REPUBLIQUE DU CAMEROUN
Paix - Travail – Patrie

UNIVERSITE DE YAOUNDE I

ECOLE NATIONALE SUPERIEURE POLYTECHNIQUE

REPUBLIC OF CAMEROUN
Peace - Work – Fatherland

UNIVERSITY OF YAOUNDE I

NATIONAL ADVANCED SCHOOL OF ENGENEERING

MASTER PRO 2 EN TELECOMMUNICATIONS

PLANNIFICATION ET INGENIEURIE DES RESEAUX DE TELECOMS

Séquence 3 : GESTION DE L'ITINERANCE, DE LA SECURITE ET DES APPELS

Equipe des concepteurs :

- Emmanuel TONYE
- Landry EWOUSSOUA

Séquence 3

GESTION DE L'ITINERANCE, DE LA SECURITE ET DES APPELS

SOMMAIRE

L'introduction à la mobilité dans les réseaux à nécessité la définition de nouvelle fonction par rapport aux réseaux fixes classiques. Le systèmes 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". En effet, contrairement aux réseaux fixes ou un numéro d'un terminal à une adresse physique fixe (prise de téléphone généralement), le numéro d'un téléphone devient du point de vue réseau, une adresse logique constante à laquelle il faut correspondre une adresse physique qui, elle, varie au grès des déplacements du terminal mobile. La gestion de l'itinérance nécessite la mise en œuvre d'une identification spécifique des usagers. De plus pour offrir des services équivalents à ceux des réseaux fixes elle doit répondre :

- la nécessité pour le système de connaître en permanence la localisation de chaque mobile pour pouvoir le joindre. ;
- à 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 communication usager

La gestion de l'itinérance engendre ainsi un trafic de signalisation important sur l'interface radio et dans le réseau, alors que dans les réseaux fixes un terminal inactif (c'est-à-dire qui n'est pas en communication) n'engendre aucun trafic sur le réseau.

L'utilisation d'un canal radio rend les communications vulnérables aux écoutes d'où des problèmes de confidentialité, et aux utilisations frauduleuses d'où des problèmes de sécurité. Le GSM a donc recours aux procédés suivants :

- Authentification de chaque abonné avant de lui autoriser l'accès à un service
- utilisation d'une identité temporaire
- Chiffrement (ou cryptage) des communications.

1. Numérotation liée à la mobilité

Le système GSM utilise quatre types d'adressage lié à l'abonné :

- 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, aussi GSM à recours au TMSI ;
- le TMSI est une identité temporaire utilisé pour identifier le mobile lors des interactions Station Mobile-Réseau ;
- Le MSISDN est le numéro de l'abonné ; c'est le seul identifiant de l'abonné mobile connu à l'extérieur du réseau GSM ;
- Le MSRN est un numéro attribué lors d'un établissement d'appel. Sa principale fonction est de contrôler l'identité IMEI de tout équipement qui désire un service.

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.

1.1 IMSI (International Mobile Subscriber Identity)

Chaque usager dispose d'une identité internationale IMSI, unique pour tous les réseaux GSM et qui ne varie pas dans le temps (sauf dans les cas de renouvellement ou de perte de carte SIM par l'abonné par exemple)

L'IMSI suit le plan d'identification E.212 de l'IUT. On le transporte aussi rarement que possible sur l'interface radio pour des questions de sécurité (pour éviter qu'un intrus l'intercepte et l'utilise en se faisant passer pour l'abonné réel) et de confidentialité (pour éviter qu'une personne à l'écoute du canal n'identifie l'abonné en communication). L'IMSI sert également au réseau à rechercher l'usager dans les cas où le TMSI n'est pas disponible.

L'IMSI est codé sur 15 digits et comprends trois parties :

- Mobile country Code (MCC) : indicatif du pays domicile de l'abonné mobile (par exemple 208 pour la France),
- Mobile network code (MMC) : indicatif du PLMN nominal de l'abonné mobile
- Mobile Subscriber Identification number (MSIN) : numéro de l'abonné mobile à l'intérieur du réseau GSM.

Les deux champs MCC et MNC permettent de déterminer, de façon unique dans le monde, le PLMN de l'abonné. Les deux premiers chiffres du champ MSIN donnent l'indicatif du HLR de l'abonné au sein de son PLMN. Les MSC/VLR sont donc capables, à partir d'un IMSI quelconque, d'adresser le HLR de l'abonné correspondant.

1.2 TMSI (Temporary Mobile Station Identify)

A l'intérieur d'une zone gérée par un VLR, un abonné dispose d'une identité temporaire, le TMSI, attribuée 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 MS-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 dépendants de VLR différents peuvent avoir le même TMSI. A chaque changement de VLR, un nouveau TMSI doit être attribué.

L'utilisation du TMSI est optionnelle. En effet, la norme GSM prévoît la possibilité pour l'opérateur de n'avoir recours qu'à l'IMSI. Cependant, pour les raisons de sécurité évoquées précédemment, il est préférable d'utiliser le TMSI.

La structure du TMSI est laissée libre à l'opérateur. Il est codé sur 4 octets. Sa structure plus courte que l'IMSI permet de réduire la taille des messages d'appel sur la voie radio.

1.3 MSISDN (Mobile Station ISDN Number)

L'identité de l'abonné GSM pour le "monde extérieur", c'est à dire pour les réseaux autres que le réseau GSM nominal de l'abonné, est le MSISDN. C'est ce

numéro que composera une personne désirant joindre un abonné GSM. Seul le HLR contient la table de correspondance entre le MSISDN et l'IMSI d'un abonné.

Le MSISDN est conforme au plan de numérotation téléphonique internationalE.164. il comprend les champs suivant :

- Country code (CC ou code pays) : indicatif du pays dans le quel l'abonné a souscrit son abonnement (237 pour le Cameroun, 228 pour le togo),
- National (Significant) mobile Number : numéro national du mobile composé du National Destination code (NDC) déterminant le PLMN particulier dans le pays et du subscriber Number (SN) attribué librement par l'opérateur.

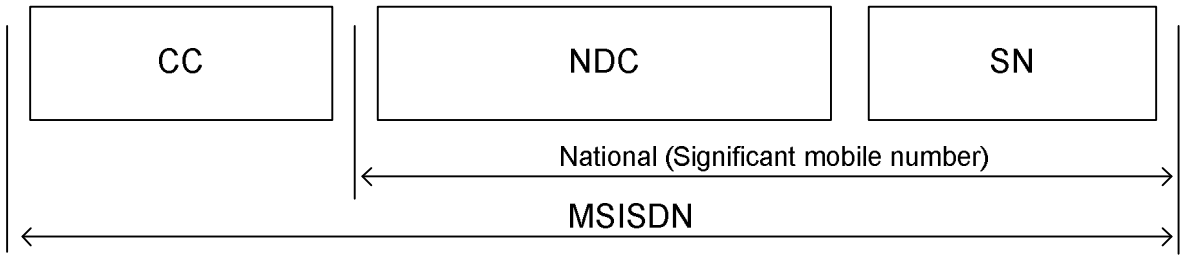

Figure 1 : Composition de l'IMSI

Comme pour l'IMSI, le MSISDN permet à un PLMN de connaître le HLR de l'abonné à partir des premiers chiffres du champ SN. La présence des champs CC et NDC permet aussi de l'utiliser comme appellation globale dans le SCCP pour le routage des messages entre PLMN quelconque et le HLR nominal de l'abonné.

1.4. 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 attribue par le VLR courant du mobile de façon temporaire et uniquement lors de l' établissement d'un appel a destination de la station mobile Le MSRN a la même structure que le MSISDN conformément au format E.164 (le MSRN peut être identique au MSISDN dans certains cas) :

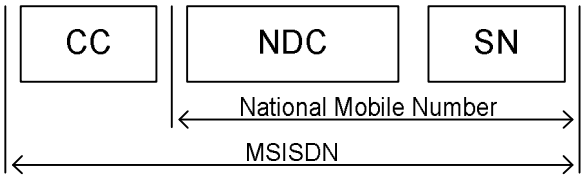

Figure 2: Structure du MSISDN

– champ CC : code pays du VLR courant du mobile,
– champ NDC : code du PLMN du VLR courant du mobile, – numéro d'abonne.

Comme le MSISDN, le MSRN a également la forme ABPQMCDU en France. Elle correspond a un numéro du MSC dans lequel se trouve l'abonne. Cet adressage est intègre au réseau national et il est compréhensible par le réseau fixe.

1.5. Exemple de mise en œuvre des différentes identités d'abonné dans GSM

L'ensemble des identités et numéros présenté dans les paragraphes précédent et utilisé lors d'un appel entrant

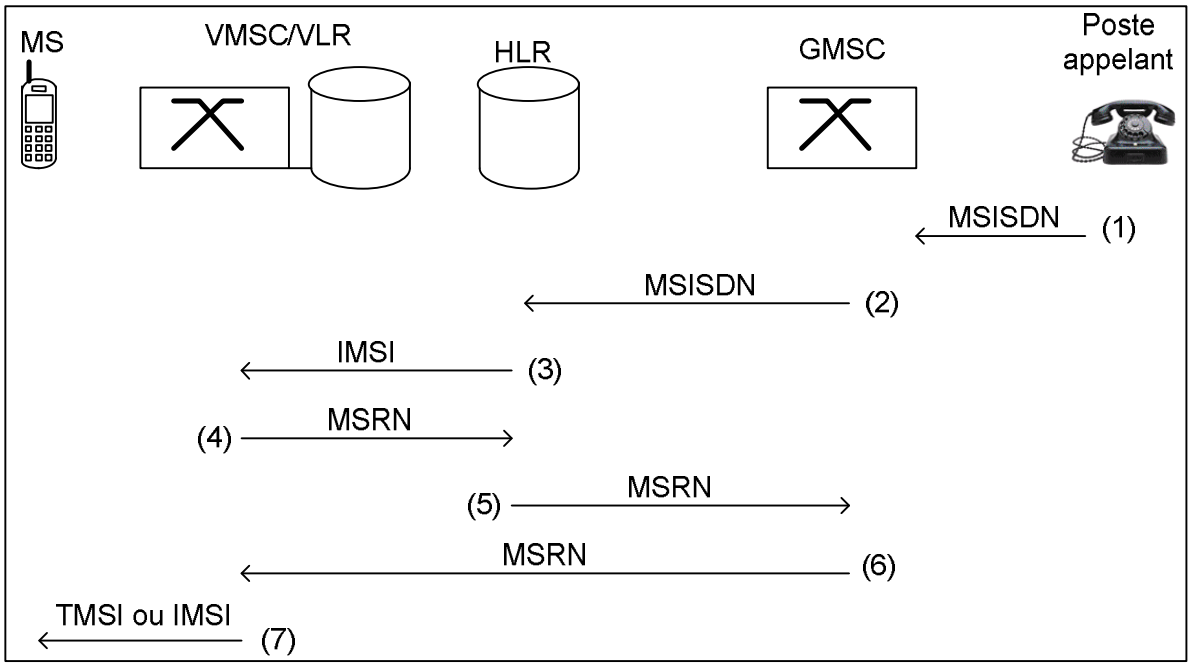

Figure 3 : Echange de différentes identités

(1) Le MSISDN est numéroté par l'appelant. L'appel est routé par le réseau vers le MSC le plus proche qui agit alors en GMSC.

(2) Le GMSC interroge le HLR pour connaître le MSC vers lequel l'appel doit être route.

(3) Le HLR traduit le MSISDN en IMSI et interroge le VLR du mobile en utilisant l'IMSI.

(4) Le VLR du mobile attribue un MSRN au mobile et transmet ce numéro au HLR.

(5) Le HLR en recevant le MSRN le transmet au GMSC.

(6) Le GMSC établit l'appel vers le MSC courant du mobile comme un appel téléphonique normal vers un abonne dont le numéro est le NISRN.

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

1.6. IMEI (International Mobile Equipment Identity)

Tout terminal est référence de manière unique par 1'IMEI, qui est codé sur au plus 15 digits :

- Type Approval Code (TAC) : champ codé sur 6 digits fournis au constructeur

lorsque le matériel a passé l'agrément,
- Final Assembly Code (FAC) : champ codé sur 2 digits qui identifie l'usine de fabrication,
- Serial Number (SNR) : numéro code sur 6 digits librement affecte par le constructeur,
Spare : digit réservé pour l'instant.

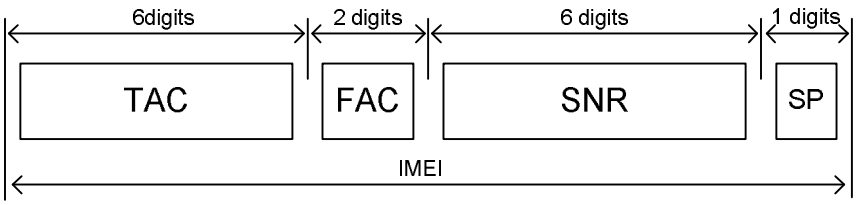

Figure 4: Structure du IMEI

2. Authentification et chiffrement

Confidentialité et sécurité sont fragilisées par l'utilisation du canal radioélectrique pour transporter les informations. Les abonnes mobiles sont particulièrement vulnérables :

- à la possibilité d'utilisation frauduleuse de leur compte par des personnes disposant de mobiles pirates », qui se pressentent avec l'identité d'abonnes autorisés,
- à la possibilité de voir leurs communications écoutées fors du transit des informations sur le canal radio.

Il faut par conséquent que les systèmes de communications mobiles mettent en oeuvre des fonctions de sécurité supplémentaires visant à protéger: à la fois les abonnés et les opérateurs. Le système GSM [GSM 02.09] intègre ainsi les fonctions suivantes :

- confidentialité de l'IMSI,
- authentification d'un abonne pour protéger l'accès aux services,
- confidentialité des données usager
- confidentialité des informations de signalisation.

2.1. Confidentialité de l'identité de l'abonné

Comme précisé précédemment, il s'agit d'éviter l'interception de l'IMSI lors de son transfert sur la voie radio par des personnes, entités ou processus non autorises. Cela permet d'assurer la confidentialité des identités de l'abonne et de renforcer le niveau de sécurité concernant les autres éléments protégés. Ainsi, il devient difficile de suivre ou de tracer un abonné mobile en interceptant les messages de signalisation échangés sur le canal radio.

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. Le réseau (typiquement au niveau d'un VLR), gère des bases de données et établit la correspondance entre TMSI et IMSI. En général, l'IMSI est transmis lors de la mise sous tension du mobile et ensuite, seuls les TMSI successifs du mobile seront

transmis sur la voie radio. Ce n'est que dans les cas où le TMSI a été perdu ou lorsque le VLR courant ne reconnaît pas le TMSI de l'abonné - par exemple après une panne ayant entraîné une perte des informations d'abonné - que la transmission de l'IMSI sur la voie radio peut être nécessaire.

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 est mis en oeuvre.

L'allocation d'un TMSI est présentée à la figure ci-dessous. Elle a lieu, par exemple, lors d'une mise à jour de localisation.

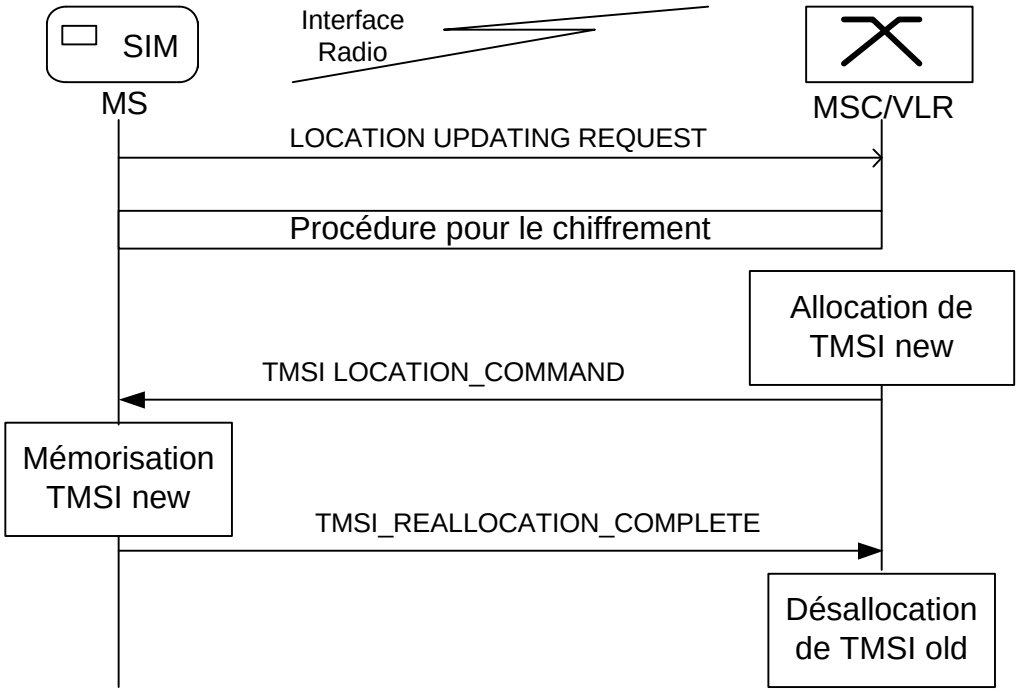

Figure 4: Allocation du TMSI

2.2 Principes généraux d'authentification et de chiffrement

Pour mettre en oeuvre 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 des arguments d'entrée RAND et la clé Ki pour l'authentification,
- un algorithme A8 pour la détermination de la clé Kc à partir des arguments d'entrée 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.

Les données RAND, SRES et Kc jouent un rôle particulier et sont groupées dans des triplets. L'utilisation de ces différents éléments pour la mise en oeuvre des fonctions de sécurité est schématisée sur la figure ci dessous

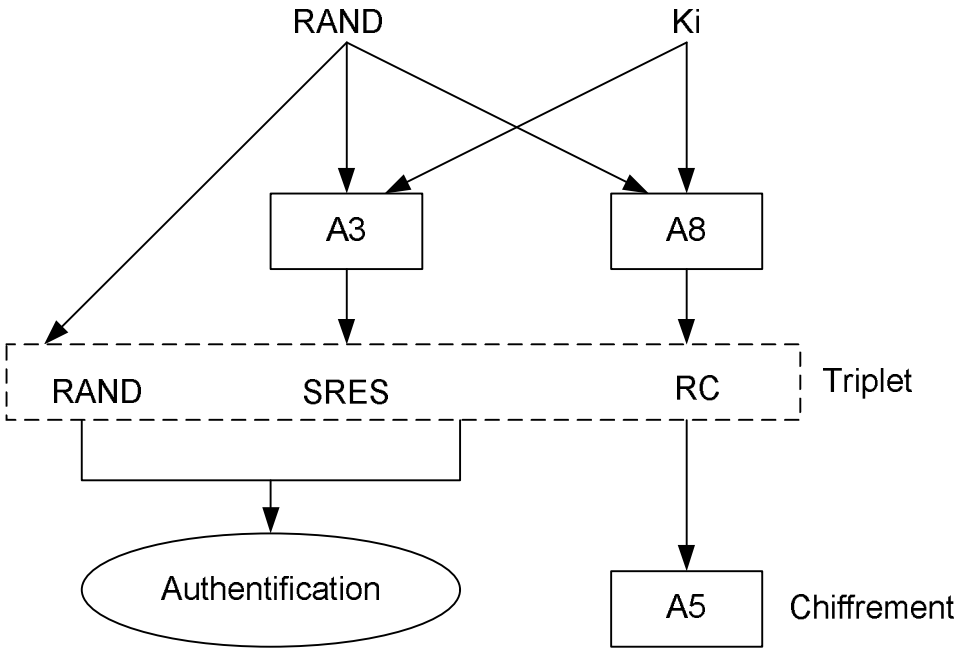

Figure 6. Utilisation des différents éléments de sécurité dans GSM

L'algorithme A3 au niveau du HLR/AUC et de la MS 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 de la MS de déterminer la clé de chiffrement Kc à l'aide de RAND et de Ki. Les triplets obtenus (RAND, SRES, Kc) permettent au réseau (au niveau du MSC/VLR) d'authentifier un abonne et de chiffrer les communications.

2.3. Authentification de l'identité de l'abonné

L'authentification permet de vérifier que l'identité transmise par le mobile (IMSI TMSI) sur la voie radio est correcte afin de protéger, d'une part l'opérateur contre ou l'utilisation frauduleuse de ses ressources, et d'autre part les abonnes en interdisant a 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. Elle est également demandé lors de la mise en oeuvre de la clé de chiffrement sur certains canaux dédies. L'authentification n'est pas nécessaire dans les procédures IMSI Attach/Detach.

Dans le cas 00 la procédure d'authentification de l'abonné échoue, l'accès au réseau est refusé au mobile.

Lors de la procédure d'authentification les échanges entre la station mobile et le réseau sont les suivants :

– le réseau transmet un nombre aléatoire RAND au mobile ;

– la carte SIM du mobile calcule la signature de RAND grâce à l'algorithme d'au-

thentification A3 et à la clé d'authentification Ki (information secrète). Le résultat calcule, note SRES, est envoyé par le mobile au réseau ;

– le réseau compare SRES au résultat calculé de son côte. Si les deux résultats sont identiques, l'abonné est authentifié.

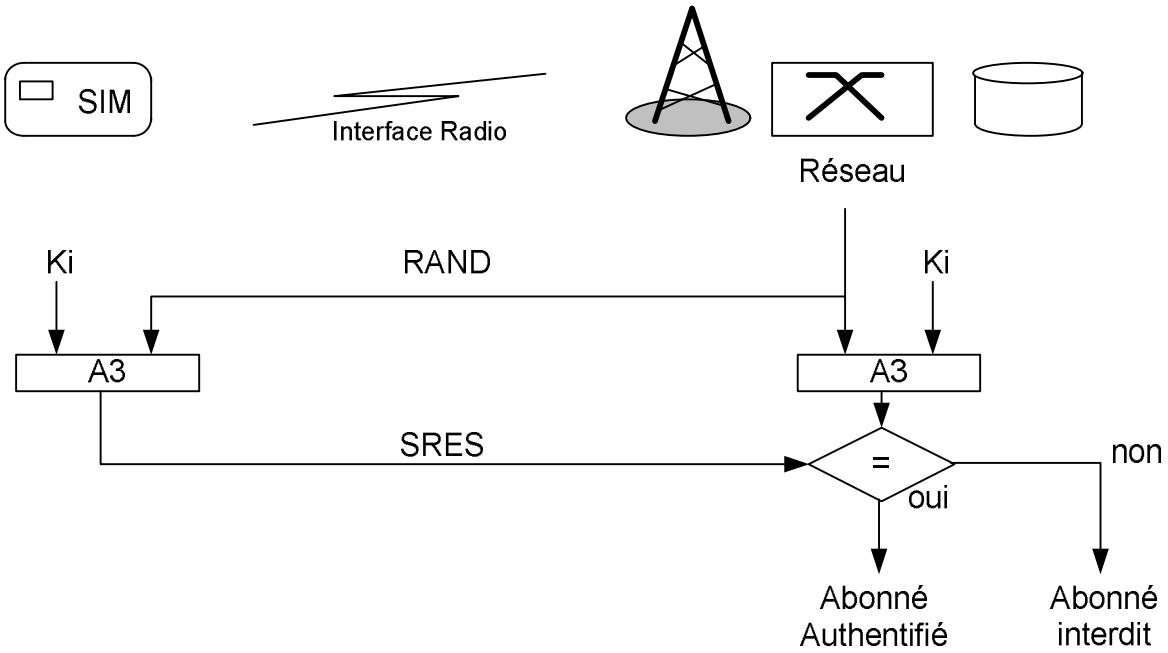

Figure 7. Déroulement global de la procédure d'authentification

2.4. 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 suivants : IMEI (identité du terminal), MS (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 MS-BTS. Ce n'est donc pas un service de confidentialité de bout en bout.

La procédure de chiffrement fait intervenir l'algorithme de chiffrement, le mode d'établissement de la clé de chiffrement et le déclenchement des processus de chiffrement /déchiffrement à chaque bout de la liaison.

2.4.1. Etablissement de la clé

Les informations transmises sur les canaux dédies 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.

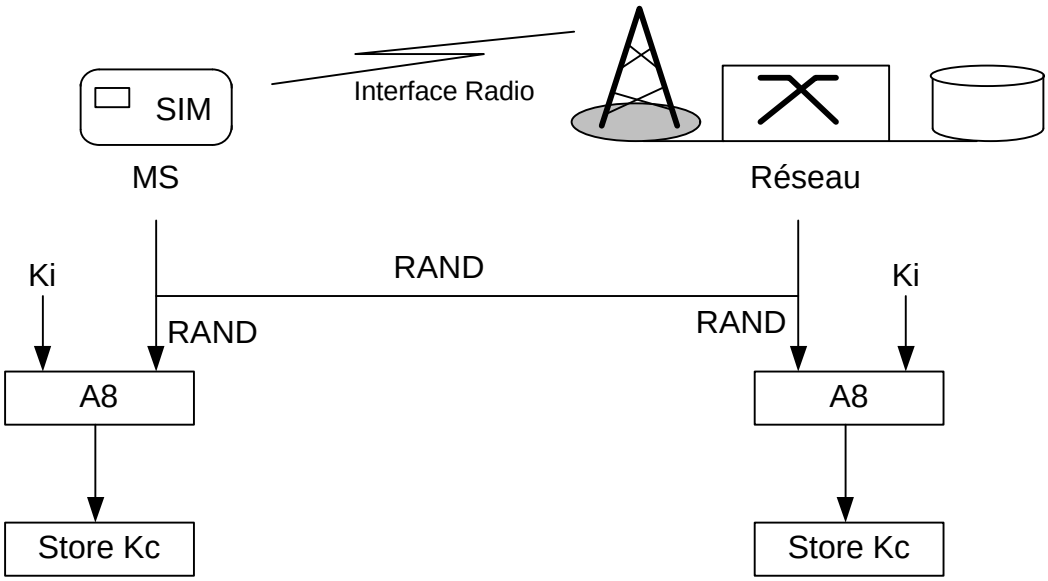

Figure 8. Etablissement de la clé de chiffrement Kc

2.4.2. Activation du chiffrement

L'algorithme A5 de chiffrement/déchiffrement est implanté dans la BTS. L'activation se fait sur la demande de la MSC mais le dialogue est géré par la BTS dans la couche RR. Notons simplement que le chiffrement ne peut pas être activé dès les premiers messages mais se fait nécessairement après une authentification car le mobile doit connaître la clé Kc.

2.5. Gestion des données de sécurité au sein du réseau

2.5.1. Gestion de la clé d'authentification Ki

La clé Ki est attribuée à l'usager, lors de l'abonnement, avec l'IMSI. Elle est stockée dans la carte SIM de l'abonné et dans l'AUC au niveau du réseau. Il peut y avoir plusieurs centres d'authentification dans un réseau GSM. On associe le plus souvent l'AUC au HLR.

Afin de limiter les possibilités de lecture de la clé Ki, celle-ci n'est jamais transmise à travers le réseau, ni sur l'interface radio, ni entre les équipements fixes.

2.5.2. Procédure générale de gestion des données

Le réseau ne calcule par les données de sécurité en temps réel au moment où il en a besoin. Force est de constater qu'il suffit au réseau de disposer d'un triplet (RAND, SRES, Kc) d'un abonné pour l'authentifier et activer le chiffrement de ses communications. Les MSCNLR et HLR échangent des triplets en utilisant le protocole MAP.

L'AUC prépare des triplets pour chaque abonné mobile et les transmet au HLR qui les stocke en réserve. Lorsque le MSC/VLR a besoin de ces triplets, il les demande en envoyant un message « MAP_SEND_AUTHENTICATION_INFO » au HLR.

Ce message contient l'IMSI de l'abonné, et la réponse du HLR contient en

général cinq triplets. Un triplet qui a été utilisé lors d'une authentification est détruit (ne sera pas réutilisé par la suite), sauf dans les cas très particuliers de défense (indisponibilité du HLR/AUC) qui ont pour conséquence de fragiliser la sécurité du réseau.

La transmission de cinq triplets dans un seul message permet de ne pas surcharger le réseau par des échanges de signalisation fréquents. Il faut remarquer que le réseau qui utilise les triplets n'a pas besoin de réseau les algorithmes A3 et A8 puisque l'argument d'entrée RAND et les résultats SRES et Kc lui sont fournis.

Il est donc envisageable que chaque opérateur ait ses propres algorithmes A3 et A8 et puisse accueillir des abonnés de réseau utilisant des algorithmes différents : 1 abonné est toujours authentifié à partir des algorithmes de son PLMN d'origine.

Il est intéressant de noter qu'aucune information confidentielle (clé Kc ou Ki, algorithmes A3, A5 ou A8) n'est transmise ni sur la voie radio ni dans le réseau. Par exemple, il faudrait intercepter plusieurs milliards de couples (RAND, SRES) pour déterminer l'algorithme A3.

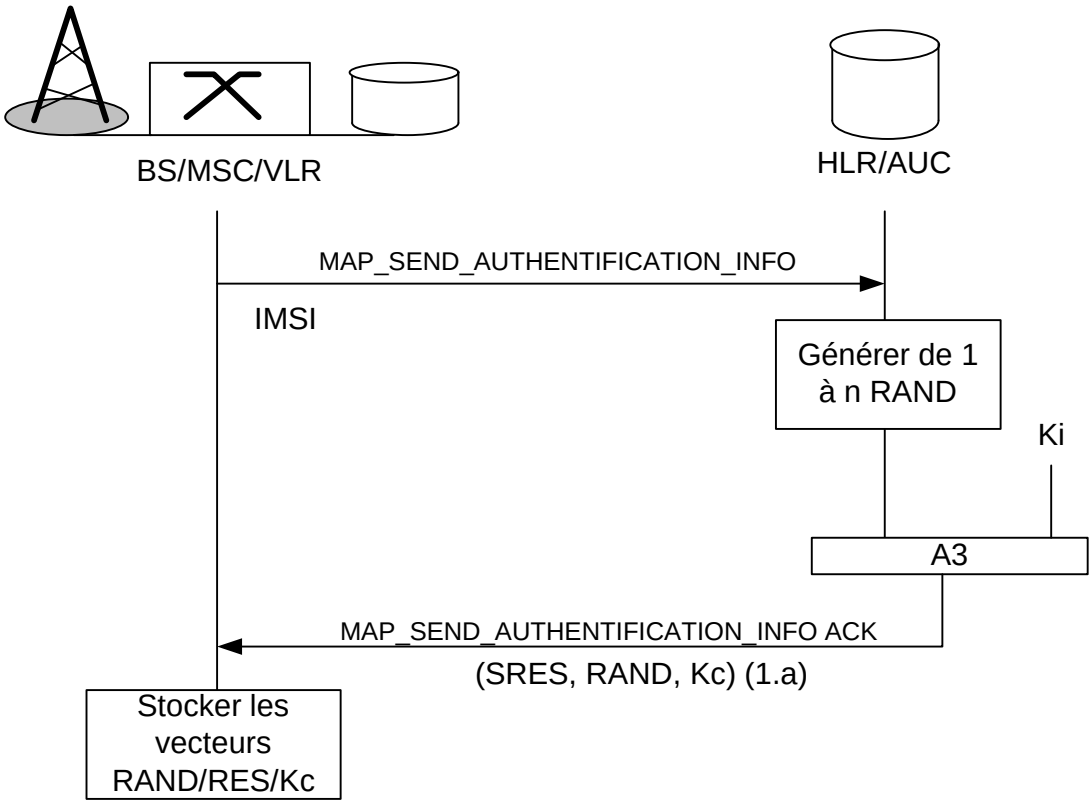

Figure 9. Transmission des informations de sécurité entre HLR et VLR

2.5.3. Transmission de la clé d'authentification

Dans la phase 1 des spécifications, il était possible d'implanter l'algorithme A3 au sein du MSC/VLR. La clé d'authentification Ki était alors communiquée par le HLR. La transmission de la clé fragilisait considérablement la sécurité du réseau.

Cette solution n'était pas adoptée par les opérateurs. Elle n'est plus possible dans la phase 2.

2.5.4. Entités du réseau où sont enregistrées les données de sécurité

Les données de sécurité sont stockées au niveau de différentes entités réseau qui sont les suivantes :

AUC : le centre d'authentification stocke les informations suivantes :

– l'algorithme d'authentification A3,

– l'algorithme de génération de clé de chiffrement A8,

– les clés Ki des abonnés du réseau GSM.

HLR : il peut enregistrer plusieurs triplets (Kc, RAND, SRES) pour chaque IMSI.

VLR : au niveau du VLR, plusieurs triplets (Kc, RAND, SRES) sont enregistrés pour chaque IMSI. Les couples TMSI (ou IMSI) et clé de chiffrement Kc sont enregistrés dans le VLR.

BTS : ces entités peuvent stocker l'algorithme de chiffrement A5 pour les données usager et pour les données de signalisation.

MS : la station mobile contient et reçoit les informations suivantes qui sont stockées dans la carte SIM de l'abonné : l'algorithme d'authentification A3, l'algorithme de chiffrement A5, l'algorithme de génération des clés de chiffrement A8, la clé d'authentification individuelle de l'utilisateur Ki, la clé de chiffrement Kc, le numéro de séquence de la clé de chiffrement et le TMSI.

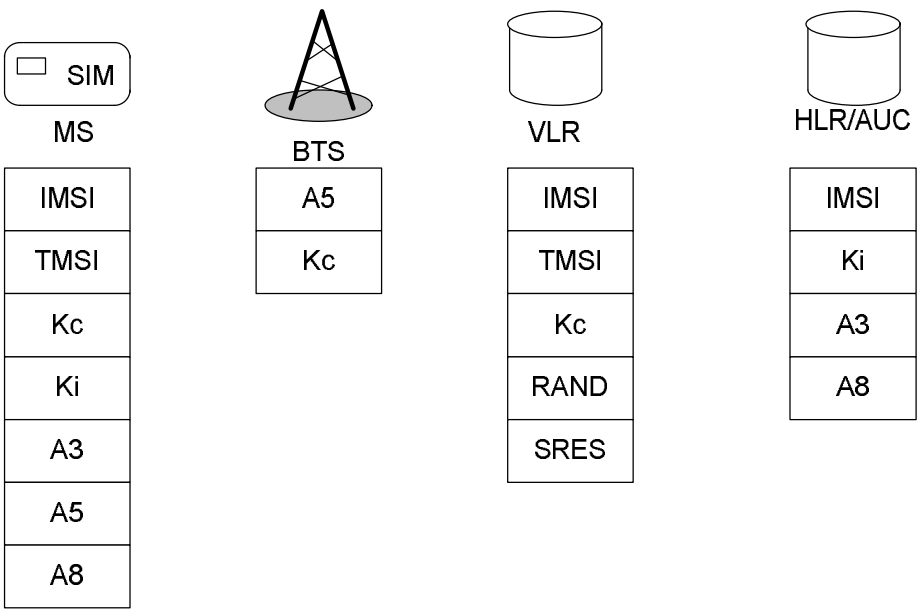

Figure 10. Sites d'enregistrement des données de sécurité

2.6. Autres mécanismes

Les mécanismes de sécurité mis en oeuvre dans GSM permettent d'obtenir des niveaux de protection très élevés pour le système et pour les abonnés. En plus de ces mécanismes, il faut mentionner la protection concernant les terminaux mobiles eux-mêmes.

L'opérateur du réseau GSM peut vérifier l'identité IMEI d'un terminal. Si celle-ci n'est pas reconnue par le réseau ou si elle fait partie d'une liste de terminaux dérobés ou piratés, l'accès du mobile au réseau est alors refusé. Le réseau peut mémoriser identité IMSI de l'abonné utilisant le terminal douteux.

3. 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 instant la position d'un mobile et/ou d'un abonné. Cette fonction est nécessaire pour que le système puisse joindre un abonné. 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, si possible, 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 à précédemment localisé l'abonné.

Ces deux mécanismes sont antagonistes dans la mesure où, lorsque la position du mobile est connue avec précision, le coût de la localisation est important alors que le coût d'une recherche éventuelle sera faible. A contrario, une connaissance imprécise de la position du mobile entraîne un coût de recherche élevé alors que le coût de la localisation aura été faible.

3.1. Présentation générale

Chaque système de communications radio mobiles (cellulaires, 3RP, radiomessageries, etc.) gère l'itinérance de ses abonnés de façon plus ou moins complexe en fonction du type de service offert, de la densité d'usagers, du taux d'appels entrants, etc.

L'une des préoccupations des concepteurs de systèmes radio mobiles est de minimiser le coût des méthodes de gestion de l'itinérance. En effet, elles n'engendrent pas de communication. Elles ne sont donc pas facturées aux abonnés mais utilisent certaines ressources du réseau. Ci-après, nous présentons les principales méthodes de gestion de l'itinérance actuellement mises en oeuvre dans les systèmes radio mobiles.

3.1.1. Systèmes sans localisation

Dans certains systèmes cellulaires de première génération, dans les réseaux radio de couverture peu étendue (certains réseaux radio mobiles d'entreprise par exemple) et dans pratiquement tous les systèmes de radiomessagerie unidirectionnelle, aucune gestion de l'itinérance des usagers n'est assurée. Aucune poursuite des mobiles n'est réalisée et lorsqu'un utilisateur est appelé, le système lance des avis de recherche sur toute la couverture radio du système.

Cette méthode a l'avantage de la simplicité de gestion. En contrepartie, elle ne peut s'appliquer qu'a des systèmes où les taux d'appels entrants sont relativement faibles ou bien à des systèmes de transport de messages courts (comme les radio-

messageries par exemple).

Bien évidemment, cette méthode reste totalement inadaptée dans le cas des systèmes de communications bidirectionnelles desservant des populations d'usagers importantes.

3.1.2. Utilisation de zones de localisation

L'utilisation des zones de localisation est basée sur le principe du regroupement de plusieurs cellules (de quelques cellules à quelques dizaines de cellules) en une zone. Ainsi le système connaît la dernière zone de localisation dans laquelle l'abonné s'est signalé mais ignore la cellule précise où se trouve l'abonné. En cas de réception d'un appel, le système va rechercher l'abonné dans cette zone de localisation en émettant des avis de recherche (ou messages paging) dans les cellules de cette zone. Cette opération induit une réduction de la consommation des ressources. Cette méthode est adoptée dans les systèmes de première génération et le système GSM.

Cette technique de localisation nécessite automatiquement une mise à jour des informations de localisation des abonnés. Cette mise à jour peut se faire de trois façons :

- La mise à jour manuelle nécessite que l'usager informe manuellement le réseau de sa position. Ce type de méthode est particulièrement adaptée aux réseaux comportant des cellules isolées et simplifie la tâche du réseau.
- La mise à jour périodique consiste à envoyer suivant une période définie, la localisation de l'abonné. Cette opération est automatiquement effectuée par le terminal. Elle a l'avantage de la simplicité mais peut conduire à une dépense inutile d'énergie, de spectre radio et de message de signalisation.
- La mise à jour sur changement de zone de localisation consiste en la diffusion périodique par les BTS du numéro de la zone à la quelle elle appartient. Ainsi les terminaux écoutent périodiquement cette voix de balise (BCCH dans le GSM) et stocke en permanence le numéro de la zone de localisation à laquelle elle appartient. Ainsi dès que le mobile s'aperçoit que le dernier numéro stocké est différent du numéro reçu, il signal sa nouvelle position au réseau.

3.2. Gestion de itinérance dans GSM

Le système GSM combine les méthodes de mise à jour de localisation périodique et sur changement de zone de localisation qui sont toutes deux basée sur l'utilisation des zones de localisation repérées par des numéros.

Une zone de localisation est identifiée par l'adresse LAI (Location Area Identification) composé des éléments suivants :

- MCC : indicatif du pays - champ également présent dans l'IMSI,
- MNC : indicatif du PLMN - champ également présent dans l'IMSI.
- LAC : Location Area Code : code de la zone de localisation librement affecte par l'opérateur (jusqu' à 2 octets au maximum).

Cette identité est définie pour chaque abonné de façon unique dans tous les PLMN GSM du monde entier.

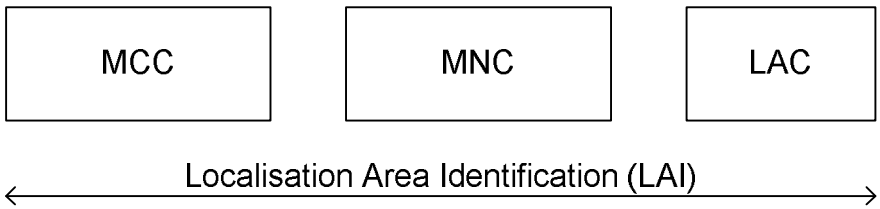

Figure11 : Structure de la LAI

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

Un VLR peut garder plusieurs zones de localisation. En revanche. Une zone de localisation ne peut pas comprendre des cellules dépendant de VLR différents.

Pour éviter les transferts inutiles de signalisation, 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.

3.2.2. Principes de gestion de l'itinérance dans GSM

Outre son rôle dans la gestion de l'itinérance des mobiles, la procédure de mise à jour de localisation permet au réseau de transférer dans le VLR l'ensemble des caractéristiques des abonnés présents sous ce VLR.

La mise à jour de localisation périodique nécessite de la part du mobile en mode veille un contact régulier avec le réseau. Les valeurs possibles de la période sont comprises entre 6 minutes et 24 heures et l'infini pour permettre d'annuler la procédure.

Afin d'éviter les recherches inutiles d'abonnes ayant mis leur mobile hors tension, la norme GSM, a défini les procédures IMSI Attach et IMSI Detach (cette dernière étant optionnelle). A cet effet, les données d'abonnement stockées dans le MSC/VLR contiennent un paramètre indiquant si le mobile est joignable (sous tension) ou pas (hors tension). Le recours à l'une ou l'autre de ces procédures permet de positionner la valeur de ce paramètre.

Pour exécuter la procédure IMSI Detach, le mobile reste sous tension quelques instants après la mise hors tension par l'usager et envoie un message « IMSI DETACH >> au MSC/VLR. L'activation de cette est laissée au choix de l'opérateur car elle n'est pas forcement optimal en terme de signalisation générée. En effet, La mise hors tension d'un grand nombre de terminal au même moment impliquant la procédure IMSI Detach peut générer une pointe de signalisation que le réseau aura du mal à écouler

La remise sous tension du terminal mobile enclenche la procédure IMSI attach qui permet de rattacher ce mobile à sa zone de localisation et signaler que le

terminal est à nouveau apte à recevoir. La procédure IMSI Attach est vue comme une mise à jour de localisation du point de vue du VLR.

Si celui-ci contient les informations concernant le mobile, aucun message ne remonte jusqu' au HLR (on a alors l'équivalent d'une mise à jour de localisation sans changement de VLR), sinon le VLR échange des messages avec le HLR (comme dans le cas une mise à jour de localisation inter-VLR avec IMSI), pour obtenir les informations (droits, données d'authentification,...) concernant l'abonné.

Lorsque le VLR n'a pas eu de contacts avec un mobile pendant une certaine période (fixée par une temporisation), le réseau peut prendre l'initiative de le « détacher » Cette procédure est appelée IMSI Detach implicate et consiste de la part du VLR à marquer un mobile comme étant détache du réseau.

Le VLR peut effacer les données d'un abonne qui n'a pas établi de contact radio pendant une période déterminée (plusieurs jours par exemple). Il fige alors le TMSI qui lui a été alloué dans le but d'éviter les conflits qui pourraient se produire si ce TMSI était alloué a un mobile différent. Cette opération s'appelle la purge des données de l'usager. Le VLR informe le HLR de cette opération qui positionne l'indicateur « MS purged » dans l'enregistrement de la MS concernée. Ainsi, toute demande de routage d'appel vers le mobile concerné sera traitée comme si le mobile n'était pas joignable. L'indicateur est désarmé des lors que le mobile effectue de nouveau une mise à jour de localisation ou un IMSI Attach.

3.3. Conclusions sur l'itinérance

Ce paragraphe décrit la gestion de l'itinérance dans le système GSM. Le coût de cette gestion est important pour l'operateur, notamment si l'on considère l'interface radio qui est une ressource rare. Ce coût est d'autant plus important que cette méthode est totalement transparente à l'utilisateur puisque réalisé: automatiquement par le mobile. La possibilité offerte actuellement à l'abonné de pouvoir recevoir des appels potentiellement sur la totalité de la zone couverte par le système peut être vue comme un service qui, à l'avenir, pourra être souscrit en spécifiant la qualité de service désirée par l'abonne. Par exemple, la possibilité de recevoir des appels dans toute la zone de couverture sera un service plus coûteux que celui offrant la possibilité de recevoir des appels uniquement dans certaines zones prédéfinies (domicile et lieu de travail par exemple).

4. Gestion des appels

Dans cette partie, nous abordons l'une des fonctions essentielles d'un système de communications, à savoir la gestion des appels usagers. Le but de cette fonction est de permettre l'acheminement et l'établissement des appels d'un abonné mobile vers un autre abonné, fixe ou mobile (appel sortant), ou d'un abonné, fixe ou mobile vers un abonné mobile (appel entrant). Les abonnés appelés et appelant peuvent se trouver soit dans le même réseau, soit dans des réseaux différents situes éventuellement dans des pays différents.

Nous examinerons successivement dans cc paragraphe : les principales entités intervenant dans l'établissement d'un appel GSM.

4.1. Principales entités intervenant dans le contrôle d'appel

Dans le traitement d'un appel, on distingue d'une part l'utilisateur et sa station mobile, et d'autre part, le BSS, le NSS (sous-système réseau) et le réseau externe (RTCP ou RNIS par exemple). Dans le NSS, les entités fonctionnelles impliquées dans le contrôle d'appel sont : le MSCNLR, le GMSC et le HLR.

Les protocoles de signalisation permettant la gestion de l'appel sont les suivants : le niveau CC (Call Control) de l'interface radio, et le protocole MAP pour les échanges entre MSCIVLR et HLR d'une part et GMSC et HLR d'autre part. Le protocole BSSMAP intervient de façon ponctuelle pour la gestion des ressources radio. Les messages de niveau CC sont directement échangés entre MS et MSC grâce au protocole DTAP entre BSS et MSC.

Pour les appels internationaux, l'interconnexion avec les réseaux téléphoniques étrangers est assurée par les commutateurs (ou centraux) de transit internationaux (CTI).

4.2. Appel sortant

4.2.1. Description

L'abonné du PLMN doit d'abord composer le numéro du correspondant demandé sur son terminal puis valide l'appel par une touche spécifique. Tant que l'appel n'est pas valide, le mobile est totalement muet vis-à-vis du réseau, la numérotation dans GSM est dite hors-ligne (off-line). Au contraire, dans le réseau te1éphonique, la numérotation se fait en ligne (on-line), car l'abonné est relié à son central de rattachement lorsqu'il numérote (confère séquence 5)

Une fois l'appel validé, la station mobile accède au réseau pour demander un canal radio sur lequel elle peut échanger de la signalisation. Elle envoie un message « CM SERVICE REQUEST » qui précise l'identité du mobile (TMSI ou IMSI), le type de service demandés (appel départ) et quelques autres informations nécessaires.

Lé réseau peut engager la procédure d'authentification, puis activer le chiffrement. Le mobile transmet ensuite le numéro du correspondant désiré. Le MSC traite l'appel comme un appel téléphonique ordinaire. Un canal radio de trafic est alloué et le mobile est commuté sur celui-ci. Lorsque le correspondant appelé décroche, la communication est établie. La durée typique entre l'accès et la première sonnerie est de six secondes.

4.2.2. Utilisation du réseau commuté

Pour établir un appel sortant, le MSC peut transférer l'appel directement au réseau commute. Dans ce cas, le tronçon au sein du réseau commuté peut être assez

important. Si l'operateur du PLMN est un opérateur privé, il a intérêt à utiliser autant que possible son réseau GSM. Pour cela. Il peut installer des circuits de parole entre les MSC et acheminer l'appel jusqu'au MSC le plus proche du CAA de l'abonné fixe demandé. Dans ce cas l'ensemble des MSC se comporte comme un réseau téléphonique fixe et le dialogue se fait en SSUTR2 (où tout protocole équivalent). Le réseau commuté est utilisé simplement pour l'appel local.

4.3. Fin de communication

Lorsque l'abonné mobile raccroche, un message 0 cc DISCONNECT est envoyé au MSC. Le MSC génère un message de fin ou de libération conformément au protocole utilisé. Dans tous les cas, le MSC renvoie un message « CC RELEASE » vers le mobile, qui l'acquitte par un message « CC RELEASE COMPLETE ». La communication est alors terminée mais il faut libérer l'ensemble des ressources : connexions établies et ressources radio.

Dans le cas du raccroché par le réseau fixe, la procédure est similaire au cas précédent. Sur la partie fixe, le raccroche se fait conformèrent au SSUTR2 ou I'ISUP. Le raccroché sur la liaison radio se fait en trois étapes : envoi d'un message, « CC DISCONNECT » par le réseau, acquittement par le mobile à l'aide: de « cc RELEASE puis émission de « CC RELEASE COMPLETE » par le MSCNLR. L'ensemble se conclut par la libération des connexions et des ressources.

4.4. Appel entrant

4.4.1. Description

Un appel entrant est un appel d'un usager mobile ou fixe vers une MS. Nous nous restreindrons au cas d'un appel venant d'un abonné fixe. Nous désignerons par VMSC, le MSC sous la couverture duquel le mobile se trouve (Visited MSC).

Pour effectuer l'appel, l'abonné fixe compose le numéro d'abonné MSISDN de l'abonné mobile demandé. Les premiers chiffres du numéro désignent le PLMN de l'abonné appelé. L'appel est routé par les commutateurs du réseau téléphonique vers le MSC le plus proche et un circuit de parole est établi jusqu'a ce MSC. Ce dernier va agir alors en GMSC.

Le GMSC interroge le HLR de l'abonné mobile demandé pour connaitre sa localisation. Le HLR vérifie que l'abonné appelé est bien valide dans le réseau, recherche son IMSI et le VLR auprès duquel il est enregistre puis demande à ce VLR un numéro MSRN. Ce numéro, une fois alloué, est mémorisé par le VLR et retransmis au GSMC. Celui-ci peut alors établir un circuit vers le VMSC par un appel téléphonique classique en utilisant le numéro MSRN comme numéro appelé. Lorsque l'appel parvient au VMSCNLR, il peut, à partir du MSRN utilisé, retrouver l'IMSI du mobile, sa zone de localisation courante et disposer éventuellement d'un TMSI.

Le VMSC diffuse un message de paging contenant un TSMI ou l'IMSI dans les cellules de la zone de localisation. Le mobile effectue alors un accès sur la cellule courante ou il se trouve. Le BSC alloue un canal dédie pour échanger de

signalisation. Le premier message émis par la MS sur le canal dédie est le message «MM PAGING RESPONSE ». Ce message est encapsulé dans d'autres messages qui permettent d'établir les différentes connexions de façon que la MS puisse dialoguer directement avec le MSC. La procédure se poursuit par l'authentification suivie du chiffrement si ces fonctionnalités sont activées. Le message d'appel est alors transmis vers la MS. La durée d'établissement d'une communication entre la fin de la composition du numéro et le début de la sonnerie est d'environ huit seconde.

Dans le cas où l'appel provient d'un mobile, les différentes phases de l'appel départ et de l'appel arrivée sont réunies. Le MSC du mobile demandeur joue le rôle de GMSC mais les échanges de messages sont inchangés.

4.4.2. Intérêt des liaisons sémaphores

Dans les anciens réseaux radio mobiles, la signalisation sémaphore n'était pas pleinement utilisée. Le HLR de chaque abonné était physiquement placé dans le MSC ou il souscrivait son abonnement : pour tout appel venant du réseau fixe, un circuit de parole était établi depuis la centrale origine de l'appel vers le MSC/HLR de l'abonné mobile. L'abonné était alors localisé et un deuxième circuit de parole était établi vers le VMSC courant.

5. Conclusion

Dans cette partie traitant de la gestion des appels dans le système GSM. Nous avons étudié les mécanismes de base et échanges de messages ayant lieu lors d'un appel entrant ou sortant, national ou international.

La grande différence entre la procédure de traitement d'un appel entrant et celle d'un appel sortant réside en ce que la première nécessite une interrogation du HLR, et cela afin de connaitre la localisation du mobile appelé. Ainsi, la gestion de l'itinérance évoquée au début de cette séquence a pour principal objectif de permettre l'acheminement des appels entrants, c'est-à-dire de fournir une qualité de service équivalente à celle du réseau fixe. Insistons une fois de plus sur l'importance du coût engendré par la gestion itinérance. Ce coût est d'autant plus important qu'il est dû à un service en réalité peu utilisé : la majorité des appels traités par les systèmes cellulaires sont des appels sortants.