transmission de signalisation…). Le RNC répond *via* le message *RRC connection setup* en utilisant un FACH dans lequel il indique au mobile l'état RRC dans lequel il doit se placer (voir section suivante) ainsi que les *bearers* radio de signalisation (SRB) à utiliser une fois la connexion établie. Au niveau de la couche physique, UTRAN signale au mobile le canal de transport et le canal physique à utiliser en indiquant le code d'embrouillage de la voie montante ainsi que l'ensemble de formats de transport et la fréquence porteuse. De plus, en fonction de l'état RRC où le mobile devra se placer, le réseau peut lui allouer une identité RNTI pour gérer sa mobilité. L'UE acquitte l'établissement de la connexion RRC avec le message *RRC connection complete*, en utilisant un DCH, si l'UE est placé dans l'état CELL_DCH ou un RACH s'il est mis dans l'état CELL_FACH. Dans ce message, l'UE indique également au réseau ses capacités matérielles et logicielles au niveau des couches L1 et L2 – y compris le fait que le terminal soit ou non bimode (GSM et UMTS).

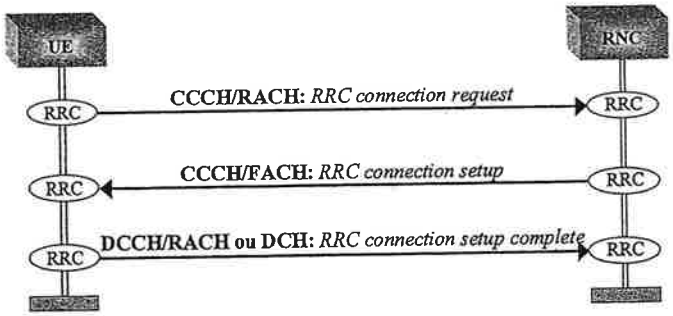


Figure 8.16. *Etablissement d'une connexion RRC*

Quant à la libération de la connexion RRC, elle est toujours commandée par la couche RRC du SRNC lorsque toutes les connexions de signalisation avec le réseau cœur sont libérées.

REMARQUE.– A un moment donné, il ne peut y avoir qu'une seule et unique connexion RRC entre l'UE et l'UTRAN et ce indépendamment d'une éventuelle inscription du terminal aux domaines CS et PS du réseau cœur.

8.8.2. *La gestion des états de service de RRC*

L'interface d'accès UMTS a été conçue pour offrir une grande flexibilité dans la gestion de la ressource radio. Cela se traduit au niveau du protocole RRC par différents états de service qui sont fonction du niveau d'activité du mobile concerné. Le principe directeur consiste à adapter à tout moment l'attribution de ressources radio à un mobile à ses besoins en trafic. La figure 8.17 présente les différents états de service du protocole RRC. Suivant qu'il y a ou non une connexion RRC, le mobile peut opérer selon deux modes :

– le mode veille (*Idle mode*). Il n'y a alors pas de connexion RRC entre l'UE et l'UTRAN ;

– le mode connecté. L'UE a établi une connexion RRC avec l'UTRAN. Le mode connecté est subdivisé en quatre états : CELL_DCH, CELL_FACH, CELL_PCH et URA_PCH.

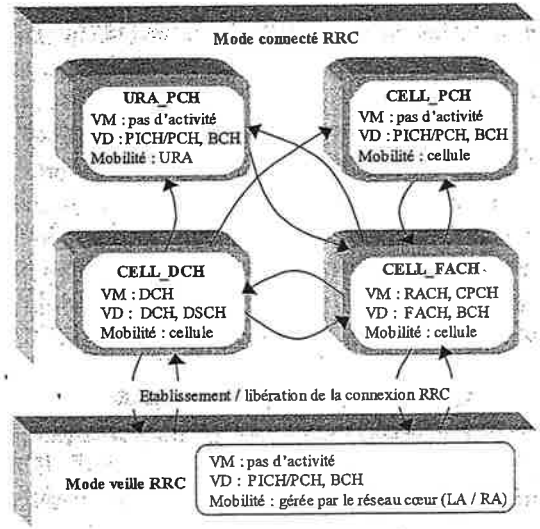


Figure 8.17. *Etats de service du protocole RRC : mobilité et canaux de transport impliqués*

Etat CELL_DCH

L'état CELL_DCH est caractérisé par l'attribution de ressources radio dédiées (un ou plusieurs canaux de transport de type DCH ou DSCH) à l'UE qui rentre dans cet état lors d'une connexion RRC ou en établissant un canal physique dédié dans l'état CELL_FACH. Les ressources dédiées sont utilisées pour un trafic de type temps réel ou pour le transfert d'une grande quantité de données utilisateur en mode paquet. L'UE reçoit aussi des messages RRC transmis sur le DCCH et, si les caractéristiques techniques du terminal le permettent, sur le BCCH. Toujours en fonction des caractéristiques du terminal, des messages d'information système peuvent être reçus *via* le FACH. La transition vers les états CELL_FACH, CELL_PCH et URA_DCH est déclenchée à travers les messages de signalisation échangés entre le réseau et l'UE. Par exemple, pour des appels en mode paquet, si les échanges de données usager sont interrompus momentanément, l'UTRAN peut demander à l'UE de passer aux états CELL_PCH ou URA_PCH. Après la libération de la connexion RRC, l'UE passe automatiquement en mode veille RRC.

Etat CELL_FACH

Dans l'état CELL_FACH, aucune ressource radio dédiée n'est attribuée à l'UE et sa mobilité est gérée au niveau cellule. Ce sont les canaux communs de transport RACH, FACH, CPCH qui sont utilisés pour les transferts entre l'UE et l'UTRAN. Cet état est adapté pour le transfert de données de petite taille sans contraintes temps réel ainsi que pour l'échange de signalisation. De plus, l'UE écoute des informations système ainsi que des messages RRC véhiculés par le BCCH, CCCH et DCCH. L'UE passe aux états CELL_PCH et URA_PCH suite à un ordre explicite de l'UTRAN. Après la fin de la connexion RRC, l'UE peut revenir à l'état veille RRC.

Etats CELL_PCH et URA_PCH

Les états CELL_PCH et URA_PCH sont des états de repos du protocole RRC en mode connecté où aucune activité dans la voie montante est présente. La transition vers ces états est commandée par l'UTRAN après, par exemple, le constat de l'absence de trafic usager prolongée. Dans ces états, l'UE est en mode de réception discontinue (DRX pour *Discontinous Reception*), son activité principale consistant en la surveillance du PICH/PCH et en la gestion de sa mobilité décrite dans les paragraphes suivants.

Avant toute reprise de trafic usager, RRC doit repasser par l'état CELL_FACH et effectuer une mise à jour de localisation dans l'UTRAN (procédures *Cell Update* ou *URA Update*). En effet, dans l'état CELL_PCH ou URA_PCH :

– lorsque du trafic usager descendant est présenté à l'UTRAN, celui-ci envoie un message de *paging* à l'UE pour lui commander de passer dans l'état CELL_FACH pour la reprise de trafic ; l'UE passe alors dans l'état CELL_FACH, lance la procédure *Cell Update* sachant que l'élément déclencheur la réponse à un *paging*, après quoi le trafic usager pourra reprendre,

– pour du trafic montant, la couche RRC de l'UE passe dans l'état CELL_FACH, lance la procédure de *Cell Update*, la raison avancée étant la reprise de trafic sur la voie montante, et lorsque cette procédure est réalisée avec succès, le trafic usager reprend.

La principale différence entre les états CELL_PCH et URA_PCH est que la position de l'UE est connue au niveau cellule pour le premier et au niveau d'un groupe de cellules URA pour le second ; le passage de l'état CELL_PCH à l'état URA_PCH permet de réduire la fréquence des mises à jour de localisation qui seront alors effectuées par l'UE à chaque changement d'URA au lieu de chaque changement de cellule. On comprend aisément l'intérêt de l'état URA_PCH dans le cas d'un UE en mode connecté sans trafic et se déplaçant rapidement dans une zone comportant des cellules de petite taille. Cet intérêt n'est toutefois effectif que lorsque chaque zone URA couvre plusieurs cellules.

Il faut noter qu'il n'y a pas de transition directe entre le mode veille et les états CELL_PCH et URA_PCH. Lorsque l'UE quitte le mode veille, il passe dans l'état CELL_DCH ou l'état CELL_FACH en fonction de la nature dédiée ou non des ressources qui lui sont allouées lors de l'établissement de la connexion RRC.

8.8.3. *La diffusion des informations système*

Les informations système sont un ensemble de données provenant du réseau cœur ou générées par l'UTRAN, le tout étant diffusé par la partie RRC du nœud B dans chaque cellule du réseau. Ces informations permettent à un UE d'identifier les cellules, de prendre connaissance de l'environnement cellulaire et de recevoir l'ensemble des paramètres permettant d'utiliser les ressources communes dans une cellule. Elles constituent en quelque sorte l'œil par lequel l'UE voit un réseau.

Définition de SIB et de MIB

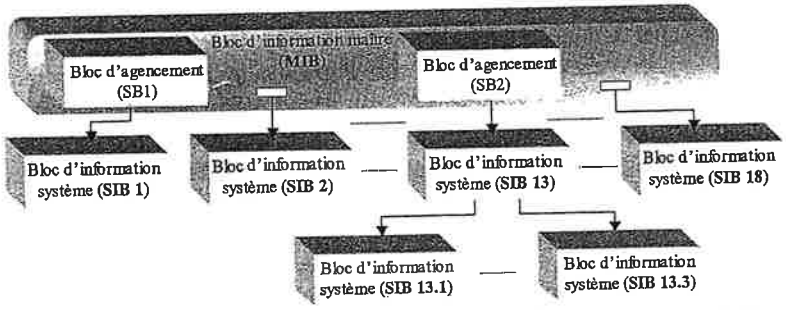
Les informations système sont organisées en blocs (SIB pour *System Information Block*) contenant chacun des informations de même nature. Les SIB sont transmis dans un message RRC *System Information* de taille fixe qui peut transporter un segment de SIB ou plusieurs SIB concaténés. La segmentation ou la concaténation des SIB est réalisée par la couche RRC de l'UTRAN en fonction de la taille des SIB par rapport à la capacité du canal de transport qui les convoie. A la réception, la couche RRC de l'UE réalise le cas échéant l'opération inverse qui est l'assemblage des segments de SIB ou la déconcaténation. Le message *System Information* est transmis sur le canal logique BCCH qui, pour la plupart des SIB, est supporté par le canal de transport BCH associé au canal physique P-CCPCH. La seule exception est le SIB 10, qui contient les paramètres de contrôle pour la fonction DRAC.

Les informations système sont diffusées périodiquement et continuellement pour permettre à tout mobile qui vient d'être mis sous tension de trouver rapidement ses marques. Cette phase passée, ce serait onéreux, en termes d'énergie, de lire les informations au rythme de leur diffusion, alors que le rythme de leur modification est plus faible. Le mécanisme utilisé par l'UTRAN pour éviter aux mobiles ce gaspillage d'énergie consiste à leur envoyer un message d'alerte à chaque fois que les informations système sont modifiées. Cela leur permet de ne surveiller que les messages d'alerte. Les mobiles, dans le mode veille ou les états CELL_PCH et URA_PCH, sont alertés à l'aide d'un message de *paging*. Les mobiles dans l'état CELL_FACH reçoivent quant à eux sur le canal FACH le message RRC *System Information Change Indication.*

La figure 8.18 illustre la structure arborescente de diffusion des informations système ainsi que l'information contenue dans chaque SIB. On distingue trois types de blocs. Le bloc d'information maître MIB (*Master Information Block*) contient les

informations de notification de modification (*tag*) et celles de localisation temporelle des blocs à lire. Le MIB est essentiel attendu que, sans son décodage, aucun autre bloc ne pourra être lu. Les informations de modification et de localisation transportées dans le MIB sont relatives à des SIB ou à des blocs d'informations d'agencement SB (SB *Scheduling Block*). Jusqu'à deux blocs d'information d'agencement peuvent être inclus dans le MIB.

En plus des références aux SIB et aux SB, le MIB contient un élément d'information *MIB value tag* permettant de signifier une modification des informations système, et un élément d'information *PLMN type* dont la valeur (GSM-MAP ou ANSI-41) désigne le type de PLMN. Une référence à un SIB ou à un SB est composée de l'information sur le type de bloc concerné (SIB ou SB) ; de la notification de modification ou non du bloc, et des informations de localisation temporelle du bloc. Ces informations concernent le nombre de segments SEG_COUNT composant le bloc, la position SIB_POS(0) du premier segment dans le cycle d'horloge système de la cellule SFN (*Cell System Frame Number*), la période de répétition SIB_REP (en nombre de trames) du bloc et de tous les segments le constituant, et enfin pour chaque segment suivant le premier, la valeur SIB_OFF (en nombre de trames) de l'offset par rapport au segment précédent.



SIB1 : Information sur des procédures NAS et sur des compteurs à utiliser par l'UE en mode veille et en mode connecté
SIB2 : Identité de l'URA courante
SIB3 et SIB4: Paramètres nécessaires à la sélection et la resélection de cellule
SIB5 et SIB6 : Information sur la configuration des canaux physiques communs et partagés dans la cellule (PRACH, PDSCH...)
SIB7 et SIB8/SIB9 : Paramètres impliqués dans les procédures du RACH et du CPCH, respectivement
SIB10 : Paramètres associés à la procédure DRAC
SIB11 et SIB12 : Information associée au prélèvement de mesures intra-fréquence, inter-fréquence et inter-RAT
SIB13 : Information liée au réseau cœur américain ANSI-41
SIB14 et SIB17 : Information propre au mode UTRA/TDD
SIB 15 : Paramètres associés aux techniques de géolocalisation
SIB 16 : Paramètres sur des configurations préétablies des *bearers* radio utilisés lors d'un *handover* intersystème
SIB 18 : Contient les identités des PLMN des cellules voisines (PLMN équivalents)

Figure 8.18. *Structure arborescente de diffusion des informations système et contenu des SIB*

Le système de datation est fondé sur l'horloge système de la cellule dont la période est de 4.096 trames, la valeur du SFN variant de 0 à 4.095. Les valeurs des paramètres d'agencement SIB_POS, SIB_REP et SIB_OFF du MIB sont prédéfinies pour faciliter sa localisation, et sont respectivement égales à 0, 8 et 2. Cela signifie que le MIB est diffusé à partir de la SFN 0 avec une répétition toutes les 80 ms.

Les blocs d'informations d'agencement SB contiennent des références à des blocs d'information système SIB. Ils sont des relais du MIB et ne contiennent que des références à des SIB, pas de références à d'autres SB.

8.8.4. *La gestion du* paging

A chaque fois que l'UTRAN souhaite alerter le mobile, il lui envoie un message RRC de *paging* de type 1 (*paging type 1*) ou de type 2 (*paging type 2*) selon l'état de service courant du protocole RRC.

Le message *paging type 1*, transmis sur le canal logique PCCH, est utilisé dans le mode veille ou dans les états CELL_PCH et URA_PCH du mode connecté pour notifier au mobile l'arrivée d'un appel entrant ou la modification des informations système diffusées dans la cellule courante ou encore pour commander au mobile de passer dans l'état CELL_FACH lorsqu'il est dans l'état CELL_PCH ou URA_PCH et que l'UTRAN a reçu du trafic descendant qui lui est destiné.

Le *paging type 2*, encore appelé *paging* dédié (*Dedicated paging*), est utilisé dans les états CELL_FACH et CELL_DCH pour notifier au mobile l'arrivée d'un appel entrant. Le message *paging type 2* est transmis sur un canal logique dédié DCCH supporté par un canal de transport de type FACH ou DCH.

Lorsque la couche RRC du mobile reçoit un message de *paging*, son comportement est fonction de la cause de l'alerte :

– si le *paging* a été déclenché par le réseau cœur, RRC informe la couche supérieure avec indication de la cause du *paging* et du domaine de service concerné ;

– s'il s'agit d'une notification de modification des informations système, alors RRC engage la lecture du canal BCH pour la mise à jour des informations modifiées ;

– dans le cas d'une commande de passage dans l'état CELL_FACH, RRC lance la procédure *Cell Update*.

8.8.5. *La sélection et la resélection de cellule*

C'est la première opération effectuée par la couche RRC d'un UE lors de sa mise sous tension. En effet, dès qu'un mobile contenant une USIM valide est mis sous tension, les couches du NAS sélectionnent un PLMN et demandent à RRC de sélectionner une cellule convenable appartenant à ce PLMN. La sélection de cellule

est également effectuée lorsqu'un UE repasse en mode veille suite à la libération d'une connexion RRC. Une fois la sélection de cellule effectuée, un UE en mode veille ou dans les états CELL_FACH, CELL_PCH ou URA_PCH, continue de surveiller le paysage radio pour rechercher régulièrement la meilleure cellule selon des critères définis. A chaque fois qu'une cellule plus adéquate est détectée, elle est substituée à celle précédemment sélectionnée. C'est ce que l'on appelle la resélection de cellule. Les procédures de sélection et de resélection de cellule sont étudiées en détail dans le chapitre 13.

8.8.6. *La gestion de la mobilité dans l'UTRAN*

Les types de procédures mis en œuvre pour la gestion de la mobilité dans l'UTRAN sont fonction de l'état dans lequel se trouve le protocole RRC. On peut en effet distinguer trois cas :

– le mode veille ;

– les états URA_PCH, CELL_PCH et CELL_FACH ;

– l'état CELL_DCH.

La mobilité dans le mode veille

Dans le mode veille RRC, l'UTRAN ignore la présence du terminal. Si l'UE est inscrit au domaine CS et/ou au domaine PS, sa mobilité est gérée exclusivement par le réseau cœur à l'aide des identités TMSI et/ou P-TMSI, respectivement. Une fois inscrit au domaine CS et/ou PS, l'UE surveille le PCH (*via* le PICH) de la cellule courante pour savoir s'il y a des appels entrants et pour savoir si les informations système ont changé. Pour ce faire, l'UE se sert de la technique DRX pour réaliser des économies de l'énergie. Dans ce mode, la gestion de la mobilité dans l'UTRAN se réduit à la procédure de resélection de cellule et à sa préparation par la surveillance des cellules voisines. Comme déjà souligné précédemment, l'UTRAN fixe les règles du jeu en diffusant dans chaque cellule des informations système dont celles relatives à la resélection de cellule (liste des cellules voisines à surveiller, informations sur les mesures à effectuer, critères de resélection…). La procédure de resélection de cellule est effectuée par l'UE de manière autonome.

La mobilité dans les états URA_PCH, CELL_PCH et CELL_FACH

Dans ces états, l'UE est connecté à l'UTRAN et possède un identificateur temporaire : U-RNTI en URA_PCH et C-RNTI en CELL_PCH et CELL_FACH. Ici aussi, le déclenchement des procédures utilisées dans la gestion de la mobilité est réalisé à l'initiative de l'UE. A la base, on a toujours la resélection de cellule qui se déroule de la même manière que le cas du mode veille, avec l'utilisation d'informations système, éventuellement différentes.

En plus de la resélection de cellule, la mise à jour de la localisation du mobile est également gérée dans ces états de la manière suivante :

– après une resélection de cellule dans l'état CELL_FACH, la procédure *Cell Update* est lancée par la couche RRC du mobile pour assurer sa localisation au niveau cellule ;

– si la resélection s'est déroulée dans l'état CELL_PCH, RRC passe dans l'état CELL_FACH et exécute la procédure *Cell Update*, puis repasse dans l'état CELL_PCH si ni le mobile, ni l'UTRAN n'a de données usager à transmettre ;

– dans le cas d'une resélection de cellule dans l'état URA_PCH, la couche RRC du mobile procède à une mise à jour de zone de localisation URA (procédure *URA Update*) si la nouvelle cellule se trouve dans une nouvelle URA, ce qui assure que le mobile soit toujours connu par l'UTRAN au niveau URA. Pour effectuer cette procédure, l'UE doit rentrer dans l'état CELL_FACH puis revenir dans l'état URA_PCH si ni le mobile, ni l'UTRAN n'ont de données usager à transmettre.

Dans tous ces cas, si la nouvelle cellule se trouve dans un nouveau RNS, l'UTRAN peut ré-attribuer au mobile un nouvel identificateur temporaire U-RNTI, notamment lorsque la procédure de mise à jour de localisation a entraîné une relocalisation de SRNS (voir chapitre 9).

La mobilité dans l'état CELL_DCH

Dans l'état CELL_DCH, le mobile est connu à la cellule près. La mobilité dans l'UTRAN est contrôlée par la couche RRC du SRNC, qui, à partir des résultats de mesures qui lui sont fournis par le mobile et sa connaissance de la topologie du réseau d'accès, peut procéder à un *soft-handover* ou un *hard-handover*.

Le *soft-handover* est exécuté à l'aide d'une procédure appelée *Active Set Update* et qui permet de mettre à jour le groupe de liens radio (*active set*) qui supporte le trafic entre le mobile et le réseau dans une situation de macrodiversité. Ce type de *handover* est qualifié de *soft* puisqu'il consiste à retirer, rajouter ou remplacer des liens tout en assurant qu'à tout moment il y a au moins un lien actif. La figure 8.19 illustre le déroulement de la procédure de *soft-handover*.

Dans le cas du *hard-handover*, il y a pendant un instant donné la rupture totale du lien radio dédié entre l'UE et l'UTRAN. Cela peut être dû au fait que le *handover* est du type interfréquence ou intersystème ou simplement que le réseau ne supporte pas le *soft-handover*. Le *hard-handover* est réalisé avec les procédures RRC de reconfiguration des ressources radio. Le chapitre 13 étudie plus en détail les principes des procédures de *soft-* et de *hard-handover*.

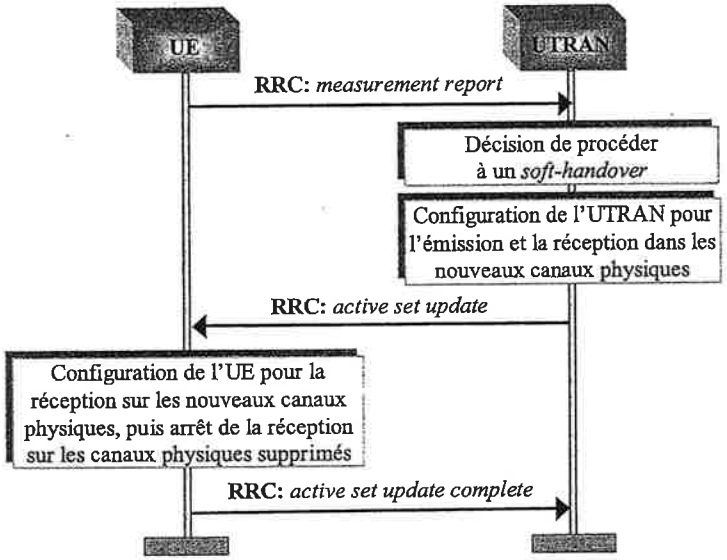


Figure 8.19. *Procédure de* soft-handover

La mobilité intersystème

Pour un mobile supportant d'autres technologies d'accès radio (RAT pour *Radio Access Technology*), RRC gère également les transitions d'état vers ou à partir de ces autres systèmes. La figure 8.20 présente les transitions d'états entre l'UTRA et le GSM. Cette figure illustre le fait que le passage direct du mode connecté UTRA vers le mode connecté GSM (et *vice versa*) est possible, alors que dans le cas du mode connecté UTRA et du mode transfert GPRS (c'est-à-dire lorsqu'un transfert de paquets est en cours), il y a toujours passage par le mode veille. Ceci est dû au fait que la mobilité sur l'interface radio dans le cas du GPRS repose sur la procédure de resélection, ce qui explique d'ailleurs les limites du GPRS quant au support de service temps réel, puisque la resélection peut durer quelques secondes et entraîne une perte importante d'information.

La resélection de cellule et le *handover* vers ou à partir de l'autre système sont possibles grâce à des mesures sur des cellules appartenant à l'autre système effectuées par le mobile (cf. chapitre 13). La norme permet cependant d'effectuer un *handover* intersystème sans mesures préalables. C'est ce que l'on appelle le *handover* aveugle (*blind handover*). Il faut noter également que la resélection intersystème peut être ordonnée par le réseau : procédure *Inter-RAT cell change order from UTRAN* (UTRAN → GPRS) et procédure *Inter-RAT cell change order to UTRAN* (GPRS → UTRAN).

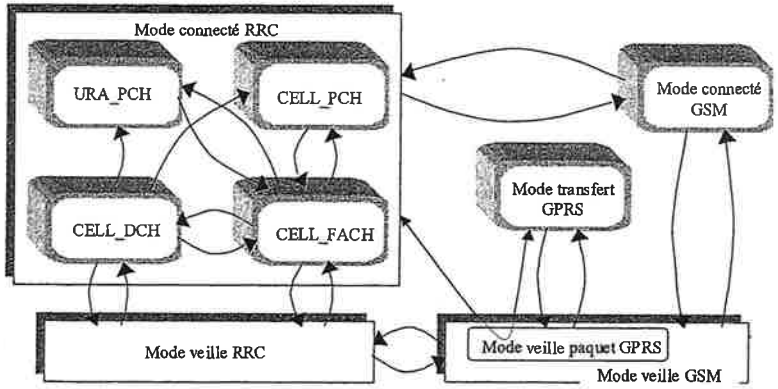


Figure 8.20. *Transition d'états entre l'UTRA et le GSM/GPRS*

8.8.7. *La gestion des* bearers *radio*

La radio est une ressource rare, la technologie d'accès CDMA est très sensible aux interférences. Or l'une des exigences fondamentales du cahier des charges de spécification du système UMTS était qu'il soit capable de fournir des services support les plus variés, configurables dynamiquement au cours d'une communication. C'est pourquoi le système a été conçu pour une gestion très flexible des ressources.

Etablissement d'un bearer *radio*

Sur le plan usager de l'interface radio, un *bearer* radio est en fait constitué d'un empilement des ressources mobilisées dans les différentes couches de protocole (canaux physiques, canaux de transport, entités RLC et entités PDCP). Il peut être vu comme la composante d'un *radio access bearer*, lequel définit un chemin de transport complet entre l'UE et le réseau cœur (cf. chapitre 5). Son établissement permet de créer un « tuyau » par lequel seront acheminées les données usagers échangées entre le mobile et l'UTRAN. Comme illustré par la figure 8.21, le message RRC *Radio bearer setup* est envoyé par le RNC au mobile. Dans ce message, la couche RRC du RNC donne des instructions à la couche RRC de l'UE pour que cette dernière configure les couches PDCP (service paquet), RLC, MAC et physique de sorte à supporter la QoS requise par le service demandé. Au niveau de la couche physique, cela concerne le type de canal de transport à utiliser (DCH ou RACH/FACH), l'ensemble de combinaisons des formats de transport (TFCS), le code d'embrouillage à utiliser dans la voie montante, la fréquence porteuse, etc. L'UE acquitte la demande d'établissement d'un *bearer* radio par le message RRC *Radio bearer setup complete*.

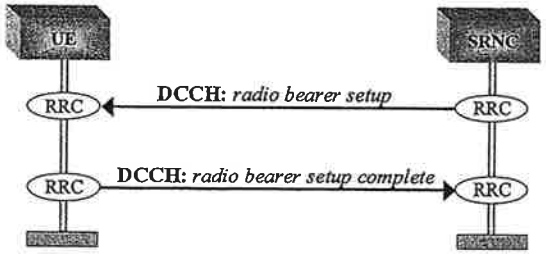


Figure 8.21. *Etablissement d'un* bearer *radio*

Les bearers *radio de signalisation*

Dans le plan de contrôle, les messages générés par RRC sont convoyés à l'aide de cinq supports radio spécifiques appelés *bearers* radio de signalisation (SRB pour *Signalling Radio Bearer*). Leur configuration est préétablie et résumée dans le tableau 8.5. En plus de la signalisation générée par RRC, ces supports sont également utilisés pour le transport de messages de signalisation NAS et des messages SMS suivant différents niveaux de priorité.

RAB de signalisation	Canal logique	Mode RLC	Utilisation (plan de contrôle)
SRB0	CCCH	VM: transparent VD: non acquitté	Transmission de messages RRC
SRB1	DCCH	non acquitté	Transmission de messages RRC
SRB2	DCCH	acquitté	Transmission de messages RRC
SRB3	DCCH	acquitté	Transmission de messages NAS avec priorité haute
SRB4	DCCH	acquitté	Transmission de messages NAS avec priorité basse (messages SMS)

Tableau 8.5. *Caractéristiques des* bearers *radio de signalisation*

Exemple de multiplexage des bearers *radio dans la voie descendante*

On considère l'exemple de la figure 8.22 où un utilisateur télécharge une page Internet en même temps qu'il reçoit des messages de signalisation du réseau cœur et de l'UTRAN. Pour ce faire, on suppose qu'un *bearer* de données et quatre *bearers* de signalisation sont mis en place par l'UTRAN. Les messages de signalisation provenant de l'UTRAN sont acheminés jusqu'à l'UE à l'aide d'un SRB1 et d'un SRB2 alors que ceux issus du réseau cœur peuvent faire appel à un SRB3 et un SRB4. Pour le transfert des données usager, l'UTRAN se sert d'un *bearer* radio de

type interactif. Les quatre *bearers* de signalisation utilisent chacun un canal logique DCCH. RLC opère en mode non acquitté dans le SRB1 et ajoute un en-tête de 8 bits alors que dans les SRB2, SRB3 et SRB4, RLC opère en mode acquitté et l'en-tête est de 6 bits. MAC multiplexe ces quatre canaux logiques en un seul canal de transport DCH. Ceci est indiqué au récepteur de l'UE à l'aide des 4 bits d'en-tête MAC. Par ailleurs, le canal logique du *bearer* radio est un DTCH et RLC opère en mode acquitté avec un en-tête de 16 bits. MAC ne faisant pas de traitement particulier, aucun en-tête n'est ajouté. Le *bearer* radio est associé à un DCH dans la couche physique lequel est multiplexé dans un seul canal physique dédié (DPCH).

Reconfiguration et libération de ressources radio

Lorsque de multiples *bearers* radio sont impliqués dans une communication (par exemple, naviguer sur Internet au même temps que l'on fait de la visiophonie), il est possible d'en libérer certains au besoin à l'aide du message *Radio bearer release*. De la même manière, il est possible de modifier la QoS des *bearers* radio courants grâce aux messages RRC de reconfiguration des ressources : *Radio bearer reconfiguration*, *Transport channel reconfiguration* et *Physical channel reconfiguration*. Du fait de la relation de dépendance entre les types de ressources des différentes couches (un canal de transport commun par exemple est forcément supporté par un canal physique commun), la reconfiguration des ressources d'une couche peut entraîner celle des ressources d'autres couches. Mais comme leurs noms ne l'indiquent pas, chacune de ces procédures peut assurer la reconfiguration de toutes les couches. Par exemple, la procédure *Transport channel reconfiguration* peut inclure la reconfiguration des canaux physiques et des entités RLC et PDCP.

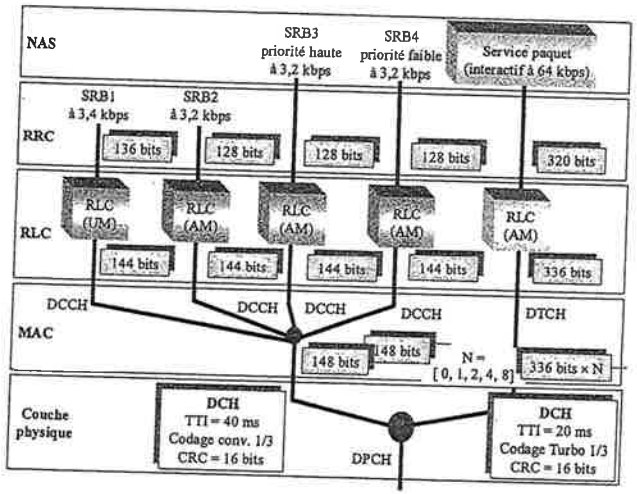


Figure 8.22. *Exemple qu'illustre la matérialisation d'un* bearer *radio de données (service paquet interactif) et sont multiplexage avec quatre* bearers *radio de signalisation*

La configuration et la libération des ressources est toujours commandée par le réseau et l'UE doit toujours envoyer en réponse un message de complétude dans le cas d'une configuration avec succès, ou un message d'erreur le cas échéant. La figure 8.23 est un exemple générique du déroulement d'une procédure de reconfiguration de ressources. Lorsque la couche physique est concernée par la reconfiguration, l'UTRAN configure d'abord sa couche physique afin de commencer à émettre et recevoir sur le nouveau canal physique, puis envoie le message de commande de reconfiguration correspondant à l'UE.

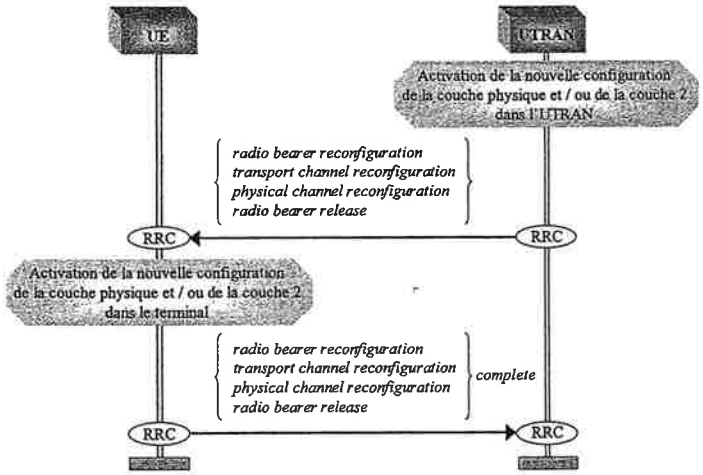


Figure 8.23. *Schématisation générique du déroulement d'une procédure de reconfiguration de ressources radio*

8.8.8. *Le contrôle des mesures*

La gestion des mesures est une fonction fondamentale du système, dans la mesure où la réalisation d'autres fonctions telles que la gestion de la mobilité dans l'UTRAN et la reconfiguration des *bearers* radio peut reposer dans la pratique sur des résultats de mesures. La norme UMTS a défini plusieurs types de mesures à effectuer et à rapporter à l'UTRAN par l'UE. Cet aspect est largement étudié dans le chapitre 13. On pourra distinguer, par exemple :

– les mesures de puissance de réception sur la cellule courante et les cellules voisines, utilisées par l'UE pour la gestion de la sélection et resélection de cellules et par l'UTRAN pour la gestion du *handover* ;

– les mesures de trafic sortant sur les canaux de transport du mobile. Le résultat de ces mesures permet à l'UTRAN de détecter la nécessité de reconfigurer les ressources attribuées à un mobile. Par exemple, lorsqu'un mobile qui transmet sur le

canal RACH rapporte des résultats de mesures indiquant que le seuil supérieur de remplissage de la mémoire de transmission est atteint, l'UTRAN peut procéder à une reconfiguration en lui attribuant des ressources dédiées (DCH) ;

– les mesures de qualité, fondées sur le BLER qui permettent de surveiller et de gérer la QoS.

8.8.9. *La gestion du chiffrement et de l'intégrité*

Le chiffrement et l'intégrité sont des fonctions essentielles pour la sécurité des échanges sur l'interface radio. La première assure la confidentialité des échanges et la seconde, qui est une nouveauté par rapport au GSM, permet l'authentification de l'origine des messages de signalisation. Ce sont des fonctions exécutées dans l'*access stratum*. Le chiffrement est effectué dans la couche RLC lorsque celle-ci opère en mode non transparent et dans la couche MAC dans le cas contraire. Quant à l'intégrité, elle est à la charge de RRC. Dans les deux cas, leur mise en œuvre est commandée par le réseau cœur (cf. chapitre 9).

La procédure *Security mode control*, illustrée par la figure 8.24 permet de démarrer ou de modifier le chiffrement ou l'intégrité. Elle est également utilisée pour arrêter le chiffrement. Sur réception d'une commande de configuration de la sécurité pour un domaine de service donné (circuit ou paquet), l'UTRAN envoie à l'UE un message RRC *Security Mode Command*, avec entre autres, les algorithmes d'intégrité (UIA) et de chiffrement (UEA) à utiliser ainsi que le paramètre FRESH. Si la configuration transportée par ce message n'est pas acceptable par l'UE, parce qu'elle est, par exemple, incompatible avec ses capacités logicielles et matérielles, le mobile retourne au réseau une réponse négative RRC *Security Mode Failure*. Si le message est acceptable, alors l'UE le prend en compte et acquitte positivement la commande à l'aide d'un message RRC *Security Mode Complete*.

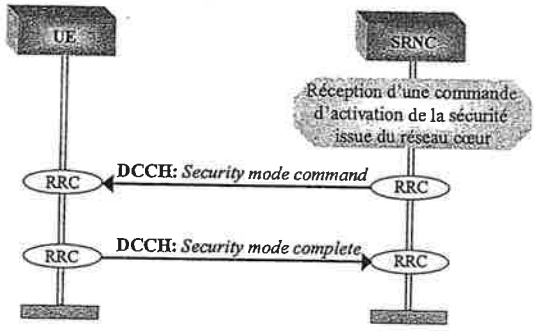


Figure 8.24. *Procédure* Security mode control

Processus de chiffrement et d'intégrité

Le processus de chiffrement (voir figure 8.25a) s'applique indépendamment à chacun des *bearers* radio et de signalisation actifs. Il implique l'utilisation de l'algorithme f8 qui reçoit en entrée la clef de chiffrement CK (cf. chapitre 9), le paramètre dynamique COUNT-C qui est incrémenté pour chaque message, l'identité du *bearer* radio BEARER, la direction de la transmission DIRECTION (voie montante ou descendante) et la taille du bloc de chiffrement LENGTH. En sortie, le bloc de chiffrement est appliqué bit à bit au message de données à transmettre. L'opération inverse est effectuée en réception pour déchiffrer le message.

En ce qui concerne le mécanisme d'intégrité (voir figure 8.25b), il s'applique indépendamment à chacun des *bearers* radio de signalisation actifs. Il est fondé sur l'algorithme f9 qui reçoit en entrée la clef d'intégrité IK (cf. chapitre 9), le paramètre COUNT-I qui est fonction du numéro de séquence RRC, le paramètre aléatoire FRESH généré par RNC, le bit de direction DIRECTION et le message de signalisation lui-même MESSAGE qui contient l'identité du *bearer* de signalisation. En sortie, on obtient le message d'intégrité MAC-I (*Message Authentication Code*) lequel est simplement attaché au message de signalisation RRC. En réception, il faudra générer le message d'intégrité XMAC-I (*eXpected MAC*) de la même manière qu'en émission. Si XMAC-I et MAC-I sont différents, l'UE considère que le message a été altéré et il ne le prend pas en compte.

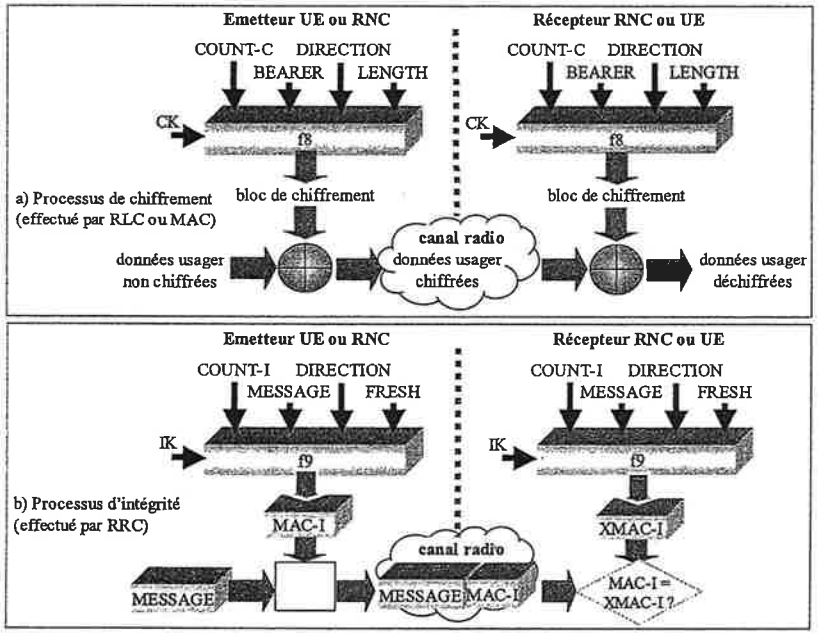


Figure 8.25. *Illustration des processus de chiffrement et d'intégrité sur l'interface radio*

8.8.10. *Le contrôle de puissance en boucle externe*

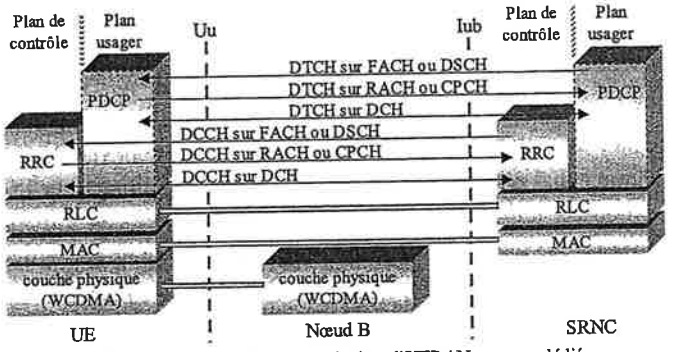
Le contrôle de puissance en boucle externe est utilisé par RRC pour fixer la valeur cible du contrôle de puissance en boucle interne exécuté par la couche physique. Il s'agit plus d'un contrôle de qualité que d'un contrôle de puissance. En effet, pour chaque canal physique de la voie descendante utilisé pour le contrôle de puissance en boucle interne, l'UE fixe un niveau cible du rapport signal à interférence SIR. Ce niveau de SIR est positionné à une valeur permettant d'assurer un niveau de taux d'erreur fixé par le réseau associé à la configuration des canaux de transport. Pour des canaux de type DCH, le taux d'erreur BLER sur les blocs de transport DCH est généralement utilisé. Dans le cas de l'utilisation du CPCH sur la voie montante, c'est le taux d'erreur binaire BER (*Bit Error Rate*) du canal physique DPCCH descendant associé qui est utilisé pour le contrôle de qualité. Le chapitre 11 donne plus de détails sur le principe du contrôle de puissance en boucle externe.

8.8.11. *Distribution des protocoles radio dans l'UTRAN*

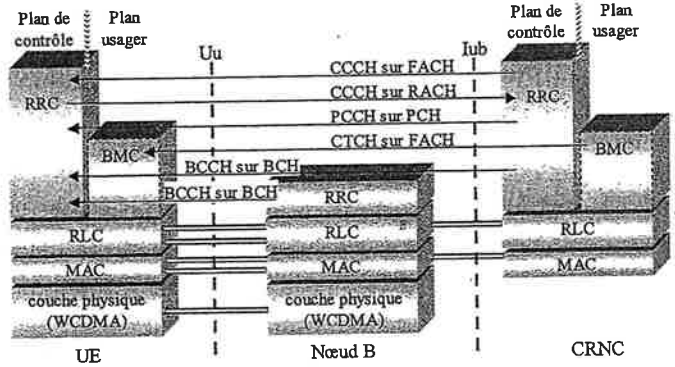
D'une manière générale, la couche physique des protocoles radio n'est présente que dans l'UE et dans le nœud B. Ceci se justifie par le besoin d'une grande réactivité dans des procédures telles que le contrôle de puissance en boucle fermée, la diversité en émission et la macrodiversité. Pour les autres couches, cela dépend du type de canal logique et de transport qu'ils soient dédiés ou communs ; de trafic ou de contrôle (cf. figure 8.26).

Distribution des protocoles pour les canaux dédiés. Un canal dédié n'est établi que lorsqu'il existe une connexion RRC. Or, une telle connexion est toujours gérée par le RNC dans son rôle de RNC serveur (SRNC), ce qui implique que les couches RRC, RLC, MAC, PDCP et BMC soient localisées dans le RNC et dans l'UE.

Distribution des protocoles pour les canaux communs. La gestion de ces canaux, mise en place indépendamment de l'existence ou non d'une connexion RRC, est à la charge d'un RNC contrôleur (CRNC). Une exception est faite pour le canal de transport BCH qui nécessite qu'une partie fonctionnelle des couches MAC, RLC et RRC soit située dans le nœud B. Les fonctions en question sont associées à la diffusion des informations système dans une cellule car la distance qui sépare les nœuds B du RNC peut être importante et causer des retards dans la diffusion de certaines de ces informations.



a) Distribution des protocoles radio dans l'UTRAN : canaux dédiés



b) Distribution des protocoles radio dans l'UTRAN : canaux communs

Figure 8.26. *Distribution des protocoles radio dans l'UTRAN. Les couches en pointillés peuvent ou non être présentes suivant le type de service courant dans le plan usager*

Chapitre 9

La gestion des appels et de la mobilité

9.1. Introduction

Dans un réseau filaire de télécommunication, l'équipement usager (par exemple l'appareil téléphonique) est relié de manière permanente au réseau par un point fixe. L'abonné ou plus exactement la prise d'abonné, est localisé et attaché au réseau de manière permanente. Pour passer un appel, l'abonné prend la ligne (décroché du combiné) et compose le numéro du correspondant à appeler. La liaison peut être dans deux états principaux :

– l'état d'attente d'appel (entrant ou sortant), lorsque aucun appel n'est établi,

– l'état connecté, lorsqu'une communication est en cours.

Le cas d'un réseau mobile de type UMTS est plus complexe pour les raisons suivantes :

– l'équipement usager n'est pas lié en permanence au réseau et n'est pas localisé de manière absolue : il peut être éteint ou dans une zone non couverte par un réseau où il est autorisé à passer des appels ;

– l'équipement usager est mobile et a besoin, pour pouvoir être joint à tout moment, de mettre à jour sa localisation à chaque fois qu'elle change. La localisation du mobile par le réseau se fait à deux niveaux : dans l'UTRAN et dans le réseau cœur. Il peut être localisé ou non dans chacun de ces domaines ;

– une zone géographique peut être couverte par les réseaux mobiles de plusieurs opérateurs différents et dans ce cas, l'équipement usager qui se trouve dans cette zone doit procéder à une sélection du réseau auprès duquel il doit s'inscrire. Le réseau, à son tour, doit contrôler l'admission des équipements tentant de s'attacher à lui. Ce contrôle inclut l'identification et l'authentification de l'équipement usager.

Il apparaît, à partir des éléments ci-dessus, que passer un appel avec un équipement mobile n'est pas aussi immédiat que le cas d'un réseau filaire. La possibilité d'établissement d'appel est soumise à un ensemble de conditions préalables :

– la sélection avec succès d'un réseau ;

– l'inscription avec succès auprès du réseau sélectionné ;

– la maintenance de la localisation de l'équipement usager.

Ces fonctions, ainsi que les appels proprement dits, sont gérés par le *non access stratum* (NAS) dont l'architecture en couche est représentée dans la figure 9.1.

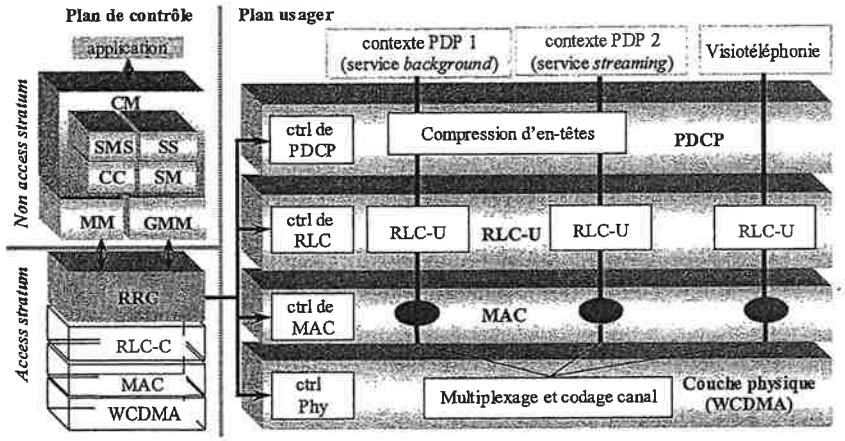


Figure 9.1. *Exemple qui montre la localisation des protocoles du* non access stratum *dans le plan de contrôle. Dans et exemple, trois* bearers *radio sont actifs dans le plan usager*

La signalisation entre un mobile et le réseau est assurée par trois sous-couches de protocoles constituant la couche 3 du système :

– la sous-couche RRC, déjà présentée dans le chapitre 8, gère la signalisation sur l'interface radio et assure un transport sécurisé des messages de signalisation des sous-couches supérieures ;

– la sous-couche MM (*Mobility Management*) gère toutes les fonctions liées à la mobilité au regard du réseau cœur (sélection de PLMN, inscription auprès du réseau, mise à jour de localisation, etc.). Elle est constituée des deux entités protocolaires MM et GMM (*GPRS Mobility Management*) dédiées respectivement à la gestion de la mobilité pour les domaines de service circuit et paquet ;

– la sous-couche CM (*Connection Management*) gère les connexions de service ; elle est composée des quatre entités CC (*Connection Control*), SM (*Session Management*), SS (*Supplementary Service*) et SMS (*Short Message Service*) dédiés respectivement à :

- la gestion des connexions dans le domaine circuit,
- la gestion des connexions dans le domaine paquet,
- l'activation des services supplémentaires,
- l'envoi et la réception de messages courts point à point.

9.2. La sélection de PLMN

Le PLMN (*Public Land Mobile Network*) désigne un réseau mobile composé d'un réseau d'accès et d'un réseau cœur. Chaque réseau dans le monde est identifié de manière unique à l'aide d'un identificateur de PLMN. Cet identificateur est composé de deux champs :

– le champ MCC (*Mobile Country Code*) qui désigne le pays dans lequel se trouve le réseau. Par exemple en France, la valeur de MCC est égale à 208. Le cas de l'Amérique du nord avec plusieurs MCC est particulier. L'attribution des codes MCC est assurée par l'UIT. Cette centralisation permet d'éviter qu'un même code MCC soit attribué à deux pays différents ;

– le MNC (*Mobile Network Code*) qui permet de différencier des réseaux ayant le même MCC. L'attribution des codes MNC est assurée par l'autorité de régulation du pays concerné. En France, les opérateurs de téléphonie mobile traditionnels, Orange, SFR et Bouygues Telecom sont identifiés par une valeur de MNC égale à 01, 10 et 20 respectivement.

Pour un mobile donné, la notion de PLMN possède plusieurs déclinaisons :

– le HPLMN (*Home PLMN*) auprès duquel l'usager a souscrit un abonnement. L'opérateur de ce PLMN est le détenteur de l'USIM de l'équipement usager ;

– le VPLMN (*Visited PLMN*) qui est un PLMN différent du HPLMN sur lequel le mobile est accepté ;

– le RPLMN (*Registered PLMN*) qui est un PLMN sur lequel une inscription est réussie. Il peut être le HPLMN ou un VPLMN.

La procédure de sélection de PLMN peut être manuelle ou automatique et suit des règles précises définies par la norme [TS 23.122]. Les PLMN autres que le HPLMN peuvent être rangés dans différentes listes de sélection avec, dans le cas d'un mobile bimode, la possibilité d'association d'une ou de plusieurs technologies d'accès radio (UTRA ou GSM) à chaque entrée des listes de sélection. Les différentes listes de sélection sont les suivantes :

– la liste de sélection contrôlée par l'utilisateur avec les technologies d'accès radio associées ;

– la liste de sélection contrôlée par l'opérateur avec les technologies d'accès associées ;

– la liste de sélection de PLMN sans technologie d'accès radio associée.

A la mise sous tension ou sur rétablissement de la perte de couverture réseau, l'UE tente d'abord de sélectionner le RPLMN (le dernier PLMN où il s'est inscrit) en utilisant toutes les technologies d'accès radio supportées. Lorsque le RPLMN est trouvé, l'UE tente l'inscription. Lorsque la sélection du RPLMN n'est pas possible (le RPLMN n'existe pas, il n'est pas disponible ou l'inscription a échoué), le mobile exécute l'algorithme de sélection selon le mode choisi : automatique ou manuel.

PLMN équivalents

Avec l'UMTS, la notion de « PLMN équivalent » a été introduite. Des PLMN équivalents le sont les uns par rapport aux autres au regard des procédures de sélection/resélection de PLMN, de sélection/resélection de cellule ou de *handover*. Un opérateur possédant à la fois un réseau GSM et UMTS peut utiliser des identificateurs de PLMN différents pour ses deux réseaux dans un même pays ou dans des pays distincts. Grâce à la liste de PLMN équivalents indiquée par le réseau courant, le terminal peut sélectionner une cellule appartenant à un réseau considéré comme « équivalent » indépendamment de la technologie d'accès radio : GSM (TDMA) ou UMTS (WCDMA). Le partage de réseaux UMTS par des opérateurs distincts et l'optimisation de la couverture radio dans des zones frontalières, sont d'autres avantages apportés par la notion de « PLMN équivalents ».

9.2.1. *Le mode automatique de sélection*

Les tentatives de sélection sont exécutées dans l'ordre suivant en ne considérant que les PLMN disponibles et autorisés :

– le HPLMN ;

– les PLMN de la liste utilisateur si elle existe dans l'ordre de priorité ;

– les PLMN de la liste opérateur si elle existe dans l'ordre de priorité ;

– la liste de sélection sans technologie d'accès associée, si les listes utilisateur et opérateur avec technologies d'accès n'existent pas ;

– la liste d'autres PLMN pour lesquels la qualité de réception est supérieure à un seuil fixé ;

– la liste d'autres PLMN ordonnés suivant la qualité de réception décroissante.

Lorsque plusieurs technologies d'accès radio sont associées à un PLMN, la norme ne spécifie pas de priorité entre les différentes technologies d'accès. Dès qu'un PLMN est trouvé et l'inscription effectuée avec succès ou que la recherche dans toutes les listes existantes a échoué, la procédure de sélection se termine. Dans le cas des deux dernières listes, le mobile effectue sa recherche dans toutes les technologies d'accès supportées avant de procéder à la sélection. Pour cela, des critères de comparaison de qualité sont définis entre technologies d'accès.

9.2.2. *Le mode manuel de sélection*

Dans le mode manuel de sélection, le mobile présente à l'utilisateur juste après sa mise sous tension, l'ensemble des PLMN disponibles sans aucune restriction (pas de vérification de leur interdiction ou non), et ce en utilisant toutes les technologies d'accès radio supportées par le mobile. La liste est présentée dans un ordre identique à celui de la sélection automatique. Une ou plusieurs technologies d'accès radio avec ordre de priorité ou non peuvent être associées à chaque PLMN de la liste. L'utilisateur choisit un PLMN de la liste qui lui est présentée avec éventuellement une technologie d'accès radio et le mobile tente l'inscription sur le PLMN choisi.

9.2.3. *La resélection de PLMN*

La resélection de PLMN consiste en la tentative de sélection d'un PLMN plus prioritaire que le PLMN courant. Elle n'est possible que lorsque le mobile est dans le mode veille. Elle est soit provoquée par l'utilisateur à tout moment, soit déclenchée automatiquement sous le contrôle d'une temporisation en situation d'itinérance, c'est-à-dire lorsque le mobile est dans un VPLMN.

La resélection de PLMN provoquée par l'utilisateur

Comme pour la sélection, la resélection de PLMN provoquée par l'utilisateur peut être effectuée en mode automatique ou manuel. La procédure de resélection en mode manuel est identique à la procédure de sélection en mode manuel. Le mode de resélection automatique suit également les mêmes étapes que le mode de sélection automatique, mais en cas d'échec de la tentative de resélection, le mobile tente de sélectionner à nouveau le PLMN qui était sélectionné avant le déclenchement de la procédure de resélection.

La resélection de PLMN en situation d'itinérance

Un mobile en itinérance peut tenter périodiquement de resélectionner son HPMLN ou un PLMN des listes de sélection utilisateur ou opérateur plus prioritaire que son VPLMN. La resélection se fera cependant avec les restrictions suivantes :

– la resélection n'est possible qu'en mode veille ;

– lorsqu'une liste de « PLMN équivalents » est fournie par le VPLMN, la resélection du HPLMN ne peut être tentée que si ce dernier ne fait pas partie des

« PLMN équivalents » et un PLMN des listes de sélection utilisateur et opérateur n'est sélectionné que s'il est plus prioritaire que tous les « PLMN équivalents » ;

– seuls les PLMN plus prioritaires du même pays que le VPLMN pourront être candidats à la resélection.

La périodicité des tentatives de resélection peut être fixée par un paramètre stocké dans la carte USIM de l'équipement mobile et pouvant prendre les valeurs de six minutes à huit heures par palier de six minutes. Lorsque ce paramètre est absent, la valeur appliquée par défaut est soixante minutes.

9.2.4. *Les PLMN « interdits »*

Il se peut qu'après une tentative d'inscription à un VPLMN, l'UE reçoive le message *PLMN NOT ALLOWED*. A partir de ce moment, ce VPLMN ne sera plus pris en compte par le terminal lors des tentatives ultérieures de sélection ou de resélection de PLMN automatiques. L'identité de ces PLMN dits « interdits » (FPLMN, pour *Forbidden PLMN*), sera stockée dans une liste prévue à cet effet dans l'USIM appelée liste de « *forbidden PLMNs* ». Un PLMN interdit ne sera effacé de la liste que par une sélection manuelle réussie de PLMN.

En plus de la liste « *forbidden PLMNs* » qui est valable pour les service circuit et paquet, l'UE gère une autre liste de PLMN interdits appelée « *forbidden PLMNs for GPRS service* » laquelle n'est valable que pour les services en mode paquet. Elle est construite avec l'identité des VPLMN qui ont rejeté une demande d'inscription au domaine PS avec pour cause *GPRS SERVICES NOT ALLOWED IN THIS PLMN*. Les VPLMN dans cette liste seront effacés après la mise hors tension du terminal ; quand la carte USIM est retirée du terminal ou encore, après une sélection manuelle réussie de PLMN qui autorise l'accès aux services paquet.

9.3. Principes de gestion de la mobilité en UMTS

La gestion de la localisation géographique des terminaux est une fonction fondamentale pour un système de communication avec des mobiles. Elle s'appuie sur la définition de zones géographiques limitées à quelques cellules et identifiées de manière unique. Lorsque l'UE n'est pas en mode connecté dans lequel il est localisé au niveau cellule, il fournit au réseau l'identité de la zone où il se trouve pour être joignable sans une diffusion exhaustive par le réseau du message destiné au mobile (*paging*). Les procédures de gestion de la localisation intègrent également la sécurisation de la liaison entre le réseau et l'UE. Toutes les procédures liées à la localisation du mobile sont déclenchées par les protocoles MM pour le domaine circuit et GMM pour le domaine paquet. Les mise à jour de localisation dans les

domaines circuit et paquet ne sont effectuées que dans certains états des protocoles MM et GMM. Ces états sont illustrés par la figure 9.2 et décrits dans le tableau 9.1, et ils sont valables pour les domaines circuit (états MM) et paquet (états GMM). Pour les principaux états de service, il est indiqué dans ce tableau si la mise à jour de localisation est effectuée ou non (voir plus loin dans ce chapitre).

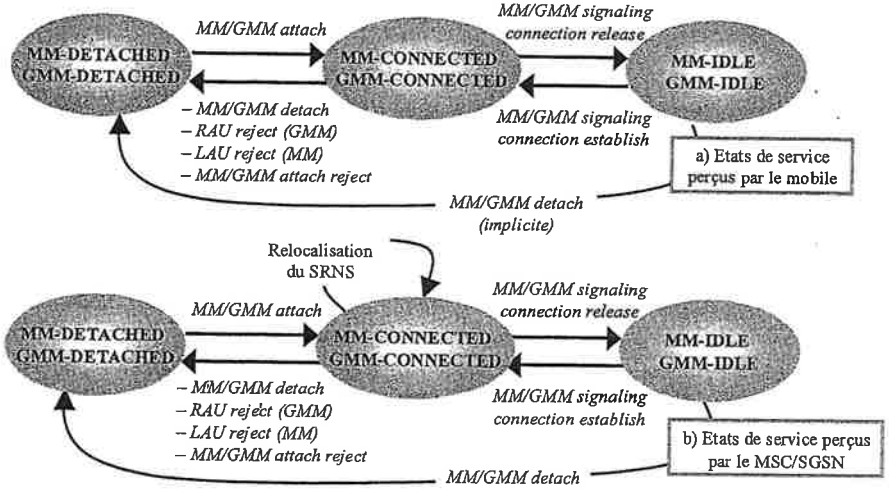


Figure 9.2. *Principaux états de service en UMTS. Dans le domaine circuit, le mobile effectue les procédures « MM attach » et « MM detach » seulement si cela est signalé par le réseau*

9.3.1. *Les zones de localisation*

Deux types de zones de localisation sont gérés par le réseau cœur :

– les zones de localisation appelées LA (*Location Area*) définies pour le domaine CS ; une LA consiste en un ensemble de cellules sous le contrôle d'un RNC et gérées par un même et unique 3G-MSC/VLR (cf. figure 9.3) ;

– les zones de localisation appelées RA (*Routing Area*) définies pour le domaine PS ; une RA peut être vue comme un sous-ensemble de cellules dans une LA sous le contrôle d'un RNC et gérées par un même et unique 3G-SGSN (cf. figure 9.3).

Pour une identification non ambiguë de chaque zone de localisation, le code identificateur LAI (*Location Area Identification*) ou RAI (*Routing Area Identification*) contient le MCC et le MNC. Les figures 9.4a et 9.4b représentent respectivement le format des codes LAI et RAI dont la structure assure une identification universelle des zones de localisation.

		MM/GMM-DETACHED	MM/GMM-IDLE	MM/GMM-CONNECTED
Description de l'état		L'UE est détaché du domaine CS/PS, et sa position est inconnue au niveau du MSC/SGSN.	L'UE s'est inscrit dans le domaine CS/PS et sa position est connue au niveau du MSC/SGSN à la LA/RA près. Aucune connexion de signalisation n'est établie entre l'UE et le domaine CS/PS.	L'UE s'est inscrit dans le domaine CS/PS. Une connexion de signalisation est établie entre l'UE et le domaine CS/PS. Possibilité de transmettre de données ou de signalisation.
Mise à jour de la localisation	**normale**	Non	Oui	Non, domaine CS, Oui[1], domaine PS
	périodique	Non	Oui	Non

Tableau 9.1. *Mise à jour de localisation du domaine circuit (MM) et du domaine paquet (GMM) selon les états de service*

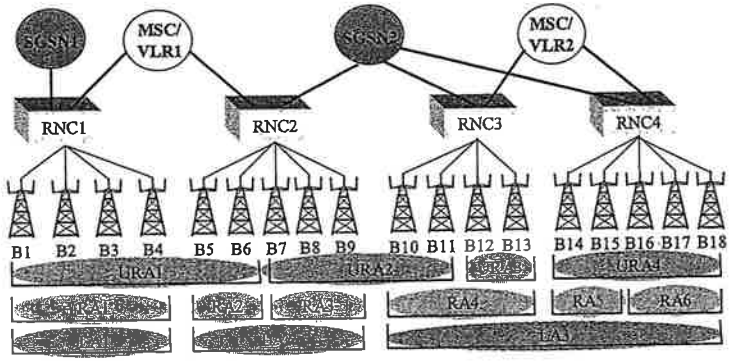


Figure 9.3. *Relation entre les différentes zones de localisation gérées par le réseau cœur et par l'UTRAN*

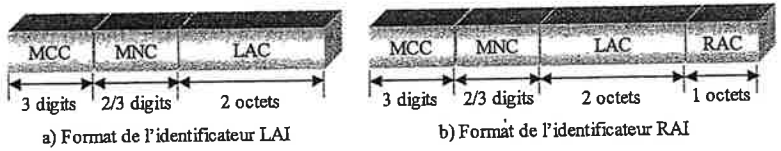


Figure 9.4. *Format des identificateurs LAI et RAI*

1. Mise à jour de localisation suite à une relocalisation du SRNS (voir plus loin dans ce chapitre).

Comme pour l'identité de PLMN, le MCC identifie le pays où se trouve le réseau alors que le MNC identifie de manière unique tout réseau dans un pays. Le LAC (*Location Area Code*) identifie de manière unique, à l'intérieur d'un réseau, toute zone de localisation du domaine circuit. Enfin, le RAC (*Routing Area Code*) identifie une zone de localisation du domaine paquet à l'intérieur d'une zone de localisation circuit. Les LA sont gérées par les VLR et les RA par les SGSN.

Le tableau 9.2 résume le partage de la gestion des zones de localisation entre le réseau cœur et l'UTRAN. Le partage équivalent dans les réseaux GSM et GPRS est indiqué à titre comparatif. Notons que, à la différence des réseaux GPRS, en UMTS la mobilité au niveau cellule est à la charge de l'UTRAN (et non pas à la charge du SGSN). De plus, l'UMTS introduit la notion d'URA (*UTRAN Registration Area*) dont la gestion est aussi à la charge de l'UTRAN (voir chapitres 5 et 8). Il n'existe pas de relation directe entre l'URA et les zones de localisation RA et LA.

	MSC/VLR (circuit)		SGSN (paquet)		UTRAN (circuit et paquet)
	GSM	**UMTS**	**GPRS**	**UMTS**	**UMTS**
Cellule	Non	Non	Oui	Non	Oui
URA	-	Non	-	Non	Oui
RA	-	Non	Oui	Oui	Non
LA	Oui	Oui	Non	Non	Non

Tableau 9.2. *Comparatif des zones de localisation en GSM, GPRS et UMTS en fonction des éléments du réseau qui les gèrent*

9.3.2. *Correspondance entre les états de service du réseau cœur et de l'UTRAN*

La gestion de la mobilité des terminaux UMTS est partagée par le réseau cœur et par l'UTRAN. Trouver une correspondance exacte entre les états de service du réseau cœur et ceux de l'UTRAN n'est pas immédiate, car l'UE ne peut être que dans un seul mode RRC indépendamment de son inscription simultanée aux domaines CS et PS. Par exemple, le mobile peut se trouver en mode MM-IDLE, ce qui correspondrait au mode veille RRC, mais en réalité opérer en mode RRC connecté si l'état côté paquet est GMM-CONNECTED. En général, on peut dire que :

– en mode *connecté RRC*, au moins l'un des états de service de l'UE vis-à-vis du réseau cœur est MM-CONNECTED ou GMM-CONNECTED, et sa mobilité est contrôlée par l'UTRAN. Aussi, lorsque l'UE se trouve dans l'un des états de ce mode (CELL_DCH, CELL_FACH, CELL_PCH ou URA_PCH), il ne tient pas compte des

informations système diffusées dans la cellule donnant l'identité des RA et LA courantes. Cela implique que le terminal n'effectue les procédures de mobilité *Location updating* (domaine circuit) et *Routing area updating* (domaine paquet) – décrites plus loin dans ce chapitre – que si cela est signalé explicitement par le SRNC (par exemple, suite à une relocalisation du SRNS),

– en mode *veille RRC*, l'UE se trouve dans les états MM-IDLE et GMM-IDLE et sa mobilité est contrôlée par le réseau cœur. L'UE lit les informations système diffusées dans la cellule courante et effectue les procédures de mise à jour de la localisation correspondantes à chaque fois qu'il rentre dans une nouvelle LA ou RA.

On peut considérer que l'UE dans les états MM-DETACHED et GMM-DETACHED se trouve également dans le mode veille RRC. Cependant, dans ces états, ni l'UTRAN ni le réseau cœur sont impliqués dans la gestion de sa mobilité.

9.4. La sécurisation de l'accès au réseau

Lors de l'inscription auprès du réseau et à chaque changement de zone de localisation, des procédures de sécurisation de l'accès peuvent être exécutées pour assurer la confidentialité, l'authenticité et l'intégrité des échanges.

9.4.1. *L'allocation d'une identité temporaire*

Tout abonné auprès d'un réseau mobile possède un identificateur permanent IMSI (voir chapitre 3). Pour assurer la confidentialité de l'identité de l'abonné, c'est-à-dire rendre difficile l'identification et la localisation malveillante de l'abonné par un intrus, le réseau évite la transmission fréquente de l'identificateur permanent sur l'interface radio. Pour cela, dès l'inscription initiale de l'abonné, le VLR (domaine circuit) ou le SGSN (domaine paquet) lui attribue un identificateur temporaire choisi dynamiquement et uniquement valable à l'intérieur d'une zone de localisation. L'identificateur temporaire est appelé TMSI (*Temporary Mobile Subscriber Identity*) pour le domaine circuit et P-TMSI (*Packet Temporary Mobile Subscriber Identity*) pour le domaine paquet. L'allocation d'identité temporaire est effectuée à la fin des procédures d'inscription ou de mise à jour de localisation ou dans une procédure spécifique. La figure 9.5 et le tableau 9.3 illustrent la procédure d'allocation d'identificateur temporaire.

Le type du message utilisé pour la commande et l'acquittement dans l'allocation d'identificateur temporaire sont fonctions du type de la procédure dans laquelle se fait l'allocation. Le tableau 9.3 donne les différents messages utilisés. Leur structure est décrite dans la spécification technique [TS 24.008].

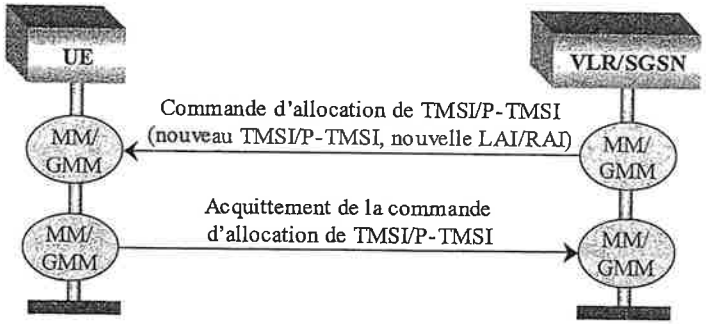


Figure 9.5. *Procédure d'allocation d'identité temporaire*

Type de procédure	Message de commande	Message d'acquittement
Inscription ou mise à jour de localisation dans le domaine CS	LOCATION UPDATING ACCEPT	TMSI REALLOCATION COMPLETE
Inscription dans le domaine PS ou inscription combinée dans les domaines PS et CS	ATTACH ACCEPT	ATTACH COMPLETE
Mise à jour de localisation dans le domaine PS ou mise à jour combinée de localisation dans les domaines PS et CS	ROUTING AREA UPDATE ACCEPT	ROUTING AREA UPDATE COMPLETE
Procédure spécifique de mise à jour de localisation	TMSI/P-TMSI REALLOCATION COMMAND	TMSI/P-TMSI REALLOCATION COMPLETE

Tableau 9.3. *Types de message utilisés dans les procédures d'allocation d'identificateur temporaire*

9.4.2. *La demande d'identification du mobile*

Cette procédure est utilisée par le réseau pour demander au mobile de lui fournir l'identificateur permanent d'abonné IMSI ou l'identificateur de l'équipement mobile IMEI (*International Mobile Equipment Identity*).

L'identificateur permanent d'abonné IMSI est demandé par le réseau lorsqu'il n'arrive plus à identifier de manière certaine le mobile à partir d'un identificateur

est normalement suivie d'une allocation d'identité temporaire.

Quant à l'IMEI, il est demandé par le réseau avec éventuellement la version de logiciel IMEISV (*IMEI Software Version*) pour vérifier que l'UE ne figure pas dans une liste d'équipements interdits (*black list*). Cette liste peut contenir les identificateurs d'équipements volés ou non homologués. La figure 9.6 est une illustration des messages échangés entre le réseau et le mobile dans le cadre de la procédure d'identification.

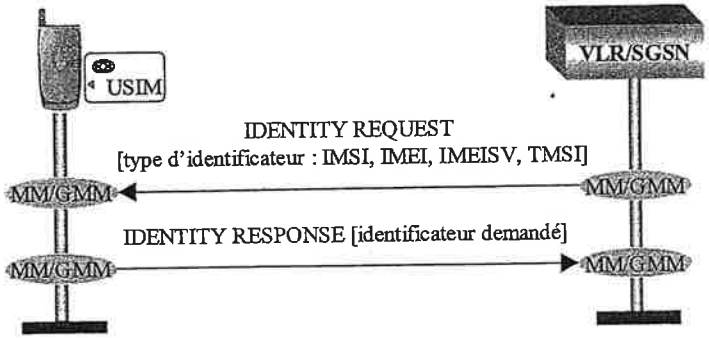


Figure 9.6. *Procédure de demande d'identification du mobile*

9.4.3. *L'activation du chiffrement et de l'intégrité*

Le chiffrement est utilisé pour la confidentialité des données usager et de la signalisation transférées sur l'interface radio. Quant à l'intégrité, qui est une nouveauté par rapport au GSM, elle permet l'authentification des messages de signalisation sur l'interface d'accès radio et constitue une fonction essentielle dans la sécurité UMTS. Ces deux fonctions sont assurées par l'interface radio (*access stratum*), mais leur activation est assurée par le réseau cœur pour chacun des domaines de service (voir aussi chapitre 8). L'activation est déclenchée par le VLR/SGSN sur réception du premier message de signalisation NAS en provenance de l'UE : *ATTACH REQUEST*, *LOCATION UPDATING REQUEST*, *ROUTING AREA UPDATE REQUEST*, *CM SERVICE REQUEST*, *PAGING RESPONSE*. Ce premier message transporte également l'identité de l'UE et un paramètre KSI (*Key Set Identifier*) permettant au réseau d'identifier, sans exécution de la procédure d'authentification, les clés de chiffrement et d'intégrité stockées dans le mobile.

La procédure d'activation du chiffrement et de l'intégrité est illustrée par la figure 9.7.

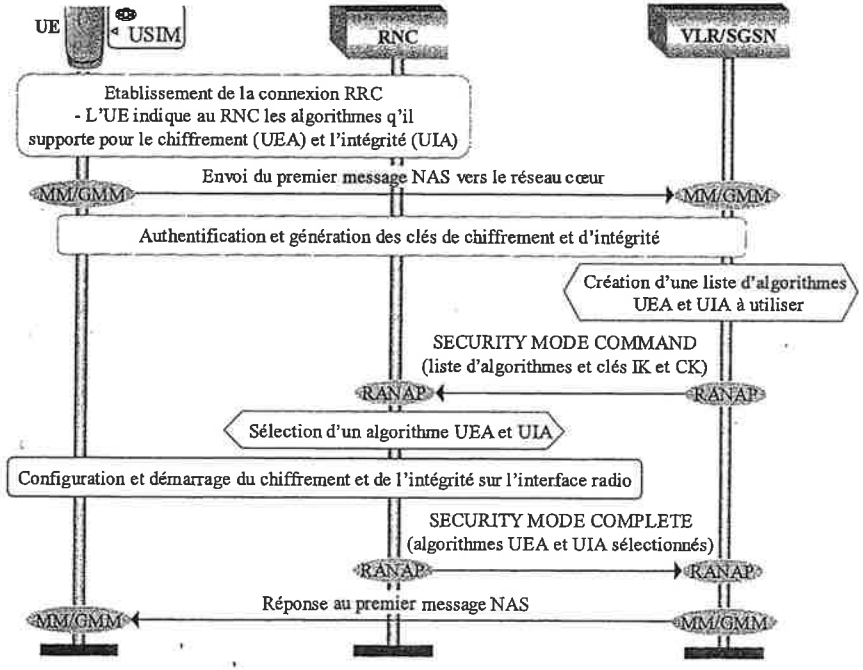


Figure 9.7. *Procédure d'activation du chiffrement et de l'intégrité*

9.4.4. *L'authentification*

La procédure d'authentification permet d'une part au réseau et au mobile de s'authentifier mutuellement, et d'autre part au réseau de fournir au mobile les paramètres permettant de calculer les clés de chiffrement et d'intégrité à utiliser de part et d'autre. Il faut noter la différence fondamentale avec le système GSM dans lequel l'authentification n'est pas réciproque, puisque le mobile n'authentifie jamais le réseau.

Le principe d'authentification mutuelle repose sur la fourniture mutuelle par le réseau et le mobile de la preuve qu'ils détiennent un secret sans le divulguer. Ce secret consiste en la clé K stockée dans l'USIM du mobile et le centre d'authentification AuC (*Authentication Centre*) du réseau. La sécurité de la procédure est garantie par le fait que la seule donnée statique (clé K) n'est jamais transmise dans les messages échangés. Seuls des paramètres dynamiques et non prédictibles parce que générés à partir de la clé K et d'un nombre aléatoire RAND sont échangés dans les messages. La figure 9.8 montre le mécanisme de génération

des paramètres d'authentification au niveau de l'AuC. Les opérations « ⊕ » et « || » représentent respectivement le « ou » exclusif et la concaténation.

L'AuC commence par générer un numéro de séquence SQN (*Sequence Number*) et un nombre aléatoire RAND (*Random*). Des techniques de génération de SQN sont décrites dans l'annexe C de la spécification [TS 33.102]. Ensuite, les paramètres SQN, RAND, K et AMF (*Authentication Management Field*) sont passés en entrée aux fonctions f1 à f5 présentes dans l'USIM et l'AuC pour produire d'autres paramètres.

L'AMF sert à signaler des paramètres supplémentaires utilisés pour une gestion plus flexible de l'authentification, comme par exemple l'indication de l'algorithme utilisé pour générer les vecteurs d'authentification lorsque plusieurs algorithmes sont possibles ; la sélection d'une limite pour la durée de vie des clés de chiffrement et d'intégrité, etc.

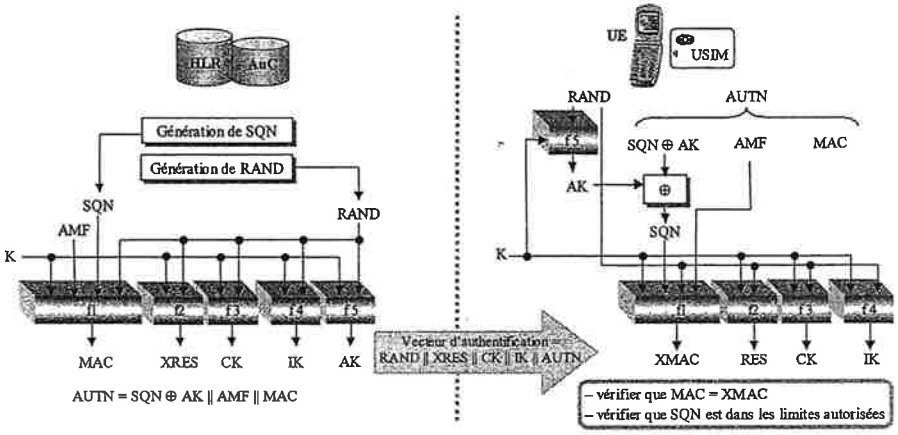


Figure 9.8. *Mécanisme de génération d'un vecteur d'authentification*

En plus des clés de chiffrement CK et d'intégrité IK, les paramètres suivants sont produits en sortie des fonctions fi :

– AK (*Anonymity Key*) est utilisé pour masquer le numéro de séquence lorsque ce dernier peut servir à une identification et une localisation malveillante du mobile ;

– XRES (*eXpected RESponse*) qui est la réponse attendue du mobile pour son authentification ;

– MAC (*Message Authentication Code*) qui est le code d'authentification du message à envoyer au mobile.

Puis l'AuC construit le jeton d'authentification AUTN constitué de trois champs contenant respectivement la valeur des paramètres SQN (masqué par un « ou » exclusif avec AK), AMF et MAC. Le vecteur d'authentification est une concaténation des paramètres RAND, XRES, CK, IK et AUTN. La figure 9.9 illustre les différentes étapes de la procédure d'authentification.

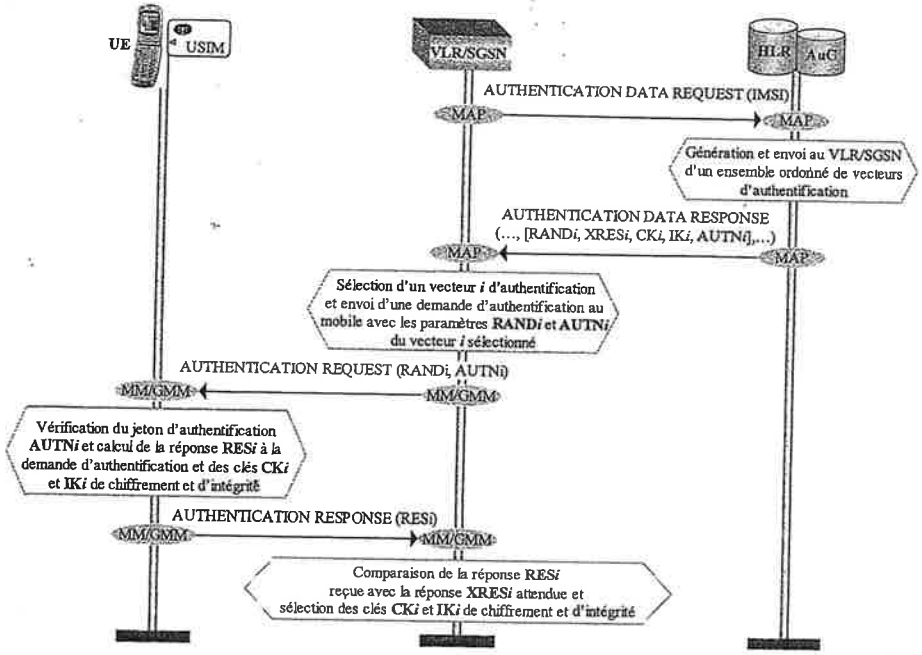


Figure 9.9. *Procédure d'authentification*

L'authentification se déroule de la manière suivante :

– sur détection d'une condition de déclenchement de l'authentification, le VLR/SGSN demande les paramètres d'authentification à l'AuC qui est la seule entité du réseau capable de les générer ;

– l'AuC génère un ensemble ordonné de vecteurs d'authentification et l'envoie au VLR/SGSN ;

– le VLR/SGSN enregistre les vecteurs reçus et en sélectionne un de rang *i* (sélection dans l'ordre), puis envoie les paramètres RAND*i* et AUTN*i* (constitué de SQN ⊕ AK, AMF et MAC) du vecteur *i* au mobile ; les autres paramètres XRES*i*, CK*i* et IK*i* ne sont pas envoyés au mobile ; XRES*i* sera utilisé pour vérifier la validité de la réponse du mobile ; CK*i* et IK*i* seront utilisés comme clés de

chiffrement et d'intégrité si l'authentification avec le vecteur *i* s'est déroulée avec succès ;

– sur réception de la demande d'authentification, l'USIM, qui détient le secret de production des paramètres d'authentification et des clés de chiffrement et d'intégrité dans le mobile, génère les paramètres XMAC*i* (*eXpected MAC*), RES*i* (*RESponse*), CK*i* et IK*i* à partir des paramètres RAND*i* et AUTN*i* reçus en déroulant le mécanisme illustré par la figure 9.8 ;

– le mobile compare ensuite les paramètres MAC reçus et XMAC générés pour authentifier le réseau, vérifie la validité du numéro de séquence SQN et dans le cas où tout est correct, envoie au réseau la réponse à la demande d'authentification avec le paramètre RES générés ;

– sur réception de la réponse du mobile, le VLR/SGSN compare le paramètre RES reçu avec XRES pour authentifier le mobile ; en cas d'égalité, la procédure d'authentification se termine et les clés CK*i* et IK*i* peuvent être utilisées de part et d'autre pour le chiffrement et l'intégrité selon les mécanismes étudiés dans le chapitre 8.

9.5. L'inscription auprès du réseau

L'inscription consiste en l'attachement de l'abonné (l'USIM) au réseau pour accéder à ses services. C'est pourquoi elle ne doit être effectuée que lorsqu'une USIM valide est activée dans le mobile. Pour le domaine circuit, une information sur la nécessité ou non, pour le mobile, d'effectuer la procédure d'attachement (mise à jour de localisation de type *IMSI attach*) est fournie par le réseau dans un élément d'information (*CS DOMAIN SPECIFIC NAS SYSTEM INFORMATION*) diffusé *via* le SIB1.

Une fois un PLMN et une cellule convenable de ce dernier sélectionnés (voir chapitre 13), et à condition que le réseau ait indiqué la nécessité d'effectuer l'attachement, le mobile tente de s'inscrire auprès du réseau pour accéder à ses services. L'inscription est faite pour chacun des deux domaines de service. C'est cette phase d'inscription qui permet au réseau d'avoir la localisation initiale du mobile et de sécuriser la liaison entre le mobile et le réseau (authentification mutuelle entre le réseau et l'abonné, identification du terminal et attribution d'identificateur temporaire au mobile).

L'inscription auprès du réseau se fait à l'aide de procédures de signalisation NAS appelée *IMSI attach* pour le domaine circuit et *GPRS attach* pour le domaine paquet.

9.5.1. *La procédure* IMSI attach

La procédure *IMSI attach* est à l'initiative du protocole MM assurant du côté du mobile la gestion de la mobilité dans le domaine circuit. Elle commence par l'envoi au MSC/VLR d'un message *LOCATION UPDATING REQUEST* avec comme paramètres, entre autres :

– le type de localisation égale à *IMSI attach* pour l'inscription ;

– l'identité de la zone de localisation LAI précédemment stockée dans l' USIM ;

– l'identité de l'UE qui peut être l'IMSI ou un TMSI valide (si l'UE en détient) ;

– le paramètre *follow on request* permettant de demander au réseau de ne pas libérer la connexion de signalisation juste après l'inscription, d'autres messages de signalisation ou de trafic devant suivre.

La figure 9.10 donne l'exemple de la toute première inscription dans le domaine circuit pour lequel l'IMSI est utilisé comme identificateur du mobile et qui ne met pas en œuvre un changement de VLR.

Sur réception du message *LOCATION UPDATING REQUEST* avec un paramètre type de localisation égal à *IMSI attach* signifiant qu'il s'agit d'une inscription, le VLR lance les procédures d'authentification (cf. figure 9.9) et d'activation du chiffrement et de l'intégrité (cf. figure 9.7) pour sécuriser la liaison. Le VLR peut optionnellement procéder à l'identification de l'équipement mobile par son IMEI ou son IMEISV.

Lorsque cette première phase se déroule avec succès, le VLR demande au HLR de prendre en compte la nouvelle localisation du mobile en lui fournissant l'IMSI du mobile et l'identificateur du VLR. Le HLR procède alors au transfert des données d'abonnement du mobile vers le VLR, puis acquitte la demande de localisation. Sur réception de cet acquittement, le VLR attribue un identificateur temporaire au mobile et lui envoie un message d'acceptation de la demande d'inscription. En plus du TMSI et du LAI, ce message peut également transporter un paramètre *follow on proceed* pour informer le mobile que la connexion de signalisation est maintenue conformément au souhait du mobile exprimé dans la demande d'inscription avec le paramètre *follow on request* et un paramètre *Equivalent PLMN* contenant une liste de « PLMN équivalents ». Enfin, pour acquitter l'allocation par le VLR d'un identificateur temporaire, le mobile lui envoie un message *TMSI REALLOCATION COMPLETE* qui termine la procédure d'inscription dans le domaine circuit.

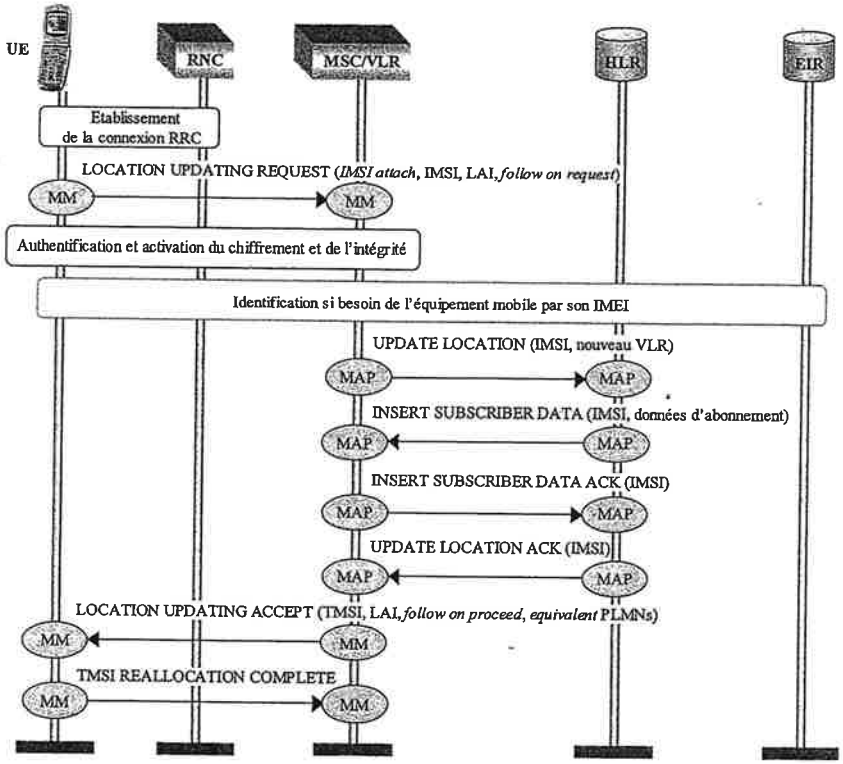


Figure 9.10. *Procédure* IMSI attach

9.5.2. *La procédure* GPRS attach

Cette procédure est utilisée soit lors d'une inscription simple dans le domaine paquet, soit lors de l'inscription combinée dans les domaines paquet et circuit. Ce dernier cas n'est possible que si l'interface optionnelle « Gs » entre le SGSN et le MSC/VLR est implémentée dans le réseau cœur. La procédure est lancée par l'entité GMM du mobile par l'envoi d'un message *ATTACH REQUEST* avec comme paramètres :

– le type d'attachement égal à *GPRS attach*, *GPRS attach while IMSI attached* ou *combined GPRS/IMSI attach* pour, respectivement, une inscription simple dans le domaine paquet, une inscription dans le domaine paquet, l'UE étant déjà inscrit dans le domaine circuit ou une inscription combinée dans les domaines paquet et circuit ;

– l'identificateur du mobile qui peut être l'IMSI ou un P-TMSI valide si le mobile en détient un ;

– la signature associée au P-TMSI si elle existe et si le P-TMSI est utilisé pour identifier le mobile ;

– la zone de localisation RAI associée au P-TMSI ;

– l'état du TMSI (*TMSI status*) utilisé dans le cas d'une inscription combinée pour indiquer la non-disponibilité dans le mobile d'un TMSI valide ;

– le paramètre *follow on request* permettant de demander au réseau de ne pas libérer la connexion de signalisation juste après l'inscription. D'autres messages de signalisation ou de trafic devant suivre après l'inscription avec succès.

Sur réception du message *ATTACH REQUEST*, le SGSN peut lancer les procédures d'identification, d'authentification et d'activation du chiffrement et de l'intégrité, en fonction des valeurs de paramètres reçus.

La figure 9.11 illustre un cas générique d'inscription combinée dans les domaines paquet et circuit avec prise en compte des cas de SGSN et de MSC/VLR ayant changé depuis le dernier détachement.

Lorsque le nouveau SGSN reçoit la demande d'attachement avec un P-TMSI comme identificateur du mobile, il identifie l'ancien SGSN à partir du RAI reçu et lui envoie un message *SEND IDENTIFICATION* pour rapatrier l'identificateur permanent du mobile et un ou plusieurs vecteurs d'authentification. Si l'ancien SGSN a pu identifier le mobile à partir des paramètres reçus, il envoie au nouveau SGSN l'IMSI du mobile et un ou plusieurs vecteurs d'authentification. Si l'ancien SGSN n'a pas pu identifier le mobile parce que le P-TMSI n'existe pas dans sa base de données ou que le contrôle de la validité du P-TMSI à l'aide de la signature P-TMSI a échoué, il notifie au nouveau SGSN que l'abonné est inconnu dans sa base. Dans le cas d'un acquittement négatif, le nouveau SGSN demande au mobile de s'identifier par son IMSI, puis procède à l'authentification et l'activation du chiffrement et de l'intégrité.

Après la sécurisation de la liaison, le nouveau SGSN continue la procédure d'inscription en demandant au HLR de prendre en compte la nouvelle localisation du mobile pour les services dans le domaine paquet. Les paramètres « numéro de SGSN » et « adresse SGSN » du message *UPDATE GPRS LOCATION* représentent respectivement le numéro téléphonique (ISDN) et l'adresse IP du SGSN. Le HLR annule la localisation dans l'ancien SGSN, transfert les données d'abonnement du mobile vers le nouveau SGSN et acquitte la demande de localisation dans le domaine paquet.

Le nouveau SGSN passe ensuite à l'inscription dans le domaine circuit par l'envoi du message *LOCATION UPDATE REQUEST* au nouveau VLR identifié grâce à son LAI. Le nouveau VLR procède alors à l'inscription du mobile dans le domaine circuit : envoi d'une demande de prise en compte de la nouvelle localisation du

mobile au HLR, annulation de la localisation dans l'ancien VLR, transfert des données d'abonnement du mobile vers le nouveau VLR et acquittement de la demande de localisation par le HLR, puis envoie un message d'acceptation de la localisation dans le domaine circuit avec attribution d'un TMSI.

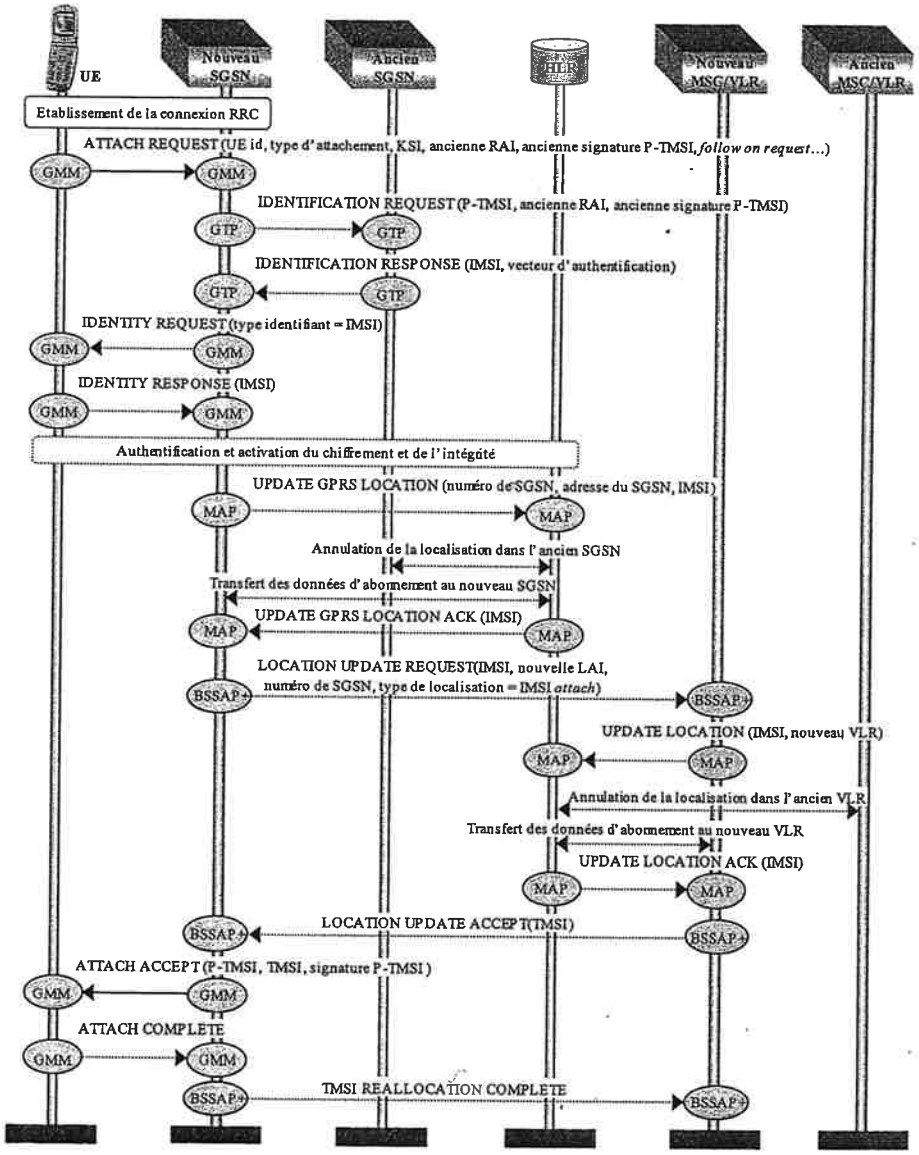


Figure 9.11. *Procédure combinée* GPRS/IMSI attach

L'inscription dans les deux domaines de services étant effectuée avec succès, le nouveau SGSN envoie au mobile le message d'acceptation transportant les identificateurs temporaires TMSI et P-TMSI et éventuellement la signature du P-TMSI. La procédure se termine par l'envoi par le mobile d'un message *ATTACH COMPLETE* au nouveau SGSN qui envoie à son tour un message *TMSI REALLOCATION COMPLETE*. Ces deux derniers messages permettent de notifier aux nouveaux nœuds du réseau cœur la prise en compte des nouveaux identificateurs temporaires.

9.6. La mise à jour de la zone de localisation du mobile

Après l'inscription auprès du réseau, le mobile doit maintenir sa localisation dans le réseau pour être joignable à tout moment malgré ses déplacements. Cela se fait à l'aide des procédures *Location updating* et *Routing area updating* pour respectivement les domaines circuit et paquet.

9.6.1. *La procédure* Location updating

On peut distinguer deux types de mise à jour de localisation dans le domaine circuit : la mise à jour normale et la mise à jour périodique. C'est cette même procédure qui est en réalité utilisée pour l'inscription (ou localisation initiale) dans le domaine circuit. Ces différents types de localisation sont engagés à l'aide du même message *LOCATION UPDATING REQUEST*, la différenciation se faisant par un paramètre qui indique le type de localisation.

La *mise à jour normale* de zone de localisation (*normal location updating*) est exécutée à chaque fois que le mobile détecte un changement de LA dans les informations système diffusées *via* le BCH dans sa cellule courante, ou que le réseau lui indique, en réponse à une demande d'établissement de connexion MM, qu'il est inconnu dans le VLR qui contrôle sa zone de localisation courante.

La *mise à jour périodique* de la zone de localisation (*periodic location updating*) est quant à elle utilisée par le mobile pour signaler périodiquement au réseau sa présence dans une LA. La périodicité est fixée par une temporisation dont la valeur est fournie par le réseau dans l'élément d'information *CS DOMAIN SPECIFIC NAS SYSTEM INFORMATION* transmis à travers certains messages du protocole RRC. La temporisation peut prendre les valeurs de 0 à 25,5 heures par pas de six minutes, 0 signifiant une période infinie, donc pas de mise à jour périodique.

La figure 9.12 montre l'exemple d'une mise à jour inter-MSC/VLR de la LA, l'ancienne et la nouvelle zones de localisation étant contrôlées par des VLR différents.

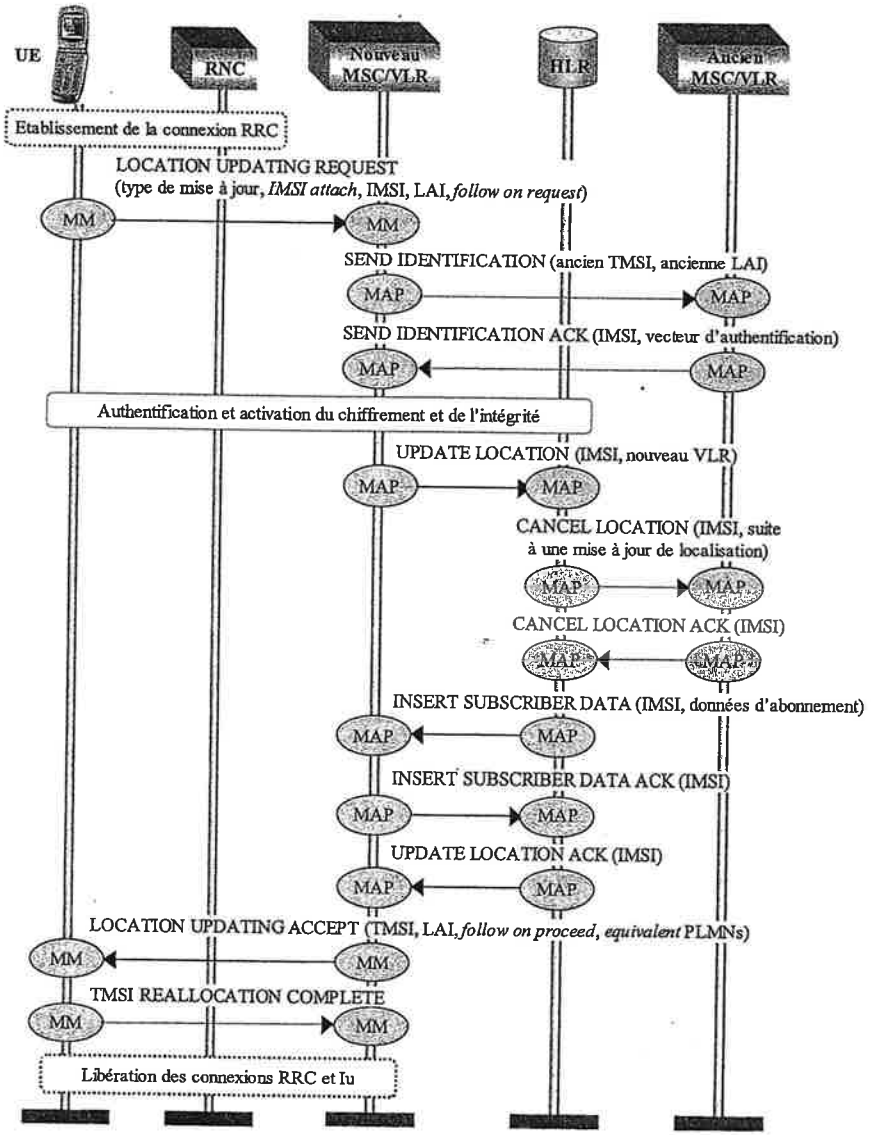


Figure 9.12. *Procédure* Location updating *inter MSC/VLR*

Le déroulement de la procédure est identique à celui de *l'IMSI attach*, la valeur du paramètre type de mise à jour dans le message *LOCATION UPDATING REQUEST* permettant de les différencier. Dans le cas d'une *location updating*, ce paramètre prend les valeurs *normal location updating* ou *periodic location updating*. Par rapport à l'exemple de procédure *IMSI attach* (cf. figure 9.10), l'exemple de la figure 9.12, qui prend en compte le cas de mise à jour inter-MSC/VLR, inclut en plus l'annulation de la localisation dans l'ancien MSC/VLR.

9.6.2. *La procédure* Routing area updating

Cette procédure est utilisée aussi bien pour la mise à jour de zones de localisation dans le domaine paquet uniquement (mise à jour de RA), que pour la mise à jour combinée dans les domaines paquet et circuit (mise à jour de RA et de LA).

Elle se décline en différents types :

– la mise à jour normale (*normal routing area updating*) engagée par le mobile lorsqu'il détecte un changement de RA dans les informations système diffusées dans sa cellule courante, ou encore pour rétablir une connexion de signalisation paquet lorsque la connexion RRC est libérée avec comme cause *DIRECTED SIGNALLING CONNECTION RE-ESTABLISHMENT* ;

– la mise à jour périodique (*periodic routing area update*) utilisée par le mobile pour signaler régulièrement au réseau sa présence dans une RA. La périodicité est contrôlée avec une temporisation T3312 dont la valeur est fournie par le réseau dans les messages *ATTACH ACCEPT* ou *ROUTING AREA UPDATE ACCEPT* ;

– la mise à jour combinée (*combined RA/LA updating*) lorsque le mobile s'est déjà inscrit auprès du réseau pour les deux domaines de services et que les conditions de déclenchement d'une mise à jour de la LA sont réunies ;

– la mise à jour combinée (*combined RA/LA updating with IMSI attach*) lorsque le mobile, qui ne s'est inscrit qu'au domaine paquet, veut effectuer une mise à jour de RA associée à une inscription dans le domaine circuit (*IMSI attach*).

La figure 9.13 est un exemple de procédure *Routing area updating* incluant tous les cas de figure, y compris ceux de mise à jour inter-SGSN et inter-MSC/VLR, ainsi que la mise à jour alors qu'une connexion de signalisation est active. Ce dernier cas n'est autorisé qu'après une relocalisation de SRNS (cf. section suivante).

La procédure est engagée par le mobile par l'envoi du message *ROUTING AREA UPDATE REQUEST* au nouveau SGSN *via* le nouveau SRNC. Le paramètre type de mise à jour permet d'indiquer le type de *Routing area updating* demandé.

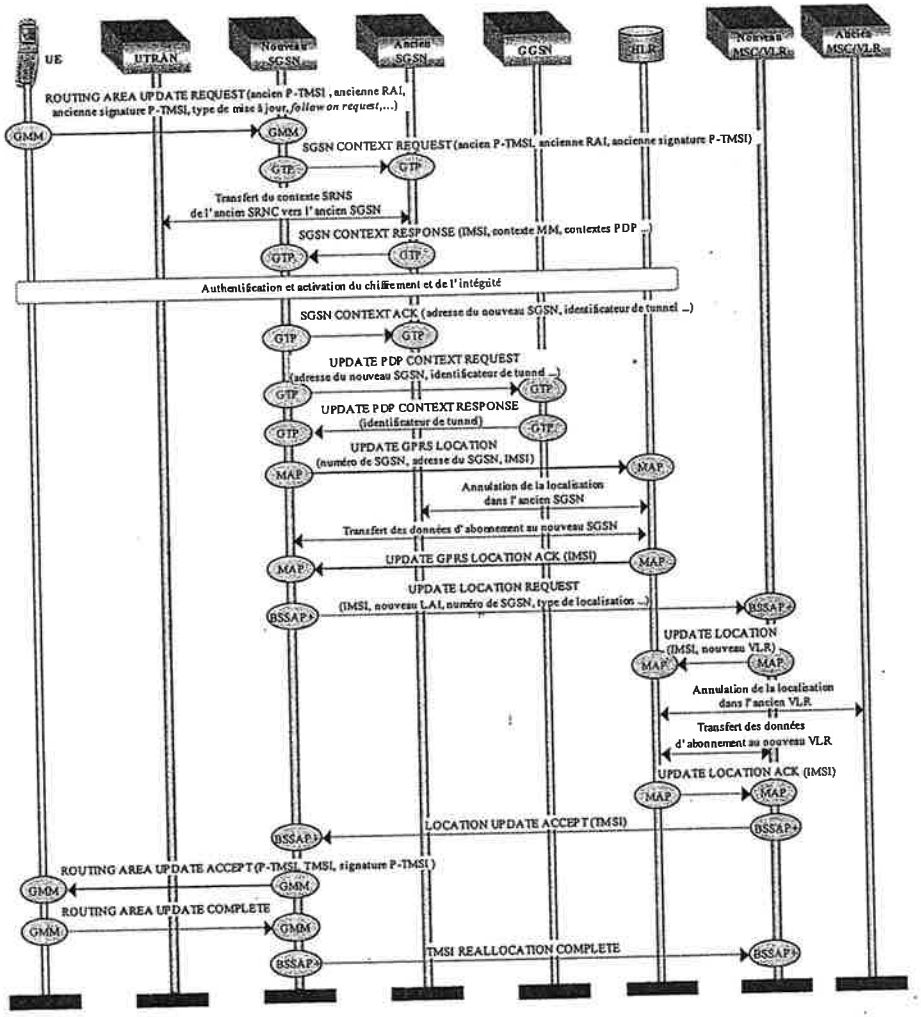


Figure 9.13. *Procédure de* Routing area updating

Si l'ancienne RA fournie dans la demande de mise à jour n'est pas contrôlée par le nouveau SGSN, celui-ci demande le contexte SGSN à l'ancien SGSN (message *SGSN CONTEXT REQUEST*). Dans le cas où une connexion de signalisation est active, ce qui signifie que la mise à jour est la conséquence d'une relocalisation de SRNS, l'ancien SGSN demande le contexte SRNS à l'ancien SRNC. Le contexte SRNS contient, pour chaque contexte PDP, les numéros de séquence de paquets GTP-SND (numéro de séquence de la prochaine PDU GTP à envoyer vers le mobile), GTP-SNU (numéro de séquence de la prochaine PDU GTP à envoyer vers le GGSN) et PDCP-SNU (numéro de séquence de la prochaine PDU PDCP attendue du mobile) utilisés pour la resynchronisation du transfert de données suite à une relocalisation de SRNS. Ces numéros de séquence sont inclus dans le message *SGSN CONTEXT RESPONSE* envoyé au nouveau SGSN en réponse à la demande de contexte SGSN. Le nouveau SGSN peut ensuite procéder à l'authentification du mobile si la réponse à la demande de contexte indique une erreur telle que par exemple une signature P-TMSI non valide, puis il envoie un message d'acquittement à l'ancien SGSN pour lui indiquer qu'il a bien reçu les informations de contexte PDP et qu'il est prêt à prendre le relais pour les transferts de messages. A la réception de cet acquittement, l'ancien SGSN routera tout message destiné au mobile vers le nouveau SGSN.

Le nouveau SGSN procède ensuite à la mise à jour du contexte PDP au niveau du GGSN, puis envoie une demande de mise à jour de localisation au HLR. Ce dernier annule alors la localisation du mobile dans l'ancien SGSN, transfert les données d'abonnement du mobile vers le nouveau SGSN puis acquitte la demande de mise à jour de localisation.

La procédure se poursuit avec la mise à jour de la localisation dans le domaine circuit qui peut être de deux types en fonction de la valeur du paramètre *type de mise à jour* dans le premier message de la procédure :

– type *IMSI attach* si le paramètre indique une mise à jour de type *combined RA/LA updating with IMSI attach* ;

– type *normal location updating* intra-VLR ou inter-VLR si le paramètre indique *combined RA/LA updating*, la nouvelle RA se trouvant dans une nouvelle LA.

La procédure se termine avec l'envoi d'un message d'acceptation de la mise à jour au mobile. Ce message peut transporter de nouveaux identificateurs temporaires (P-TMSI et/ou TMSI) et dans ce cas, la prise en compte de ces identificateurs est notifiée aux nouveaux SGSN et MSC/VLR à l'aide des messages *ROUTING AREA UPDATE COMPLETE* et TMSI *Reallocation Complete*.

9.6.3. La relocalisation de SRNS

La relocalisation de SRNS (*SRNS relocation* ou encore *Streamlining*) est une nouveauté par rapport au système GSM. Elle consiste à changer le RNC serveur (SRNC) localisé dans le SRNS (*Serving RNS*) d'un mobile connecté au réseau, c'est-à-dire le RNS supportant la connexion Iu avec le réseau cœur. La procédure est toujours décidée par le SRNC dans les situations suivantes :

– au cours d'une communication, le mobile s'est éloigné de son SRNC et le chemin qui le lie à ce dernier comprend un RNC en dérivation (DRNC) qui est

utilisé grâce à une interface « Iur » comme relais pour les échanges entre le mobile et son SRNC. Afin d'alléger le trafic sur l'interface « Iur » (optimisation de l'utilisation des ressources UTRAN), le SRNC peut utiliser la procédure *SRNS relocation* pour modifier le chemin du trafic de données en transférant le rôle de SRNC au DRNC ;

– suite à une resélection de cellule, le mobile connecté au domaine paquet et utilisant des ressources radio communes, engage une procédure RRC de *Cell update* ou *URA update* (cf. chapitre 8). La cellule cible est sous le contrôle d'un autre RNC (SRNC cible) qui relaye le message vers le SRNC source à l'aide du protocole RNSAP (message RNSAP *UPLINK SIGNALLING TRANSFER INDICATION*). Si l'interface « Iur » entre les SRNC source et cible ne supporte pas de trafic utilisateur (seulement de la signalisation entre RNC), le SRNC source met alors en œuvre la procédure *SRNS relocation* pour transférer le rôle de SRNC au SRNC cible ;

– sur la base des résultats de mesure reçus du mobile, le SRNC qui connaît la topologie du réseau décide d'effectuer un *hard-handover* vers une cellule contrôlée par un autre RNC ; il procède alors à une relocalisation de SRNS avant d'établir le nouveau lien.

Les figures 9.14 et 9.15 illustrent les cas de la procédure *SRNS relocation* avec et sans l'utilisation de l'interface « Iur », respectivement. Notons que dans ce dernier cas, la procédure *SRNS relocation* est accompagnée d'un *hard-handover*, c'est-à-dire d'une reconfiguration des ressources physiques.

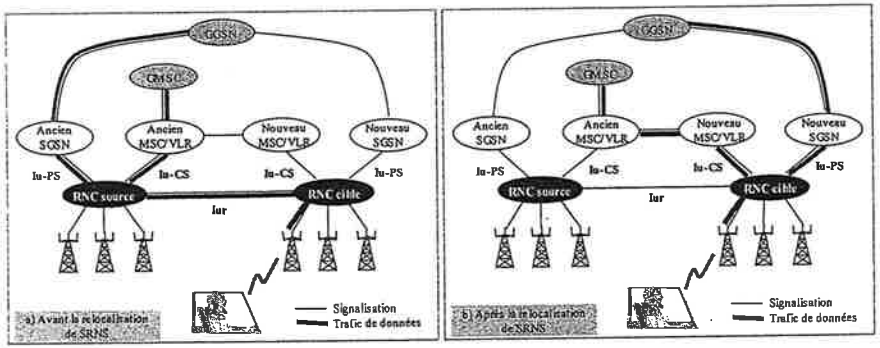


Figure 9.14. *Procédure* SRNS relocation *effectuée avec interface « Iur » supportant le trafic de données générées par l'utilisateur*

Les SRNC source et cible peuvent dépendre du même MSC/VLR (*intra-MSC/VLR SRNS relocation*) ou de MSC/VLR différents (*inter-MSC/VLR SRNS relocation*) pour le domaine circuit. Cela s'applique également au domaine paquet où l'on parlera d'*intra-SGSN SRNS relocation* et d'*inter-SGSN SRNS relocation*.

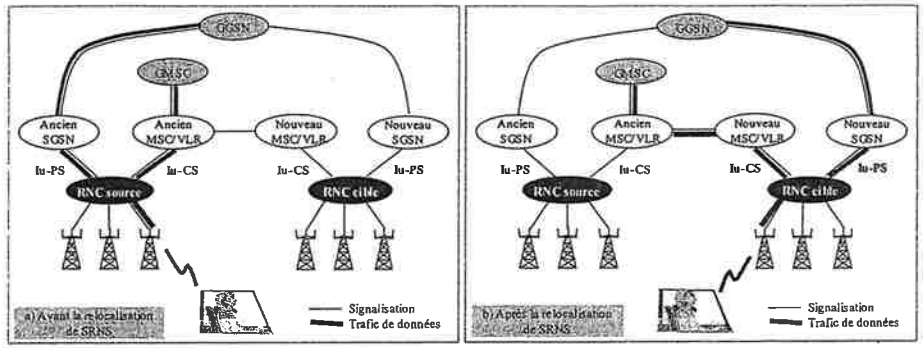


Figure 9.15. *Procédure* SRNS relocation *effectuée sans l'intervention de l'interface « Iur » supportant le trafic de données générées par l'utilisateur*

Lorsque le mobile est connecté aux deux domaines de service (circuit et paquet), la relocalisation doit être effectuée pour les deux domaines et coordonnée par le SRNC cible, le succès de la procédure étant conditionné par la réussite des deux relocalisations.

Les figures 9.16 et 9.17 sont respectivement des exemples de procédure de relocalisation de SRNS inter-MSC/VLR et inter-SGSN (en présence de l'interface Iur).

Lorsque la décision de procéder à une relocalisation de SRNS est prise par le SRNS source, celui-ci le fait savoir à son MSC/VLR appelé dans la figure 9.16 ancien MSC/VLR. Ce dernier confectionne alors un message de demande de relocalisation de SRNS (*RELOCATION REQUEST*) destinée au SRNC cible et l'envoie au nouveau MSC/VLR dans un message *PREPARE HANDOVER REQUEST*. Le nouveau MSC/VLR fait suivre la demande de relocalisation au SRNC cible dont l'identité lui est fournie par l'ancien MSC/VLR. Le message *RELOCATION REQUEST* contient toutes les informations sur les ressources à transférer du SRNC source vers le SRNC cible. Ce dernier acquitte la demande après avoir établi les ressources requises. Il faut cependant noter que dans le cas de plusieurs RAB à transférer, si le SRNC cible ne peut pas allouer toutes les ressources demandées, il le fait savoir au SRNC source qui peut alors accepter ou non le transfert partiel des RAB. Dans le cas d'un transfert partiel, les RAB non transférés sont libérés. Le message d'acquittement *RELOCATION REQUEST ACKNOWLEDGE* est envoyé à l'ancien MSC/VLR *via* le nouveau MSC/VLR qui le fait suivre dans un message *PREPARE HANDOVER RESPONSE*.

Après cette phase de préparation, si l'ancien MSC/VLR veut toujours continuer la procédure, il envoie le message *RELOCATION COMMAND* au SRNC source pour lui faire savoir que les ressources sont déjà allouées dans le SRNC cible et, le cas échéant, les RAB à libérer. Le SRNC source déclenche alors l'exécution de la

relocalisation par l'envoi du message *RELOCATION COMMIT* au SRNC cible. Lorsque ce dernier détecte l'exécution de la relocalisation, il le fait savoir au nouveau MSC/VLR par le message *RELOCATION DETECT* et commence à jouer le rôle de RNC serveur (SRNC) pour l'UE concerné auquel il peut attribuer un nouveau U-RNTI. Cela est indiqué par l'UTRAN dans les messages *UTRAN MOBILITY INFORMATION/CONFIRM*.

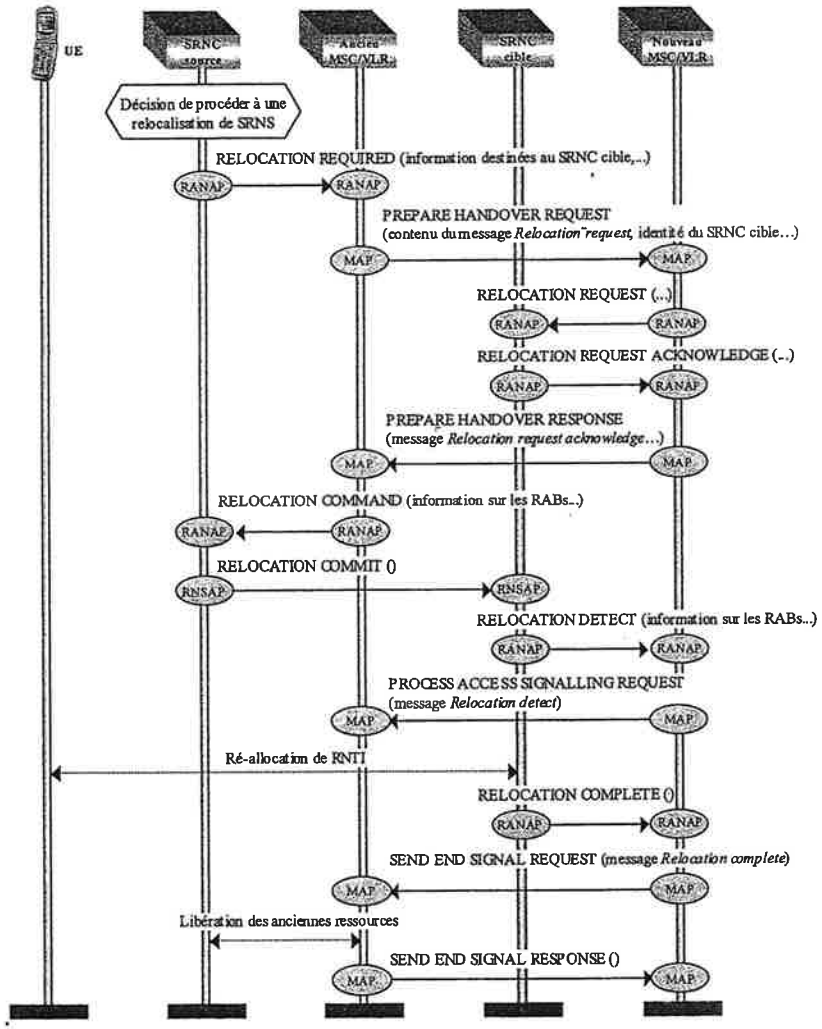


Figure 9.16. *Exemple de procédure* SRNS relocation *inter-MSC/VLR*

Le nouveau MSC/VLR, sur réception du message de détection de l'exécution de la relocalisation le fait suivre à l'ancien dans le message *PROCESS ACCESS SIGNALLING REQUEST* et bascule le transfert de données avec le mobile sur le SRNC cible. Après l'allocation de l'identificateur temporaire au mobile, le SRNC cible envoie à son MSC/VLR un message *RELOCATION COMPLETE* de complétude de la relocalisation. Le nouveau MSC/VLR utilise alors le container *SEND END SIGNAL REQUEST* pour faire suivre ce message à l'ancien MSC/VLR. Celui-ci libère les anciennes ressources et envoie la réponse *SEND END SIGNAL RESPONSE* au nouveau MSC/VLR qui clôt la procédure en libérant les ressources qui étaient mobilisées pour sa conduite.

Le déroulement de la procédure *SRNS relocation* inter-SGSN (cf. figure 9.17) est quasi identique au cas de l'exemple de la figure 9.16. Les seules différences que l'on peut noter sont les suivantes :

– le remplacement des messages container MAP par des messages container GTP ;

– la mise à jour des contextes PDP auprès du GGSN ;

– après réception du message *RELOCATION COMMIT*, le SRNC source arrête l'envoi de paquets vers le mobile et transfert les paquets temporisés (reçus par le GGSN) vers le SRNC cible ;

– sous la demande du nouveau SRNC lors des échanges liés à la ré-allocation du RNTI, le mobile effectue la procédure *RA updating*.

9.6.4. Le détachement du réseau

Comme pour l'attachement, deux procédures différentes *IMSI detach* et *GPRS detach* sont utilisées par la couche MM/GMM pour le détachement du mobile du réseau cœur.

La procédure IMSI detach

La procédure *IMSI detach* est engagée par le mobile et optionnellement par le réseau. Elle est utilisée par l'UE pour se détacher du domaine de services circuit lors de sa mise hors tension ou lorsque la carte USIM lui est retirée en étant sous tension. La procédure consiste en l'envoi par le mobile d'un message d'indication *IMSI DETACH INDICATION* à destination du MSC/VLR. Comme pour l'*IMSI attach*, la nécessité d'engager la procédure est indiquée au mobile dans les informations système spécifiques aux domaines circuit diffusées dans le message SIB1.

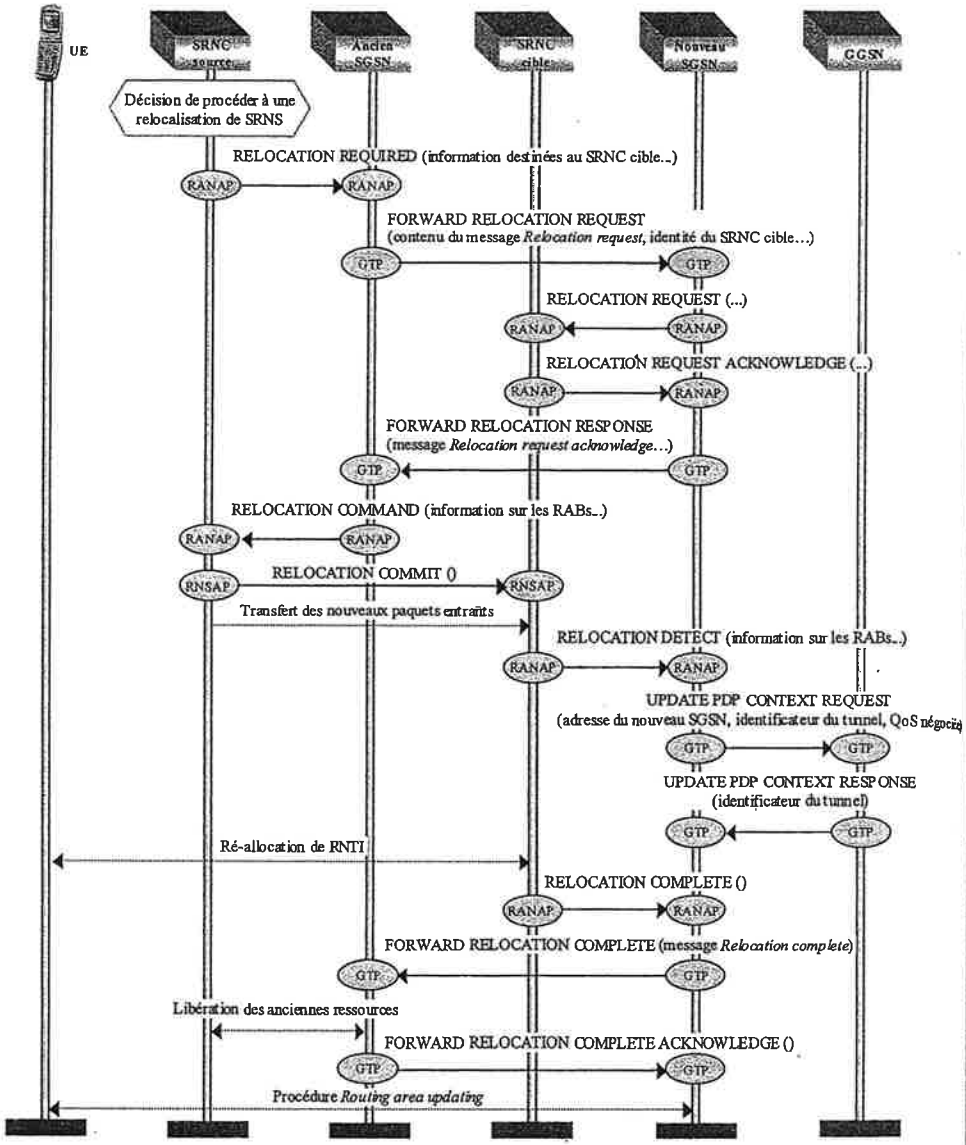


Figure 9.17. *Exemple de procédure* SRNS relocation *inter-SGSN*

La procédure GPRS detach

La procédure *GPRS detach* peut être engagée aussi bien par le mobile que par le réseau. Elle est engagée par l'UE pour les mêmes raisons que l'*IMSI detach* (mise hors tension, retrait de l'USIM) et par le réseau lorsque par exemple une panne a entraîné une perte de contexte. Elle peut être utilisée pour un détachement simple du domaine paquet, un détachement combiné des domaines paquet et circuit, mais aussi pour un détachement simple du domaine circuit. La procédure est engagée avec le message *DETACH REQUEST* qui est acquitté avec le message *DETACH ACCEPT* lorsque la cause de détachement n'est pas une mise hors tension du mobile.

9.7. L'établissement d'appel

La fonction principale d'un réseau de télécommunications est de passer des appels pour accéder à des services et cette fonction est assurée dans le mobile par la sous-couche CM. Celle-ci est libérée des préoccupations liées à la gestion de l'interface radio (transfert fiable et sécurisé des messages, changement de cellule, etc.) et à la gestion de la mobilité (sélection de PLMN, mise à jour de localisation, etc.) qui sont assurées respectivement par les protocoles RRC et MM/GMM.

9.7.1. Appel circuit

Les appels peuvent être déclenchés par le mobile (appel sortant) ou par le réseau (appel entrant) et pour différents types de services (téléphonie, visiophonie, data...). La figure 9.18 est un exemple d'appel sortant vers le domaine circuit.

Sur demande d'une application, la sous-couche CM du mobile déclenche la procédure d'établissement d'appel par une demande de service adressée à la sous-couche MM. Le message de demande de service est transmis au RNC dans un message RRC *INITIAL DIRECT TRANSFER* avec indication du domaine circuit comme destinataire. Le RNC établit une connexion de signalisation (connexion Iu) avec le MSC/VLR et lui fait suivre le message CM *SERVICE REQUEST*. Ce message contient le type de service demandé (établissement d'appel normal, établissement d'appel d'urgence, envoi de SMS, activation de service supplémentaire), l'identité du mobile, etc.

Après la sécurisation de la liaison par l'authentification et l'activation du chiffrement et de l'intégrité, le mobile envoie au MSC le message CC *SETUP* qui contient toutes les informations nécessaires à l'établissement de l'appel.

Si le MSC/VLR juge l'appel recevable, il peut envoyer au mobile un message *CALL PROCEEDING* pour lui indiquer que la demande d'appel est acceptée et est en train d'être traitée. Si requises par le service demandé, les ressources radio (RAB) radio sont établies. Le MSC/VLR peut également envoyer au mobile un message *ALERTING* lorsque l'usager distant a commencé à être sonné. Sur réception de ce message, le

mobile appelant génère, en local, une indication de sonnerie d'appel, qui peut également être générée par le réseau si le *codec* est déjà activé.

Lorsque l'usager distant accepte l'appel, le MSC/VLR l'indique au mobile par un message *CONNECT*. Le mobile active alors le *codec*, envoie un acquittement *CONNECT ACKNOWLEDGE* au réseau et arrête la sonnerie locale si elle a été générée.

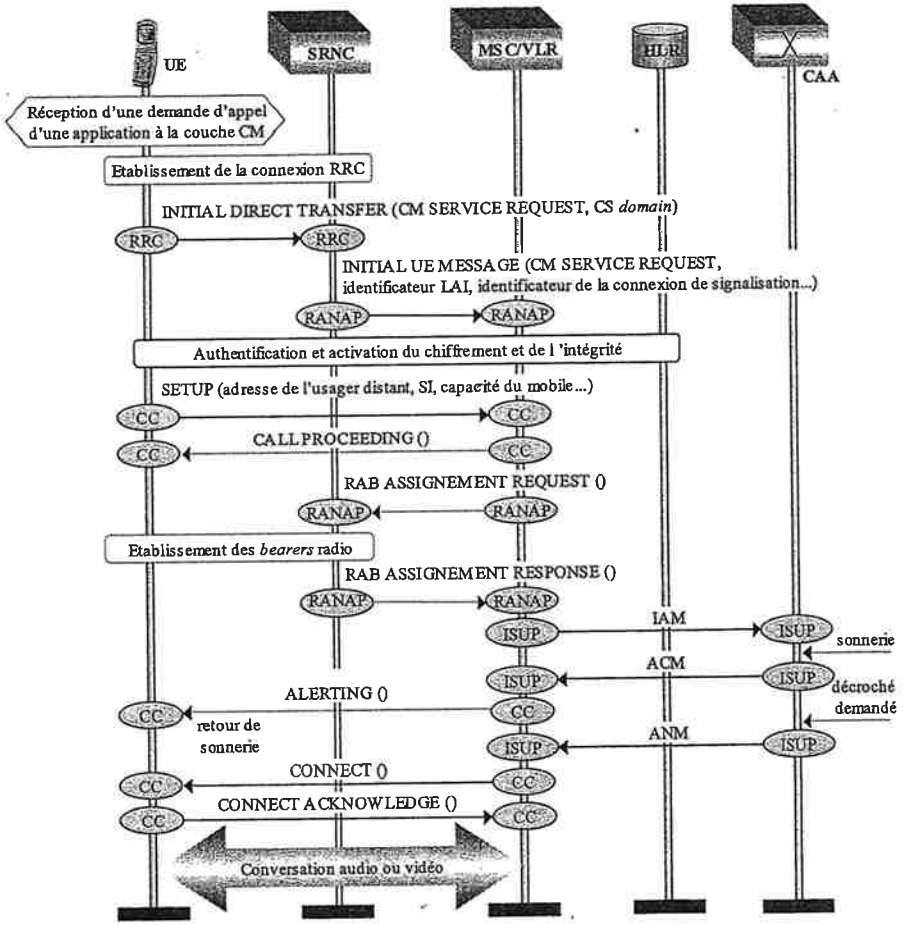


Figure 9.18. *Procédure d'appel sortant dans le domaine circuit*

Par rapport à un appel sortant, un appel entrant présente quelques différences sur le déroulement de la procédure. En effet, l'appel entrant est engagé par le réseau avec un message de *paging*. Sur réception de ce message, la couche RRC du mobile informe la couche MM et établit une connexion RRC si ce n'était pas encore fait. Puis le container *INITIAL DIRECT TRANSFER* est utilisé par la couche RRC pour convoyer vers le SRNC le message MM *PAGING RESPONSE* de réponse au *paging*, avec indication du domaine de service concerné en l'occurrence le domaine CS. Le SRNC utilise le container RANAP *INITIAL UE MESSAGE* pour remettre le message *PAGING RESPONSE* au MSC/VLR. Ensuite, le MSC/VLR déroule les procédures de sécurisation de la liaison et envoie au mobile le message de *SETUP*. La couche CC du mobile peut alors confirmer par un message *CALL CONFIRMED* la réception de cette demande d'établissement d'appel, puis envoyer au réseau un message *ALERTING* dès que le signal d'appel est généré au niveau du mobile. La procédure d'appel entrant se termine par l'envoi d'un message *CONNECT* par le mobile et son acquittement par le réseau avec un message *CONNECT ACKNOWLEDGE*.

9.7.2. Appel paquet

L'établissement d'un appel (session) dans le domaine paquet consiste souvent en l'activation d'un contexte PDP (*PDP Context*) à l'initiative du mobile ou du réseau, pour le transfert de données usager. Un service tel que l'envoi de SMS ne nécessite pas d'activation de contexte PDP, seule une connexion de service étant établie avant le transfert de message. La figure 9.19 est un exemple d'activation de contexte PDP à l'initiative du réseau.

Au départ de la procédure illustrée par l'exemple de la figure 9.19, le mobile est attaché au domaine paquet et la connexion RRC entre l'UTRAN et le mobile n'est pas établie (le mobile est dans l'état veille RRC). La procédure d'appel entrant est déclenchée lorsque le GGSN reçoit du réseau externe à commutation de paquets un PDU, consistant dans cet exemple en une demande d'établissement de contexte PDP. Si aucun contexte PDP n'est établi pour le mobile adressé, le GGSN demande au HLR les informations nécessaires au routage de l'appel (message *MAP SEND ROUTING INFORMATION FOR GPRS*). Si le mobile est joignable, le HLR fournit au GGSN l'adresse du SGSN contrôlant la RA où se trouve le mobile. Le GGSN notifie alors la demande d'activation de contexte PDP au SGSN, qui, après certaines vérifications (IMSI connu, mobile bien attaché...), accepte la requête et envoie une demande de *paging* au RNC serveur du mobile. Puisqu'aucune connexion RRC n'est établie entre le mobile et le RNC, ce dernier envoie un message de *paging* de type 1 (un *paging* de type 2 aurait été envoyé si une connexion RRC était établie).

Sur réception du message de *paging*, le mobile procède à l'établissement d'une connexion RRC, puis envoie au réseau une demande de service avec comme cause la réponse à un *paging* (*paging response*). Ce message est envoyé dans le container RRC *INITIAL DIRECT TRANSFER* au RNC et relayé par celui-ci vers le SGSN dans un container RANAP *INITIAL UE MESSAGE*, le routage étant effectué grâce au paramètre *PS domain* indiquant que le message est destiné au domaine paquet.

Après une sécurisation réussie de la liaison par l'authentification et l'activation du chiffrement et de l'intégrité, le SGSN envoie la requête d'établissement de contexte PDP au mobile *via* le RNC. Le mobile envoie alors la commande d'activation de contexte PDP au SGSN qui, à son tour, demande au GGSN la création du contexte PDP, procède à l'établissement des ressources radio (RAB) et acquitte positivement la demande du mobile par l'envoi d'un message d'acceptation de la commande d'activation de contexte PDP. A partir de là, le canal de trafic est considéré établi et le transfert des données usager peut commencer.

Pour un appel sortant la procédure commence par la demande de service envoyée par le mobile au réseau avec comme cause une signalisation de niveau CM (*SIGNALLING*). Une connexion RRC est établie si elle ne l'est pas encore, puis la demande de service est envoyée dans un container RRC *INITIAL DIRECT TRANSFER* au RNC. Sur acceptation par le réseau de la demande de service, le mobile engage l'activation proprement dite du contexte PDP et la suite de la procédure est similaire au cas de l'appel entrant.

Un contexte PDP actif peut être modifié à l'initiative du mobile, du SGSN ou du GGSN. La modification concerne certains des paramètres qui ont été négociés lors de l'activation telle que par exemple la QoS. Une procédure de modification de contexte PDP est par exemple déclenchée par le SGSN lorsqu'une donnée d'abonnement telle que la QoS souscrite est modifiée par le HLR. Sur rupture de la liaison radio ou détection d'une situation d'inactivité, le RNC peut libérer les RAB ou la connexion Iu avec comme conséquence la modification locale des contextes PDP dans le mobile et le réseau pour des trafics de type *streaming* ou conversationnel, afin de suspendre l'envoi des paquets de données. Après rétablissement de la connexion radio, le mobile réactive les contextes PDP à l'aide de la procédure de modification de contexte PDP.

Comme pour l'activation et la modification, une désactivation de contexte PDP peut être effectuée à l'initiative du mobile, du SGSN ou du GGSN. La procédure *PDP Context Deactivation* s'appuie sur les messages *DELETE PDP CONTEXT REQUEST* et *DELETE PDP CONTEXT RESPONSE* entre SGSN et GGSN, et les messages *DEACTIVATE PDP CONTEXT REQUEST* et *DEACTIVATE PDP CONTEXT ACCEPT* entre le mobile et le SGSN. Après l'échange de ces messages, la procédure se termine par la libération des ressources radio.

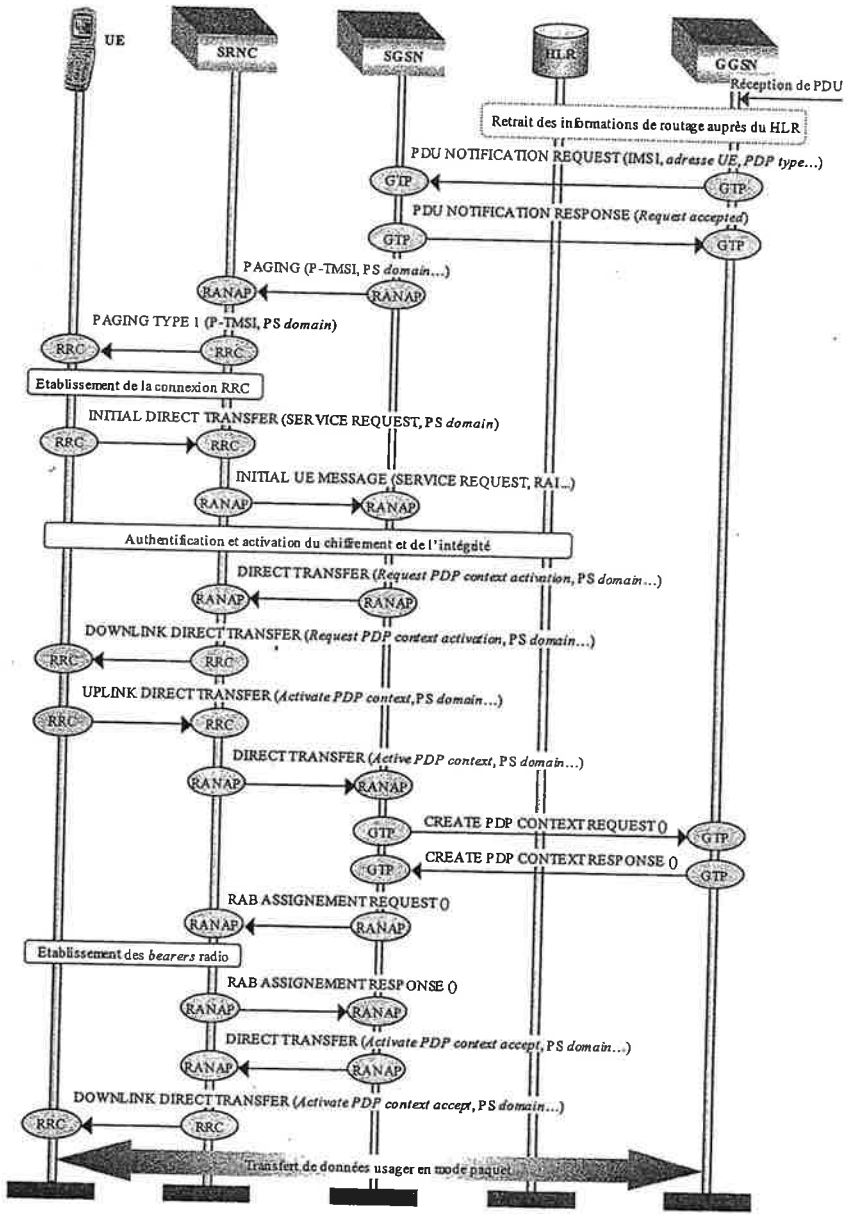


Figure 9.19. *Exemple d'établissement d'un contexte PDP à l'initiative du réseau*

9.8. *Handover* intersystème entre réseaux GSM et UMTS

Comme cela a été étudié dans le chapitre 4, les spécifications techniques du 3GPP permettent à un terminal bimode Type 2 d'être itinérant dans un réseau GSM et UMTS, et ce pour des services en mode circuit et paquet – pourvu que ces derniers soient supportés par le réseau d'accueil.

9.8.1. Handover *intersystème en mode circuit : UMTS vers GSM*

La figure 9.20 illustre un exemple des échanges de signalisation nécessaires à faire basculer une communication en cours d'un réseau UMTS vers un réseau GSM. Les deux réseaux peuvent appartenir au même opérateur ou à des opérateurs différents et partager ou non le même MSC. Dans cet exemple, on considère que le basculement est du type inter-MSC.

Suite à des mesures effectuées par l'UE, le SRNC fait savoir au 3G-MSC de la nécessité de basculer vers une cellule GSM de meilleure qualité que la cellule UMTS courante (message RANAP *RELOCATION REQUIRED*). Grâce à l'interface « E », le 3G-MSC envoie à son homologue 2G-MSC la demande de *handover* à travers le message MAP *PREPARE HANDOVER*. Ce dernier va ensuite transférer cette requête vers le BSC (GSM) correspondant en utilisant le message BSSMAP *HANDOVER REQUEST*. Le BSC se met en contacte avec la BTS GSM cible laquelle va préparer les ressources radio correspondantes qui seront indiquées au mobile dans le message BSSMAP *HANDOVER REQUEST ACK*. Ce message sera encapsulé dans le message MAP *PREPARE HANDOVER RESPONSE* et envoyé au 3G-MSC. A sa réception, le 3G-MSC doit négocier avec le 2G-MSC l'établissement d'une connexion en mode circuit à l'aide de la signalisation ISUP.

Lorsque le circuit est établi entre les deux MSC, le 3G-MSC donne l'ordre à l'UE de basculer vers la cellule GSM par l'intermédiaire du SRNC qui génère le message RRC *HANDOVER FROM UTRAN COMMAND*. Une fois que l'UE a achevé avec succès l'accès radio à la cellule GSM, le BSC le communique au 2G-MSC à travers le message *HANDOVER DETECT*. Le message *HANDOVER COMPLETE* est utilisé par l'UE pour indiquer au BSC et au 2G-MSC que le *handover* s'est bien déroulé. Ce message est encapsulé dans un message MAP *SEND END SIGNALLING REQUEST* et il est ensuite transféré au 3G-MSC dans le but de lui signaler que le SRNC peut d'ores et déjà libérer les ressources au niveau de l'interface Iu. A ce stade, la communication en mode circuit reprend dans la cellule GSM en tenant compte du fait que le chemin des données usager est : destinataire ↔ 3G-MSC ↔ 2G-MSC ↔ BSC ↔ UE alors qu'avant le *handover* il était : destinataire ↔ 3G-MSC ↔ RNC ↔ UE. Notons que le 3G-MSC garde le contrôle de la communication et c'est lui qui signale la fin de l'appel au 2G-MSC à l'aide de la signalisation ISUP et du message MAP *SEND END SIGNAL RESPONSE*.

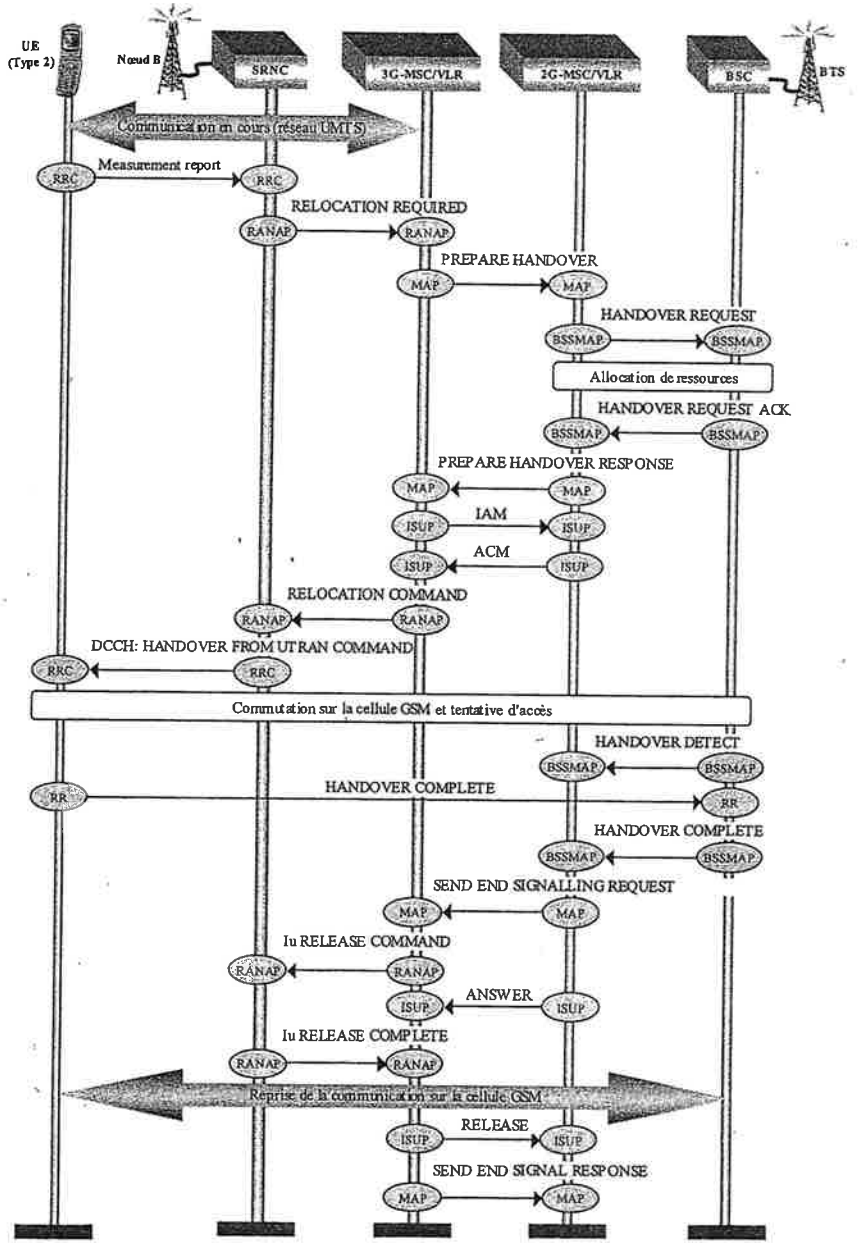


Figure 9.20. *Exemple d'un* handover *inter-MSC d'un réseau UMTS vers un réseau GSM*

9.8.2. Handover *intersystème en mode circuit : GSM vers UMTS*

Il existe une équivalence exacte entre les messages de signalisation liés au *handover* générés par les couches RR/BSSMAP/MAP (GSM) et les messages générés par les couches RRC/RANAP/MAP (UMTS). Aussi, la description du déroulement de la procédure de *handover* de l'UMTS vers le GSM illustrée par la figure 9.20, est valable pour le cas d'un *handover* intersystème du GSM vers l'UMTS illustré par la figure 9.21.

Il faut noter qu'après avoir effectué avec succès le basculement de la communication de la cellule GSM vers la cellule UMTS, le contrôle de la connexion reste sous la responsabilité du 2G-MSC.

9.8.3. *Commutation intersystème en mode paquet : UMTS vers GPRS*

On étudie ici le cas où l'UE bascule d'une cellule UMTS vers une cellule GPRS. Les procédures à effectuer dépendent de l'état de service du mobile avant le changement de cellule :

– l'UE est dans l'état GMM-IDLE. Lorsque les RA des réseaux UMTS et GPRS sont différentes, la procédure GPRS *routing area updating* est effectuée. Si les réseaux GPRS et UMTS partagent la même RA, la procédure GPRS *routing area updating* est accomplie selon une variante nommée « *Selective RA update* » [TS 23.060],

– l'UE est dans l'état GMM-CONNECTED. Dans ce cas, l'UE effectue la procédure GPRS *routing area updating* qu'il s'agisse ou non de la même RA. Une mise à jour combinée de RA/LA peut aussi être effectuée.

La figure 9.22a, montre le cas où les réseaux radio du GSM et de l'UMTS partagent un même SGSN. Dans cet exemple, on suppose que l'UE est dans l'état GMM-CONNECTED et qu'il est engagé dans la transmission de paquets au moment de la prise de décision par le SRNC de basculer vers une cellule GPRS. Lorsque la décision est prise, l'UE arrête la transmission.

Après avoir établi une connexion LLC (propre au GPRS), entre l'UE et le SGSN, l'UE envoie le message GMM *ROUTING AREA UPDATE REQUEST* via le réseau radio GSM. Puisque l'UE transmettait des paquets usager avant le basculement, le SGSN échange les messages RANAP *SRNS CONTEXT REQUEST & RESPONSE* avec le SRNC dans le but d'obtenir les paramètres GTP-SND, GTP-SNU et PDCP-SND et de reprendre la transmission de paquets dans les voies montante et descendante avec un minimum de pertes.

A ce stade, le SRNC arrête l'envoi de paquets vers l'UE et commence à temporiser les nouveaux paquets venant du GGSN. Avant de continuer, le SGSN peut vérifier l'identité de l'UE et ses conditions d'abonnement. En cas de problème, le SGSN rejettera la demande de mise à jour de la RA. Dans le cas contraire, le SGSN envoie au SRNC le message RANAP *DATA FORWARD COMMAND* pour que celui-ci lui transfère les paquets temporisés qui non pas encore été remis à l'UE. Au bout d'une certaine période, la connexion Iu est libérée. Le SGSN remet à jour le contexte PDP et alloue si nécessaire un nouveau P-TMSI à l'UE indiqué dans le message GMM *ROUTING AREA UPDATE ACCEPT*. L'UE envoie enfin le message GMM *ROUTING AREA UPDATE COMPLETE* dans le cas d'une ré-allocation de P-TMSI.

9.8.4. *Commutation intersystème en mode paquet : GPRS vers UMTS*

Les mêmes règles considérées pour le passage d'une cellule UMTS vers une cellule GPRS s'appliquent au cas du basculement d'une cellule GPRS vers une cellule UMTS. Il faut simplement tenir compte du fait que l'état GPRS-STANDBY est équivalent à l'état GMM-IDLE et que l'état GPRS-READY est équivalent à l'état GMM-CONNECTED.

La figure 9.22b illustre un exemple des échanges entre l'UE et le réseau lorsque le BSC décide de basculer d'une cellule GPRS vers une cellule UMTS. On suppose que l'UE est dans l'état GPRS-READY avant que le BSC prenne la décision de basculer vers une cellule UMTS. Cet exemple s'applique dans le cas où l'UE est en train de transmettre des paquets avant le changement de réseau. Après avoir reçu l'ordre, il doit arrêter la connexion LLC et effectuer la procédure de mise à jour de RA dans le réseau UMTS (cf. figure 9.22b).

En comparant les exemples des figures 9.22a et 9.22b, la principale différence repose sur le fait qu'il n'y a pas de retransmission de paquets du BSC vers le SGSN. Les données sont en effet temporisées dans le SGSN lui-même. L'allocation de ressources radio pour la reprise de la transmission de paquets dans la voie montante et descendante est également différente en raison de la différence des technologies radio.

REMARQUE.– Dans le cas d'un basculement inter-SGSN, le nouveau SGSN doit demander à l'ancien SGSN, après réception du message *ROUTING AREA UPDATE REQUEST*, les caractéristiques des contextes PDP actifs à l'aide du message GTP *SGSN CONTEXT REQUEST* [TS 23.060].

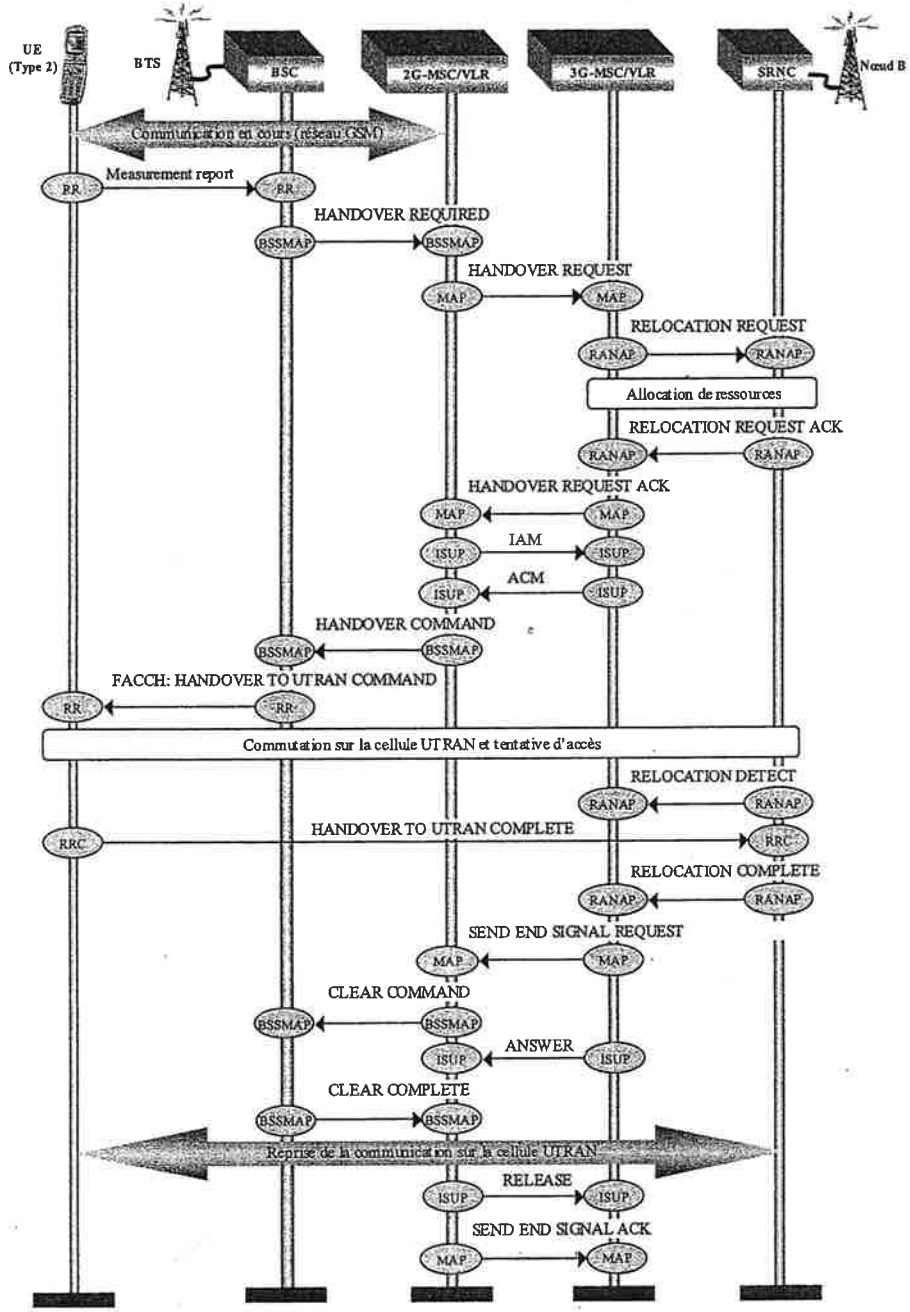


Figure 9.21. *Exemple d'un* handover *inter-MSC d'un réseau GSM vers un réseau UMTS*

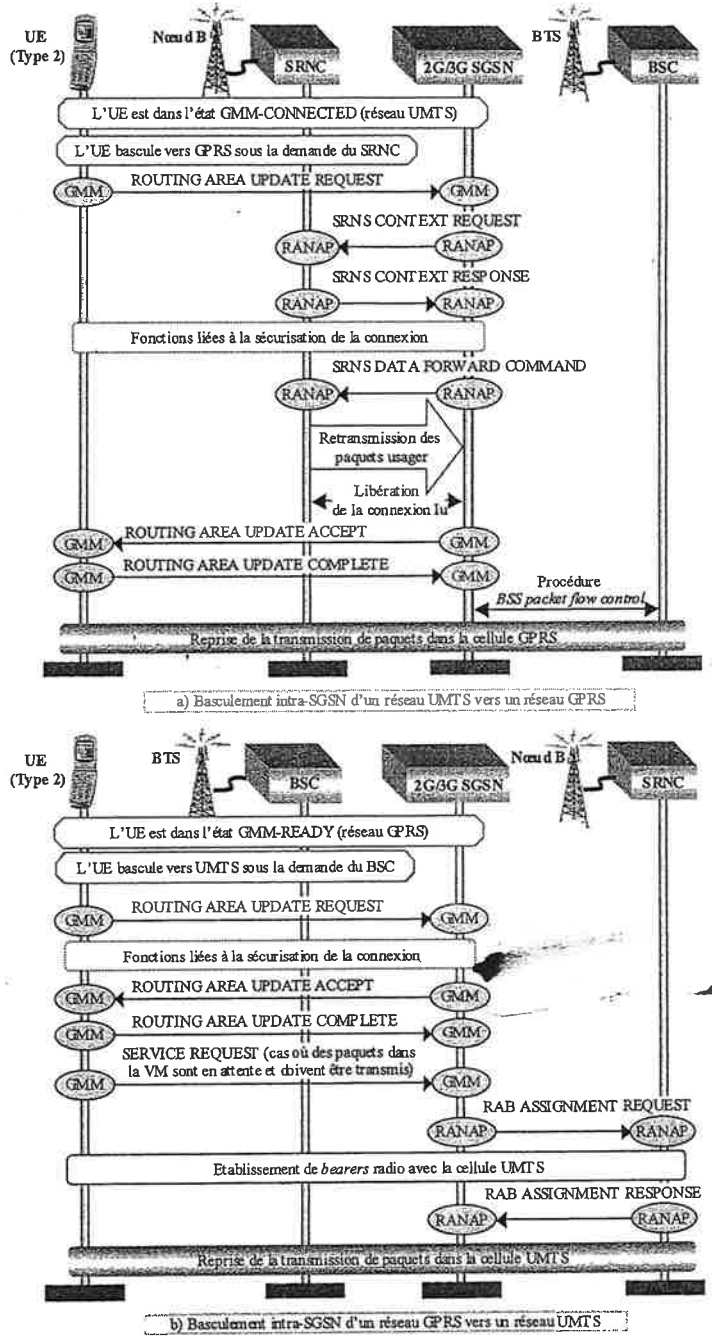


Figure 9.22. *Exemples d'un changement de cellule intersystème pour un service paquet*