Titre: Title:	Mécanismes de contrôle basés sur IP dans une architecture UMTS évoluée
Auteur: Author:	Youssef Eddahbi
Date:	2005
Type:	Mémoire ou thèse / Dissertation or Thesis
Référence: Citation:	Eddahbi, Y. (2005). Mécanismes de contrôle basés sur IP dans une architecture UMTS évoluée [Master's thesis, École Polytechnique de Montréal]. PolyPublie. https://publications.polymtl.ca/7370/

URL de PolyPublie: PolyPublie URL:	https://publications.polymtl.ca/7370/
Directeurs de recherche: Advisors:	Samuel Pierre
Programme: Program:	Génie informatique

UNIVERSITÉ DE MONTRÉAL

MÉCANISMES DE CONTRÔLE BASÉS SUR IP DANS UNE ARCHITECTURE UMTS ÉVOLUÉE

YOUSSEF EDDAHBI
DÉPARTEMENT DE GÉNIE INFORMATIQUE
ÉCOLE POLYTECHNIQUE DE MONTRÉAL

MÉMOIRE PRÉSENTÉ EN VUE DE L'OBTENTION
DU DIPLÔME DE MAÎTRISE ÈS SCIENCES APPLIQUÉES
(GÉNIE INFORMATIQUE)
AVRIL 2005

Your file Votre référence
ISBN: 0-494-01315-X
Our file Notre référence
ISBN: 0-494-01315-X

UNIVERSITÉ DE MONTRÉAL
ÉCOLE POLYTECHNIQUE DE MONTRÉAL

Ce mémoire intitulé :

MÉCANISMES DE CONTRÔLE BASÉS SUR IP DANS UNE ARCHITECTURE UMTS ÉVOLUÉE

présenté par : EDDAHBI Youssef
en vue de l'obtention du diplôme de : Maîtrise ès sciences appliquées
a été dûment accepté par le jury d'examen constitué de :

M. CHAMBERLAND Steven, Ph.D., président
M. PIERRE Samuel, Ph.D, directeur de recherche et membre
M. QUINTERO Alejandro, Doct., membre

REMERCIEMENTS

À mon directeur de recherche, M. Samuel Pierre, pour son soutien et ses conseils tout au long de ce projet de recherche.

À M. Laurent Marchand, M. Yves Lemieux ainsi que toute l'équipe du centre de recherche de Ericsson Canada, pour leurs conseils et leur aide technique indispensable à la réalisation de ce projet.

À mes parents, mon frère, ma sœur et mes amis, pour leur soutien continu durant mes études.

Enfin, à mes collègues du LARIM, avec qui j'ai eu l'occasion d'échanger et de collaborer durant mon séjour au laboratoire.

RÉSUMÉ

Les premiers réseaux cellulaires 3G entrent en opération à plusieurs endroits dans le monde. Ils promettent des services variés et des débits de données atteignant 2 Mbits/sec. Ils marquent le début de la convergence entre Internet et les réseaux mobiles. Pour la prochaine évolution, on envisage déjà une architecture toute-IP (All-IP). Dans les réseaux mobiles de prochaines générations, les communications utiliseront IP de bout en bout, les débits de données seront plus élevés et les nœuds mobiles profiteront d'une mobilité globale, c'est-à-dire qu'ils pourront accéder à un service réseau IP à partir de plusieurs technologies d'accès différentes (multi-accès). Cette évolution se fera par itération et nécessitera une intégration des mécanismes de signalisation basés sur IP avec les mécanismes de signalisation des différents types de réseaux d'accès.

Dans ce mémoire, nous nous intéressons à la technologie de troisième génération de type UMTS (*Universal Mobile Telecommunications System*). Dans ce type de système, les mécanismes de contrôle utilisent des protocoles spécifiques à UMTS, définis par l'organisme 3GPP (*3rd Generation Partnership Project*). L'utilisation de protocoles de contrôle spécifiques rend toutefois l'intégration avec d'autres technologies d'accès plus difficile. En effet, il serait souhaitable de pouvoir utiliser les mêmes mécanismes de contrôle avec n'importe quel type de technologie d'accès.

Dans cette visée, nous proposons un scénario d'évolution pour la technologie UMTS, qui facilitera l'intégration avec d'autres technologies d'accès dans le contexte des réseaux mobiles de prochaines générations. Nous définissons une architecture UMTS évoluée qui utilise un réseau cœur IPv6 où sont déployés des protocoles de contrôle basés sur IP, défini par l'IETF (*The Internet Engineering Task Force*). Plus particulièrement, nous abordons les mécanismes d'authentification, de signalisation de qualité de service et de gestion de la mobilité. De plus, nous souhaitons que notre proposition ait un impact minimal sur le réseau d'accès radio de UMTS. Pour ce faire, nous définissons une mise en correspondance des protocoles de contrôle IPv6 et UMTS afin de réutiliser la signalisation existante à l'intérieur du

réseau d'accès radio.

Un modèle analytique nous permet d'analyser la performance de notre proposition pour l'aspect de la gestion de la mobilité. Nous évaluons comment l'architecture évoluée UMTS, ainsi que la mise en correspondance de protocole de contrôle peuvent améliorer la performance de la relève inter-technologique, dans un environnement où il y a des zones de couverture UMTS et WLAN (*Wireless Local Area Network*). Nous comparons notre proposition par rapport à une approche conventionnelle utilisant un système UMTS standard, en calculant le délai moyen de la relève inter-technologique lors du déplacement d'un nœud mobile. Nous constatons que notre proposition améliore considérablement le délai moyen de la relève inter-technologique entre un système UMTS et WLAN. Nous remarquons aussi que le gain de performance tient surtout de la mise en correspondance de protocoles plutôt que de l'intégration des protocoles basés sur IP à l'intérieur du réseau cœur. Nous en concluons que notre proposition devrait être avantageuse, surtout dans des environnements urbains où la densité de zones de couverture WLAN est élevée.

ABSTRACT

In several places worldwide, the first 3G wireless networks are being deployed. They promise to offer various services and data throughputs reaching 2Mbits/sec. This marks the beginning of the convergence between the Internet and wireless networks. For the next evolution of wireless networks, an All-IP architecture is already anticipated. In next generation mobile networks, communications will use the IP protocol from end-to-end, data throughputs will increase and mobile units will achieve global mobility, meaning they will be able to gain access to an IP network service from multiple different access technologies (mutli-access). This evolution will be iterative and will require the integration of IP based signalling mechanism with the signalling mechanism of the different types of access networks envisioned.

In this project, we are interested the third generation technology of type UMTS (Universal Mobile Telecommunications System). In this type of system, the signalling mechanism use UMTS specific control protocols, defined by 3GPP (3rd Generation Partnership Project). However, the use of specific control protocols makes the integration with other access technologies more difficult. Indeed, it would be desirable to be able to use the same control mechanisms with any type of access technology.

Accordingly, we propose an evolution scenario for the UMTS technology, which will facilitate the integration with other access technology in the context of next generation mobile networks. We define an evolved architecture, which uses an IPv6 core network where IP-based control protocols, defined by the IETF (The Internet Engineering Task Force), are deployed. Particularly, we are interested in the control mechanism for authentication, quality of service signaling, and mobility management. Moreover, we want our proposition to have a minimal impact on the UMTS radio access network. With this intention, we define a protocol mapping between IPv6 and UMTS control protocols in order to reuse existing signaling within the radio access network.

An analytical model has allowed us to analyze the performance of the mobility management aspect of our proposition. We have evaluated how the evolved

UMTS architecture, in addition to the control protocol mapping may improve the inter-technological handover, in an environment where there is UMTS and WLAN (Wireless Local Area Network) coverage. We compared our proposition with a conventional approach, which uses a standard UMTS system, by calculating the average inter-technological handover delay during the movement of a mobile node. We observed that our proposition considerably improves the inter-technological handover between UMTS and WLAN systems. We also notice that the benefit mostly comes from the mapping of control protocols rather than the integration IP-based protocols into the core network. We conclude from this, that our proposition would be beneficial mostly in an urban environment where there is a higher density of WLAN coverage.

TABLE DES MATIÈRES

LISTE DES FIGURES

LISTE DES TABLEAUX

LISTE DES SIGLES ET ABRÉVIATIONS

2G	Deuxième Génération
3G	Troisième Génération
3GPP	Third Generation Partnership Project
3GPP2	Third Generation Partnership Project 2
4G	Quatrième Génération
AAA	Authentication, Authorization and Accounting
AES	Advanced Encryption Standard
AKA	Authentication and Key Agreement
AMPS	Advanced Mobile Phone System
AR	Access Router
AuC	Authentication Center
AUTN	Authentication Token
BU	Binding Update
BU	Binding Update
CDMA	Code Division Multiple Access
CK	Cipher Key
CoA	Care-of Address
CS	Circuit Switched
DAD	Duplication Address Detection
DRNC	Drifting Radio Network Controller
EAP	Extensible Authentication Protocol
EIR	Equipment Identity Register
FDMA	Frequency Division Multiple Access
GGSN	Gateway GPRS Support Node
GIF	GPRS Interworking Function
GMM	GPRS Mobility Management
GMSC	Gateway Mobile Switching Center
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications

GTP-C	GPRS Tunnelling Protocol – Control Plane
GTP-U	GPRS Tunnelling Protocol – User Plane
HA	Home Agent
HLR	Home Location Register
HMIPv6	Hierarchical MIPv6
HPMRSVP	Hierarchical Proxy Mobile Resource Reservation Protocol
IK	Integrity Key
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPv6	Internet Protocol version 6
ITU	International Telecommunication Union
LA	Location Area
LBU	Local Binding Update
LCoA	Local Care-of Address
MAC	Medium Access Layer
MAP	Mobile Anchor Point
MAP-SS7	Mobile Application Part
MIPv6	Mobile IP version 6
MN	Mobile Node
MSC/VLR	Mobile Switching Center/Visitor Location Register
NAS	Network Access Server
NC	Corresponding Node
PDCP	Packet Data Convergence Protocol
PDP	Packet Data Protocol
PS	Packet Switched
P-TMSI	Packet – Temporary Mobile Subscriber Identity
RA	Routing Area
RAB	Radio Access Bearer
RAI	Routing Area Identification
RANAP	Radio Access Network Application Part
RCoA	Regional Care-of Address
RLC	Radio Link Layer

RNC	Radio Network Controller
RRC	Radio Resource Control
RSVP	Resource Reservation Protocol
SCCP	Signalling Connection Control Part
SGSN	Serving GPRS Support Node
SM	Session Management
SQN	Sequence Number
SRNC	Serving Radio Network Controller
TCAP	Transaction Capabilities Application Part
TDMA	Time Division Multiple Access
UMTS	Universal Mobile Telecommunications System
UTRAN	UMTS Terrestrial Radio Access Network
WAF	WLAN Adaptation Function
WCDMA	Wideband Code Division Multiple Access
WLAN	Wireless Local Area Network

CHAPITRE 1

INTRODUCTION

Les premiers réseaux cellulaires de troisième génération (3G) entrent en opération à quelques endroits dans le monde. Les réseaux 3G promettent d'offrir des services variés et des transmissions de données atteignant 2 Mbits/sec (Mbps), ce qui permettra le déploiement d'applications plus gourmandes en bande passante. Ils marquent le début de la convergence entre Internet et les réseaux mobiles. Pour la prochaine évolution des réseaux mobiles, on projette une architecture *tout-IP* (*All-IP*). Les communications utiliseront le protocole Internet (IP) de bout en bout, les débits de données seront plus élevés (possiblement plusieurs dizaines de Mbps) et les utilisateurs profiteront d'une mobilité globale. On entend par *mobilité globale* la capacité d'avoir un accès continu à un service à partir de différents types de réseau d'accès et ce, à n'importe quel endroit dans le monde. Les terminaux mobiles multi-accès doivent être en mesure de contrôler leur accès au réseau, indépendamment de la technologie d'accès utilisée. L'évolution vers ces réseaux de prochaines générations sera itérative et se fera à partir des réseaux mobiles existants. Il est donc essentiel d'envisager une intégration des mécanismes de contrôle basés sur IP avec les mécanismes des différents types de réseaux d'accès aujourd'hui disponibles (LAN, WLAN, UMTS, CDMA2000, Bluetooth, etc.), objet de ce mémoire.

Dans ce premier chapitre, nous introduisons quelques concepts de base relatifs aux réseaux multi-accès, présentons ensuite quelques aspects de la problématique, formulons les objectifs de recherche et terminons par un bref aperçu de la suite de ce mémoire.

1.1 Définitions et concepts de base

Bien qu'il n'y ait pas encore de consensus sur la définition exacte de ce que sera la quatrième génération (4G) des réseaux mobiles, on s'entend pour dire que les réseaux de prochaines générations seront des réseaux dits *multi-accès*. Cela signifie que les utilisateurs pourront accéder à un service réseau grâce à plusieurs types de réseaux d'accès différents. Les multiples réseaux d'accès hétérogènes seront reliés à un même réseau de transport IP. Les terminaux mobiles pourront passer d'une technologie d'accès à une autre sans discontinuité du service.

En principe, la technologie d'accès employée devrait être complètement transparente pour l'utilisateur ou l'application qui utilise le service réseau. Pour ce faire, on s'entend pour utiliser IP comme protocole commun à toutes les technologies d'accès. Les applications sur le terminal n'utiliseront que le service IP et des protocoles de contrôle basés sur IP. Les paquets IP seront ensuite adaptés et transportés par les couches sous-jacentes des différentes technologies d'accès déployées. La Figure 1.1 illustre une architecture typique d'un réseau multi-accès.

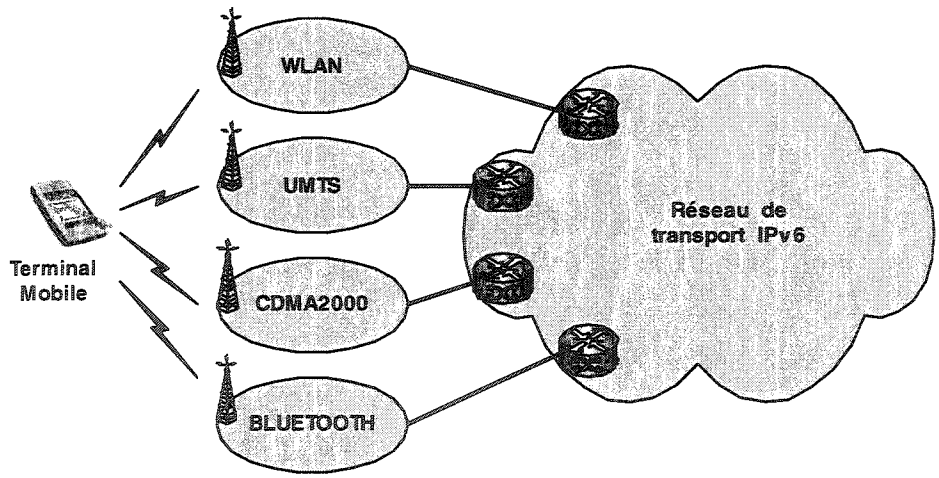

Figure 1.1 Architecture d'un réseau mobile multi-accès

Les *protocoles de contrôle* permettent à l'usager ainsi qu'au réseau de contrôler l'accès et l'utilisation des ressources du réseau. Ils servent à authentifier et autoriser

l'usager et/ou le réseau, à gérer la mobilité des usagers dans le réseau, à signaler la connexion afin d'assurer une certaine qualité de service, à imputer des frais pour l'utilisation du réseau ou encore à exploiter et surveiller les ressources du réseau, que ces ressources soient radio ou filaire. Normalement, chaque technologie d'accès possède ses propres mécanismes de contrôle. Il n'est cependant pas souhaitable qu'une application doive employer les mécanismes de contrôle de chacune des technologies d'accès déployées afin d'obtenir un service réseau. Ainsi, dans le but de faire abstraction de chacun des mécanismes dépendant de la technologie d'accès, on envisage des mécanismes basés sur le protocole IP. Dans ce mémoire, nous nous intéressons à trois mécanismes de contrôle particuliers : l'authentification, la gestion de la mobilité et la signalisation de qualité de service.

L'*authentification* consiste à vérifier et valider l'identité de l'usager voulant accéder au réseau. Notons que pour certaines technologies, comme UMTS, l'authentification se fait dans les deux sens, c'est-à-dire que le réseau aussi est authentifié auprès de l'usager. Dans un réseau multi-accès, l'usager ou l'application devrait utiliser des mécanismes d'authentification et d'autorisation basés sur le protocole IP pour accéder aux ressources du réseau.

La *gestion de la mobilité* consiste à permettre à un usager de garder un accès au service lorsqu'il se déplace et change son point d'attache au réseau. L'objectif est de pouvoir se déplacer dans le réseau sans interruption du service. Dans un réseau multi-accès, le changement de point d'accès au réseau peut se produire à l'intérieur de la zone de couverture d'une technologie d'accès, donc intra-technologique ou encore lors d'un changement de technologie d'accès, on dit alors inter-technologique.

La *signalisation de qualité de service* permet au terminal d'établir et de négocier avec le réseau une session en spécifiant des caractéristiques de qualité de service. Selon les ressources disponibles et le profil de l'usager, le réseau peut établir la session et garantir certains paramètres caractérisant le flux de données de la session. La qualité de service d'une session se caractérise par des paramètres comme le débit garanti, le débit maximal, le délai, la gigue, etc. Par exemple, une application qui veut établir une session

pour de la voix doit obtenir une garantie sur le débit et le délai de transmission des paquets durant cette session. Le type de paramètre et la façon de les garantir dépendent grandement des mécanismes de qualité de service utilisés dans le réseau de transport IP et de la technologie d'accès utilisée. Dans un contexte multi-accès, une application doit être en mesure de faire la signalisation de qualité de service avec un protocole basé sur IP plutôt que d'utiliser les mécanismes spécifiques à chaque technologie d'accès.

1.2 Éléments de la problématique

Le manque d'interaction des mécanismes de contrôle IP et UMTS est à la base de la problématique de ce mémoire. Lorsqu'un paquet IP traverse un système UMTS, que ce paquet soit des données ou un message de contrôle, il doit être encapsulé avant de traverser le réseau UMTS en entier. Ce n'est que lorsqu'il atteint le nœud à la limite du réseau UMTS que le paquet IP est restitué pour être acheminé normalement sur le réseau IP. Les paquets de contrôle IP sont donc transportés de bout en bout à travers tout le réseau UMTS, dans une forme de tunnel, comme si c'était une liaison de couche 2.

Cette encapsulation engendre une redondance de mécanisme de contrôle. Étant donné que le réseau UMTS est utilisé comme une liaison de couche 2 pour transporter tous les paquets IP, tous les mécanismes de contrôle basés sur IP sont invisibles au réseau UMTS. Ainsi, en plus d'envoyer des messages de contrôle au niveau IP, le terminal doit utiliser les mécanismes de contrôle UMTS pour accéder au réseau. Cette duplication de mécanismes est inefficace et entraîne une mauvaise utilisation des ressources dans le réseau.

Dans un contexte multi-accès, un usager qui désire utiliser un accès UMTS ne peut pas s'authentifier de façon globale avec un protocole basé sur IP, il doit d'abord s'authentifier auprès du système UMTS avant d'obtenir un accès au service IP. Il en va de même pour la signalisation de qualité de service, UMTS dispose de ses propres mécanismes. Il est possible pour une application d'utiliser un protocole de signalisation

basé sur IP, mais l'interaction avec les mécanismes de qualité de service UMTS est très limitée.

UMTS possède ses mécanismes de gestion de la mobilité qui sont utilisés lorsque le terminal mobile se déplace à l'intérieur de sa zone de couverture. Lors d'un changement de type d'accès, aucune interaction n'est possible entre les mécanismes inter-technologiques basés sur IP et UMTS. En somme, nous estimons que ceci est dû à une mauvaise intégration de la suite de protocoles IP dans l'architecture UMTS. Une meilleure intégration des protocoles de contrôle IP avec UMTS simplifierait le système en plus d'éliminer la redondance de mécanismes de contrôle.

1.3 Objectifs de recherche

L'objectif principal de ce mémoire est de concevoir un schéma d'intégration des protocoles de contrôle basés sur IPv6 avec la technologie de troisième génération UMTS. Nous sommes intéressés à trois mécanismes en particulier : la gestion de mobilité, l'authentification et la signalisation de qualité de service. Nous cherchons une méthode pour transmettre des messages de contrôle entre une application utilisant IPv6 (terminal mobile) et un réseau de transport IPv6, par l'intermédiaire d'un réseau d'accès radio de type UMTS. Plus spécifiquement, nos objectifs de recherche sont :

- proposer une architecture d'évolution des systèmes UMTS qui facilite l'intégration de protocoles basés sur IPv6;
- définir une mise en correspondance des protocoles de contrôle basés sur IPv6 avec les protocoles de contrôle UMTS dans le but d'éviter la redondance de mécanismes;
- évaluer de la performance de la relève inter-technologie de la nouvelle architecture avec la mise en correspondance de protocoles de contrôle.

1.4 Pan du mémoire

Ce mémoire est divisé en cinq chapitres. Après ce premier chapitre d'introduction, le deuxième chapitre fait une revue de la technologie UMTS et des travaux les plus pertinents sur les réseaux multi-accès parus dans la littérature, pour ensuite examiner certains mécanismes de contrôle basés sur IP. Le troisième chapitre expose le scénario d'évolution de l'architecture UMTS que nous voulons proposer ainsi que notre solution de conversion de protocole de contrôle. Par la suite, une analyse des résultats obtenus est présentée au quatrième chapitre. Enfin, le cinquième chapitre conclut ce mémoire et énonce quelques avenues de recherche futures.

CHAPITRE 2

ANALYSE DE L'ÉVOLUTION DES RÉSEAUX MOBILES BASÉS SUR UMTS

Les premiers réseaux mobiles de type cellulaire ont été déployés au début des années 80. Ils utilisent la technologie AMPS (*Advanced Mobile Phone System*). Ces réseaux constituent la première génération de réseaux cellulaires. Ce sont des systèmes analogiques avec multiplexage fréquentiel FDMA (*Frequency Division Multiple Access*). Dans les années 90, on a vu l'émergence des réseaux cellulaires de deuxième génération (2G). Quatre technologies de deuxième génération ont été développées : D-AMPS, PDC, GSM et CDMA. Bien que ces technologies soient incompatibles, elles présentent plusieurs caractéristiques communes. Elles utilisent des *codecs* (codeur-décodeur) pour numériser la voix et elles multiplexent plusieurs communications sur une même bande de fréquence. Deux techniques de multiplexage sont utilisées : TDMA (*Time Division Multiple Access*) ou CDMA (*Code Division Multiple Access*).

Aujourd'hui, les premiers réseaux de troisième génération (3G) commencent à être déployés. Comme pour le 2G, le 3G permet des communications numériques pour la voix mais ajoute le transport de données. Bien qu'il soit possible de transmettre des données avec le 2G, les technologies 3G sont plus adaptées pour transporter plusieurs types de trafic de données avec des débits plus élevés et plusieurs niveaux de qualité de service. L'ITU (*International Telecommunication Union*), dans le cadre du projet IMT-2000, a débuté le processus de standardisation du 3G. Par la suite, d'autres organismes ont développé et proposé des standards, respectant la norme IMT-2000. Bien que cinq standards aient été acceptés par IMT-2000, seulement deux technologies sont déployées par les opérateurs, UMTS développé par 3GPP (*3rd Generation Partnership Project*) et

Cdma2000, développé par 3GPP2 (*3rd Generation Partnership Project 2*). Pour un résumé plus détaillé de l'historique des réseaux cellulaires et des différentes technologies cellulaires, se référer à [1] et [7]. La façon dont se déroulera l'évolution des réseaux cellulaires dans les prochaines années n'est pas très claire. S'il n'y a pas encore de définition sur le 4G, certains proposent des façons de faire évoluer les systèmes 3G actuels. Ce sont les systèmes 3G évolués ou encore B3G (*Beyond-3G*).

Ce chapitre se veut une revue des technologies et des travaux de recherche pertinents à ce projet de recherche. Dans un premier temps, nous présentons la technologie UMTS. Par la suite, nous présentons quelques travaux qui ont été faits sur les systèmes B3G. Dans la dernière partie de ce chapitre, nous étudions les protocoles de contrôles basés sur IP que nous envisageons pour ce projet.

2.1 UMTS

Dans cette section, nous décrivons le système de troisième génération de type UMTS. Nous présentons l'architecture générale du système, puis nous nous concentrons sur le transport de données. Par la suite, nous présentons les protocoles de contrôle.

2.1.1 Architecture Générale UMTS

La Figure 2.1 illustre l'architecture d'un réseau de type UMTS avec les différents éléments qui la constituent. Le système UMTS et son architecture sont décrits en détail dans [2] et [3]. L'architecture UMTS se divise en deux parties, le réseau d'accès radio, appelé UTRAN (*UMTS Terrestrial Radio Access Network*) et le réseau cœur du système appelé CN (*Core Network*). Cette séparation a pour but d'isoler à l'intérieur du UTRAN tout l'aspect des radiocommunications afin de le rendre complètement transparent pour le CN.

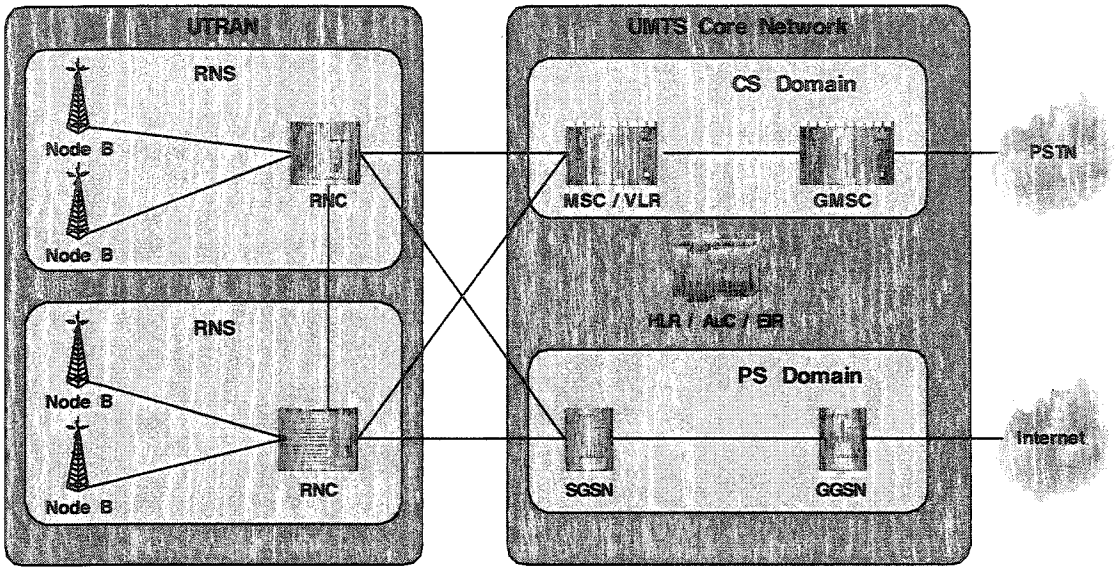

Figure 2.1 Architecture générale UMTS

Le UTRAN fourni un service de porteuse, appelé RAB (*Radio Access Bearer*), qui procure les communications entre le CN et le nœud mobile, appelé MN[1]. Le UTRAN implémente la technologie radio WCDMA [4] (*Wideband Code Division Multiple Access*) pour offrir ces services de communication. L'encapsulation de l'accès radio physique dans le UTRAN donne l'illusion d'un canal de communication fixe, entre le CN et MN, mais permet aussi de faire évoluer ces deux parties du système de façon indépendante. Le CN est une plateforme dont le rôle est de gérer toutes les communications du réseau UMTS. La technologie de transport physique employé dans le CN n'est pas imposée dans les spécifications de 3GPP, le choix revient à l'opérateur. De plus, on distingue deux domaines dans le CN de UMTS, le domaine à commutation de circuit appelé domaine CS (*Circuit Switched*) et le domaine à commutation de paquets appelé domaine PS (*Packet Switched*). Dans le cadre de ce projet, nous nous intéressons au domaine PS. Le tableau 2.1 explique le rôle de chacun des éléments de l'architecture UMTS.

---

[1] Nous utilisons le terme MN (« Mobile Node »), très répandu dans la littérature technique mais les termes UE (« User Equipment ») ou MS (« Mobile Subscriber »), trouvés dans la documentation 3GPP, pourraient aussi être utilisés. Par souci de clarté, nous n'utilisons que le terme MN dans ce document.

Tableau 2.1 Description des éléments dans un réseau UMTS

Élément	Description / tâche
Node B	C'est la station de base (*Base Station*) dans UMTS. Il sert à la transmission radio, fait la conversion de signal et la correction d'erreur au niveau radio. Il couvre une ou plusieurs cellules.
RNC	*Radio Network Controller*. C'est un commutateur qui multiplexe et démultiplexe le trafic des usagers. Il gère les ressources radio et contrôle la congestion dans le UTRAN.
MSC/VLR	*Mobile Switching Center/Visitor Location Register*. Il est responsable des communications à commutation de circuit. Il s'occupe de la gestion des connexions, la gestion de mobilité, la sécurité et l'imputation de frais de service pour les communications en mode circuit.
GMSC	*Gateway Mobile Switching Center*. Il s'occupe de la transmission des communications entrantes/sortantes vers des réseaux à commutation de circuits externes.
SGSN	*Serving GPRS Support Node*. Il est responsable des sessions à commutation de paquet. Il s'occupe de la gestion des sessions, de la gestion de mobilité, de sécurité et de l'imputation de frais de service pour les communications en mode paquet.
GGSN	*Gateway GPRS Support Node*. Il est responsable des connexions en mode paquets vers les réseaux externes comme l'Internet. Il sert aussi de coupe-feu et fait l'allocation dynamique d'adresse IP.
HLR	*Home Location Register*. C'est une base de donnée contenant les informations sur les abonnés du système, leurs services, leur possibilité d'itinérance, les classes de qualité de service auxquelles ils ont droit.
AuC	*Authentication Centre*. C'est une base de donnée qui génère les vecteurs d'authentification. Ces vecteurs contiennent les paramètres que le VLR et le SGSN utilisent pour leurs activités de sécurité.
EIR	*Equipment Identity Register*. Il contient l'information sur l'identification du matériel des MN dans le réseau.

2.1.2 Architecture du domaine PS

Dans le cadre de ce mémoire, nous nous intéressons au domaine PS de l'architecture UMTS. La Figure 2.2 illustre le domaine PS avec les différentes interfaces entre les éléments du système. Les interfaces sont ouvertes et définies dans les spécifications de 3GPP. Uu est l'interface radio entre le UTRAN et le MN, elle est implémentée avec WCDMA. L'interface Iu est le point d'interconnexion entre le UTRAN et le CN. Dans le domaine PS, il s'agit plus particulièrement de l'interface Iu-PS. Iur est une interface optionnelle entre les RNC. Lorsqu'elle est présente, elle permet une gestion de la mobilité inter-RNC plus étendue, sans la participation du CN. L'interface Gn interconnecte le SGSN et le GGSN tandis que l'interface Gr permet au SGSN de communiquer avec le HLR.

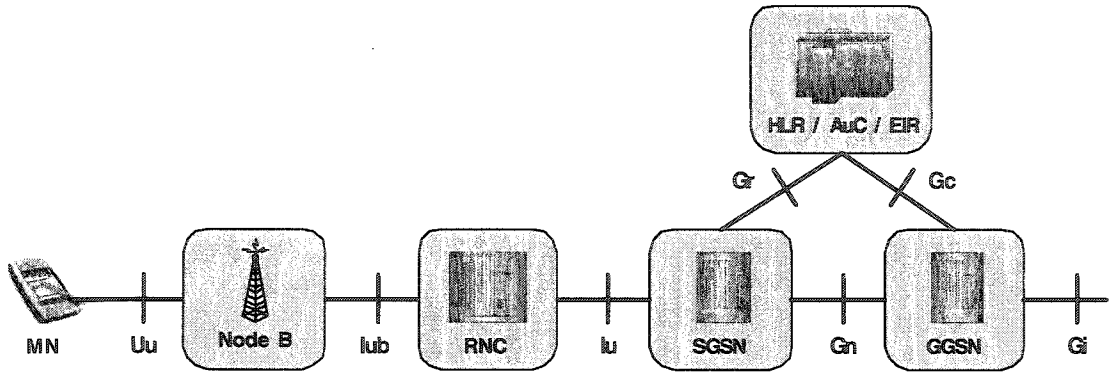

Figure 2.2 Architecture et interfaces du domaine PS

À chaque interface, plusieurs protocoles en couches régissent les échanges entre les éléments du réseau. 3GPP définit deux plans de protocole, les protocoles du plan usager (*User Plane Protocols*) et les protocoles du plan contrôle (*Control Plane Protocols*). Les premiers servent à transférer les données des communications des usagers tandis que les seconds servent à contrôler les ressources et supporter les communications dans le système. Dans ce mémoire, nous nous intéressons aux protocoles de contrôle. La Figure 2.3 montre la pile de protocoles du plan contrôle entre le MN et le GGSN. Pour plus de détails, se référer à la spécification technique [16] de 3GPP.

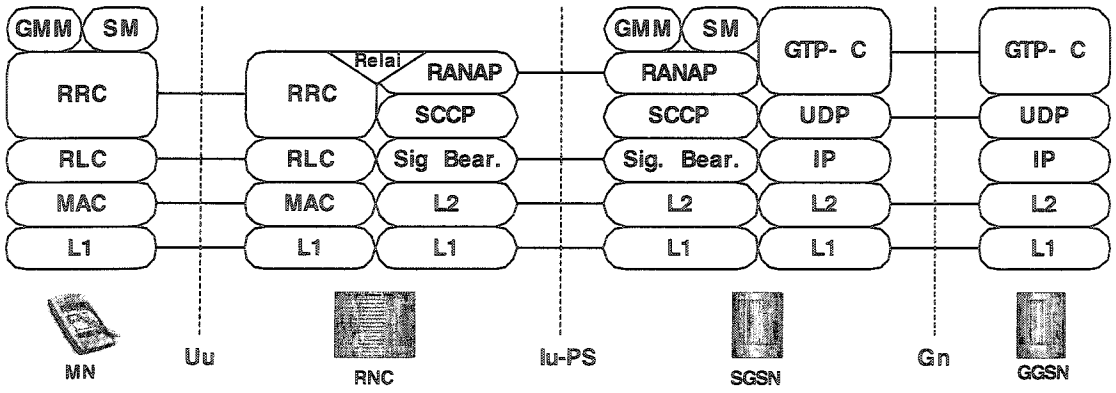

Figure 2.3 Pile de protocoles dans le plan de contrôle du MN au GGSN

Notons que les protocoles RLC, MAC et L1 dans la partie radio (Uu) ainsi que les protocoles de la couche physique L1/L2 dans le reste du réseau, servent autant à véhiculer le trafic de données usager que le trafic de contrôle. Cette couche offre un service de transport générique pour le plan usager et le plan de contrôle. Dans la nomenclature 3GPP, il s'agit de la couche ou du sous-système du réseau de transport UMTS.

Tableau 2.2 Description des protocoles du plan de contrôle

Protocoles	Description
GMM / SM	*GPRS Mobility Management, Session Management.* Ces protocoles supportent les fonctionnalités de gestion de mobilité et de gestion de session entre le CN et MN.
RRC	*Radio Resource Control.* Ce protocole permet de contrôler les ressources radio et supporte ainsi toutes les fonctionnalités de gestion de ressource radio dans le UTRAN. Il sert aussi à transporter la signalisation provenant des couches supérieures (GMM et SM).
RANAP	*Radio Access Network Application Protocol.* Ce protocole s'occupe de la signalisation entre le SGSN et le UTRAN sur l'interface Iu. Il sert à la gestion des porteuses RAB, des connexions GTP et des ressources de communication sur l'interface Iu. De plus, il encapsule et transporte la signalisation des couches supérieures (GMM et SM).
SCCP	*Signalling Connection Control Part.* Ce protocole offre un service de transport de signalisation pour les couches supérieures basé sur le système SS7 (*Common Channel Signalling System No. 7*). Le système SS7 est un standard de l'ITU pour la signalisation téléphonique.
Sig. Bear.	*Signalling Bearer.* La porteuse de signalisation sert de couche d'adaptation qui varie selon la technologie de transport choisi par l'opérateur. La spécification [18] de 3GPP définit trois situations possibles.
GTP- C	*GPRS Tunnelling Protocol - Control Plane.* Ce protocole permet l'échange de message de signalisation entre les multiples SGSN ainsi qu'entre les SGSN et les GGSN.
RLC	*Radio Link Layer.* Ce protocole procure un contrôle de lien logique au-dessus de l'interface radio.
MAC	*Medium Access Layer.* Ce protocole contrôle la signalisation de l'accès aux canaux de communication radio.
L1 (Uu)	*Physical Radio Layer.* C'est la couche physique qui implémente WCDMA
L1-L2 (Iu)	Ces couches dépendent de l'opérateur. Dans la norme de 3GPP, il peut sélectionner ATM ou IP pour son réseau de transport UTRAN à l'interface Iu. La couche physique (L1) terrestre peut être implémentée par des technologies de transmissions numériques comme PDH ou SDH.

La Figure 2.4 illustre la pile de protocoles de contrôle entre un SGSN et un HLR mais elle est identique pour tous les nœuds qui communiquent avec le HLR, c'est-à-dire le SGSN, GGSN, MSC/VLR ou GMSC.

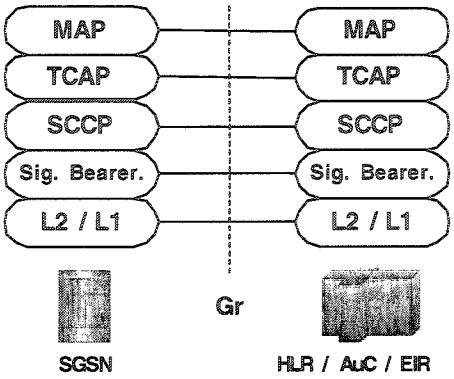

Figure 2.4 Pile de protocoles dans le plan de contrôle entre le SGSN et le HLR

Tableau 2.3 Description des protocoles du plan de contrôle (avec le HLR)

Protocoles	Description
MAP	*Mobile Application Part.* Ce protocole sert à la signalisation entre le HLR et les autres nœuds du réseau. Il supporte l'authentification, l'identification d'équipement, l'autorisation d'itinérance, la facturation, etc. La spécification technique [19] définit ce protocole.
TCAP	*Transaction Capabilities Application Part.* Ce protocole fait partie de la suite de protocole du système SS7 et encapsule les messages MAP. Il supporte l'échange d'information entre les nœuds facilitant l'implémentation de service intelligent.

2.1.3 Mécanisme de contrôle UMTS (Domaine PS)

Dans cette section, nous décrivons les mécanismes de contrôle UMTS qui réalisent l'authentification, la gestion de session de transfert de données ainsi que la gestion de la mobilité. Ces mécanismes sont implémentés avec les protocoles de la couche GMM et SM illustrés précédemment. Les protocoles GMM et SM [17] régissent les communications entre le MN et le réseau cœur CN. Ils font partie de la couche de protocoles systèmes (*System network protocols*) de UMTS qui permet la création des services de communications pour les usagers. Ces protocoles s'exécutent par-dessus les protocoles du réseau radio (UTRAN), entre le MN et le CN. Plusieurs procédures définissent ces protocoles. Nous décrivons les procédures qui supportent les mécanismes de contrôle couverts dans le cadre de ce projet. Le protocole GMM procure les procédures pour contrôler la gestion de la mobilité et l'authentification tandis que les

procédures du protocole SM servent à établir et contrôler des sessions de transfert de données.

Authentification UMTS

Dans un système UMTS, l'authentification de l'usager se fait lors de la procédure d'attachement GPRS (*GPRS Attach Procedure*) du protocole de gestion de mobilité GMM. L'attachement au réseau constitue la première étape pour un MN qui veut accéder au service GPRS. C'est pendant l'attachement au réseau que l'usager est authentifié grâce à la procédure (ou sous-procédure) d'authentification et d'échange de clés AKA (*Authentication and Key Agreement*). L'identification de l'usager se fait par l'identificateur IMSI (*Internationnal Mobile Subscriber Identity*). Une fois la procédure AKA terminée, la procédure d'attachement se poursuit et se termine. Suite à la procédure d'attachement, le MN et le réseau sont authentifiés, un contexte de mobilité est créé dans le MN ainsi que dans le SGSN, les informations sur le profil de l'usager reçues du HLR permettent au SGSN d'autoriser l'accès aux différents services lorsque le MN en fera la demande. La procédure d'attachement est définie en détails dans la spécification technique de 3GPP [16].

Procédure d'authentification et d'échange de clés (AKA)

La procédure AKA est au centre du système de sécurité d'accès UMTS. En plus de réaliser l'authentification mutuelle de l'usager et du réseau, cette procédure fournit les clés cryptographiques nécessaires pour le chiffrement des communications et la protection de l'intégrité de la signalisation dans le UTRAN. Cette procédure est exécutée lorsqu'il y a attachement d'un MN au réseau mais elle peut aussi être exécutée durant d'autres procédures, par exemple lors la procédure de *Routing Area Update*. Elle implique, le MN, le SGSN auprès duquel se fait l'attachement ainsi que le centre d'authentification AuC (intégré au HLR). Elle est initiée par le SGSN à partir du moment où il connaît l'identité IMSI de l'usager concerné. La Figure 2.5, illustre la procédure AKA.

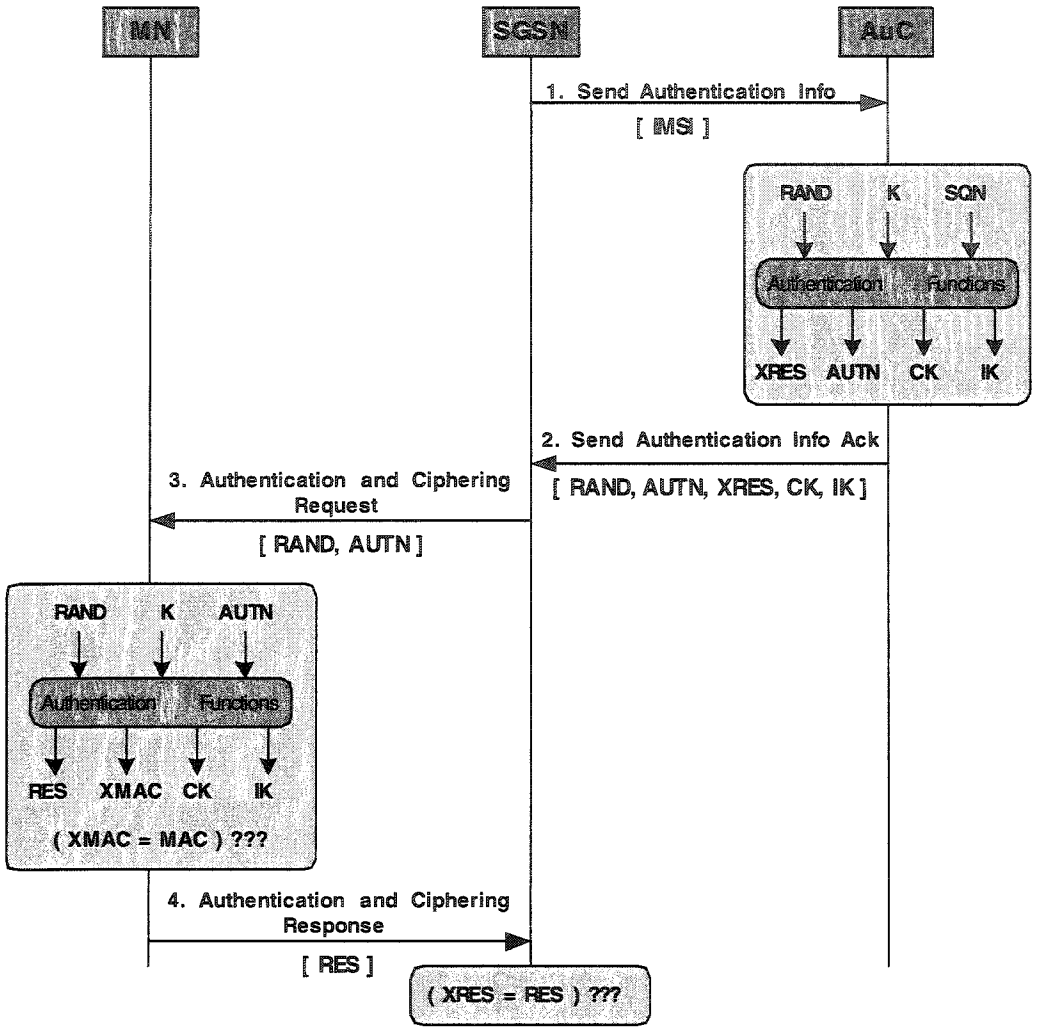

Figure 2.5 Procédure d'authentification et d'échange de clés (AKA)

Le mécanisme d'authentification se base sur un secret, la clé maîtresse K (*Master Key*), partagée entre l'usager et la base de donnée du réseau d'origine. La clé maîtresse K, d'une longueur de 128 bits, est stockée dans le module USIM (*UMTS Subscriber Identity Module*) de l'usager et le centre d'authentification AuC. Le module USIM, implémenté sous forme d'une carte à puce, contient des informations du profil de service de l'usager et implémente les fonctions de sécurité. Les fonctions de sécurité sont des fonctions mathématiques unidirectionnelles qui ont la caractéristique d'être faciles et rapides à calculer mais pratiquement impossibles à inverser. Par exemple, les fonctions de hachage sont des fonctions unidirectionnelles. Ces fonctions unidirectionnelles, qui

servent à générer les différents paramètres du vecteur d'authentification, sont connues du USIM et du AuC.

1. Le SGSN initie la procédure en envoyant l'identificateur IMSI de l'usager au AuC. Le AuC génère un ou plusieurs vecteurs d'authentification à partir de la clé maîtresse K, d'un numéro de séquence SQN de 48 bits et d'un nombre aléatoire RAND de 128 bits. Quatre paramètres sont générés : une clé de chiffrement CK (*Cipher Key*) de 128 bits, une clé pour la protection d'intégrité IK (*Integrity Key*) de 128 bits, un paramètre de réponse attendue XRES (*Expected Response*) de 32 à 128 bits, ainsi qu'un marqueur d'authentification AUTN (*Authentication Token*) de 128 bits.
2. Le AuC envoie ensuite un ou plusieurs vecteurs d'authentification au SGSN. Ceci évite au SGSN de contacter le AuC pour chaque authentification. Un vecteur d'authentification est composé des quatre paramètres générés à l'étape 1 et du nombre aléatoire RAND. Le SGSN sauvegarde les vecteurs d'authentification reçus. Les clés CK et IK serviront à protéger les communications, une fois la procédure d'authentification terminée. Le paramètre XRES sert à valider l'identité de l'usager.
3. Le SGSN envoie les paramètres RAND et AUTN d'un vecteur d'authentification au MN. Le USIM contenu dans le MN exécute les fonctions d'authentification en utilisant sa clé maîtresse K, ainsi que les paramètres RAND et AUTN reçu. Le marqueur AUTN contient, de façon cachée, le numéro de séquence SQN ainsi qu'un code d'authentification de message MAC (*Message Authentication Code*). Il sert à vérifier que le vecteur d'authentification a été généré par une entité connaissant la clé maîtresse K (AuC). Le USIM génère ainsi ses clés CK et IK pour protéger les communications, un paramètre RES, qui servira à l'authentifier auprès du réseau, et enfin le paramètre attendu XMAC (*Expected MAC*). En le comparant avec le MAC reçu du SGSN, il s'assure de l'identité du réseau qui lui offre le service.

4. Si le réseau est authentifié, le MN envoie une réponse au SGSN contenant le paramètre RES. Le SGSN peut s'assurer de l'identité de l'usager en vérifiant que le paramètre RES reçu du MN est le même que le XRES contenu dans le vecteur d'authentification utilisé.

Ceci couvre la procédure de base AKA de UMTS sans les différents cas d'erreur possible ou les détails mathématiques du calcul et de la validation des paramètres d'authentification. Les détails de cette procédure se trouvent dans la spécification technique [20] de 3GPP.

Gestion de session UMTS

La gestion de session se fait grâce au protocole SM (*Session Management*). Le MN, le SGSN ainsi que le GGSN sont les éléments du réseau impliqués dans la gestion de session de transfert de données. Le protocole SM sert à établir, modifier ou terminer des sessions entre le MN et le SGSN, tandis qu'entre le SGSN et le GGSN, c'est le protocole GTP-C qui régit les communications. Dans un système UMTS, une session correspond à un contexte PDP (*Packet Data Protocol*). Pour chaque session de transfert de données, un contexte PDP doit être créé. Les paquets sont encapsulés dans une forme de tunnel pour traverser le réseau jusqu'au GGSN, où les paquets sont acheminés vers des réseaux externes selon leur destination et le type de trafic. Il s'agit du tunnel GTP (*GPRS Tunnelling protocol*). Le principal avantage de cette encapsulation est de permettre le transfert de n'importe quel type de paquet de donnée, IPv4, IPv6, PPP, etc. La Figure 2.6 illustre le transport et l'encapsulation des données dans un réseau UMTS.

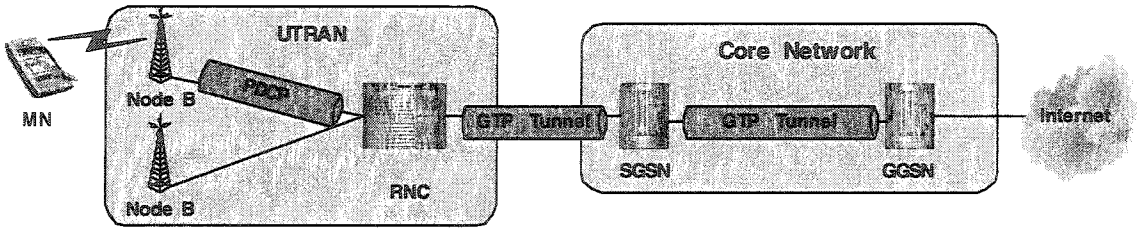

Figure 2.6 Encapsulation des données d'usager

Le contexte PDP contient les informations qui caractérisent la session de transfert de données. Les informations portent entre autre sur l'acheminement et la qualité de service du trafic. UMTS définit quatre classes de qualité de service qui peuvent être assignées aux différents types de trafic ainsi que plusieurs autres paramètres plus spécifiques permettant de quantifier certaines propriétés du flux de données, comme le débit garanti, le débit maximum, le délai, le taux d'erreur, etc. La spécification technique [21] de 3GPP contient les détails des attributs de qualité de service.

Procédure d'activation de contexte PDP

Nous décrivons maintenant, avec la Figure 2.7, la procédure d'activation d'un contexte PDP, lorsqu'un usager veut établir une session de transfert de données.

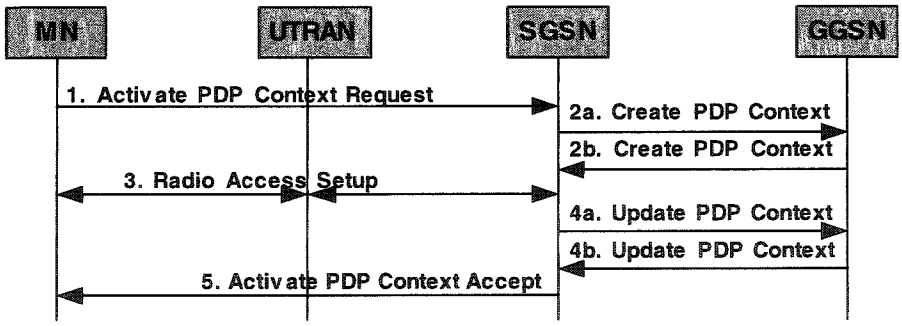

Figure 2.7 Activation d'un contexte PDP

1. Le MN initie la procédure en faisant la requête d'activation d'un contexte PDP au SGSN. Il inclut dans sa requête les informations caractérisant la session désirée, les paramètres de qualité de service, le type de service et le réseau externe à contacter.
2. Le SGSN valide la requête d'activation de contexte PDP avec les informations de l'abonnement de l'usager. Il vérifie que les paramètres sollicités dans la requête respectent les valeurs contenues dans le profil de l'usager. Il peut même restreindre la valeur de certains paramètres de qualité de service avant de poursuivre la procédure. Le SGSN envoie un message de création de contexte

PDP au GGSN. Le GGSN insère une nouvelle entrée dans une table de contexte PDP. Avec la création de ce contexte PDP, le GGSN pourra accepter et acheminer les paquets entre le SGSN et le ou les réseaux externes. Le GGSN peut restreindre la qualité de service associé au contexte PDP selon ses capacités et ses ressources disponibles. Ensuite, le GGSN envoie un message de réponse au SGSN contenant les paramètres du contexte PDP créé.

3. Le SGSN fait la demande au UTRAN de réserver les ressources radio nécessaires à la session demandée. Il s'agit de réserver et d'assigner une ou des porteuses RAB au contexte PDP concerné.
4. Si à l'étape 3, les ressources radio sont insuffisantes pour satisfaire les requis de qualité de service demandée et que les attributs doivent être réduits, le SGSN est contraint de modifier le contexte PDP et d'informer le GGSN de la modification des paramètres en mettant à jour le contexte PDP.
5. Le SGSN envoie un message d'acceptation pour l'activation de contexte PDP au MN. Il inclut les paramètres finaux définissant le contexte PDP qui a été établi. Après cette dernière étape, le SGSN est en mesure d'acheminer les paquets associés à ce contexte PDP, entre le MN et le GGSN.

Gestion de la mobilité UMTS

La gestion de la mobilité est accomplie à plusieurs niveaux dans un système UMTS mais elle est en grande partie réalisée par le UTRAN. Le réseau UMTS est logiquement structuré en plusieurs zones de niveaux hiérarchiques différents qui servent de référence dans les procédures de gestion de mobilité. La Figure 2.8 illustre cette structure logique.

La zone LA (*Location Area*) sert dans le domaine de commutation de circuit. Elle correspond à la zone de couverture sous laquelle un MN peut se déplacer sans devoir exécuter la procédure de mise à jour de la zone LA (*Location Area Update*). Une zone LA est constituée de une ou plusieurs cellules et un MSC/VLR contrôle une ou plusieurs zones LA.

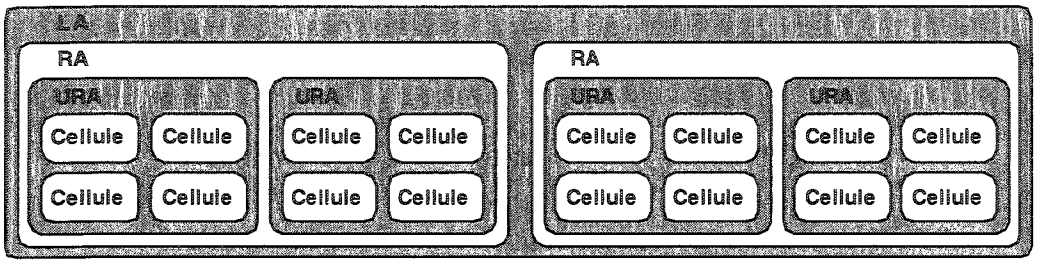

Figure 2.8 Structure logique de zone de couverture

La zone RA est similaire à la zone LA mais dans le domaine de commutation de paquets (domaine PS). Elle correspond à la zone de couverture sous laquelle un MN peut se déplacer sans devoir exécuter la procédure de mise à jour de zone RA (*Routing Area Update*). Une zone RA est toujours plus petite ou égale à une zone LA. Une zone LA peut contenir une ou plusieurs zones RA et une zone RA ne peut être partagée entre deux zones LA. Une zone URA sert également dans le domaine PS. Elle correspond à un sous-ensemble de cellule dans une zone RA. En pratique, cette zone coïncide avec la zone de couverture d'un RNC. La cellule est la plus petite zone d'un système UMTS. C'est la zone de couverture radio d'une antenne cellulaire. Notons que le CN n'est pas au courant de la zone d'une cellule, il considère seulement les ensembles de cellules, soit les URA, RA et LA.

Une particularité du mode d'accès CDMA, et invariablement WCDMA, est qu'il est possible pour un mobile d'être à tout moment connecté à plusieurs cellules en même temps. Le signal est reçu et transmis par plusieurs antennes en même temps. Les signaux radio provenant des antennes des différentes cellules sont ensuite combinés pour former un seul signal. Cette façon de faire permet de diminuer la puissance des signaux radio et donc l'interférence radio. La réduction d'interférence permet d'accroître la capacité globale du réseau, même si plus de connexions (donc de ressources) sont utilisées pour implémenter cette technique. On utilise les termes micro-diversité et macro-diversité pour décrire où se fait la recombinaison de signal. Lorsque le NodeB combine les signaux provenant de plusieurs secteurs ou cellules sous son contrôle, il s'agit de micro-

diversité et lorsque la recombinaison se fait au niveau du RNC, il s'agit alors de macro-diversité. La Figure 2.9 illustre cette situation.

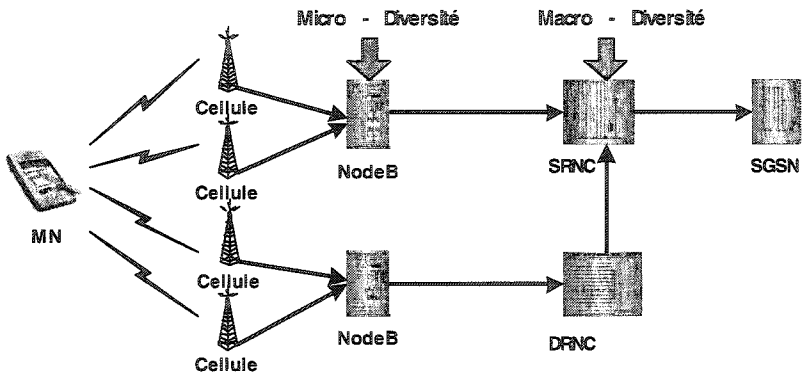

Figure 2.9 Recombinaison d'un signal provenant de plusieurs sources

Dans la terminologie UMTS, le RNC effectuant la recombinaison (macro-diversité) s'appel le SRNC (*Serving RNC*), et lorsqu'une partie du signal provient d'un autre RNC, il s'agit du DRNC (*Drifting RNC*). Cette nomenclature est utilisée dans les procédures de gestion de mobilité UMTS. C'est ainsi que la majeure partie de la gestion de la mobilité des usagers est prise en charge à l'intérieur du UTRAN, sans que le CN ne soit mis à contribution. Ce n'est que lorsqu'il y a changement de zone RA que le CN est impliqué.

3GPP a défini un modèle d'état pour régir les procédures de gestion de mobilité dans le système. L'état de mobilité indique les informations disponibles, la précision avec laquelle l'emplacement de l'abonné est connu, ainsi que les fonctionnalités qui lui sont accessibles. Le contexte de mobilité, lorsqu'il est présent, contient ces informations et il est sauvegardé par le MN et le SGSN. Ce n'est qu'une fois qu'un contexte de mobilité est établi, grâce à la procédure d'attachement présentée précédemment, que le SGSN peut acheminer du trafic pour l'abonné. Nous présentons ici, le modèle d'état dans le domaine PS. Les trois états possibles sont :

PMM-Detached: Il n'y a aucune communication entre le MN et le réseau UMTS. Aucune information de contexte n'est présente dans le MN ou dans le SGSN. Aucune information sur l'emplacement du MN n'est disponible. Cet état correspond au moment où le MN est éteint ou lorsqu'il n'a pas de carte USIM.

PMM-Idle: Un contexte de mobilité est établi dans le MN et le SGSN qui le sert. L'emplacement du MN est connu au niveau de la zone RA dans laquelle il se trouve. Pour communiquer avec le MN, le SGSN doit le *pager*. Le MN doit effectuer la procédure de mise à jour de la zone RA lorsqu'il change de zone. L'état passe à PMM-Connected lorsqu'une connexion de signalisation est établie entre le MN et le SGSN.

PMM-Connected: Il y a un contexte de mobilité dans le MN et le SGSN. L'emplacement du MN est connu au niveau du RNC qui le sert (SRNC). C'est le SRNC qui suit la position du MN. Une connexion de signalisation existe entre le MN et le SGSN. Après une procédure de signalisation complétée, le SGSN peut relâcher la connexion de signalisation, ce qui change l'état de mobilité à PMM-Idle. La Figure 2.10 illustre le modèle d'état avec les transitions possibles.

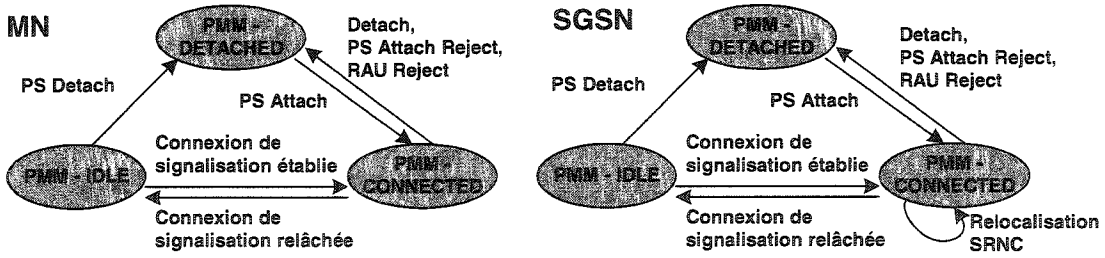

Figure 2.10 Modèle d'état de mobilité du domaine PS

Plusieurs procédures sont définies par le protocole GMM de UMTS. En plus de servir à la gestion de mobilité des usagers dans le réseau, ces procédures accomplissent l'attachement au réseau, l'authentification des usagers et du réseau ainsi que les échanges de paramètres de sécurité. Nous présentons ici la procédure de GMM, qui permet de gérer la mobilité de l'usager lorsqu'il se déplace dans le réseau. Il s'agit de la procédure de mise à jour de la zone RA (*Routing Area Update*). Elle est exécutée dans

deux situations. La première, de façon périodique pour rafraîchir d'état de mobilité entre le MN et le SGSN. La deuxième, lorsque la zone de couverture RA change lors d'un déplacement. Pour détecter un changement de zone de couverture, le MN se fie à l'information RAI (*Routing Area Identification*) qu'il reçoit du réseau. En le comparant avec le RAI sauvegardé dans son contexte de mobilité, le MN détermine qu'il a changé de zone de couverture.

Procédure de mise à jour de la zone RA

La procédure de mise à jour de la zone RA définie par 3GPP est relativement complexe car elle tient compte de plusieurs scénarios. L'exécution de la procédure change selon qu'il s'agit d'une mise à jour périodique ou d'une mise à jour déclenchée par un changement de zone RA; là encore, il peut s'agir d'un changement de zones RA sous le contrôle d'un même SGSN (intra-SGSN) ou sous le contrôle de SGSN différents (inter-SGSN). Le cas d'une mise à jour périodique est toujours intra-SGSN. De plus, l'état de mobilité de l'abonné, PMM-Idle ou PMM-Connected, a aussi un impact sur les étapes de cette procédure. Ainsi, plusieurs étapes de cette procédure ne s'exécutent que dans certains scénarios. Les différentes possibilités d'exécution de la procédure sont donc nombreuses. De plus, plusieurs étapes de la procédure générale impliquent l'interaction et l'échange d'information avec le UTRAN. Or, nous préférons ne pas entrer dans les détails du réseau d'accès UTRAN dans ce texte. Ainsi, nous présentons ici une version simplifiée de la procédure de mise à jour de la zone RA; elle contient cependant toutes les étapes d'échange d'information entre le MN, le SGSN et les autres nœuds du CN. La Figure 2.11 illustre le diagramme de séquence de la procédure de mise à jour de la zone RA.

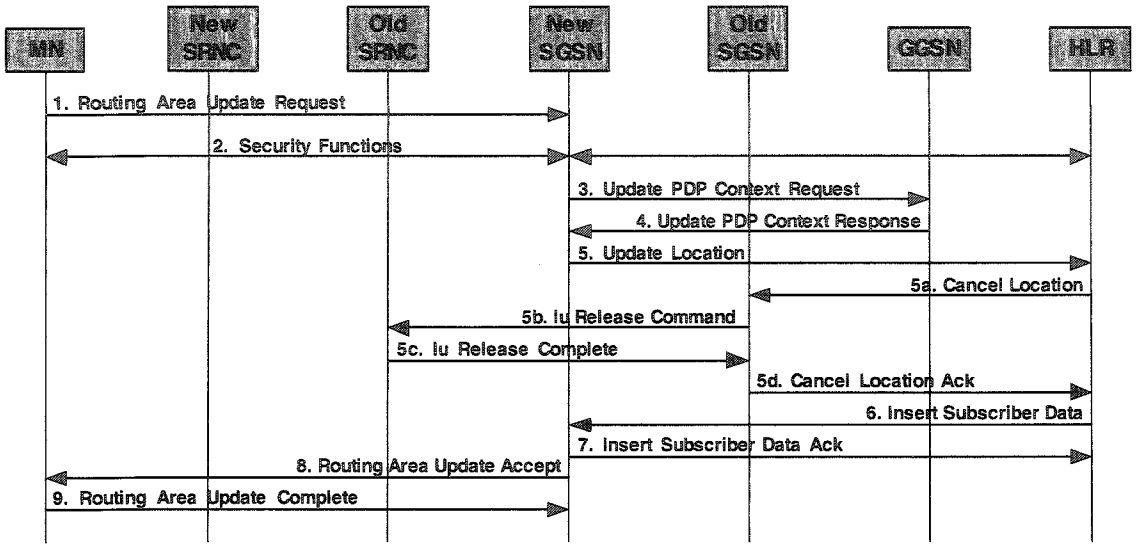

Figure 2.11 Procédure de mise à jour de la zone RA

1. Après avoir été informé d'un changement de RAI, le MN initie la procédure en envoyant une requête de mise à jour au SGSN.
2. Optionnellement, le SGSN peut exécuter la procédure d'authentification comme lors d'un attachement au réseau.
3. Lorsqu'il y a changement de SGSN, celui-ci demande une mise à jour des contextes PDP auprès du GGSN pour que ce dernier achemine le trafic destiné au MN concerné vers le nouveau SGSN.
4. Le GGSN confirme la mise à jour des contextes PDP.
5. Le SGSN demande au HLR de mettre à jour sa base de données sur la position du MN, sur l'identité du SGSN qui lui donne le service. Le HLR contacte l'ancien SGSN et l'informe qu'il peut supprimer les renseignements du MN qu'il sauvegardait (information d'abonnement, contextes, etc.). L'ancien SGSN confirme cette suppression au HLR, et ce dernier confirme la mise à jour de sa base de données au nouveau SGSN.
6. Le HLR envoie les données sur l'abonnement de l'usager (services autorisés, qualité de service autorisé, etc.) au nouveau SGSN.
7. Le nouveau SGSN confirme la réception des données d'abonnement au HLR.

8. Le SGSN accepte la mise à jour de la zone RA. En même temps, le SGSN peut renouveler les identificateurs temporaires du MN (P-TMSI, TMSI).
9. Le MN confirme la terminaison de la procédure lorsqu'on lui alloue un nouvel identificateur temporaire.

2.2 Évolution des réseaux mobiles

Comment se fera l'évolution des réseaux mobiles dans le futur? Quelles technologies permettront le déploiement de nouveaux services de données plus gourmands en capacité? Plusieurs chercheurs des milieux académique et industriel se posent la question. Même s'il n'y a pas encore de définition précise de ce que sera la prochaine génération de réseau mobile, on en connaît déjà plusieurs caractéristiques. Plusieurs travaux dans le domaine partagent une vision globale commune sur ce que seront les systèmes de prochaine génération. On envisage tout d'abord de faire évoluer les technologies existantes, pour augmenter la capacité des réseaux mobiles, mais aussi d'intégrer plusieurs types de technologie pour former des réseaux mobiles multi-accès dans le but d'offrir un service ubiquitaire, c'est-à-dire disponible n'importe où, n'importe quand. Certains anticipent que cette évolution sera suivie d'une révolution, c'est-à-dire l'introduction d'un tout nouveau type d'accès radio, qui permettra d'atteindre des débits beaucoup plus importants.

2.2.1 Une vision commune

Dans [8], les auteurs présentent comment différentes techniques radio permettront de faire évoluer la technologie WCDMA actuelle, dans le but d'augmenter la capacité des systèmes 3G, qu'ils appellent 3G évolué. Initialement, WCDMA devait permettre des débits maximaux de 2Mbps mais, avec le développement de nouvelles techniques, des débits bien au-delà de 10Mbps pourraient être atteints. Les auteurs annoncent aussi l'utilisation de WLAN comme technologie complémentaire pour les opérateurs, sans toutefois parler de multi-accès. De plus, ils prévoient que le 4G sera une révolution du point de vue de l'accès radio plutôt qu'une évolution des technologies

actuelles. Ils croient indispensable le développement d'une nouvelle interface radio pour le 4G, permettant d'atteindre des débits de 100Mbps en mouvement et jusqu'à 1Gbps en immobilité ou mouvement lent. Cette technologie ne serait pas disponible avant la prochaine décennie.

Ces données se retrouvent également dans [9], où les auteurs exposent la vision de l'ITU-R (ITU - *Radiocommunication Standardization Sector*) sur l'évolution des réseaux mobiles. La vision de l'ITU-R prévoit également que plusieurs types de réseaux d'accès seront interconnectés entre eux par un sous-réseau IP dans le but d'offrir un service intégré aux usagers. L'interconnexion des multiples réseaux d'accès devra être en mesure d'assurer la continuité de service lors d'une relève dite verticale. La relève verticale a lieu lorsque le changement de point d'attache au réseau implique un changement de type d'accès (inter-technologique), contrairement à une relève horizontale où le changement de point d'attache se fait dans le même type d'accès (intra-technologique).

Dans [10], l'ubiquité des communications sans fil est identifiée comme un concept clé pour les réseaux de prochaines générations. L'accès ubiquitaire deviendra possible avec une architecture qu'ils appellent « multi-réseau », où plusieurs types de réseaux d'accès sont utilisés. La technologie d'accès est transparente pour l'usager et les services. Ils identifient le besoin d'une technologie qui permet de faire l'intégration des différentes technologies d'accès. À ce besoin, ils ne voient d'autre alternative que d'utiliser le protocole IP comme base d'intégration.

Dans [11], le concept ABC, pour *Always Best Connected* est exposé. Cela signifie que l'usager n'est pas seulement connecté à tout moment, mais aussi qu'il est connecté avec le meilleur type d'accès possible parmi plusieurs technologies d'accès. La façon de déterminer le meilleur type de connexion dépend de plusieurs facteurs comme les préférences personnelles, la capacité du dispositif de communication, les requis de l'application, la sécurité nécessaire, le ou les opérateurs, les ressources réseau disponibles ou encore les couvertures des différents réseaux. Nous retenons la vision des auteurs sur le AAA (*Authentication, Authorization and Accounting*). Ils expliquent

comment une infrastructure intégrée de AAA permettrait de faire l'authentification, l'autorisation et la facturation, peu importe le type d'accès ou l'opérateur offrant le service. Les auteurs proposent un protocole de AAA basé sur IP standardisé par l'IETF, organisme responsable du développement des protocoles utilisés par Internet.

La question de la mobilité est davantage étudiée dans [12] où les auteurs s'intéressent à gestion de la mobilité globale. Ils décrivent une architecture de réseau de prochaine génération dite hiérarchique avec des cellules plus ou moins grandes selon le type d'accès radio. La Figure 2.12, extraite de [12], illustre les zones de couverture disposées de façon hiérarchique. Selon la zone de couverture et les critères de sélection du type d'accès, un mobile peut se connecter à différentes cellules.

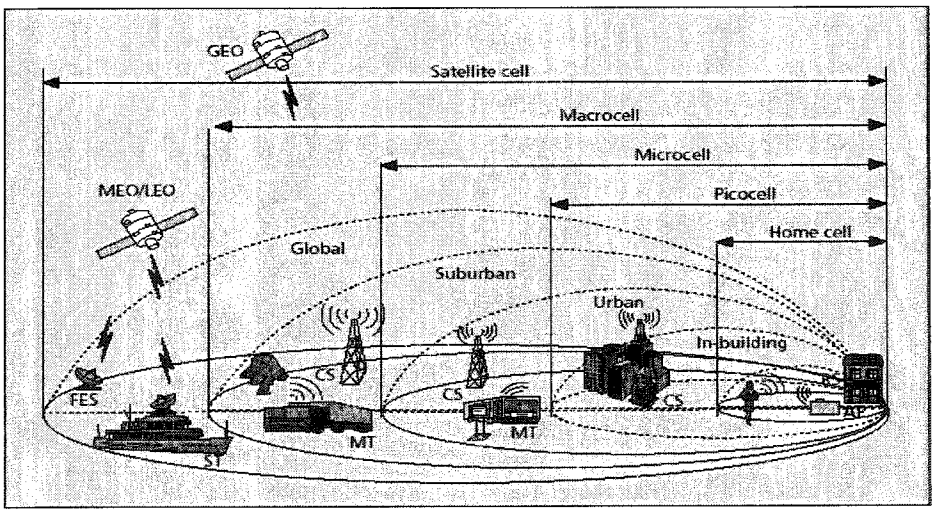

Figure 2.12 Zones de couverture radio hiérarchique

Au niveau de la cellule locale (*Home Cell*), des technologies comme WLAN ou Bluetooth sont utilisées. Pour les Pico-cellules, on utilise un mélange de technologies de WLAN ou de réseaux cellulaires 2G et 3G. Cependant, les technologies 2G et 3G servent surtout à couvrir les Micro-cellules et les Macro-cellules. La cellule satellite correspond à la zone de couverture d'un satellite en orbite. Les auteurs indiquent qu'une gestion de la mobilité globale nécessite une intégration des mécanismes de gestion de

mobilité de chacun des types d'accès. Ici encore, les auteurs voient une solution basée sur IP Mobile comme la plus susceptible de permettre une mobilité globale.

2.2.2 Intégration 3G – WLAN

Plusieurs travaux de recherche s'intéressent à l'aspect multi-accès des réseaux de prochaines générations. Dans [13], les auteurs se penchent sur la question de l'intégration des technologies WLAN et GPRS (General Packet Radio Service). Cet article traite de GPRS comme un service de données pouvant être utilisé dans un réseau de 2.5G ou 3G. Les auteurs présentent deux approches d'intégration WLAN-GPRS proposées dans la littérature technique. Il s'agit de l'approche à *couplage fort* (*tight coupling*) et de l'approche à *couplage faible* (*loose coupling*). La Figure 2.13 illustre les points où se fait l'interconnexion selon les deux approches de couplage.

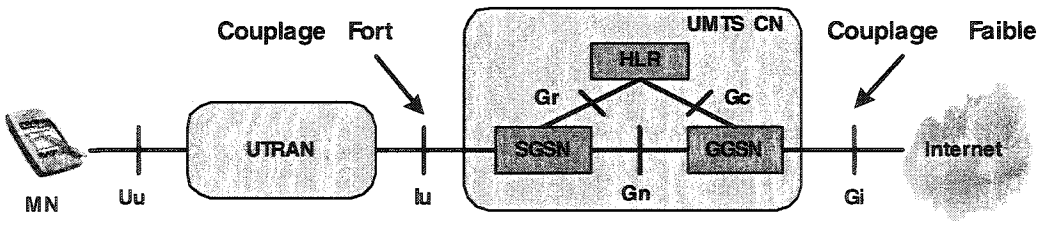

Figure 2.13 Point de référence pour deux approches de couplage

Dans l'approche à *couplage faible*, il n'y a pas d'interface entre le réseau WLAN et le réseau GPRS, l'interconnexion se fait à l'extérieur du système GPRS. Ainsi, les données provenant du WLAN accèdent directement au réseau externe et les mécanismes de contrôle GPRS ne sont pas utilisés. La gestion de la mobilité inter-technologique se fait avec IP Mobile. L'approche à *couplage fort* consiste à connecter le réseau d'accès WLAN au réseau cœur GPRS comme si c'était un autre réseau d'accès radio. Cette approche nécessite l'introduction de deux composantes d'inter-fonctionnement afin de préserver les interfaces standardisées de GPRS et rendre la partie radio de WLAN transparente. Entre le réseau cœur et le réseau d'accès WLAN, une fonction GIF (*GPRS*

Interworking Function). À l'intérieur du MN, se trouve une fonction WAF (*WLAN Adaptation Function*). La Figure 2.14 montre où se situent ces deux fonctions.

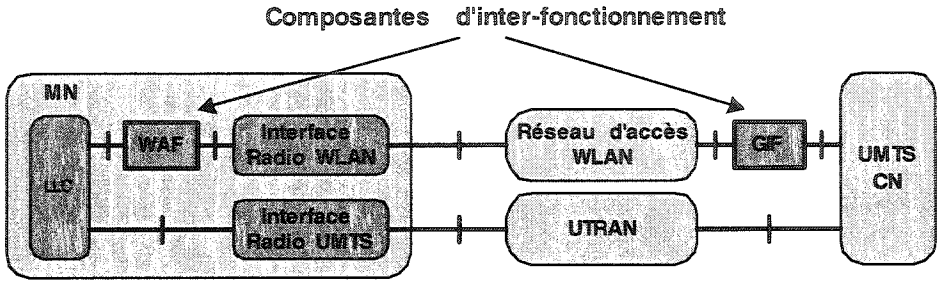

Figure 2.14 Composantes d'inter-fonctionnement dans une architecture WLAN

Dans cette approche, la relève verticale est assurée par le système GPRS pour lequel il s'agit d'un changement de zones RA et donc d'une relève intra ou inter-SGSN. L'approche de couplage fort s'applique principalement au cas où le réseau WLAN appartient à l'opérateur cellulaire. De plus, seuls les terminaux WLAN qui implémentent la fonction d'adaptation WAF peuvent être utilisés. L'approche à couplage faible s'applique plus largement dans le cas où plusieurs réseaux cellulaires ou WLAN indépendants sont interconnectés. Les auteurs avancent que la tendance générale est de suivre l'approche à couplage faible. Plusieurs préfèrent cette dernière car elle utilise des protocoles de l'IETF, ce qui la rend plus ouverte et facilite l'intégration ultérieure avec d'autres technologies d'accès.

L'architecture d'intégration des technologies WLAN et UMTS proposée par 3GPP est présentée dans [14]. La principale motivation de l'effort de standardisation est de permettre au fournisseur de service UMTS d'offrir un service d'accès WLAN complémentaire au service cellulaire. Cette architecture d'intégration est décrite dans les spécifications de 3GPP [23] et [24]. La gestion de la mobilité, éventuellement basé sur IP Mobile, ainsi que l'aspect de la qualité de service demeurent pour un développement futur. La Figure 2.15 illustre l'architecture WLAN utilisant l'abonnement 3GPP dans un scénario d'itinérance, où un serveur AAA du réseau WLAN sert de proxy entre le MN et le serveur AAA du réseau d'origine.

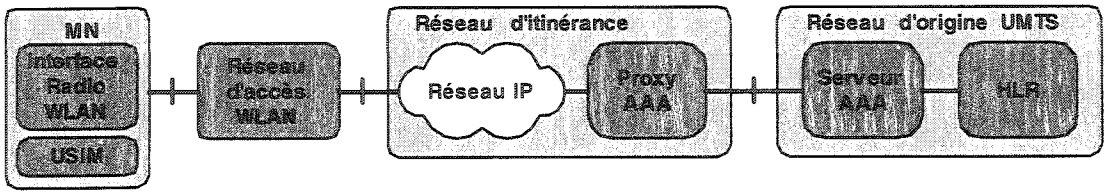

Figure 2.15 Architecture AAA WLAN

L'architecture d'intégration de 3GPP utilise 802.11i, le nouveau standard de sécurité pour WLAN de IEEE. Ce standard inclut le chiffrement des communications avec AES ainsi que le contrôle d'accès et l'authentification avec EAP. AES (*Advanced Encryption Standard*) est un standard cryptographique et EAP (*Extensible Authentication Protocol*) est un protocole de transport pour des méthodes d'authentification de bout en bout, donc entre le MN et le serveur AAA. Il ne définit pas de procédure mais plutôt un cadre pour des procédures plus spécifiques. 3GPP utilise la méthode spécifique EAP-AKA [30] qui permet d'encapsuler la procédure AKA de UMTS à l'intérieur du protocole EAP. Avec 802.11i et EAP-AKA, il est possible d'authentifier un nœud mobile dans un réseau WLAN à partir des informations de son abonnement UMTS. Notons aussi que 802.11i ne définit pas le protocole pour transporter pour les messages EAP jusqu'au serveur AAA; toutefois le standard de facto est *Diameter*. Nous décrivons les protocoles EAP et *Diameter* dans la prochaine section.

Dans [15], les auteurs font une comparaison de trois stratégies d'intégration des technologies UMTS et WLAN. Ils se concentrent sur la gestion de la mobilité et proposent une évaluation de la performance des différentes stratégies en mesurant la latence de la relève verticale. Deux des stratégies sont équivalentes aux approches présentées en [13]. L'approche *IP Mobile* est l'équivalent de l'approche à couplage faible tandis que l'approche *Émulateur* correspond à l'approche à couplage fort. Ils proposent aussi une troisième approche qu'ils appellent *Gateway*. Dans cette approche, illustré à la Figure 2.16, un nouveau nœud, le *Gateway*, sert d'interface entre les réseaux UMTS et WLAN. Ce nœud achemine le trafic de donnée pour les mobiles en itinérance

sous la zone de couverture de l'autre réseau. Deux cas d'itinérances sont possibles selon la provenance de l'utilisateur : s'il s'agit d'un utilisateur UMTS qui passe dans la zone WLAN ou vice versa. En plus de permettre une exploitation indépendante des deux types de réseau, cette approche ne nécessite pas l'utilisation d'un autre protocole comme IP Mobile pour la gestion de la mobilité.

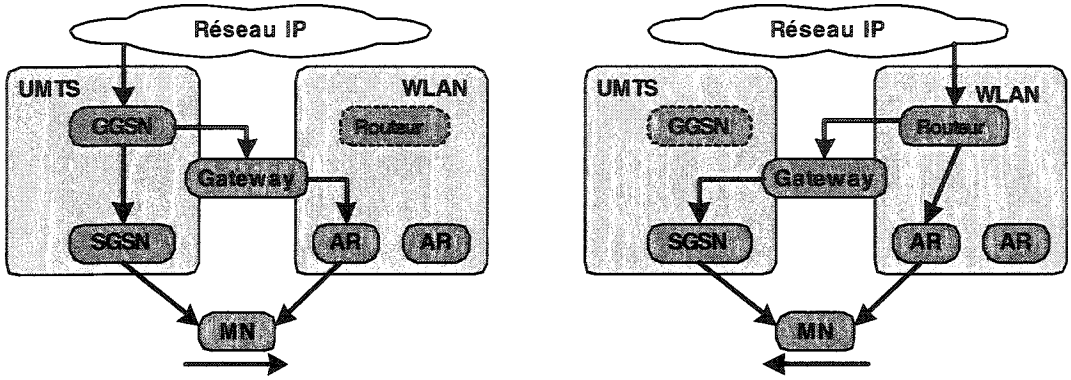

Figure 2.16 Architecture de l'approche *Gateway*

Suite à des simulations, les auteurs observent que l'approche *Émulateur* démontre les meilleures performances tandis que l'approche *Gateway* obtient des latences de relève un peu supérieures. Ces deux approches établissent des temps de relève en dessous des 150ms, même pour un grand nombre d'utilisateurs dans le réseau. L'approche IP Mobile obtient des latences de relève les plus grandes. Avec un grand nombre d'utilisateurs dans le réseau, la latence dépasse les 200ms, ce qui est trop pour du trafic avec des contraintes temps réel comme la voix ou la vidéoconférence. Ils concluent que l'approche IP Mobile, même si elle permet une grande flexibilité d'intégration, occasionne une latence trop grande lors d'une relève inter-technologique.

En somme, nous croyons que l'intégration des protocoles IP avec le système UMTS n'est pas adéquate. Nous avons vu que tout le trafic IP, y compris les paquets de contrôle, est encapsulé dans un tunnel à partir du MN jusqu'à ce qu'il quitte le réseau UMTS, au GGSN. Certains auteurs affirment que cette encapsulation jusqu'au GGSN induit une latence trop élevée pour les protocoles de contrôle IP. Dans le cas de la

gestion de mobilité inter-technologique avec IP Mobile, cette latence nuit grandement à la performance de la relève. Dans un système multi-accès où des mécanismes de contrôle IP sont utilisés, cette encapsulation empêche toute interaction entre les protocoles de contrôle IP et les protocoles UMTS. Cette façon de faire engendre un dédoublement de mécanismes de contrôle.

2.3 Protocoles de contrôle IP

Dans cette section, nous présentons les protocoles de contrôle IP que nous envisageons pour les réseaux mobiles de prochaine génération. La Figure 2.17 illustre cette architecture globale IP. Les technologies d'accès ont en commun qu'elles supportent toutes le protocole IP. En se déplaçant, le MN est capable de garder sa connexion même s'il change de type d'accès. Le Routeur d'Accès (AR) sert de point d'attache au réseau de transport IPv6.

Dans ce mémoire nous employons le protocole IPv6. La gestion de mobilité au niveau IP est assurée par IPv6 Mobile [25], l'authentification utilise le protocole *Diameter* [27], et la signalisation de qualité de service est réalisée avec le protocole HPMRSVP [40].

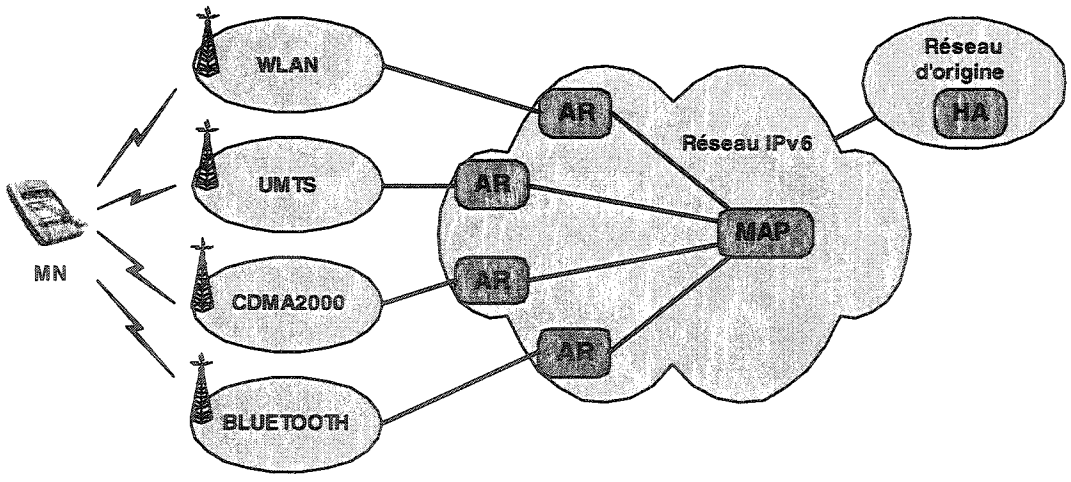

Figure 2.17 Architecture multi-accès avec MIPv6 et HMIPv6

2.3.1 IPv6 Mobile (MIPv6)

Le protocole IPv6 Mobile permet de faire de la gestion de la mobilité au niveau IP. Les éléments du réseau impliqués dans ce protocole sont le nœud mobile (MN), le Routeur d'Accès (AR), le *Home Agent* (HA) et le Nœud Correspondant (NC)[2]. Dans MIPv6, le MN est joignable par deux adresses IP, son adresse dite nominale basée sur le préfixe de sous-réseau de son réseau d'origine et une adresse secondaire, appelé CoA (*Care-of-Address*), basée sur le préfixe de sous-réseau du réseau visité. Dans son réseau d'origine, les paquets destinés au MN lui sont acheminés à son adresse nominale par les mécanismes IP classiques. Dans un réseau visité, les paquets sont acheminés au MN à une ou plusieurs adresses CoA. Pour chaque adresse CoA qu'il désire utiliser, le MN doit faire une association (*Binding*) entre son adresse nominale et l'adresse CoA. C'est le HA du réseau d'origine qui enregistre et maintient ces associations d'adresses. Deux modes de communication entre le MN et le NC sont définis dans MIPv6, le mode « bidirectionnel » et le mode « route optimisée ». La Figure 2.18 illustre les deux modes de communication.

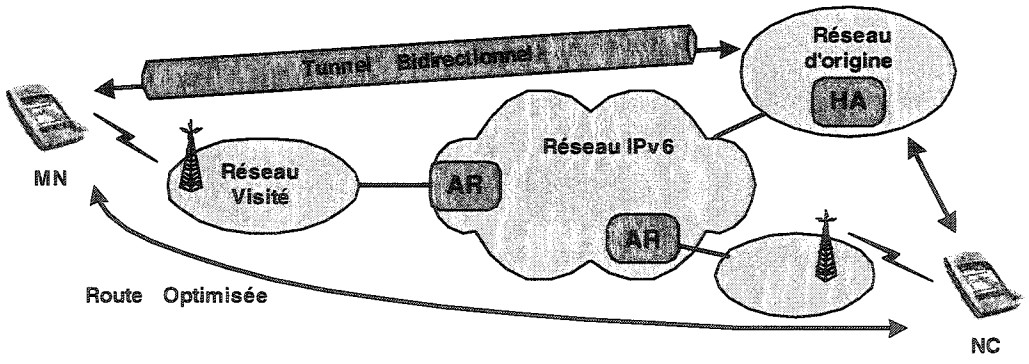

Figure 2.18 Mode de communication entre un MN et un NC dans MIPv6

[2] Nous utilisons l'acronyme NC plutôt que CN, utilisé dans la documentation MIPv6 pour ne pas confondre avec l'acronyme identique utilisé dans la nomenclature UMTS pour désigner le « Core Network ».

Dans le mode bidirectionnel, le NC n'a pas besoin de supporter MIPv6 pour échanger des données avec le MN, il envoie et reçoit les paquets avec l'adresse nominale du MN. C'est le HA, dans le réseau d'origine, qui intercepte les paquets destinés au MN, les encapsule et les transmet à travers un tunnel bidirectionnel jusqu'au MN. Les paquets provenant du MN sont transportés à travers le tunnel jusqu'au HA qui les achemine au NC. Dans le mode de route optimisée, le MN enregistre son association d'adresse CoA auprès du NC. Le MN et le NC peuvent ainsi communiquer directement sans que les paquets passent par le HA dans le réseau d'origine. Ce mode nécessite cependant que le NC implémente les mécanismes d'associations d'adresses de MIPv6.

Enregistrement de l'adresse CoA

Lorsqu'il est en mouvement, le MN peut changer de sous-réseau et donc de point d'attache AR. Dans chacun des sous-réseaux, les AR émettent à intervalle de temps régulier un message appelé *Router Advertisement*. Ces messages contiennent le préfixe d'adresse du sous-réseau pris en charge par le AR. En comparant le préfixe contenu dans ces messages avec celui de son adresse CoA courante, le MN peut détecter qu'il se déplace dans un nouveau sous-réseau. En changeant son point d'attache AR, le MN doit aussi changer son adresse CoA et donc mettre à jour l'association (BU : *Binding Update*) de son adresse CoA avec son adresse nominale auprès du HA. La Figure 2.19 illustre le diagramme de séquence de la procédure de mise à jour de l'association d'adresse CoA avec l'adresse nominale.

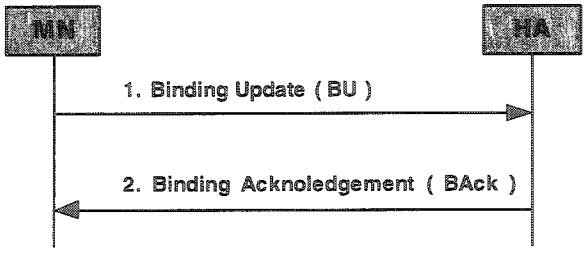

Figure 2.19 Mise à jour d'une association d'adresse MIPv6

1. En détectant un changement de sous-réseau, le MN envoie un message de mise à jour (BU) au HA contenant une nouvelle CoA proposée. À la réception du BU, le HA doit effectuer une détection de duplication d'adresse (DAD : *Duplicate Address Detection*). Cette étape permet de s'assurer que l'adresse CoA proposée n'est pas déjà utilisée par un autre MN. Si l'association est possible, le HA met à jour sa table d'association (*Binding cache*).
2. Le HA envoie un message BA (*Binding Acknowledgement*) au MN, qui dans le cas d'un succès, confirme l'enregistrement de l'association d'adresse et dans le cas d'un échec donne une raison.

Notons qu'une durée de vie est associée à une association d'adresse. Avant l'expiration de cet intervalle de temps, le MN doit faire une mise à jour de son adresse CoA, même s'il ne change pas de sous-réseau. Cet intervalle de temps peut être suggéré par le MN dans le BU, mais si le HA ne l'accepte pas, il en donne un autre dans le BA. Lorsqu'il retourne dans son réseau d'origine, le MN fait une mise à jour en indiquant une durée de vie de zéro afin d'annuler toute association d'adresse.

Pour utiliser le mode de communication de route optimisée, le MN doit enregistrer son adresse CoA auprès du NC pour que celui-ci puisse lui envoyer les paquets directement. Avant que le MN puisse mettre à jour son association d'adresse auprès du NC, ce dernier doit s'assurer que c'est le véritable MN qui fait la demande d'enregistrement. Ceci se fait grâce à la procédure de retour de routabilité (*Return Routability procedure*). Cette procédure, définie en détails dans la spécification de MIPv6 [25], permet au NC d'établir avec une certaine assurance qu'il reçoit l'enregistrement d'association du MN légitime. Par la suite, la procédure de mise à jour de l'association auprès du NC se fait comme la mise à jour d'association avec le HA, c'est-à-dire avec l'échange de messages BU et BA.

2.3.2 IPv6 Mobile Hiérarchique (HMIPv6)

Avec MIPv6, lorsqu'un MN change de point d'attache AR ou que la durée de vie d'une association d'adresse se termine, il doit mettre à jour son association avec le HA et avec tous les NC avec qui il communique en mode route optimisée. Ceci peut nécessiter un grand nombre de messages de signalisation, proportionnel au nombre de NC. En ajoutant un niveau hiérarchique dans l'architecture de MIPv6, HMIPv6 permet de réduire grandement le nombre de messages échangés pour mettre à jour les associations d'adresses du MN. HMIPv6 introduit un nouvel élément, le MAP (*Mobility Anchor Point*) qui sert de HA local pour les MN dans un domaine donné. La Figure 2.17 illustre où se situe le MAP dans l'architecture. Tant qu'il demeure dans le domaine du MAP, il suffit au MN de faire des mises à jour locales de son association, sans mettre à jour le HA et tous les NC.

HMIPv6 définit deux nouvelles adresses. L'adresse RCoA (*Regional Care-of Address*) est construite avec le préfixe de sous-réseau du MAP tandis que l'adresse LCoA (*Local Care-of Address*) est construite avec le préfixe du de sous-réseau du AR auquel s'attache le MN. Notons qu'avec HMIPv6, les messages de *Router Advertisement* diffusés par les AR contiennent le préfixe de sous-réseau du AR et le préfixe du sous-réseau du ou des MAP disponibles. Il faut donc deux associations d'adresses. La première, entre son adresse nominale et son adresse RCoA auprès du HA et des NC avec qui il communique, la deuxième, entre son adresse RCoA et son adresse LCoA auprès du MAP. Ainsi, le HA et les NC communiquent avec le MN en utilisant son adresse RCoA. En tant que HA local, le MAP intercepte les paquets destinés au MN à son adresse RCoA. Il les encapsule et les transmet au MN à son adresse LCoA. Les paquets provenant du MN sont transportés dans le tunnel jusqu'au MAP qui les achemine au HA ou au NC. L'adresse RCoA ne change pas tant que le MN demeure à l'intérieur du domaine du MAP. Le MN n'a qu'à mettre à jour son adresse LCoA auprès du MAP.

Enregistrement des adresses LCoA et RCoA

Lorsqu'il se déplace dans un nouveau sous-réseau et qu'il découvre un nouveau domaine MAP, le MN doit s'enregistrer auprès du MAP pour ensuite s'enregistrer auprès du HA dans son réseau d'origine. La Figure 2.20 suivante illustre la procédure de mise à jour de l'association de l'adresse LCoA avec l'adresse RCoA et de l'adresse RCoA avec l'adresse nominale.

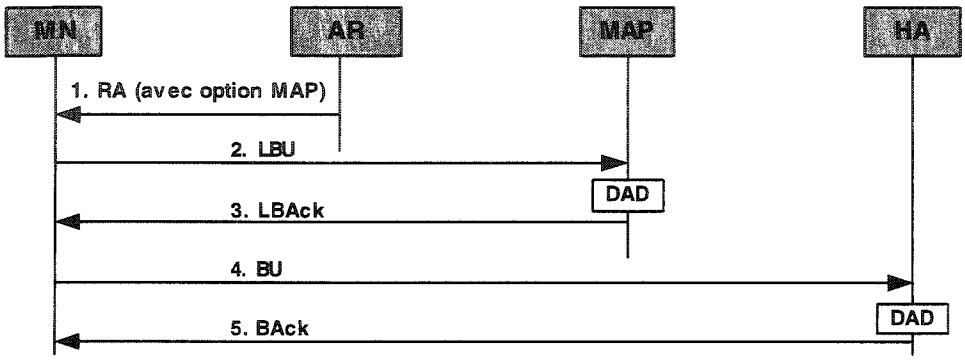

Figure 2.20 Mise à jour d'une association d'adresse HMIPv6

1. Le AR diffuse à intervalle de temps régulier des messages de *Router Advertisement* contenant les préfixes du AR et du ou des MAP disponibles.
2. Le MN envoie un message de mise à jour locale (LBU : *Local Binding Update*) au MAP contenant une association LCoA et RCoA proposée. Le MAP effectue un DAD pour s'assurer que l'adresse LCoA n'est pas déjà utilisée. Ensuite, il met à jour sa table d'association (*Binding cache*).
3. Le MAP envoie un message d'acquittement LBA au MN pour indiquer le succès ou l'échec de l'enregistrement de l'association.
4. Le MN envoie un message de mise à jour local (BU) au HA avec l'association de l'adresse RCoA et l'adresse nominale du MN. Le HA effectue un DAD pour s'assurer que l'adresse RCoA n'est pas déjà utilisée. Le HA met à jour sa table d'association (*Binding cache*).
5. Le HA envoie un message d'acquittement BA au MN.

La mise à jour de l'association de l'adresse RCoA avec l'adresse nominale (étapes 4 et 5) se fait de façon similaire avec le ou les NC qui communiquent avec le MN.

2.3.3 Protocole de AAA Diameter

Le protocole de base *Diameter* [27] est un protocole de AAA qui sert à transporter l'information nécessaire pour réaliser l'authentification, l'autorisation et la comptabilité. Utilisé seul, ce protocole permet de faire de la comptabilité (*Accounting*) seulement. Pour faire de l'authentification et de l'autorisation, il doit être augmenté par une *Application Diameter*. Une *application Diameter* ajoute des commandes et des attributs au protocole de base. Le protocole Diameter s'exécute entre un client et un *serveur Diameter*. Le *client Diameter* est un dispositif (NAS : *Network Access Server*) en bordure de réseau qui donne accès au réseau à un utilisateur. Le *serveur Diameter* est celui qui authentifie et autorise l'utilisateur. Les messages *Diameter* sont transportés par le protocole TCP/IP et assume que le transport des messages est sécurisé en utilisant IPSEC [6]. La Figure 2.21 illustre les acteurs dans le protocole *Diameter*.

Figure 2.21 Protocole *Diameter*

EAP (*Extensible Authentication Protocol*) [28] est un protocole cadre (*framework*) standard qui peut supporter plusieurs méthodes d'authentification. C'est un protocole qui s'exécute de bout-en-bout, entre l'utilisateur et le serveur d'authentification (serveur EAP). Cependant, comme l'illustre la Figure 2.22, il peut y avoir un *Authentificateur* qui agit comme intermédiaire dans l'échange et donne accès au service à l'utilisateur.

Figure 2.22 Protocole EAP et méthode d'authentification de bout en bout

Les messages EAP sont transportés sur un lien dédié entre l'utilisateur et le serveur EAP, comme une connexion PPP ou une lien de couche 2 (LAN, WLAN ou autre). Cependant, entre l'*Authentificateur* et le *serveur EAP*, un lien direct est rarement possible, car ils peuvent être dans des domaines différents, dans une situation d'itinérance par exemple. C'est pour cette raison qu'il est nécessaire d'utiliser un protocole de transport AAA, comme *Diameter*, pour transporter les messages EAP entre l'*Authentificateur* et le *serveur EAP*. Le protocole EAP est extensible, il permet d'implémenter une procédure d'authentification spécifique, entre l'utilisateur et le *serveur EAP*. L'*Authentificateur*, lorsqu'il est présent, donne l'accès à l'utilisateur mais ignore les détails de la procédure. Ceci permet de changer la méthode spécifique d'authentification sans modifier l'*Authentificateur*.

L'*application Diameter-EAP* [29] permet de transporter des messages EAP entre un NAS (*Authentificateur* EAP) et un serveur AAA (Serveur EAP) avec le protocole *Diameter*. Cette application définit des nouvelles commandes et des nouveaux attributs qui permettent d'encapsuler les messages EAP (*EAP-Payload*) dans une session *Diameter*. La Figure 2.23 montre un diagramme de séquence des messages échangés lors d'une procédure d'authentification utilisant l'application *Diameter*-EAP.

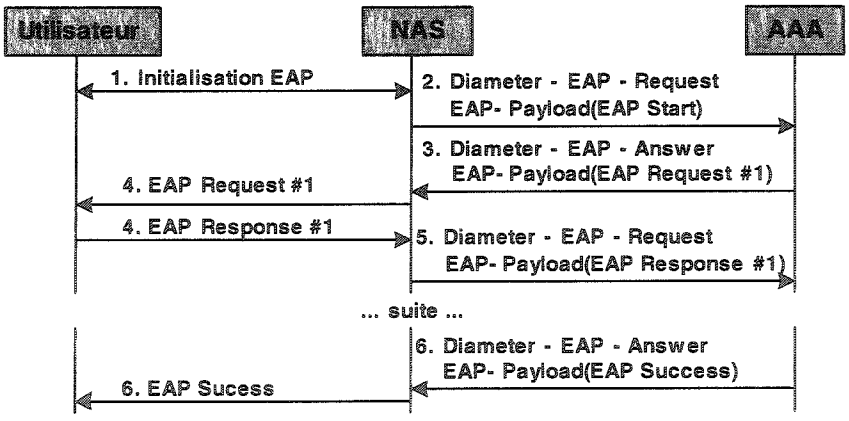

Figure 2.23 Procédure d'authentification avec Diameter -EAP

1. Initialisation de EAP lorsqu'un utilisateur se connecte au NAS.

2. Le NAS envoie une requête *Diameter* au serveur AAA pour commencer la procédure d'authentification de l'utilisateur.
3. Le serveur AAA commence la procédure d'authentification avec une réponse *Diameter* encapsulant la première requête EAP.
4. Le NAS transmet la requête EAP à l'utilisateur. Celui-ci renvoie la réponse EAP au NAS. Normalement le premier échange EAP sert à établir l'identité de l'usager.
5. Le NAS encapsule la réponse EAP dans une requête *Diameter* et l'envoie au serveur AAA.

Les étapes 3, 4 et 5 sont répétées autant de fois que nécessaire selon la procédure d'authentification spécifique utilisée.

6. Une fois que tous les échanges de la procédure d'authentification sont terminés, le serveur AAA envoie une réponse *Diameter* au NAS indiquant le succès ou l'échec de l'authentification. La réponse peut contenir un message EAP à transmettre à l'utilisateur pour indiquer le succès de la procédure.

2.3.4 Protocole HPMRSVP

Dans le domaine IP, nous souhaitons utiliser le protocole HMPRSVP [40] (*Hierarchical Proxy Mobile Resource Reservation Protocol*). Comme RSVP [38], ce protocole permet de faire de la réservation de ressources dans un réseau d'accès IP afin de garantir un niveau de qualité de service. Cependant, contrairement à RSVP, HPMRSVP est adapté à un environnement d'utilisateur mobile. En effet, HPMRSVP se base sur l'architecture de HMIPv6 et utilise le MAP comme proxy de réservation de ressources. La réservation de ressources se fait localement dans le domaine du MAP, où se trouve le nœud mobile. Elle se fait aussi localement dans le domaine du nœud correspondant. La Figure 2.24 illustre l'utilisation du protocole HPMRSVP dans une architecture HMIPv6. On y voit que la réservation est faite localement dans chacun des domaines d'accès. HPMRSVP suppose que les mécanismes dans le sous-réseau de

transport, entre les deux domaines MAP, garantissent le niveau de qualité de service suffisant.

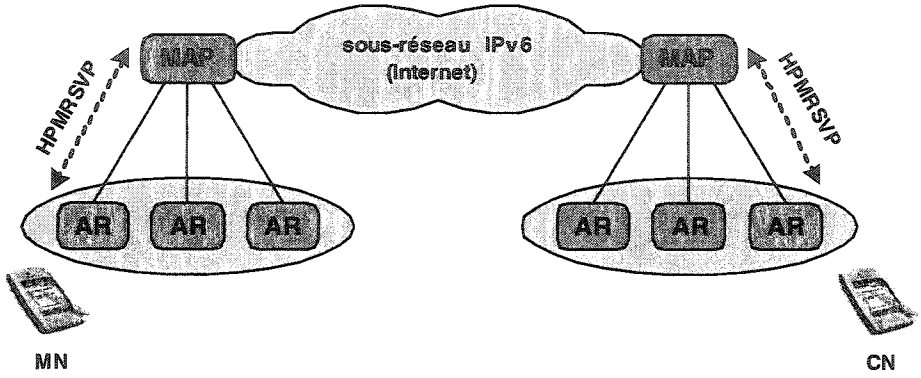

Figure 2.24 Réservation de ressource inter-domaine avec HPMRSVP

HPMRSVP utilise les mêmes messages de signalisation que le protocole RSVP. Cependant, HPMRSVP est orienté émetteur, c'est-à-dire que la réservation est faite par l'entité qui émet les données, avec le message « PATH » [38]. Ainsi à l'intérieur d'un domaine, le nœud mobile fait la réservation sur le lien ascendant, tandis que le MAP, au nom du nœud correspondant, fait la réservation sur le lien descendant. La Figure 2.25 illustre la séquence d'échange de messages lors d'une réservation de ressources locales pour un flux de données bi-directionnel.

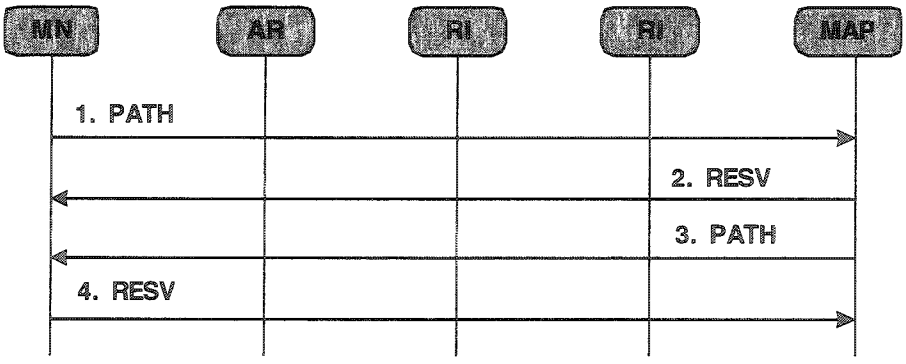

Figure 2.25 Diagramme de séquence d'une réservation locale bi-directionnelle

1. Le MN envoie un message PATH pour faire la réservation sur le lien ascendant. Ce message est acheminé par le AR et les RI (Routeur Intermédiaire) jusqu'au MAP.
2. Le MAP confirme la réservation en envoyant le message RESV au MN.
3. Le MAP (proxy de réservation de ressources) envoie un message PATH pour faire la réservation sur le lien descendant.
4. Le MN confirme la réservation en envoyant le message RESV au MAP.

Le protocole HPMRSVP est actuellement un *Draft* soumis à l'IETF. Cette spécification du protocole HPMRSVP contient les détails sur la réservation initiale ou la modification de la réservation des ressources locales. Ce document propose aussi différentes stratégies de relève entre deux routeurs d'accès qui tiennent compte de la réservation des ressources.

CHAPITRE 3

INTÉGRATION DE MÉCANISMES DE CONTRÔLE BASÉS SUR IP DANS LE RÉSEAU CŒUR UMTS

Dans le chapitre précédent, nous avons présenté la technologie UMTS, son architecture ainsi que les mécanismes qui contrôlent l'authentification, la gestion de la mobilité et la signalisation de qualité de service. Nous avons résumé la vision partagée par plusieurs experts de ce que seront les réseaux mobiles de prochaines générations. Puis, nous avons décrit des protocoles de contrôle basés sur IP que nous envisageons dans ce mémoire. Ces protocoles basés sur IP sont définis par des RFC ou des *Drafts* maintenus au sein de l'organisme de standardisation IETF. Dans ce troisième chapitre, nous présentons notre proposition d'évolution pour les systèmes UMTS qui intègre des mécanismes de contrôle basés sur IP dans le réseau cœur. Pour commencer, nous décrivons les caractéristiques et l'architecture du système que nous proposons. Ensuite, nous expliquons l'intégration des protocoles de contrôle IP dans cette architecture. Enfin, nous présentons la manière dont la mise en correspondance de protocole se fait pour chacun des mécanismes de contrôle que nous considérons, soient l'authentification, la signalisation de qualité de service ainsi que la gestion de la mobilité.

3.1 Caractéristiques du système proposé

Comme nous l'avons vu au chapitre précédent, l'architecture UMTS est divisée en un réseau d'accès UTRAN et un réseau cœur. Notre proposition consiste à utiliser un réseau entièrement IP dans le réseau cœur UMTS. De plus, nous proposons de remplacer les protocoles de contrôle UMTS utilisés dans le réseau cœur par des protocoles de contrôle basés sur IP. Nous voulons laisser le UTRAN tel qu'il est, il ne doit y avoir

aucun impact (ou un minimum). Notons que cette proposition s'applique au domaine PS seulement et pour le trafic IPv6 uniquement. Pour le trafic IPv4, les mécanismes UMTS classiques sont maintenus.

Nous proposons également de faire une mise en correspondance entre les protocoles UMTS et les protocoles basés sur IP. Les protocoles de contrôle IP ou UMTS fonctionnent de façon très similaire. Par exemple, dans la gestion de la mobilité, le message de BU (*Binding Update*) du protocole MIPv6 dans le domaine IP et le message de mise à jour de la zone RA (*Routing Area Update*) du protocole GMM dans le domaine UMTS ont la même fonction, c'est-à-dire mettre à jour la position courante du MN afin de permettre au réseau cœur de garder la connectivité avec le MN.

Dans le UTRAN, la signalisation UMTS ne change pas, mais en bordure du réseau cœur, les messages de contrôle UMTS sont « convertis » en messages de contrôle de protocole IP, puis acheminés dans le réseau cœur. Le processus est le même au niveau du MN, l'application utilise les protocoles basés sur IP, qui sont traduits en protocoles UMTS pour être transmis par le module radio. La Figure 3.1 illustre de façon simplifiée la mise en correspondance entre les protocoles de contrôle UMTS et IP.

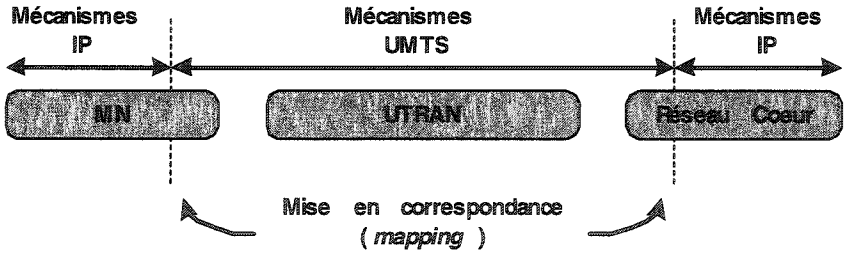

Figure 3.1 Mise en correspondance de protocoles de contrôle

La mise en correspondance (*mapping*) de messages de contrôle permet d'éviter le transport de messages comme des données usager. En réutilisant la signalisation UMTS à travers le UTRAN, on élimine le dédoublement de mécanismes de contrôle et on peut ainsi réduire l'utilisation de ressources radio. Reprenons l'exemple de gestion de la mobilité; lorsque le MN génère un message BU, ce message est traduit en message

Routing Area Update, puis transmis à travers le UTRAN. Lorsqu'il arrive au réseau cœur, la traduction inverse est effectuée et le message BU est restitué. Ainsi, il n'est plus nécessaire pour le MN d'activer un contexte PDP (session de transfert de données) à chaque fois qu'il envoie un message BU.

En éliminant la redondance et l'encapsulation de messages de contrôle IP, nous croyons ainsi obtenir une meilleure intégration des mécanismes IP. De plus, dans le contexte multi-accès des réseaux mobiles de prochaines générations, l'utilisation de protocoles de contrôle IP standardisés facilitera l'intégration avec d'autres technologies d'accès.

3.2 Architecture d'un système UMTS évolué

Dans le système UMTS évolué que nous envisageons, l'architecture HMIPv6, présenté au chapitre précédent, est intégrée à l'architecture du réseau cœur. Les éléments du réseau cœur intègrent les fonctions des éléments réseau d'une architecture HMIPv6. Comme nous l'expliquons plus loin, ceci permet d'utiliser HMIPv6 pour faire la gestion de la mobilité à l'intérieur du réseau UMTS (relève inter-SGSN). Nous intégrons les fonctionnalités de routeur d'accès (AR) dans le SGSN, que nous appelons le EGSN (*Evolved GPRS Support Node*), ainsi que les fonctionnalités de MAP dans le GGSN, que nous appelons le MER (*Mobility Edge Router*).

Dans cette architecture, nous voulons supprimer les protocoles de contrôle UMTS dans le réseau cœur, pour les remplacer par des protocoles basés sur IP. Le protocole GTP-C, entre le SGSN et le GGSN, ainsi que le protocole MAP-SS7[3] (*Mobile Application Part*), entre le SGSN et le HLR, sont retirés pour être remplacés par des protocoles IP standardisés. Notons que ce changement concerne seulement les trois mécanismes de contrôle énoncés précédemment, les protocoles GTP-C et MAP-SS7

[3] Nous utilisons l'acronyme MAP-SS7 parce que l'acronyme MAP est déjà utilisé pour désigner l'élément de réseau *Mobile Anchor Point* dans HMIPv6. Nous choisissons MAP-SS7 parce que ce protocole est basé sur le protocole de signalisation SS7.

peuvent servir à plusieurs autres fonctions de contrôle que nous ne considérons pas dans ce mémoire. La Figure 3.2 illustre l'architecture évoluée UMTS.

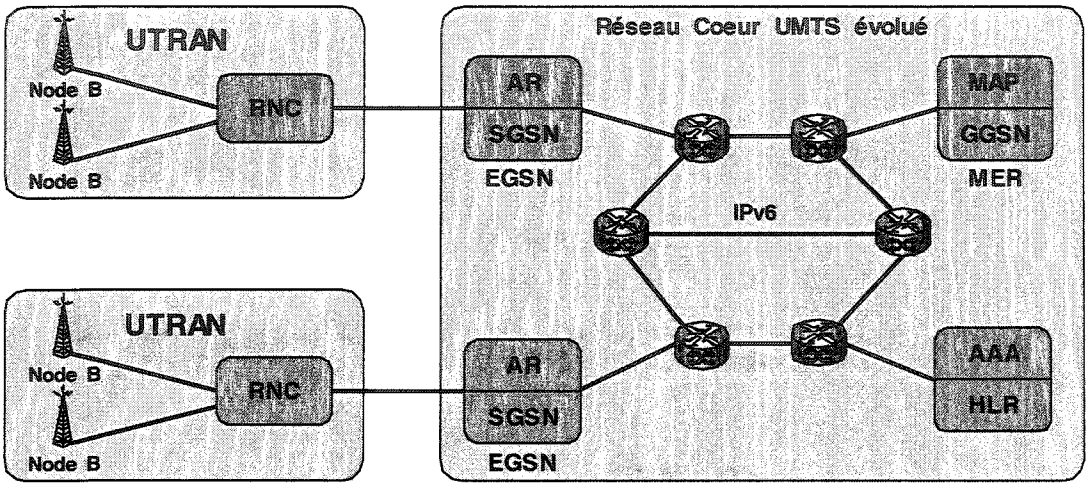

Figure 3.2 Architecture UMTS évoluée

Pour l'authentification, nous proposons d'utiliser le protocole de transport *Diameter* avec le protocole extensible d'authentification EAP. Pour ce faire, il faut ajouter la fonctionnalité de *client Diameter* au EGSN, pour qu'il communique avec un serveur AAA. Ce dernier doit avoir une interface ou encore coexister avec le HLR pour qu'il puisse y prélever les informations sur les utilisateurs. Nous souhaitons utiliser le protocole HPMRSVP pour la signalisation de qualité de service. Il faut donc intégrer la fonction de proxy de qualité de service, tel que défini par le protocole HPMRSVP dans le MER. Comme nous le mentionnons au chapitre 2, dans un système UMTS, la majeure partie de la gestion de la mobilité est prise en charge par le UTRAN et les éléments du réseau cœur interviennent peu. Cependant, lorsque le SGSN intervient pour une mise à jour périodique ou une relève inter-SGSN (inter-EGSN), nous utilisons HMIPv6 pour assurer cette gestion de la mobilité. Le EGSN, qui se trouve à la frontière du réseau cœur, a également la responsabilité de faire la mise en correspondance de protocoles de contrôle avec le UTRAN. La mise en correspondance de protocole est traitée dans la section suivante.

Dans cette architecture évoluée, le transport des données usagers dans le réseau cœur n'utilise plus le protocole GTP, il se fait directement par la couche IP. Notons que l'architecture UMTS conventionnelle, tel que définie par 3GPP, utilise déjà IP dans le réseau cœur. Cependant, comme l'illustre les piles de protocole à la Figure 2.3, la couche IP sert de transport pour les tunnels GTP qui encapsulent les paquets de données d'usagers. Ce n'est qu'à la sortie du réseau UMTS que ces paquets de données sont restitués et acheminés normalement sur un réseau IP externe comme l'Internet. Comme l'illustre la Figure 3.3, l'encapsulation n'existe plus dans le réseau cœur de l'architecture proposée; à partir du EGSN, les paquets IP usagers sont acheminés directement par la couche IP.

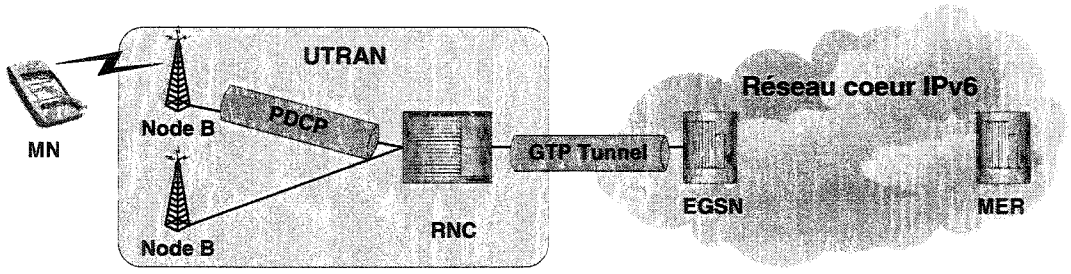

Figure 3.3 Encapsulation des données d'usagers dans l'architecture évoluée

3.3 Mise en correspondance de protocole de contrôle

Dans cette section, nous définissons la mise en correspondance de protocole de contrôle. Il s'agit de la mise en correspondance entre les protocoles de contrôle UMTS et les protocoles de contrôle basés sur IP. Nous expliquons d'abord les concepts avec lesquels nous établissons les règles de correspondance et, par la suite, nous précisons comment faire la conversion pour les mécanismes de contrôle considérés dans ce mémoire, soit l'authentification, la signalisation de qualité de service et la gestion de la mobilité.

Nous entendons par mise en correspondance (*mapping*) de protocole, l'activité de convertir un message d'un protocole donné avec un message équivalent dans un autre protocole, sans qu'il n'y ait de perte d'information, pour que le message originel puisse être reconstitué ultérieurement par une mise en correspondance inverse. Bien entendu, les deux protocoles à mettre en correspondance doivent avoir le même rôle et un fonctionnement similaire. Ainsi, pour que la mise en correspondance entre deux protocoles soit possible, la séquence d'échange de messages ainsi que les machines à états des entités impliquées dans la procédure de contrôle doivent être équivalentes et compatibles. Il est cependant possible d'associer un message d'un protocole à plusieurs messages d'un autre protocole, et vice versa. Une telle situation nécessite en général que l'élément qui fait la conversion de protocole garde une trace et de l'information sur l'état des échanges de messages en cours.

Chaque message de contrôle contient un ou plusieurs paramètres. Il faut donc établir une correspondance entre les paramètres des messages équivalents des deux protocoles concernés. Les paramètres ne doivent pas obligatoirement avoir les mêmes valeurs et/ou formats, mais il doit y avoir des règles de correspondance établies pour qu'il n'y ait pas d'ambiguïté lors d'une conversion et ce, dans les deux directions.

Il est possible que certains paramètres d'un protocole n'aient pas de correspondance dans un autre protocole. Dans cette situation, nous pouvons soit réutiliser des paramètres optionnels ou encore concaténer (*piggybacking*) les paramètres qu'on ne peut pas convertir avec les messages de l'autre protocole. La Figure 3.4 illustre un exemple de mise en correspondance de paramètres entre des messages de deux protocoles. Les paramètres circonscrits par des « [ ] » sont optionnels.

Dans la Figure 3.4, le protocole B correspond au protocole intermédiaire; dans notre cas, il s'agit des protocoles GMM et SM de UMTS. Comme nous voulons minimiser les impacts sur ces protocoles, nous optons pour la réutilisation de paramètres optionnels plutôt que de définir de nouveaux paramètres.

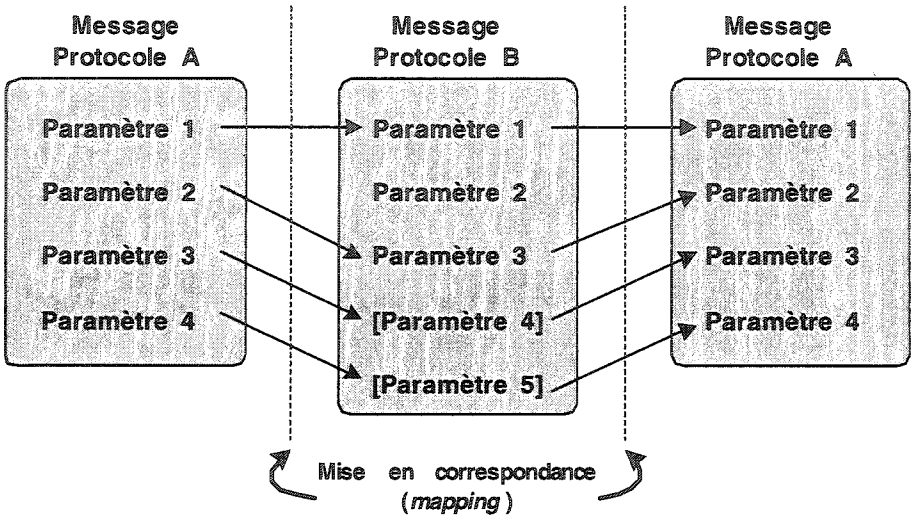

Figure 3.4 Mise en correspondance des paramètres entre deux protocoles

Cependant, dans certaines situations, il n'est pas possible de réutiliser des paramètres existants. Les messages des protocoles GMM et SM sont de longueur variable car certains paramètres sont optionnels ou de longueur variable. Les spécifications techniques de UMTS [34] définissent la structure des messages de couche 3 dans le plan contrôle. Les protocoles GMM et SM font partie de cette couche. Les messages des protocoles de couche 3 contiennent une partie obligatoire et une partie optionnelle (possiblement vide). Les spécifications indiquent qu'une entité qui traite ces messages doit être préparée à recevoir des messages de longueur variable, pouvant contenir des paramètres optionnels qui lui sont inconnus. Ceci permet à une implémentation de supporter plusieurs versions d'un protocole. Les paramètres optionnels inconnus doivent tout simplement être ignorés par une entité qui ne les reconnaît pas. Il est donc possible d'ajouter des paramètres à un message des protocoles GMM et SM sans impact sur le fonctionnement du système.

Dans un système UMTS, les protocoles de contrôle GMM et SM régissent les communications du domaine PS entre le MN et le réseau cœur. Ces protocoles sont définis par des procédures qui contiennent plusieurs échanges de message entre le MN et le SGSN, ainsi qu'entre le SGSN et les autres éléments du réseau cœur, c'est-à-dire les

autres SGSN, le HLR ou les GGSN. Nous définissons une mise en correspondance entre les messages définis dans les procédures GMM et SM de UMTS avec les messages de contrôle définis par les protocoles basés sur IP. Pour chaque mécanisme de contrôle que nous examinons dans ce mémoire, le Tableau 3.1 présente les procédures UMTS et les protocoles IP que nous jumelons.

Tableau 3.1 Association de procédure UMTS avec des protocoles IP

Mécanisme de Contrôle	Procédure UMTS	Protocole basé sur IP
Authentification	Authentification et échange de clés (GMM)	Diameter et EAP-AKA
Signalisation de qualité de service	Activation de Contexte PDP (SM)	HPMRSVP
Gestion de la mobilité	Mise à jour de la zone RA (GMM)	HMIPv6

La mise en correspondance de protocoles de contrôle nécessite une fonction de conversion qui doit être présente aux extrémités du domaine du UTRAN, c'est-à-dire dans le MN ainsi qu'à l'entrée du réseau cœur, dans le EGSN. La Figure 3.5 illustre l'architecture du système évolué avec les différents éléments fonctionnels et la mise en correspondance des protocoles de contrôle.

Le MN illustré à la Figure 3.5 est divisé en deux entités logiques : le TE (*Terminal Equipment*) et le MT (*Mobile Termination*). Cette séparation logique suit le modèle UMTS, qui définit le TE comme la partie du MN qui est le point de terminaison du service de télécommunication et le MT comme le point de terminaison de la transmission radio. Le TE fournit les fonctions de communication standards aux applications usagers, il est indépendant du système mobile utilisé. Le MT est dépendant du système mobile et implémente les protocoles de communication UMTS. Le TE communique avec le MT à travers une fonction d'adaptation, situé dans le MT, qui

convertit les communications provenant du TE pour utiliser les protocoles UMTS. Pour plus de détails sur la séparation TE - MT, tel que définie par 3GPP, se référer à [16], [35] et [36].

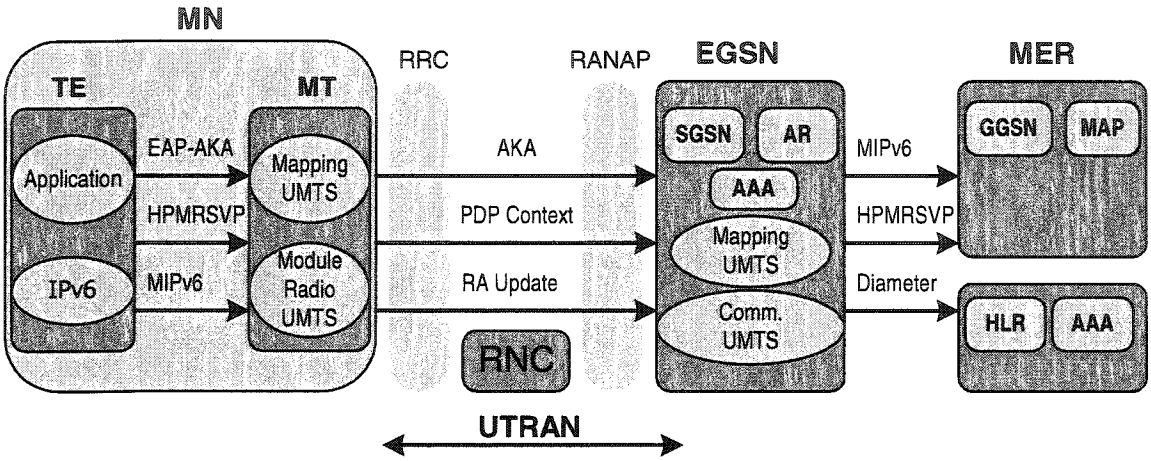

Figure 3.5 Mise en correspondance de protocoles de contrôle IP – UMTS

Cette séparation logique a l'avantage de permettre au TE, qui est indépendant de la technologie d'accès, d'utiliser plusieurs types de MT selon le type d'accès avec lequel il veut communiquer. Ainsi, pour l'application, il n'y a aucune différence du point de vue du service de télécommunication offert par le TE. C'est la fonction d'adaptation à l'intérieur du MT qui est responsable de faire la mise en correspondance entre les protocoles de contrôle standards utilisés par l'application avec le TE et les protocoles de contrôle utilisés par la technologie d'accès implémentée par le MT. Dans notre cas, il s'agit d'un MT de type UMTS. Comme nous voulons utiliser des protocoles standard basés sur IP avec un système UMTS, nous devons définir la mise en correspondance qui doit se faire dans la fonction d'adaptation du MT. Cette fonction d'adaptation doit également être implémentée dans le EGSN pour faire la mise en correspondance inverse, étant donné que nous voulons utiliser les protocoles IP dans le réseau cœur.

3.3.1 Authentification

Normalement dans un système UMTS, l'authentification de l'usager et du réseau se fait par l'exécution de la procédure AKA (*Authentication and Key Agreement*). Elle est exécutée en premier lieu durant l'attachement au réseau du MN mais elle peut être répétée ultérieurement au cours des autres procédures de signalisation GMM. Dans le système UMTS évolué, nous souhaitons garder l'authentification basée sur cette procédure.

Tel que décrit au chapitre précédent, la procédure AKA comporte l'authentification mutuelle de l'usager et du réseau qui fournit le service ainsi que la génération des clés cryptographiques nécessaires à la protection des communications dans le UTRAN.

Pour implémenter le mécanisme d'authentification dans le domaine IP, nous utilisons la éthode spécifique EAP-AKA proposée à l'IETF. Cette méthode a été développée afin de reproduire la procédure AKA de UMTS en utilisant le cadre EAP. Elle permet ainsi d'utiliser la procédure AKA avec n'importe quel type de lien qui supporte l'échange de messages EAP. Dans le contexte du système évolué que nous considérons, la mise en correspondance entre la méthode AKA implémenté dans le protocole GMM et la méthode EAP-AKA est directe car les formats des paramètres à mettre en correspondance sont les mêmes. La Figure 3.6 illustre le diagramme de séquence de l'exécution d'une procédure d'authentification avec la conversion de protocole dans le MT au niveau du MN ainsi que dans le EGSN à la frontière du réseau cœur.

Ce diagramme de séquence illustre la procédure AKA se faisant en deux échanges aller-retour, donc en quatre messages. On remarque aussi que la fonction de communication UMTS, où se fait la conversion des protocoles de contrôle, ainsi que la fonction de Serveur EAP, sont toutes les deux incluses dans le EGSN. En effet, dans l'architecture du système, c'est le EGSN qui agit comme authentificateur (Serveur EAP). Il doit donc y avoir une conversion de protocole interne. Il serait cependant

possible qu'une implémentation ne fasse pas de conversion inverse afin d'optimiser l'exécution de la procédure.

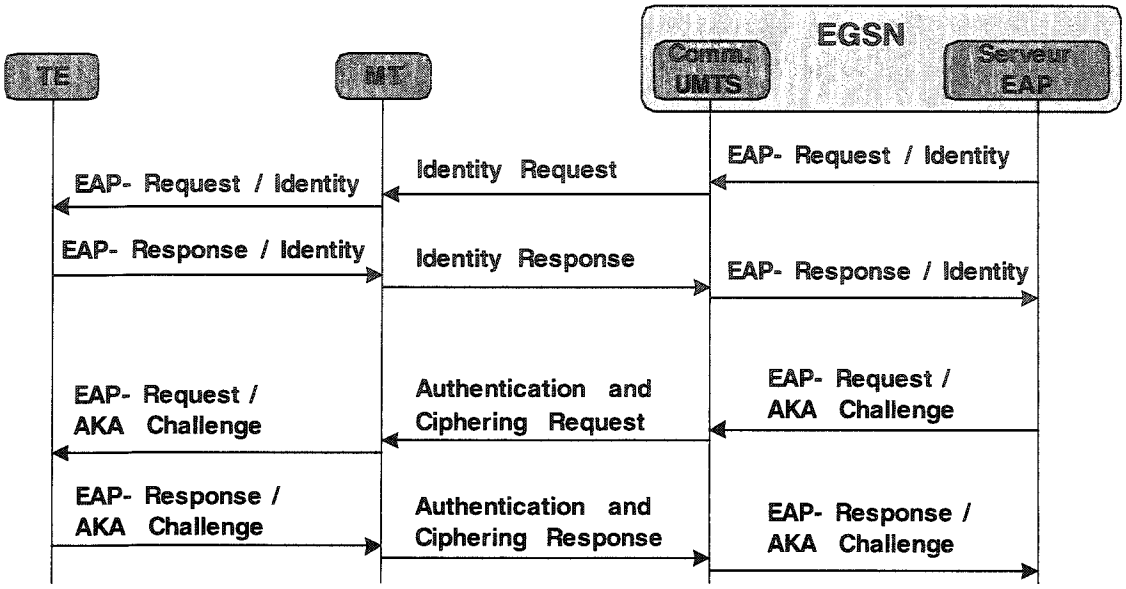

Figure 3.6 Procédure AKA avec mise en correspondance au MT et au EGSN

L'utilisation de EAP-AKA comme protocole dans le domaine IP donne l'avantage qu'il n'est pas nécessaire de convertir des paramètres. Étant donné que EAP-AKA reproduit la procédure AKA, les paramètres et leurs formats sont les mêmes. Le Tableau 3.2 présentent les paramètres contenus dans les messages échangés lors de cette procédure.

Notons que le Tableau 3.2 ne présente que les paramètres UMTS que nous considérons dans la mise en correspondance, les messages complets contiennent plusieurs autres paramètres. Pour plus de détails sur le contenu des messages, se référer aux spécifications techniques [17]. De plus, nous avons mis en gras, les paramètres qui ne peuvent être mis en correspondance et qui doivent être ajoutés aux messages GMM.

Tableau 3.2 Mise en correspondance des paramètres des messages AKA

EAP - AKA		UMTS	
Message	**Paramètres**	**Message**	**Paramètres**
EAP-Request / Identity	• AT_PERMANENT_ID_REQ	Identity Request	• Identity type
EAP-Response / AKA-Identity	• AT_IDENTITY	Identity Response	• Mobile Identity
EAP-Request / AKA-Challenge	• AT_RAND • AT_AUTN • **AT_MAC**	Authentication and Ciphering Request	• Authentication parameter RAND • Authentication parameter AUTN • **EAP-AKA MAC parameter**
EAP-Response / AKA-Challenge	• AT_RES • **AT_MAC**	Authentication and Ciphering Response	• Authentication parameter Response (RES) • Authentication Response parameter (extension) • **EAP-AKA MAC parameter**

En effet, bien que EAP-AKA reproduise la procédure AKA, ce protocole ajoute un attribut (AT_MAC) dans les messages d'authentification. Cet attribut permet d'authentifier les messages EAP échangés. C'est un code d'authentification calculé avec une fonction de hachage sur le message EAP entier. Il est donc nécessaire de transporter cet attribut supplémentaire comme un paramètre optionnel additionnel dans les messages UMTS qui traversent le UTRAN.

Afin d'authentifier un utilisateur, le EGSN doit obtenir un ou plusieurs vecteurs d'authentification du HLR. Dans un système UMTS classique, le SGSN utilise le protocole MAP-SS7 pour communiquer avec le HLR. Dans le système UMTS évolué, nous souhaitons utiliser le protocole *Diameter*. Comme nous le mentionnons au deuxième chapitre, le protocole *Diameter* ne peut être utilisé seul, une *application Diameter* est nécessaire pour définir comment des informations d'authentification sont transportées. Dans notre cas, ce serait pour le transport des vecteurs d'authentification. Or, nous nous sommes rendu compte que cet aspect du problème a déjà été abordé.

L'organisme 3GPP propose en effet une *application Diameter* capable de transporter les vecteurs d'authentification. Les spécifications techniques [32] et [33] définissent cette *application Diameter*. Nous retenons donc la proposition de 3GPP dans notre architecture évoluée pour transporter les vecteurs d'authentification dans le réseau cœur.

La combinaison de EAP-AKA et de *Diameter* permet donc de reproduire la procédure AKA de UMTS. Nous constatons que l'organisme 3GPP a déjà entamé des travaux dans cette direction dans le but de permettre aux opérateurs de service UMTS d'offrir un accès WLAN à leurs abonnés à partir de leur souscription 3G. Cette approche est cependant applicable à d'autres technologies d'accès, pourvu que le protocole EAP puisse être utilisé. Dans un contexte multi-accès, ceci permettrait d'avoir un mécanisme d'authentification globale, indépendant de la technologie d'accès.

3.3.2 Signalisation de qualité de service

Dans un système UMTS, la signalisation de qualité de service se fait avec le protocole gestion de session SM. Ce protocole permet d'activer, de modifier ou de désactiver des contextes PDP, qui correspondent à des sessions de transfert de données. Lors de l'activation d'un contexte PDP, le système UMTS réserve des ressources radio dans le UTRAN et crée dans le SGSN et le GGSN, les contextes nécessaires au traitement de la session de transfert de données. Avant que la signalisation de qualité de service puisse avoir lieu, un contexte de mobilité pour le MN doit être détenu par le SGSN, c'est-à-dire qu'il est authentifié et sa position courante est connue.

Dans le système UMTS évolué que nous proposons, nous remplaçons le protocole SM par le protocole HPMRSVP dans le domaine IP, c'est-à-dire dans le réseau cœur ainsi que dans le MN, entre le TE et le MT. La Figure 3.7 illustre l'utilisation des deux protocoles de signalisation de qualité de service dans l'architecture évoluée.

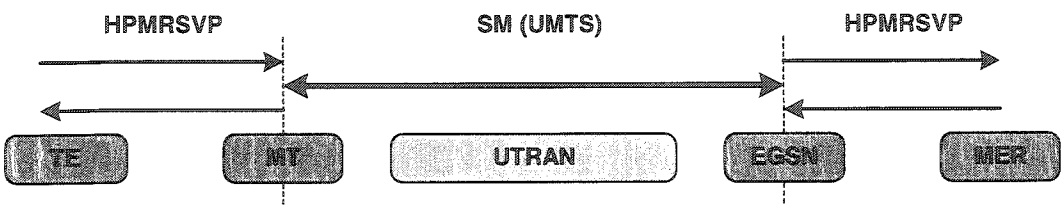

Figure 3.7 Signalisation de qualité de service dans l'architecture UMTS évoluée

Bien que les protocoles SM de UMTS et HPMRSVP servent tous les deux à la signalisation de qualité de service, ils n'ont pas un fonctionnement identique. Tout d'abord, l'activation de contexte PDP du protocole SM permet d'établir une session de transfert de données bidirectionnel, tandis qu'avec HPMRSVP, la signalisation se fait de façon unidirectionnelle, en partant de l'émetteur du flux de donnée. Ainsi, pour faire un échange de données bidirectionnel entre deux interlocuteurs avec le protocole HPMRSVP, deux sessions unidirectionnelles doivent être établies. Chacune des entités impliquées dans l'échange établit une session pour l'envoi de données en amont, étant donné que HPMRSVP est orienté émetteur. De plus, nous verrons plus loin que pour caractériser la qualité de service sollicitée par une session, les deux protocoles n'utilisent pas exactement les mêmes paramètres. Il est donc essentiel de tenir compte des différences de fonctionnement de ces deux protocoles pour établir leur mise en correspondance.

Contrairement à l'authentification, la mise en correspondance des protocoles de signalisations de qualité de service n'est pas directe. La séquence et le nombre de messages de contrôle échangés lors de la procédure de signalisation ne sont pas les mêmes. Il est donc inévitable que plusieurs messages HPMRSVP soient convertis en un seul message SM. Il revient aux entités réalisant la conversion des protocoles (MT et EGSN) de garder une trace de la séquence de messages et l'information sur l'état de la procédure. La Figure 3.8 illustre le diagramme de séquence de l'établissement d'une session de transfert avec la conversion de protocole dans le MT au niveau du MN ainsi que dans le EGSN à la frontière du réseau cœur. Dans ce diagramme, nous présentons

seulement la séquence d'échange de message, la conversion des paramètres est traitée plus loin.

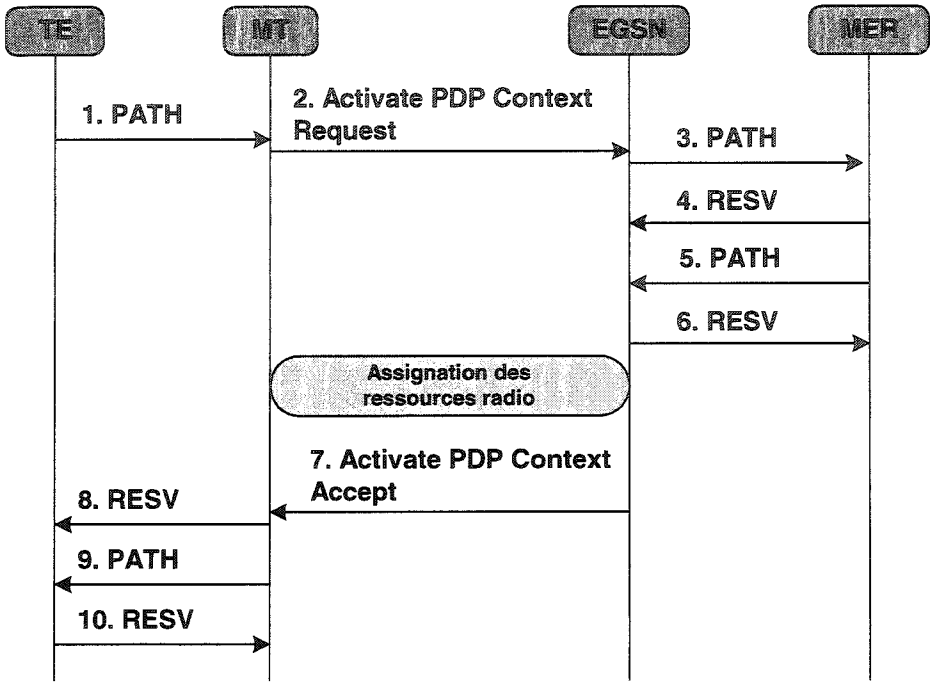

Figure 3.8 Signalisation de qualité de service avec mise en correspondance au MT et au EGSN

La procédure se déroule comme suit :

1. Le TE envoie un message PATH pour initier la réservation de ressources en amont.
2. Le MT, à la réception du message PATH, fait la conversion des paramètres de qualité de service, puis génère le message de requête d'activation de contexte PDP. Notons qu'à ce moment, le profil de qualité de service inclus dans la requête d'activation de contexte PDP ne contient que les paramètres de la session de transfert dans une direction, en amont.
3. Le EGSN, à la réception du message *Activate PDP Context Request*, reconstitue le message PATH et l'envoie vers le MER.

4. Le MER, à la réception du message PATH en provenance du EGSN, envoie un message RESV pour confirmer la réservation de ressources.
5. Le MER envoie un message PATH pour réserver les ressources en aval, au nom de l'entité avec laquelle le MN communique pour cette session (*Corresponding Node*).
6. Le EGSN, à la réception du message PATH en provenance du MER, envoie un message RESV pour confirmer la réservation de ressources. À ce moment, le EGSN détient toutes les informations sur la réservation des ressources en amont et en aval pour la session de transfert de données. Le EGSN est en mesure de réserver les ressources radio dans le UTRAN.
7. Après que les ressources radios aient été assignées, le EGSN envoie un message d'acceptation d'activation de contexte PDP vers le MT. Notons qu'à ce moment, le profil de qualité de service inclus dans le message d'acceptation contient les paramètres de la session de transfert dans les deux directions, en amont et en aval.
8. Le MT, à la réception du message *Activate PDP Context Accept*, envoie un message RESV au TE pour confirmer la réservation de ressources.
9. Le MT envoie un message PATH vers le TE pour lui indiquer la réservation de ressource en aval.
10. Le TE, à la réception du message PATH en provenance du MT, envoie un message RESV pour confirmer la réservation de ressources.

Le diagramme de séquence des messages de contrôle présenté permet de saisir comment se déroule une procédure de signalisation de qualité de service avec mise en correspondance. Cependant, afin de convertir les différents messages de contrôle entre les deux protocoles, il est nécessaire d'établir des règles de conversion pour les paramètres inclus dans ces messages. Le format des messages du protocole HPMRSVP suit le format des messages défini dans le protocole RSVP. Par exemple, un message PATH de HPMSRVP a le format suivant :

```
<Path Message> ::=  <Common Header>
                    [<INTEGRITY>]
                    <SESSION>
                    <FLOWSPEC>
                    <RSVP_HOP>
                    <TIME_VALUES>
                    [<POLICY_DATA>]
```

L'objet FLOWSPEC (en caractère gras) contient les informations de qualité de service du flux de données de la session. Les objets circonscrits par des « [ ] » sont optionnels. Les paramètres inclus dans chacun des objets ainsi que leurs formats sont décrits dans la spécification de RSVP [38].

Le format des messages du protocole de gestion de session SM est défini dans les spécifications techniques de UMTS [17]. À titre d'exemple, le message « *Activate PDP Context Request* » est présenté au Tableau 3.3. L'élément d'information caractérisant la qualité de service de la session a été mis en caractère gras. La colonne « Présence » indique si les éléments d'information contenus dans le message sont obligatoires (M) ou optionnels (O).

Tableau 3.3 Format d'un message « *Activate PDP Context Request* »

Type d'élément d'information	Présence
Protocol discriminator	M
Transaction identifier	M
Message type (Activate PDP context request)	M
Network service access point identifier	M
LLC service access point identifier	M
Quality of service	M
Packet data protocol address	M
Access point name	O
Protocol configuration options	O

Afin d'activer le contexte PDP adéquat pour le flux de données de la session, le système a besoin de convertir les paramètres de qualité de service inclus dans les

messages HPMRSVP en paramètres de qualité de service UMTS, ce qui permet de faire la réservation de ressources adéquate dans le UTRAN.

Pour définir le niveau de qualité de service désiré, HPMRSVP, comme RSVP, utilise l'objet FLOWSPEC, qui contient un TSPEC et un RSPEC. Le TSPEC définit les propriétés du flux de données de la session, tandis que le RSPEC définit le niveau de réservation requis. Ensemble, ces deux structures contiennent sept paramètres. Les spécifications techniques de RSVP [38] et IntServ [39] de l'IETF expliquent en détails le rôle de ces paramètres. Le Tableau 3.4 présente les paramètres de qualité de service utilisés dans HPMRSVP.

Tableau 3.4 Paramètres de l'objet FLOWSPEC dans HPMRSVP

Paramètres de qualité de service	
TSPEC	Token Bucket Rate
	Token bucket size
	Peak rate
	Minimum packet size
	Maximum packet size
RSPEC	Reservation Level
	Slack Term

Les paramètres qui définissent le profil de qualité de service dans UMTS sont plus nombreux. En plus de la classe de service, treize paramètres sont disponibles pour caractériser la qualité de service nécessaire pour une session. Les attributs de qualité de service, ainsi que les valeurs qu'ils peuvent prendre sont décrits en détails dans les spécifications techniques de UMTS [21]. Le Tableau 3.5 répertorie les paramètres de qualité de service de UMTS. Notons que les quatre premiers paramètres (en caractère gras) sont considérés comme les plus importants car ce sont eux qui influencent le plus la quantité de ressources à réserver dans le UTRAN (bande passante, priorité de service).

Tableau 3.5 Attributs de qualité de service UMTS

Attributs de qualité de service
Service Class
Maximum bit rate
Guaranteed bit rate
Delay
Maximum SDU (Service Data Unit)
Delivery Order
SDU format information
SDU error ratio
Residual bit error ratio
Delivery of erroneous SDU
Traffic handling priority
Allocation/Retention
Source statistic Descriptor
Signaling indication

Afin d'assurer que la réservation de ressources dans le UTRAN soit adéquate pour la session de transfert de données et qu'elle soit équivalente à la réservation de ressources dans le domaine IP, il faut établir des valeurs pour les attributs UMTS à partir de la valeur des paramètres de l'objet FLOWSPEC du message PATH. Les paramètres qui ont le même rôle dans les deux protocoles peuvent être convertis facilement. Le Tableau 3.6 présente les paramètres de qualité de service équivalents dans les deux domaines.

Tableau 3.6 Correspondance de paramètres de qualité de service

HPMRSVP		UMTS	
Token Bucket Rate	octets/sec	Guaranteed Bit Rate	kbits/sec
Peak rate	octets/sec	Maximum Bit Rate	kbits/sec
Maximum packet size	octets	Maximum SDU	octets

Comme il n'est pas possible d'associer tous les paramètres UMTS à des paramètres HPMRSVP, il faut donc leur assigner des valeurs par défaut en s'assurant que les valeurs attribuées permettent d'offrir la qualité de service adéquate pour la

session signalée. En pratique, la majorité des paramètres de qualité de service sont établis et fixés par les opérateurs [5]. Les profils de qualité de service sont préétablis pour chacun des services offerts par les opérateurs. De plus, certains paramètres dépendent de l'entente d'abonnement des utilisateurs du système et leurs appareils mobiles sont configurés par les opérateurs pour supporter un nombre limité de profil de qualité de service. Il est donc réaliste de supposer des valeurs par défaut pré-configurées pour les paramètres de qualité de service de UMTS n'ayant pas d'équivalent dans HPMRSVP. Nous portons notre attention sur deux paramètres, soit la classe de service et le délai. Ces deux paramètres sont étroitement liés, car la principale différence entre les différentes classes de service est leur sensibilité au délai. Le Tableau 3.7 présente les quatre classes de service UMTS avec leurs attributs de délai et de symétrie de trafic.

Tableau 3.7 Comparaison de classes de service UMTS

Traffic class	Conversational	Streaming	Interactive	Background
Symétrie	Symétrique	Asymétrique	Asymétrique	Asymétrique
Délai (ms)	100 – 250	250 – secondes	N/A	N/A

Or, dans notre situation, la signalisation de qualité de service avec HPMRSVP s'applique à du trafic IPv6 temps réel; on peut donc éliminer les classes de service *Interactive* et *Background*. La classe de service pourrait donc être *Conversational* ou *Streaming* et le délai entre 100 et 250 ms ou encore supérieur à 250 ms. Comme il n'y a aucune information de délai provenant des messages du protocole HPMRSVP, on ne peut se baser sur le délai pour faire la sélection. Il y a plusieurs façons de traiter ce problème. La première et la plus simple, c'est de s'en remettre aux paramètres par défaut configurés par le fournisseur de service. Deuxièmement, il serait possible de modifier les messages HPMRSVP en ajoutant un paramètre de délai dans l'objet FLOWSPEC. Le TE, en envoyant un message PATH, devrait donner une valeur de délai de transfert maximum. Cette valeur pourrait ensuite être utilisée comme attribut dans le domaine UMTS. Dans notre architecture, nous optons pour la première façon, car elle n'impose pas de modification au protocole HPMRSVP et qu'en pratique, la valeur de délai ne peut

être garantie. En effet, il est presque impossible de garantir le temps maximum que prendra un paquet pour se rendre à destination. À la sortie du réseau UMTS, le paquet peut visiter plusieurs domaines indépendants avant d'arriver dans le domaine du destinataire. Étant donné que le protocole HPMRSVP ne permet de faire la réservation de ressources qu'à l'intérieur des domaines de la source et du destinataire, on ne peut donc pas garantir le temps de transfert de bout en bout. Pour ces raisons, nous décidons qu'une classe de service et une valeur de délai par défaut seront fixées pour toutes les sessions qui proviendront d'une signalisation avec le protocole HPMRSVP.

Les paramètres de qualité de service HPMRSVP n'ont pas tous un équivalent dans le domaine UMTS, mais ils doivent tout de même être transportés à travers le UTRAN afin de pouvoir ensuite reconstituer les messages HPMRSVP. De plus, outre les paramètres qui définissent la qualité de service, les messages PATH et RESV peuvent contenir plusieurs autres objets. Le protocole HPMRSVP suit la sémantique du protocole RSVP, ce qui veut dire que les messages PATH ou RESV peuvent contenir plusieurs types d'objets. Ces objets transportent des informations d'identification de session, de sécurité, etc. Comme il n'est pas possible de trouver un équivalent dans les messages d'activation de contexte PDP, nous devons ajouter (*piggybacking*) les objets HPMRSVP aux messages de SM. Pour ce faire, nous utilisons un champ optionnel des messages d'activation de contexte PDP, le champ « *Protocol configuration options* » (voir Tableau 3.3). Cet élément d'information sert spécifiquement à transporter des options et des données provenant d'un protocole externe associé au contexte PDP, dans notre cas, HPMRSVP. Il est de longueur variable allant de 2 à 253 octets. À l'intérieur de ce champ, les informations sont encodées de façon TLV (Type - Longueur - Valeur). Nous proposons donc de transmettre les objets contenus dans les messages HPMRSVP à l'intérieur de ce champ d'information, pour qu'ils puissent être transportés à travers le UTRAN.

3.3.3 Gestion de la mobilité

Le troisième mécanisme de contrôle que nous abordons dans ce mémoire est la gestion de la mobilité. Dans un système UMTS, la gestion de la mobilité est grandement prise en charge par le réseau d'accès radio (UTRAN), mais lorsque le réseau cœur est impliqué, c'est le protocole GMM qui est utilisé. Ce protocole remplit plusieurs fonctions, mais du point de vue de la gestion de la mobilité, il permet de mettre à jour la position et les informations dans le contexte de mobilité des usagers du système. Cette mise à jour est faite périodiquement ou encore lorsqu'un nœud mobile, en se déplaçant, change de zone de couverture RA. Dans le réseau cœur, le contexte de mobilité est détenu par le SGSN qui sert le nœud mobile. Un SGSN peut desservir une ou plusieurs zones RA. Le nœud mobile est informé d'un changement de zone RA en écoutant l'information système qui est diffusée à travers tout le réseau. L'information système permet de contrôler l'opération du UTRAN. En plus d'identifier et de délimiter les différentes zones de couverture, elle informe les nœuds mobiles des paramètres essentiels aux communications radios dans le UTRAN et elle indique les services accessibles par le réseau cœur.

Dans le système évolué que nous envisageons, nous utilisons le protocole HMIPv6 dans le domaine IP, entre le TE et le MT ainsi que dans le réseau cœur. Ce protocole permet de gérer la mobilité des nœuds mobiles à l'intérieur du domaine d'un MER. La Figure 3.9 illustre la mise en correspondance des protocoles de gestion de la mobilité entre le domaine IP et le domaine UMTS.

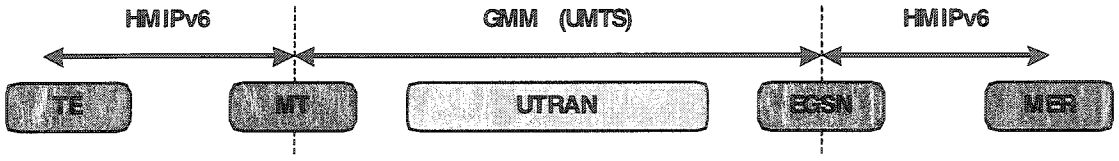

Figure 3.9 Gestion de la mobilité dans l'architecture UMTS évoluée

Mis à part les mécanismes de gestion de la mobilité à l'intérieur du UTRAN, on peut dire que les protocoles de gestion de la mobilité IP et UMTS ont un fonctionnement similaire. Le nœud mobile met à jour son état et sa position courante auprès du réseau de façon périodique ou encore lorsqu'il détecte qu'il change de zone de couverture. Dans les deux technologies, la détection des changements de zones de couverture se fait grâce aux informations diffusées par le système dans tout le réseau. Dans un système UMTS, ces zones de couverture correspondent aux zones RA, tandis qu'au niveau IP, il s'agit des sous-réseaux IP.

Afin de mettre en correspondance les protocoles HMIPv6 et GMM, nous proposons de synchroniser le fonctionnement de HMIPv6 avec la machine à états de mobilité GMM et de réutiliser la signalisation UMTS pour véhiculer les informations de mise à jour d'association d'adresse locale de HMIPv6. Nous associons un sous-réseau IP à une zone de couverture RA, ainsi nous pouvons profiter des procédures de mise à jour de zone RA (*Routing Area Update*) pour faire les mises à jour d'association d'adresse IP locale LBU (*Local Binding Update*). À chaque zone RA, un seul sous-réseau IP est associé. Dans un système UMTS conventionnel, plusieurs zones RA peuvent être sous le contrôle d'un SGSN. Mais, dans notre proposition, pour des fins de simplicité, nous limitons notre système à une seule zone RA par EGSN.

La Figure 3.10 résume la séquence d'échanges de messages lors d'une procédure de mise à jour locale d'un nœud mobile avec la conversion de protocole dans le MT au niveau du MN ainsi que dans le EGSN à la frontière du réseau cœur. Dans ce diagramme, nous présentons seulement la séquence d'échanges de messages, la conversion des paramètres est traitée plus loin. Voici la description de chacune des étapes de l'exécution de la procédure de mise à jour de l'état (position, association d'adresse, etc.) du nœud mobile auprès du réseau cœur.

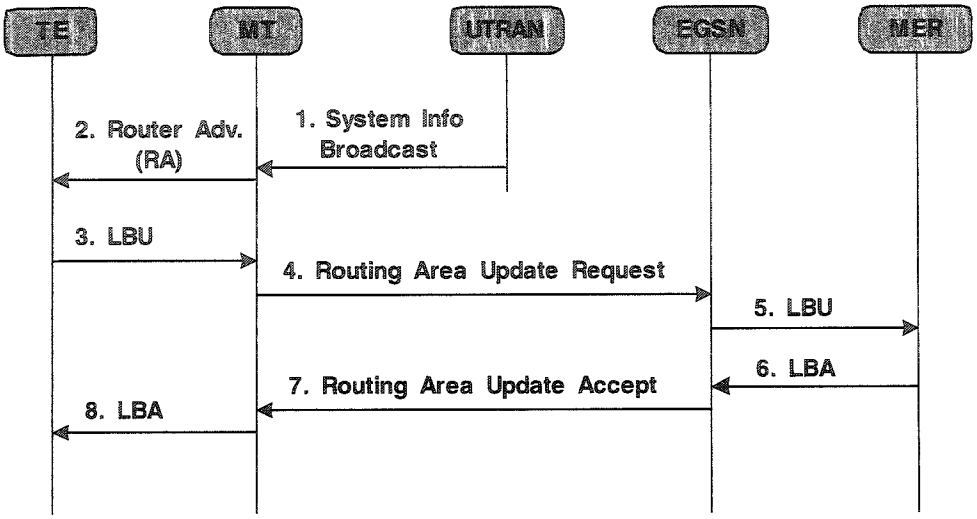

Figure 3.10 Gestion de la mobilité avec mise en correspondance au MT et au EGSN

1. Le système diffuse dans chaque cellule du réseau l'information système, qui inclut les identifiants des différentes zones de couverture.
2. Lorsqu'un changement de zone de couverture RA (sous-réseau IP) est détecté, le MT génère un message de *Router Advertisement* pour informer le TE du changement de sous-réseau.
3. Le TE, à la réception du message de *Router Advertisement*, détecte un changement de sous-réseau. Il envoie un message de mise à jour d'association d'adresse locale (*Local Binding Update*) au MER.
4. Le MT, à la réception du message LBU, fait la conversion du message pour générer le message de *Routing Area Update Request* et l'envoie au EGSN.
5. Le EGSN, à la réception du message de *Routing Area Update Request*, reconstitue le message de LBU et l'envoie vers le MER.
6. Le MER, à la réception du message LBU, fait le traitement approprié (DAD, mise à jour de la *Binding Cache*) et envoie un message d'acquittement LBA vers le EGSN.

7. Le EGSN, à la réception du message LBU, fait la conversion de message pour génèrer un message de *Routing Area Update Accept* et l'envoie vers le MT.
8. Le MT, à la réception du message de *Routing Area Update Accept*, reconstitue le message LBA et l'envoie au TE pour acquitter la mise à jour, ce qui termine la procédure.

La séquence d'échanges de messages permet de décrire le comportement des éléments du système avec la mise en correspondance de protocoles. Toutefois, la mise en correspondance requiert également la définition des règles de conversion des messages entre les deux protocoles, ce que nous allons maintenant aborder.

Nous traitons la conversion des messages en deux parties. Nous commençons par expliquer la conversion de paramètres entre les messages de mise à jour IP (*Binding Update* et *Binding Acknowledgement*) et UMTS (*Routing Area Update*). Par la suite, nous expliquons comment nous utilisons le mécanisme de diffusions d'information système du UMTS pour délivrer l'information des messages de *Router Advertisement* aux nœuds mobiles dans le UTRAN.

Dans HMIPv6, lorsqu'un MN veut mettre à jour son association d'adresse locale, il envoie un message de *Local Binding Update* (LBU). Ce message de mise à jour est envoyé au MAP (destination) et contient la nouvelle adresse locale (source) à renouveler dans l'association d'adresse. Le message contient un paramètre de numéro de séquence pour protéger contre la répétition de messages. Il contient aussi un paramètre de durée de vie (*lifetime*) de la nouvelle association d'adresse suggérée par le nœud mobile. Cette valeur peut être changée par le MAP et renvoyée dans le message d'acquittement (LBA). Les Tableaux 3.8 et 3.9 présentent le contenu des messages de demande et d'acquittement de mise à jour d'une association d'adresse locale dans HMIPv6. La description détaillée et le format des différents paramètres inclus dans ces messages sont décrits dans les spécifications de MIPv6 [25] et HMIPv6 [26].

Tableau 3.8 Message de demande de mise à jour locale

Local Binding Update (LBU)		
Source	Local Care-of address (LCoA)	
Destination	MAP address	
Parameters	Regional Care-of address (Destination option)	
	Seq. number	
	Lifetime	
	Flags	Acknowledge (A)
		Home Registration (H)
		Link-Local Address Compatibility (L)
		Key Management Mobility Capability (K)
		MAP Registration (M)

Tableau 3.9 Message d'acquittement de mise à jour locale

Local Binding Acknowledgment (LBA)		
Source	MAP address	
Destination	Local Care-of address (LCoA)	
Parameters	Status	
	Seq. number	
	Lifetime	
	Flags	Key Management Mobility Capability (K)
Type-2 Routing Header	Regional Care-of address	

Dans UMTS, les messages du protocole GMM pour mettre à jour la zone de couverture RA sont définis dans la spécification technique [17]. Ces messages contiennent beaucoup d'attributs, certains sont obligatoires (M) mais plusieurs sont optionnels (O). Nous ne décrivons pas en détail le contenu de chaque message, mais à titre d'exemple, le Tableau 3.10 présentent le nom des attributs dans le message d'acceptation de mise à jour (*Routing Area Update Accept*).

Tableau 3.10 Message d'acceptation de mise à jour de la zone RA

Routing Area Update Accept	
Type d'élément d'information	**Présence**
Protocol discriminator	M
Skip indicator	M
Message type (Routing area update accept)	M
Force to standby	M
Update result	M
Periodic RA update timer	**M**
Routing area identification	M
P-TMSI signature	O
Allocated P-TMSI	O
MS identity	O
List of Receive N-PDU Numbers	O
Negotiated READY timer value	O
GMM cause	O
T3302 value	O
Cell Notification	O
Equivalent PLMNs	O
PDP context status	O
Network feature support	O
Emergency Number List	O

Le paramètre *Periodic RA update timer* indique la période de temps avant laquelle le nœud mobile doit mettre à jour son état auprès du réseau cœur. Ce paramètre constitue le seul paramètre qui nécessite une mise en correspondance entre les deux protocoles. Dans HMIPv6, le paramètre *lifetime* est proposé par le nœud mobile mais il est confirmé par le MAP dans le message de LBA. Cette conversion se produit seulement pour les messages d'acceptation puisque ce paramètre n'existe pas dans le message de demande de mise à jour de GMM. Le Tableau 3.11 présente le paramètre à convertir avec ses unités de temps. Notons que, dans le cas de GMM, l'unité de temps peut varier.

Tableau 3.11 Correspondance de paramètres de gestion de mobilité

HMIPv6		GMM (UMTS)	
Locale Binding Acknowledge		**Routing Area Update Accept**	
Lifetime	unités de 4 sec.	Periodic RA update timer	unités de 2 sec. ou 1 min. ou déci-heures

Étant donné que la conversion de paramètre se limite à un seul paramètre, il est nécessaire d'annexer les messages de HMIPv6 avec les messages de GMM pour les transporter dans le UTRAN. Contrairement au cas de la signalisation de qualité de service (SM), il n'existe pas d'attribut dans les messages du protocole GMM pour transporter des paramètres d'un protocole externe. Il est donc nécessaire d'en ajouter un pour transporter le contenu du message LBU et LBA avec le message de *Routing Area Update Request et Routing Area Update Accept*. Ce paramètre est du type TLV (type - longueur - valeur), il contient le message de LBA entier comme « valeur ». Il est simplement ajouté à la liste des paramètres optionnels des messages de mise à jour de la zone RA. La spécification technique du protocole RRC [37] contient tous les détails sur la structure des éléments de l'information système.

Précisons que la mise en correspondance que nous définissons dans cette section s'applique à la mise à jour de l'association de l'adresse locale (LBU) auprès du MER, que nous annexons à la mise à jour de la zone de couverture RA. En ce qui concerne l'association d'adresse auprès du HA et des nœuds correspondants, qui inclut la procédure de retour de routabilité (*Return Routability*), nous ne réutilisons pas la signalisation UMTS.

En effet, dans ce mémoire nous abordons la gestion de la mobilité à l'intérieur du réseau cœur UMTS, ce qui s'applique à la mise à jour locale à l'intérieur du domaine du MER, et non pas à la mise à jour auprès du HA et des nœuds correspondants, dont le nombre est variable. Aussi, il serait difficile d'établir des règles de correspondance adéquates avec les procédures UMTS, car en plus d'être variables en nombre, les

enregistrements auprès du HA et des CN sont caractérisés par une séquence d'échange de messages bien différente de la signalisation UMTS.

De plus, nous croyons qu'il n'est pas nécessaire de faire une mise en correspondance pour les enregistrements auprès du HA et des nœuds correspondants car ils font partie d'une phase de signalisation préliminaire à l'établissement d'une session de communication avec le nœud mobile. Cette phase préliminaire inclut les communications nécessaires pour établir des associations de sécurité (entre MN et HA, ou MN et MAP), afin d'utiliser IPSEC pour protéger les mises à jour d'association d'adresse. Elle inclut aussi l'exécution de la procédure de retour de routabilité, afin de permettre le mode de communication optimisé de IPv6 Mobile. Et c'est aussi durant cette phase que le nœud mobile va initier la session de communication avec un ou des correspondants. L'initiation d'une session est la négociation des caractéristiques d'une session entre deux (ou plus) interlocuteurs, avant que cette session soit établie. Par exemple, avant l'établissement d'une session de transfert d'une vidéoconférence, les partis doivent se mettre d'accord sur le type de transmission, le codec à utiliser, le débit du flux de données, le délai maximum, etc. Un protocole comme comme SIP (*Session Initiation Protocol*) peut être utilisé pour accomplir cette étape. Cette phase de signalisation préliminaire nécessite un grand nombre (variable avec le nombre de correspondants) d'échanges de messages de contrôle entre le MN et plusieurs autres éléments. Il est donc préférable d'établir une session de transfert de données (contexte PDP) spécifiquement pour l'échange de tous ces messages préliminaires avant d'établir la session de transfert pour la communication en tant que tel.

Ainsi, l'utilisation de la mise en correspondance de protocoles dans la gestion de la mobilité est une optimisation, qui sert dans une situation de relève locale (changement de zone de couverture), lorsqu'un nœud mobile change de point d'attache (Routeur d'accès). Cette optimisation permet d'éviter le délai associé à l'activation d'un contexte PDP pour envoyer le message de mise à jour d'association d'adresse (LBU).

En plus des mises à jour périodiques, suite à l'expiration d'un compteur, le nœud mobile doit mettre à jour son état auprès du réseau cœur lorsqu'il détecte un changement

de sous-réseau (zone de couverture RA). Dans HMIPv6, les messages de *Router Advertisement* servent à détecter ces changements. Ces messages font partie du protocole de *Neighbor Discovery* de IPv6 [41]. Ce protocole permet de trouver des routeurs et de découvrir la présence d'autres nœuds sur un lien. Les messages de *Router Advertisement* indiquent aux nœuds sur un lien les diverses informations de configuration nécessaires aux communications IPv6. Ces messages contiennent entre autres le ou les préfixes de sous-réseau du lien sur lequel ils sont diffusés et, dans un environnement HMIPv6, l'option de MAP indique l'adresse du MAP qui dessert le domaine. Ces informations permettent au nœuds mobiles de configurer (*Stateless Address Autoconfiguration*) leur adresse locale (LCoA) ainsi que leur adresse régionale (RCoA). Le Tableau 3.12 illustre le contenu de ce type de messages. Le contenu et le format des informations dans ces messages sont décrits en détail dans les spécifications de *Neighbor Discovery* [41], MIPv6 [25] et HMIPv6 [26].

Tableau 3.12 Message de *Router Advertisement* dans HMIPv6

<table>
<tr><th colspan="5">Router Advertisement</th></tr>
<tr><td>Source</td><td colspan="4">On-link Router address</td></tr>
<tr><td>Destination</td><td colspan="4">All-nodes multicast address (FF02::1)</td></tr>
<tr><td rowspan="4">Parameters</td><td rowspan="2">Flags</td><td colspan="3">M</td></tr>
<tr><td colspan="3">O</td></tr>
<tr><td colspan="4">Router lifetime</td></tr>
<tr><td colspan="4">Reachable time</td></tr>
<tr><td rowspan="8">Options</td><td colspan="4">Retrans timer</td></tr>
<tr><td rowspan="5">Prefix Information option</td><td rowspan="3">Flags</td><td>On-link (L)</td></tr>
<tr><td>Autonomous (A)</td></tr>
<tr><td>Router address (R)</td></tr>
<tr><td colspan="2">Valid lifetime</td></tr>
<tr><td colspan="2">Preferred lifetime</td></tr>
<tr><td colspan="2">Prefix</td></tr>
<tr><td rowspan="5">MAP option</td><td colspan="2">Distance</td></tr>
<tr><td colspan="2">Pref.</td></tr>
<tr><td colspan="2">R Flag</td></tr>
<tr><td colspan="2">Valid lifetime</td></tr>
<tr><td colspan="2">MAP Global Address</td></tr>
</table>

Normalement, dans un domaine IPv6, ce message est « multicasté » à intervalles de temps réguliers (configurable) par le routeur d'accès pour informer les nœuds sur son lien. Cependant, comme nous voulons éviter d'activer un contexte PDP, pour envoyer ces messages comme n'importe quel paquet de donnés, nous proposons de réutiliser les mécanismes de diffusion d'information de UMTS.

Le *System Information Broadcast* de UMTS est diffusé, sur un canal radio dédié, dans toutes les cellules du réseau. L'information système est divisée en plusieurs blocs d'information qui regroupent des éléments d'information de même nature, appelé *System Information Block* (SIB). Ces blocs d'information sont organisés selon le *Master Information Block* (MIB) qui contient des références vers les différents SIB. La spécification technique du protocole RRC de UMTS [37] définit comment se fait la diffusion de l'information système. La spécification décrit 17 types de blocs, leur contenu ainsi que leur utilité. Chaque bloc d'information a un contenu et un rôle différent. Par exemple, le SIB 1 contient des informations sur les temporisateurs (*timer*) et les compteurs utilisés par les nœuds mobiles dans les communications avec le réseau. Les SIB 2 et 3 contiennent les informations qui servent à la gestion de la mobilité à l'intérieur du UTRAN. La Figure 3.11 illustre la relation entre le MIB et les SIB.

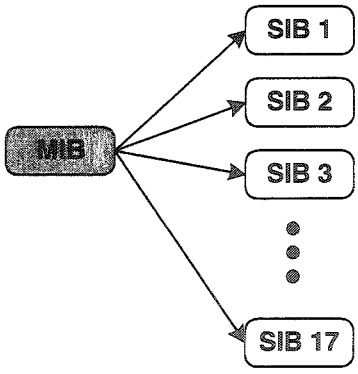

Figure 3.11 Structure (simplifiée) des blocs d'information système

Comme nous voulons réutiliser ce mécanisme de diffusion, nous proposons de définir un nouveau type de bloc d'information, dédié à la distribution de l'information

utile à la gestion de la mobilité IPv6. Ce nouveau bloc d'information (SIB 18) est ajouté aux autres SIB et le MIB doit contenir une référence vers ce nouveau bloc. Son contenu est simplement le message de *Router Advertisement* décrit plus haut. Un MT supportant la fonctionnalité de HMIPv6 pourrait extraire l'information de ce bloc et générer le message de *Router Advertisement* pour l'envoyer au TE. Grâce à cette intégration, il n'est pas nécessaire d'activer un contexte PDP avec chacun des nœuds mobiles dans le réseau, uniquement pour l'envoi des messages de *Router Advertisement.*

Ceci complète la mise en correspondance pour l'aspect de la gestion de la mobilité dans l'architecture évoluée que nous proposons. Ainsi, dans ce chapitre, nous avons présenté une architecture évoluée pour les systèmes UMTS, qui utilisent des mécanismes de contrôle basés IPv6. De plus, nous avons expliqué une conversion de protocole de contrôle qui permet de réutiliser la signalisation UMTS à l'intérieur du UTRAN, afin d'éliminer la redondance de mécanismes de contrôle et permettre une meilleure utilisation des ressources. Nous croyons qu'une telle architecture facilitera l'intégration avec d'autres technologies d'accès dans le contexte des réseaux mobiles multi-accès de prochaine génération.

CHAPITRE 4

ÉVALUATION DE PERFORMANCE

Dans le chapitre précédent, nous avons présenté notre proposition d'évolution pour les systèmes UMTS qui intègre des mécanismes de contrôle basés sur IP. Nous avons décrit les caractéristiques ainsi que l'architecture du système. Ensuite, nous avons présenté l'intégration des protocoles de contrôle IP dans cette architecture. Cette intégration comporte la mise en correspondance des protocoles de contrôle entre le domaine IP et le domaine UMTS, ce qui permet la réutilisation de la signalisation UMTS dans le UTRAN. Dans ce quatrième chapitre, nous évaluons notre proposition d'évolution dans le contexte d'un système multi-accès. Cependant, comme nous l'expliquons plus loin, cette évaluation s'attarde seulement à l'aspect de la gestion de la mobilité. Nous comparons l'utilisation d'un système UMTS évolué avec l'utilisation d'un système UMTS conventionnel, dans une situation de relève inter-technologique avec la technologie WLAN.

4.1 Méthode d'évaluation

Dans ce mémoire, nous traitons de trois mécanismes de contrôle : l'authentification, la signalisation de qualité de service, et la gestion de la mobilité. Il est cependant difficile de faire une évaluation sur les trois aspects de notre proposition, soit pour des raisons d'ordre technique ou encore parce qu'il n'est pas possible de mesurer de façon quantitative l'amélioration que notre proposition apporte. De plus, nous croyons qu'une évaluation complète de tous les aspects de notre proposition constitue une tâche d'envergure exagérée pour le cadre de ce mémoire.

Pour l'authentification, nous proposons de remplacer les protocoles définis par 3GPP par des protocoles basés sur IP définis par l'IETF. Dans un contexte multi-accès, cette approche facilite l'intégration de la technologie UMTS avec les autres technologies d'accès. En utilisant des protocoles IP comme base commune pour l'authentification, il devient possible d'utiliser le même mécanisme d'authentification avec plusieurs types d'accès. Ainsi, l'appréciation d'utilisation de protocole IP pour l'authentification est plutôt qualitative.

Pour la signalisation de qualité de service, nous proposons d'utiliser HPMRSVP dans le réseau cœur, plutôt que le protocole SM défini par 3GPP. Le protocole SM sert à initialiser le tunnel GTP qui encapsule les données de la session jusqu'au GGSN. Il serait intéressant d'évaluer la performance de notre proposition et de la comparer à un système UMTS conventionnel pour du trafic temps réel. Or, HPMRSVP est en cours de développement, il n'y a donc pas encore d'implémentation disponible. Il n'y a pas non plus de simulateur qui nous permettrait de simuler l'utilisation de HPMRSVP avec un système UMTS. Il est donc techniquement difficile d'évaluer cet aspect de la proposition.

Dans ce chapitre, nous évaluons l'aspect de la gestion de la mobilité inter-technologique qui utilise le système UMTS évolué que nous proposons. L'utilisation d'un simulateur s'est avéré impossible pour faire cette évaluation, car aucun simulateur disponible ne permet de simuler tous les protocoles de gestion de mobilité dont nous avons besoin : MIPv6, HMIPv6 et GMM (UMTS). Nous avons plutôt opté pour une évaluation de performance à l'aide d'un modèle analytique du système. En effet, grâce à une étude du coût d'une mise à jour de l'association d'adresse locale auprès du MER, nous pouvons comparer la performance de notre proposition à celle d'un système UMTS conventionnel.

4.2 Gestion de la mobilité inter-technologique

Dans le système multi-accès que nous considérons, la gestion de la mobilité inter-technologique se fait au niveau IP, avec le protocole HMIPv6. Une relève verticale se fait lors d'un changement de routeur d'accès (sous-réseau IP) à l'intérieur du domaine d'un MAP. Chaque relève, ou changement de sous-réseau, engendre une mise à jour de l'association d'adresse locale auprès du MER (MAP).

Nous voulons étudier comment notre proposition d'architecture ainsi que la mise en correspondance de protocoles de contrôle améliore le délai de la relève dans un contexte multi-accès. La Figure 4.1 illustre les deux situations que nous voulons comparer, c'est-à-dire la relève inter-technologique entre un réseau WLAN et UMTS, qui utilise un système UMTS conventionnel ou un système UMTS évolué. À gauche, on présente l'architecture évoluée et à droite l'architecture conventionnelle.

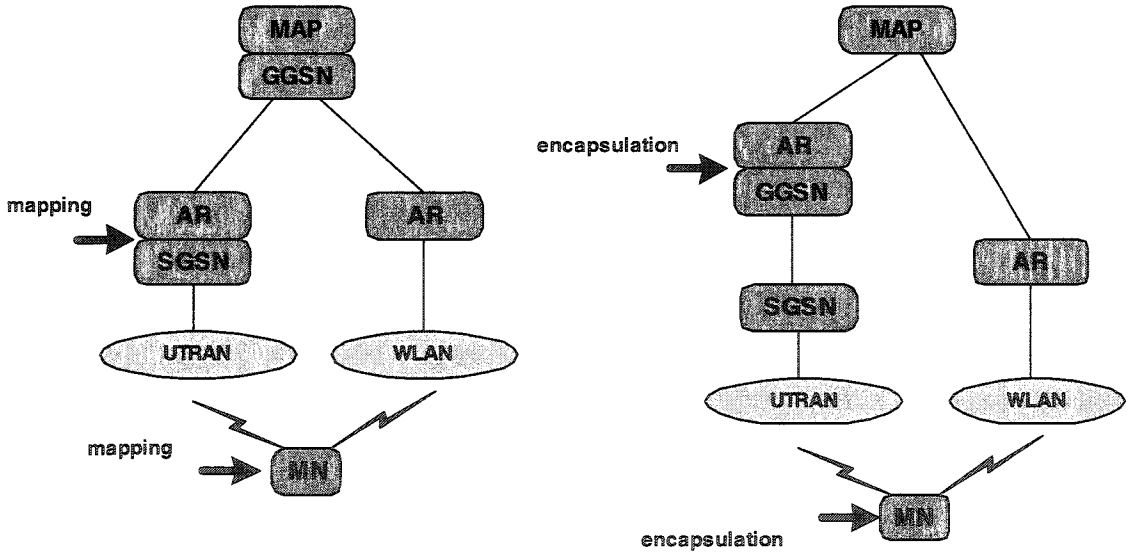

Figure 4.1 Architecture pour une relève inter-technologique UMTS - WLAN

Le système UMTS évolué défini au chapitre précédent comprend deux améliorations par rapport à l'architecture conventionnelle. Premièrement, nous intégrons l'architecture HMIPv6 à l'intérieur du réseau cœur, ce qui enlève un niveau hiérarchique

dans le réseau en plus d'enlever l'encapsulation GTP. Deuxièmement, nous utilisons la mise en correspondance de protocoles de contrôle afin de réutiliser la signalisation UMTS dans le UTRAN, ce qui évite le dédoublement de message de contrôle. Dans le but d'étudier l'impact de chacune de ces améliorations sur le système, nous définissons les trois scénarios présentés au Tableau 4.1.

Tableau 4.1 Scénarios d'utilisation du système UMTS

Scénarios	Description
Scénario 1	Une architecture UMTS conventionnelle.
Scénario 2	Une architecture UMTS évoluée, c'est-à-dire qui intègre HMIPv6 (SANS mise en correspondance de protocoles de contrôle).
Scénario 3	Une architecture UMTS évoluée, c'est-à-dire qui intègre HMIPv6 (AVEC mise en correspondance de protocoles de contrôle).

Selon le scénario considéré, la mise à jour auprès du MER ne se fera pas de la même façon. Afin de les étudier, nous présentons la procédure de mise à jour dans un système UMTS pour chacun des scénarios identifiés, ainsi que la procédure de mise à jour dans un système WLAN.

4.2.1 Procédure de mise à jour dans le scénario 1

Dans le premier scénario, c'est une architecture conventionnelle qui est utilisée. La procédure de mise à jour de l'association d'adresse locale auprès du MAP se fait comme l'illustre la Figure 4.2. Ce scénario suit la procédure définie par 3GPP pour utiliser MIPv6. En effet, le nœud mobile doit activer un contexte PDP pour envoyer tous les messages de signalisation, encapsulés dans un tunnel GTP jusqu'au GGSN qui agit comme routeur d'accès.

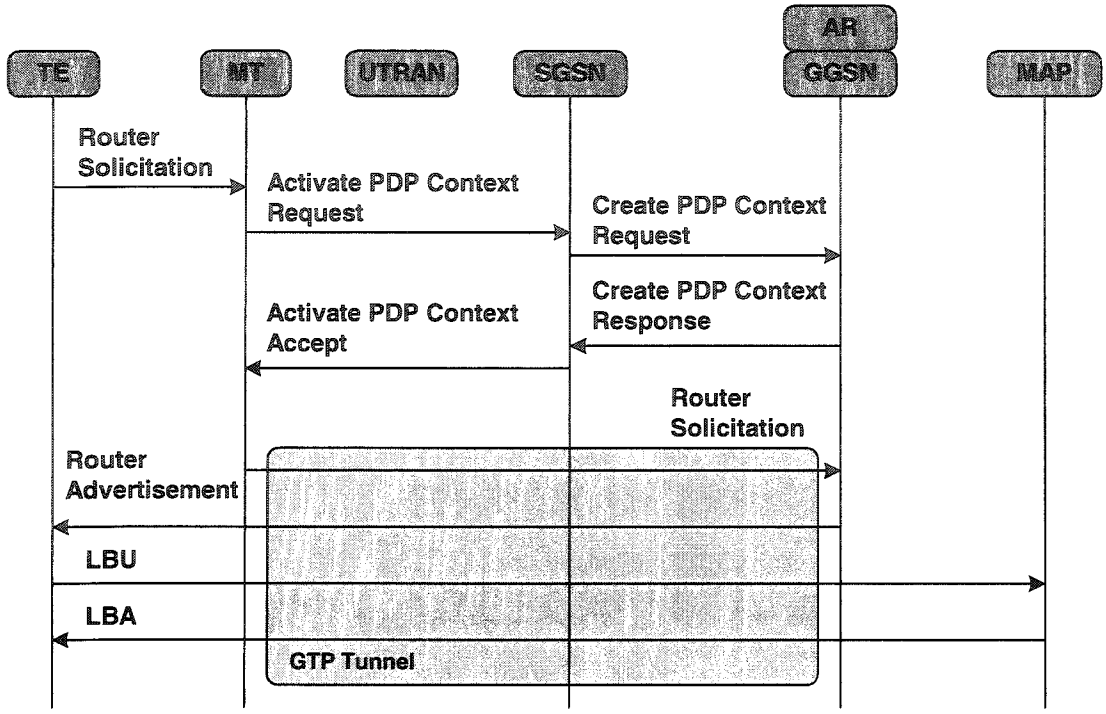

Figure 4.2 Mise à jour dans une architecture UMTS conventionnelle

La procédure de mise à jour s'exécute comme suit :

1. Le TE initie la procédure en envoyant un message de *Router Solicitation*. Au MT, ce message déclenche l'activation d'un contexte PDP.
2. Une fois le tunnel GTP établi, le message de *Router Solicitation* est acheminé au routeur d'accès (GGSN).
3. Le routeur d'accès répond par un message de *Router Advertisement*. Ce message contient les informations de préfixe réseau nécessaires au MN pour la configuration d'une nouvelle adresse locale.
4. Une fois sa nouvelle adresse locale configurée, le TE envoie un message de mise à jour (LBU) au MER. Ce message est acheminé dans le tunnel GTP jusqu'au GGSN, puis normalement sur le réseau IP externe jusqu'au MER.

5. Le message d'acquittement (LBA) est envoyé du MER au nœud mobile. Une fois ce message reçu, le MN peut utiliser la nouvelle adresse locale et la relève inter-technologique est terminée.

L'approche UMTS conventionnelle offre l'avantage de permettre au nœud mobile de se déplacer dans toute la zone de couverture UMTS en restant dans le même sous-réseau IP. Le MN n'a donc plus besoin de faire de mise à jour auprès du MER sauf s'il change de technologie d'accès.

4.2.2 Procédure de mise à jour dans le scénario 2

Dans le deuxième scénario, nous utilisons l'architecture évoluée présentée au chapitre précédent, sans faire de mise en correspondance de protocole de contrôle. L'architecture de HMIPv6 est intégrée au réseau cœur UMTS. Le SGSN devient un routeur d'accès (EGSN) et on associe un sous-réseau IP à chaque *Routing Area*. Le MAP est intégré au GGSN (MER). Comme la mise en correspondance n'est pas utilisée, l'activation d'un contexte PDP est nécessaire pour acheminer les messages de signalisation à travers un tunnel GTP. Cependant, le tunnel s'arrête au SGSN, les messages sont ensuite acheminés normalement sur le réseau IP jusqu'au MER. La Figure 4.3 illustre la procédure de mise à jour auprès du MER dans le scénario 2.

La procédure de mise à jour se déroule comme suit :

1. Le TE initie la procédure en envoyant un message de *Router Solicitation*. Au MT, ce message déclenche l'activation d'un contexte PDP.
2. Une fois le tunnel GTP établi, le message de *Router Solicitation* est acheminé au routeur d'accès (SGSN).
3. Le routeur d'accès répond par un message de *Router Advertisement*. Ce message contient les informations de préfixe réseau nécessaires au MN pour la configuration d'une nouvelle adresse locale.

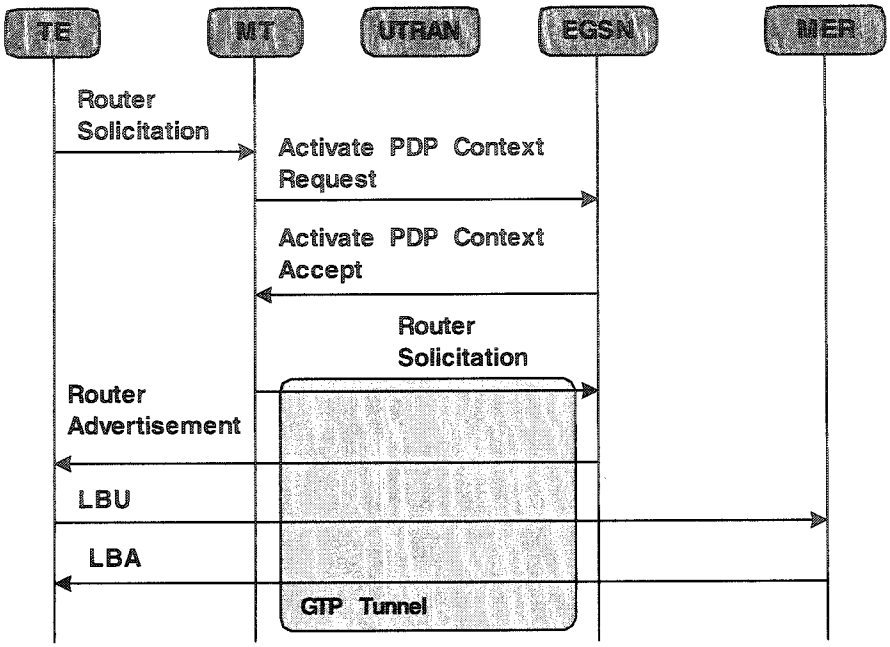

Figure 4.3 Mise à jour dans une architecture évoluée (sans mise en correspondance)

4. Une fois sa nouvelle adresse locale configurée, le TE envoie un message de mise à jour (LBU) auprès du MER. Ce message est acheminé dans le tunnel GTP jusqu'au SGSN, puis normalement sur le réseau cœur IP jusqu'au MER.
5. Le message d'acquittement (LBA) est envoyé du MER au nœud mobile. Une fois ce message reçu, le MN peut utiliser la nouvelle adresse locale et la relève est terminée.

4.2.3 Procédure de mise à jour dans le scénario 3

Dans le troisième scénario, nous utilisons l'architecture évoluée comme dans le scénario 2, sauf que la mise en correspondance de protocoles de contrôle est mise à profit. Il n'est plus nécessaire d'activer un contexte PDP pour acheminer les messages de signalisation à travers un tunnel GTP. À la place, les messages de signalisation UMTS sont utilisés pour acheminer les messages de contrôle IP à travers le UTRAN. De plus, le mécanisme de diffusion de l'information système (*System Information*

Broadcast) de UMTS est utilisé pour transmettre les informations de préfixe de sous-réseau IP. Le message de *Router Advertisement* peut donc être généré par le MT, ce qui évite d'envoyer le message de *Router Solicitation* jusqu'au EGSN. La Figure 4.4 illustre la procédure de mise à jour auprès du MER dans le scénario 3.

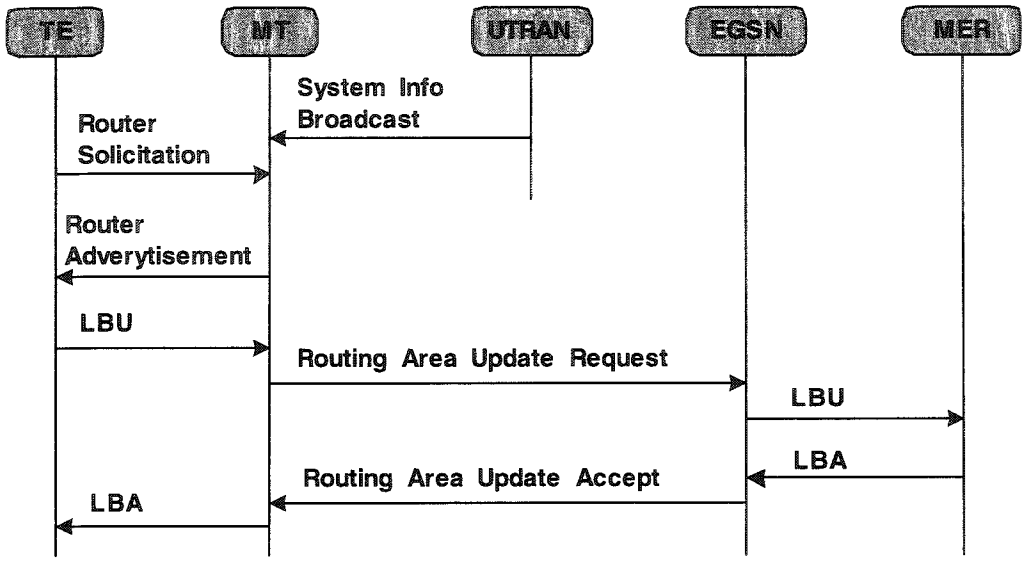

Figure 4.4 Mise à jour dans une architecture évoluée (avec mise en correspondance)

Cette procédure de mise à jour est expliquée en détails dans le troisième chapitre. Toutefois, nous la résumons ici:

1. Le TE initie la procédure en envoyant un message de *Router Solicitation.*
2. En réponse à ce message, le MT génère un message de *Router Advertisement* à partir des informations reçues dans le *System Information Broadcast.*
3. Une fois sa nouvelle adresse locale configurée, le TE envoie un message de mise à jour (LBU). Ce message est acheminé au EGSN en utilisant le message de *Routing Area Update Request*, puis normalement sur le réseau cœur IP jusqu'au MER.

5. Le message d'acquittement (LBA) est envoyé du MER au nœud mobile. Une fois ce message reçu, le MN peut utiliser la nouvelle adresse locale et la relève est terminée.

4.2.4 Procédure de mise à jour dans un WLAN

Nous décrivons maintenant la procédure de mise à jour auprès du MER, lorsque le nœud mobile change de sous-réseau WLAN ou encore lorsqu'il arrive dans une zone de type WLAN et qu'il décide de quitter le système UMTS. Dans un WLAN, les messages de *Router Advertisement* sont diffusés à intervalles de temps réguliers. Le nœud mobile n'a pas besoin de les solliciter.

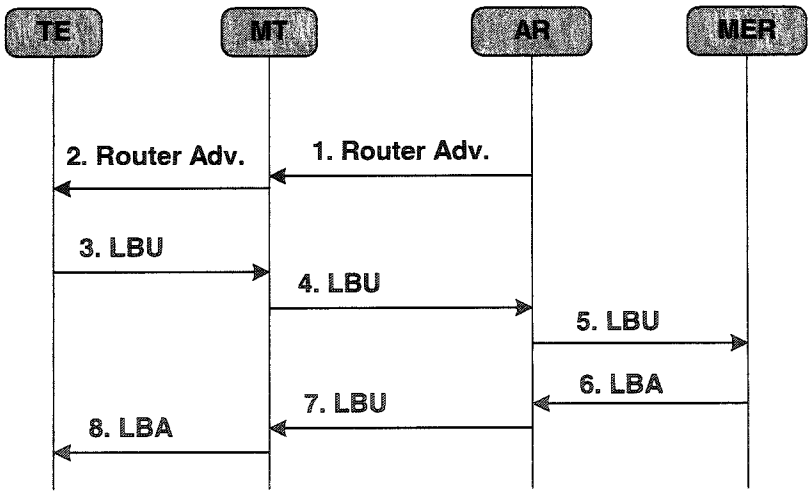

Figure 4.5 Mise à jour dans un WLAN

La procédure de mise à jour se déroule comme suit :

1. À la réception d'un message de *Router Advertisement*, le nœud mobile se configure une nouvelle adresse locale.
2. Une fois sa nouvelle adresse locale configurée, le TE envoie un message de mise à jour (LBU). Ce message est acheminé jusqu'au routeur d'accès sur l'interface radio WLAN par le MT (de type WLAN).

3. Le LBU est ensuite acheminé normalement sur le réseau cœur IP jusqu'au MER.
5. Le message d'acquittement (LBA) est envoyé du MER au nœud mobile. Une fois ce message reçu, le MN peut utiliser la nouvelle adresse locale et la relève est terminée.

4.3 Modèle analytique

Lorsqu'un nœud mobile change de sous-réseau IP, il doit se configurer une nouvelle adresse locale et mettre à jour son association d'adresse auprès du MER. Le délai de la relève est le temps qui s'écoule entre le moment où le nœud mobile initie la relève et le moment où le nœud mobile peut utiliser sa nouvelle adresse locale dans le nouveau sous-réseau, c'est-à-dire lorsqu'il reçoit le message d'acquittement (LBA).

Notre modèle analytique permet de mesurer le coût, en délai, d'une mise à jour de l'association d'adresse locale auprès du MER. En se basant sur les procédures de mise à jour présentées dans la section précédente, nous pouvons déterminer le coût en délai d'une opération de mise à jour pour chacun des scénarios que nous avons identifiés. Dans notre modélisation, nous utilisons les variables suivantes :

U_S : Coût d'une mise à jour dans une architecture UMTS standard;

U_E : Coût d'une mise à jour dans une architecture UMTS évoluée (sans mise en correspondance);

U_{EM} : Coût d'une mise à jour dans une architecture UMTS évoluée (avec mise en correspondance);

U_W : Coût d'une mise à jour dans un réseau WLAN;

L_U : Coût de transmission d'un message de signalisation UMTS à travers le UTRAN (GMM ou SM);

L_{CN} : Coût de transmission d'un message de signalisation UMTS à travers le réseau cœur (GTP-C);

D_U : Coût de transmission d'un paquet IP dans un contexte PDP à travers le UTRAN;

D_{CN} : Coût de transmission d'un paquet IP dans un contexte PDP à travers le réseau cœur;

D_{IP} : Coût de transmission d'un paquet IP dans un réseau IP (réseau cœur ou autre);

D_M : Coût de transmission d'un paquet IP entre le TE et le MT;

D_W : Coût de transmission d'un paquet IP dans le réseau d'accès WLAN;

E : Coût d'encapsulation ou de désencapsulation des données dans un tunnel GTP;

C : Coût de la conversion d'un message de contrôle d'un protocole à un autre.

4.3.1 Fonctions de coût

Voici donc les fonctions de coût pour les scénarios identifiés plus haut.

Coût d'une mise à jour auprès du MER dans une architecture UMTS conventionnelle :

$$U_S = 4D_M + 2(L_U + L_{CN}) + 4(D_U + D_{CN}) + 2D_{IP} + 8E \quad (4.1)$$

Coût d'une mise à jour auprès du MER dans une architecture UMTS évoluée, c'est-à-dire qui intègre HMIPv6 (SANS mise en correspondance de protocoles de contrôle) :

$$U_E = 4D_M + 2L_U + 4D_U + 2D_{IP} + 8E \quad (4.2)$$

Coût d'une mise à jour auprès du MER dans une architecture UMTS évoluée, c'est-à-dire qui intègre HMIPv6 (AVEC mise en correspondance de protocoles de contrôle) :

$$U_{EM} = 4D_M + 2L_U + 2D_{IP} + 5C \quad (4.3)$$

Coût d'une mise à jour auprès du MER dans une zone de type WLAN :

$$U_W = 2D_W + 2D_{IP} \quad (4.4)$$

4.3.2 Modèle de mobilité

Dans cette analyse, nous nous intéressons au changement de zone de couverture qui engendre une mise à jour de l'association d'adresse locale au niveau du MER. Nous admettons que l'accès de type WLAN est prioritaire, c'est-à-dire que dès qu'un nœud mobile arrive dans ce type de zone, il s'y connecte. Lors d'un changement de zone de couverture, un nœud mobile peut arriver dans une zone du type UMTS ou WLAN. S'il s'agit d'un nouveau WLAN, il y a forcément un changement de routeur d'accès, le nœud mobile doit mettre à jour son association d'adresse auprès du MER. S'il s'agit d'une zone UMTS, il y a plusieurs possibilités. Si le nœud mobile provient d'une zone WLAN, alors il doit y avoir une mise à jour de l'association d'adresse. Si le nœud mobile était déjà dans une zone UMTS avant le déplacement, deux cas sont possibles. Dans l'architecture conventionnelle, il n'y a pas de mise à jour à faire. Dans l'architecture évoluée, si les deux zones de couverture appartiennent à des zones RA différentes, il y doit y avoir une mise à jour auprès du MER.

La Figure 4.6 présente un exemple d'un réseau multi-accès où plusieurs zones WLAN sont réparties aléatoirement à l'intérieur de la zone de couverture réseau UMTS, divisée en plusieurs zones RA. Dans cet exemple, le réseau UMTS est constitué de quatre zones de couverture RA, tandis que huit sous-réseaux WLAN sont présents. De plus, chaque zone WLAN a une couverture équivalente à environ un seizième (1/16) de la zone de couverture RA. En supposant que les utilisateurs sont uniformément répartis, la probabilité qu'un utilisateur soit dans une zone de type WLAN est donc 2/16, et dans la zone UMTS, de 14/16.

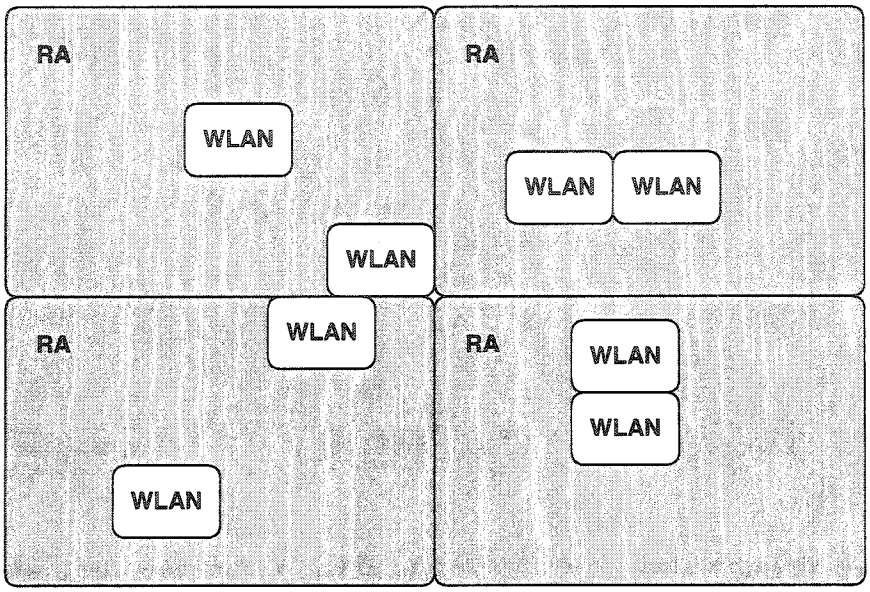

Figure 4.6 Exemple d'un réseau multi-accès constitué de zones UMTS (RA) et WLAN

Les utilisateurs se déplacent à vitesse constante dans toutes les directions de façon équiprobable. Un déplacement unitaire consiste en un déplacement égal à la zone de couverture d'un WLAN. Les zones de WLAN sont réparties aléatoirement dans toute la zone de couverture globale du réseau UMTS. La Figure 4.7 illustre une zone RA divisée en plusieurs zones de déplacement unitaires, une de ces zones est un WLAN. Nous supposons que tous les côtés des zones RA ont le même nombre de zones de couvertures unitaires.

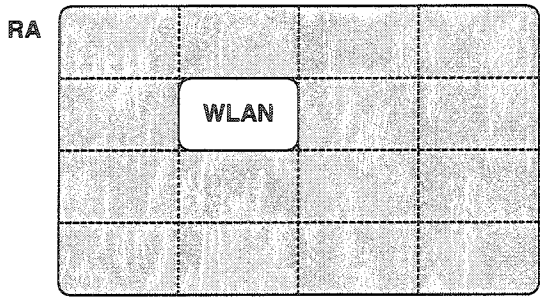

Figure 4.7 Zones de déplacement unitaires dans une zone de couverture RA

Les Figures 4.6 et 4.7 représentent des cas particuliers, mais le nombre de zones RA, la grandeur des zones RA, c'est-à-dire le nombre de zones unitaires qu'elles contiennent, ainsi que le nombre de zones de WLAN présentes dans un système constituent des caractéristiques topologiques et géographiques de ce système. Nous voulons évaluer la performance de notre proposition par rapport à une approche classique en faisant varier ces caractéristiques.

Étant donné que nous n'avons pas de données géographiques, il est difficile d'évaluer les probabilités de déplacement entre les différents types de zones de couverture. Nous faisons donc l'hypothèse que le type de la zone de couverture, après un déplacement, est indépendant du type de la zone avant ce déplacement. Ainsi, si on suppose que la probabilité d'un déplacement vers une zone d'un type particulier (événement A) est indépendante du type de la zone d'où provient le MN (événement B), alors la probabilité qu'un MN se déplace vers une zone d'un type est égale à la probabilité d'être dans cette zone. Sachant que les événements A et B sont indépendants, on peut écrire:

$$P(A \mid B) = \frac{P(AB)}{P(B)} = \frac{P(A)P(B)}{P(B)} = P(A) \tag{4.5}$$

À chaque déplacement, un utilisateur peut arriver dans une zone WLAN ou UMTS. La probabilité d'arriver dans une zone unitaire du type WLAN est égale à la proportion du nombre de zones WLAN par rapport au nombre de zones de couverture unitaire totale.

À partir de cette hypothèse, on peut déterminer la probabilité qu'un changement se fasse vers chacun des types de zone de couverture. Nous utilisons les paramètres suivants :

P_{WLAN} : probabilité d'une mise à jour dans une zone de type WLAN;

P_{UMTS} : probabilité d'une mise à jour dans une zone de type UMTS;

Z_S : type de la zone de couverture unitaire suivante;

Z_C : type de la zone de couverture unitaire courante;

W : type de zone WLAN;

U : type de zone UMTS;

P_W : probabilité d'être dans une zone de type WLAN;

P_U : probabilité d'être dans une zone de type UMTS;

P_{INTER} : probabilité d'un mouvement inter-zone de couverture RA;

x : longueur d'un côté d'une zone de couverture RA.

En tenant compte de l'hypothèse formulée plus haut, la probabilité qu'une mise à jour se fasse dans une zone de type WLAN, lors d'un déplacement unitaire, est:

$$\begin{aligned} P_{WLAN} &= P(Z_S = W \mid Z_C = W) \cap P(Z_C = W) \; + \; P(Z_S = W \mid Z_C = U) \cap P(Z_C = U) \\ &= P_W \cap P_W \quad + \quad P_W \cap P_U \\ &= P_W P_W \quad + \quad P_W P_U \end{aligned} \tag{4.6}$$

La probabilité qu'une mise à jour se fasse dans une zone de type UMTS dépend de l'architecture UMTS qui est utilisée. Dans le cas de l'architecture conventionnelle, une mise à jour est nécessaire seulement lorsqu'un nœud mobile passe d'une zone WLAN à une zone UMTS. Aucune mise à jour n'est nécessaire pour tout déplacement entre deux zones UMTS. Ainsi, cette probabilité peut être exprimée comme suit :

$$\begin{aligned} P_{UMTS} &= P(Z_S = U \mid Z_C = W) \cap P_W \\ &= P_U \cap P_W \\ &= P_U P_W \end{aligned} \tag{4.7}$$

Dans le cas de l'architecture évoluée que nous proposons, la mise à jour auprès du MER doit se faire lorsqu'un utilisateur passe d'une zone WLAN à une zone UMTS, mais aussi lors d'un déplacement d'une zone UMTS à une autre, si ces zones unitaires font partie de deux zones RA différentes (U_i et U_j) :

$$P_{UMTS} = P(Z_S = U \mid Z_C = W) \cap P(Z_C = W) + P(Z_S = U_j \mid Z_C = U_i) \cap P(Z_C = U) \tag{4.8}$$

Pour qu'il y ait changement de zones RA lors d'un mouvement, il faut que le nœud mobile soit dans une zone unitaire en bordure d'une zone RA. Ainsi, la probabilité qu'un nœud mobile se déplace dans une autre zone RA est égale à la probabilité que le nœud mobile soit en bordure de la zone RA, multiplié par la probabilité de faire un déplacement vers une zone unitaire dans une autre zone RA. Cette probabilité dépend de la grandeur de la zone RA. En considérant des zones RA avec des côtés de longueur « x », nous pouvons formuler la probabilité d'un mouvement inter zone RA :

$$\begin{aligned} P_{INTER} &= \frac{4(x-2)}{x^2} \times \frac{1}{4} + \frac{4}{x^2} \times \frac{2}{4} \\ &= \frac{(x-2)}{x^2} + \frac{2}{x^2} \\ &= \frac{x}{x^2} = \frac{1}{x} \end{aligned} \tag{4.9}$$

P_{INTER} indique la probabilité d'un déplacement vers une zone unitaire appartenant à une autre zone RA. Cependant, cette probabilité ne tient pas compte de la nature de ladite prochaine zone, elle pourrait être UMTS ou WLAN. Nous sommes

intéressés au cas où la prochaine zone unitaire se trouverait dans une zone RA différente *ET* qu'elle soit de type UMTS :

$$\begin{aligned} P(Z_S = U_j \mid Z_C = U_i) &= P_{INTER} \cap P_U \\ &= P_{INTER} P_U \end{aligned} \tag{4.10}$$

En tenant compte de (4.10) on peut réécrire la probabilité qu'une mise à jour se fasse dans une zone de type UMTS:

$$\begin{aligned} P_{UMTS} &= P(Z_S = U \mid Z_C = W) \cap P(Z_C = W) + P(Z_S = U_j \mid Z_C = U_i) \cap P(Z_C = U) \\ &= P_U \cap P_W + P_{INTER} P_U \cap P_U \\ &= P_U P_W + P_{INTER} P_U P_U \end{aligned} \tag{4.11}$$

4.3.3 Fonction de coût moyen

À partir des probabilités de mise à jour pour chacun des types d'accès, nous pouvons écrire la fonction de coût moyen d'une mise à jour lors d'un changement de zone unitaire :

$$C_{MOYEN} = P_{WLAN} \times U_{WLAN} + P_{UMTS} \times U_{UMTS} \tag{4.12}$$

4.4 Paramètres d'expérimentation

De façon générale, nous considérons que le coût de transmission d'un message de signalisation est égal au coût de transmission d'un paquet de données d'usager. Nous faisons cette hypothèse pour simplifier les calculs de coût, mais surtout pour simplifier le nombre de paramètres différents ainsi que le nombre de valeurs possibles. De plus,

nous considérons négligeable le coût de transmission entre le TE et le MT (D_M), c'est-à-dire la transmission qui se fait à l'intérieur du nœud mobile.

Le délai de transmission à travers le UTRAN constitue le délai de transmission le plus important dans un système UMTS. En admettant que les délais de transmission des paquets de données et de signalisation sont les mêmes, nous pouvons considérer que les paramètres L_U et D_U sont équivalents. Le Tableau 4.2 présente les valeurs minimum et maximum que peuvent prendre les paramètres utilisés dans les calculs de coût. Ces valeurs sont approximatives.

Tableau 4.2 Intervalle de délai (ms) de transmission dans le UTRAN

Paramètres	Min	Max
L_U, D_U	50	100
L_{CN}, D_{CN}, D_{IP}	3	10
E	1	3
C	0.5	1

Les délais de transmission des paquets dans le réseau fixe sont beaucoup moins grands que dans le UTRAN. Ils dépendent principalement de la technologie de transport utilisée et du nombre de routeurs intermédiaires. Comme pour le UTRAN, nous considérons les délais de transmission de paquets de données et de contrôle comme équivalents, donc les paramètres L_{CN}, D_{CN} et D_{IP} prennent les mêmes valeurs. Aussi, nous considérons que la transmission de données à travers le tunnel GTP n'engendre pas de délai additionnel par rapport à la transmission de données directement par la couche IP. Comparativement au délai de transmission, les délais pour l'encapsulation des données ou la conversion de protocole sont beaucoup plus petits. Ils ont donc un impact moindre sur le coût moyen d'une mise à jour. Le temps de transmission sur une interface radio WLAN est relativement petit comparativement à la technologie UMTS. Dans notre étude, nous utilisons une valeur moyenne de 10 ms pour D_W. Nous ne définissons pas d'intervalle pour ce paramètre car il n'a pas d'impact sur la mise à jour dans le réseau

UMTS. En plus des paramètres de délai, les facteurs qui définissent la topologie du réseau peuvent avoir un impact important sur la performance de la relève inter-technologique. Le Tableau 4.3 présente les valeurs que peuvent prendre les paramètres « x » et P_W ($P_U = 1 - P_W$).

Tableau 4.3 Valeurs de paramètres topologiques

Paramètres	Min	Max
x	5	400
P_W	0.1	0.8

Dans notre évaluation, nous étudions l'effet de la densité de zone de type WLAN, donc la probabilité qu'une zone unitaire soit du type WLAN, P_W. Aussi, nous croyons que la taille des zones de couverture RA, de longueur de côté « x », a un impact sur la performance de notre proposition, car un changement de zone RA engendre une mise à jour auprès du MER.

4.5 Analyse des résultats

Dans cette section, nous discutons des résultats obtenus en calculant le coût moyen de mise à jour par changement de zone unitaire pour les trois scénarios identifiés. Nous étudions l'impact de la variation des paramètres présentés dans la section précédente sur le coût moyen. La Figure 4.8 présente le coût moyen de mise à jour en faisant varier les coûts de transmission dans le UTRAN. Les valeurs utilisées pour les autres paramètres sont : L_{CN}, D_{CN} et $D_{IP} = 7.5$, $D_M = 0$, $D_W = 10$, $E = 3$, $C = 0.5$, $x = 50$, $P_W = 0.3$, $P_U = 0.7$.

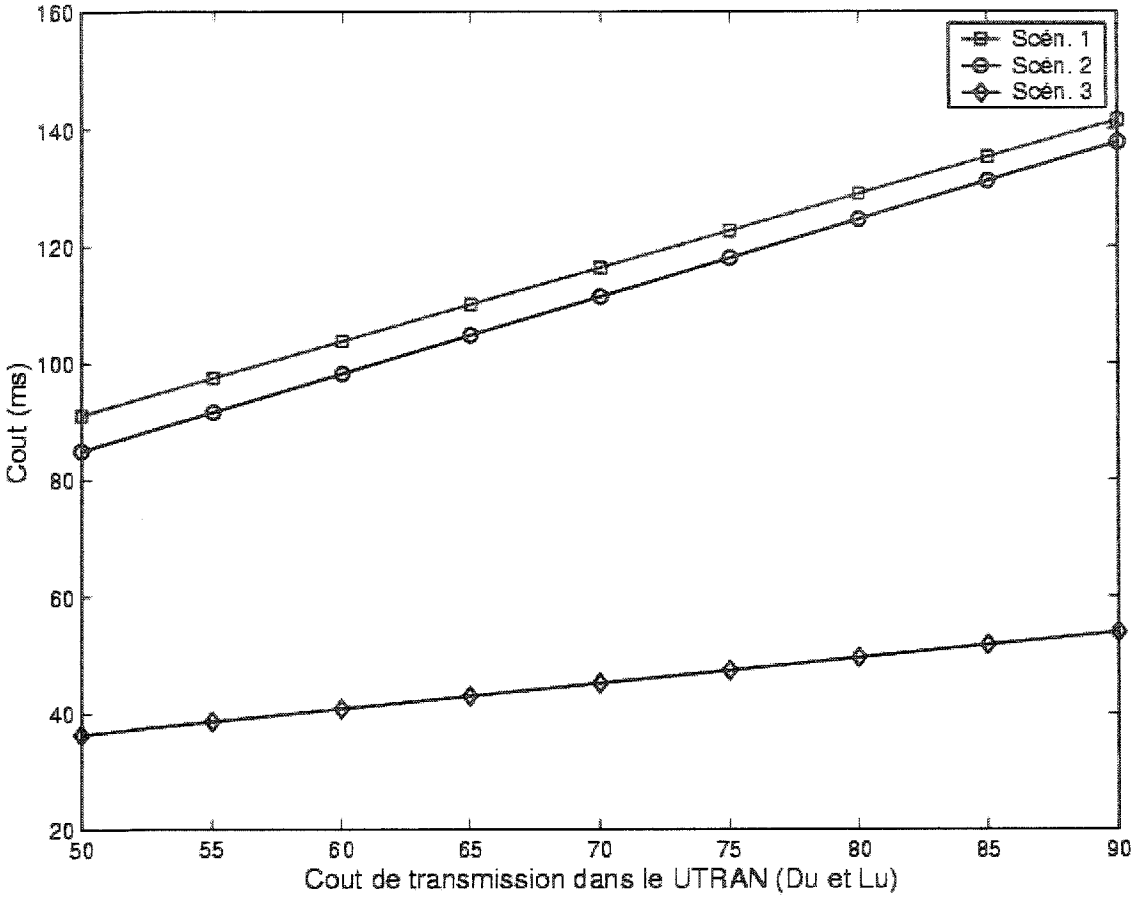

Figure 4.8 Variation du délai de transmission dans le UTRAN

Tout d'abord, nous constatons que le coût moyen d'une mise à jour par déplacement unitaire pour le scénario 3 est considérablement inférieur aux deux autres scénarios. Ceci s'explique par l'utilisation de la mise en correspondance de protocoles, qui évite le délai nécessaire à l'activation d'un contexte PDP. Aussi, le scénario 2 obtient un coût moyen légèrement inférieur au scénario 1. Cette légère différence est due au fait que, dans le scénario 1, les messages LBU et LBA doivent sortir du réseau UMTS avant d'atteindre le MAP, ce qui ajoute un délai supplémentaire. Avec l'augmentation des délais de transmission dans le UTRAN, le délai moyen dans les scénarios 1 et 2 augmente plus rapidement que dans le scénario 3. Nous expliquons encore cette différence par la mise en correspondance de protocoles. En réutilisant la

signalisation UMTS, la mise en correspondance permet de réduire le nombre d'échanges de messages à travers le UTRAN, ce qui rend le scénario 3 moins sensible à l'augmentation du délai transmission dans le UTRAN.

La Figure 4.9 présente le coût moyen de mise à jour en faisant varier les coûts de transmission dans le réseau fixe. Les valeurs utilisées pour les autres paramètres sont : L_U, $D_U = 70$, $D_M = 0$, $D_W = 10$, $E = 3$, $C = 0.5$, $x = 50$, $P_W = 0.3$, $P_U = 0.7$.

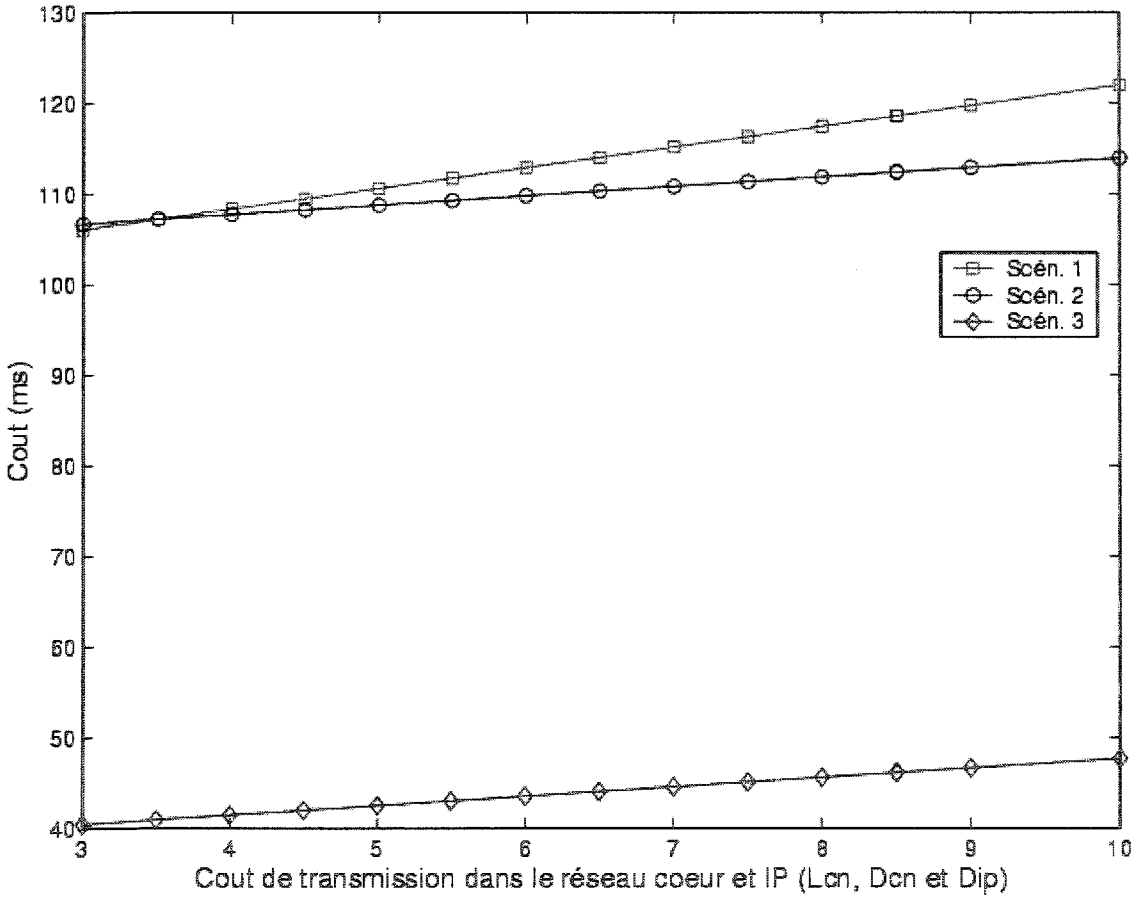

Figure 4.9 Variation du délai de transmission dans le réseau fixe

Nous constatons que le coût moyen de mise à jour est beaucoup moins affecté par la variation du coût de transmission dans le réseau fixe, ce qui est normal étant donné la

proportion de ce coût par rapport au coût total de la mise à jour. Une fois encore, le coût moyen de mise à jour dans le scénario 2 est inférieur au scénario 1. Dans le scénario 2, les messages LBU et LBA n'ont pas besoin de sortir du réseau UMTS pour atteindre le MAP qui est intégré au GGSN, ce qui évite des coûts de transmission supplémentaires. Cependant, comme on peut le remarquer à la Figure 4.9, pour des coûts de transmission sur réseau fixe faibles, cet avantage du scénario 2 s'estompe et les coûts moyens deviennent égaux.

Nous n'estimons pas nécessaire d'étudier l'effet de la variation des paramètres de coût d'encapsulation des données (E) et de coût de mise en correspondance (C), car ils sont responsables d'une faible proportion du coût moyen de mise à jour. Nous croyons que les résultats seraient très semblables à ceux présentés aux Figures 4.8 et 4.9.

Nous allons maintenant étudier l'impact de la variation des paramètres topologiques du réseau sur le coût de mise à jour moyen dans les trois scénarios. Nous étudions d'abord l'effet de la variation de la densité de zones de type WLAN et ce, dans deux situations bien différentes, lorsque les zones RA sont de taille petite ou grande. Ensuite, nous présentons l'effet de la variation de la taille des zones RA sur la performance des trois scénarios. Nous utilisons encore deux situations différentes : quand la densité de présence de zone WLAN est très faible ou très grande.

La Figure 4.10 présente le coût moyen de mise à jour en faisant varier la densité de présence de zones de type WLAN avec des petites zones RA. Les valeurs utilisées pour les autres paramètres sont : L_U, $D_U = 70$, L_{CN}, D_{CN} et $D_{IP} = 7.5$, $D_M = 0$, $D_W=10$, $E = 3$, $C = 0.5$, $x = 20$.

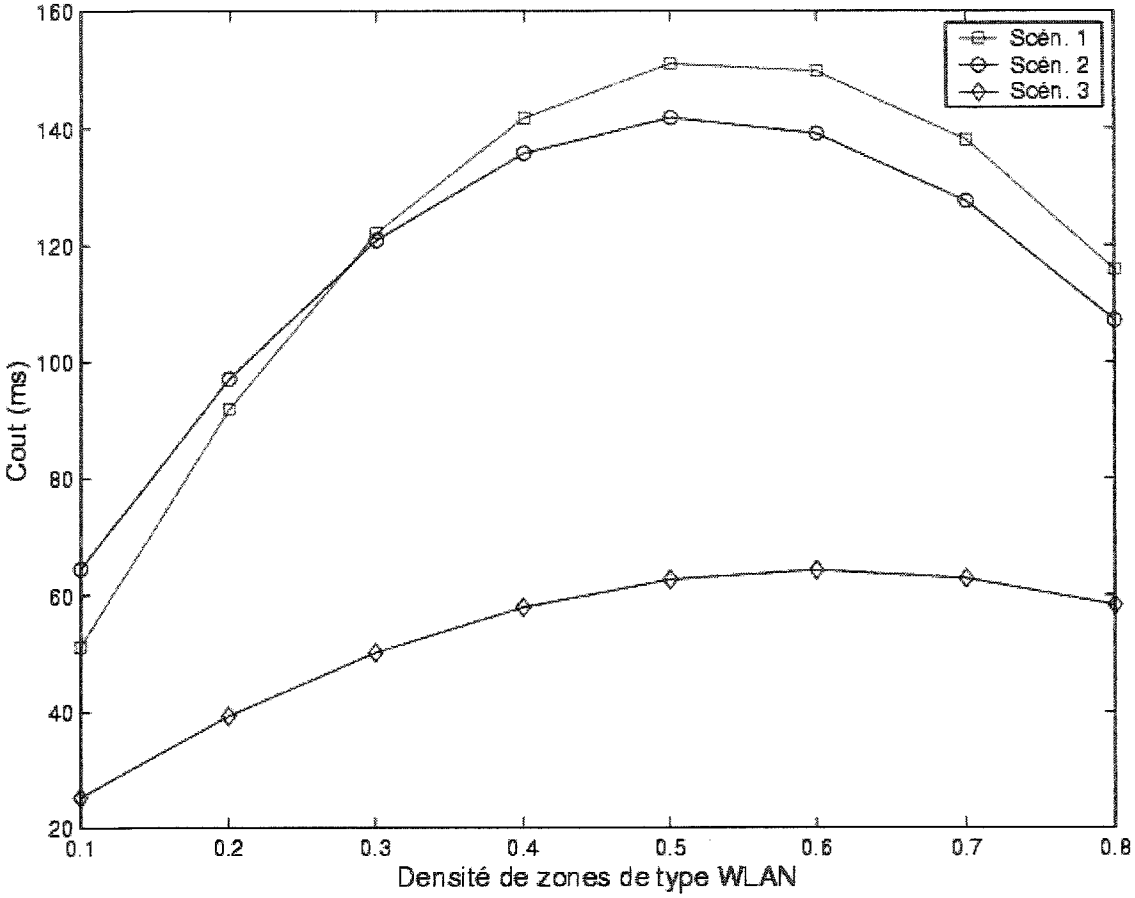

Figure 4.10 Variation de la densité des zones de couverture de type WLAN pour des petites zone de Routing Area

La Figure 4.11 présente le coût moyen de mise à jour en faisant varier la densité de présence de zones de type WLAN avec des grandes zones RA. Les valeurs utilisées pour les autres paramètres sont : L_U, $D_U = 70$, L_{CN}, D_{CN} et $D_{IP} = 7.5$, $D_M = 0$, $D_W = 10$, $E = 3$, $C = 0.5$, $x = 1000$.

Premièrement, nous remarquons que, lorsque la densité de présence de zones de type WLAN atteint 50-60% ($P_W = 0.5$ et 0.6), le coût moyen de mise à jour atteint son sommet pour les trois scénarios étudiés. Ceci est cohérent car c'est à cette densité que la probabilité de changement de type d'accès par déplacement unitaire est le plus élevé.

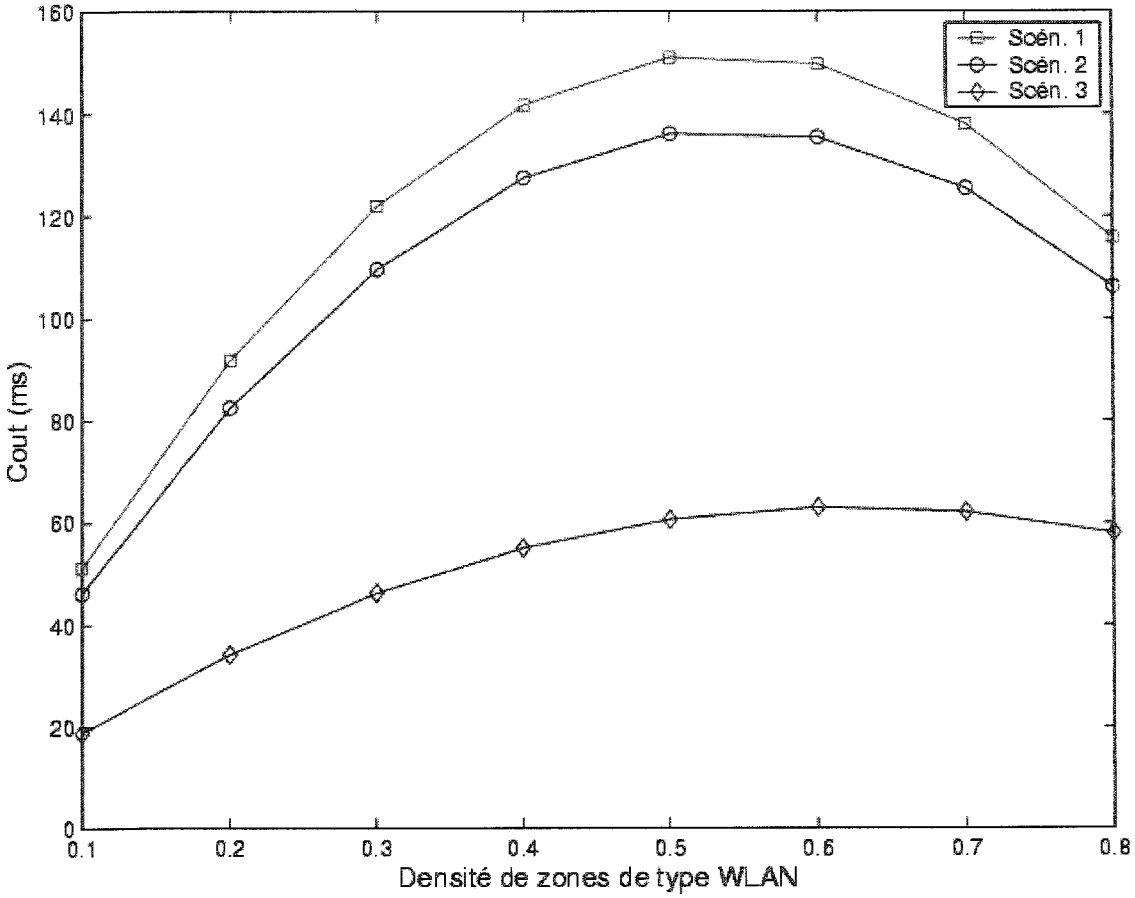

Figure 4.11 Variation de la densité des zones de couverture de type WLAN pour des grandes zones de couverture *Routing Area*

Nous observons que, à la Figure 4.10, donc pour une petite taille de RA, le scénario 2 obtient des coûts moyens plus élevés que le scénario 1 lorsque la densité de WLAN est faible. Aussi, nous remarquons que la variation du coût moyen du scénario 1 est identique dans deux cas étudiés (Figure 4.10 et 4.11). Ceci s'explique par le fait que, dans l'architecture conventionnelle (scénario 1), la taille de la zone RA n'a aucun impact, car il n'y a pas de mise à jour pour n'importe quel déplacement à l'intérieur du réseau UMTS. Lorsque P_W dépasse la valeur de 0.5, les figures 4.10 et 4.11 sont quasi identiques, ce qui nous laisse croire qu'au delà de ce seuil, la taille de la zone RA a peu d'impact sur la différence de performance des trois scénarios présentés. Nous allons

maintenant étudier plus en détail l'effet de la taille de la zone RA sur le coût moyen de mise à jour auprès du MER.

La Figure 4.12 présente le coût moyen de mise à jour en faisant varier la taille des zones RA avec une densité de WLAN faible. Les valeurs utilisées pour les autres paramètres sont : L_U, D_U = 70, L_{CN}, D_{CN} et D_{IP} = 7.5, D_M = 0, D_W= 10, E = 3, C = 0.5, P_W = 0.1.

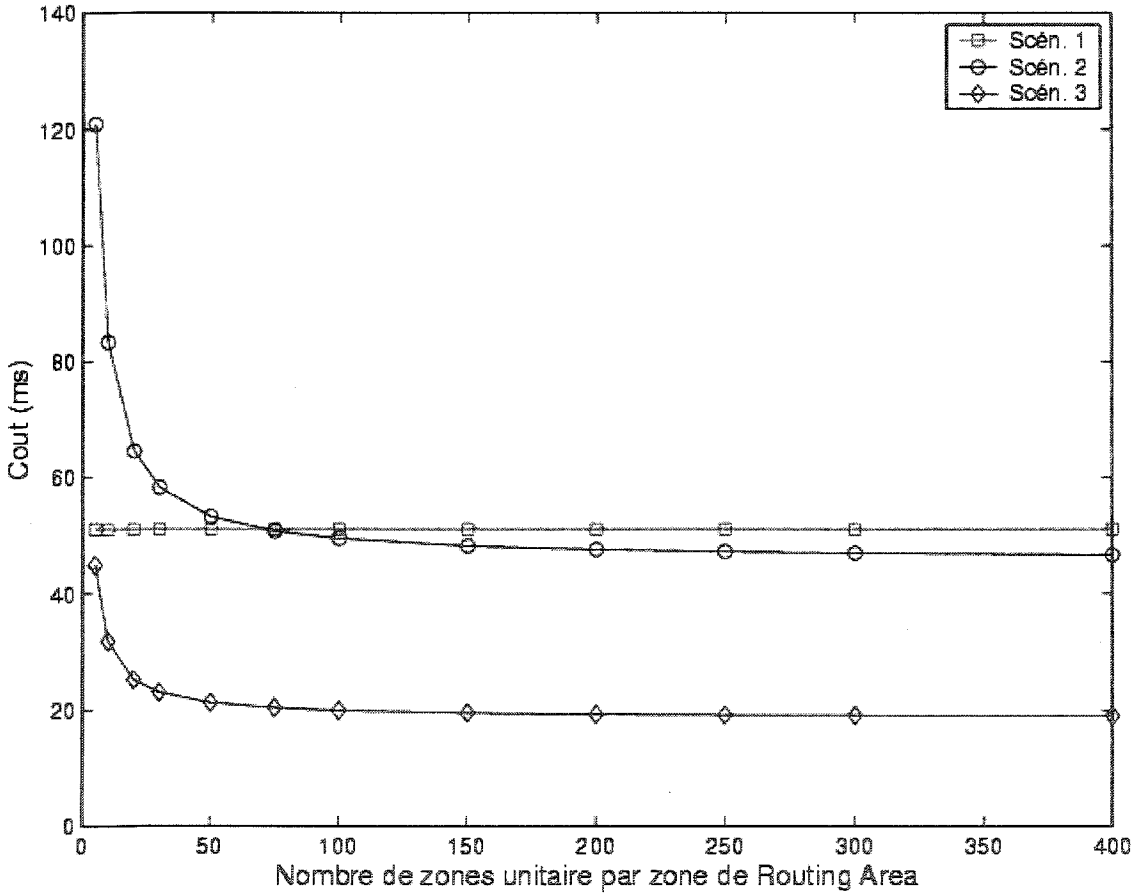

Figure 4.12 Variation de la taille zone de couverture *Routing Area* avec une densité de WLAN faible

La Figure 4.13 présente le coût moyen de mise à jour en faisant varier la taille des zones RA avec une densité de WLAN élevée. Les valeurs utilisées pour les autres

paramètres sont : L_U, D_U = 70, L_{CN}, D_{CN} et D_{IP} = 7.5, D_M = 0, D_W= 10, E = 3, C = 0.5, P_W = 0.8.

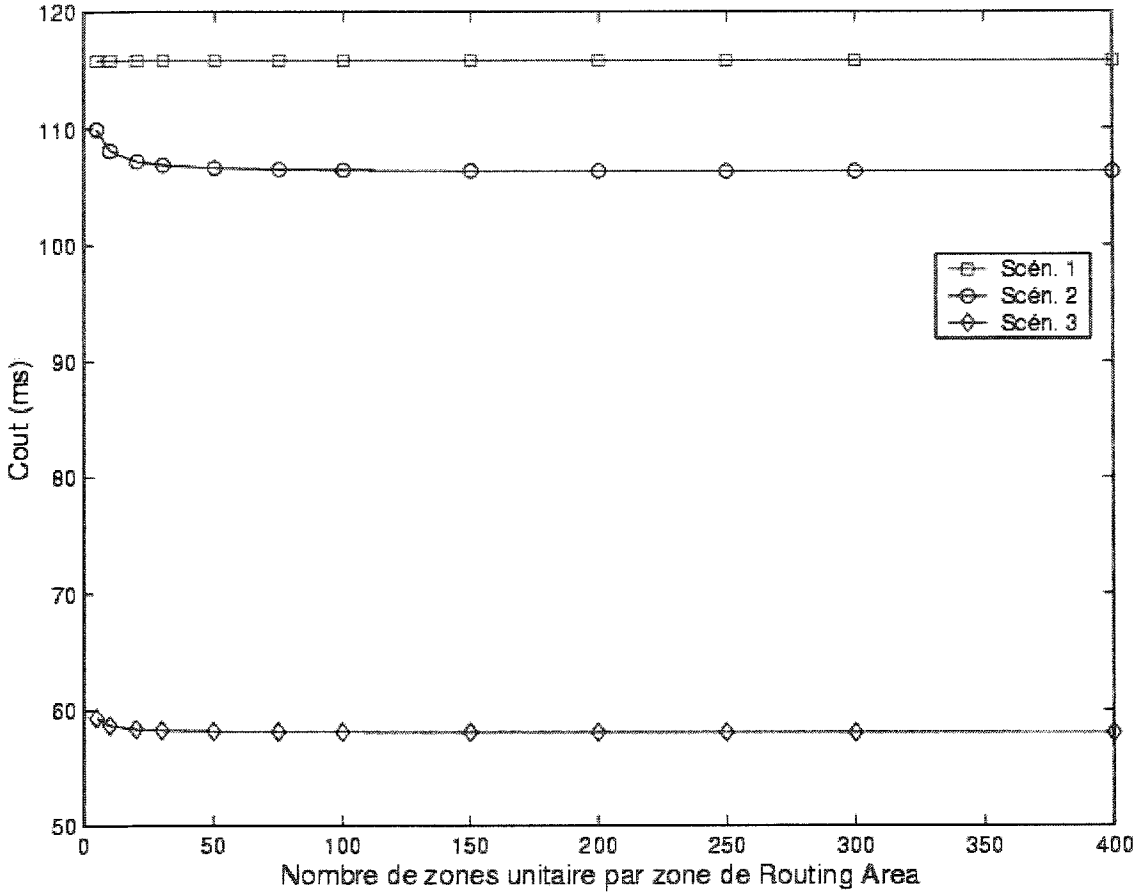

Figure 4.13 Variation de la taille zone de couverture *Routing Area* avec une densité de WLAN élevée

Les résultats présentés aux Figures 4.12 et 4.13 démontrent plus clairement que la taille des zones RA n'a aucun impact sur le scénario 1. Comme nous avons expliqué plus haut, ceci est dû au fait que, dans l'architecture UMTS conventionnelle, un changement de zone RA n'implique pas de changement de sous-réseau IP et donc pas de mise à jour auprès du MER. Les scénarios 2 et 3, qui utilisent l'architecture évoluée, sont au contraire sensibles à la taille des zones RA. Comme le montrent les Figures 4.12

et 4.13, plus les zones RA sont petites, plus les coûts moyens de mise à jour sont plus élevés, ce qui est dû aux changements de sous-réseau plus fréquents. Ce phénomène est accentué lorsque la densité de WLAN est petite. Dans cette situation, l'architecture que nous proposons est beaucoup moins efficace. En effet, comme le montre la Figure 4.12, lorsque la taille de zone RA est petite ($x < 50$), le scénario 2 obtient des coûts moyens bien supérieurs au scénario 1, tandis que le scénario 3 obtient des coûts moyens tout juste meilleurs que le scénario 1. Enfin, nous observons que la taille des zones RA dépasse un certain seuil, c'est-à-dire la longueur de côté (x) dépasse la valeur 100, le coût moyen de mise à jour ne change presque plus.

En somme, nous considérons que notre proposition améliore considérablement la gestion de la mobilité dans un contexte multi-accès. Nous observons que, de façon générale, c'est la mise en correspondance de protocoles de contrôle qui a le plus d'impact sur le coût moyen de mise à jour. Nous croyons que l'utilisation de notre proposition serait plus bénéfique dans un environnement urbain, où la densité des zones de type WLAN est élevée et donc le nombre changements de sous-réseaux est fréquent. Comme le montre la Figure 4.13, où P_W est égale à 0.8, la diminution du coût moyen de mise à jour atteint 50%.

CHAPITRE 5

CONCLUSION

Dans ce cinquième et dernier chapitre, nous résumons les travaux réalisés dans le cadre de ce mémoire, pour ensuite identifier les limitations de notre proposition. Enfin, nous identifions quelques avenues de recherches futures possibles.

5.1 Synthèse de la proposition

Les réseaux mobiles de prochaines générations seront multi-accès, c'est-à-dire que les utilisateurs du système pourront accéder aux services du réseau à partir de plusieurs technologies d'accès différentes. Afin de faire abstraction du type d'accès utilisé pour les communications, on envisage d'utiliser des protocoles de contrôle communs basés sur le protocole IP. Il est cependant essentiel que les mécanismes de contrôle IP soient intégrés aux mécanismes spécifiques des différentes technologies d'accès envisagées.

Dans ce mémoire, nous nous intéressons plus particulièrement à la technologie de troisième génération de type UMTS. Dans le but de faciliter l'utilisation des systèmes UMTS dans un contexte multi-accès, nous proposons une évolution de ce type de système qui intègre des mécanismes de contrôle IP. Nous considérons les mécanismes d'authentification, de signalisation de qualité de service et de gestion de la mobilité.

Notre proposition consiste en une architecture évoluée qui intègre à l'intérieur du réseau cœur UMTS, les fonctionnalités d'éléments de réseau IP définies par les protocoles de contrôle IP que nous considérons. Les protocoles de contrôle IP que nous utilisons sont définis au sein de l'organisme IETF. De plus, dans le but d'éliminer la redondance des mécanismes de contrôle, nous définissons une mise en correspondance

entre les protocoles de contrôle UMTS et IP. Ceci permet de réutiliser la signalisation UMTS à l'intérieur du UTRAN en plus de minimiser l'impact sur cette partie du système.

Aussi, à l'aide d'un modèle analytique de la relève UMTS-WLAN, nous avons pu faire une analyse de la performance de la mise à jour inter-technologique dans un environnement HMIPv6. Nous avons comparé notre proposition par rapport à une approche conventionnelle utilisant un système UMTS standard, en calculant le coût moyen de mise à jour d'une association d'adresse locale auprès d'un MAP lors du déplacement d'un nœud mobile. Nous avons constaté que notre proposition améliore grandement la relève inter-technologique entre un système UMTS et WLAN. De façon générale, le coût moyen de mise à jour lors d'un déplacement est beaucoup moins grand. Nous remarquons aussi que le gain de performance tient surtout de la mise en correspondance de protocoles plutôt que de l'intégration à l'intérieur du réseau cœur UMTS des protocoles de contrôle basés sur IP. Nous en concluons que notre proposition est avantageuse, surtout dans des environnements urbains où la densité de zones de couverture WLAN est élevée.

5.2 Limitations des travaux

Dans ce mémoire, nous avons présenté notre proposition puis nous avons fait une évaluation de performance pour l'aspect de la gestion de la mobilité. Comme nous l'expliquons au chapitre 4, nous n'avons pas fait d'évaluation pour les aspects de l'authentification et de la signalisation de qualité de service. Il est difficile d'évaluer l'aspect de l'authentification car l'amélioration qu'apporte notre proposition est qualitative; elle facilite l'utilisation d'un mécanisme d'authentification commun avec d'autres types d'accès. Pour la signalisation de qualité de service, il est techniquement difficile de faire une évaluation car le protocole HPMRSVP est encore en développement, aucune implémentation existe et aucun simulateur de réseau ne dispose de modèles complets et fonctionnels pour HPMRSVP, HMIPv6 et UMTS. Ceci nous a

empêché de comparer notre proposition à une approche conventionnelle pour des sessions de transfert de données temps réel dans un environnement multi-accès avec relève inter-technologique. Toutefois, l'analyse de performance réalisée nous a démontré que notre proposition permettrait d'améliorer considérablement le délai de mise à jour d'une association d'adresse locale lors d'une relève inter-technologique.

5.3 Travaux futurs

Les travaux futurs que nous estimons intéressants sont directement reliés aux limitations que nous avons identifiées. Avec des ressources appropriées, il serait pertinent de faire une évaluation du type preuve de concept avec une implémentation. En plus d'apporter une autre source de mesure de performance pour la relève inter-technologique, ce type d'évaluation permettrait de vérifier la conversion de messages lors de la mise en correspondance de protocoles de contrôle. Également, il serait intéressant d'évaluer l'utilisation du système UMTS évolué avec d'autres types de technologies d'accès.

Enfin, nous croyons à propos d'étudier la possibilité de faire une telle intégration de protocoles basés sur IP pour d'autres mécanismes de contrôle comme l'imputation de frais de service et l'autorisation, le transfert de contexte ou d'information sur le profil des utilisateurs.

BIBLIOGRAPHIE

[1] TANENBAUM, Adrew S., 2003, *Computer Networks*, Prentice Hall PTR, 2001, 912 pages.

[2] MURATORE, Flavio, 2001, *UMTS: mobile communications for the future*, John Wiley & Sons, 2001, 264 pages.

[3] Kaaranen, Heikki, AHTIAINEN, Ari, LAITINEN, Lauri, NAGHIAN, Siamäk, NIEMI, Valtteri, 2001, *UMTS networks: Architecture, Mobility, and Services*, John Wiley & Sons, 326 pages.

[4] HOLMA, Harri, TOSKALA, Antti, 2004, *WCDMA for UMTS: radio access for third generation mobile communications*, 2e Edition, John Wiley & Sons, 478 pages.

[5] WISELY, Dave, EARDLEY, Philip, BURNESS, Louise, 2002, *IP for 3G: networking technologies for mobile communications*, John Wiley & Sons, 304 pages.

[6] DORASWAMY, Naganand, HARKINS, Dan, 1999, *IPSec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks*, 1er Edition, Prentice Hall PTR, 288 pages.

[7] DE Vriendt, Johan, LAINÉ, Philippe, LEROUGE, Christophe, XU, Xiaofeng, 2002, « Mobile network evolution: A revolution on the move ». *IEEE Communications Magazine*, vol. 40, no. 4, pp. 104-111.

[8] HONKASALO, Harri, PEHKONEN, Kari, NIEMI, Markku T., LEINO, Anne T., 2002, « WCDMA and WLAN for 3G and beyond », *IEEE Wireless Communications*, vol. 9, no. 2, pp. 14-18.

[9] KIM, Yungsoo, JANG JEONG, Byung, CHUNG, Jaehak, HWANG, Chan-Soo, RYU, Joon S., KIM , Ki-Ho, KYUN KIM, Young, 2003, « Beyond 3G: Vision, requirements, and enabling technologies », *IEEE Communications Magazine*, vol. 41, no. 3, pp. 120-124.

[10] BEREZDIVIN, Robert, BREINIG, Robert, TOPP, Randy, 2002, « Next-generation wireless communications concepts and technologies », *IEEE Communications Magazine*, vol. 40, no. 3, pp. 108-116.

[11] Gustafsson, Eva, JONSSON, Annika, 2003, « Always best connected », *IEEE Wireless Communications*, vol. 10, no. 1, pp. 49-55.

[12] ZAHARIADIS, Theodore B., VAXEVANAKIS, Konstantinoss G., TSANTILAS, Christos P., ZERVOS, Nikolaos A., NIKOLAOU, Nikos A., 2002, « Global roaming in next-generation networks », *IEEE Communications Magazine*, vol. 40, no. 2, pp.145-151.

[13] Salkintzis, Apostolis K., FORS, Chad, PAZHYANNUR, Rajesh, 2002, « WLAN-GPRS integration for next-generation mobile data networks », *IEEE Wireless Communications*, vol. 9, no. 5, pp. 112-124.

[14] AHMAVAARA, Kalle, HAVERINEN, Henry, PICHNA, Roman, 2003, « Interworking architecture between 3GPP and WLAN systems », *IEEE Communications Magazine*, vol. 41, no. 11, pp. 74-81

[15] TSAO, Shiao-Li, LIN, Chia-Ching, 2002, « Design and evaluation of UMTS-WLAN interworking strategies », *Vehicular Technology Conference 2002*, VTC IEEE 56th, vol.2, pp.777-781.

[16] The 3rd Generation Partnership Project, 2004, *General Packet Radio Service (GPRS); Service description; Stage 2 (Release5)*, TS23.060, version 5.9.0, 210 pages.

[17] The 3rd Generation Partnership Project, 2004, *Mobile radio interface Layer 3* specification*; Core network protocols; Stage3 (Release5)*, TS24.008, version 5.12.0, 487 pages.

[18] The 3rd Generation Partnership Project, 2004, *Signalling System No. 7 (SS7) signalling transport in core network; Stage 3*, TS29.202, version 5.2.0, 19 pages.

[19] The 3rd Generation Partnership Project, 2004, *Mobile Application Part (MAP) specification (Release5)*, TS29.002, version 5.10.0, 1240 pages.

[20] The 3rd Generation Partnership Project, 2004, *3G security; Security architecture (Release5)*, TS33.102, version 5.4.0, 61 pages.

[21] The 3rd Generation Partnership Project, 2004, *Quality of Service (QoS) concept and architecture (Release5)*, TS23.107, version 5.12.0, 41 pages.

[22] The 3rd Generation Partnership Project, 2004, *Feasibility study on 3GPP system to Wireles Local Area Network (WLAN) interworking*, TS22.934, version 6.2.0, 30 pages.

[23] The 3rd Generation Partnership Project, 2004, *Requirements on 3GPP system to Wireless Local Area Network (WLAN) interworking*, TS22.234, version 6.1.0, 13 pages.

[24] The 3rd Generation Partnership Project, 2004, 3GPP system to Wireless Local Area Network (WLAN) interworking; System description (Release6), TS23.234, version 6.1.0, 50 pages.

[25] JOHNSON, David, PERKINS, Charles, ARKKO, Jarri, 2004, *Mobility Support in IPv6*, IETF RFC3775, 165 pages.

[26] SOLIMAN, Hesham, CASTELLUCIA, Claude, EL MALKI, Karim, BELLIER Ludovic, *Hierarchical Mobile IPv6 mobility management (HMIPv6)*, IETF draft-ietf-mipshop-hmipv6-04.txt, 28 pages.

[27] Calhoun, Pat, LOUGHNEY, John, GUTTMAN, Erik, ZORN, Glen, ARKKO, Jarri, *Diameter Base Protocol*, IETF RFC3588, 147 pages.

[28] BLUNK, Larry, VOLLBRECHT, John, ABOBA, Bernard, CARLSON, James, LEVKOWETZ, Henrick, 2004, *Extensible Authentication Protocol (EAP)*, IETF RFC3748, 67 pages.

[29] ERONEN, Pasi, HILLER, Tom, ZORN, Glen, *Diameter Extensible Authentication Protocol (EAP) Application*, IETF draft-ietf-aaa-eap-09.txt, 38 pages.

[30] ARKKO, Jarri, HAVERINEN Henry, 2003, *Extensible Authentication Protocol Method for UMTS Authentication and Key Agreement (EAP-AKA)*, IETF draft-arkko-pppext-eap-aka-12.txt, 75 pages.

[31] National Institute of Standards and Technology, 2001, *Federal Information Processing Standards (FIPS) Publication 197, "Advanced Encryption Standard (AES)"*, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf (page consultée le 18 Octobre 2004), 51 pages.

[32] The 3rd Generation Partnership Project, 2004, *3G Security; Wireless Local Area Network (WLAN) interworking security (Release 6)*, TS33.234, version 6.3.0, 84 pages.

[33] The 3rd Generation Partnership Project, 2004, *3GPP system to Wireless Local Area Network (WLAN) interworking; Stage 3 (Release 6)*, TS29.234, version 6.0.0, 56 pages.

[34] The 3rd Generation Partnership Project, 2004, *Mobile radio interface signalling layer 3;General aspects (Release 5)*, TS24.007, version 5.2.0, 140 pages.

[35] The 3rd Generation Partnership Project, 2004, *General on Terminal Adaptation Functions (TAF) for Mobile Stations (MS)(Release 5)*, TS27.001, version 5.8.0, 82 pages.

[36] The 3rd Generation Partnership Project, 2004, *Packet Domain;Mobile Station (MS) supporting Packet Switched Services (Release 5)*, TS27.060, version 5.6.0, 33 pages.

[37] The 3rd Generation Partnership Project, 2004, *Radio Resource Control (RRC); Protocol Specification (Release 5)*, TS25.331, version 5.8.0, 1003 pages.

[38] BRADEN, Bob, ZHANG, Lixia, BERSON, Steve, HERZOG, Shai, JAMIN, Sugih, *Resource Reservation Protocol Version 1 Functional Specification*, IETF RFC 2205, 112 pages.

[39] WROCLAWSKI, John, *The Use of RSVP with IETF Integrated Services*, IETF RFC 2210, 33 pages.

[40] ABONDO, Charles, PIERRE, Samuel, *Hierarchical Proxy Mobile Ressource Reservation Protocol*, IETF draft-abondo-hmprsvp-00.txt, 13 pages.

[41] NARTEN, Thomas, NORDACK, Erik, SIMPSON, William A., HESHAM Soliman, *Neighbor Discovery for IP version 6 (IPv6)*, IETF draft-ietf-ipv6-2461bis-02.txt, 86 pages.