Liste des Abréviation :

AP: Point d'accès
AR : Routeur d'accès
AsR : Association Response : Réponse d'association d'un MN avec un AP
BS: Station de Base
CN: Correspondent Node
MIH: Media Independent Handover
MN: Nœud Mobile
ND: Neighbor Discovery
NS: Network Simulator
RA: Router Advertisement
RS : Router Solicitation
SAP : Service Access Point

Table des matières

Tables des figures

INTRODUCTION GENERALE

INTRODUCTION GENERALE

Jour après jour, les services mobiles de toute sorte deviennent une exigence, la réalisation pratique et la mise en marche de ces services nécessite la découverte des nouvelles technologies et architectures. Ces nouvelles technologies qui viennent nous offrir un gain appréciable dans un sens ou dans un domaine donné cachent derrière elles des problèmes qui seront découverts rapidement. On reste toujours affronté au paradoxe suivant : gagner dans un sens, c'est perdre dans un autre. Le succès des réseaux locaux sans fil s'explique facilement par leur facilité de déploiement, associée à des coûts faibles, c'est ici que réside leur grande particularité. Dans ce sens le monde de recherche de plus en plus la mobilité et de nouveaux moyens de communication sans fil: Téléphonie sans fil, ordinateurs sans fil, organiseurs sans fil. Mais un appareil sans fil ne signifie pas seulement un dispositif qui peut fonctionner seul grâce à ses batteries. Le nouvel univers du sans fil est aussi celui d'un univers complètement connecté. Des appareils connectés l'un avec l'autre et avec le Web sans fil, des gens connectés les uns aux autres grâce à des appareils sans fil et connectés à l'Internet pendant leurs déplacements.

Le monde est toujours en état d'évolution, de nouveaux réseaux se trouvent posés au marché et surtout des réseaux sans fils. La gestion de ce type de réseaux (sans fil) devient de plus en plus populaire, les infrastructures des réseaux hétérogènes croissent. D'où la nécessité de passer d'un réseau à un autre croît et par suite se bouger librement entre les différents réseaux tout en gardant toujours la connexion courante, et en minimisant autant que possible les pertes (mobilité transparente). Cela peut prendre le nom de l'utilisation simultanée de différents réseaux d'accès et des technologies.

De plus, avec l'accroissement rapide de l'accès mobile à l'Internet, et son augmentation suite à la popularité croissante de WiFi (WLANs basés sur IEEE 802.11), et le déploiement mondial des réseaux sans fil de large secteur tels que GPRS et la troisième génération des réseaux sans fils (UMTS), un nombre de plus en plus important de dispositifs mobiles tels que des ordinateurs portables (*laptops*) et PDAs sont équipés pour se connecter aux réseaux multiples.

Différentes évolutions sont en cours aussi bien pour permettre des extensions pour la sécurité, la qualité de service et le *handover* que pour améliorer le débit, la couverture et permettre les réseaux ad-hoc et la cohabitation avec les autres types de réseau.

Des réseaux sans fil tels que UMTS et WLAN peuvent être arrangés comme recouvrement sur la base de leur couverture offerte ; un tel arrangement est connu comme réseau sans fil de recouvrement (*wireless overlay network*). Par exemple, UMTS peut fournir l'assurance nationale ou des larges continents, alors que WLAN basés sur 802.11 fournirent seulement une couverture locale sans fil ainsi que pour *Bleutooth*. Un mobile peut choisir de faire un *handover* vertical entre les différents réseaux ou non selon la couverture offerte, ou selon des politiques telles que la largeur de bande de réseau, la charge, le coût, la sécurité, la QoS, ou même la préférence d'utilisateur.

Les conséquences de l'utilisation des réseaux multiples en parallèle sont loin d'être négligeables. Ces conséquences découlent directement des utilisations que les gens en font, utilisations prévues ou inattendues.

Cette introduction générale était fort bien nécessaire pour situer notre projet. En effet, face à cette grande diversité de réseaux existants à notre temps et ayant la tentative de nous sentir totalement libre et mobile lors de nos communications, il était temps pour étudier le

Handover entre les différentes technologies existantes sans aucune coupure et avec un minimum possible de pertes, ce mécanisme est appelé le *Handover Vertical*.
L'objectif cette étude est donc d'étudier le *Handover Vertical* ainsi de proposer une méthode pour le réaliser et d'analysé les performances de ce dernier et d'étudier le *handover* sécurisé entre les réseaux UMTS et WLAN.
La suite de ce rapport va être comme suit:

Première partie : État de l'art
Au début un état de l'art sur la sécurité est détaillé dans le chapitre I, par la suite les réseaux mobiles sans fil sont exposés dans le Chapitre II, et dans le chapitre III qui le dernier dans cette première la mobilité est bien introduite. Dans la deuxième partie sera consacré à l'analyse des performances.

Deuxième partie : Analyse de performance de *handover* vertical entre réseaux UMTS et WLAN
Présentation du travail fait en simulation, du choix du logiciel, des divers cas simulés et l'analyse des résultats obtenus. Cela fera l'objet du chapitre IV.

Troisième partie : Proposition d'un *handover* sécurisé
Dans le dernier chapitre (chapitre V) nous proposons un mécanisme d'authentification pour le réseau hétérogène UMTS/WLAN.

Enfin nous essayons de tirer les conclusions qui s'imposent et nous proposons quelques perspectives pour le développement futur de ce travail.

Nous avons rassemblé à la fin de notre manuscrit quelques annexes utiles et bien entendu une bibliographie complète.

Partie I : État de l’art

CHAPITRE 1

État de l'art sur la sécurité des réseaux

Chapitre I : État de l'art sur la sécurité des réseaux

Ce chapitre traite les différents aspects de la sécurité des réseaux à savoir les attaques, les services, les mécanismes utilisés par les services pour contrer les attaques, ensuite nous présentons le modèle général de la sécurité de réseau.

INTRODUCTION

Les réseaux joue un rôle qui n'a cessé d'accroitre jour après jour, le déploiement de nouveaux réseaux soulève des problèmes de fonctionnement comme des problèmes de sécurité, dans le présent chapitre nous traitons la sécurité des réseaux d'une façon générale en essayant de donner une vision claire sur les différents éléments qui touche ce domaine.

I. Les types des attaques

Une attaque est toute action qui compromet la sécurité d'information d'une organisation.

La recommandation X.800 **[8]** et le RFC 2828 **[9]** classifient les attaques en terme d'attaques passives et actives.

1. Les attaques passives

Une attaque passive est une situation dans laquelle un intrus empêche le bon fonctionnement du réseau sans qu'il entraîne la destruction des données. Cependant il rassemble l'information pour un usage personnel ou pour une attaque future. Il existe deux types d'attaques passives à savoir : *interception de contenu* et *analyse de trafic* [1].

- ✧ **L'interception de contenu :** Dans ce type d'attaques, l'opposant intercepte le contenu d'un message dont la consultation n'est pas autorisée.

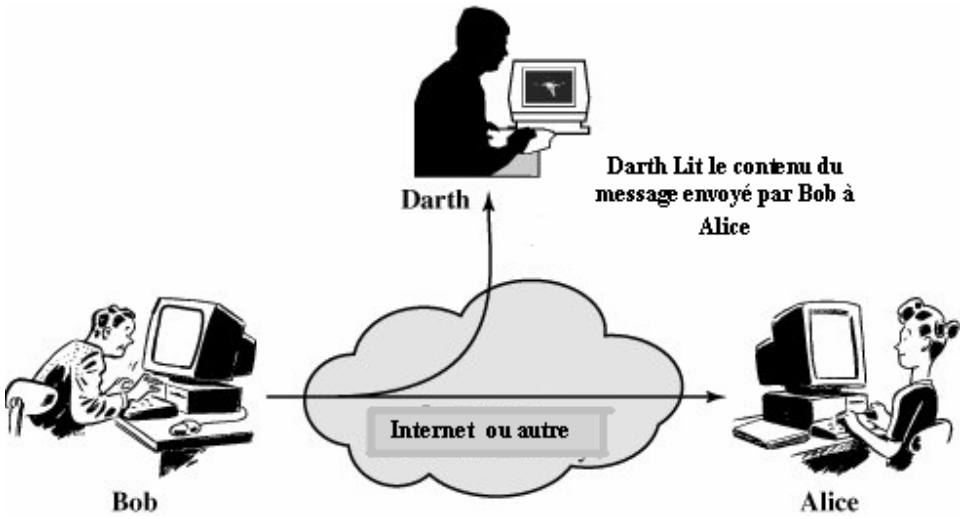

Figure 1: Interception de contenu

Ce message peut contenir, par exemple la clé secrète d'une session utilisée pour chiffrer des données durant celle-ci. Ce genre d'attaque signifie que l'intrus peut obtenir des informations qui sont parfois confidentielles. Il est difficile à détecter.

- ✧ **L'analyse de trafic :** Le deuxième type d'attaque passive, analyse de trafic, est plus subtile (figure 2). Il est parfois possible pour l'intrus de connaître l'endroit et l'identité du dispositif ou de l'utilisateur communiquant. Cela sera suffisant pour tirer l'information voulue. Un intrus pourrait seulement avoir besoin des informations suivantes :
- ✧ Qui envoie le message,
- ✧ A qui le message été envoyé,
- ✧ La fréquence ou la taille du message.

Une telle attaque est connue comme analyse de trafic.

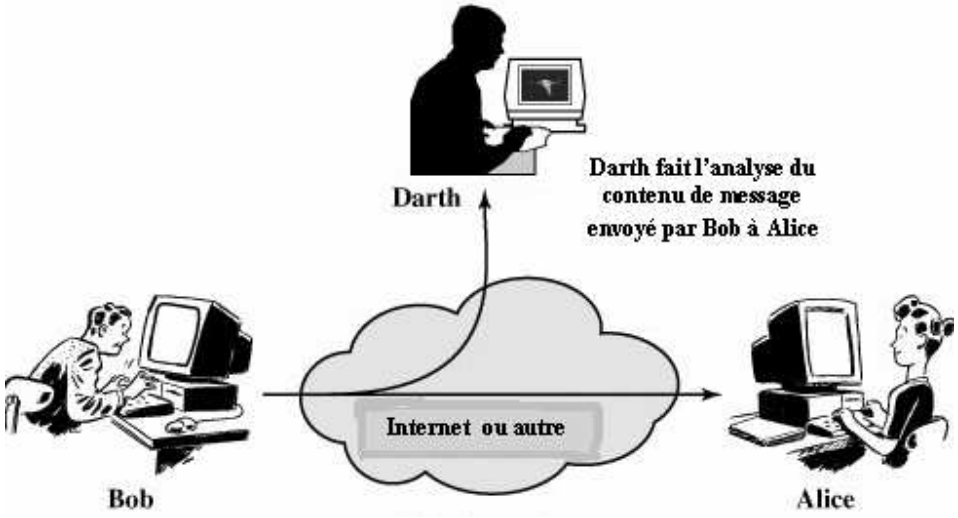

Figure 2: l'analyse de trafic

2. Les attaques actives

Les attaques actives entraînent une certaine modification des données ou insertion de nouvelle données et peuvent être divisées en quatre catégories: la mascarade (usurpation), le rejeu, la modification des messages et le déni de service.

- ✧ **La Mascarade** a lieu quand une entité feint pour être une entité différente (figure 3). Une mascarade inclut souvent des autres formes d'attaque active. Par exemple, lors d'authentification, des paramètres de connexion (*login* et *mot de passe* par exemple) peuvent être capturés et rejoués après qu'un ordre valide d'authentification a eu lieu. De ce fait, elle permet à une entité légale d'obtenir plus des privilèges pour avoir un accès non autorisé.

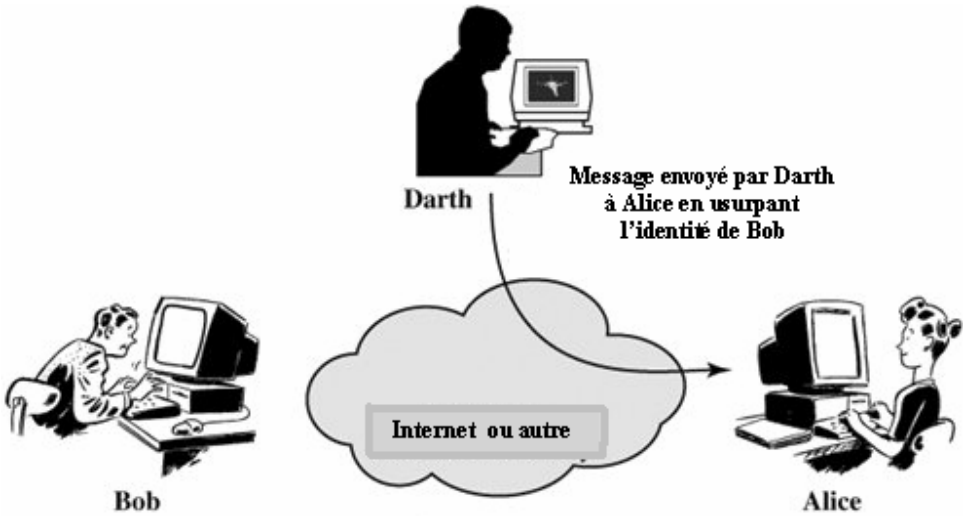

Figure 3: La mascarade

✧ **Le Rejeu** implique la capture d'un message et sa retransmission pour produire un effet non autorisé (figure 4).

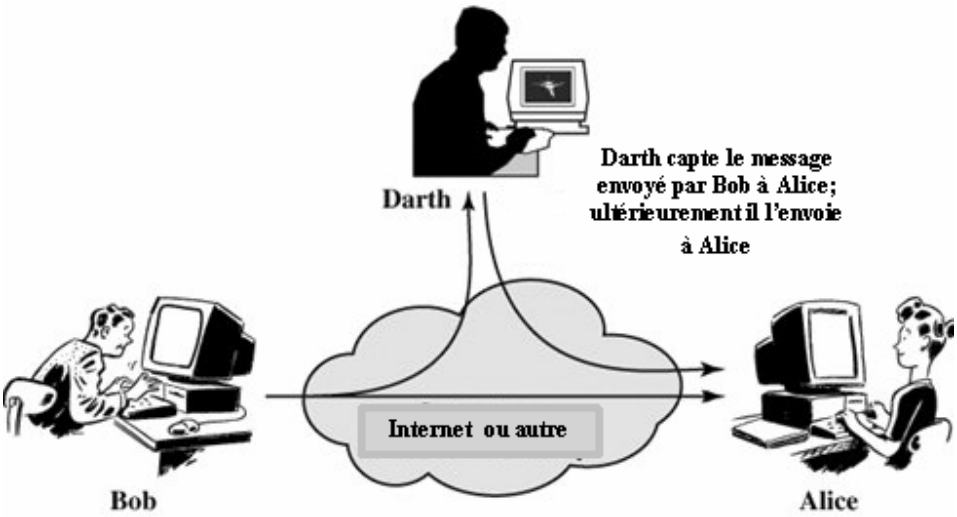

Figure 4 : le rejeu

✧ **La Modification des messages** signifie qu'une partie d'un message envoyé est changée, ou que des messages sont retardés ou rejoués pour produire un effet non autorisé (figure 5). Par exemple, message signifiant « Permettez à *Bob* de lire les dossiers confidentiels des comptes clients » est modifiée pour signifier que « Permettez à *Darth* de lire les dossiers confidentiels des comptes clients».

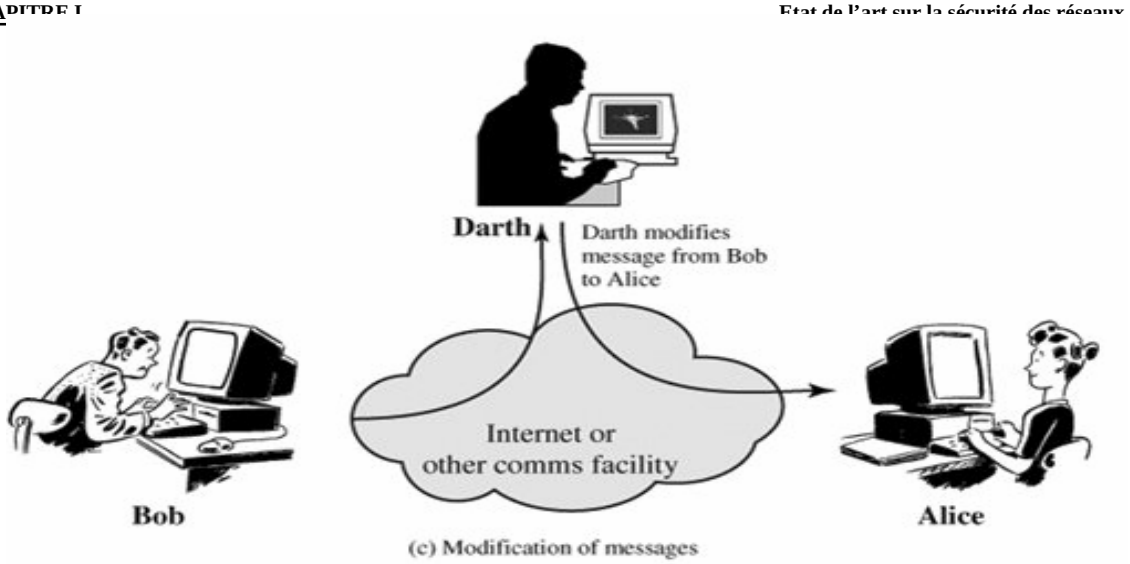

Figure 5 : la modification des messages

- **Le Déni de service** empêche l'utilisation ou la gestion des équipements de communications (figure 6). Cette attaque peut avoir une cible spécifique, par exemple, une entité peut supprimer tous les messages dirigés vers une destination particulière (par exemple, le service d'audit de sécurité). Une autre forme d'attaque peut être la panique d'un réseau entier, ou en le surchargeant avec des messages afin de dégrader la performance (le réseau peut devenir indisponible).

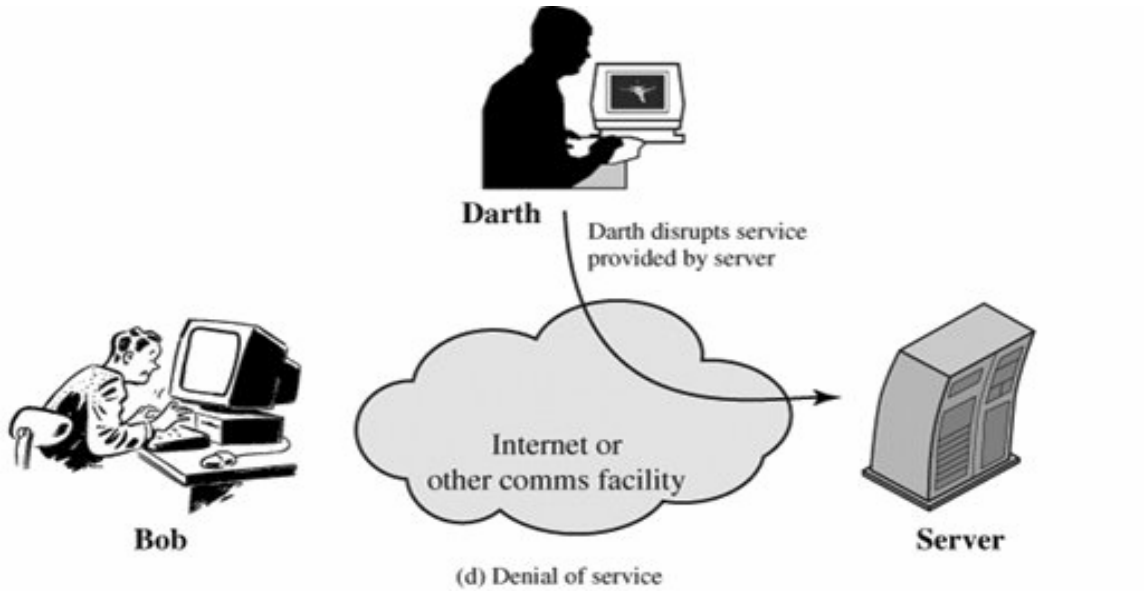

Figure 6: le déni de service

II. Les Services de Sécurité

La recommandation X.800 de ITU-T **[8]** définit un service de sécurité comme étant un service fourni par une couche de protocole du modèle OSI, qui assure la sécurité de

système ou le transfert de données. Une définition plus précise est trouvée dans RFC 2828 **[9]**, qui stipule que: **''***un service de sécurité est fourni par un système pour donner une protection aux ressources de système; Les services de sécurité implémentent des politiques de sécurité et sont mises en œuvre à l'aide des mécanismes de sécurité***''**.
Nous présentons brièvement les différents types de services de sécurité :

1. L'Authentification

L'effet d'assurer qu'une communication est authentique. Dans le cas d'un message simple, tel qu'un signal d'alarme, la fonction du service d'authentification est d'assurer le destinataire que le message est de la source de la laquelle il prétend être.

Deux services spécifiques d'authentification sont définis dans **[8]**:

- **L'authentification de paire à paire :** c'est l'action qui consiste à prouver son identité pour l'entité homologue déclarée. Ce service est généralement rendu par l'utilisateur d'un '' *échange d'authentification*'' qui implique un certain dialogue entre les tiers communicants.
- **L'authentification de l'origine de données :** sert à prouver que les données reçues ont bien été émises par l'émetteur déclaré. Ce type de service supporte des applications comme le courrier électronique où il n'y a aucune interaction antérieure entre les entités communicantes.

2. Le Contrôle d'accès

C'est la capacité de limiter et contrôler l'accès aux ressources matériels et logiciels d'un système via les liaisons de communication. Pour réaliser ceci, chaque entité qui essaye de se connecter doit tout d'abord s'identifier. Chaque utilisateur possède des droits d'accès particuliers aux ressources.

3. La Confidentialité

La confidentialité est la protection des données transmises contre des attaques passives. Elle assure la protection du contenu de données transmission de données. Plusieurs niveaux de la protection peuvent être identifiés. La confidentialité concerne la protection de toutes les données sur une connexion ou des données dans un bloc spécifique, ou des champs sélectionnés ou encore des informations qui peuvent être déduites par analyse de trafic. Par exemple, quand une connexion TCP est établie entre deux entités, ladite protection empêche la connaissance de n'importe quelles données d'utilisateur transmises durant celle-ci.

4. L'Intégrité

Un service d'intégrité orienté connexion traite un flot de données (messages) et assure que les messages reçus sont celles envoyés, sans duplication, insertion, modification et suppression. D'autre part, un service d'intégrité sans connexion, assure généralement la protection contre la modification de message seulement.

Nous pouvons faire une distinction entre le service avec et sans recouvrement. Puisque le service d'intégrité est lié aux attaques actives, nous sommes concernés par la détection plutôt que la prévention. Si une violation d'intégrité est détectée, alors le service peut rapporter cette violation et une intervention humaine ou logicielle est exigée pour restaurer après la violation. il existe des mécanismes pour restaurer l'intégrité des données. L'incorporation des mécanismes de restauration automatisés est généralement l'alternative la plus attrayante.

5. La non-répudiation

La non-répudiation empêche l'expéditeur ou le récepteur de nier un message transmis. Elle assure la protection contre un dénie (une négation) par une entité d'avoir participé à une partie ou toute la communication. Ainsi, quand un message est envoyé, le récepteur peut montrer que l'expéditeur a envoyé le message. De même, quand un message est reçu, l'expéditeur peut montrer que le récepteur a reçu le message.

6. La Disponibilité

C'est l'aptitude d'un système ou une ressource de système à pouvoir être accessible et fonctionnel à un instant donné par une entité autorisée du système. Une variété d'attaques peut avoir lieu lors de la perte de la disponibilité, tel que le déni de service.

Le tableau ci-dessous (*tableau 1*) indique le rapport entre les services de sécurité et les attaques.

	ATTAQUES					
SERVICE	**Interception de contenu**	**Analyse de trafic**	**Mascarade**	**Vioaltion d'accès**	**Déni de serivce**	**Modification des messages**
Authentification			Oui	Oui		Oui
Contrôle d'accès			Oui	Oui		Oui
Confidentialité	Oui	Oui	Oui	Oui		
Intégrité			Oui	Oui		Oui
La non-répudiation			Oui	Oui		Oui
Disponibilité			Oui	Oui	Oui	Oui

Tableau 1: la relation entre les services de sécurité et les attaques.

III. Les Mécanismes de Sécurité

Les moyens utilisés par les services pour contrer les attaques. Ils sont définies dans deux documents de référence à savoir : ITU-T X.800 **[8]** et RFC 2828 **[9]**. Ils se sont divisés en deux parties ceux qui sont implantés dans une couche spécifique de protocole et ceux qui ne sont pas spécifiques à aucune couche de protocole particulier ou service de sécurité. **[8]** distingue les mécanismes réversibles et irréversibles de chiffrement. Un mécanisme réversible de chiffrement est un algorithme de chiffrage qui permet à des données d'être chiffrées et plus tard déchiffrées. Les mécanismes irréversibles de chiffrement incluent les algorithmes de hachage et les codes d'authentification de message (*Message Authentification Code*, MAC), qui sont employés dans la signature numérique et le scellement qui consiste à adjoindre au message un sceau ou MAC.

1. Les Mécanismes Spécifiques de Sécurité

Ils peuvent être incorporés à la couche de protocole appropriée afin de fournir certains services de sécurité d'OSI. Parmi ces mécanismes on peut citer :

- **Le Chiffrement :** Le chiffrement peut assurer la confidentialité soit des données, soit du flux de données et peut jouer un rôle dans un certain nombre d'autres mécanismes de sécurité ou les compléter. Les algorithmes de chiffrement peuvent être réversibles ou irréversibles. Un algorithme de chiffrement réversible peut être de deux types:
  - **Le Chiffrement symétrique** (c'est-à-dire à clé secrète), dans lequel la connaissance de la clé de chiffrement implique une connaissance de la clé de déchiffrement et vice versa;
  - **Le Chiffrement asymétrique** (par exemple, à clé publique) dans lequel la connaissance de la clé de chiffrement n'implique pas la connaissance de la clé de déchiffrement, ou vice versa. Les deux clés de ce système sont parfois appelées "clé publique" et "clé privée";

  Les algorithmes de chiffrement irréversibles peuvent ou non utiliser une clé. Lorsqu'ils utilisent une clé, celle ci peut être publique ou secrète. L'existence d'un mécanisme de chiffrement implique l'utilisation d'un mécanisme de gestion de clés, sauf dans le cas de certains algorithmes de chiffrement irréversibles.
- **La Signature Numérique :** Des données ajoutées, ou une transformation cryptographique, à une unité de données qui permet au destinataire de prouver la source et l'intégrité de l'unité de données et de se protéger contre l'usurpation.
- **Le Contrôle d'accès :** C'est une variété de mécanismes qui applique des droits d'accès aux ressources.
- **L'Intégrité des données :** C'est une variété de mécanismes qui assure l'intégrité des données.
- **L'Échange d'authentification :** Un mécanisme prévu pour assurer l'identité d'une entité au moyen d'échange d'information.
- **Le Remplissage du trafic :** L'insertion de bit dans les zones vides d'un flux de données pour contrarier les tentatives de l'analyse de trafic.

- **Le Contrôle de Routage (***Routing Control***):** Permet le choix des routes physiquement sécuriser pour certaines données et permet le changement de routage, particulièrement quand on suspecte une violation de sécurité.
- **Le Certificat :** L'utilisation d'un tiers de confiance pour assurer certaines propriétés d'un d'échange de données.

2. Les Principaux Mécanismes de Sécurité

Ces sont des mécanismes qui ne sont pas spécifiques à aucun service de sécurité ou couche particulière de protocole OSI. On peut noter les cas suivants :

- **Fonctionnalité de confiance (***Trusted Functionality***) :** Ce qui est perçu correct en respectant quelques critères (par exemple, établi par une politique de sécurité).
- **Étiquette de sécurité :** Étiquette sur une ressource (qui peut être une unité de données) indiquant le nom ou les attributs de sécurité de cette ressource.
- **Détection d'événement :** Détection des événements appropriés de sécurité.
- **Audit de Sécurité (***Security Audit Trail***):** Données collectées et potentiellement employées pour faciliter un audit de sécurité, qui est un examen indépendants des enregistrements et des activités de système.
- **Recouvrement de Sécurité (***Security Recovery***) :** Effectué suite à une demande des mécanismes, tels que les fonctions de manipulation d'événement (*event handling*).

Le tableau ci-dessous (tableau 2), basé sur **[8]**, indique le rapport entre les services de sécurité et les mécanismes de sécurité.

SERVICE	MECANISMES							
	Chiffrement	Signature Numérique	Contrôle d'accès	Intégrité de données	Échange d'authentification	Remplissage du trafic	Contrôle de routage	Cer-tificat
Authentification de paire à paire	Oui	Oui			Oui			
Authentification d'origine de données	Oui	Oui						
Contrôle d'accès			Oui					
Confidentialité	Oui						Oui	
Confidentialité de flot de données	Oui					Oui	Oui	
Intégrité de données	Oui	Oui		Oui				
La non-répudiation		Oui		Oui				Oui
Disponibilité				Oui	Oui			

Tableau 2: la relation entre les services de sécurité et les mécanismes.

IV. Les Modèles de Sécurité des Réseaux

Il existe deux principaux modèles de sécurité pour les réseaux.
Le premier modèle (voir figure 7) regroupe beaucoup de notions vues auparavant. Ce modèle indique les quatre tâches dans la conception d'un service de sécurité :

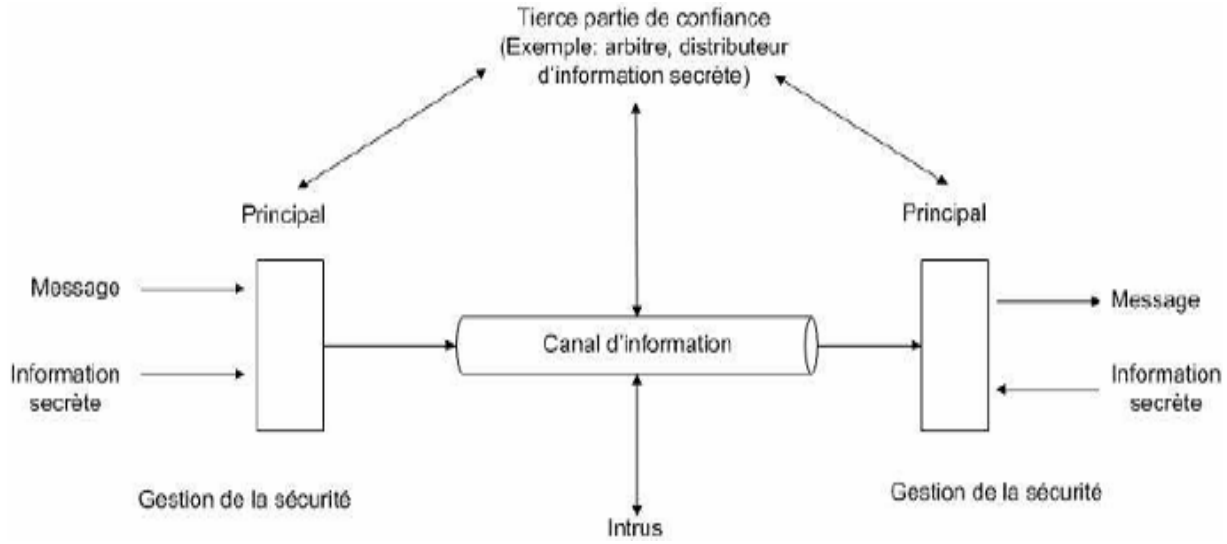

Figure 7: Le modèle général de Sécurité des réseaux

i. Concevoir un algorithme pour la transformation sécuritaire,
ii. Générer le code secret à utiliser avec l'algorithme,
iii. Développer une méthode de distribution et de partage du code secret,
iv. Spécifier le protocole à utiliser par les deux parties pour mettre en œuvre l'algorithme.

L'autre modèle de sécurité est le modèle de sécurité des accès réseau (voir figure 8), qui permet pour un système d'information de se protégé contre les accès non désiré. L'intrus peut être un humain comme le *hacker* ou un logiciel tel que vers, cheval de troie. Il essaye de pénétrer les systèmes qui sont accessible par réseau. Un autre type d'accès non désiré est l'insertion d'un code malicieux au du système qui exploite des vulnérabilités de ce dernier. Les informations du système peuvent être des ressources comme les processeurs, les données, les traitements ou les logiciels. Les programmes peuvent présenter deux genres de menaces :

- ✧ **L'usurpation :** L'intrus peut intercepter ou modifier les données par violation d'accès.
- ✧ **Le déni de service :** L'intrus dans ce cas exploite les services pour empêcher à un utilisateur autorisé d'utiliser une ressource.

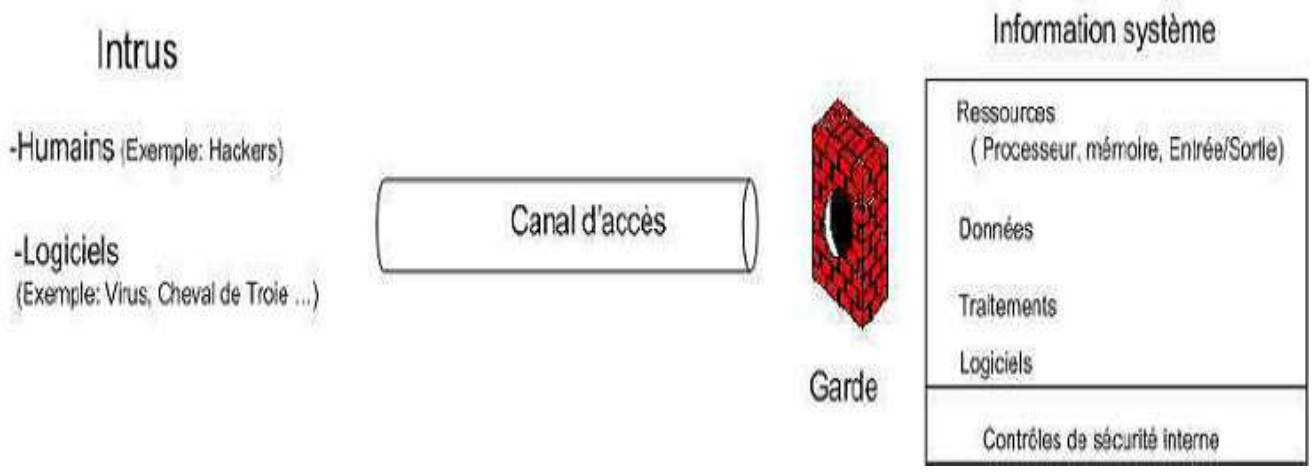

Figure 8: Le modèle de sécurité des accès réseau

V. Les Protocoles de sécurité des réseaux

Dans cette section nous présentons brièvement quelques protocoles de sécurité que nous allons référencer dans notre proposition (voir chapitre V).

1. IPSec

IPSec vise à sécuriser les échanges au niveau de la couche réseau. Le réseau IPv4 étant largement déployé et la migration complète vers IPv6 nécessitant encore beaucoup de temps, il est vite apparu intéressant de définir des mécanismes de sécurité qui soient communs à la fois à IPv4 et IPv6. Ces mécanismes sont couramment désignés par le terme IPsec pour IP Security Protocols.

IPsec fournit:

- ✧ Confidentialité et protection contre l'analyse du trafic,
- ✧ Authentification des données (et de leur origine),
- ✧ Intégrité des données (en mode non connecté),
- ✧ Protection contre le rejeu,
- ✧ Contrôle d'accès.

IPsec est une extension de sécurité pour le protocole Internet IP. Il peut être mis en œuvre sur tous les équipements du réseau. Exemple d'utilisation : Les réseaux privés virtuels ou VPN ou bien la sécurisation des accès distants à un intranet.

2. AAA: *Authorization, Authentification and Accounting*

En sécurité informatique, **AAA** correspond à un protocole qui réalise trois fonctions : l'authentification, l'autorisation, et la traçabilité (*en anglais : Authentication, Authorization, Accounting*).

La liste de protocoles AAA est :

- ✧ **RADIUS (*Remote Authentication Dial-In User Service*) :** C'est un protocole client-serveur permettant de centraliser des données d'authentification. En français on préfère souvent parler d'identification pour traduire l'anglais authentication, car l'identification effectuée par un serveur Radius est une vérification de nom d'utilisateur (attribut 1 User-Name) et de mot de passe (attribut 2 *User-Password* ou 3 *Chap-Password*). L'authentification en français est définie comme la vérification approfondie par un expert ou un officier ministériel et correspond à l'anglicisme authentification forte pour "*strong authentication*", mais l'abus de langage est courant.
- ✧ **DIAMETER :** C'est un protocole d'authentification, successeur du protocole RADIUS. Ce protocole est défini par la RFC 3588, et définit les pré-requis minimums nécessaire pour un protocole AAA;

TACACS : (Terminal Access Controller Access-Control System) : C'est un protocole d'authentification distante utilisé pour communiquer avec un serveur d'authentification, généralement utilisé dans des réseaux UNIX. TACACS permet à un serveur d'accès distant de communiquer avec un serveur d'authentification dans l'objectif de déterminer si l'utilisateur a le droit d'accéder au réseau.

- ✧ **TACACS+.**
- ✧

D'autres protocoles utilisés généralement avec les protocoles AAA :

- ✧ PPP
- ✧ EAP
- ✧ LDAP

CONCLUSION

Tout au long de ce chapitre nous avons abordés les éléments de base de la sécurité des réseaux, à savoir les attaques que ce soient passives ou actives, des services qui consolident la sécurité des données et des transferts sont aussi vues, les mécanismes qui implémentent ces services sont détaillés, les différents modèles de sécurité ont été schématise, et ensuite quelques protocoles de sécurité que nous allons utilisés ultérieurement sont aussi abordés.

CHAPITRE 2

Etat de l'art sur les réseaux mobiles sans fils

Chapitre II : État de l'art sur les réseaux mobiles sans fils

Dans ce chapitre nous commençons par présenter les réseaux sans fil en mettant l'accent sur le WLAN, ensuite les réseaux cellulaires sont présentés.

INTRODUCTION

Depuis quelques années, le domaine des réseaux informatiques connaît une forte évolution, avec des besoins croissants des utilisateurs en terme de mobilité. Un utilisateur veut pouvoir se déplacer tout en restant connecté au réseau qui lui permet de communiquer avec d'autres utilisateurs. Ce nouveau besoin oblige la définition d'un ensemble de procédures pour tenir compte de la mobilité.

En effet, lorsque l'utilisateur se déplace (itinérance ou *roaming*), il va falloir le localiser de façon à pouvoir gérer ses communications. A un instant donné, un utilisateur n'est accessible que dans la limite d'une certaine cellule. L'utilisateur changeant de cellule lors de ses déplacements, pose alors le problème de *handover* qui consiste à permettre à un utilisateur de rester connecté au réseau malgré le changement de zone. Le contexte de mobilité rend plus complexe les procédures à mettre en œuvre pour assurer l'acheminement des données entre l'utilisateur et son (ses) correspondant(s); ces deux entités pouvant être mobiles. Il va falloir définir des procédures permettant de maintenir les communications entre l'utilisateur et son (ses) correspondant(s).

Aussi bien dans le domaine de la téléphonie que de l'informatique, il s'agit de développer des architectures et les protocoles associés pour prendre en compte l'itinérance, le *handover* et le routage dans un contexte de mobilité.

Le domaine de la téléphonie a été le premier à s'intéresser au concept de mobilité et a abouti jusqu'à aujourd'hui à la définition de trois générations de systèmes mobiles.

Les évolutions en téléphonie mobile introduisent des modes de fonctionnement (système cellulaire par exemple, . . .) et des nouveaux besoins (*handover* par exemple, . . .) sur lesquels va s'appuyer la mobilité en informatique pour fonctionner.

I. Les réseaux sans fil

Comme pour les réseaux filaires, il existe différents types de réseaux sans fil : les réseaux personnels "WPAN" (*Wireless Personal Area Networks*), les réseaux locaux "WLAN" (*Wireless Local Area Networks*), les réseaux métropolitains "WMAN" (*Wireless Metropolitan Area Networks*) et les réseaux nationaux "WWAN" (*Wireless Wide Area Networks*). Passons un peu pour voir les caractéristiques de ces différents types.

1. Les réseaux sans fil de type "WPAN"

Les «WPAN» sont des réseaux sans fil de faible portée (quelques dizaines de mètres) qui sont des réseaux à usage personnel. Ils sont déjà présents sous différents noms :

- ✧ **Bluetooth :** connu encore sous la norme 802.15.1, *Bluetooth* est aujourd'hui présent dans de nombreux dispositifs. Malgré un débit de 1 Mb/s et une portée d'environ 30

mètres, *Bluetooth* offre de nombreuses possibilités grâce à la faible consommation de ses équipements.
Bluetooth opère sur 2.4 Ghz, il est intégré en standard dans Windows XP et disponible depuis 2001 en carte PCMCIA. On trouve des composants *Bluetooth* dans beaucoup d'ordinateurs portables mais aussi dans de nombreux périphériques (appareils photos, téléphones portables, assistants personnels,...). La norme 802.15.3 (*Bluetooth2*) qui devrait prochainement voir le jour est une version annoncée plus rapide avec de débits de 11, 22 33, 44 et 55 Mb/s, et pouvant intégrer des mécanismes de sécurité, qui font actuellement défaut dans le protocole *Bluetooth*. Parmi ces mécanismes on peut citer les notions de sécurité de groupe, élection automatique d'un chef de groupe, authentification mutuelle et gestion de clés de confidentialité.

✧ **ZigBee :** Avec un débit plus faible que *Bluetooth* (20 et 250 Kb/s), la norme 802.15.4 (*ZigBee*) pourrait être très utilisée dans les années à venir. Les équipements *ZigBee* moins consommateurs et moins onéreux que les équipements *Bluetooth* devraient trouver leur place dans les périphériques informatiques mais également en domestique (éclairage, système de sécurité,...).

✧ **Les liaisons infrarouges :** Les liaisons infrarouges sont très utilisées pour des communications à courte distance, cependant leur sensibilité aux perturbations empêche le développement de cette technologie dans les réseaux sans fil supérieurs à une distance d'une dizaine de mètres. Néanmoins, la portée d'interception peut-être très supérieure.

2. Les réseaux sans fil de type "WMAN" (La norme 802.16 ou Wimax)

Encore à l'état de norme pour le moment, les réseaux sans fil de type "WMAN" ne sont pas des projets très avancés. Cependant la B.L.R. (*Boucle Locale Radio*) fait partie des réseaux sans fil de type "WMAN". Sur la bande des 3,5 Ghz et des 26 Ghz et avec un débit de 2 Mb/s, la BLR est une technologie sans fil capable de relier les opérateurs de téléphonie à leurs clients grâce aux ondes radio sur une distance de 4 à 10 kilomètres.
802.16a permet un débit de 32 à 134 Mb/s sur la bande de 3.5 Mhz. Et ce qui devrait attirer l'attention est 802.16b ou WHUMAN, qui permet des réseaux métropolitains, avec gestion de bande passante et des émetteurs entre eux, sur la bande des 5 GHz.

3. Les réseaux sans fil de type "WWAN"

Bien que ces réseaux ne soient pas connus sous ce nom, ce sont aujourd'hui les réseaux sans fil les plus utilisés en France. Les technologies cellulaires tel que le GSM (Global *System for Mobile Communication*), le GPRS (*General Packet Radio Service*) et l'UMTS (*Universal Mobile Telecommunication System*) font ou feront partie de ce type de réseau (voir ci-dessous pour plus de détaille).

4. Les réseaux sans fil de type "WLAN" (La norme 802.11)

La norme IEEE 802.11 (ISO/IEC 8802-11) est un standard international décrivant les caractéristiques d'un réseau local sans fil (WLAN), ce dernier est utilisée comme prolongation de l'infrastructure des LAN. On trouve les normes IEEE 802.11b et 802.1a. La norme IEEE 802.11b s'appelle commercialement *Wi-Fi* pour *Wirless Fidelity*. Elle utilise la bande des 2,4 Ghz et permet un débit de 11 Mb/s. La norme IEEE 802.11a, appelée *Wi-Fi 5*, utilise la bande des 5 Ghz et permet un débit de 54 Mb/s.
Il existe également de nombreuses technologies propriétaires utilisant la bande des 2,4 Ghz, concurrentes aux normes IEEE mais abandonnées car elles sont supplantées par 802.11, comme *Home RF* d'Intel ou *OpenAir*. Une norme européenne défini par l'ETSI incluant d'origine la qualité de service et la gestion dynamique des fréquences et utilise également la bande des 5 GHz, est appelée *Hiperlan 2*, mais il semble difficile de prévoir un avenir à la normalisation de l'ETSI dans ce domaine car celle-ci n'est pas soutenue par les industriels.
Les réseaux sans fils doivent effectuer un compromis entre la portée et le débit disponibles. Différentes évolutions sont en cours aussi bien pour permettre des extensions pour la sécurité, la qualité de service et le *handover* que pour améliorer le débit et la couverture.
Elle définit aussi une partie des couches de bases du modèle OSI : la couche physique et la couche liaison de données.
Le premier service de la norme 802.11 est de fournir l'unité de données de service MAC (*Medium Access Control* - contrôle d'accès au medium) (MSDU : *MAC Service Data Units*) entre une paire au niveau de contrôle de la liaison logique (LLC : *Logical Link Controls*). Typiquement, une carte radio (*Radio Card*) et AP fournissent des fonctions de la norme 802.11 [1].

i. Les caractéristiques (*Features*)

La norme 802.11 fournit la fonctionnalité de MAC et PHY pour une connexion *wireless* des stations fixes, nomades ou mobiles se déplaçant aux vitesses piétonnières ou véhiculaires dans une zone locale [23]. La norme 802.11 tient compte des différences suivantes entre les réseaux filaires et les réseaux sans fil (WLANs) :

- **Gestion de l'alimentation (*Power Management*):** La plupart des cartes de réseau (*Network Interface Card* -NIC) pour WLAN sont disponibles dans le format de PCMCIA, ainsi on peut équiper des ordinateurs portables avec une connexion *wireless*. Le problème, est que l'interface réseau à besoin d'une batterie pour. L'addition d'un NIC de WLAN à un ordinateur portable peut rapidement vider les batteries. Les experts de IEEE 802.11 ont développé des solutions pour conserver l'énergie de la batterie, tel que par exemple le passage en mode de veille pour la carte réseau quand il n'y a pas de transmissions à effectuer.
- **La largeur de la bande:** Dans L'industrie, le milieu académique et médical la largeur de la bande de fréquence utilisée n'est pas grande, maintenant des débits plus petits qu'est offert pour certaines applications. Cependant les experts d'IEEE 802.11 ont adoptés des méthodes de compression pour une meilleure utilisation de la bande passante disponible.

- ✧ **La sécurité:** Les signaux de WLAN peuvent être reçus sans avoir besoin d'une connexion filaire, tel que câble coaxial ou fibre optique. Du point de vu de la sécurité WLAN ont une zone beaucoup plus grande à protéger. Le comité de normalisation responsable de définition des mécanismes de sécurité pour la série de protocole IEEE 802 a développé de solution de sécurité pour IEEE 802.11.
- ✧ **L'adressage :** La topologie d'un réseau sans fil est dynamique, ce qui entraîne que l'adresse de destination ne correspond pas toujours à l'endroit de la destination. Ceci pose un problème lorsqu'on achemine des paquets à travers le réseau vers la destination prévue. La recommandation 802.11f concernant le protocole interne de point d'accès (*Inter Access Point Protocol* - IAPP) résout le problème.

ii. La topologie

Un LAN 802.11 est basé sur une architecture cellulaire, du point de vue de topologie, 802.11 définit deux modes d'opération : le mode infrastructure BSS (*Basic Service Set*)(voir figure 9.b) et le mode ad-hoc IBSS (*Independant Basic Service Set*) (voir figure 9.a).
La topologie du mode ad-hoc est très simple et l'ensemble des stations communique directement, par paires, sans aucune fonction de relais de messages. Le mode infrastructure est beaucoup plus répandu que le mode ad-hoc et il définit un élément central, le point d'accès - AP (*Access Point*). Tous les messages passent par le point d'accès qui les relaie localement vers leur destination.

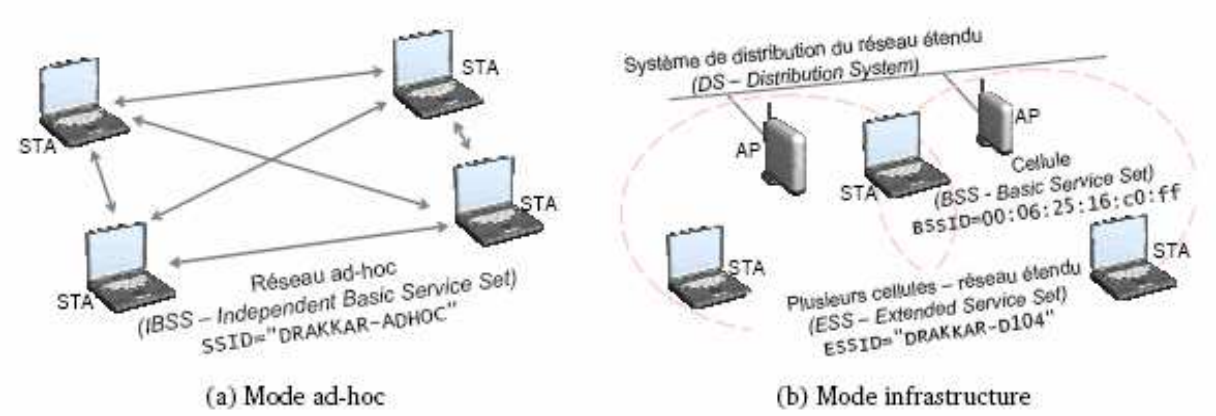

Figure 9: Topologie d'un réseau sans-fil (IEEE 802.11).

iii. L'architecture protocolaire

La norme 802.11 s'attache à définir les couches basses du modèle OSI pour une liaison sans fil utilisant des ondes électromagnétiques, c'est-à-dire :

- ✧ La couche physique (notée parfois couche PHY), proposant trois types de codage de l'information :
  - o *Frequency Hopping Spread Spectrum* (FHSS) dans la bande 2.4 Ghz,
  - o *Direct Sequence Spread Spectrum* (DSSS) dans la bande 2.4 Ghz,
  - o *InfraRed* (IR).

- La couche liaison de données, constitué de deux sous-couches :
  - Le contrôle de la liaison logique (*Logical Link Control* ou LLC),
  - Le contrôle d'accès au support (*Media Access Control* ou MAC).

La couche MAC 802.11 est responsable en plus des fonctions standards remplies par les couches MAC, des fonctions qui sont typiquement relatives aux couches supérieures, comme la Fragmentation, la retransmission des paquets et l'*Acknowledges*.
L'architecture logique 802.11 de la norme qui s'applique à chaque station se compose d'un MAC simple et d'un ou plusieurs PHYs (voir figure 10).

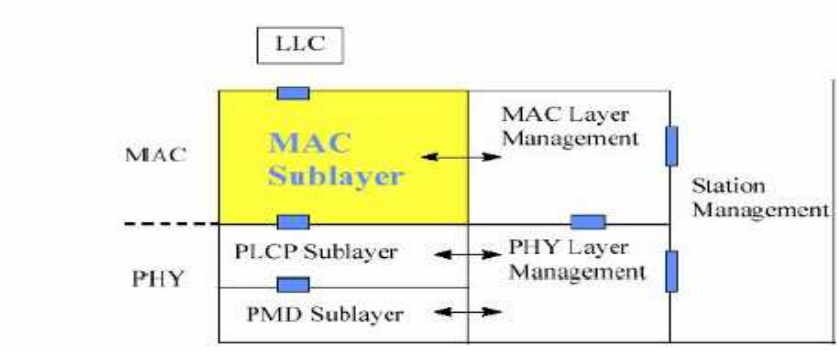

Figure 10 : Architecture protocolaire d'IEEE 802.11.

PLCP: *Physical Layer Convergence Procedure.*
PMD: *Physical Medium Dependent.*

- L'entité MAC
  - mécanisme d'accès de base,
  - fragmentation,
  - chiffrage.
- l'entité MAC Layer Management
  - synchronization,
  - gestion de puissance,
  - roaming,
  - MAC MIB.
- Physical Medium Dependent Sublayer (PMD)
  - modulation et codage.
- PHY Layer Management
  - canal accordant (channel tuning),
  - PHY MIB.
- Station Management
  - interagit avec MAC Management et PHY Management.

II. Les réseaux cellulaires

Dans cette section nous allons présenter brièvement chacune des normes GSM, GPRS et UMTS, tout en insistant sur le derniers qui va être l'objet de notre simulation après.

1. La Notion de réseau cellulaire

Les réseaux de téléphonie mobile sont basés sur la notion de cellules, c'est-à-dire des zones circulaires se chevauchant afin de couvrir une zone géographique. Les réseaux cellulaires reposent sur l'utilisation d'un émetteur-récepteur central au niveau de chaque cellule, appelée "station de base " (en anglais *Base Transceiver Station*, notée BTS). Plus le rayon d'une cellule est petit, plus la bande passante disponible est élevée. Ainsi, dans les zones urbaines fortement peuplées, des cellules d'une taille pouvant avoisinée quelques centaines mètres seront présentes, tandis que de vastes cellules d'une trentaine de kilomètres permettront de couvrir les zones rurales. Dans un réseau cellulaire, chaque cellule est entourée de 6 cellules voisines (c'est la raison pour laquelle on représente généralement une cellule par un hexagone voir figure 11). Afin d'éviter les interférences, des cellules adjacentes ne peuvent utiliser la même fréquence. En pratique, deux cellules possédant la même gamme de fréquences doivent être éloignées d'une distance représentant deux à trois fois le diamètre de la cellule.

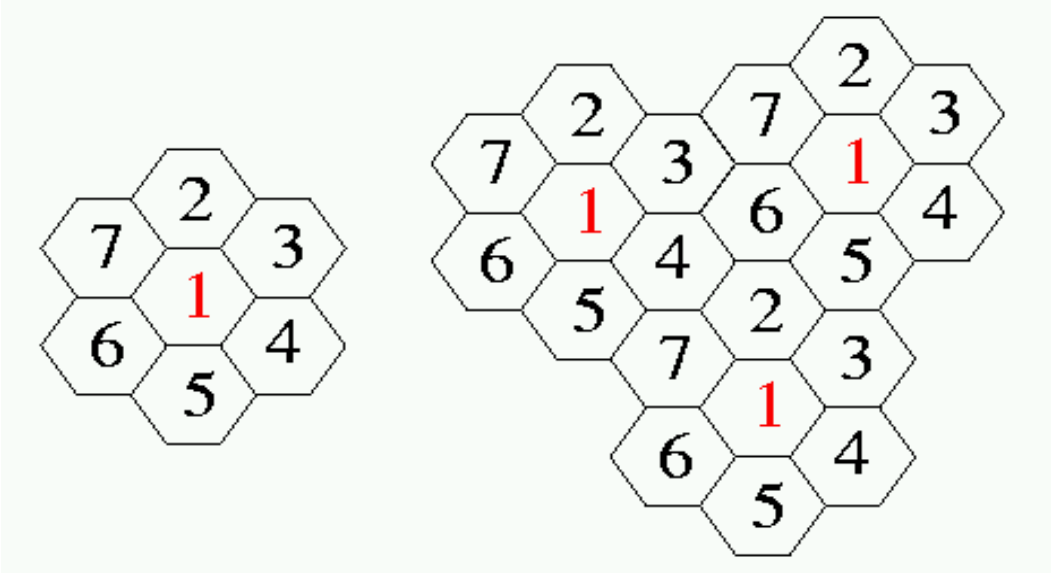

Figure 11: Figure représentant un motif élémentaire (à gauche) et un ensemble de motifs dans un réseau (à droite).

2. GSM

a. La présentation du réseau GSM

Le réseau GSM (*Global System for Mobile communications*) est issue d'un effort soutenu de standardisation mené à l'ETSI (Organe européen de Normalisation en télécommunications) et aussi le standard de téléphonie dit "de seconde génération " (2G) car, contrairement à la première génération de téléphones portables, les communications fonctionnent selon un mode entièrement numérique. Baptisé "Groupe Spécial Mobile" à l'origine de sa normalisation en 1982, il est devenu une norme internationale en 1991.Le standard GSM utilise les bandes de fréquences 900 MHz en Europe et 1800 MHz. Aux Etats-Unis par contre, la bande de fréquence utilisée est la bande 1900 MHz. La norme GSM autorise un débit maximal de 9,6 kbps, ce qui permet de transmettre la voix ainsi que des données numériques de faible volume, par exemple des messages textes (**SMS**, pour *Short Message Service*) ou des messages multimédias (**MMS**, pour *Multimedia Message Service*). Dans cette section, nous passerons en revue différents aspects de la technologie GSM: notion de réseau cellulaire, puis nous détaillons l'architecure du réseau GSM.

b. L'architecture du réseau GSM

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

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

Les éléments de l'architecture d'un réseau GSM sont repris sur le schéma de la figure 12.

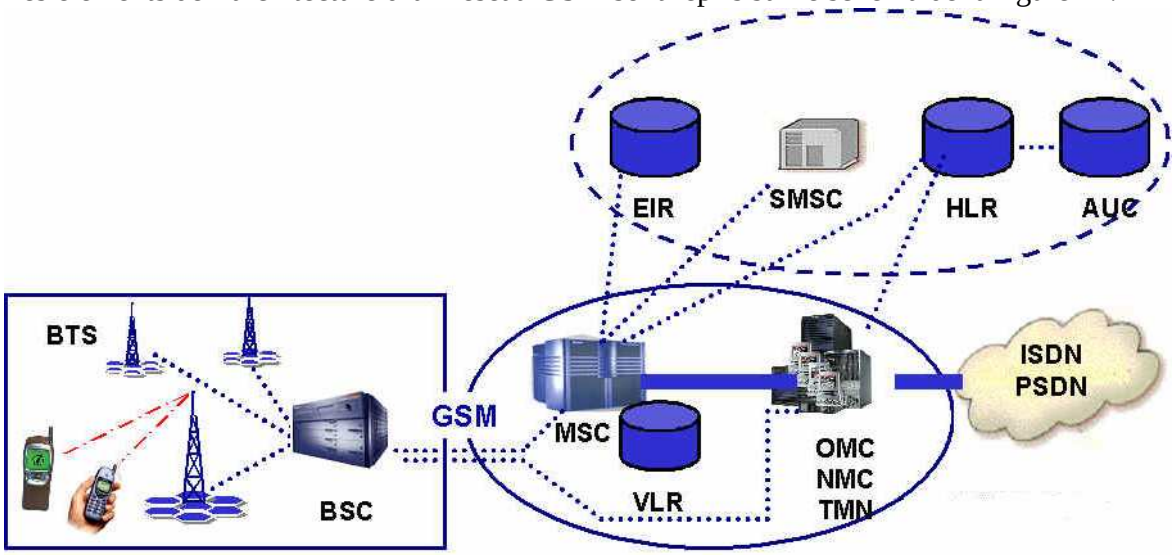

Figure 12: Architecture du réseau GSM.

i. Le sous-système radio

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

- ✓ **Le mobile**
- ✓ **La station de base (BTS)**
- ✓ **Le contrôleur de station de base (BSC)**

ii. Le sous-système réseau

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

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

- ✓ **Le centre de commutation mobile (MSC)**
- ✓ **L'enregistreur de localisation nominale (HLR)**
- ✓ **Le centre d'authentification (AuC).**

Le centre d'authentification remplit cette fonction de protection des communications. Pour ce faire, les normes GSM prévoient deux mécanismes:

- ✧ **Le chiffrement des transmissions radio,**
- ✧ **L'authentification des utilisateurs du réseau au moyen d'une clé K_i.**

On peut dès lors distinguer trois niveaux de protection:

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

- ✓ **L'enregistreur de localisation des visiteurs (VLR)**
- ✓ **L'enregistreur des identités des équipements (EIR)**

iii. Le centre d'exploitation et de maintenance

Cette partie du réseau regroupe trois activités principales de gestion:

- ✧ **La gestion administrative,**
- ✧ **La gestion commerciale,**
- ✧ **La gestion technique.**

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

3. GPRS

a. Introduction

Le service GPRS, *General Packet Radio Service*, définit une architecture de réseaux à commutation par paquets avec gestion de la mobilité et accès par voie radio. Un réseau GPRS comprend des abonnés propres, mobiles ou fixes, et peut être relié à divers réseaux de données fixes reposant sur différents protocoles : IP mais aussi X.25, protocole orienté connexion de l'ITU (*International Telecommunication Union*). Notons que le protocole réseau, quel qu'il soit, est désigné sous le terme générique de PDP, *Packet Data Protocol*.

Dans le cas où GPRS offre un service IP, un terminal GPRS dispose d'une adresse IP dont le champ réseau est spécifique au réseau GPRS, d'autre part tout mobile GPRS dispose d'un IMSI et il est identifié au sein du réseau avec son IMSI.
Les recommandations GPRS reprennent l'architecure du BSS mais définissent une architecture de réseau fixe différente du NSS, ce dernier étant plutôt dédié à la commutation de circuit. La gestion de l'itinérance reprend les principes et l'architecture de GSM. Avec GPRS, le BSS devient un sous-réseau d'accès multiservice : il peut être relié à un NSS classique et à un **réseau fédérateur GPRS**. Il est cependant possible de déployer un réseau GPRS pur sans NSS. Les principes de GPRS reprennent les concepts d'IP mobile et de CDPD, *Cellular Digital Packet Data*, développé aux Etats-Unis.
Un des intérêts du GPRS est de profiter du multiplexage statistique dans le BSS par l'utilisation de la transmission par paquets sur la voie radio. Ainsi, plus d'un slot par trame TDMA peuvent être utilisés avec GPRS ce qui permet d'atteindre un débit théorique jusqu'à **171.2 kbit/s**.
Notons que les fonctions de sécurité disponibles dans GSM en mode circuit sont également prévues dans GPRS : authentification de l'abonné, confidentialité de l'identité de l'utilisateur et des informations transmises.

b. Les caractéristiques du GPRS

- ✧ Commutation de paquet (de données) dans un réseau GSM (phase 2+)
- ✧ Débit variable (9,6Ks à 144Ks)
- ✧ Point à Point/ Point à MultiPoint
- ✧ Facturation : au volume

c. L'architecture générale du GPRS

i. Réseau fédérateur GPRS

Le réseau GPRS est un réseau à datagrammes IP constitué de routeurs IP. Il existe deux types de routeurs IP : ceux qui permettent aux paquets de circuler à l'intérieur d'un même réseau

GPRS et ceux qui permettent aux paquets de migrer vers d'autres réseaux de données (IP, X25, autre réseau GPRS), appelés plus généralement réseaux PDP :

- ✧ Le nœud de service GPRS (SGSN, Serving GPRS Support Node) est relié aux BSC du sous-système radio (BSS) de GSM et gère les MS présentes dans une zone donnée. Son rôle est de délivrer des paquets aux MS, issus du PLMN.
- ✧ Le nœud passerelle GPRS (GGSN, Gateway GPRS Support Node) sert de passerelle entre les SGSN du réseau GPRS et les autres réseaux de données. Il permet aux paquets issus de réseaux PDP externes d'être acheminés vers le SGSN de leur destinataire ou de router les paquets issus du réseau GPRS auquel il appartient vers le réseau extérieur adéquat.

L'ensemble des SGSN, GGSN et éventuels routeurs IP vers des réseaux IP extérieurs forme le réseau fédérateur GPRS. Chaque SGSN et GGSN possède une adresse IP fixe au sein de ce réseau.

ii. Architecture en couches

Deux plans sont à distinguer dans GPRS : le plan usager (transmission) et le plan de contrôle (signalisation).

i. Plan usager ou de transmission

- ✧ **Côté réseau fédérateur :** le routage vers des terminaux utilise le principe de **l'encapsulation** et des **protocoles tunnel GTP** (*GPRS Tunnel Protocol*). L'encapsulation consiste à placer une suite d'éléments binaires **PDU** (*Packet Data Unit*) issus d'une couche n entre l'en-tête et la séquence de contrôle d'erreur de la couche inférieure n-1. Le protocole de la couche n-1 ne s'intéresse pas à la nature des données transportées par la couche n. Dans GPRS, des datagrammes IP ou des paquets X25 sont encapsulés dans des datagrammes IP. Les datagrammes IP contiennent les adresses des SGSN et GGSN concernés. Le réseau IP se comporte comme un tunnel vis à vis des paquets X25 qui entrent à une extrémité du réseau pour en sortir à l'autre bout. Le protocole GTP du SGSN et du GGSN établit une **liaison de données** entre la station mobile et son SGSN en utilisant le principe du passage en tunnel entre le SGSN et le GGSN. Le protocole GTP s'appuie soit sur TCP, *Transport Control Protocol* (fiable), soit sur UDP, *User Datagram Protocol* (non fiable mais temps-réel) selon la nature des données à transmettre. La norme requiert que les deux types de protocoles de transport soient disponibles entre le SGSN et le GGSN dans le plan de transmission.
- ✧ **Côté BSS :** le **protocole SNDCP** (*Subnetwork Dependent Convergence Protocol*) du SGSN multiplexe plusieurs PDU de différents réseaux PDP, et effectue une compression et une segmentation des PDU de niveau réseau (appelés PDU PDP) avant de les transmettre à la couche LLC.

ii. Plan de contrôle ou de signalisation

Lorsqu'un réseau combine le mode GPRS-paquet et le mode GSM-circuit, il est nécessaire que le SGSN dialogue avec les HLR, EIR et le MSC/VLR pour coordonner la gestion de la localisation. De même le GGSN dialogue avec le HLR. Les dialogues utilisent les **protocoles**

MAP (SGSN – HLR ou EIR et GGSN – HLR) et **BSSAP+** (SGSN – MSC/VLR), cette dernière est une adaptation du BSSAP.
Sur le réseau d'accès, la couche réseau comprend deux sous-couches :

- ✧ La sous-couche **SM** (Session *Management*) permet au mobile de demander la mémorisation d'un contexte PDP (*Packet Data Protocol*) dans le SGSN et GGSN. Ainsi les paquets du réseau PDP externe sont routés par le GGSN vers le SGSN sans consultation de la base de données de localisation.
- ✧ La sous-couche **GMM** (*GPRS Mobility Management*) gère l'itinérance du terminal mobile dans le réseau.

iii. Couches communes aux plans de signalisation et de transmission

- ✧ La couche **LLC**, *Logical Link Control*, assure des échanges de données entre le mobile et le SGSN, elle prend également en charge le chiffrement spécifique à GPRS.
- ✧ La couche **RLC** (*Radio Link Control*) fournit une liaison entre le mobile et le BSS. Ce protocole dépend étroitement de l'interface radio utilisée.
- ✧ La couche **MAC** (*Medium Access Control*) contrôle l'accès au canal radio, elle alloue des ressources au mobile uniquement lorsque celui-ci a des données à transmettre et permet ainsi le **multiplexage statistique**.
- ✧ Le **BSSGC** (*BSS GPRS Control*) transporte des informations de routage et de qualité de service entre le BSS et le SGSN, il permet la retransmission automatique des trames par le BSS et assure que le BSS est transparent aux données utilisateurs GPRS.

La figure suivante montre l'architecture du réseau GPRS :

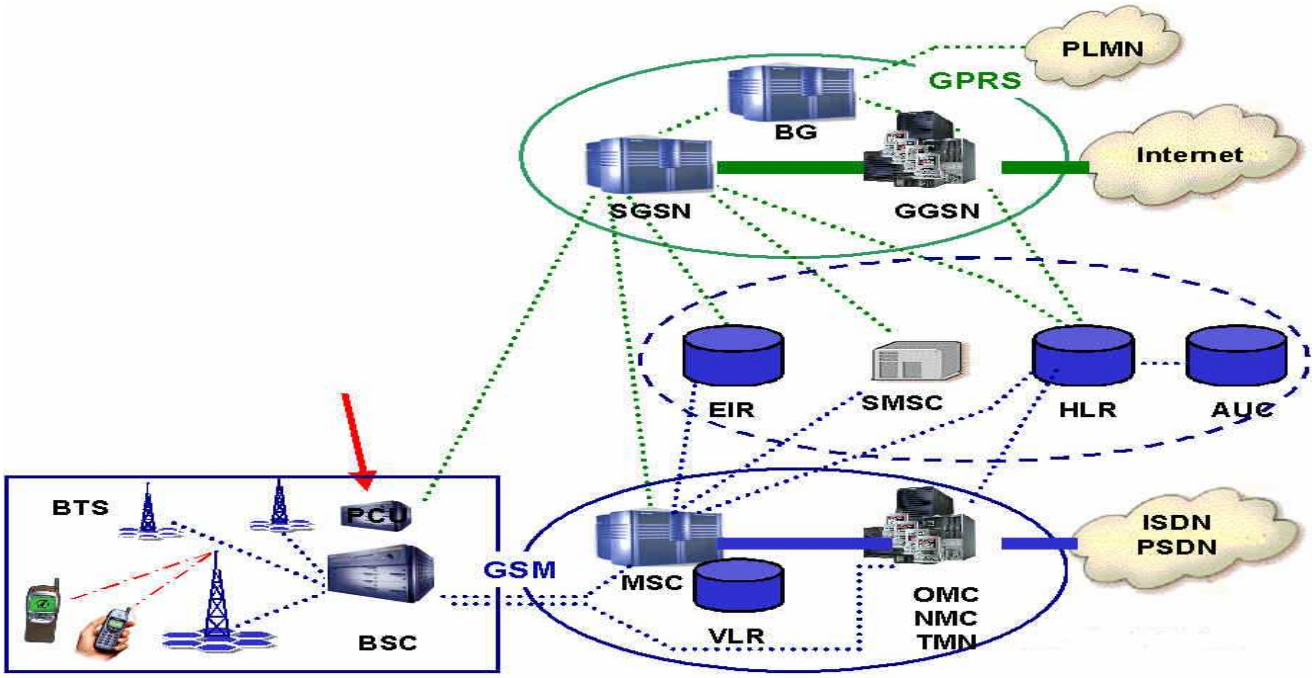

Figure 13 : Architecture du réseau GPRS

La norme GPRS étant décrite, il faut alors définir la norme UMTS et voir si elle a des points communs avec la précédente.

4. UMTS

a. Introduction

UMTS, *Universal Mobile Telecommunications Service*, est l'approche européenne aux systèmes mobiles de la troisième génération (normalisé par ETSI) et il peut être vu comme "successeur" de GSM.

L'UMTS est conçu de manière à proposer les débits suivants :

- ✧ 144 kbits/s en environnement extérieur,
- ✧ 384 kbits/s en environnement urbain extérieur,
- ✧ 2 Mbits/s usager quasiment immobile et proche de l'antenne d'émission de la cellule.

Un système mondial requiert en effet des bandes de fréquences et un moyen d'utilisation communs. L'objectif a été partiellement atteint : en Europe et au Japon, la même interface air ou radio (WCDMA) doit être utilisée, mais en Amérique du Nord, aucun spectre supplémentaire n'est disponible (ils ont déjà été vendus pour les systèmes 2G), donc une autre technique sera utilisée.
UTRAN, *Universal Terrestrial Radio Interface Network*, est un compromis entre deux modes : FDD-WCDMA et TDD-WCDMA, c'est une solution mixte qui permet une utilisation complète des bandes des fréquences allouées par l'IMT-2000 (*International Mobile Telephony 2000*). En effet, les fréquences appariées devront être traitées en mode FDD-WCDMA tandis que les non-appariées devront être traités en mode TDD-WCDMA.

b. Constitution du réseau UMTS

Dans UMTS on trouve une séparation de la couche d'accès du reste du réseau, ce qui accroît l'évolutivité de la norme UMTS. Cela permettra de faire évoluer l'interface radio en minimisant les impacts sur les équipements du réseau.

c. Réseau cœur et réseau d'accès

Le réseau UMTS est composé d'un réseau cœur et d'un réseau d'accès. L'interface entre ces deux réseaux est appelée "Iu". Cette interface a été définie d'une manière aussi générique que possible afin d'être capable de connecter, en plus de l'UTRAN situé entre le relais radio appelé NodeB et le réseau coeur de l'UMTS, des réseaux d'accès de technologies différentes au réseau cœur de l'UMTS.

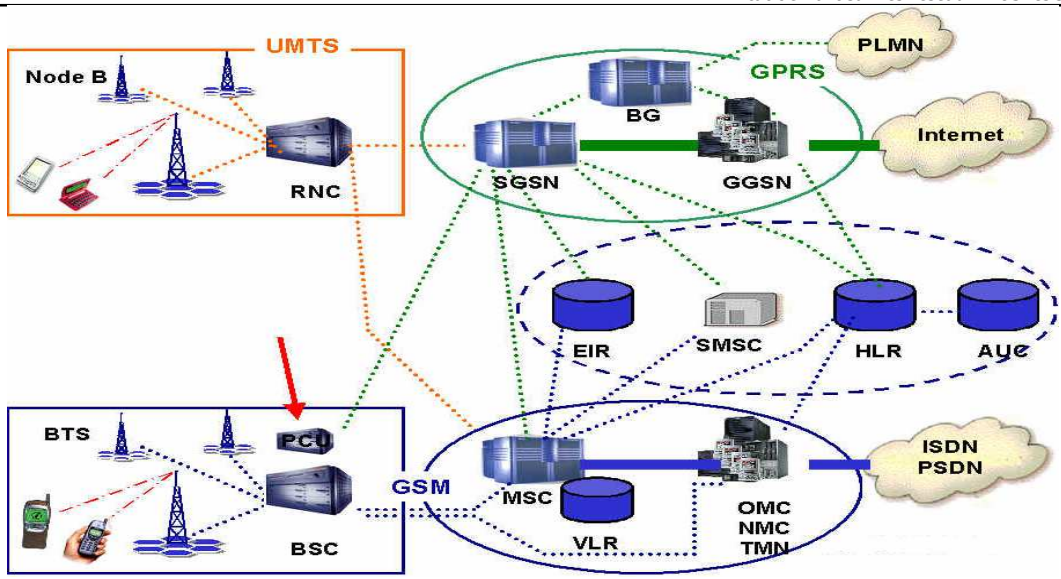

Figure 14 : Architecture du réseau UMTS avec les réseaux d'accès GSM et UTRAN

i. Le réseau cœur

Le réseau cœur de l'UMTS est scindé en 2 domaines de service :

- ✧ Le CS (*Circuit Switched*) domain,
- ✧ Le PS (*Packet Switched*) domain.

Le domaine CS est utilisé pour la téléphonie tandis que le domaine PS permet la commutation de paquets (utilisé pour les données, Internet...). Ainsi les téléphones de 3° génération peuvent gérer simultanément une communication paquet et circuit. Cette notion de domaine permet de modéliser la notion de service dans le réseau cœur et donne la possibilité de créer ultérieurement d'autres domaines de service. Les éléments du réseau cœur sont répartis en 3 groupes, comme l'illustre la figure ci-dessous. Le domaine CS comprend le MSC, le GMSC et le VLR. Le domaine PS comprend le SGSN et le GGSN. Le dernier groupe comprend les éléments communs aux domaines PS et CS, le HLR, l'EIR, et l'AuC.

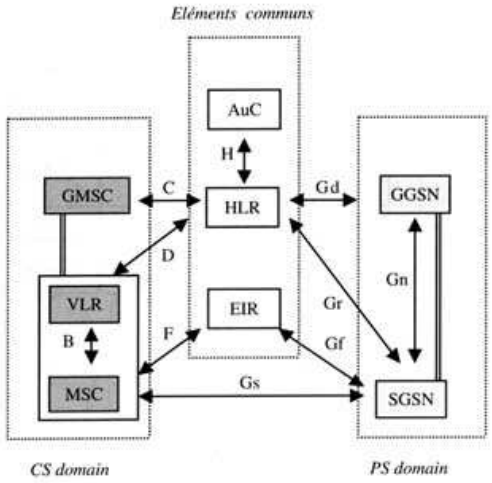

Figure 15 : Le réseau cœur de l'UMTS

1er. Les composants du réseau cœur

Les composants du réseau cœur sont :

Le groupe des éléments communs

- Le HLR
- L'AuC (*Authentication Center*)
- L'EIR

Le groupe des éléments du domain CS

- Le **MSC** (*Mobile-services Switching Center*) est un commutateur de données et de signalisation. Il est chargé de gérer l'établissement de la communication avec le mobile.
- Le **GMSC** (*Gateway MSC*) est un MSC un peu particulier servant de passerelle entre le réseau UMTS et le RTCP (Réseau Téléphonique Commuté Public). Lorsqu'on cherche à joindre un mobile depuis un réseau extérieur à l'UMTS, l'appel passe par le GMSC, qui effectue une interrogation du HLR avant de router l'appel vers le MSC dont dépend l'abonné.
- Le **VLR** (*Visitor Location Register*) est une base de données attachée à un ou plusieurs MSC. Le VLR est utilisé pour enregistrer les abonnés dans une zone géographique appelée LA (*Location Area*). Le VLR contient des données assez similaires à celles du HLR. Le VLR mémorise pour chaque abonné plusieurs informations telles que l'identité temporaire du mobile (pour limiter la fraude liée à l'interception et à l'utilisation frauduleuse de l'IMSI) ou la zone de localisation (LA) courante de l'abonné.

Le groupe des éléments du domaine PS

- Le **SGSN** (*Serving GPRS Support Node*).
- Le **GGSN** (*Gateway GPRS Support Node*).

2e. Le réseau d'accès UTRAN

La figure suivante illustre les éléments du réseau d'accès :

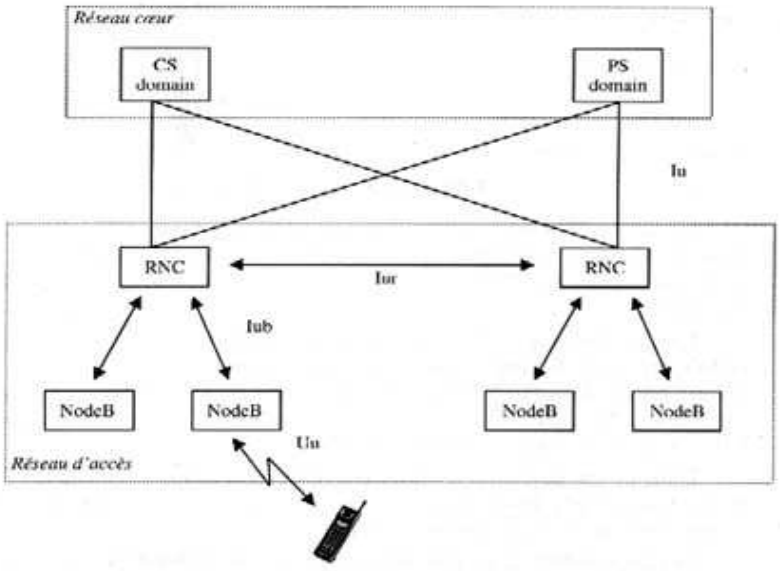

Figure 16 : Réseau d'accès UTRAN

Les différents constituants

- Le **NodeB** : son rôle principal est d'assurer les fonctions de réception et de transmission radio pour une ou plusieurs cellules de l'UTRAN.
- Le RNC (*Radio Network Controller*) : son rôle principal est le routage des communications entre le NodeB et le réseau cœur.

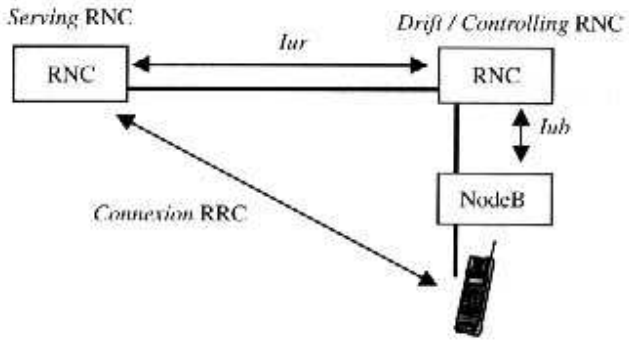

Figure 17 : RNC et NodeB

Lorsqu'un mobile est en communication (cf figure ci-dessus), une connexion RRC (*Radio Resource Control*) est établie entre le mobile et un RNC de l'UTRAN. Le RNC en charge de cette connexion est appelé SRNC (*Serving RNC*). Lorsque l'usager se déplace dans le réseau, il peut être conduit à changer de cellule en cours de communication, et peut même se retrouver dans une cellule faisant partie d'un NodeB ne dépendant plus de son SRNC. On appelle alors *Controlling RNC*, le RNC en charge de ces cellules distantes. D'un point de vue RRC, le RNC distant est appelé drift RNC. Les données échangées entre le serving RNC et le mobile transitent par les interfaces Iur et Iub. Le drift RNC joue donc le rôle de simple routeur vis à vis de ces données.

L'interface radio de l'UTRAN

L'Annexe II donne plus des détaille.

CONCLUSION

Nous avons présenté dans ce chapitre les différents réseaux mobiles sans fils, au début les réseaux sans fil et en particulier IEEE 802.11 sont présenter, par la suite les principaux réseaux de télécommunication sont détailler, cependant il reste de parler de l'impact de la mobilité sur ces différents réseaux c'est ce que essaye le chapitre suivant montré.

CHAPITRE 3

État de l'art sur la Mobilité

Chapitre III : La mobilité dans les réseaux sans fils

Dans le présent chapitre nous présentons en premier lieu les différents types de mobilité, en second lieu nous abordons la notion de *Handover* (transfert automatique de communication), puis nous détaillons en dernier lieu les principaux protocoles de mobilité.

INTRODUCTION

La mobilité se traduit par la possibilité que certaines entités peuvent être déplacées entre des points d'attachement différents. Nous énumérons quelques exemples, illustrés dans la figure 18 :

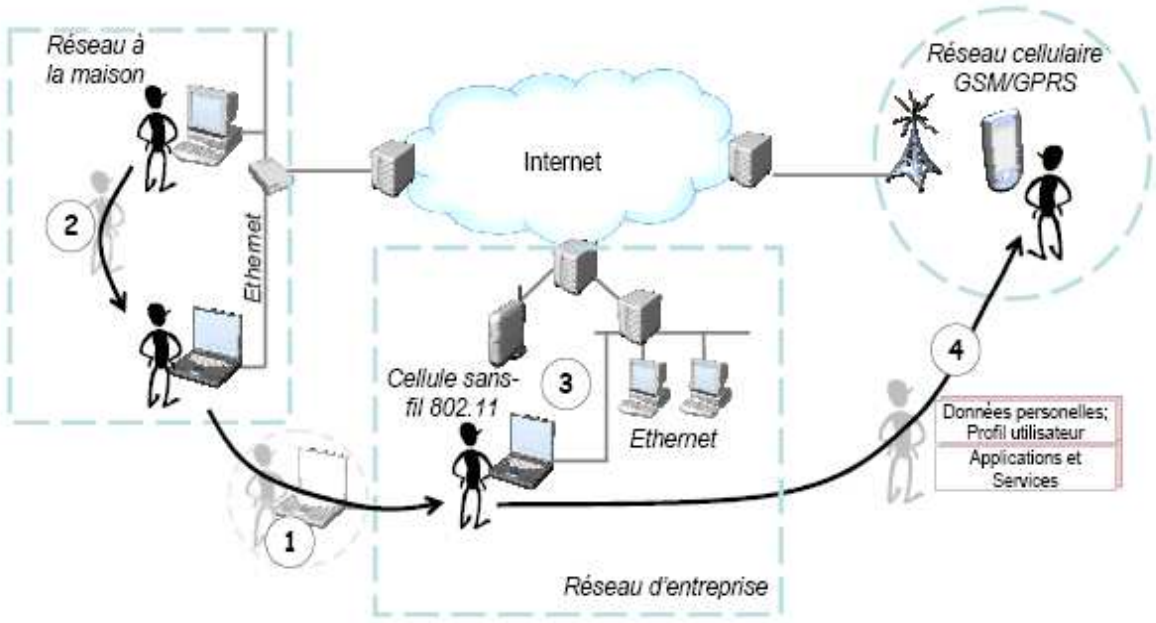

Figure 18: Types de mobilité

- (1) Un terminal est physiquement déplacé à un autre endroit et reconnecté à l'Internet par le biais d'un nouveau réseau;
- (2) Un utilisateur décide d'utiliser un nouveau terminal;
- (3) Un terminal connecté simultanément à plusieurs réseaux change l'interface active;
- (4) Parallèlement au déplacement de l'utilisateur, des données personnelles et applications portables sont migrées sur un autre terminal;
-

I. Classification de la mobilité dans les réseaux

La mobilité est souvent gérée en séparant la micro mobilité de la macro mobilité. La macro mobilité concerne les mouvements des utilisateurs à grande échelle. La micro mobilité désigne les mouvements des mobiles à petite échelle, dans un même domaine [23].

1. La macro Mobilité

La macro mobilité désigne les mouvements inter-sites des mobiles. Elle désigne aussi la possibilité pour un utilisateur mobile de quitter son réseau d'abonnement pour se rendre dans un autre domaine du réseau IP. Lors de son arrivée dans ce nouveau domaine, l'utilisateur s'approprie une adresse temporaire puis s'assure de l'exécution de son enregistrement auprès de l'agent local de sa zone d'abonnement. Une fois ces formalités remplies, l'utilisateur est en mesure de poursuivre ses déplacements. Elle se préoccupe de la gestion du déplacement du noeud mobile à grande échelle, entre différents réseaux d'accès sans fil reliés à l'Internet ou autres. Une amélioration célèbre dans le domaine de la macro mobilité est le protocole Mobile IP qui permet aux stations IP de changer leur point d'attache entre différents réseaux administratifs. Mais malheureusement, les mécanismes de Mobile IP [13] présentent certains inconvénients, notamment un temps de latence important.

2. La micro Mobilité

On parle de la micro mobilité quand la mobilité d'une hôte a lieu à l'intérieur d'un domaine et reste invisible pour les hôtes externes. Une fois qu'un *datagramme* destiné à l'hôte mobile arrive à la bordure du domaine, le protocole de micro-mobilité doit assurer par des moyens et fonctions spécifiques la remise du *datagramme* à l'hôte mobile à l'intérieur du domaine. Les objectifs des protocoles de micro-mobilité sont d'assurer un *handover* rapide avec peu de pertes de paquets, tout en préservant la transparence vis-à-vis des hôtes correspondantes et couches supérieures, pour garder ouvertes les connexions TCP actives et pour gérer la mobilité dans des aires de taille limitée (domaine, site). De nombreux protocoles aux caractéristiques très variées ont été proposés pour la gestion de la micro-mobilité. Parmi ces solutions, on cite HAWAII[26] (*Handoff-Aware Wireless Access Internet Infrastructure*), *Cellular IP* [27] et MIP-RR (*Mobile IP Regional Registration*). Cependant, *Cellular IP* et Hawaii n'utilisent pas le routage IP ordinaire.

II. Notion de Handover

Dans cette section nous parlons de la mobilité et de *handover*. Le *handover* ou transfert intercellulaire est la fonction qui autorise le passage d'une cellule à une autre sans interruption de la communication. La mobilité souvent utilisée pour les réseaux filaires et en particulier les réseaux IP, alors que la *handover* est employée pour les réseaux sans fil, elle est composante de la gestion de mobilité et se produit au niveau de la couche physique et liaison de données.

Le *Handover* (Europe) (ou *Handoff* (*North America*)) est le processus qui se produit quand un mobile "est remis" d'un point d'accès (AP – *Access Point*) à un autre, c.-à-d., le point d'accès que le mobile emploie change.

Nous distinguons plusieurs types de handover:

- ***Soft Handover :*** Le mobile peut communiquer avec l'ancien et le nouveau AP (voir figure 20).
- ***Hard Handover* :** Le mobile communique soit avec l'ancien soit avec le nouveau AP (voir figure 20).
- ***Seamless Handover*:** Le *Handover* est transparent pour l'utilisateur et l'application (par exemple : pas d'effet sur le trafic entrant et sortant du Mobile).
- ***Fast Handover* :** Le temps d'interruption est très faible pendant le *Handover*.
- ***Horizontal Handover* :** Lorsque la nouvelle cellule est de même nature que l'ancienne (voir figure 19).
- ***Vertical Handover :*** Lorsque la nouvelle cellule est de nature différente que l'ancienne (voir figure 19).

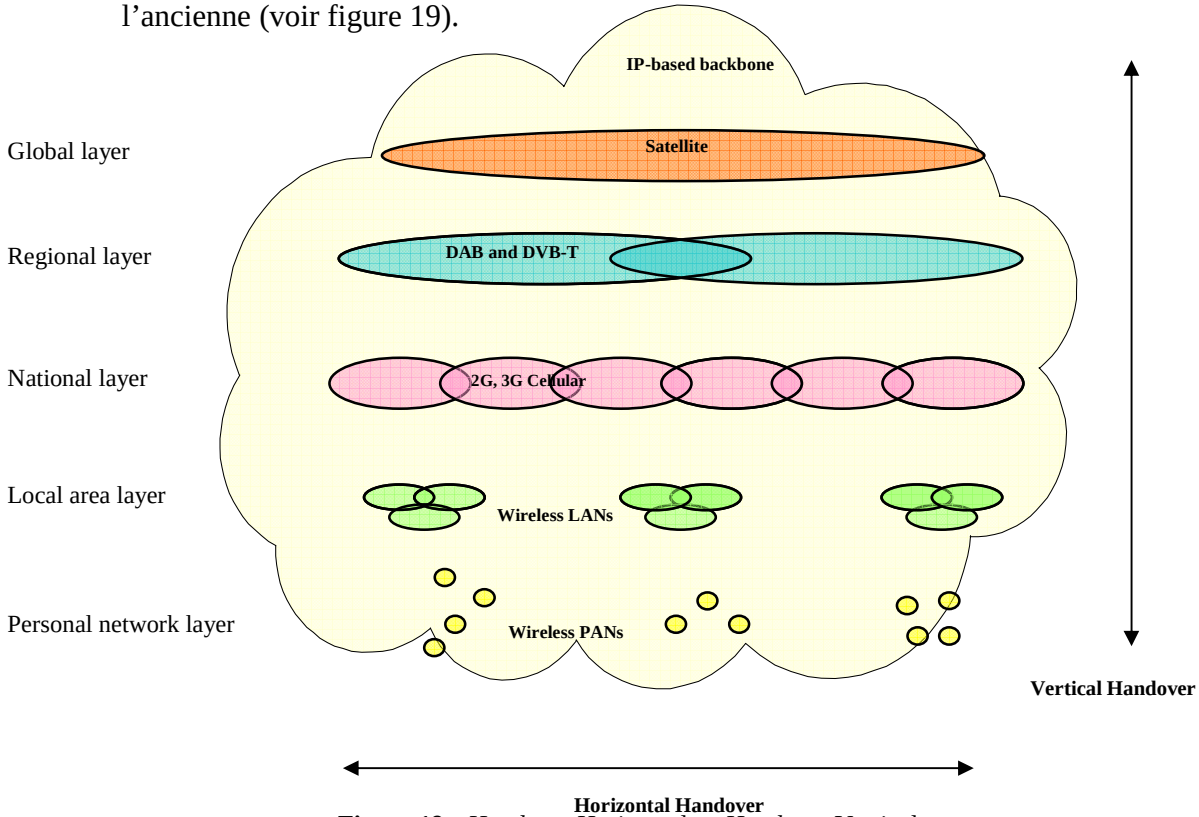

Figure 19 : *Handover* Horizontal vs *Handover* Vertical.

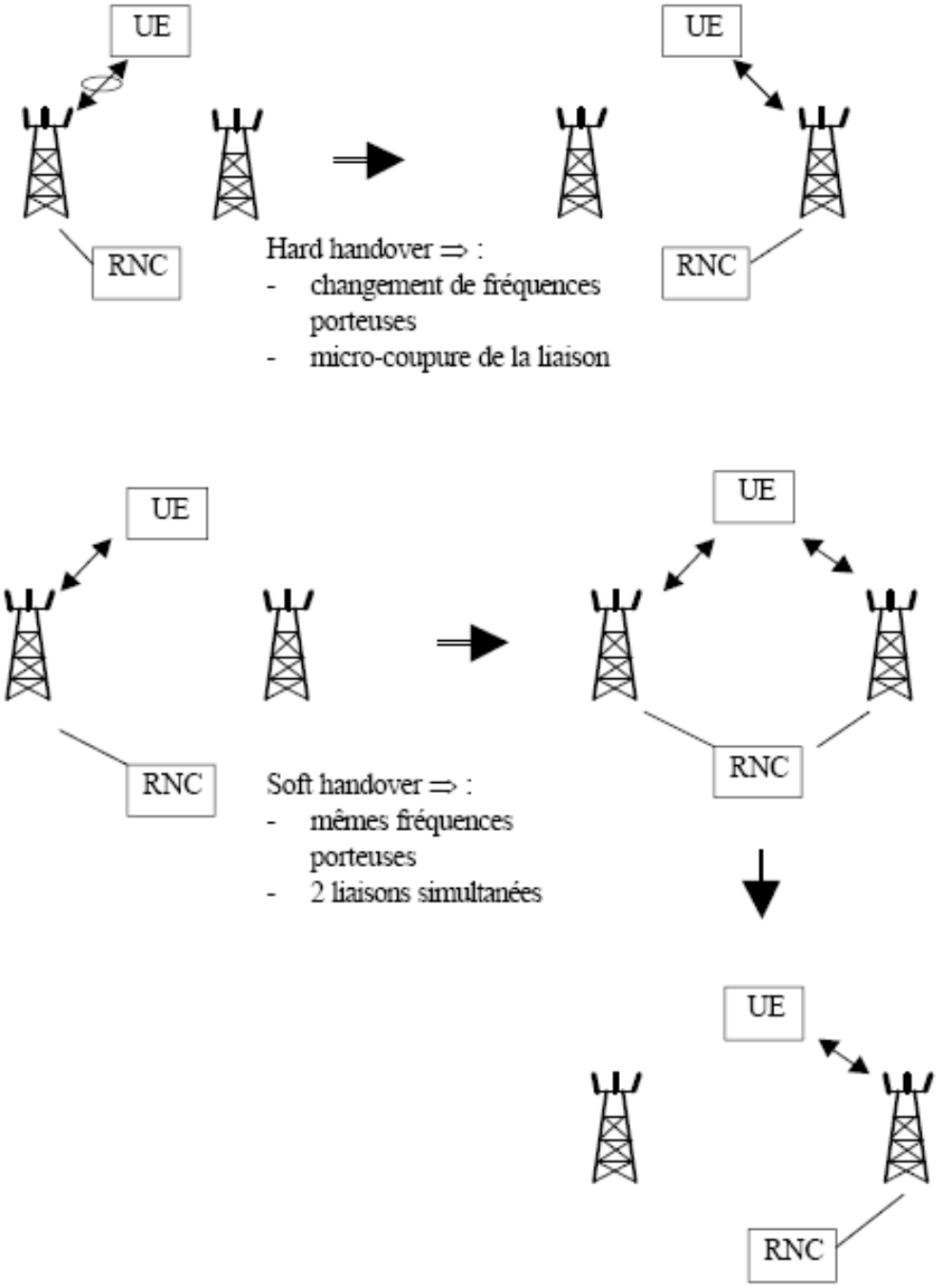

Figure 20 : *Soft Handover & Hard Handover*

1. Les étapes de Handover

De manière générale, la procédure de *handover* se réalise en trois phases principales.

- **Phase 1 :** Au cours de ses déplacements, le composant mobile mesure et évalue périodiquement le lien radio (la puissance du signal reçue, le taux d'erreurs binaires, etc). En cas de détection de l'affaiblissement du signal, le composant mobile sélectionne un composant d'accès offrant un meilleur signal et demande une association avec ce dernier;
- **Phase 2 :** Si l'association est acceptée, le composant mobile et le gestionnaire de la nouvelle zone s'authentifient. Une adresse temporaire est attribuée au composant mobile. Le transfert de la connexion vers le nouveau lien et la libération de l'ancien lien sont ensuite effectués;
- **Phase 3 :** Si l'association est refusée, le mobile continue à rechercher un composant d'accès avec lequel une association est possible. Les communications en cours continuent sur l'ancien lien.

2. Les protocoles de contrôle du Handover

Les procédures de *handover* impliquent l'utilisation d'un ensemble de protocoles pour signaler à une entité qu'un *handover* a été exécuté et que la connexion doit être redéfinie. Quand un mobile se déplace d'un point à un autre, il exécute la *handover* d'un point d'attachement à l'autre. Dans le *hard handover* la nouvelle connexion est établie après que l'ancienne est terminée, pour le *soft handover* le passage d'une cellule à l'autre sans aucune rupture de lien en maintenant le deux connexions simultanément jusqu'à ce que le transfert soit fini. La décision pour exécuter la *handover* peut être prise au niveau de réseau, dans *network-controlled handover (NCHO)*, au niveau de mobile, dans *mobile controlled handover (MCHO)* ou l'information peut être envoyée par le mobile et par la suite utilisée par l'entité de réseau pour prendre la décision de *handover*. Ceci s'appelle *mobile assisted handover (MAHO)*. L'entité qui décide du *handover* emploie quelques métriques, algorithmes, et mesures de performance afin de prendre la décision.

III. Handover dans les réseaux mobiles et fixes

1. Mobilité dans les réseaux filaires

Afin de mieux comprendre la mobilité, il est important d'étudier les protocoles de mobilité. Cette section présente quelques protocoles qui gèrent la mobilité.
Nous avons structuré ces protocoles en deux groupes principaux. À la première partie, nous avons décrit les protocoles de réseaux locaux sans fil et à la deuxième partie, les protocoles de réseaux Internet. Pour chaque protocole, nous avons décrit les architectures sur lesquelles il peut être déployé, les procédures qu'il définit ainsi que les couches protocolaires sur lesquelles il s'appuie.

a. Mobile IP

Le développement des extensions du protocole IP pour la mobilité des hôtes a débuté au sein de l'IETF (*Internet Engineering Task Force*) au début des années 90. Les extensions du protocole IP sont regroupées dans le protocole appelé *Mobile IP*, le même nom que le groupe

de travail qui les a introduit[1]. L'Internet a continué d'évoluer et des nouvelles problématiques et contraintes sont apparues.
En réponse, des nouvelles fonctionnalités et améliorations ont été proposées et ajoutées au standard spécifié initialement dans le RFC 2002[13].
Actuellement, les documents les plus récents qui spécifient les extensions pour la mobilité des hôtes sont le RFC 3344[14] pour IPv4 et le RFC 3775[11] pour sa version IPv6.
Mobile IP se veut une solution qui intervient exclusivement au niveau IP et qui fournit la transparence vis-à-vis des couches supérieures, y compris le protocole TCP. L'autre point important pris en compte dès le début dans la conception de *Mobile IP*, au moins pour sa version v4, a été la compatibilité avec les hôtes correspondants. Nous discutons dans cette section le protocole *Mobile IPv4*.

i. Les Caractéristiques

Le *Mobile IP* est spécifique pour la gestion de la macro-mobilité [25, 27]. Il permet à un noeud connecté à l'Internet de se déplacer librement d'un point à l'autre, sans perturber la connectivité bout à bout. Les noueds mobiles (MN) sont exigés pour sécuriser l'enregistrement de *Care-of-Address* (CoA) avec leur *Home Agent* (HA) duranr le *roaming* dans un domaine étranger. Si cependant des mécanismes de sécurité ne sont pas utilisés, le réseau peut être compromis par des attaques à distance de redirection par des noeuds malveillants. Les éléments et la terminologie qui composent un réseau géré par *Mobile IP* sont (voir la figure 21) :

- ✧ **Agent Mère (Home Agent - HA) :** un routeur situé dans le réseau administratif du mobile.
- ✧ **Agent Relais (Foreign agent -FA) :** un routeur situé dans le réseau visité par le mobile.
- ✧ **Nœud Mobile (Mobile Node -MN or STA in IEEE 802.11):** A la possibilité d'utiliser deux adresses IP : une adresse mère et une adresse mobile qui change à chaque point de connexion.
- ✧ **Nœud Correspondant (Correspondent Node -CN).**

Les besoins remplis par le protocole Mobile IP
Mobile IP a été créé pour répondre à des besoins précis :

- ✧ Un mobile doit être capable de communiquer avec d'autres machines après avoir changé son point d'attachement sur Internet
- ✧ Un mobile doit être capable de communiquer uniquement avec son adresse principale, indépendamment de sa localisation sur l'Internet,

[1] L'ancien groupe *mobileip* est maintenant divisé en deux groupes indépendantes, un pour chaque de deux versions IPv4 et IPv6.

- ✧ Un mobile doit pouvoir communiquer avec une autre machine, sans que celle-ci implémente le protocole Mobile IP,
- ✧ Un mobile ne doit par être plus exposé qu'une autre machine sur l'Internet.

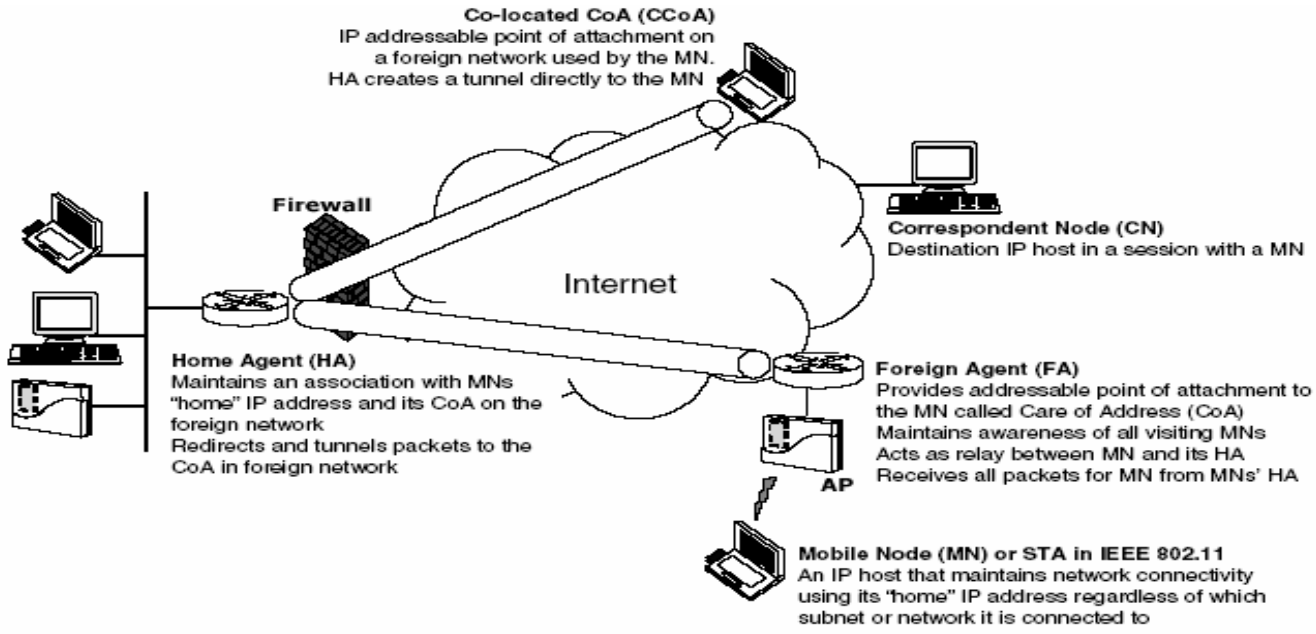

Figure 21: Les composantes de Mobiles.

CoA: *Care-of-Address* (Adresse temporaire).

ii. Architecture de Mobile IP

Dans *Mobile IP*, un hôte a toujours associé une adresse IP de base qui reste inchangée. Celle-ci correspond au sous-réseau d'origine de l'hôte mobile. Quand l'hôte se connecte dans un sous-réseau différent, il dispose d'une adresse temporaire, propre au nouveau point d'attachement. Il continue cependant d'utiliser son adresse IP fixe dans la communication avec ses correspondants. Dans le schéma d'opération présenté dans la figure 22, les paquets destinés à l'hôte mobile sont toujours adressés à son adresse de base. Un nœud spécial dans le sous-réseau d'origine, appelé agent mère, intercepte les paquets et les remet à l'emplacement actuel de l'hôte mobile.

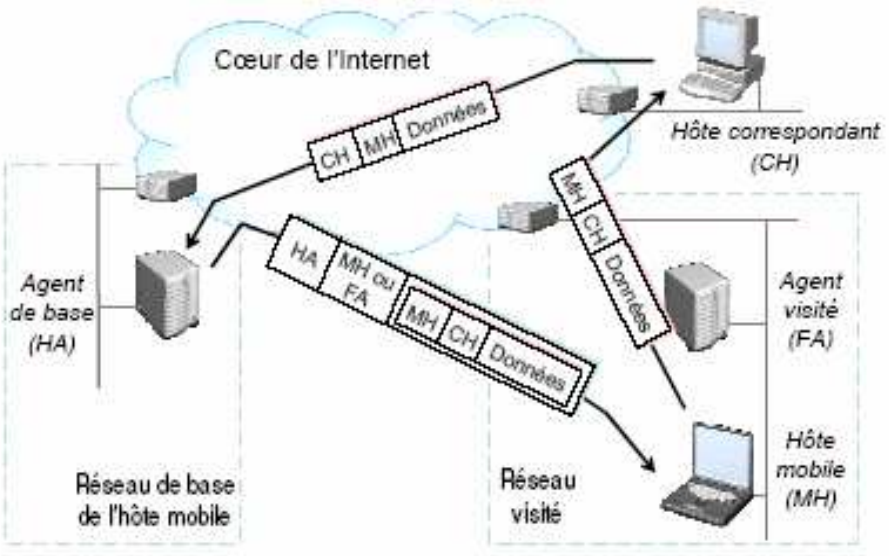

Figure 22: L'architecture de Mobile IP.

L'hôte mobile peut utiliser deux méthodes différentes pour recevoir les paquets qui lui sont adressés pendant qu'il se trouve connecté sur un autre sous-réseau qui celui d'origine.
Dans la première, l'hôte mobile reçoit sa propre adresse IP sur le réseau visité, par exemple par un service de configuration automatique comme DHCP [17]. Chaque paquet reçu dans une première phase par l'agent-mère est empaqueté dans un nouveau *datagramme* qui est transmis directement à cette adresse. L'hôte mobile reçoit ce *datagramme* et extrait le paquet original, contenant son adresse de base. La deuxième méthode est motivée par le fait qu'il est difficile de réserver et gérer d'une manière efficace un espace d'adresses pour les machines mobiles qui visitent un domaine. *Mobile IP* introduit alors la notion d'*agent visité*, un autre noeud spécial qui se trouve dans le réseau visité et qui représente l'hôte mobile auprès du son agent-mère. Dans ce cas, les paquets envoyés à l'adresse de base de l'hôte mobile et interceptés par l'agent de base sont encapsulés et retransmis à l'agent visité. Celui-ci récupère les paquets originaux et les remets à l'hôte mobile sur le lien local.
Dans le sens inverse, les paquets envoyés par l'hôte mobile à ses correspondants ne passent pas par l'agent-mère du réseau d'origine et sont routés normalement à travers Internet en fonction de leur adresse destination. Parce que les hôtes correspondantes ignorent les mécanismes de *Mobile IP*, l'hôte mobile doit utiliser son adresse de base comme adresse source de paquets envoyés. Cette différence entre les deux chemins suivis par les paquets reçus et les paquets envoyés par l'hôte mobile s'appelle *routage triangulaire*.

iii. Les interactions entre l'hôte mobile et les agents Mobile IP

Un hôte mobile peut déterminer si elle est sur son réseau d'origine ou pas par un mécanisme de découverte d'agents de mobilité. *Mobile IP* utilise les paquets ICMP [18] existants de type *Router Advertisement* et *Router Solicitation* et y rajoute des extensions spécifiques.
Les paquets envoyés par les agents visités contiennent notamment les adresses temporaires à utiliser et plusieurs autres informations comme le temps de validité de message ou la disponibilité de l'agent. Les agents de base n'ont pas d'adresse temporaire à diffuser, le but de leurs messages est que l'hôte mobile se rende compte de son reconnexion sur le réseau d'origine et cesse d'utiliser *Mobile IP*.

Pour qu'une hôte mobile puisse demander à son agent de base une redirection de messages vers une adresse temporaire, *Mobile IP* utilise deux messages spéciaux (*Registration Request* et *Registration Reply*), les deux envoyés par UDP sur le port numéro 434. Le processus d'enregistrement vise notamment à notifier à l'agent de base le couple d'adresses fixe/temporaire nécessaire pour la redirection de ses paquets. L'éventuel agent visité a un rôle passif dans la procédure d'enregistrement et il ne fait que passer les messages de demande de l'hôte mobile à l'agent de base et les réponses en sens inverse.
Le processus d'enregistrement d'une adresse temporaire doit être authentifié et sécurisé, puisque sinon quelqu'un d'autre peut demander à un agent de base une redirection vers son adresse et intercepter tous les paquets destinés à une certaine adresse. Pour l'authentification, la méthode préconisé est de signer les messages conformément à l'algorithme HMACMD5 (*Hashed Message Authentication Code with Message Digest version 5*) [19], utilisant une clé de 128 bits échangée auparavant.

iv. L'acheminement des datagrammes

L'agent de base doit utiliser deux fonctions spéciales du protocole ARP (*Address Resolution Protocol*) [20] - *proxy ARP* et *gratuitous ARP* - pour intercepter sur le réseau d'origine les datagrammes destinées à l'hôte mobile. Même dans le cas où la fonction d'agent de base est remplie par l'unique routeur du sous-réseau, ces fonctionnalités d'ARP restent nécessaires pour capturer les paquets envoyés par les autres machines sur le lien local. Pour cela, dès qu'il reçoit une demande d'enregistrement d'un hôte mobile, l'agent de base diffuse un paquet *ARP Reply*. Le rôle de ce message est de mettre à jour les caches ARP des autres machines et de faire correspondre son adresse physique à l'adresse fixe de l'hôte mobile. Ensuite, il répond à toutes les requêtes ARP subséquentes sur l'adresse fixe de l'hôte mobile. À son reconnexion sur le réseau d'origine, l'hôte mobile doit diffuser un paquet *ARP Reply* avec son propre adresse physique pour remettre à jour les caches ARP et se désenregistrer de l'agent de base.
Finalement, on précise comment la redirection des paquets de l'agent de base vers l'emplacement actuel de l'hôte mobile est réalisée. La technique utilisée, qui consiste à encapsuler le datagramme IP originale dans un en-tête IP supplémentaire, s'appelle *tunnelling* (voir figure 23). Le *datagramme* obtenu comme résultat de l'encapsulation est envoyé par l'agent de base à l'adresse temporaire de mobile. Plusieurs algorithmes d'encapsulation sont spécifiés par *Mobile IP*.
Celui qui doit être implémenté par toutes les entités impliquées (c'est-à-dire l'hôte mobile, l'agent de base et si le cas l'agent visité) est l'encapsulation IP-en-IP [21]. Cet algorithme est préféré aux autres car il est le seul à permettre la fragmentation des paquets sur les liens si leur taille dépasse la valeur de MTU (*Maximum Transmission Unit*).

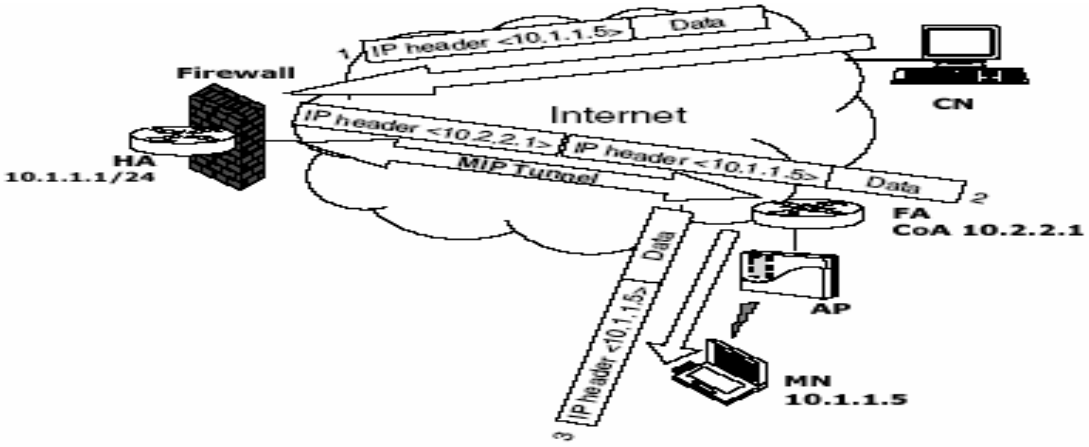

Figure 23 : *Tunnelling.*

b. Mobile IPv6

Mobile IPv6 [11] est basé sur les mêmes principes de base que son correspondant pour IPv4. Cependant, il comporte un nombre des améliorations, possibles grâce aux fonctionnalités supplémentaires présentes dans IPv6.

i. Les Caractéristiques

Le protocole Mobile IPv6 (MIPv6) définit des concepts et des procédures permettant à un noeud mobile en itinérance (*roaming*) dans un réseau Internet IPv6, de maintenir ses communications lors de ses déplacements de façon transparente de ses correspondants.
Introduire la mobilité dans IPv6 entraîne une modification de l'architecture classique des réseaux Internet. De nouvelles entités vont apparaître permettant de tenir compte de la mobilité.

- ✧ **Noeud mobile (MN, Mobile Node) :** représente tout nœud capable de se déplacer dans le réseau tout en restant accessible.
- ✧ **Réseau mère (Home Network) :** représente le réseau principal du mobile.
- ✧ **Agent mère (Home Agent) :** est un routeur du réseau mère du mobile. Il permet de localiser à tout moment le noeud mobile.
- ✧ **Réseau étranger ou visité (Visited Network) :** est un réseau temporaire auquel un mobile est connecté à un instant donné.
- ✧ **Correspondant (Correspondent Node) :** est un nœud du réseau avec lequel le mobile communique.

La figure 24 présente l'architecture d'un réseau Mobile IPv6. Les différentes entités d'un réseau MIPv6 y sont présentées. Un nœud mobile est susceptible de se déplacer de son réseau mère vers un réseau visité 1 puis d'un réseau visité 1 vers un autre réseau visité 2.

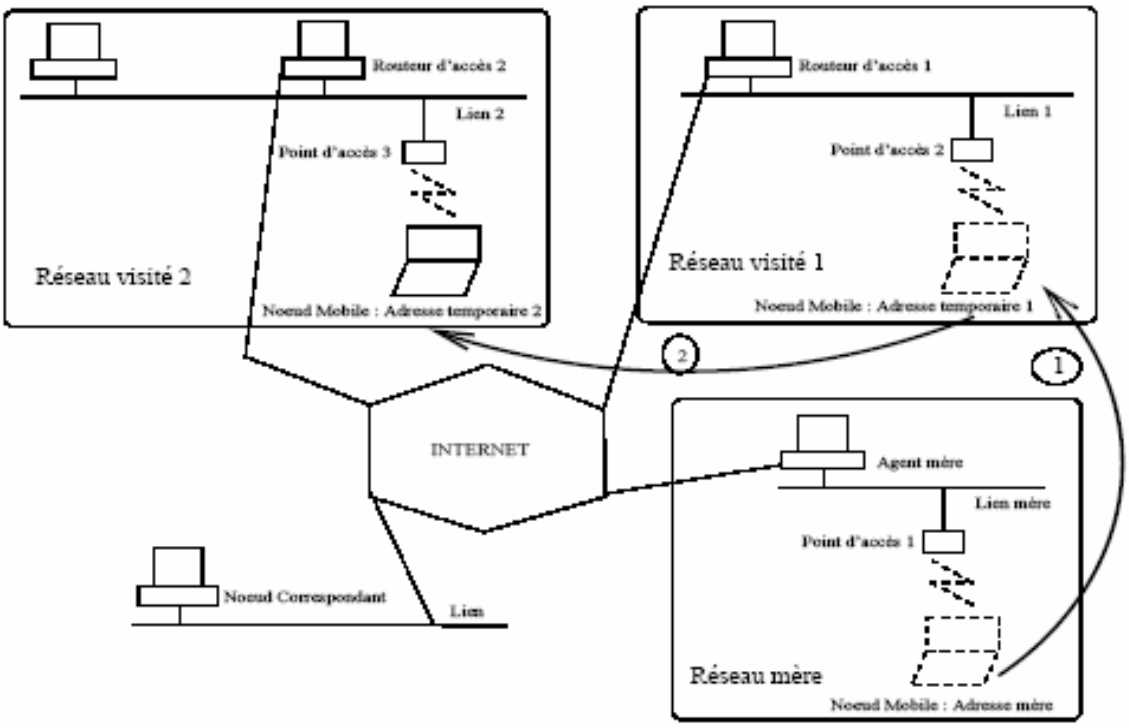

Figure 24: Architecture d'un réseau Mobile IPv6.

ii. Quelques concepts

Avant de décrire les procédures de mobilité définies dans le protocole Mobile IPv6, il est important de rappeler quelques concepts et notions.

- **Adresse mère ou principale (HoA, *Home Address*) :** représente l'adresse permanente du mobile. Elle permet de référencer le mobile de manière unique dans le réseau.
- **Adresse temporaire (CoA, *Care-of-Address*) :** est attribuée à un mobile lorsque celui-ci change de réseau.
- **Préfixe de sous-réseau (*Subnet prefix*) :** est une suite de bits permettant d'identifier un sous-réseau. L'adresse de tous les noeuds du réseau débute par cette suite.
- **Identifiant d'interface (ID, Interface Identifier) :** permet d'identifier l'interface d'un noeud sur un lien.
- **Adresse lien local (LLoA, *Link Local Address*) :** identifie un noeud sur un lien. Elle est composée d'un préfixe prédéfini (FE80) sur 64 bits et d'un identifiant d'interface sur 64 bits. Sa portée est locale (Lien).
- **Adresse globale unicast :** identifie de façon unique un interface. Elle est constituée d'un préfixe de 64 bits et d'un identi ant d'interface de 64 bits. Sa portée est globale (réseau).
- **Adresse non spécifiée (*Unspecified Address*) :** n'est assignée à aucun interface et désigne l'absence d'adresse. Elle est utilisée par un noeud qui essaie d'obtenir une adresse IPv6.
- **Adresse multicast :** identifie un ensemble d'interfaces. Un paquet émis à une adresse *multicast* est adressé à l'ensemble des interfaces identifiées par cette adresse. Deux types d'adresses *multicas*t sont généralement utilisés. L'adresse *multicast* des noeuds (*all nodes multicast addresses: FF02 ::1*) qui identifie le groupe de tous les noeuds IPv6 se trouvant sur le lien local. L'adresse *multicast* des routeurs (*all routers multicast addresses: FF02::2*) qui identifie l'ensemble des routeurs IPv6 se trouvant sur le lien local.

Différents messages sont définis ou utilisés par le protocole Mobile IPv6 pour gérer la mobilité.

- ✧ **Mise à jour de l'association (BU, Binding Update) :** permet à un noeud mobile d'informer son agent mère et ses correspondants de sa nouvelle association entre l'adresse mère et sa nouvelle adresse temporaire.
- ✧ **Acquittement de l'association (BAck, Binding Acknowledgment) :** permet à un noeud d'acquitter un Binding Update.
- ✧ **Annonce de routeur (RA, Router Advertisement) :** est émis périodiquement ou en réponse à une sollicitation de routeur. Ce message contient les informations sur le réseau notamment le pré xe du réseau et l'adresse du routeur.
- ✧ **Sollicitation de routeur (RS, Router Solicitation) :** permet à un noeud d'obtenir des routeurs un message d'annonce de routeur.
- ✧ **Sollicitation de voisin (NS, Neighbor Solicitation) :** est émis par un noeud afin d'obtenir l'adresse de lien d'un noeud cible tout en fournissant son adresse de lien.
- ✧ **Annonce de voisin (NA, Neighbor Advertisement) :** est émis par un noeud en réponse d'une sollicitation de voisin. Le message non sollicité d'annonce de voisin (*Unsolicited Neighbor Advertisement*) est émis par un noeud pour propager une information, par exemple le changement de son adresse.

iii. Les procédures de mobilité dans Mobile IPv6

Le but de Mobile IPv6 comme celle de Mobile IP est de rendre joignable à tout instant un périphérique mobile. Pour que cela soit possible, il faut que ce périphérique garde toujours un identifiant unique quelque soit le réseau dans lequel il se trouve. En d'autres termes, cet équipement doit toujours avoir la même adresse IP. Également, puisqu'il n'y a que peu de systèmes qui utilisent le protocole IPv6, le protocole Mobile IPv6 bénéficie d'un avantage important, car il ne vise la compatibilité avec les machines existantes. Cet avantage majeur est utile surtout pour optimiser le routage ; rappelons que la difficulté rencontrée dans l'extension similaire de Mobile IP était justement l'incompatibilité avec les hôtes correspondantes n'implémentant pas les mécanismes en cause. Un autre élément important est que la protection de mises à jour envoyées aux hôtes correspondantes par l'hôte mobile ne demande ni d'avoir établi une association de sécurité auparavant, ni l'existence d'une infrastructure d'authentification. À la place, une méthode appelée *return routability*[2] est utilisée pour s'assurer que la vraie hôte mobile envoie le message de mise à jour. On estime donc que l'optimisation de route sera utilisée à l'échelle globale, entre toutes les hôtes mobiles et leurs correspondants.

L'hôte mobile peut acquérir son adresse temporaire dans le domaine visité par le mécanisme standard d'auto-configuration d'IPv6 [12]. L'espace d'adressage d'IPv6 est très large et on n'a plus besoin d'un agent visité pour représenter plusieurs hôtes mobiles par une seule adresse. Pour cela, on a supprimé les agents visités de l'architecture d'IPv6, une différence très importante par rapport à la version IPv4 où leur présence était préférée. En revanche, on élimine la possibilité que les agents visités coopèrent pour minimiser la perte des paquets lors d'un *handover*.

[2]Un mécanisme qui garantir l'acheminement d'un message de réponse au bon destinataire.

À la place, Mobile IPv6 se sert du fait qu'une machine peut avoir plusieurs adresses IPv6 par interface. Les terminaux peuvent ainsi garder ouverte l'ancienne connexion et continuer à recevoir des paquets à cette adresse même après qu'il est configuré avec une nouvelle adresse.
Les correspondants d'un hôte mobile envoient les *datagrammes* en utilisant l'adresse temporaire de l'hôte mobile sur le réseau visité. L'adresse fixe est incluse dans le nouvel en-tête de routage IPv6. En sens inverse, l'hôte mobile utilise une autre fonctionnalité de IPv6, l'option de destination de type *Home Address*, pour s'identifier. Utiliser ces mécanismes IPv6 à la place de l'encapsulation réduit la surcharge observée dans Mobile IPv4, tout en permettant aux niveaux supérieurs de ne voir que l'adresse fixe de mobile et donc continuer à fonctionner de manière transparente.

2. Handover dans les réseaux mobiles

a. Handover dans IEEE 802.11

IEEE 802.11 définit trois scénarios différents de *handover* [10] (voir la figure 25S) :

1. **Aucune transition :** Deux sous-classes qui sont habituellement indistinguible sont identifiées :
    a. Statique-aucun mouvement ;
    b. Mouvement Local : mouvement dans *Basic Service Set* (*BSS*) (c.-à-d., couverture d'AP).
2. **Transition d'AP :** Ce type est défini comme un mouvement de station d'un AP à l'autre dans le même *extended service set* (ESS).
3. **ESS-transition :** Mouvement d'une station d'un BSS dans un ESS à un BSS dans un ESS différent. Habituellement un réseau WLAN a à moins un ESS et un sous-réseau d'IP. Ce cas signifie ce qui suit :
    a. Inter-système (sous-réseau d'IP) *Handover*.
    b. Inter-domaine *handover* (par exemple, entre deux réseaux différents).

La plupart des solutions de *handover* disponibles sur le marché sont fournir pour les deux premiers scénarios; celles-ci peuvent être faites en utilisant La couche de liaison de données, qui est le contrôle d'accès au medium (*Medium Access Control* - MAC). Le dernier scénario exige la participation des couches supérieures.

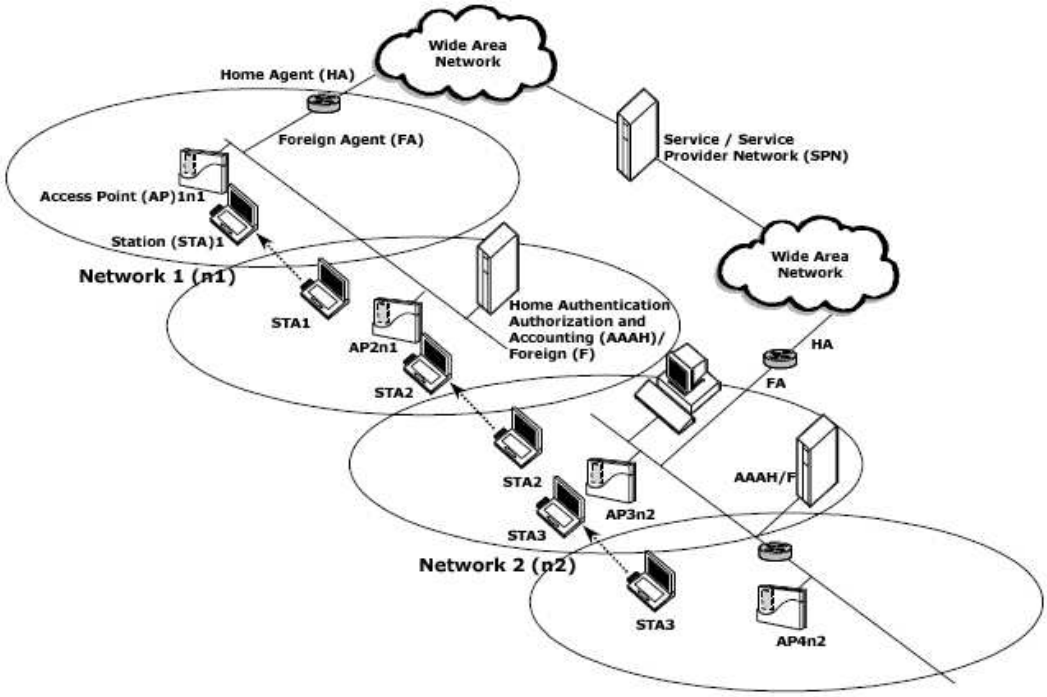

Figure 25: IEEE 802.11 *handover* scenarios.

b. Handover dans UMTS

i. Introduction

L'infrastructure fixe des réseaux de mobilophone inclut les stations de base distribuées dans toute la surface couverte du réseau, qui offrent la connectivité par l'intermédiaire de l'interface d'air aux mobilophones dans leur secteur d'assurance. Tant qu'il est active (par exemple, pendant un appel) un mobile utilise un canal radio fourni par sa station de base et parfois il devient nécessaire ou souhaitable de changer le canal assigné ou plus souvent la station de base, le procédé par lequel ceci se produit se nomme *Handover*. Dans des réseaux UMTS, les canaux utilisés par des mobiles peuvent être soutenus par l'intermédiaire des stations de base multiples simultanément par le "Soft handover" et ainsi la simple décision de handover (cas du GSM) est remplacée par des décisions pour créer la(les) connexion(s) à la(aux) nouvelle(s) station(s) de base et pour enlever la(les) connexion(s) existante(s). L'échec d'ajouter des connexions aux stations de base voisines, augmente le niveau de l'interférence éprouvé en cellules voisines et peut avoir d'impact sur la capacité de maintenir la qualité de l'appel, tout en inutilement ajoutant des rendements de connexions qui améliorent un peu la qualité mais consomme la capacité de la cellule voisine. UMTS *Handover* reste encore "*mobile assisted*" et "*Network Controlled*" (c-à-d le mobile produit des rapports de mesure, détaillant sa perception, la puissance et la qualité du canal courant et la puissance des cellules voisines, mais il est contrôlé par le réseau car c'est ce dernier qui prend la décision réelle, tout en utilisant les rapports du mobile et les mesures semblables qu'il fait).

ii. Les catégories du Handover

Les catégories du Handover (également désigné sous le nom du *handoff*) sont les suivantes :

- ✧ **Hard Handover :** Il signifie que tous les anciens liens radio dans l'UE sont enlevés avant que les nouveaux liens radio soient établis. *Hard Handover* peut être sans couture (*seamless*) ou avec couture (*non-seamless*). Le *Hard Handover* sans couture signifie que le *handover* n'est pas perceptible à l'utilisateur. Dans la pratique un *handover* qui exige un changement de la fréquence porteuse (*handover* d'inter-fréquence) est toujours exécuté en tant que *hard handover*.
- ✧ **Soft Handove :** Il signifie que les liens radio sont ajoutés et enlevés d'une manière que l'UE garde toujours au moins un lien radio à l'UTRAN. Le *Soft handover* est exécuté au moyen de macro diversité, qui se rapporte à la condition que plusieurs liens radio sont en activité en même temps. Le *Soft handover* peut être employé quand des cellules utilisant la même fréquence sont changées.
- ✧ **Softer handover :** Il est un cas spécial de *Soft handover* où les liens radio qui sont ajoutés et enlevés appartiennent au même NodeB.

D'une façon générale nous pouvons distinguer le *handover* d'intra-cellule et le *handover* d'inter-cellule. Pour UMTS les types suivants de *handover* sont indiqués:

- ✧ *Handover* 3G -3G (entre UMTS et autres systèmes 3G)
- ✧ FDD soft/softer handover
- ✧ FDD inter-frequency hard handover
- ✧ FDD/TDD Handover (changement de cellule)
- ✧ TDD/FDD Handover (changement de cellule)
- ✧ TDD/TDD handover
- ✧ Handover 3G - 2G (e.g. handover vers GSM)
- ✧ Handover 2G - 3G (e.g. handover depuis GSM)

La cause la plus évidente pour exécuter un handover est celle ci, dû à son mouvement, un utilisateur peut être servi en une autre cellule plus efficacement (comme moins d'émission de puissance, moins d'interférence). Il peut cependant également être exécuté pour d'autres raisons telles que la commande de charge de système.
L'ensemble actif (**Active Set**) est défini comme étant l'ensemble de Node-Bs dont l'UE est simultanément relié (c-à-d, les cellules d'UTRA assignant actuellement un *downlink* DPCH à l'UE constituent l'ensemble actif).
Des cellules, qui ne sont pas incluses dans l'ensemble actif, mais sont incluses dans le CELL_INFO_LIST appartiennent à **Monitored Set**.
Les cellules détectées par les UE, qui ne sont ni dans le CELL_INFO_LIST ni dans l'ensemble actif appartiennent au **Detected Set**. Le reportage des mesures de l'ensemble détecté est seulement applicable aux mesures d'intra-fréquence faites par UEs dans l'état de CELL_DCH.

iii. Les Différents types de mesures d'interface d'air

- ✧ **Mesures d'Intra-fréquence :** mesures sur les canaux physiques de *downlink* à la même fréquence que l'ensemble actif. Un objet de mesure correspond à une cellule.
- ✧ **Mesures d'Inter-fréquence :** mesures sur les canaux physiques de *downlink* aux fréquences différentes de la fréquence de l'ensemble actif. Un objet de mesure correspond à une cellule.
- ✧ **Mesures d'Inter-RAT :** mesures sur les canaux physiques de *downlink* appartenant à une autre technologie d'accès radio qu'UTRAN, par exemple GSM. Un objet de mesure correspond à une cellule.
- ✧ **Mesures du volume de trafic :** mesures sur le volume de trafic d'*uplink*. Un objet de mesure correspond à une cellule.
- ✧ **Mesures de qualité :** mesures des paramètres de qualité de *downlink*, par exemple taux d'erreur de bloc de transport de *downlink*. Un objet de mesure correspond à un canal de transport en cas de BLER. Un objet de mesure correspond à un *timeslot* en cas de SIR (TDD seulement).
- ✧ **Mesures d'UE-internal :** mesures de la puissance de transmission d'UE et du niveau de signal reçu par l'UE.
- ✧ **Mesures de positionnement d'UE :** Mesures de la position d'UE.

L'UE supporte un certain nombre de mesures fonctionnant en parallèle. L'UE supporte également que chaque mesure soit commandée et rapportée indépendamment de toute autre mesure.

iv. L'optimisation de Handover

Visant à optimiser le handover seulement d'une perspective d'utilisateur exige de maintenir la connexion de la plus haute qualité à tout moment, aussi bien que d'assurer une probabilité acceptable que la qualité demeurera haute. Ceci exige d'augmenter le nombre de handovers pour s'assurer que le mobile reste sur la meilleure cellule à tout moment, tout en diminuant le nombre de handovers inutiles pour réduire au minimum les brèves interruptions et la chance d'échec qui sont associés à chaque handover. Cependant, l'optimisation de la perspective de réseau, exige de maintenir la qualité appropriée de tous les appels, tout en soutenant autant d'appels que possible.

CONCLUSION

Nous avons commencé ce chapitre par la définition de la mobilité dans les réseaux. Nous avons ensuite présenté les différents types de mobilité.
Dans la deuxième partie du chapitre, nous avons parlé de *Handover,* par la suite nous avons précisé les principaux protocoles de mobilité ensuite nous pouvons dire que les normes de grande couverture sont décrites tel que GSM, GPRS et UMTS. Nous allons analyser dans le chapitre suivant la mobilité hétérogène et les performances d'un réseau hétérogène UMTS et 802.11.

Partie II : Analyse de performance de handover vertical entre réseaux UMTS et WLAN

CHAPITRE 4

Étude de performance dans le cadre d'une mobilité hétérogène : cas UMTS/802.11

Chapitre IV : Étude de performance dans le cadre d'une mobilité hétérogène : cas UMTS/802.11

Nous commençons ce chapitre par introduire les métriques de performance, en second lieu nous décrivons l'architecture proposée, puis le modèle de simulation sera présenté en en troisième, et en dernier lieu nous analysons les différents résultats obtenus.

INTRODUCTION

Les protocoles de mobilité permettent le support du *handover* entre les deux architectures. A présent, il est intéressant d'expliciter l'exécution à proprement parler du *handover* inter-système entre UMTS et 802.11. En effet, le protocole de mobilité autorise l'interaction de couche réseau ou supérieur entre les deux réseaux. Cependant, UMTS traite la mobilité par *handover* et resélection de cellule alors que 802.11 traite la mobilité par transitions.

↳ Problématique de la recherche

Constitue les réseaux hétérogènes dans nos jours un domaine de recherche très important, vu le nombre des normes mobiles qui n'a cessé d'augmenter et les problèmes d'interaction qu'en résulte nous allons essayer dans cette section de répondre sur les questions suivantes : Comment les réseaux hétérogènes est considéré comme un nouveau domaine de recherche ? C'est quoi la mobilité dans ces réseaux ? Par la suite nous présentons notre étude de cas pratique UMTS/802.11, et finalement Quel est l'impacte de la sécurité dans le cas de *handover* ?

Avec la croissance exponentielle de l'Internet et l'expansion des réseaux cellulaires, l'Internet sans fil devient une réalité. En raison de la bande passante limitée et du prix de service élevé des réseaux cellulaires, il y a une tendance d'intégrer le WLAN et les réseaux cellulaires, qui fourniront aux utilisateurs la connexion à l'Internet "n'importe quand et n'importe où" (*any-time, any-where*) aussi bien avec un débit plus important et moins coûteux de données dans la zone de couverture qui est limitée.

Cette évolution de réseau, et l'émergence de nouveau protocole IP tel qu'IPv6, nous mène vers l'hypothèse que les plus part des réseaux sans fil qui interagir par l'intermédiaire d'IP que ces interactions seront basé sur une plateforme IPv6 dans le future.

La gestion de la mobilité est considérée comme étant le principal élément dans ce nouveau type de réseau, nous voulons dire par cela que le *handover* entre ces différents réseaux faira l'objet da notre étude.

I. Les métriques de performance

Dans cette section, nous discutons les métriques de performance utilisées pour mesurer les effets de *handover* sur la performance de MN.

1. La durée de *handover* (*handover latancy*)

La durée (ou latence) de *handover* est le temps nécessaire pour accomplir le *handover*. Elle inclut la détection de mouvement, la prise de décision, l'attribution de la nouvelle adresse et la redirection du trafic. Le début de *handover* est l'instant où la MN entre/quitte la cellule. Pendant le *handover*, la MN ne peut pas utilisée l'interface sur laquelle oriente son flux, jusqu'à ce que le *handover* s'achève. Cependant, pendant le *handover*, la MN pourrait émettre et recevoir des paquets sur une autre interface.

2. Les paquets perdus (*Packet loss*)

Les paquets perdus sont le rapport entre les paquets jetés en raison des erreurs et les paquets prévus pendant le *handover*.

3. la probabilité de générer un faux trigger (*Probability of wrong link trigger generation*)

Le *trigger* est une procédure déclenché par une entité et générant un événement à exécuter par une autre entité homologue. La génération d'un faux trigger peut être expliquée par un MN comme le début de *handover*. Quelques *triggers* (par exemple *Link down*) sont générés par la suite d'une perte de paquet ou d'une mesure de qualité de signal, un MN peut déclenche un faux *trigger* à cause d'une collision ou d'une interférence temporaire.

4. Le facteur de déconnexion (*Disconnection factor*)

Le facteur de déconnexion est le rapport entre le temps de déconnexion, quand un MN ne peut pas recevoir du trafic à travers ses interfaces, et la durée de *handover*. Le temps de déconnexion varie entre 0 et la durée de *handover*. Par exemple, si l'une des interfaces du MN tombe en panne, le MN sera déconnecté cette interface jusqu'à ce qu'il accomplisse un *handover* vertical sur une autre interface. Dans ce cas-ci, le temps de déconnexion sera égal à la durée de *handover*.

5. la charge de signalisation (*Signalling load*)

Elle comprend la charge de signalisation et de contrôle des messages engendré par l'utilisation de *Mobile IPv6 et* produit par le MN et le réseau résulte de *handover* d'un AR à un autre.

6. Le débit *(Throughput)*

Le calcul du débit est essentiel pour évaluer le taux de données reçu par MN**.** Le débit peut être perturbé par la perte et la retransmission de paquet causé par dégradation de *handover* et de signal.

II. L'architecture proposée à l'étude

L'architecture proposée consiste à interconnecter le réseau UMTS et IEEE 802.11 pour permettre à simuler le *handover* entre le deux réseaux.

Elle comprend d'une part un réseau IEEE 802.11 et d'autre part un réseau UMTS et un nœud d'interconnexion. La section suivante détaille le modèle de simulation pour permettre la simulation de ladite architecture.

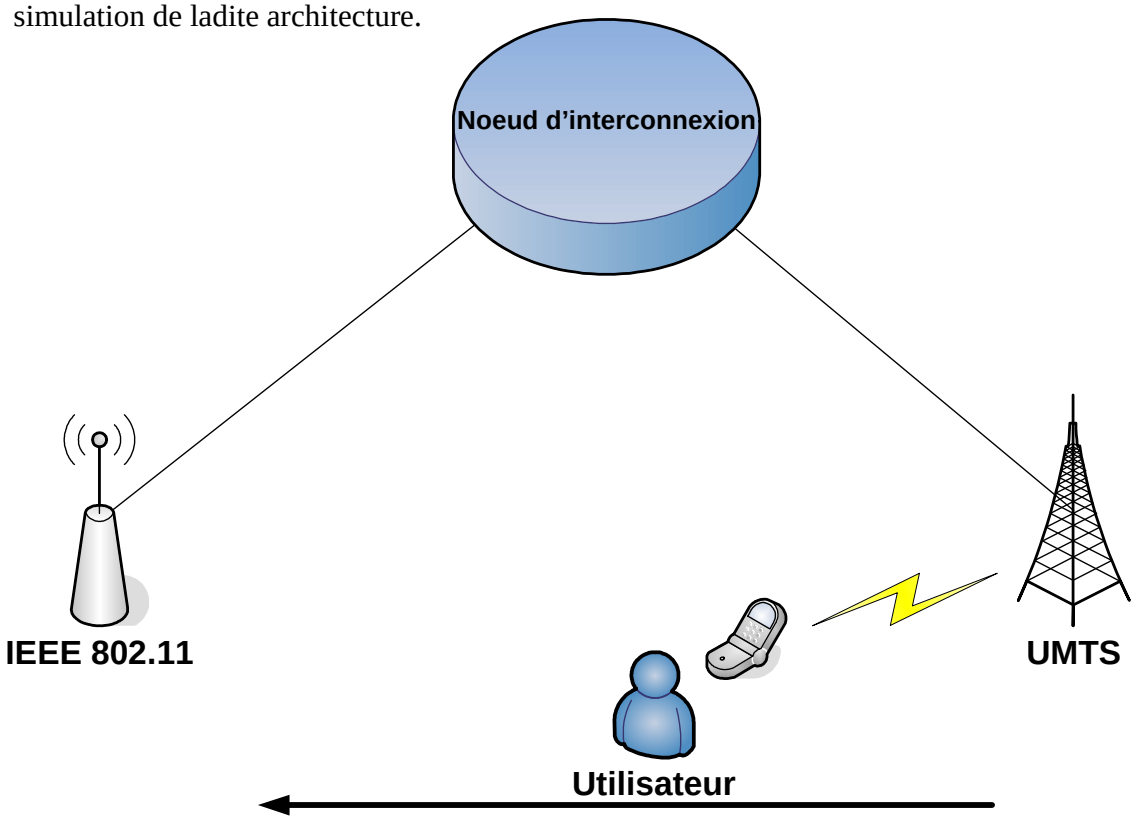

Figure 26 : Architecture proposée

III. Le Modèle de Simulation

Dans cette section nous décrivons le modèle de simulation et nous détaillons par la suite les différents éléments.

1. L'architecture implémentée

L'architecture implémenté repose sur le standard IEEE 802.21 **[29]**, il est constitué principalement de trois composante : le réseau sans fil *IEEE 802.11*, le réseau d'*UMTS* et l'entité de *Handover*. La figure ci-dessous décrit l'architecture implémentée.

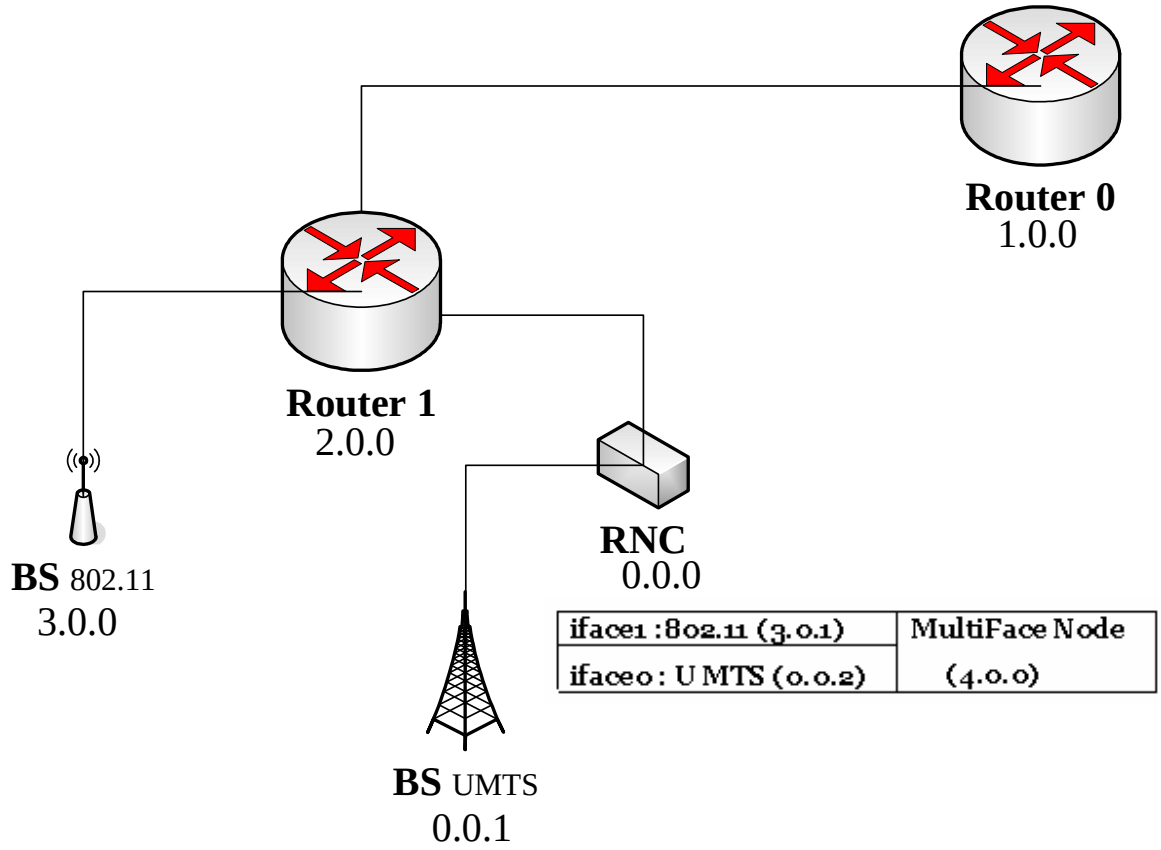

Figure 27 : Architecture implémenté

c. Implémentation dans NS-2

La simulation a était effectuée sur la version ns-2.29, des modifications et des améliorations pour ns-2 ont était réalisés afin de se conformer avec le standard IEEE 802.21. Parmi ces changements nous citons :

- ✧ Intégration du modèle *UMTS* dans le noyau de NS,
- ✧ Conception d'un nœud hétérogène d'interfaces multiples,
- ✧ Implémentation Agent *Neighbor Discovery* (découverte de voisins) pour permettre au couche 3 un mécanisme efficace de découverte des voisins,
- ✧ Un agent *Media Independent Handover* implémentant les événements et les commandes de 802.21,
- ✧ Modules de *handover* supportant les différentes politiques.

d. IEEE 802.11 & NS-2

Le modèle 802.11 disponible dans NS-2 a été modifié pour s'adapter avec les besoins de mobilité de IEEE 802.21; Les dispositifs suivants ont été ajoutés au modèle :

- ✧ Transmission de messages *beacon* par AP,
- ✧ L2 triggers (voir le paragraphe **e**),
- ✧ Association Demande/Réponse et balayage multiple de canal.

Le procédé de *handover* L2 comprend les trois étapes suivantes : **(1)** une étape de découverte où le MN détermine l'ensemble d'APs disponibles, **(2**) une étape d'authentification où le MN et le AP s'authentifient selon les protocoles d'IEEE 802.1X et d'IEEE 802.11i, et **(3)** l'étape d'association où le MN demande une association avec AP sélectionné. Le modèle de simulation actuel n'inclut pas l'étape d'authentification.

e. UMTS & NS-2

Le modèle UMTS utilisé est basés sur le modèle d'EURANE **[30]** (*Enhanced UMTS Radio Access Network*). Les extensions EURANE développé dans le cadre du projet SEACORN pour *Ericsson Telecommunication B.V.* a été considérées pour ce projet. EURANE ajoute 3 noeuds à savoir: le RNC, la BS et l'UE UMTS autorisant le support des canaux FACH, RACH, DCH et HS-DSCH. Les canaux FACH et RACH sont des canaux communs aux UEs d'une même cellule alors que le canal DCH est un canal dédié pour UE. Le canal HS-DSCH permet le transport de données utilisateur à haut débit grâce à la technique HSDPA. Ces noeuds implémentés sont caractérisés principalement par les services de segmentation et retransmission de données. Le *handover* entre canaux RACH/FACH et DCH est supporté.
Les hypothèses principales dans ce modèle sont comme suit. Tous les noeuds sont accessibles à tout instant et la cellule d'UMTS couvre toute la surface de simulation sauf indication contraire.

f. L'entité de handover implementé

Afin de modéliser la mécanisme du *handover* inter-système UMTS/802.11, une implémentation de *MIH Function* conformément au standard 802.21, la figure ci-dessous présente l'architecture utilisée.

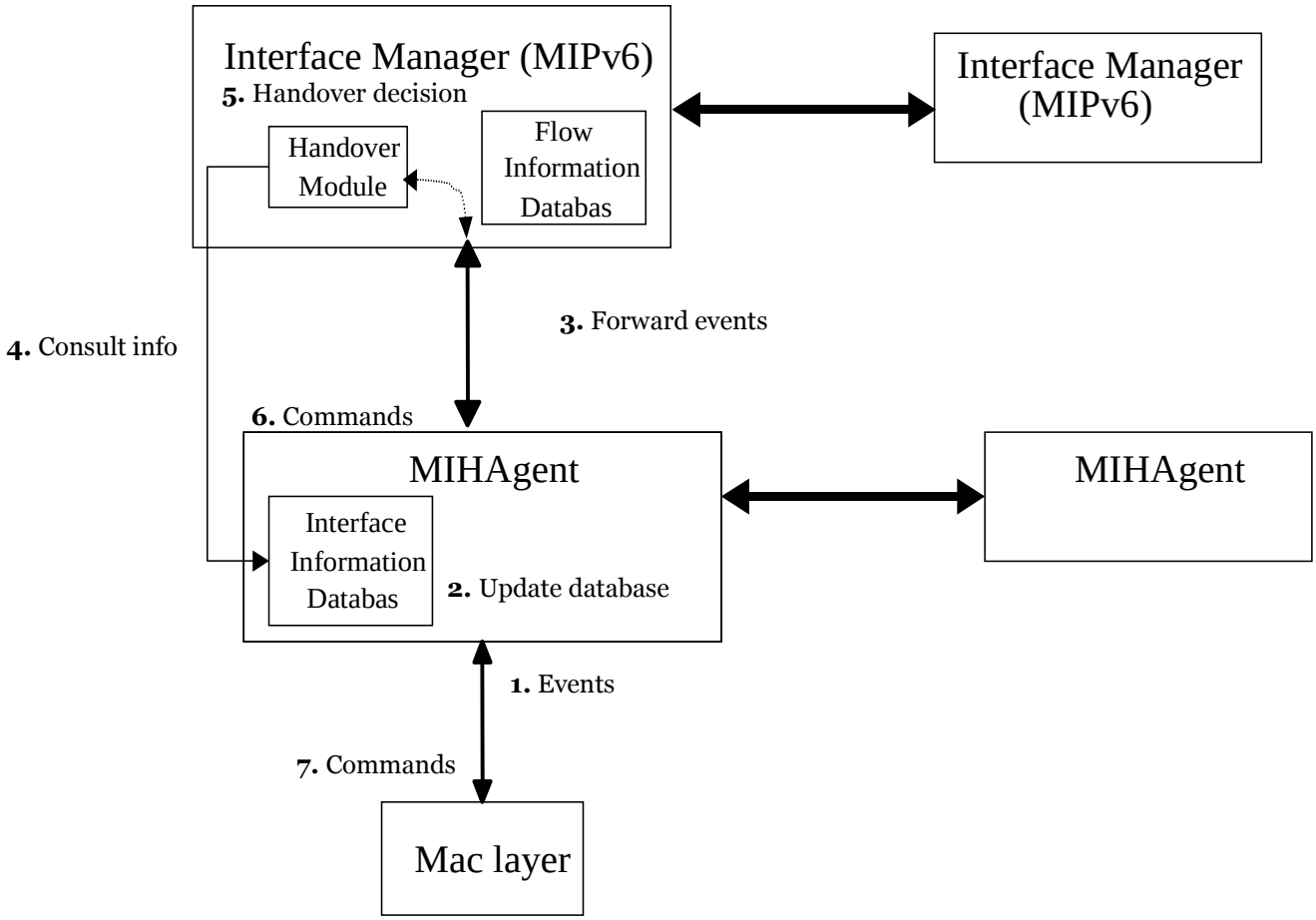

Figure 28: Le modèle de MIH dans NS-2

Les fonctionnalités suivantes sont actuellement implémentées dans le modèle :

Catégorie	Fonction
Event Service	Link Event Register Link Event Deregister Link Detected Link UP Link Down Link Going Down Link Event Rollback
Command Service	MIH statistique MIH *Handover* Initialisation
MIH Protocol	Event Registration Link Events Handover Initialisation (demande/réponse) Statistique (demande/réponse)

La figure 29 représente l'interaction de MIHF avec les différents composants du noeud. Le MIHF est implémenté comme agent et peut donc envoyer les paquets de la couche 3 au MIHF distant. Le MIHF contient la liste d'interfaces locales pour obtenir leur statut et pour

contrôler leur comportement. L'utilisateur MIH est également implémenté comme agent et enregistré avec MIHF pour recevoir des événements des interfaces locales et distantes.

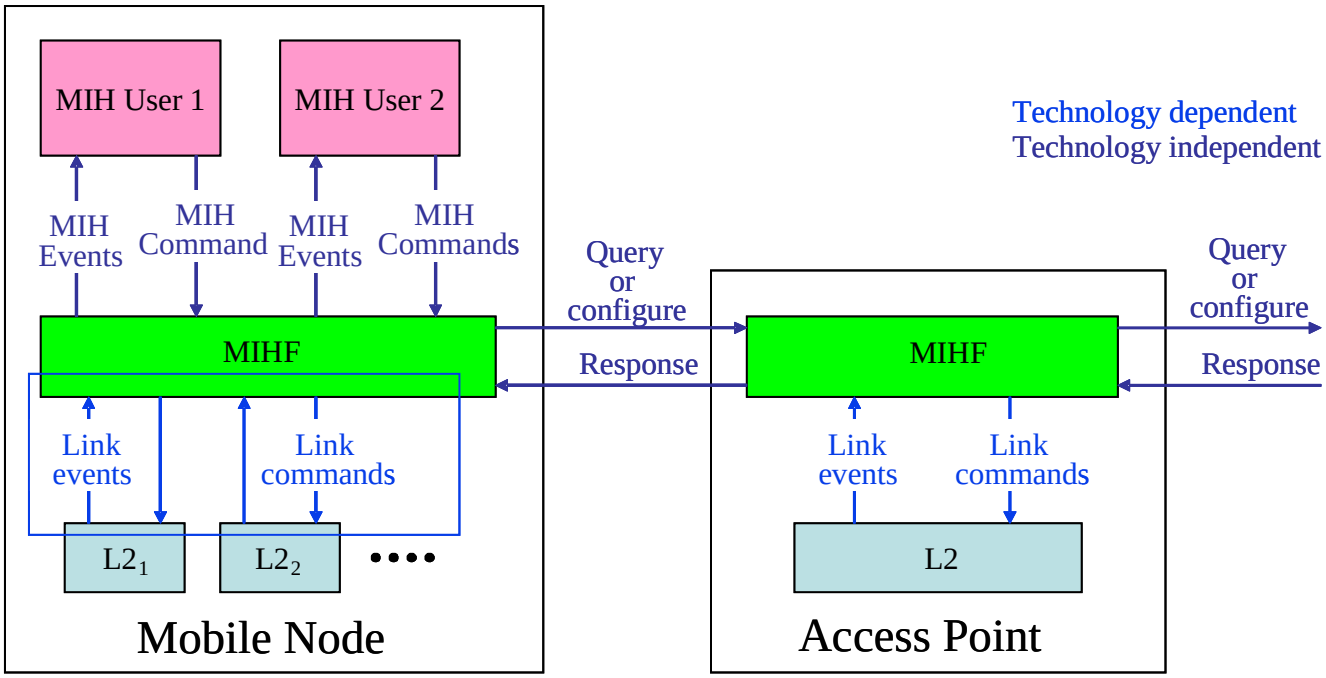

Figure 29: Vue d'ensemble de conception de MIH

g. Triggers

Les *triggers* (déclenchements en français) suivants ont été implémenté dans le MN de 802.11.

i. Link Detected

À la couche MAC, l'événement *Link Detected* est généré lors de la réception d'un message de *beacon* provenant d'un autre AP (mode passif). Si un MN fonctionne en mode actif, alors il envoie le résultat de l'étape découverte au module de *handover*. Un *Link Detected* est alors généré pour chaque AP trouvé.

ii. Link Up

Un *Link Up* est généré lors de la réception d'un message de *Association Response* (association du MN avec un AP) avec un acquittement indiquant que le MN est accepté dans la cellule.

iii. Link Down

L'événement de *Link Down* est généré quand la couche MAC du MN est déconnecté d'un AP. Ceci se produit pour l'un des cas suivant :

- ✧ N paquets consécutifs sont arrivés avec des erreurs. Par défaut N est égal à 5.

- ✧ Une AsR est reçu indiquant que le MN est rejeté de son AP actuel.
- ✧ La couche MAC du MN est demandé pour se cxonnecté à un AP.

iv. Link Going Down

Un *link Going Down* est généré quand la puissance entre deux paquets consécutifs au niveau du récepteur diminue. Posons P_n (en watt) la puissance du nième paquet reçu, et P_{Th} la puissance exigée pour recevoir des paquets sans erreurs, un *link Going Down* est déclenché, si les deux conditions suivantes sont verifiées :

$P_n < \alpha P_{Th}$ (1)
$P_n < P_{n-1}$ (2)

Où α est le coefficient de seuil de niveau d'énergie.

v. Link Rollback

Un *Link Rollback* est étroitement lié avec *Link Going Down*. Si un paquet avec un niveau d'énergie élevé est reçu après un *Link Going Down*, alors la couche génére un *Link Rollback* pour annuler le dernier *Link Going Down* produit. Ainsi, un *Link Rollback* est produit si les trois conditions suivantes sont verifiées :

$P_{n-2} > P_{n-1}$ (1)
$P_{n-1} < \alpha P_{Th}$ (2)
$P_n > P_{n-1}$ (3)

vi. Link Handoff Imminent

Un *Link Handoff Imminent* est généré au niveau de la couche MAC à chaque changement de l'AP.

vii. Link Handoff Complete

Un *link Handoff Complete* est généré lors de la réception d'un message *AsR* qui indique que l'association avec l'AP cible est acceptée.

2. Le Scénario de Simulation

Le scénario considéré pour les résultats de simulation qui suivent se compose d'une cellule WLAN située à l'intérieur d'une cellule UMTS (voir figure 6). Nous supposons qu'un MN (équipé d'une interface multiple) est connecté au réseau UMTS avant qu'il traverse le réseau WLAN. Dans ce scénario le MN effectue deux *handover*. La première *handover* de WLAN à UMTS est exécutée quand le MN entre dans la zone couverte par l'AP de WLAN. L'autre *handover* entre WLAN et UMTS est exécutée quand le MN quitte la zone de couverture de AP du WLAN.

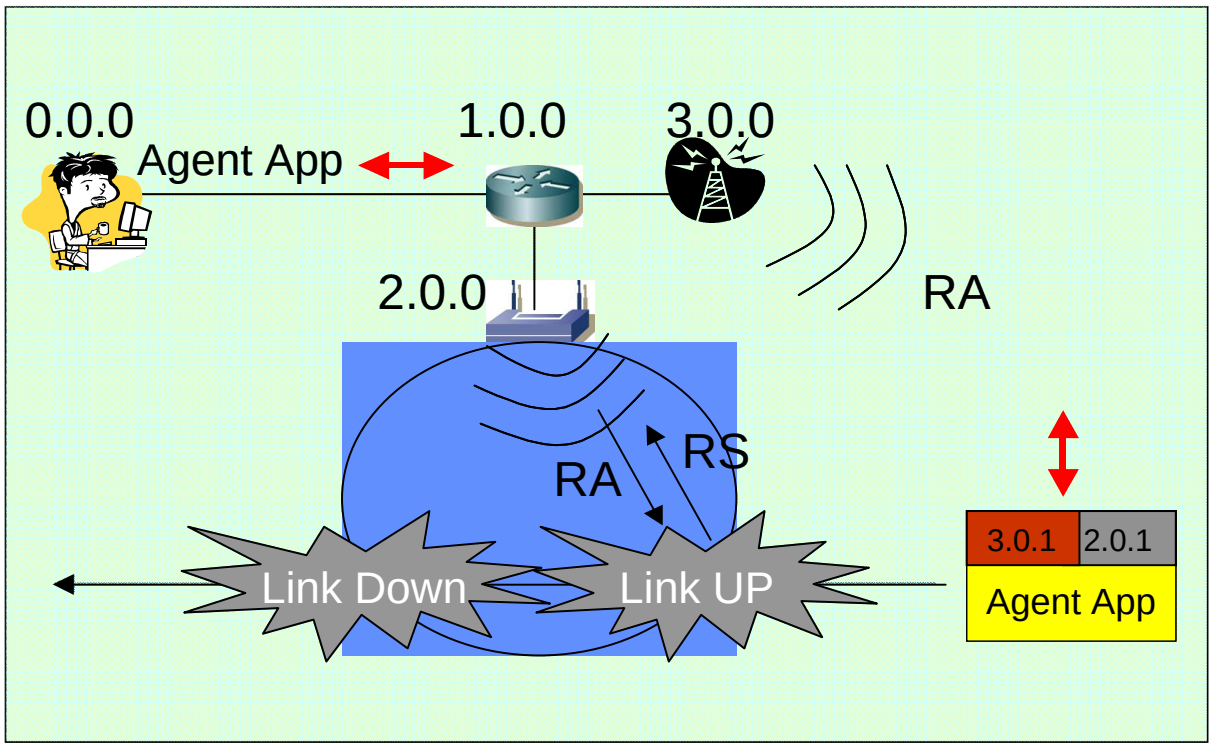

Figure 30 : Scénario de simulation

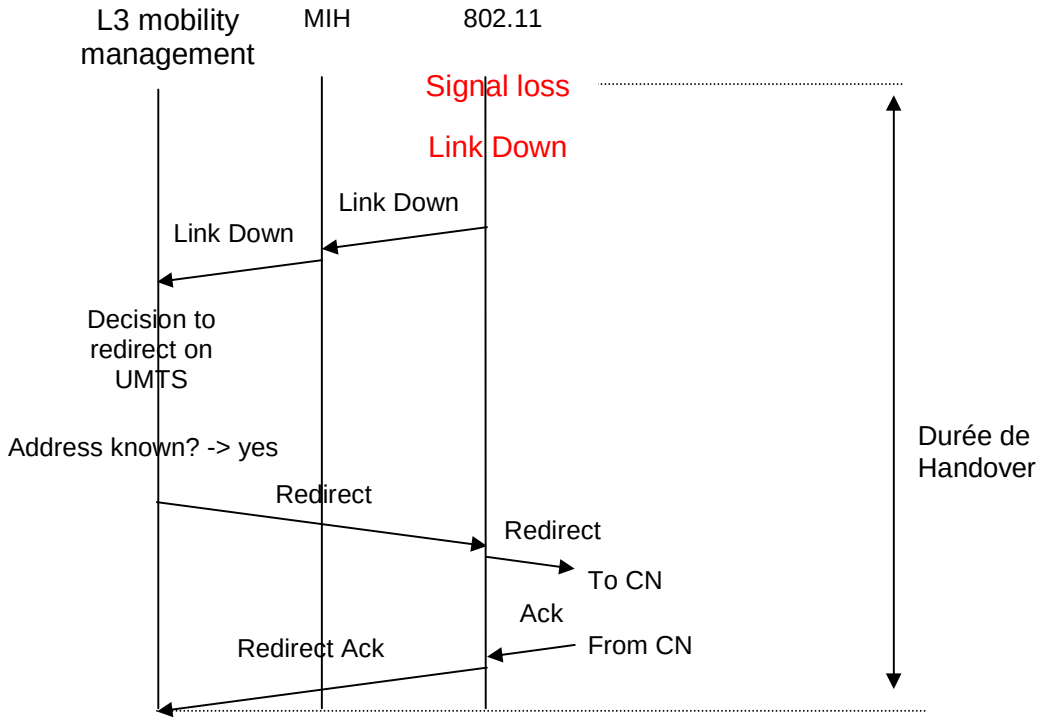

Figure 31 : Le MN quitte la cellule de WLAN

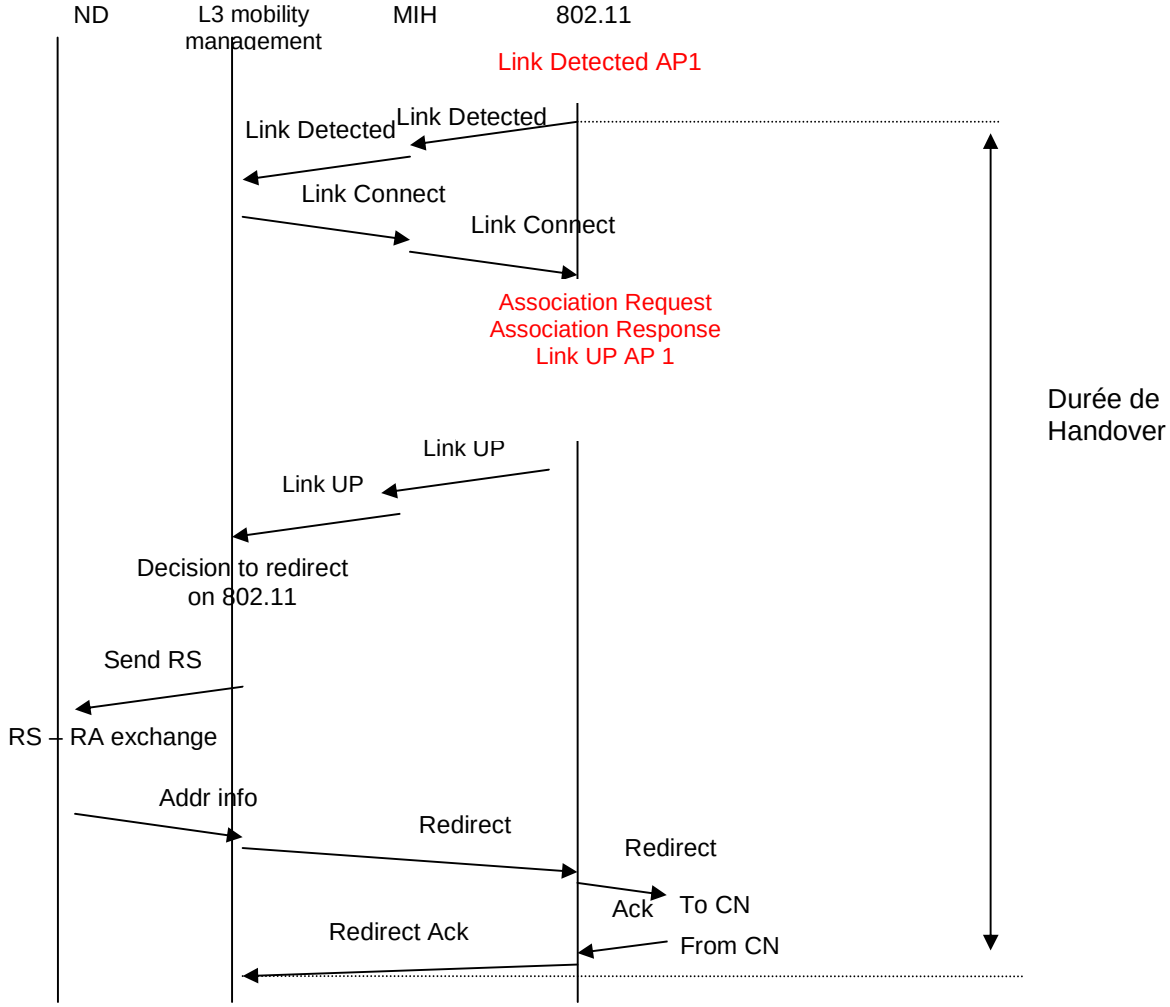

Figure 32 : Le MN entre dans la cellule de WLAN

Les détaillées illustrée sur les figures 7 et 8, sont comme suit :

- ✧ Le MN commence dans UMTS et se déplace vers le WLAN,
- ✧ Une fois que le MN entre dans WLAN, il reçoit une *beacon* de l'AP et envoie un *Link Detected* au module de MIH.
- ✧ Le module de MIH questionne le module de *handover* à propos de l'interface à utiliser.
- ✧ Dès que l'interface de WLAN est l'interface préférée à utiliser, le module de *handover* demande une connexion à l'AP et redirige le trafic du MN vers le WLAN.
- ✧ Le module de MIH envoie une commande de connexion à la couche MAC. Ceci marque le début de l'étape d'association.
- ✧ Une fois que la connexion avec la couche 2 est établi, un *Link UP* est généré par la couche MAC et envoyé au module de MIH. Le MIH déclenche alors un message RS afin de découvrir le préfixe d'IP du nouveau lien.
- ✧ L'AR répondant au RS suit les règles définies par le module ND (c.-à-d. dépendant de MAX_RA_DELAY_TIME et MIN_DELAY_BETWEEN_RA comme défini dans RFC2461).
- ✧ Quand le MN reçoit le RA, il rédirige le trafic vers l'interface de WLAN.

- ✧ En quittant la cellule, le MN reçoit des paquets avec des erreurs. Quand le nombre de paquets consécutifs reçus par erreur atteint un seuil choisi, un *Link Down* est produit généré et la couche MAC est déconnectée.
- ✧ Le module de *handover* reçoit un *Link Down* et rédirige le trafic vers UMTS (par le module de MIH).

IV. Résultats de Simulation

Après avoir décrit le scénario utilisé, nous discutons dans cette partie les résultats obtenus.

1. Effet du MAX_RA_DELAY_TIME sur la performance de Handover

Quand le MN entre dans la cellule de WLAN, un *Link Up* est généré dès que la connexion L2 sera établie (réception d'un RaS réussi), et un RS est émis. La détection de mouvement est accomplie quand le MN reçoit le premier message RA. La seule variable dans ce processus est le retard introduit par l'AR quand elle répond à un RS, qui dépend du MAX_RA_DELAY. La figure **Erreur ! Source du renvoi introuvable.**27 montre l'impact du MAX_RA_DELAY_TIME sur la durée du *handover*, quand le MAX_RA_DELAY_TIME change de 0 à 0.5s, elle prouve que la durée du *handover* change linéairement de 110ms à 350ms quand MAX_RA_DELAY_TIME change de 0 à 0.5s. La raison pour laquelle qu'un délai aléatoire du retard est nécessaire avant d'envoyer un RA en *multicast* pour éviter des collisions quand plusieurs routeurs opérationnels sur le même lien. Ce délai permet également à un routeur de recueillir plusieurs sollicitations et de répondre avec un seul RA à plusieurs sollicitations reçues au cours d'une courte durée.
Il est important de noter que l'utilisation d'un *Link Up* permet d'améliorer la bande passante due aux RA. En outre, si MAX_RA_DELAY_TIME est configuré convenablement (devrait dépendre du nombre de routeurs présent sur le lien), la durée de *handover* peut être réduite jusqu'à 110ms.
La figure 10 montre l'importance ou l'efficacité de détection de mouvement. Il change de 15% quand il n'y a aucun retard dans la réponse de RS, à 70% quand un délai aléatoire entre 0 et 500ms est introduit.

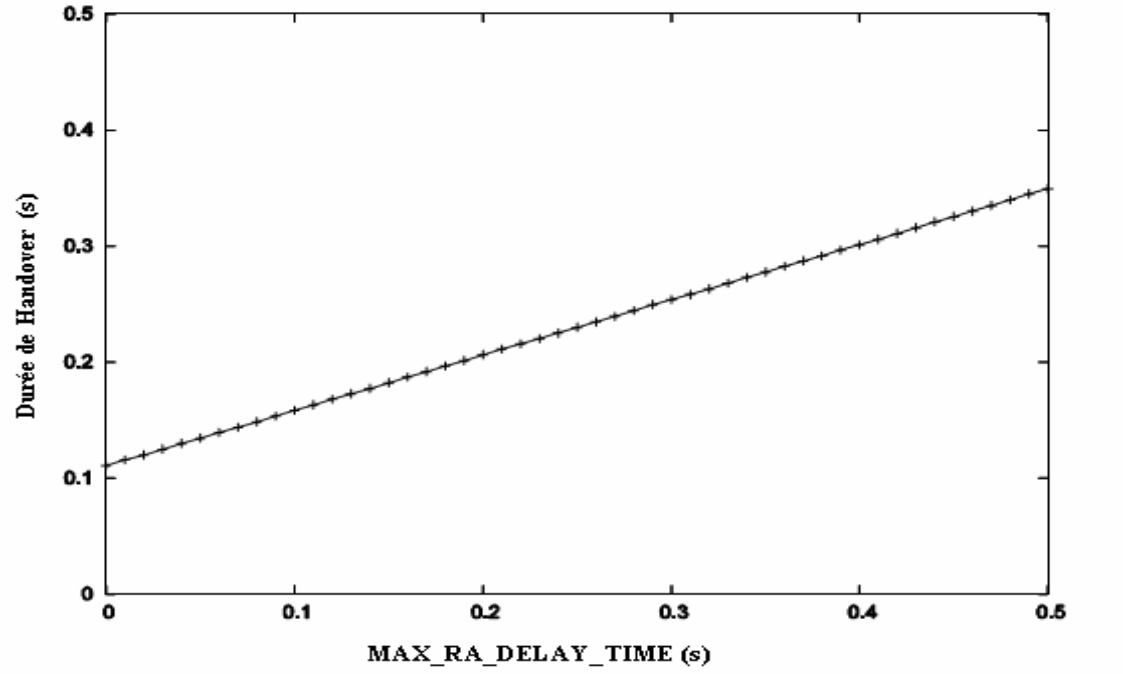

Figure 33 : Impact de MAX_RA_DELAY sur la durée de *handover* d'UMTS à WLAN

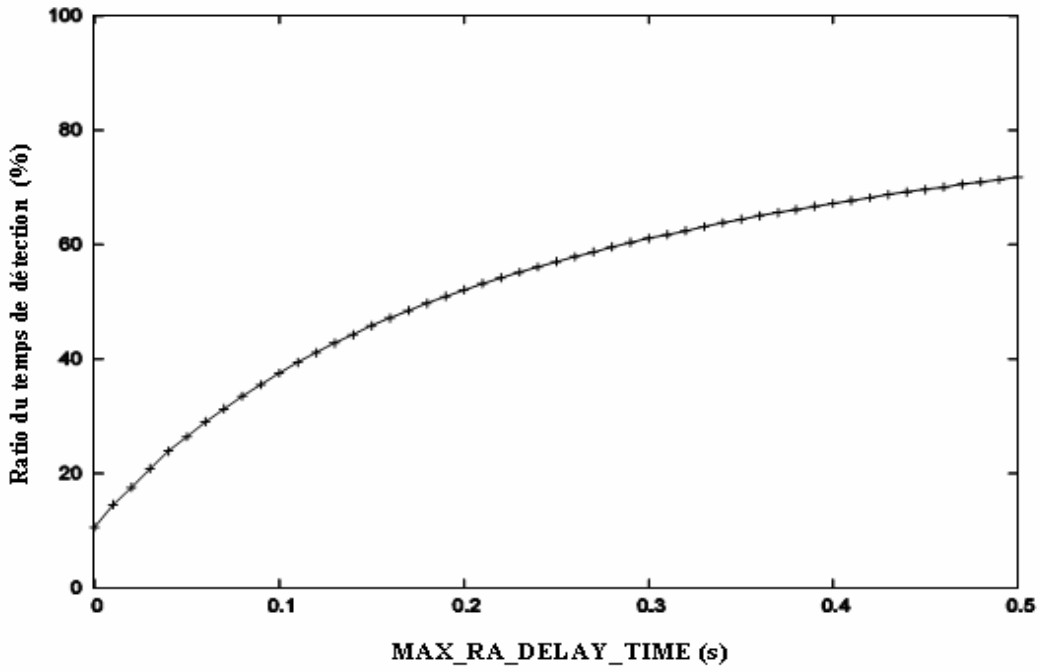

Figure 34: Impact de MAX_RA_DELAY sur la détection du mouvement durant le *handover* de UMTS à WLAN

2. L'influence du seuil de "*beacon*" manqué sur la performance du *handover*

Quand le MN quitte WLAN, il génère un *Link Down* suivant les conditions décrites dans la section ***1.g.iv*** Ensuite, le MN redirige le trafic vers l'interface UMTS, qui est déjà configurée

(c.-à-d., il n'y a aucun besoin de découvrir le routeur par défaut ou de créer une nouvelle adresse). Dans cette section, nous supposons qu'un *Link Down* est généré après un certain nombre de *beacon* consécutives manqués.

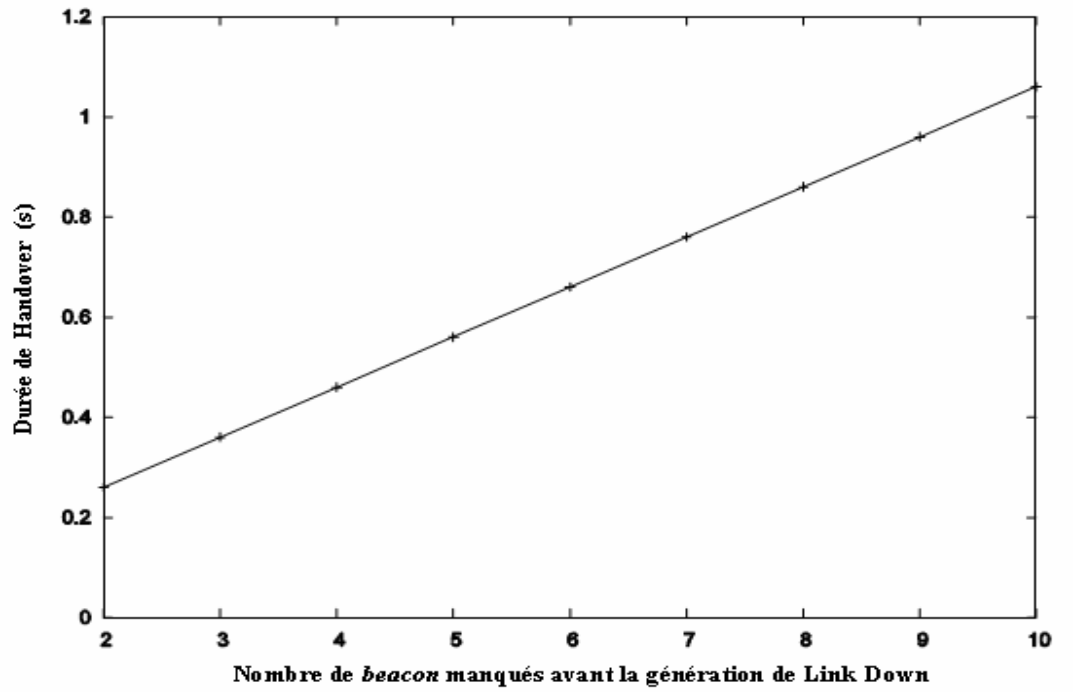

Figure 35: L'impact du nombre de *beacon* consécutifs manqués sur le *handover* de WLAN vers UMTS

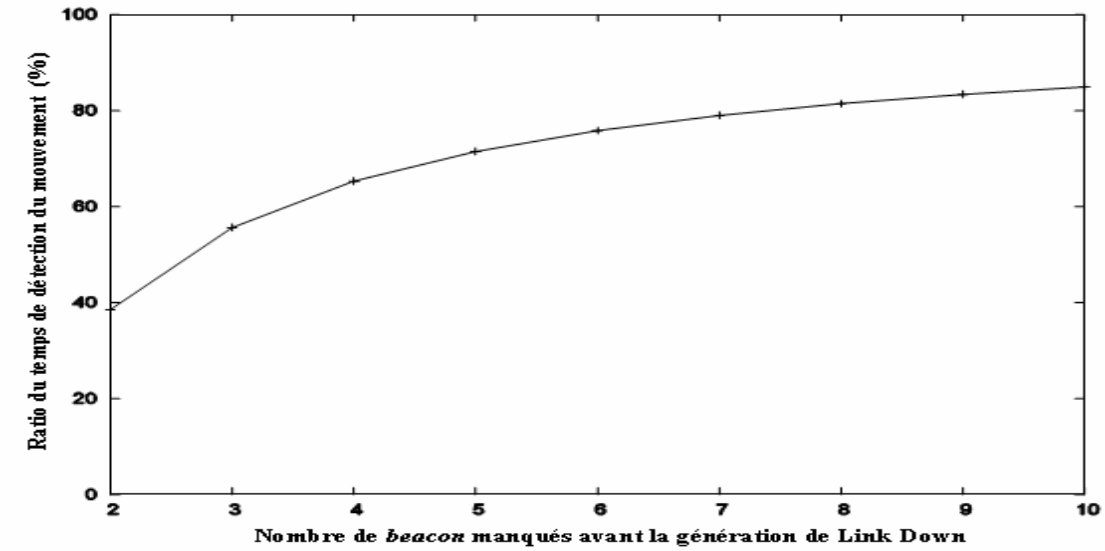

Figure 36: L'impact du nombre de *beacon* consécutifs manqués sur la détection du mouvement durant le *handover* d'UMTS vers WLAN

La figure 35 montre l'impact du nombre de *beacon* consécutif manqué sur la durée de *handover*. Nous ramarquons que pour chaque nouvel *beacon* manqué et avant de générer un *Link Down* une augmentation de la durée de *handover* par 100ms. La figure 36 montre l'efficacité de détection de mouvement, qui change de 38% à 84% de la durée de *handover*.

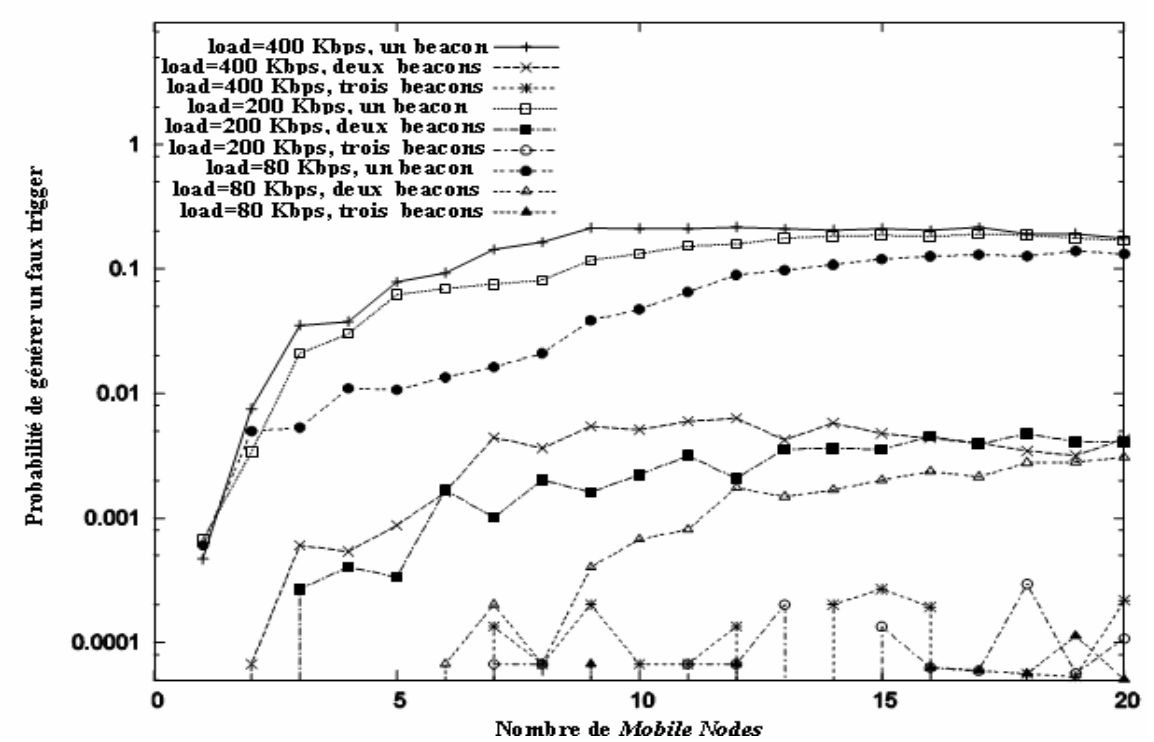

Figure 37: Probabilité de générer un faux *Link Down* quand ce *Link Down* est basé sur le nombre de *beacon* manqués

Afin de permettre le meilleur choix du seuil de *beacon* manqué, la figure 37 montre à la probabilité qu'un faux *Link Down* est généré en respectant le de *beacon* consécutifs manqués. Dans ce cas-ci, le nombre de stations stationnaires dans le WLAN change de 1 à 20. Les résultats de la figure 37 sont donnés pour différentes charge (*load*) par station. Quand le seuil considéré est un seul *beacon* manqué, la probabilité de générer un faux *Link Down* est élevée. Quand le WLAN contient plus que 5 stations, la probabilité de manquer un *beacon* est entre 1/100 et 1/10 quand la *load* offerte par station est égal à 80 kbit/S. La probabilité de générer un faux *Link Down* est aux alentours de 1/10 pour les *loads* de 200 et 400 Kbit/S. si un *Link Down* est généré après deux *beacon* consécutifs manqués, la probabilité de produire un faux événement est toujours au-dessous de 1/250.
En conclusion, il est important de savoir la valeur de la charge (*load*) afin de déterminer le seuil toléré pour les *beacon manqués* avant la génération d'un *Link Down*. D'après les résultats de simulation obtenus, ce seuil peut être égal à 2 par défaut.

3. L'effet du seuil d'erreur de paquet sur la performance du *handover*

La figure 38 montre l'impact du seuil d'erreur de paquet sur la durée du *handover*. La durée du *handover* augmente de 160ms à 358ms quand le seuil d'erreur de paquet varie de 1 à 50. La figure 39 montre l'efficacité de détection de mouvement durant le *handover*.
La figure 40 montre la probabilité de générer un faux *Link Down* en fonction de charge (*load)* d'un seul AP. La probabilité de générer un faux événement avec un seuil d'erreur vaut 3 paquets est négligeable (approximativement 1/10000). Par conséquent, la valeur recommandée - seuil d'erreur de paquet- soit 4.

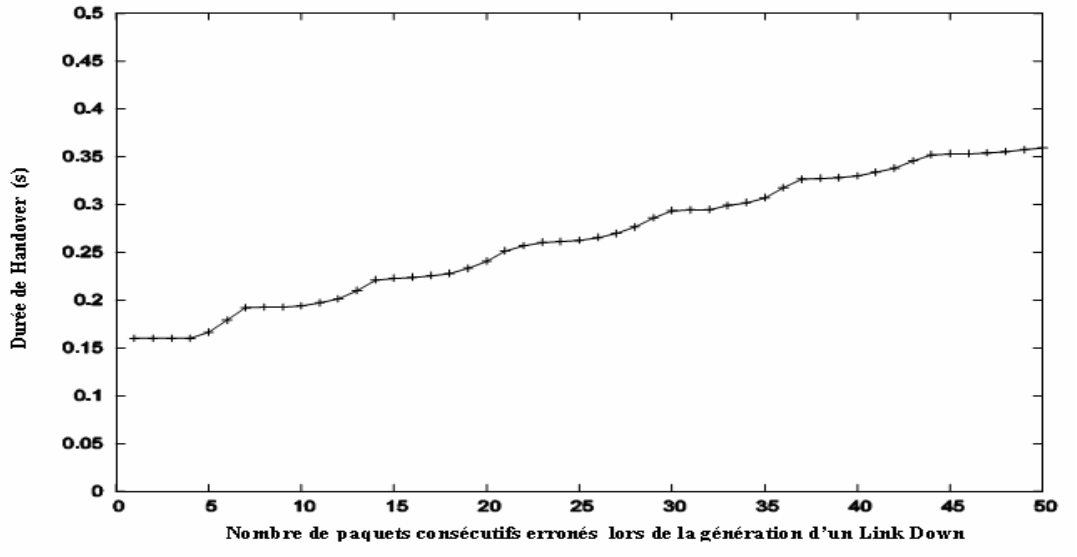

Figure 38 : Impact du nombre de paquets consécutifs reçus avec erreurs sur le *handover de* UMTS vers WLAN

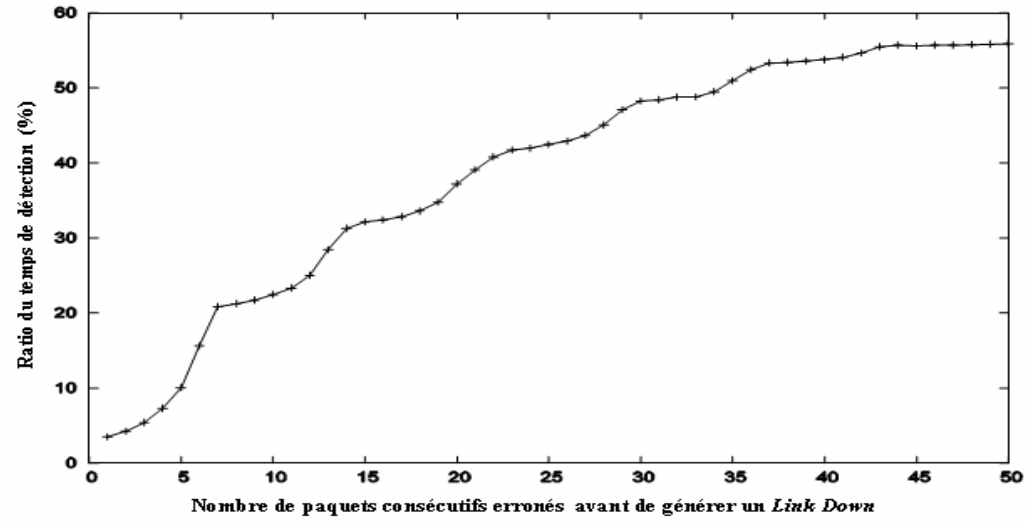

Figure 39 : Impact du nombre de paquets consécutifs resçus avec erreurs sur le rapport de la détection de mouvement durant le *handover* d'UMTS vers WLAN

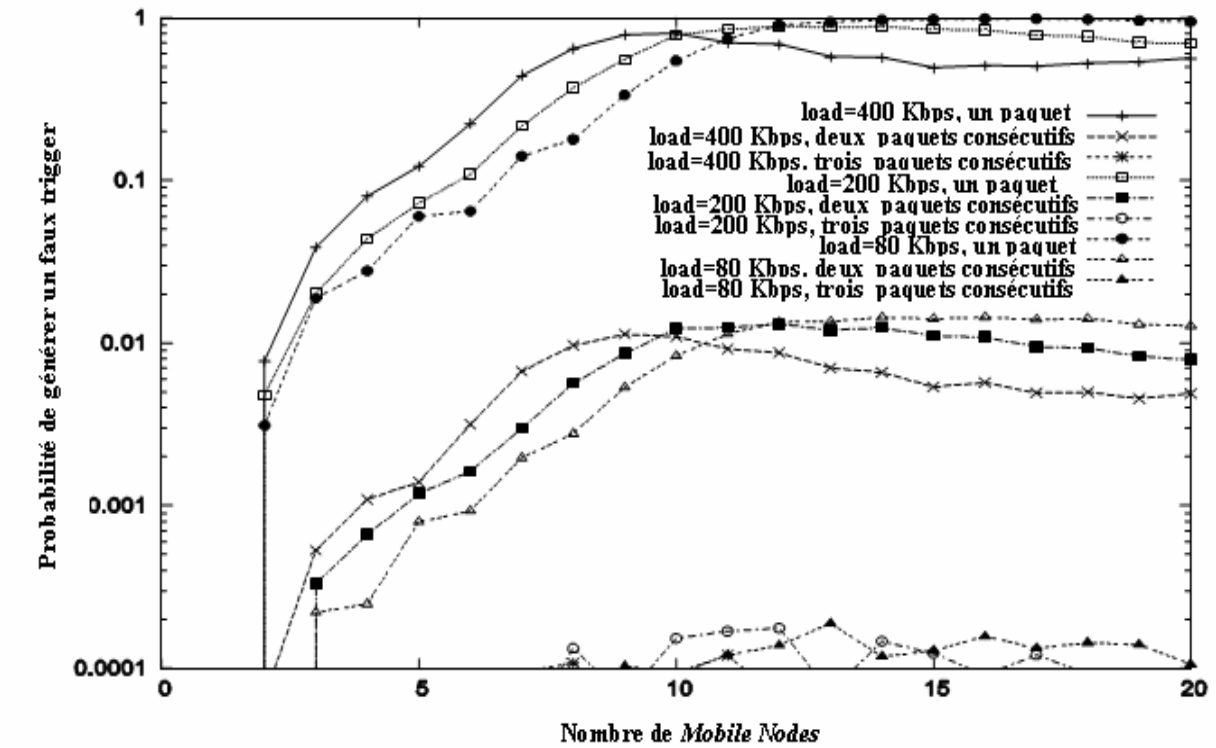

Figure 40 : Probabilité de générer un faux *Link Down*, quand ce *Link Down* est basé sur le nombre de paquets reçus avec erreurs

CONCLUSION

Dans ce chapitre, nous avons présenté l'architecture implémentée et nous avons décrit aussi le scénario de simulation afin d'étudier les performances du *handover* entre UMTS et IEEE 802.11.

Dans la première partie un aperçu général sur l'environnement du travail est abordé puis les différents éléments à ajouter ou à modifier sont détaillés. Dans la seconde partie nous avons analysé les résultats obtenus.

Finalement, après avoir étudié les métriques de performance du *handover* du réseau hétérogène, une étude de l'amélioration de la performance du *handover* sécurisé sera décrite dans le chapitre suivant.

Partie III : Proposition d'un *handover* sécurisé

CHAPITRE 5

Étude de *Handover* Sécurisé dans le cadre d'une mobilité hétérogène : Application entre UMTS et 802.11

Chapitre V : Étude de *Handover* Sécurisé dans le cadre d'une mobilité hétérogène : Application entre UMTS et 802.11

INTORDUCTION

Dans le chapitre III nous avons analysé les performances de *handover* entre UMTS et WLAN, un autre aspect d'importance extrême lors de l'exécution de *handover* que nous comptons discuter dans le présent chapitre c'est la sécurité. Dans un document récent publié par le groupe de recherche IEEE de 802.21 est intitulé *Security Optimization During Handovers*, il expose deux problématique à savoir la première est *Security Signaling Optimization during Handover* (l'optimisation de la signalisation de sécurité durant le *handover*) et la seconde est *MIH level security mechanism* (mécanisme de sécurité de MIH), après une longue analyse de deux problèmes nous avons décidé de faire une proposition pour le premier problème est en regardant un particulier l'authentification. En se basant sur une étude qui traite le problème de l'authentification dans le réseau hétérogène [11] nous avons pu élaboré une méthode d'authentification que nous avons appliquée dans le cas de l'interaction de UMTS et WLAN.

Ce chapitre est organisé comme suit. Au début nous parlons de Mobile IP et AAA et les associations de sécurité entre le deux protocoles, puis nous parlons de l'authentification, la gestion de clé dans UMTS, WLAN et Internet qui constitue le support de services, nous proposons par la suite les mécanismes d'authentification et de gestion des clés pour l'interaction entre UMTS et WLAN, et finalement la nouvelle signalisation de *handover* sera présenté.

I. Interaction entre Mobile IP et AAA

La gestion de la mobilité est un élément primordial dans les réseaux mobiles qui permet à un utilisateur mobile de continuer ses échanges des données en toute transparence, avant d'entamer la procédure du *handover* sécurisé entre UMTS et WLAN nous allons présenter l'interaction de Mobile IPv6 avec le protocole AAA à l'aide des associations de sécurité.

1. Mobile IPv6

Mobile IPv6 a été développé pour permettre à un MN de maintenir sa connexion à l'Internet en se déplaçant d'un AR à l'autre. Comme nous avons détaillé dans le chapitre 3 (§ II.1.b) le fonctionnement de Mobile IPv6, dans ce chapitre notre proposition pour un *handover* sécurisé tient en compte le Mobile IPv6. Afin de fournir la *seamless mobility*, on a proposé *Fast Handover* [50] et *Hierarchical Mobile IP* [51] comme des extensions de Mobile IPv6 pour réduire la latence de *Handover* et la perte de paquet.

2. AAA

Entendre le Mobile IPv6 pour effectuer des opérations commerciales à travers des domaines Administratifs, nécessite l'utilisation du Protocole AAA (*Authentication, Authorisation and Accounting*) [31]. Quand un utilisateur mobile doit accéder à des ressources fournies par un domaine administratif autre que son domaine mère, il doit être authentifié localement afin de s'assurer qu'il est autorisé à employer les ressources.

Bien que dans les réseaux cellulaires, par exemple GSM et UMTS, la mobilité et les problèmes liés à l'utilisation de AAA sont bien résolus, ils ont toujours lieu à sa dans l'Internet. Le groupe de recherche *IRTF AAAarch* a proposé une architecture générique de AAA [32] afin de permettre à une grande variétée d'applications qui fonctionne dans un environnement multi domaine, d'utiliser la fonctionnalité de AAA. Dans une telle architecture, des serveurs AAA génériques sont déployés dans différents domaines, qui sont capables d'authentifier des utilisateurs, de gérer les demandes d'authentification, et de rassembler des données.

Le RFC 2977 [33] décrivent une infrastructure permettant à des serveurs AAA d'authentifier et d'autoriser les demandes de MN d'accès au réseau. Un MN appartenant à son domaine mère a besoin des ressources dans un domaine étranger en fournissant une référence à un agent local. L'agent local consulte *local AAA authority* (AAAL) pour prouver l'authenticité de la référence fournie à l'aide d'un canal sécurisé. L'AAAL peut ne pas avoir l'information nécessaire pour vérifier la référence, dans ce cas il contacte une autorité externe (un autre AAAL) qui est le serveur AAA mère de MN (AAAH), pour obtenir ladite information.

Le protocole largement déployé du AAA est le *RADIUS* [34], qui a été conçu au début pour fournir une liaison point à point (PPP), mais il a certaines limitations mentionnées dans le RFC 3127 [35]. Un nouveau protocole RADIUS [36] est conçu afin fournir un les fonctionnalités de AAA pour des applications telles que l'accès de réseau ou la mobilité IP, qui sont considérés acceptable d'après le RFC 3127 [35]. On a également proposé son extension pour mobile IPv6 [37].

3. Les associations de sécurité

Pour le déploiement de mobile IP dans un environnement commercial, la sécurité est primordiale.

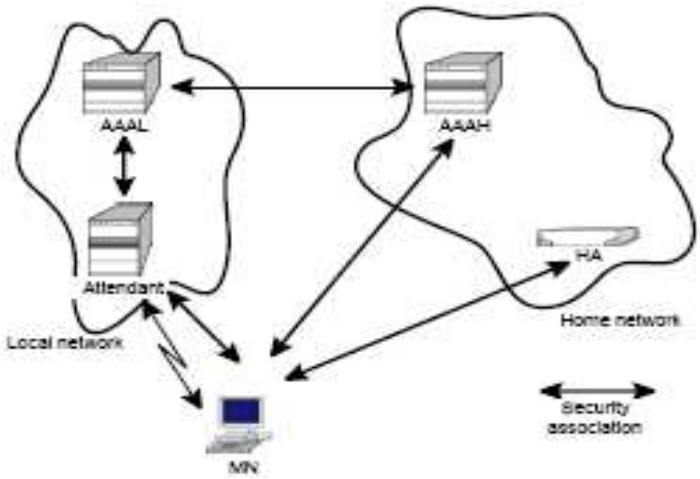

Figure 41 : Modèle de sécurité associant Mobile IP et AAA

IPsec [38] fournit les possibilités de sécuriser la communication à travers l'Internet. Un concept principal dans IPSec pour assurer l'authentification et la confidentialité est l'association de sécurité (*security association*), qui est un rapport à sens unique entre un émetteur et un récepteur, et offre des services de sécurité au trafic IP. Les clés secrètes d'IPSec**,** doivent être généré et distribuées aux entités participant dans la communication manuellement ou en utilisant des protocoles, tel que IKE [39].
Le protocole Mobile IPv6 spécifie un modèle de sécurité et exige l'utilisation d'IPsec pour protéger l'intégrité et l'authenticité des mises à jour et des acquittements [40] entre un MN et son réseau domicile voir figure 41. Les données communiquées entre l'AAAL et l'agent local peuvent être transmis via un canal sécurisé, parce qu'ils sont dans le même domaine. Il peut également supposer l'existence d'une clé secrète permanente partagée par le MN et l'AAAH. La communication entre l'AAAL et l'AAAH peut être protégée par un canal sécurisé préétablie grâce au *roaming* entre les deux domaines. Pour l'association de sécurité entre le MN et HA, le Mobile IPv6 exige une gestion manuelle et permet aussi la gestion automatique de clé à l'aide du protocole IKE. Cependant, la configuration manuelle n'est pas évolutif (*scalable*), et IKE a besoin de d'échanges beaucoup de message entre le MN et le HA [41]. D'ailleurs, il est également difficile de préétablir l'association de sécurité entre le MN et l'agent local donc, il doit dynamiquement l'établir sur demande.

II. Les Méthodes d'authentifications

Dans cette section, nous discutons l'authentification et les méthodes de gestion de clé pour UMTS, WLAN et l'Internet que nous jugeons nécessaires avant de détailler l'architecture et le modèle de *handover* proposé.

1. Le réseau UMTS

UMTS réalise l'authentification mutuelle d'un utilisateur et du réseau basés sur une *challenge-response* et un protocole basé sur un nombre de séquence [42]. Il emploie une clé secrète permanente K, qui est partagée entre les modules *User Services Identity Module* (USIM) situé dans *User Equipment* (UE) et centre d'authentification (AuC – *Authentification Center*) situé dans *Home Environment* (HE), il est important de signaler que seulement le deux modules mentionnés ci-dessous ont accès à la clé K. Au début, *International Mobile Subscriber Identity* (IMSI) est envoyée de l'UE non protégé au *Visitor Location Register* (VLR)/*Serving GPRS Support Node* (SGSN) par l'intermédiaire de *Radio Network System* (RNS), et encore transmis au *Home Location Registor* (HLR) de UE. Dans HE, des vecteurs d'authentification sont générés, chaque vecteur se compose d'un nombre aléatoire RAND, d'une réponse attendue XRES, d'une clef de cryptage CK, d'une clef d'intégrité IK et d'un jeton d'authentification AUTN. Les vecteurs d'authentification sont envoyés au VLR/SGSN, RAND et AUTN d'un vecteur sont envoyés à UE. L'UE authentifie le réseau en utilisant AUTN. Si l'authentification est réussie, elle calculera une réponse RES, une clé de cryptage CK, et une clé d'intégrité IK en utilisant la clef secrète K et le RAND. L'authentification est réussite si XRES et RES de l'utilisateur sont identiques. CK et d'IK vont être envoyé au RNS pour être utiliser respectivement en tant que clé de cryptage et d'intégrité. Le processus d'authentification est détallé sur la figure 42.

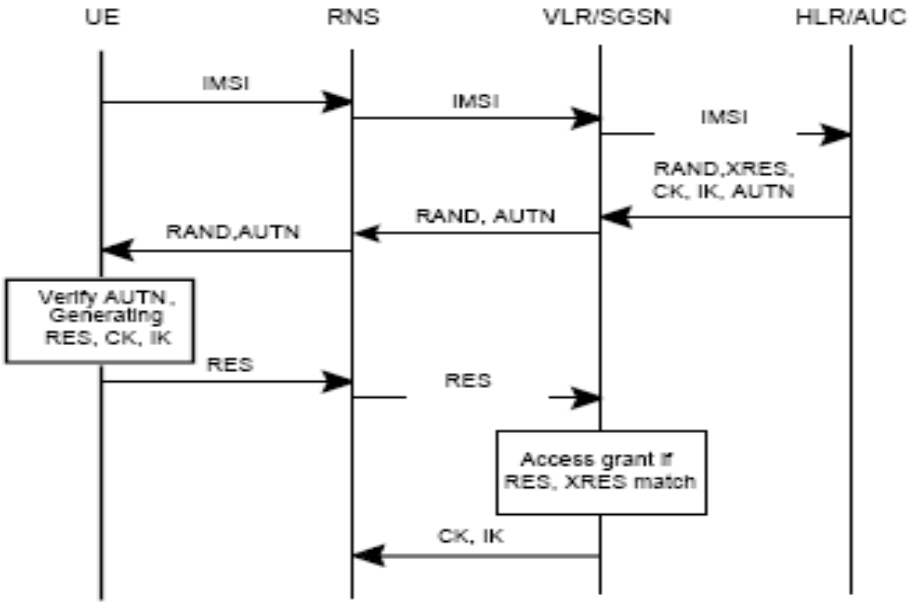

Figure 42 : Authentification et la génération de la clé pour UMTS

2. Le WLAN

Le standard IEEE WLAN 802.11i est normalisé pour améliorer la sécurité [43]. L'authentification de 802.11i implique trois entités : la station sans fil (STA), le point d'accès (AP), et le serveur d'authentification (AS).

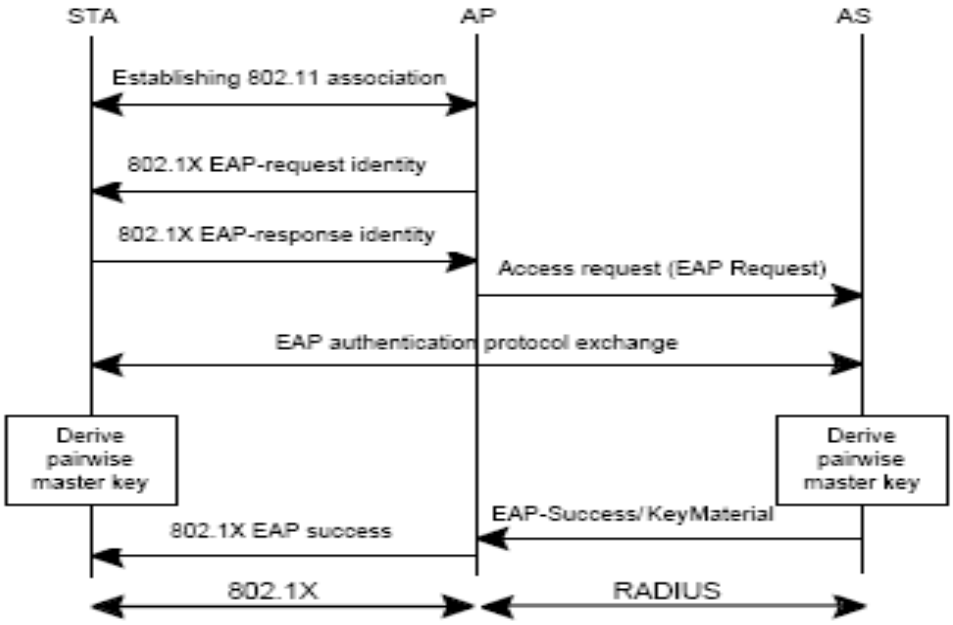

Figure 43 : Authentification de 802.11i

Le processus d'authentification se compose de deux phases: établissement de l'association 802.11, et l'authentification de 802.1X EAP (*Extensible Authentication Protocol*) [44], voire figure 43. Pendant la première phase, un STA est associé à un AP, et l'initialisation des paramètres de sécurité d'AP est faite.
La phase d'authentification utilise le protocole EAP, STA et AS sont mutuellement authentifiés. EAP contient plusieurs modèles d'authentification (*Authentication framework*) et supporte différentes méthodes d'authentification. Il supporte aussi une dérivation hiérarchique de clés principale afin de fournir les éléments essentiels pour compléter l'authentification. L'architecture de clé hiérarchique s'applique aussi à 802.11i. Dans la phase d'authentification, tous les deux AS et STA génèrent une *Master key* (MK) comme une clé mère, puis chacune dérive une paire de clé (PMK : *Pairwise Master Key*) pour être utilisé par le STA et son AP. Après l'authentification, un *four-way handshake* est exécutée entre le STA et son AP et une paire de clé (PTK : *Pairwise Transit Key*) est encore dérivé du PMK, et utilisé par le STA et l'AP afin de protéger l'ensemble de clé aussi que les données transfert. 802.11i également fournit plusieurs méthodes pour la confidentialité de données, l'authentification de l'origine de données et protection contre le rejeu.
Puisque le PMK est lié au STA et à son AP, quand le *handover* se produit, un nouveau PMK doit être dérivé et distribué au STA et au nouvel AP. Afin de mieux compléter le processus de *handover*, 802.11i propose également un mécanisme de pré-authentification pour la couche liaison de données, c.-à-d. un STA peut authentifier plusieurs AP avant que le *handover* se produit. Après le *handover*, le STA et le nouvel AP utilise *four-way handshake* pour dériver un nouveau PTK.

3. L'Internet

Les protocoles mobiles IP et AAA permettent aux utilisateurs mobiles d'obtenir les services d'Internet à travers différents domaines.

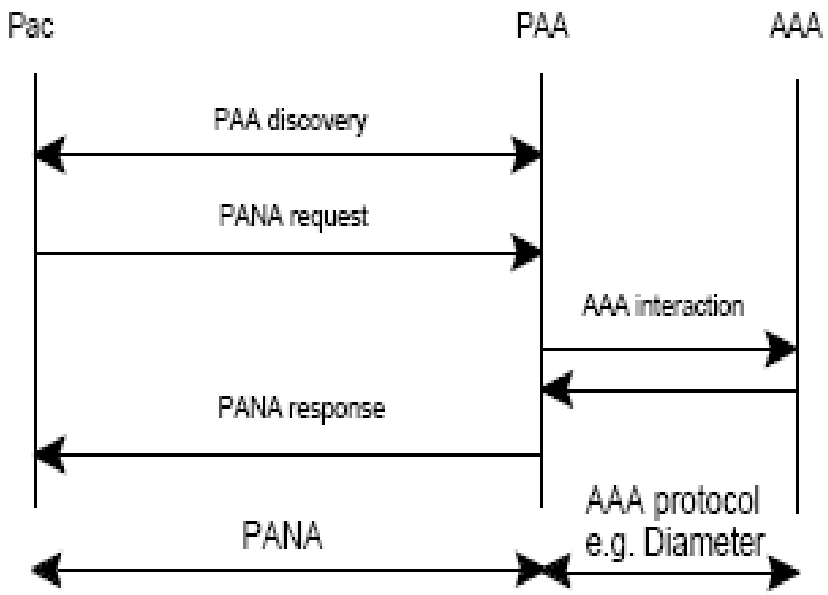

Figure 44 : Exemple de PANA

Diameter est un protocole AAA entre les serveurs AAA et les clients, il ne spécifie aucun mécanisme particulier pour l'authentification d'accès au réseau entre un MN et un client AAA. Le groupe de travail d'IETF *Protocol for Carrying Authentication for Network Access* (PANA) a pour objectif de concevoir un protocole d'authentification d'accès à la couche réseau [45].
Dans PANA, l'entité désirant obtenir l'accès au réseau s'appelle PANA Client (PaC), et l'entité pour authentifier le PaC et garantit l'accès au réseau s'appelle *PANA Authentication Agent* (PAA). PANA identifie EAP comme sa charge utile qui peut supporter des différents méthodes d'authentification. Bien que EAP tourne au-dessus de la couche liaison de données, PANA permet à EAP de fonctionner au-dessus de l'IP, la figure 44 montre un simple échange de message de PANA. Au début, l'adresse IP d'un PAA est découvert et une session de PANA est établie entre un PaC et le PAA. L'authentification est effectuée en transférant des messages EAP dans des messages PANA entre le PaC et le PAA. Le PAA peut interagir avec un autre serveur AAA pour authentifier le PaC en utilisant les protocoles AAA, tel que *diameter*.
PANA se fonde sur des méthodes EAP pour établir une association de sécurité entre le PaC et le PAA pour se protéger.
En permettant la re-authentification rapide, PANA permet à un PaC de rétablir la session sans passer par le processus d'authentification.

4. L'interaction différentes méthodes d'authentification

Chacun de réseau UMTS et WLAN 802.11 possède sa propre méthode pour l'authentification et la dérivation de clé de la couche liaison de données. Pour l'accès sans fil, la sécurité de couche de liaison de données est indispensable, la raison est qu'il est particulièrement vulnérable aux attaques, ainsi la signalisation de la couche liaison de données et les données sensibles de l'utilisateur doivent être protégées. Par exemple, si la couche liaison de données n'est pas sécurisée, il est possible de lancer un déni de service, par conséquence n'importe quels mécanismes de sécurité pour les couches supérieures ne seront fonctionnels.
Tandis que le processus d'authentification d'UMTS est en fait une combinaison de la dérivation de clé et de la gestion de mobilité, ces processus sont encore séparés dans l'Internet. Le protocole de la couche réseau AAA peut être indépendant de la technologie sous-jacent de la couche liaison de données, fournit ainsi une méthode générique AAA pour interagir de divers systèmes. Si les protocoles AAA de la couche réseau sont employés pour l'accès sans fil, en plus de l'IPSec qui est exigé, la sécurisation de la couche liaison de données est également nécessaire. En principe, les clés de sécurité de la couche réseau et la couche liaison de données peuvent être dérivées dans des processus séparés, et la gestion de mobilité et les procédures d'AAA peuvent également être découplées l'un de l'autre. Mais la signalisation pour ces procédures exigera beaucoup d'accès au HA du MN, qui occupe beaucoup de la bande passante, et peut mener à une longue latence de signalisation**.** Une solution optimale est de combiner la gestion de mobilité avec la procédure d'AAA, et

entretemps la dérivation de clés de la couche réseau et celle de la liaison de données est effectuée.

III. L'architecture proposée

L'architecture que nous proposons consiste à utiliser les protocoles AAA, *Diameter*, EAP, PANA, Mobile IPv6 et IPSec.
Dans cette section nous discutons le modèle générique d'AAA par la suite nous détaillons la méthode d'authentification et nous terminons avec la méthode de gestion de clé que nous avons proposé.

1. Le Modèle Général

En analysant la fonctionnalité d'AAA, les entités d'UMTS, WLAN et l'Internet montrent quelques ressemblances. Ainsi le protocole AAA pour l'accès sans fil à l'Internet dans toutes les architectures IP peut être décrit par un modèle général. En Supposant qu'un client (*supplicant* --- dans le tableau il est désigné par *A authentifié*) a un contrat de service avec son réseau mère, quand il désire avoir accès à un réseau étranger, il doit être authentifié par le réseau. Les informations de l'utilisateur seront envoyées à un authentificateur local, et l'authentificateur contacte l'AAAL pour la décision d'authentification. L'AAAL peut ne pas avoir assez d'information pour authentifier le client et contactera dans ce cas l'AAAH dans le HA du client. Les entités présentes dans le modèle général, par exemple A authentifié, l'authentificateur, l'AAAL et l'AAAH chacune a sa correspondante dans les différentes technologies, conformément au Tableau 1. Il n'y a pas AAAH pour PANA et WLAN, parce que PANA considère seulement l'authentification entre l'utilisateur et le réseau d'accès, et le WLAN ne traite pas le réseau mère.

	A authentifié	Authentificateur	AAAL	AAAH
IP mobile	MN	Agent	AAAL	AAAH
PANA	PaC	PAA	Serveur AAA	
UMTS	UE	RNS	VLR/SGSN	HLR/AuC
802.11	STA	AP	AS	

Tableau 3 : Entités d'AAA

D'après le § II.4 nous avons montré que l'IPSec entre le MN et l'authentificateur aussi, entre le MN et le HA doivent être établis dynamiquement. En outre, la sécurisation de la couche liaison de données entre le MN et l'authentificateur est nécessaire. Si la couche liaison de données est sécurisée entre le MN et l'authentificateur, l'IPSec entre le MN et l'agent n'est pas nécessaire

2. Authentification

Dans le futur scénario d'interaction de réseaux sans fil basé sur IP, les AP seront également des routeurs, par exemple, l'architecture développée par Moby Dick [46]. L'avantage de la méthode d'authentification de couche réseau est que c'est une méthode générique, qui peut

être utilisée pour différentes implémentation de la couche liaison de données, et indépendant de n'importe quelle technologie de la couche liaison de données [45]. Par conséquent, elle convient au scénario d'interaction de réseaux sans fil basé sur IP. Le couplement de PANA et de *Diameter* peuvent fournir l'authentification de la couche de réseau; PANA est employé pour l'authentification d'accès entre un client et un authentificateur, et le *Diameter* est utilisé pour la communication entre les serveurs AAA et les clients.
La figure 45 montre le processus d'authentification pour un MN qui est une concaténation de PANA au niveau du lien sans fil et de *Diameter* au niveau du réseau, tous les deux diffusent des messages EAP pour l'authentification. Quand un MN est attaché au réseau, il découvre l'agent AAA en envoyant un message PANA de découverte. Des *cookies* sont échangés dans les messages qui suivent, ils sont utilisés pour empêcher les attaques de genre utilisation non autorisé de ressource. Des messages EAP sont échangés entre le MN et ses serveurs AAA pendant l'authentification; EAP permet à différentes méthodes d'authentification d'être utilisées, et il est supporté par PANA et *Diameter*. Les messages détaillés dépendent de la méthode d'authentification choisie par le réseau. Par exemple, en utilisant l'algorithme *UMTS Authentication and Key Agreement* (AKA) dans les messages EAP [47], le MN et le réseau d'accès sont mutuellement authentifiés nécessitant seulement un seul accès au réseau mère. Le processus décrit ci-dessus ressemble à celle d'UMTS illustrée dans la figure 2 mais, les messages d'authentification échangés sont des messages EAP encapsulé dans des paquets IP. Les messages sont échangés sur le lien sans fil en utilisant PANA, et sur le réseau en utilisant *Diameter* à l'aide de l'infrastructure AAA.

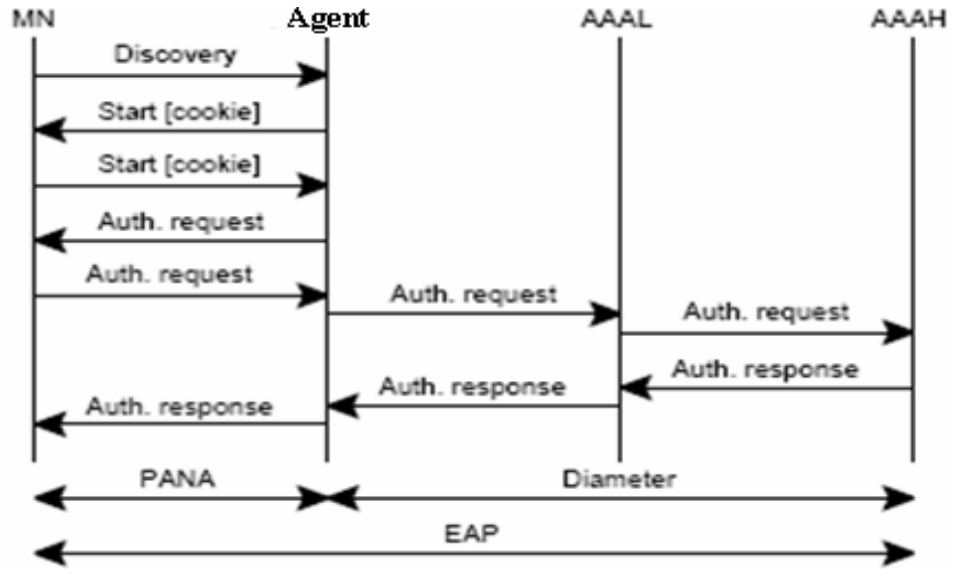

Figure 45 : Signalisation de l'authentification

L'agent peut être un AR fournissant le service mobile IP, et également agir en tant que PaC pour communiquer les messages de PANA avec MN, pendant ce temps, il peut fonctionner comme *AAA attendant* pour communiquer avec AAAL. Selon la technologie utilisée, l'agent

peut aussi préformer les fonctions de réseau et de la radio comme RNS en cas d'UMTS ou AP en cas de WLAN. S'il a une interface sans fil avec MN, il a besoin également des clés de sécurité pour la couche liaison de données afin de protéger les données échangées.
Le scénario d'authentification mentionné ci-dessus est une approche générique pour la couche réseau, indépendant de n'importe quelle technologie de la couche liaison de données. Les différentes méthodes d'authentification peuvent être supportées grâce à l'utilisation d'EAP. L'infrastructure AAA peut également être utilisée afin d'optimiser la gestion de mobilité. Par exemple, l'extension *Diameter Mobile IPv6* [48] emploie l'infrastructure AAA pour supporter la gestion de mobilité et pour distribuer les clés de sécurité. Ceci demande en outre une interface entre AAAH et AH.

3. Génération de clé

Les clés nécessaires pour IPSec exigé par Mobile IPv6 peuvent être dérivées en utilisant IKE. Cependant, les entités d'AAA peuvent jouer un rôle important dans la dérivation et la distribution des clés. *Diameter* est utilisé pour aider à la distribution des clés, celles-ci peuvent être dérivées en utilisant des nombres aléatoires ou l'algorithme de *Diffie-Hellman* [48]. Afin d'avoir une connexion sécurisée pour la couche liaison de données, les clés de sécurité de ladite couche doivent être dérivées. Ceci peut être réalisé en les combinant avec la dérivation des clés d'IPSec.
PANA et *Diameter* utilisent EAP pour envoyer les messages d'authentification, et EAP utilise une architecture hiérarchique pour les clés. L'architecture hiérarchique de clés sera bénéfique pour la dérivation de clé de la couche liaison de donnés, aussi bien que pour le *handover* verticale, qui sera discutée dans la prochaine section. Par exemple, la dérivation de clé basée sur des nombres aléatoires est comme suit. Après la réception de la demande d'authentification d'un MN envoyé par AAAL dans un domaine différent, l'AAAH génère deux nombres aléatoires, un pour IPSec utilisé entre le MN et HA, et l'autre pour la clé de sécurité de la couche liaison de données entre le MN et l'agent (*attendant*). Par la suite AAAH dérive des clés pour IPSec et de la couche de liaison de données en utilisant les deux nombres aléatoires, et partage ce secret le MN**.** La clé d'IPSec sera envoyée à l'HA à travers un canal sécurisé dans le réseau mère (*home network)* du MN, et l'HA utilise ladite clé pour dériver des clés *inbound* et *outbound* d'IPsec partagées avec le MN. Dans le message de réponse d'authentification, l'AAAH envoie à l'AAAL la clé de la couche liaison de données et deux nombres aléatoires en utilisant des messages *diameter*. Et l'AAAL utilisera la clé de la couche liaison de données comme une clé *Master Session Key* (MSK) d'EAP pour dériver une clé clef *Transient Session Key* (TSK) et envoie le TSK à l'agent pour compléter le cryptage. Les deux nombres aléatoires générés par l'AAAH seront également transfert dans le message de réponse d'authentification puis envoyés au MN. Le MN utilisera ces deux nombres aléatoires et la clé partagée pour dériver les clés d'IPSec avec HA, et également le MSK et le TSK.

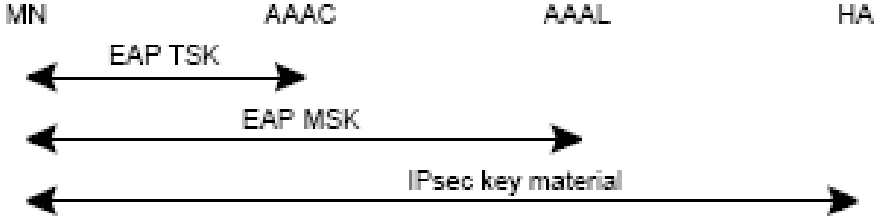

Figure 46 : Les clés dérivées

Le scénario proposé est une combinaison d'authentification et de dérivation de clé pour IPSec et la couche liaison de données. Les clés dérivées sont montrées dans la figure 46. Le MSK est partagé entre AAAL et le MN. Le TSK est partagé entre le MN et l'agent, et les clés de sécurité peuvent être dérivées de TSK pour différentes technologies de la couche liaison de données. L'algorithme de dérivation de clés ainsi d'authentification sont indépendant de la technologie déployé au niveau de la couche liaison de données, par conséquence il est recommandé pour les réseaux hétérogènes sans fil. Cet algorithme n'exclut aucune autre dérivation de clés, et ils peuvent être dérivés et distribués de la même manière une fois nécessaires.

IV. La procédure de *Handover* proposée

Dans cette section nous allons décrit le *handover* sécurisé, au début nous discutons les pré-requis pour exécuter le *handover* et puis nous détaillons le *Fast Handover* proposé.

1. Préambule

IPv6 mobile [40] ne traite pas la façon dont les sessions AAA peuvent être rétablies dans le nouveau réseau après *handover*. Afin de rétablir rapidement le contexte de service après *handover*, on a proposé le protocole de transfert de contexte [49] par l'IETF. Le contexte de service, comme le QoS et le contexte AAA peuvent être transférés à partir de l'ancien routeur d'accès (oAR- *old Access Router*) au nouveau routeur d'accès (nAR- *new Access Router*), ainsi le contexte de service peut être rétabli rapidement sans exiger au MN de l'établir à partir de zéro. Pour un MN l'adresse temporaire CoA dans le réseau étranger, sera utilisé avec son adresse dans le réseau mère pour assortir la politique de sécurité d'IPsec [40].
Par conséquent, après *handover*, l'IPSec entre le MN et HA peut rester sans changement.
Dans ce cas, le transfert de contexte est utile. Mais le transfert de contexte, particulièrement s'il est utilisé dans l'interaction entre UMTS et WLAN, a ses limitations, parce que certaine informations ne peut pas être transférée, mais devrait être plutôt renouvelées après le *handover*. Par exemple, dans le cas de *handover* entre deux technologies différents (comme notre cas : UMTS et WLAN), due aux différentes options d'accès sans fil, l'autorisation d'accès dans l'ancien réseau peut ne pas être valide dans le nouveau réseau, c'est-à-dire, un service est utilisé dans l'une de technologie d'accès peut n'est pas existé dans l'autre technologie.
Dans ce cas, avant le *handover*, le serveur AAA doit être consulté et la nouvelle autorisation doit être issue du nouveau réseau d'accès. En outre, le *handover* vertical, renouvelle les clés de sécurité pour la nouvelle couche de liaison de données, parce que celle-ci peut utiliser un algorithme de cryptage diffèrent de l'ancien. Il est également nécessaire que les nouvelles clés soient indépendantes des anciennes clés de la couche liaison de données, puisque une contrainte de sécurité pour un lien d'accès n'est pas nécessairement la même pour un autre lien.

2. Fast Handover

Depuis que le transfert de contexte seul ne fonctionnera pas pour le *handover* vertical, une signalisation est sollicitée pour le rétablissement du contexte AAA dans le nouveau réseau. Afin de réduire la latence de *handover* due aux mécanismes de sécurité utilisé, la nouvelle autorisation et les clés de la couche liaison de données peuvent être obtenues avant le

handover. Ces mécanismes peuvent être combinés avec *Fast Handover* proposées par IETF [50], de sorte que *seamless handover* soit possible, voir figure 47.

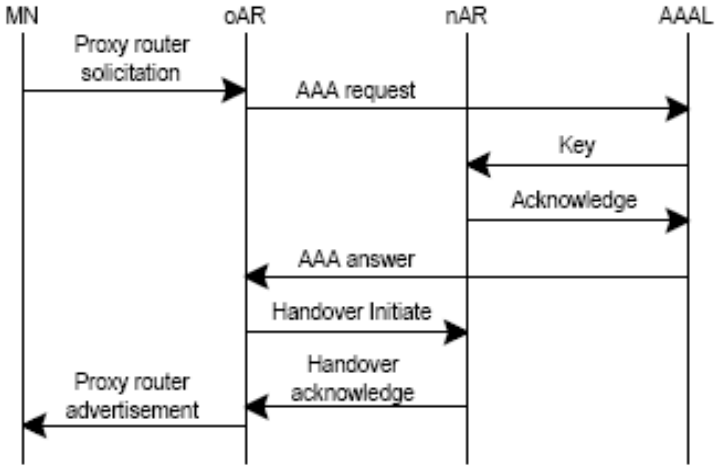

Figure 47 : Signalisation de *Fast handover*

Avant le *handover*, le MN envoie un RS à l'ancien routeur d'accès (oAR) indiquant l'identité du nouveau routeur d'accès (nAR) afin de demander le support de *Fast Handover* (*to request Fast Handovers support*). Avant de continuer la procédure de *Fast Handover*, l'oAR envoie tout d'abord une demande AAA à l'AAAL au nom du MN. L'AAAL fait la nouvelle autorisation et dérive un nouveau TSK en utilisant un défi (*challenge*) et le MSK partagé avec le MN. L'AAAL envoie alors le TSK au nAR. Quand un acquittement est reçu de l'nAR, un acquittement d'AAA avec le défi sera envoyé à l'oAR. L'oAR continue alors la *Fast handover* en envoyant un message d'initiatisation de *handover* au nAR, les informations de contexte peuvent être incluses dans ce message. Après la réception du message de l'acquittement de *handover* du nAR, l'oAR peut envoyer RS du *Proxy* avec le défi au MN. Le MN peut alors dériver un nouveau TSK en utilisant le MSK et le défi, et continue à exécuter le *handover*.
Il peut voir qu'en combinant la re-autorisation et la nouvelle dérivation des clés à l'aide de la signalisation de *Fast Handover* avant l'exécution de *handover*, la latence due au *handover* est maintenue petite, ainsi le *seamless handover* est possible. En outre, en utilisant l'architecture hiérarchique de clé d'EAP, la nouvelle clé de la couche de liaison de données peut être indépendante et dérivée de l'ancienne clé, et la signalisation est exigée seulement dans le même domaine.

CONCLUSION

En guise de conclusion nous avons vu dans ce chapitre une proposition d'un *handover* sécurisé dans un réseau hétérogène constitué de deux réseaux UMTS et WLAN, en outre pour supporter l'interaction d'UMTS et du WLAN dans les réseaux sans fil basé sur IP, une architecture générique d'AAA et le mécanisme d'AAA sont nécessaires. L'interaction passe sur une architecture générique d'AAA proposée par le groupe de recherche d'IRTF *AAAarch Research Group*. L'authentification est effectuée au niveau de la couche réseau par la concaténation de *Diameter* et de PANA et en utilisant EAP comme support pour les méthodes d'authentification. En plus, par l'intégration de la dérivation des clés avec le processus d'authentification, les clés de la couche réseau et de la couche liaison de données peuvent être dérivés. Pour le *handover* vertical entre le deux réseaux, seul le transfert de contexte n'est pas complet, parce que la nouvelle autorisation et les nouvelles clés de sécurité de la couche liaison de données doivent être obtenues par le nouveau réseau. Ces procédures peuvent être combinées avec des la signalisation de *Fast Handover*, ainsi la latence résultante du *handover* est maintenue petite.

CONCLUSION & PERSPECTIVES

CONCLUSION

CONCLUSION & PERSPECTIVES

Notre objectif, précisé dès le départ, était de balayer les diverses technologies de communications sans fils que se soient celles de couverture locale tel que WLAN, ou de couverture globale tel que UMTS, dans le but à arriver à la combinaison de ces technologies ensemble et à aboutir à passer d'une à une autre d'une façon transparente.

Pour arriver là, il a fallu traverser beaucoup d'obstacles et passer des heures à apprendre, concevoir, installer et même programmer. Il était très difficile de trouver des informations significatives sur l'Internet, surtout que le sujet que nous abordons est un sujet très récent et les études déjà faites et sont très publiées peu.

Le standard international *IEEE 802.11* décrit les caractéristiques d'un réseau local sans fil, son réseau est basé sur une architecture cellulaire où le système est divisé en des cellules BSS dont chacune est contrôlée par une station de base AP.

Les stations, se trouvant dans le BSS, communiquent ensemble soit directement l'un avec l'autre en mode ad'hoc, soit via l'AP en mode d'infrastructure.

Le *Handover* entre ces différents types de réseaux devient alors une nécessité ainsi qu'un potentiel qui ouvre la porte à beaucoup des applications.

Quant à la partie purement pratique de mon travail, je peux évoquer les points suivants :

- ✧ Se familiariser avec le logiciel choisi NS était une phase délicate, cela revient au fait que ce logiciel utilise plusieurs langages de programmation, TCL, OTCl et le C++. Par suite, pour un cas comme le mien où il était nécessaire de créer quelque chose qui n'existe pas encore dans NS, il était nécessaire d'entrer dans plusieurs détails qui ne peuvent du tout être classifiés comme faciles.
- ✧ J'ai affronté un grand problème qui n'était pas prévu dès le départ, c'est le problème de l'incompatibilité existante dans NS, par suite un patch qui fonctionne normalement sur une version de NS, ne fonctionne pas sur une autre. Et vu que le scénario que j'ai proposé nécessite l'utilisation de plus d'un patch tel que chacun d'eux fonctionne sur une version différentes de NS, je me trouve devant un seul choix, c'est de changer un peu dans le scénario de telle sorte à conserver le but désiré et dans le même temps dépasser le problème d'incompatibilité.
- ✧ Toutefois, il est nécessaire de noter à ce stade là que l'installation de NS ainsi que des *patch* correspondants pose pas mal de difficultés, parfois ça dépend du PC lui-même et des programmes qui y sont installés et parfois il donne des erreurs sans savoir même quelles sont les causes.

Dans le dernier chapitre nous avons proposé une méthode d'authentification pour un réseau hétérogène UMTS/WLAN.

Finalement, il faut bien signaler quelques perspectives pour l'avenir. Avoir la possibilité d'améliorer l'architecture proposée pour diminuer la latence de *handover*.

Encore en ce qui concerne le *Handover* Vertical sécurisé nous envisageons de l'implémenter sous NS-2.

Signalons en fin que ce sujet est très récent et cette étude est plutôt le sujet d'une thèse. Le travail que j'ai fait n'est qu'une introduction et il reste beaucoup du travail à faire.

BIBIOLGRAPHIE & NETOGRAPHIE

BIBLIOGRAPHIE

BIBIOLGRAPHIE & WEBOGRAPHIE

[1] Bishop, M. Computer Security: Art and Science. Boston: Addison-Wesley, 2003.
[2] Bishop, M. Introduction to Computer Security. Boston: Addison-Wesley, 2005.
[3] Pfleeger, C. Security in Computing. Upper Saddle River, NJ: Prentice Hall, 2002.
[4] Pieprzyk, J.; Hardjono, T.; and Seberry, J. Fundamentals of Computer Security. New York: Springer-Verlag, 2003.
[5] Schneier, B. Secrets and Lies: Digital Security in a Networked World. New York: Wiley 2000.
[6] William Stallings Cryptography and Network Security Principles and Practices. New York: Prentice Hall 2005.
[7] Anand R.Prasad, Neeli R. 802.11 WLANS and IP Networking. Boston: Artech House 2005.
[8] ITU-T. Security architecture for open systems interconnection for ccitt applications. X.800 (Recommendation), Geneva 1991.
[9] R. Shirey. Internet Security Glossary. RFC 2828, Mai 2000.
[10] ISO/IEC 8802-11, ANSI/IEEE Std 802.11, First Edition 1999-00-00, Information Technology — Telecommunications and information exchange between systems — Local and metropolitan area networks — Specific requirements — Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications.
[11] D. Johnson, C. Perkins, and J. Arkko. Mobility Support in IPv6. RFC 3775 (Proposed Standard), Juin 2004.
[12] S. Thomson and T. Narten. IPv6 Stateless Address Autoconfiguration. RFC 2462 (Draft Standard), Décembre 1998.
[13] Perkins., C., "IP Mobility Support. RFC 2002 (Proposed Standard), Octobre 1996.
[14] Obsoleted by RFC 3220, Mis à jour par RFC 2290. C. Perkins. IP Mobility Support for IPv4. RFC 3344 (Proposed Standard), Août 2002.
[15] 802 groups websites: http://grouper.ieee.org/groups/802/.
[16] Mobile IP WG: http://www.ietf.cnri.reston.va.us/html.charters/mobileipcharter.html.
[17] R. Droms. Dynamic Host Configuration Protocol. RFC 2131 (Draft Standard), Mars 1997. Mis à jour par RFC 3396.
[18] J. Postel. Internet Control Message Protocol. RFC 792 (Standard), Septembre 1981. Mis à jour par RFC 950.
[19] H. Krawczyk, M. Bellare, and R. Canetti. HMAC: Keyed-Hashing for Message Authentication. RFC 2104 (Informational), Février 1997.
[20] D.C. Plummer. Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware. RFC 826 (Standard), Novembre 1982.
[21] C.Perkins. IP Encapsulation within IP. RFC 2003 (Proposed Standard), Octobre 1996.
[22] G. Heine. *GSM networks: protocols, terminology, and implementation*. Artech House, 1999.
[23] Anand R.Prasad, Neeli R. 802.11 WLANS and IP Networking. Boston: Artech House 2005.

[24] Laurentiu Sorin PAUN. Thèse, Gestion de la mobilité dans les réseaux ambiants ,2005.
[25] Francine NGANI NOUDEM. Thèse, Une méthodologie pour le test de conformité et d'interopérabilité des protocoles de mobilité ,2006.
[26] P. Rinbold. Un cadre générique de comparaison pour la micro-mobilité sous IP. Technical report, Groupe Infonet, Université de Namur, Belgique, Octobre 2001.
[27] A. T. Campbell, J. Gomez, and A. G. Valko. An Overview of Cellular IP, 1999.
[28] Site Web de NS-2: *www.isi.edu/nsnam/ns.*
[29] Site Web de IEEE 802.21: *www.ieee802.org/21/.*
[30] Site Web de EURANE: *www.ti-wmc.nl/eurane/.*
[31] Charles E. Perkins, "*Mobile IP Joins Forces with AAA*" IEEE Personal Communications, Aug. 2000.
[32] C. de Last, et al. "*Generic AAA Architecture*" IETF RFC 2903, Aug. 2000.
[33] S. Glass, et al. "*Mobile IP Authentication, Authorization, and Accounting Requirements*" IETF RFC 2977 Oct. 2000.
[34] Rigney, C., Willens, S., Rubens, A. and W. Simpson, "*Remote Authentication Dial In User Service (RADIUS)*" IETF RFC 2865, Jun. 2000.
[35] D. Mitton, M. St.Johns, S. Barkley, D. Nelson, B. Patil, M. Stevens and B. Wolff, "*Authentication, Authorization, and Accounting: Protocol Evaluation*" IETF RFC 3127, Jun. 2001.
[36] P. Calhoun, J. Loughney, E. Guttman, G. Zorn and J. Arkko, "*Diameter Base Protocol*" IETF RFC 3588, Sep. 2003.
[37] Stefano M. Faccin et al., "*Diameter Mobile IPV6 application*" IETF Internet draft, draft-le-aaa-diameter-mobileipv6-03, Apr. 2003.
[38] S. Kent, and R. Tension, "*Security Architecture for the Internet Protocol*" IETF RFC 2401, Nov. 1998.
[39]D. Harkins and D. Carrel, "*The Internet Key Exchange (IKE)*" IETF RFC 2409, Nov. 1998.
[40] D. Jingoism, C. Parkins, J. Argue, "*Mobility Support in IPv6*" IETF draft-ITV-mobiles-ipv6-19.txt, work in progress, Oct. 2002.
[41] J. Arkko, V. Devarapalli, and F. Dupont, "*Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents*" IETF draft-ietf-mobileip-mipv6-ha-ipsec-06.txt, work in progress, Jun. 2003.
[42] 3GPP TS 33.102, V5.1.0 "3G Security: Security Architecture,"Dec. 2003.
[43] IEEE Std 802.11i/D4.1, "*Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Medium Access Control (MAC) Security Enhancements*" Jul. 2003.
[44] IEEE Draft P802.1X/D11, "*Standards for Local and Metropolitan Area Networks: Standard for Port based Network Access Control*" Mar. 2001.
[45] D. Forsberg et al., "*Protocol for Carrying Authentication for Network Access*" IETF Internet draft, draft-ietf-pana-pana-01.txt, Jun. 2003
[46] Moby Dick, "*Mobility and Differentiated Services in a Future IP Network*", http://www.ist-mobydick.org, Jan. 2003.
[47] J. Arkko and H. Haverinen, "*EAP AKA Authentication*" IETF Internet draft, draft-arkko-pppext-eap-aka-11.txt, Oct. 2003.
[48] Stefano M. Faccin et al., "*Diameter Mobile IPV6 application*" IETF Internet draft, draft-le-aaa-diameter-mobileipv6-03, Apr. 2003.

[49] J. Loughney, et al., "*Context Transfer Protocol*" IETF Internet draft, draft-ietf-seamoby-ctp-03.txt, Jun. 2003.
[50] Rajeev Koodli, "*Fast Handovers for Mobile IPv6*" IETF Internet draft, draft-ietf-mobileip-fast-mipv6-06.txt, Mar. 2003.
[51] Hesham Soliman, Claude Castelluccia, Karim El-Malki, Ludovic Bellier, "*Hierarchical Mobile IPv6 mobility management (HMIPv6)*" draft-ietf-mobileip-hmipv6-08.txt, work in progress, Jun. 2003.
[52] Wenhui Zhang, "*Interworking Security in Heterogeneous Wireless IP Networks*" University of Stuttgart, 2004.

ANNEXES

ANNEX I : NS-2

Pour la simulation nous avons utilisé NS-2 [28] qui est un logiciel de simulation de réseaux informatiques. Il est principalement bâti avec les idées de la conception par objets, de réutilisabilité du code et de modularité. Il est devenu aujourd'hui un standard de référence en ce domaine. C'est un logiciel dans le domaine public disponible sur l'Internet. Son utilisation est gratuite. Tout d'abord nous introduisons NS-2 et par la suite nous étudions un cas d'utilisation.

Introduction

Le simulateur est conçu principalement pour le monde de l'Internet et plus particulièrement pour le protocole TCP. Cependant, sa bonne organisation hiérarchique a permis son extension aux nouveaux protocoles du monde Internet (application, transport, et routage), aux nouveaux supports de transmission (LAN, satellite, mobile, ATM), et aux nouvelles architectures proposées pour améliorer la qualité du service dans l'Internet (RED, DiServ, IntServ). Il contient les fonctionnalités nécessaires à l'étude des algorithmes de routage unipoint ou multipoint, des protocoles de transport, de session, de réservation, des services intégrés, des protocoles d'application comme HTTP. De plus le simulateur possède déjà une palette de systèmes de transmission (couche 1 de l'architecture TCP/IP), d'Ordonnanceurs et de politiques de gestion de files d'attente pour effectuer des études de contrôle de congestion. La liste des principaux composants actuellement disponible dans NS par catégorie est:

Application	Web, ftp, telnet, générateur de trafic (CBR, ...)
Transport	TCP, UDP, RTP, SRM
Routage	Statique, dynamique (vecteur distance) et routage multipoint (DVMRP, PIM)
Gestion de file d'attente	RED, DropTail, Token bucket
Discipline de service	CBQ, SFQ, DRR, Fair queueing
Système de transmission	CSMA/CD, CSMA/CA, lien point à point

Utilisation du Simulateur

Du point de vue de l'utilisateur, la mise en œuvre de ce simulateur se fait via une étape de programmation en langage *Tcl,* qui décrit la topologie du réseau et le comportement de ses composants, puis vient l'étape de simulation et enfin l'interprétation des résultats.
L'exemple ci-dessous simule un réseau de quatre noeuds avec deux sources de paquets. Lors de la visualisation, on souhaite que les paquets d'une source apparaissent en bleu, les autres en rouge. On remarque la visualisation de la file d'attente de messages qui se forme au noeud 2, puisque les trafics en entrée sont assez proches de la saturation.

```
#création d'un simulateur
set ns [new Simulator]

#Création du fichier de tracage de paquets
set trace [open out.tr w]
$ns trace-all $trace

#Quand la simulation est terminée, la procedure finish est appelée, l'exécution de nam
#permet la visualisation de la topologie et des paquets transitant
proc finish {} {
        global ns trace
        $ns flush-trace
        close $trace
        close $namf
        exec nam out.nam &
        exit 0
    }

#Création de 4 noeuds
set n0 [$ns node]
set n1 [$ns node]
set n2 [$ns node]
set n3 [$ns node]

#Création de lignes de communication full duplex entre noeuds
$ns duplex-link $n0 $n2 1Mb 10ms DropTail
$ns duplex-link $n1 $n2 1Mb 10ms DropTail
$ns duplex-link $n3 $n2 1Mb 10ms DropTail
#Création d'agents UDP, les données dans NS sont transmises entre agents
set udp0 [new Agent/UDP]
$ns attach-agent $n0 $udp0
set udp1 [new Agent/UDP]
$ns attach-agent $n1 $udp1

#Création d'application génératrice de paquets à vitesse constante
#paquets de 500 bytes générés toutes les 5ms
#l'agent cbr0 est implanté sur le noeud n0 et cbr1 sur le noeud n1
set cbr0 [new Application/Traffic/CBR]
$cbr0 attach-agent $udp0
$cbr0 set packetSize_ 500
$cbr0 set interval_ 0.005
set cbr1 [new Application/Traffic/CBR]
$cbr1 attach-agent $udp1
$cbr1 set packetSize_ 500
$cbr1 set interval_ 0.005
```

```
#Création d'un agent vide, destiné à recevoir les paquets, implanté dans n1
set null0 [new agent/Null]
$ns attach-agent $n3 $null0

#routage des trafics
$ns connect $cbr0 $null0
$ns connect $cbr1 $null0

#début et fin de génération de paquets par cbr0 et cbr1
$ns at 0.5 "$cbr0 start"
$ns at 1.0 "$cbr1 start"
$ns at 4.0 "$cbr1 stop"
$ns at 4.5 "$cbr0 stop"

#Simulation durant 5 secondes avec appel de procédure finish
$ns at 5.0 "finish"

#Début de la Simulation
$ns run
```

L'exécution de NAM dans la procédure "*finish*" permet de visualiser dynamiquement des paquets circulant entre les nœuds :

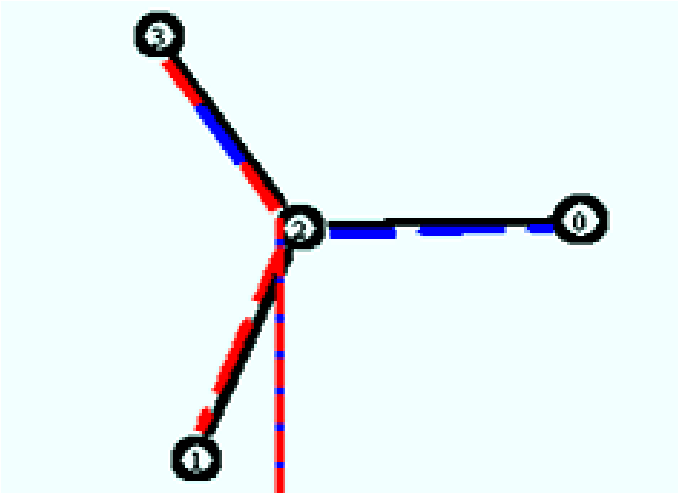

Figure 1 : Visualisation par NAM

ANNEX II : L'interface radio de l'UTRAN

I. L'architecture en couches

Les protocoles de l'interface radio s'appliquent aux 3 premières couches du modèle OSI (*Open Systems Interconnections*), qui sont la couche physique, la couche liaison de données, et la couche réseau (routage).

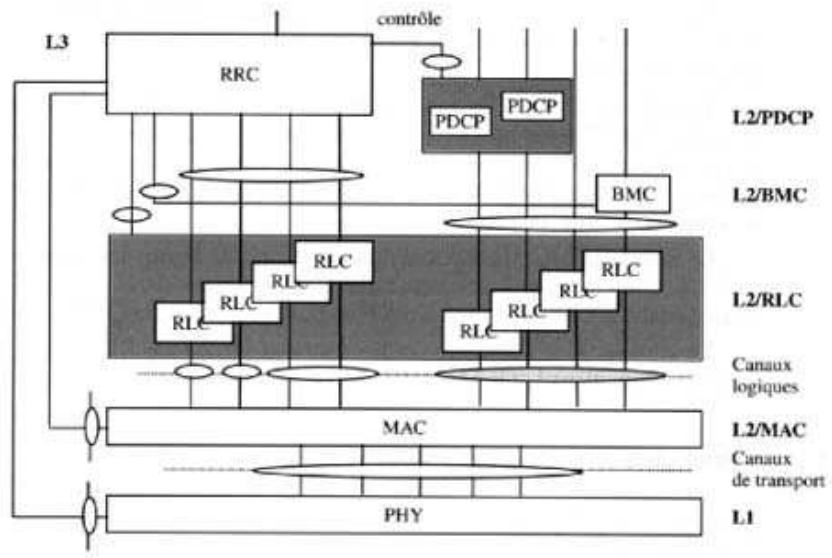

Figure 1 : Vue en couche de l'interface radio de l'UTRAN

- ✧ Le **niveau 1 (**PHY**)** représente la couche physique de l'interface radio. Elle réalise entre autre les fonctions de codage de canal, d'entrelacement et de modulation.
- ✧ Le **niveau 2** comprend les couches PDCP, RLC, MAC et BMC.

  - ☑ Le transport fiable des données entre 2 équipements est assuré par la couche **RLC** (*Radio Link Control*). Le protocol RLC ressemble beaucoup aux protocoles tels que HDLC et LAPD.
  - ☑ La couche **MAC** (*Medium Access Control*) remplit la fonction de multiplexage des données sur les canaux de transport radio.
  - ☑ La couche **PDCP** (*Packet Data Convergence Protocol*) a deux fonctions principales. Tout d'abord elle permet d'assurer l'indépendance des protocoles radio de l'UTRAN (couches MAC et RLC) par rapport aux couches de transport réseau. Cette indépendance permettra de faire évoluer les protocoles réseau (par exemple de passer de l'IPv4 à l'IPv6) sans modification des protocoles radio de

l'UTRAN. D'autre part, la couche PDCP offre les algorithmes **de compression de données ou d'en-tête de paquets de données**, permettant un usage plus efficace des ressources radio.

- ☑ La couche **BMC** (*Broadcast/Multicast Control*) assure les fonctions de diffusion de messages sur l'interface radio.

✧ Le **niveau 3** de l'interface radio contient la couche RRC (Radio Resource Control). La fonction principale de cette couche est la gestion de la connexion de signalisation établie entre l'UTRAN et le mobile. Cette connexion est utilisée lors des échanges de signalisation entre le mobile et l'UTRAN, par exemple, à l'établissement et à la libération de la communication.

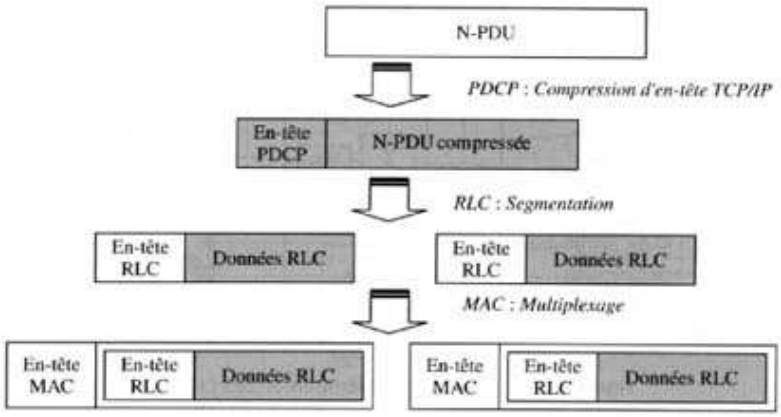

Figure2 : Encapsulation des paquets arrivant du réseau cœur

II Cas d'un paquet IP

Le paquet d'information reçu par l'UTRAN et provenant du réseau cœur est la N-PDU (Network PDU). Dans le cas d'un paquet IP, l'en-tête de la N-PDU est compressé par la couche PDCP, c'est à dire remplacé par un en-tête PDCP de taille plus réduite. Cette nouvelle PDU est ensuite segmentée par la couche RLC, qui ajoute à chaque segment son propre en-tête. La RLC-PDU est alors traitée par la couche MAC, qui ajoute un en-tête lorsqu'un multiplexage est effectué.

III Cas du transport de la voix

Pour la voix, le fonctionnement est beaucoup plus simple. Les couches RLC et MAC sont utilisées en mode transparent (ni segmentation, ni multiplexage des trames de phonie) ; la couche PDCP est dans ce cas inutile.

IV Protocoles réseaux

Nous avons décrit l'interface radio de l'UTRAN et les protocoles associés. Mais l'UTRAN ne se limite pas à l'interface radio. En raison des nombreux nœuds réseau définis dans l'UTRAN (NodeB et RNC), un ensemble de protocoles et d'interfaces appartenant à la partie terrestre a été défini pour permettre à ces différents nœuds d'échanger de la signalisation et des données usager. Notons que l'interface radio (aussi nommée interface air) de l'UMTS est basée sur le WCDMA (Wideband Code Distributed Multiple Access), qui elle-même réutilise largement le concept CDMA.