS est limité à 160 caractères de 7 bits, soit 140 bytes.
3. Le protocole *Supplementary Services* (SS) prend en charge les compléments de services. La liste de ces services est longue mais, à titre d'exemple, citons le *Calling Line Identification Presentation* (CLIP), le *Calling Line Identification Restriction* (CLIR) et le *Call Forwarding Unconditional* (CFU).
4. Le protocole *Mobility Management* (MM) gère l'identification, l'authentification sur le réseau et la localisation d'un terminal. Cette application se trouve dans le sous-réseau de commutation (NSS) et dans le mobile car ils doivent tous deux connaître la position du mobile dans le réseau.

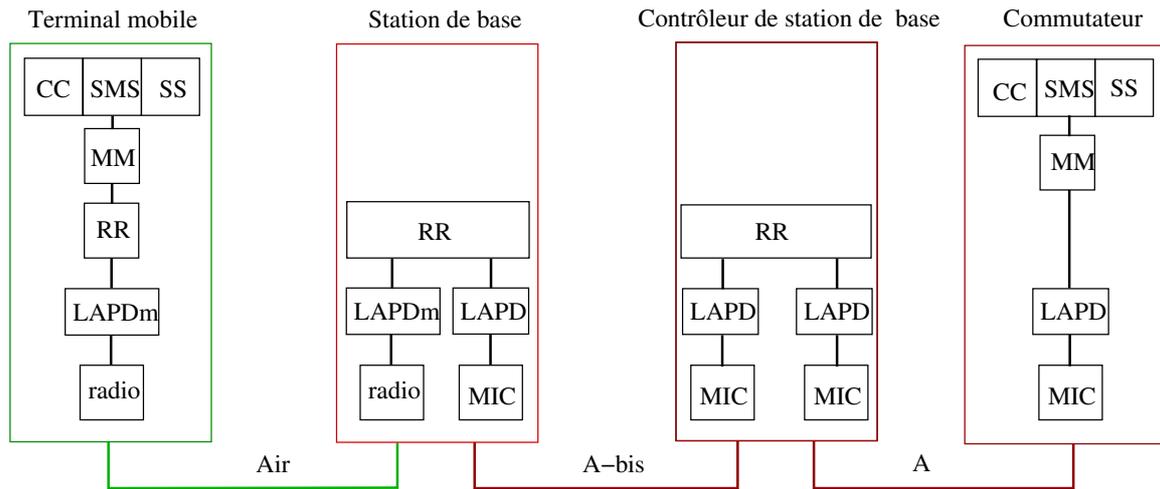


FIG. 7 – Piles de protocoles de différents sous-systèmes du réseau GSM (d’après [3, page 58]).

- Le protocole *Radio Ressource management* (RR) s’occupe de la liaison radio. Il interconnecte une BTS et un BSC car ce dernier gère l’attribution des fréquences radio dans une zone.

Les trois premiers protocoles applicatifs pré-cités (CC, SMS et SS) ne sont implémentés que dans les terminaux mobiles et les commutateurs ; leurs messages voyagent de façon transparente à travers le BSC et le BTS.

5.2 Les interfaces A-bis, A et X25

Présentons brièvement les trois types d’interface qui relient le BSC respectivement à la station de base (interface A-bis), au commutateur (interface A) et au centre d’exploitation et de maintenance (interface X25).

5.2.1 L’interface A-bis

La couche physique est définie par une liaison PCM à $2 [Mb/s]$ ⁸ (recommandation de la série G de l’ITU) et la couche liaison de données est composée du protocole *Link Access Protocol D-channel* (LAPD).

Comme le canal de liaison PCM a un débit unitaire de $64 [kb/s]$ et que le débit par canal radio GSM est de $13 [kb/s]$, il faut donc adapter le débit. Cette fonction est appelée *transcodage* et elle est réalisé dans une unité appelée *Transcoding Rate and Adaptation Unit* (TRAU). Deux solutions sont techniquement possibles et rencontrées dans les réseaux GSM :

- Mutliplexer quatre canaux à $13 [kb/s]$ pour produire un canal à $64 [kb/s]$.
- Faire passer le débit de chaque canal à $64 [kb/s]$.

Tout est affaire de compromis et de choix. L’avantage de la première solution est de diminuer le débit entre la station de base et le BSC où le trafic est fortement concentré. La seconde solution offre par contre l’avantage de banaliser les équipements du système en ramenant tous les équipements à $64 [kb/s]$. Souvent, la deuxième solution est utilisée au niveau des commutateurs et la première au niveau du BSC afin de garder l’avantage du faible débit de parole.

5.2.2 L’interface A

La couche physique est toujours définie par une liaison à PCM à $2 [Mb/s]$ mais c’est le protocole CCITT numéro 7 qui est utilisé pour la couche liaison de données.

5.2.3 L’interface X25

Cette interface relie le BSC au centre d’exploitation et de maintenance (OMC). Elle possède la structure en 7 couches du modèle OSI.

⁸Une telle liaison offre 32 canaux à $64 [kb/s]$.

5.3 Typologie des paquets

Chaque trame consiste en un certain nombre de bits. Ces bits sont organisés suivant une structure qui diffère en fonction du protocole applicatif mis en œuvre pour chaque slot mais aussi de l'état intermédiaire du protocole considéré.

La durée d'un paquet (0,577 [ms]) correspond à l'émission de 156,25 bits, dont 114 bits de message "net". En admettant que les slots se suivent sans interruption, un simple calcul ($\frac{156,25}{0,577 \times 10^{-3}}$) montre que le débit maximum vaut 270 [kb/s]. En pratique, le débit maximum utile (en mode *full-rate*) ne dépasse pas 13 [kb/s] en raison des bits nécessaires à la correction d'erreurs. Pour la transmission des données, cette limite descend même à 9,6 [kb/s] en raison de la sur-protection nécessaire à la garantie d'un taux d'erreur acceptable.

La norme définit 5 types de paquets fonctionnels, appelés *bursts* dans la terminologie GSM :

1. Les *bursts d'accès* qui sont envoyés par les mobiles lorsqu'ils veulent entrer en contact avec le réseau.
2. Les *bursts de synchronisation* qui contiennent les informations sur la localisation et les fréquences utilisées.
3. Les *bursts normaux* qui transportent les messages.
4. Les *bursts de correction de fréquence*.
5. Les *bursts de bourrage (dummy packet)* qui sont placés dans les espaces vides si aucune donnée ne doit être envoyée. Pour être précis, ce burst est composé de 2 salves de 58 bits préfixés interrompus par une séquence d'entraînement de 26 bits.

Tous les types de *burst* ont une forme semblable. Ils sont composés, dans l'ordre, de :

- bits d'en-tête (*tail bit*, *TB*), nécessaires à la synchronisation. Ils correspondent toujours au code 000 sauf pour les *bursts d'accès*.
- 148 bits utiles dont le format dépend du type de *burst*.
- bits de fin, aussi appelés *tail bit*, terminés par une période temporelle de garde requise pour permettre à l'émetteur de réduire sa puissance de 70 [dB]. Elle sert aussi à compenser la durée de transmission qui est variable pour la réception d'un paquet au suivant si le mobile a bougé.

La structure des 5 types de *burst* est représentée à la figure 8.

5.3.1 Le burst d'accès

Ce burst est émis, sur un canal dédié, par la station mobile lorsqu'elle cherche à entrer en contact avec le réseau soit pour l'établissement d'une communication, soit pour un *handover*. Il est le plus court des quatre types car il ne contient que 77 bits (41 bits de synchronisation et 36 bits d'information). Son temps de garde est de 68,25 bits, soit 0,252 [ms]. Ce temps de garde permet de tenir compte de grandes cellules et d'établir ainsi une communication avec un mobile distant jusqu'à 35 [km].

En calculant la durée de voyage d'un burst, la station peut asservir l'instant du début d'émission pour compenser le retard entraîné par la propagation des ondes. En effet, l'horloge interne des récepteurs est synchronisée grâce à un top de synchronisation envoyé par la station de base.

5.3.2 Le burst de synchronisation

Pour ce type de burst, 78 bits d'informations sont véhiculés pour les stations mobiles. Ces bits contiennent les renseignements concernant les fréquences à utiliser et la localisation (identité de la station de base, de la zone et de la cellule).

5.3.3 Le burst normal

Ce burst transporte $2 \times 57 = 114$ bits d'information séparées par 26 bits qui sont une séquence d'apprentissage destinée à régler les paramètres de réception. De plus, la zone TB correspond à 8,25 bits. Enfin, il faut ajouter à cela 2 bits qui indiquent s'il s'agit d'un canal de données ou d'un canal de signalisation et 6 bits pour marquer la montée ou la descente en amplitude.

5.3.4 Le burst de correction de fréquence

Le type de burst au format le plus simple. La station de base envoie 142 bits de données servant à prévenir des interférences possibles avec des fréquences voisines.

5.3.5 Le burst de bourrage

Lorsqu'un mobile est allumé, le terminal teste le niveau de puissance des fréquences des cellules proches pour déterminer la station de base à laquelle il doit s'asservir. Le burst de bourrage (*dummy burst*) est une séquence prédéfinie qui sert donc d'étalon de puissance. Il est aussi utilisé pour forcer une décision de *handover*.

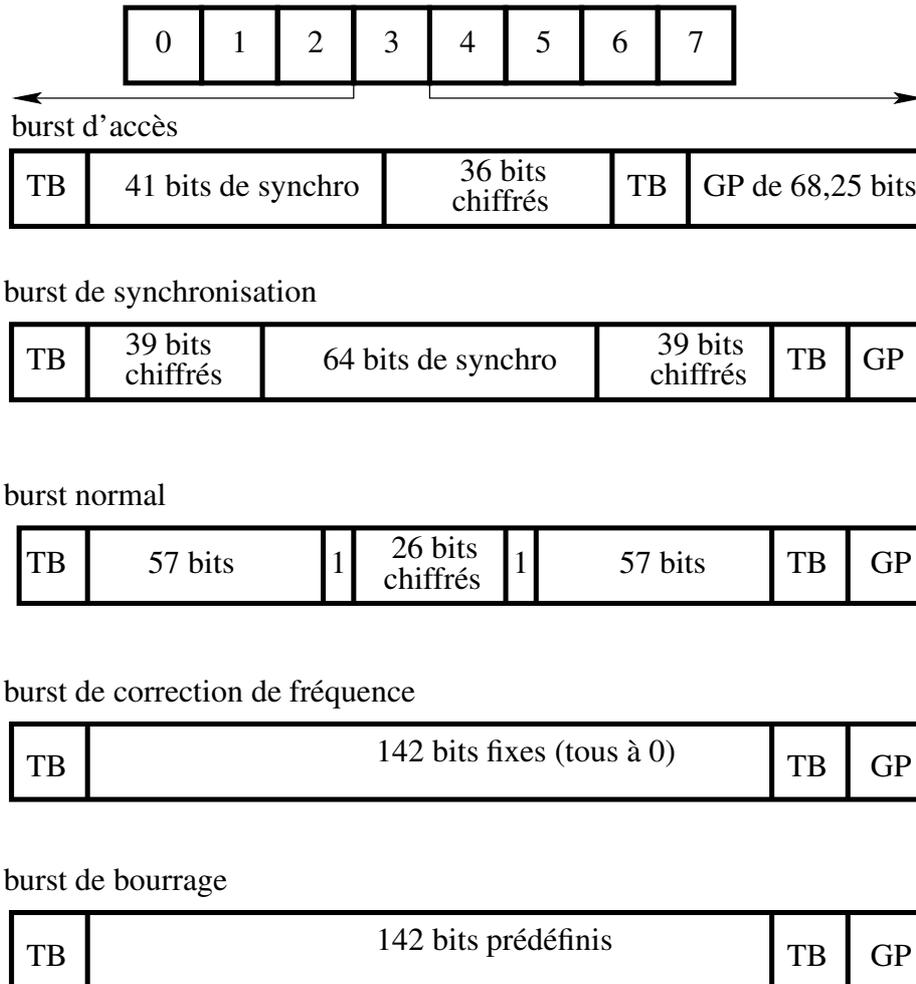


FIG. 8 – Structures des 5 types de *burst* définis par la norme GSM (d'après la norme et [4, page 140]).

Références

- [1] G. Heine. *GSM networks : protocols, terminology, and implementation*. Artech House, 1999.
- [2] X. Lagrange, P. Godlewski, et S. Tabbane. *Réseaux GSM-DCS*. Hermès, troisième édition, 1997.
- [3] J. Tisal. *Le réseau GSM. L'évolution GPRS : une étape vers UMTS*. Dunod, troisième édition, 1999.
- [4] B. Walke. *Mobile Radio Networks : networking, protocols and traffic performance*. John Wiley & Sons, 2002.

Glossaire

AuC	<i>Authentication Center</i> . Centre d'authentification (lié à un HLR) utilisé dans les réseaux GSM.	7
authentification	Fonction cryptographique qui consiste à identifier une personne. Cette fonction peut être assurée par différentes implémentations dont PGP par exemple.	7
BSC	<i>Base Station Controller</i> . Station qui contrôle les communications d'un groupe de cellules dans un réseau de communications GSM. Elle concentre le trafic de plusieurs BTS.	4
BTS	<i>Base Transceiver Station</i> . Station de base d'un réseau GSM. Elle permet notamment d'émettre et de recevoir un signal radio.	4
CA	<i>Certification Authority ou Cell Allocation</i> . L'autorité de certification est une entité d'un système transactionnel électronique sécurisé. Généralement, cette autorité délivre et vérifie des certificats. Dans la terminologie GSM, il s'agit de la liste des numéros de fréquences utilisées dans une cellule.	10
CDMA	<i>Code Division Multiple Access</i> . Technologie de transmission numérique permettant la transmission de plusieurs flux simultanés par répartition de code. Cette technologie permet une utilisation permanente de la totalité de la bande de fréquences allouée à l'ensemble des utilisateurs. La technologie prévoit un mécanisme d'accès aux ressources.	4
cellule	En radiocommunications, zone géographique élémentaire d'un réseau radiocellulaire à laquelle on affecte un ensemble de fréquences non réutilisables dans les zones contiguës. C'est également le nom donné à un paquet ATM qui a une taille de 53 bytes dont 48 sont destinées à recevoir les données d'un utilisateur.	2
CFU	<i>Call Forwarding Unconditional</i> . Numéro de téléphone vers lequel tout appel est redirigé à la demande de l'abonné appelé.	12
chiffrement	Terme qui désigne l'action de chiffrer un texte, des informations ou des données. Le chiffrement consiste à transformer un texte de sorte qu'il faille une clé pour comprendre le message.	7
CLIP	<i>Calling Line Identification Presentation</i> . Service complémentaire de téléphonie qui consiste à afficher le numéro du correspondant sur le terminal.	12
CLIR	<i>Calling Line Identification Restriction</i> . Service complémentaire de téléphonie qui empêche que le numéro du correspondant n'apparaisse sur le terminal d'un utilisateur.	12
concentrateur	Organe permettant de concentrer le trafic et pouvant posséder une intelligence capable de gérer diverses commutations et divers protocoles.	7
décibel	Unité, notée dB, servant à mesurer la puissance.	2
DCS	<i>Digital Communication System</i> . Un système GSM porté de la bande de fréquences des 900 [MHz] vers 1800 [MHz]. Le système DCS-1800 a plus de canaux (374) mais les protocoles et services sont quasi identiques.	4
EIR	<i>Equipment Identity Register</i> . Identifiant destiné à permettre de désactiver un téléphone mobile (GSM) qui aurait été volé.	7
FDMA	<i>Frequency Division Multiple Access</i> . Technique de répartition de ressources par multiplexage fréquentiel. Cette technique prévoit un mécanisme d'accès aux ressources.	4, 9
FH	<i>Frequency Hopping</i> . Technique du saut de fréquences qui consiste à modifier la fréquence porteuse d'un signal modulé en suivant une liste pré-déterminée.	10
FM	<i>Frequency Modulation</i> . Modulation de fréquences. Technique par laquelle on module la fréquence instantanée d'une porteuse au moyen du signal modulant à transmettre.	9
GMSC	<i>Gateway Mobile Switching Center</i> . Centre de commutation pour mobile semblable à un MSC. Il est placé en bordure de réseau d'un opérateur GSM de manière à permettre l'interconnexion avec d'autres réseaux.	7
GMSK	<i>Gaussian Minimum Shift Keying</i> . Nom de la technique de modulation numérique utilisée pour la transmission radio des mobiles GSM.	9
GPRS	<i>General Packet Radio Service</i> . Technologie de transmission par paquets facilitant l'accès à Internet à haut débit par GSM. Le débit peut varier de 56 jusqu'à 115 [kb/s]. Il est également possible d'établir des connexions permanentes.	1

GSM	<i>Global System for Mobile Communications.</i> Standard de téléphonie mobile adopté en Europe, en Asie et en Australie.	1, 3
handover	Terme désignant le mécanisme par lequel un mobile peut transférer sa connexion d'une station de base vers une autre ou, sur la même station, d'un canal radio vers un autre.	13
HLR	<i>Home Location Register.</i> Base de données centrale d'un réseau GSM contenant toutes les informations relatives aux abonnés du réseau (profil, position actuelle, . . .).	7
HSN	<i>Hopping Sequence Number.</i> Une classe de paramètres, définis dans la norme GSM, pour configurer la séquence de porteuses utilisées pour des sauts de fréquences.	10
hypertrame	L'unité temporelle la plus longue de la hiérarchie GSM. Elle totalise 3 heures, 28 minutes, 53 secondes et 760 millisecondes. Elle est composée de 2048 supertrames, composées elles-mêmes de 1326 multitrames.	10
IMEI	<i>International Mobile station Equipment Identity.</i> Numéro unique identifiant un terminal GSM ; il est indépendant du numéro d'abonné et il permet de désactiver un équipement volé.	8
IMSI	<i>International Mobile Subscriber Identity.</i> Numéro international unique d'un abonné GSM.	4, 5, 7
IS-95	Norme américaine de réseau cellulaire (dit de seconde génération ou 2G) basée sur la méthode d'accès CDMA.	4
ISDN	<i>Integrated Services Digital Network</i> Désigne le réseau téléphonique numérique RNIS.	7
LAPD	<i>Link Access Protocol D-channel.</i> Protocole de liaison de données utilisée dans le réseau GSM. Il est défini dans la famille des recommandations X25 de l'ITU.	12
MA	<i>Mobile Allocation.</i> Liste des numéros de fréquences utilisables pour des sauts de fréquences dans un réseau GSM.	10
MAIO	<i>Mobile Allocation Index Offset.</i> Décalage permettant à chaque terminal GSM d'utiliser une série de fréquences différentes d'un mobile à l'autre pour les sauts de fréquence.	10
MCC	<i>Mobile Country Code.</i> Nombre à 3 chiffres identifiant un pays (Belgique = 206, France = 208).	5
MNC	<i>Mobile Network Code.</i> Un nombre à 2 chiffres utilisé par identifier un PLMN.	5
MSC	<i>Mobile Switching Center.</i> Centre de commutation pour mobile. Cet équipement réalise la commutation des appels d'une ou plusieurs cellules.	7, 11
MSISDN	<i>Mobile Subscriber ISDN.</i> Numéro d'abonné au réseau GSM. Il est possible d'avoir plusieurs numéros (pour des services différents) au sein d'une seule carte SIM.	4, 5
MSK	<i>Minimum Shift Keying.</i> Technique de modulation numérique consistant à effectuer une fonction XOR entre 2 bits successifs préalablement à une modulation de fréquence à 2 états.	9
NSS	<i>Network Switching Center.</i> Sous-système d'un réseau de téléphonie mobile. C'est la partie qui prend principalement en charge la commutation des appels, la signalisation et l'identification.	7, 12
PCM	<i>Pulse Code Modulation.</i> Nom américain pour désigner la modulation par impulsions codées (MIC). Cette technique, utilisée principalement en téléphonie, convertit un signal analogique en un signal de téléphonie numérique à 64 [kb/s]. En toute rigueur, on ne devrait pas parler de modulation.	12
PIN	<i>Personal Identification Number.</i> Code (mot de passe) nécessaire à chaque connexion d'un GSM au réseau.	4, 5
PLMN	<i>Public Land Mobile Network.</i> Il s'agit du réseau GSM, DCS ou PCS d'un opérateur dans un pays. Le "Network Color Code" identifie un PLMN dans un pays.	5
PUK	<i>PIN Unblocking Key.</i> Code nécessaire au déverrouillage d'une carte SIM.	5
RNIS	<i>Réseau Numérique à Intégration de Services.</i> Désigne le réseau téléphonique numérique. Au niveau du réseau, les signaux numériques utiles sont transmis à des multiples de 64[kb/s].	7
roaming	Nom anglais pour désigner le fait qu'un utilisateur de GSM peut se déplacer d'une cellule à l'autre ou d'un réseau à un autre sans rupture de connexion. L'abonné qui utilise sa carte SIM est facturé par son opérateur. Cette opération est rendue possible grâce aux accords de roaming conclus entre les différents opérateurs.	5, 7
RTC	<i>Réseau Téléphonique Commuté.</i> Terme technique désignant le réseau téléphonique fixe.	2
SIM	<i>Subscriber Identity Module.</i> Micro-processeur implanté dans une carte. Par extension, on parle de la carte SIM. Elle est insérée dans un GSM pour réaliser une série de fonctions et contenir une mini-base de données.	4
SMS	<i>Short Message Service.</i> Système permettant l'envoi de messages comprenant au plus 160 caractères (de 7 bits), soit 140 bytes, à un téléphone GSM.	12
TA	<i>Timing Advance.</i> Le décalage temporel utilisé pour prévenir les collisions entre messages envoyés par différents mobiles vers une station de base dans un réseau GSM.	11
TDMA	<i>Time Division Multiple Access.</i> Technique de répartition de ressources par multiplexage temporel. Cette technique prévoit un mécanisme d'accès.	4, 9

TMSI	<i>Temporary Mobile Subscriber Identity</i> . Numéro attribué temporairement à un utilisateur GSM en fonction de sa localisation.	5
trame	En traitement d'images, la trame est la grille d'échantillonnage. On considère généralement la trame carrée mais la trame peut aussi être rectangulaire ou hexagonale. Dans le cas du format entrelacé, la trame désigne une image ne contenant que les lignes paires ou impaires de l'image. En télécommunications, trame désigne un ensemble d'informations numériques temporelles constituant un tout.	9
transcodage	Aussi appelé transrating. Il s'agit d'un procédé de changement du débit d'un signal comprimé.	12
TRAU	<i>Transcoding Rate and Adaptation Unit</i> . Unité de transcodage utilisée dans les réseaux GSM pour convertir un signal de 13 [kb/s] en un signal de 64 [kb/s] et vice-versa.	12
UMTS	<i>Universal Mobile Telecommunications System</i> . Nom du standard de téléphonie mobile de troisième génération pour l'Europe.	1, 4
VLR	<i>Visitor Location Register</i> . Registre local d'une zone comprenant plusieurs cellules d'un réseau GSM. Ce registre contient l'identité des utilisateurs présents dans la zone.	7
X25	Série de protocoles, définis par l'ITU, destinés à la transmission de données. Leur utilisation est aujourd'hui largement supplantée par l'utilisation des protocoles à technologie Internet.	7
XOR	<i>eXclusive OR</i> . Fonction logique du OU exclusif. Le résultat de la fonction vaut 0 si les deux états sont à 0 ou à 1. Il vaut 1 dans les autres cas.	9