

Table des matières

Introduction générale.....	1
Chapitre1 : Généralité sur NEMO	
I. 1.Introduction	2
I. 2. problématique	2
I. 3 .Définition	4
I. 4 .Les applications	4
I. 4.1. Les réseaux de capteurs	4
I. 4.2. Les réseaux d'accès à Internet	5
I. 4.3. Les réseaux personnels	5
I. 5. Caractéristiques	6
I. 5.1. Taille	6
I. 5.2. Hétérogénéité des MNNs	6
I. 5.3. Mobilité enchaînée	7
I. 5.4. Hétérogénéité des réseaux d'accès	7
I. 5.5. Multidomiciliation	7
I. 5.6. Interaction entre réseau Ad Hoc et réseau mobile	7
I. 5.7. Fréquence distincte de changement du point d'ancrage	8
I. 5.8. Variation dynamique de débit	8
I. 6 .L'architecture de NEMO	8
I. 7. fonctionnalité	9
I. 8. Les avantages et Les inconvénients	12
I. 9. Conclusion	15

Chapitre2 : Gestion de mobilité

II. 1. Introduction	16
II. 2. Type de mobilité.	16
II. 2.1. Micro-mobilité.....	16
II. 2.2. Macro-mobilité	17
II. 3. Définition de Handover	17
II. 4. Les raisons pour exécuter un Handover	17

II. 4.1. Qualité signal	17
II. 4.2. Le trafic.....	17
II. 5. Les différentes phases du Handover	18
II. 5.1. Phase de découverte	18
II. 5.2. Phase de décision	19
II. 5.3. Phase d'exécution du Handover	19
II. 6. Type de Handover	19
II. 6.1. Hard Handover	19
II. 6.2. Soft Handover	21
II. 6.3. Fast Handover	22
II. 6.4. Smooth Handover	26
II. 6.5. Handover sans coutures ou Seamless Handover	27
II. 7. Les paramètres de qualités de service	30
II. 7.1. Le délai	30
II. 7.2. La gigue	31
II. 7.3. Le taux de perte de paquet	31
II. 7.4. Le débit.....	31
II. 8. Analyse du délai du Handover NEMO	31
II. 8.1. Délai du Handover L2	31
II. 8.2. Délai du Handover L3	33
II.8.3 .Evaluation numérique.....	34
II. 9. Conclusion	37

Chapitre3 : simulation & résultats

III. 1. Introduction	38
III. 2. Présentation de logiciel	38
III. 2.1. Définition de NS2	38
III. 2.2. Composants	38
III. 2.3. Organisation du simulateur	39
III. 2.4. Architecture du réseau.....	40
III. 2.5. Création d'un scénario	41
III. 2.6. Les modules nécessaires pour la simulation	41
III. 2.6.1. Module de découverte voisin	41
III. 2.6.2. Le service MIH (Media Independant Handover)	41

III. 2.6.2.1. Présentation du standard IEEE802.21	42
III. 2.6.3. La gestion de mobilité MIPv6	42
III. 2.7. Paramétrage et configuration du réseau	44
III. 2.7.1. Les paramètres de simulation	44
III. 2.7.2. Les paramètres de réseau Wifi	45
III. 2.7.3. Configuration du point d'accès	45
III. 2.7.4. Paramètres du réseau WiMAX.....	46
III. 2.7.5. Configuration de la station de base (WiMAX1)	46
III. 2.7.6. Configuration de la station de base (WiMAX2).	46
III. 3. Simulations.....	47
III. 3.1.La topologie de réseau sous NS2	47
III. 3.2. débit	48
III. 3.3. Nombre des paquets perdus	49
III. 3.4. délai de transmission	51
III.4. Conclusion	53
Conclusion générale.	54

<u>Figure I. 1 :Exemples d'applications des réseaux NEMO.</u>	5
<u>Figure I. 2 :Architecture de NEMO.</u>	8
<u>Figure I. 3 :Fonctionnement de base du protocole NEMO BS...</u>	10
<u>Figure I. 4 :Changement dans le message BU pour le support NEMO.</u>	11
<u>Figure I. 5 :Option du préfixe pour le support NEMO.</u>	11
Figure I.6 : Changement dans le message Back pour le support NEMO	12
Figure II.1 : Hard Handover	19
FigureII.2 :SoftHandove	21
Figure II.3:FastHandover	22
Figure II.4:Procédure du mode prédictif de FHO.	24
FigureII.5:Procédure du mode réactif de FHO	25
Figure II. 6: Principe de fonctionnement Smooth Handover	25
Figure II.7: Principe de fonctionnement Seamless Handover	27
Figure II.8: Procédure de Seamless Handover.	28
Figure II.9: Procédures du Handover NEMO BS	32
Figure II.10: Délai du Handover NEMO (Handover L3)	34
Figure II.11: Délai total du Handover NEMO (Handover global).	35
Figure III.1 : Flot de simulation avec NS-2	39
Figure III.2 : Composants d'un modèle de réseaux en NS	40
Figure III.3 : Vue d'ensemble de conception de MIH	42
Figure III.4 : Mécanisme de base de mobilité IPv6	43
Figure III.5 : Optimisation du routage entre le correspondant et le mobile	44
Figure III.6 : topologie de réseu NEMO	47

Figure III.7 : La variation de débit en fonction de temps.	48
Figure III.8 : variation de débit moyen en fonction de la vitesse.....	49
Figure III.9 : La variation de nombre de paquets perdus en fonction de temps	50
Figure III.10 : Taux de paquets perdus en fonction de la vitesse	51
Figure III.11 : Evolution du délai de transmission du temps.....	51
Figure III.12 : Le délai en fonction de la vitesse	52

Liste de tableaux

Tableau II.1: les types de handover de différents réseaux.....	30
Tableau III.1 : Les paramètres du simulation.....	44
Tableau III.2 : Les paramètres de réseau WiFi.....	45
Tableau III.3 : Les paramètres du point d'accès WiFi.....	45
Tableau III.4 : Les paramètres du réseau WiMAX.....	46
Tableau III.5 : Les paramètres de la station de base WiMAX1	46
Tableau III.6 : Les paramètres de la station de base WiMAX2.....	46

Résumé

L'objectif du présent travail consiste à concevoir et développer une architecture logicielle qui permet la mobilité d'un réseau entier (NEMO).

L'étude réalisée a nécessité l'implémentation des mécanismes efficaces de handover et de la mobilité afin de garantir la continuité de service lorsque le réseau mobile se déplace entre des réseaux hétérogènes c'est-à-dire son routeur mobile change de point d'attachement.

Mots clés : réseau mobile, NEMO, Handover, MIPv6, MIH.

Abstract

The objective of this work is to design and develop a software architecture that allows the mobility of an entire network (NEMO).

The study required the implementation of effective mechanisms for handover and mobility to ensure continuity of service when the mobile network moves between heterogeneous networks is to say mobile router changes its point of attachment.

Introduction générale

Depuis quelques années, les appareils mobiles font partie de notre vie de tous les jours. Néanmoins pour être pleinement utilisables, les téléphones intelligents, tablettes et portables ont une condition nécessaire : être connectés à Internet ou un autre réseau de grande envergure.

Les environnements mobiles se caractérisent par la présence de plusieurs terminaux portables ayant chacun un ou plusieurs moyens de communication sans fil. Ces interfaces de communication sans fil permettent aux terminaux, tout en se déplaçant, de communiquer entre eux ou avec des stations fixes. Ces environnements présentent de grandes différences par rapport aux environnements traditionnels ou fixes. Pour des raisons de taille et de poids, les terminaux portables disposent de ressources moins importantes par rapport à celles qu'offrent des stations fixes. On affiche un désir de la part des usagers à bénéficier d'un accès Internet sans discontinuité de leurs applications réseaux usuelles lors de leurs déplacements, de sorte que nous avons des réseaux entiers constitués de dispositifs sans fils se déplaçant ensemble et désirant cette qualité de service. Les systèmes de transport (avion, bateau, TGV, train, tramway, métro, train, bus, voiture,...) sont un environnement typique. Ainsi, nous parlerons de mobilité lorsque la localisation d'un équipement ou d'un réseau change dans la topologie Internet. La gestion de la mobilité constitue aujourd'hui un véritable challenge dans l'Internet nouvelle génération. En effet, le problème de dualité de l'adressage IP, conçu initialement pour supporter un double rôle d'identification et de localisation dans la topologie Internet, ne permet pas une connectivité sans interruption des services. Lors de son changement de réseau, un terminal mobile par exemple change de point d'attachement (routeur d'accès), son adresse IP change également, il n'est plus joignable par ses correspondants et ses sessions actives sont interrompues. Des architectures de gestion de la mobilité sont donc nécessaires. Il est aujourd'hui communément admis que ces architectures doivent séparer les deux rôles d'identification et de localisation de l'adresse IP. La gestion de la mobilité implique en général un handover vertical nécessitant la reconfiguration d'adresse IP et la mise à jour de cette nouvelle localisation pour le maintien des sessions.

Les réseaux mobiles et la gestion de leur mobilité permettent en effet de réaliser tout un ensemble de scénarii permettant le déploiement d'applications multimédia en tout lieu et à tout instant, mais nécessitant la prise en compte de l'environnement mobile dans lequel sont situés les équipements.

Le but de ce projet de fin d'étude est donc de mettre l'accent sur la notion du réseau mobile (NEMO) et de modéliser une plate forme de développement permettant de mettre en œuvre des outils afin d'étudier et analyser la gestion de la mobilité dans ce type de réseaux.

Le premier chapitre sera consacré à la présentation générale du réseau NEMO, en focalisant sur l'architecture et la fonctionnalité de ce type de réseau.

Le deuxième chapitre sera réservé à l'étude de la gestion de mobilité et aux spécificités du Handover en détaillant ses phases et ses types notamment dans le cadre du réseau NEMO

Le troisième chapitre comprendra les différentes étapes de notre travail de simulation incluant le scénario de modélisation à traiter puis l'évaluation et l'analyse des résultats obtenus.

Chapitre1 :

Généralités sur le NEMO

I.1. Introduction :

Dans le domaine des transports intelligents communicants comme dans beaucoup d'autres, le développement très rapide des technologies de communication sans fil ouvre des perspectives nouvelles. Il est maintenant envisageable de déployer, dans les véhicules, des applications impliquant des communications avec d'autres véhicules ou avec l'infrastructure en profitant des capacités de communication environnantes. Ces dernières peuvent être déployées pour un usage spécifique mais disposer de capacité inutilisée pouvant être réaffectée de manière temporaire ou permanente à d'autres usages. Cela permet de réduire les coûts de déploiement des nouveaux services dans la mesure où les technologies utilisées sont déjà déployées. Il faut pour cela que les équipements embarqués soient opportunistes en profitant séquentiellement ou simultanément de ce qu'on pourrait appeler la "diversité technologique".

L'ISO a débuté en 2003 la standardisation de CALM qui définit l'architecture protocolaire des équipements embarqués dans les véhicules. Le choix d'IPv6 et de Mobile IPv6 (tous les deux sont définis à l'IETF), a été fait pour la communication entre le véhicule et l'Internet. Cela permet de supporter le grand nombre potentiel d'équipements communicants. Le protocole NEMO permet quant à lui de supporter les changements d'attachement dans le réseau IP et de cacher cette mobilité aux éléments embarqués.

Ces protocoles sont par nature capables de supporter les attachements multiples à l'Internet en utilisant une ou plusieurs interfaces de communication. Pourtant, la gestion des différentes interfaces et des réseaux d'accès d'attachement est un problème déjà difficile sur les terminaux mobiles qui se complique lorsque le nombre d'entités impliquées augmente comme dans le cas des réseaux mobiles (véhicule). [5]

I.2. problématique :

Depuis quelques années déjà, les terminaux informatiques deviennent moins encombrants et par conséquent plus mobiles. Par ailleurs les possibilités de se connecter à l'Internet se multiplient. Il s'en suit une mobilité induite par l'utilisation de plusieurs technologies d'accès (Ethernet, WiFi, GPRS,...) sur un même terminal dans la même journée. Les études sont actuellement conduites par les constructeurs et les opérateurs pour fournir des infrastructures mobiles utilisant de nouvelles technologies radio, WiFi et WiMax notamment, ont pour objet d'offrir la continuité des services en cours de déplacement, comme le permet le GSM dans le cas de la téléphonie mobile. Cela nécessite que les applications ne soient pas interrompues lors des épisodes de mobilité.

Enfin, les sociétés de transport désirant offrir un service de connexion à leurs clients en déplacement et les fabricants de véhicules, qui interconnectent de plus en plus d'équipements à bord, envisagent la question de la mobilité d'un réseau entier et non plus uniquement celle d'équipements isolés.

Le problème de la mobilité dans IP peut se décomposer en trois sous-problèmes distincts :

- pouvoir communiquer.
- être joignable.
- conserver les communications en cours lors des déplacements.

Le premier problème est élégamment résolu par le mécanisme d'auto configuration d'IPv6, en effet, dès que le terminal a réussi à construire une adresse IPv6 globale, il est capable de communiquer avec toute autre station sur l'Internet. Mobile IPv6 (MIPv6) modifie très peu ces mécanismes. Il ne requiert que de nouvelles directives de configuration permettant d'accélérer le processus. Le délai d'acquisition d'une adresse globale routable est en effet critique dans les situations de mobilité.

Le second problème est résolu pour les postes IP fixes par le DNS qui établit la relation entre un nom logique connu de tous et une adresse IP (Nommage). Dans le contexte de la mobilité, la fréquence d'attribution d'une nouvelle adresse est incompatible avec la mise à jour du DNS distribué. D'autres mécanismes ont été proposés.

Le troisième problème est plus difficile à résoudre. Il a pour origine la dualité des fonctions d'une adresse IPv6. Cette dernière identifie de manière unique sur l'Internet un terminal, ou pour être plus précis une interface réseau d'un terminal. Elle permet aussi de localiser un nœud dans la topologie de l'Internet. Ainsi chaque fois qu'un nœud se déplace, ce dernier doit changer d'adresse pour que la nouvelle adresse corresponde à sa nouvelle localisation (fonction de localisation). Malheureusement son identification change aussi ce qui pose des problèmes aux couches supérieures. En effet, TCP utilise le quintuplé : Adresse IPv6 source, Adresse IPv6 destination, Port source, Port destination et numéro de protocole pour identifier une connexion. Lorsqu'un de ces éléments change, il ne s'agit plus pour lui de la même session et les communications en cours sont interrompues.

Dès 1998, l'IETF a standardisé une solution de mobilité IP pour IPv4 [RFC 3344]. Les contraintes liées à la modification d'un protocole très largement déployé ont limité le travail à la modification du comportement du mobile lui-même (sans implication du correspondant pour qui la mobilité devait être transparente) et à l'ajout de nouvelles entités dans le réseau. IPv6 offrait l'opportunité du déploiement d'un nouveau protocole intégrant dès l'origine la mobilité. Les correspondants peuvent ainsi être mis à contribution pour des traitements liés à la mobilité. De plus la conception plus moderne d'IPv6 permet d'alléger les mécanismes d'encapsulation et de profiter des mécanismes d'auto configuration.

Des désaccords concernant la sécurisation de Mobile IPv6 (c.f. Les risques induits par la mobilité et leur limitation) et les différentes optimisations possibles, ont rendu la standardisation de Mobile IPv6 longue et laborieuse, les RFCs n'ayant été publiés qu'en juin 2004. La gestion de la mobilité dans IPv6 est maintenant définie dans le RFC 3775 pour ses aspects fonctionnels. Le RFC 3776 traite pour sa part des aspects liés à la sécurité de la signalisation de la mobilité.

Si les travaux dans le domaine de la mobilité IP se sont dans un premier temps exclusivement consacrés au support des stations mobiles, le besoin de fournir un accès Internet permanent aux routeurs mobiles et aux stations situées dans un réseau en mouvement (réseau mobile) est aujourd'hui clairement identifié. Les problèmes spécifiques posés par ce type de mobilité sont traités à l'IETF au sein du groupe de travail NEMO (Network MObility) récemment créé. Ces travaux ont abouti à l'édition du RFC 3963 qui spécifie des fonctionnalités semblables à celles de MIPv6 dédiées aux routeurs mobiles. [1]

Nous allons détailler le protocole de mobilité du réseau NEMO.

I.3 .Définition :

Un réseau mobile est défini comme un ensemble de sous-réseaux connectés à l'Internet par l'intermédiaire d'un ou plusieurs routeurs mobiles qui changent leurs points d'attache à l'Internet. [2]

Les routeurs mobiles en mouvement passant d'un réseau d'accès à un autre conservent les connexions réseaux de manière transparente pour les stations ou terminaux embarqués.

I.4 .Les applications :

Les applications possibles des réseaux mobiles sont nombreuses et très variées. Celles-ci incluent en particulier :

I.4.1. Les réseaux de capteurs :

Ils sont déployés dans les véhicules (avions, trains, bateaux, Voitures). Certains ont besoin d'interagir avec des serveurs dans l'Internet, par exemple pour assurer la transmission de données nécessaires à la navigation, pour procéder à la maintenance et au contrôle de l'état du véhicule, etc. Un autre exemple, encore futuriste, est celui des vêtements intelligents dans lesquels sont incorporés des capteurs (humidité, température, rythme cardiaque, tension artérielle, etc.) permettant entre autres le contrôle en temps réel de l'état de santé d'un Patient. [5]

I.4.2. Les réseaux d'accès à Internet :

Ils sont déployés dans les transports publics comme bus, trains et taxis offrant une borne d'accès Internet aux passagers. Exemple tout aussi démonstratif est celui d'une compagnie de

transport ferroviaire ou aérienne offrant un accès Internet permanent et ininterrompu à ses passagers. Cet accès pourrait non seulement permettre aux passagers de se connecter sur un site distant, télécharger de la musique et de la vidéo depuis n'importe quel fournisseur de service, ou de surfer sur la toile sans interruption de service en utilisant les appareils proposés par la compagnie, mais aussi de s'y connecter en utilisant leur propre ordinateur portable ou téléphone. [5]

I.4.3. Les réseaux personnels :

Ils sont constitués d'un ensemble d'appareils électroniques de petite taille (cardio-fréquencemètre, montre, téléphone cellulaire, assistant personnel, appareil photo digital, etc.) portés par les personnes. De nombreux scénarii d'utilisation des PANs peuvent être imaginés, notamment pour des applications liées à la sécurité civile (police, pompiers) (Boot, 2002), à la médecine (Ernst, 2004) et bien entendu aussi à l'armée. Par exemple, un fauteuil roulant, un sac, ou un vélo équipé d'un PAN pourrait permettre, à un handicapé moteur, à une personne ayant des déficiences mentales, ou à un sportif, d'être suivi à distance et en temps réel (par un médecin, la famille, la cellule antidopage, etc.) et d'appeler automatiquement les secours en cas de défaillance, et pourraient aussi bien répondre aux besoins de la police, des pompiers, des journalistes, etc. [5]

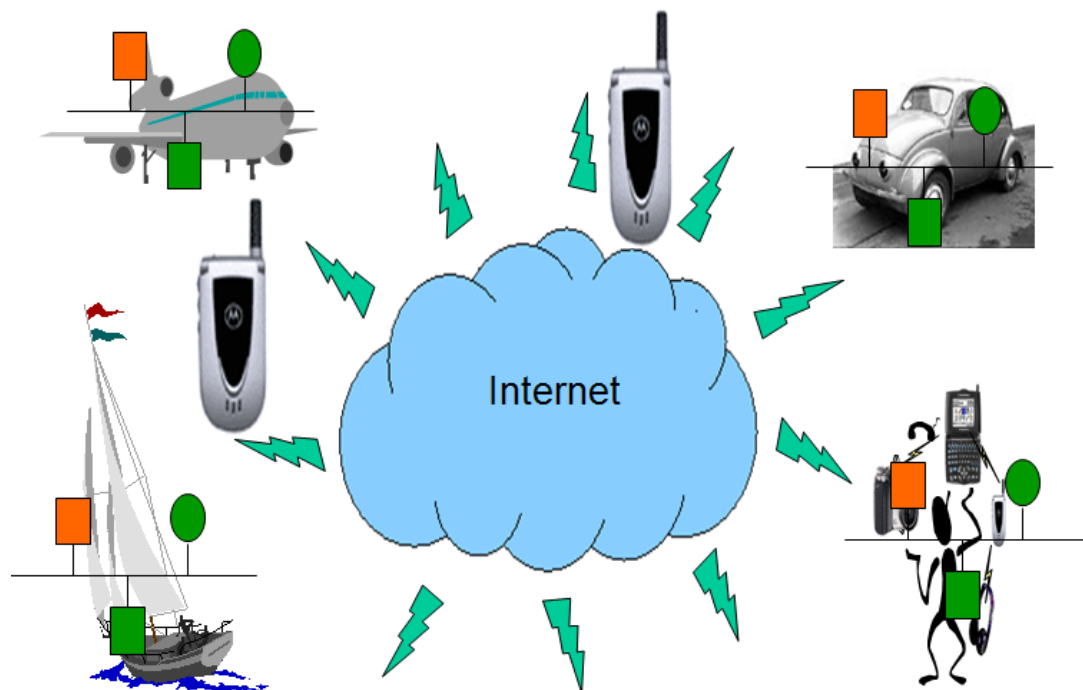


Figure I. 1 : Exemples d'applications des réseaux NEMO.

I.5. Caractéristiques :

Un réseau embarqué de type IP, c'est-à-dire un réseau mobile. Ils démontrent aussi que les réseaux mobiles peuvent avoir des caractéristiques et donc des besoins très différents d'un cas à l'autre [5] :

I.5.1. Taille :

Les réseaux mobiles peuvent être de taille variable, allant de l'ordre de quelques MNNs dans le cas d'un PAN jusqu'à plusieurs centaines de stations interconnectées par plusieurs routeurs et sous-réseaux dans le cas d'un train. Le nombre de correspondants, quant à lui, est indépendant du nombre de MNNs, mais peut potentiellement être très grand. [5]

I.5.2. Hétérogénéité des MNNs :

Les nœuds embarqués (MNNs) peuvent être de trois types. Un LFN est un nœud résidant de manière permanente dans le réseau mobile et ne changeant pas son point d'ancrage (par exemple un capteur de pression des pneus ou de température). Un LMN est un nœud mobile appartenant au réseau mobile et capable de changer son point d'ancrage dans le réseau mobile, voire de le quitter (la clef du véhicule), tandis qu'un VMN est un nœud mobile n'appartenant pas au réseau mobile mais capable de s'y attacher (équipements appartenant aux passagers tels un ordinateur portable ou un PDA). [5]

I.5.3. Mobilité enchaînée (Nested Mobility) :

Un réseau mobile pouvant accueillir soit une station mobile, soit un routeur mobile servant lui même de passerelle à un autre réseau mobile, la mobilité des réseaux peut être récursive. Dans le cas d'un bus servi par un MR et offrant un accès Internet aux stations mobiles (VMN) des passagers, nous avons deux niveaux de mobilité. Dans le cas d'un passager disposant d'un PAN qui à son tour permet l'ancrage d'un VMN, nous devons faire face à trois niveaux de mobilité. Le réseau et les MRs qui connectent l'ensemble à Internet sont respectivement appelés root-NEMO et root-MR. Les autres réseaux (respectivement MRs) se servant d'un root-NEMO pour se connecter à Internet sont nommés sub-NEMO et sub-MRs. [5]

I.5.4. Hétérogénéité des réseaux d'accès :

Un réseau mobile peut prendre ancrage à l'Internet via des points très éloignés dans la topologie, et d'autre part le faire par le biais de technologies hétérogènes. Il est ainsi raisonnable de considérer le cas où les réseaux mobiles non seulement changent de réseau d'accès, mais certainement aussi de fournisseurs de service ou de domaine administratif (mobilité globale). Dans un tel cas, la sécurisation des données de contrôle, le contrôle

d'accès aux ressources du réseau visité, et l'adaptation des applications à la bande passante disponible sont des besoins cruciaux. [5]

I.5.5. Multidomiciliation (Multihoming) :

Un réseau mobile est dit multi domicilié lorsqu'il a plusieurs points d'ancrage à Internet, c'est-à-dire lorsqu'il est simultanément connecté à Internet via plusieurs MRs ou lorsqu'un MR a plusieurs interfaces externes, ou plusieurs adresses sur son interface externe. Les motivations et les bénéfices attendus sont les mêmes pour un réseau fixe ou mobile, mais la mobilité rend cette configuration plus fréquente. En effet, une telle configuration permet de pallier aux pannes, de partager les flux, de mettre en place des préférences ou plus simplement de garantir un meilleur accès à l'Internet en faisant appel à plusieurs technologies. Cette possibilité de se connecter par l'intermédiaire d'un ou plusieurs routeurs mobiles disposant au total de plusieurs interfaces externes nécessite de considérer les aspects de changement d'interface et de changement de routeur mobile. [5]

I.5.6. Interaction entre réseau Ad Hoc et réseau mobile :

Les réseaux ad hoc sont des réseaux sans infrastructure, dont l'ensemble des nœuds sont des routeurs mobiles, avec ou sans sous-réseau attaché à leur interface interne, et dont la topologie est très dynamique. Les routes de la source à la destination (en règle générale toutes deux situées à l'intérieur du réseau ad hoc) sont calculées dynamiquement. L'hétérogénéité des MNNs peut mener à confondre réseaux mobiles et réseaux ad hoc car il est possible qu'un réseau ad hoc constitue un réseau mobile et inversement qu'un ensemble de réseaux mobile constitue un réseau ad hoc. [5]

I.5.7. Fréquence distincte de changement du point d'ancrage :

A chaque configuration, et selon l'usage, correspond une certaine fréquence de mobilité. Un métro, par exemple, suit une trajectoire déterminée à vitesse déterminée, probablement au sein d'un seul fournisseur d'accès. Les handovers sont donc prévisibles. Un piéton ou une automobile en milieu urbain, en revanche, change de trajectoire, de vitesse, et de réseau d'accès ; les handovers sont donc très difficilement prévisibles. Ils seront en revanche semi-prévisibles dans le cas d'une voiture sur autoroute. [5]

I.5.8. Variation dynamique de débit :

Lorsque le routeur mobile change le point d'attachement, le réseau NEMO prend le débit de réseau d'accès (WIFI, GSM, WIMAX,...)

- WIMAX : 70 Mbit/s
- WIFI : compris entre 1 et 54 Mbits/s.
- GSM : 13 Kbits/s.
- GPRS : 171,2 Kbits/s.
- UMTS : 2Mbits/s.

I.6 .L'architecture de NEMO :

Le réseau NEMO, de l'IETF est dérivé de Mobile IP pour gérer la mobilité des réseaux IP. Un sous-réseau comporte des nœuds mobiles. Ce sous-réseau est associé à un réseau mère et peut changer de réseau en changeant de point d'accès. Un des objectifs est de ne pas imposer des modifications aux nœuds mobiles. [3]

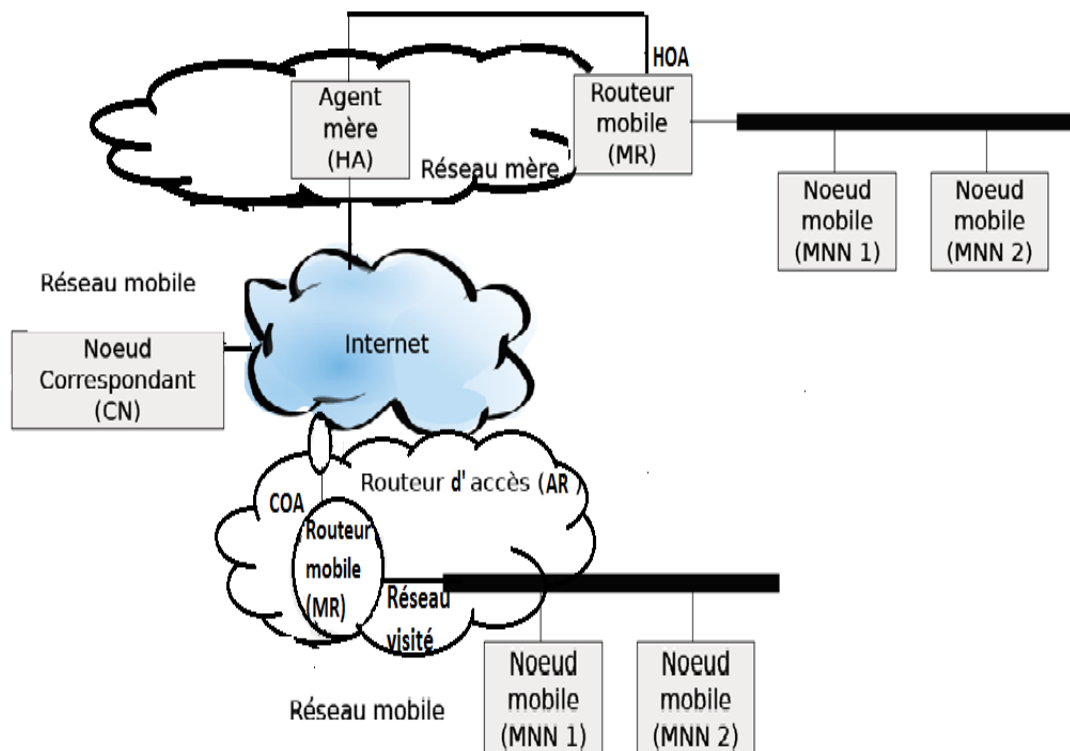


Figure I. 2 : Architecture de NEMO.

Les nouvelles entités sont introduites :

Home Network ou réseau mère : c'est le réseau auquel est attaché initialement un MR.

Home Agent (HA) ou agent mère : un routeur d'accès particulier situé dans le réseau mère qui participe à la gestion de la mobilité du réseau mobile.

Foreign Network ou réseau visité : n'importe quel réseau autre que le réseau mère auquel le réseau mobile est connecté.

Le routeur d'accès (RA): situe dans le réseau visité qui fournit au MNN de réseau mobile un service de routage des paquets qui lui sont destinés par le HA

Correspondant Node (CN) ou nœud correspondant : est un terminal en communication avec le MNN. Un CN peut être fixe ou mobile. [6]

Mobile Network Nodes (MNN) : est un nœud mobile qui fait partie du réseau mobile.

Le routeur mobile (MR) : est l'entité la plus importante de NEMO. Le changement de point d'accès ne provoque pas de changement d'adresse IP du MNN. La gestion de la mobilité est déléguée au MR. [3]. Le MR admet au minimum deux interfaces : une interface interne (Ingress Interface, IIF) et une interface externe (Egress Interface, EIF). L'interface IIF est configurée avec une adresse IP prise du préfixe MNP, tandis que l'interface EIF est configurée avec l'adresse HoA lorsque le réseau NEMO (plus précisément le MR) est attaché au réseau mère (Home Network), c'est l'adresse mère unique par laquelle il est accessible quand il est lié au réseau mère. Lorsque le MR est attaché à un réseau visité, l'interface EIF sera configurée avec une adresse temporaire CoA. [6]

I.7. Fonctionnalité :

Le groupe de travail NEMO a pour objectif de gérer la mobilité IP, c'est-à dire le changement de réseau d'accès, au niveau d'un routeur appelé routeur mobile (Mobile Router, MR). Le réseau NEMO est attaché au réseau d'accès par le biais du routeur mobile qui contrôle son mouvement. La règle fondamentale est de ne pas imposer de modifications sur les nœuds localisés derrière le routeur (MNNs) et de maintenir les sessions, sans optimisation de routage.

Toutes les communications depuis et vers les nœuds mobiles situés au sein du réseau NEMO passent à travers le MR. Un préfixe IPv6 (Mobile Network Prefix, MNP) est délégué par le Home Agent au MR pour l'annoncer aux MNNs situés au sein du réseau NEMO. [6]

a-Opérations du protocole NEMO Support Basique (NEMO BS) :

Le protocole de routage le plus utilisable dans le réseau NEMO c'est le protocole NEMO BS qui possède les mêmes opérations conduites par MIPv6.

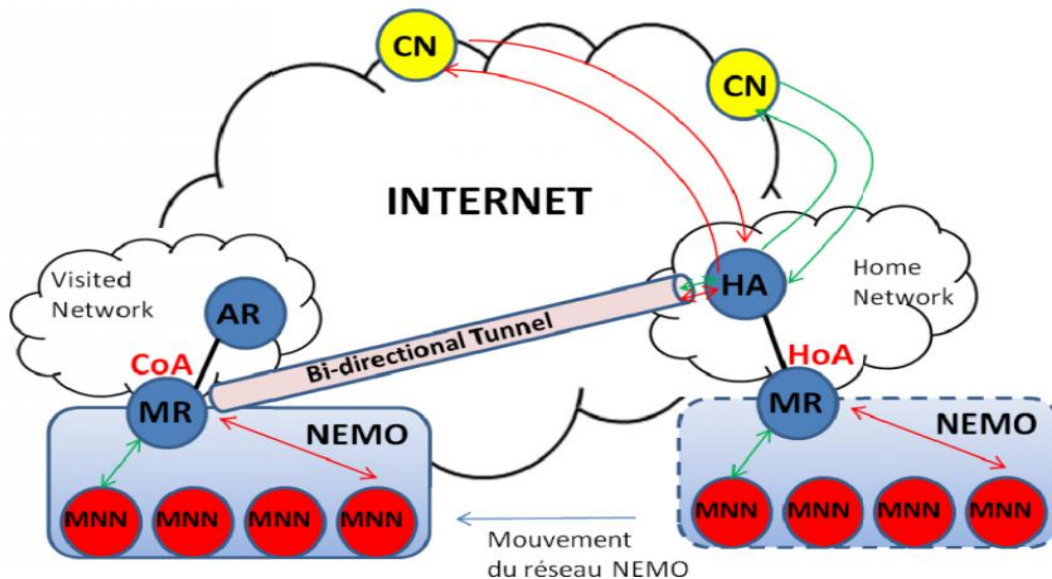


Figure I. 3 : Fonctionnement de base du protocole NEMO BS.

Quand le MR s'éloigne du réseau mère et s'attache à un nouveau routeur d'accès, il acquiert une adresse temporaire CoA. Il envoie immédiatement un binding update (BU) à son HA. Quand le HA reçoit cette mise à jour, il crée dans son binding cache une entrée indiquant la nouvelle adresse CoA de l'actuel point d'attachement du MR. [6]

Le MR peut à tout moment agir soit comme un nœud mobile ou comme un routeur mobile. Si le MR vise à agir en tant que routeur mobile et à fournir la connectivité aux nœuds dans le réseau mobile NEMO, il indique ceci au HA en plaçant le Flag R à la valeur 1 dans le message BU. Il inclut également les informations sur le préfixe du réseau mobile de sorte que le HA peut expédier les paquets destinés aux MNNs du réseau mobile NEMO. [6]

Quand le HA reçoit le message binding update du MR, il répond par un message binding Ack (Back) avec un Flag R=1. Tous les messages de signalisation entre le MR et le HA en particulier les BU/Back doivent être protégés par IPsec [7].

Une fois le processus de mise à jour est terminé, un tunnel IP-in-IP [8] bidirectionnel est établi entre le HA et le MR. Ce tunnel peut être protégé par IPsec ou non. Le tunnel bidirectionnel est créé entre le MR et son HA en fusionnant deux tunnels bidirectionnels.

Le tunnel du MR vers le HA a comme point d'entrée du tunnel, l'adresse CoA du MR et l'adresse du HA comme point de sortie du tunnel. Le tunnel du HA vers le MR a comme point d'entrée, l'adresse du HA et comme point de sortie, l'adresse CoA du MR. Tout le trafic IPv6 depuis et vers le réseau mobile NEMO transite par ce tunnel bidirectionnel.

Quand un nœud correspondant CN envoie un paquet de données à un nœud MNN dans le réseau mobile NEMO, ce paquet est reçu par le HA qui l'achemine au MR par ce tunnel.

L'envoi du paquet dans le tunnel est fait en employant l'encapsulation IPv6-dans-IPv6, arrivant au routeur mobile, il le dé-encapsule et le transmet au nœud MNN. Pour le trafic lancé par le réseau mobile, le MR emploie la direction inverse du tunnel, mais avant ; il doit s'assurer que le trafic provient bien d'un des nœuds du réseau mobile si non, il rejette le paquet. [6]

b-Format des messages BU et BAcK du protocole NEMO BS :

➤ Message BU:

Un nouveau bit R (Flag R) est inclus dans le paquet binding update pour indiquer au HA qu'il s'agit d'un routeur mobile et non un nœud mobile (R=1 correspond à un MR, R=0 correspond à un MN). Une option du préfixe MNP du réseau mobile est incluse également dans le message BU pour indiquer l'information du préfixe du réseau mobile au HA. [6]

					Sequence #	
A	H	L	K	R	Reserved	LifeTime
Mobility options						

Figure I. 4 : Changement dans le message BU pour le support NEMO.

Option du préfixe :

Le NEMO ajoute une option de préfixe (Figure I. 5) dans le champ « Mobility Options » du message BU de MIPv6.

Type	Length	Reserved	Prefix Length
Mobile Network Prefix (MNP)			

Figure I. 6 : Option du préfixe pour le support NEMO.

- Type : valeur égal à 6
- Length (8 bits) : indiquant la longueur en octets de l'option, à l'exception des champs « Type » et « Length ».
- Reserved : Ce champ est inutilisé maintenant. La valeur doit être initialisée à 0 par l'expéditeur et doit être ignoré par le récepteur.
- Prefix Length (8 bits) : indiquant la longueur du préfixe IPv6 contenu dans l'option.



- Mobile Network Prefix (MNP) : un champ de 16 octets contenant le préfixe du réseau mobile.

➤ Message BACk

Le bit R est inclus dans le message BACk (Figure I.7) pour indiquer que le HA qui a traité le message BU correspondant supporte les routeurs mobiles. Il est placé à 1 seulement si le flag R du message BU correspondant était mis à 1.

	Status	K	R	Reserved
Sequence #	LifeTime			
Mobility Options				

Figure I.8 : Changement dans le message BACk pour le support NEMO.

I.8. Les avantages et Les inconvénients :

a- Les avantages :

- L'avantage le plus attrayant du protocole NEMO BS est sa simplicité, étant donné qu'il s'agit d'une extension logique des opérations de MIPv6 aux routeurs mobiles et leurs HAs. [6]
- Lors d'un mouvement, les mécanismes de NEMO entrent en jeu pour assurer de manière transparente aux utilisateurs une connectivité IPv6 ainsi qu'une continuité des flux. [4]

b- Les inconvénients :

Le déploiement pratique des réseaux mobiles dans le contexte NEMO dépendra de la capacité de celui-ci à surmonter quelques problèmes qui nécessitent des recherches davantage. Nous citons :

- **Optimisation du routage :**

L'optimisation de routage (Route Optimization, RO) consiste à fournir un mécanisme pour éliminer l'inefficacité du tunneling des paquets du MR vers son HA avant d'être émis au CN (routage triangulaire). La RO permettrait donc de faire un routage direct des MNNs ou du MR vers les CNs. Ce qui permet ainsi de réduire le délai de livraison des

paquets, la charge du réseau Internet et évite des goulots d'étranglement au niveau des HAS. Cependant, contrairement à MIPv6, le protocole NEMO BS ne supporte pas ce mécanisme. Le groupe de travail de NEMO a publié la RFC 5522 pour documenter ces problèmes liés au RO. Jusqu'à présent aucune solution n'est standardisée. [6]

- **Performance du handover :**

Le protocole NEMO BS hérite les inconvénients de MIPv6 notamment en termes de délai de handover et la perte de paquets induite. Cela peut être pénalisant pour les applications temps réel et exigeantes en QoS. Des optimisations sont donc nécessaires pour réduire ou même anéantir ces effets. Des solutions reposant sur les améliorations existantes de MIPv6 (tel que FMIPv6) ont été déjà fait leur apparition [10], mais les performances obtenues restent encore insuffisantes. [6]

- **Multi-domiciliation (Multihoming) :**

Le multihoming est la capacité d'avoir plusieurs chemins à Internet, ceci peut est possible si le MR dispose de multiples interfaces ou si le réseau NEMO est desservi par plusieurs MRs, ces deux cas de figures conduiront à l'acquisition de plusieurs adresses CoAs, et donc plusieurs tunnels.

Le protocole NEMO BS est une extension de MIPv6 pour la prise en charge de la mobilité d'un réseau NEMO desservi par un seul MR, il ne supporte pas donc le multihoming. Le groupe de travail NEMO a publié la RCF 4980 dans laquelle les issues du multihoming sont analysées. Le développement de support de mobilité dans le contexte du multihoming est une issue ouverte. [6]

- **Sécurité :**

Le NEMO hérite certains inconvénients de MIPv6 tels que les menaces de sécurité. Dans diverses attaques (redirection attacks, trafic hijacking, denial of service) contre NEMO ont été décrites et ont mené à l'adoption d'IPSec pour protéger le trafic d'arrivée (inbound) et le trafic de départ (outbound) de NEMO.

Dans l'architecture NEMO, la mobilité est masquée aux MNNs (MNNs unaware of mobility), il est donc important que le NEMO fournit la sécurité quand le réseau mobile est attaché à un réseau étranger. Le NEMO doit permettre aux utilisateurs de différents domaines de se connecter à Internet via son MR. Dans de tels cadres, les modèles de confiance statiques ne sont pas applicables. Cependant, il n'est pas mentionné comment les issues d'autorisation et d'authentification sont manipulées dans l'environnement NEMO particulièrement pour le handover. Ainsi, de nombreuses approches d'authentification pour le handover du réseau NEMO ont été proposées. Malheureusement, avec ces propositions, les menaces de sécurité ne sont pas toutes maîtrisées et le problème de sécurité dans NEMO reste toujours ouvert.[6]

- **Contrôle d'accès :**

Les mécanismes de contrôle d'accès ont été développés pour autoriser et gérer l'accès d'une station dans un réseau quelconque, mais pas pour permettre l'accès à un MR et au réseau qui lui est attaché. Il est nécessaire de mettre en place une procédure permettant aux VMNs de bénéficier de l'accès qu'a obtenu le MR. Ces aspects ont été étudiés dans (Ng et al. 2002; Zrelli et al, 2005; Bournelle et al, 2006) mais les problèmes soulevés n'ont pas été jugés au cas des réseaux mobiles spécifiques et ne sont donc pas traités dans le groupe de travail NEMO. Ils doivent pourtant être résolus pour permettre un déploiement commercial du RFC 3963. [5]

I.9. Conclusion :

Dans ce chapitre, nous avons présenté des concepts généraux sur le réseau NEMO en focalisant sur l'architecture et la fonctionnalité de ce type de réseau.

Du fait de ses applications et ses caractéristiques, le réseau mobile NEMO dispose de nombreux avantages lui permettant de s'imposer.

Chapitre2 :

Gestion de la mobilité

II.1. Introduction :

Les possibilités de se connecter à Internet à tout moment et en tout lieu se multiplient aujourd'hui avec l'avènement des nouvelles technologies d'accès sans fil et le déploiement par les opérateurs d'infrastructures mobiles faisant usage de ces technologies. Il s'en suit une mobilité induite par l'utilisation de plusieurs outils de travail mobiles (PDA, SmartPhone, Laptop, etc). Ainsi, on affiche aujourd'hui un désir croissant de la part des utilisateurs en déplacement à bénéficier d'un accès Internet sans discontinuité de leurs applications réseaux habituelles.

Depuis quelques années déjà, des recherches ont été entamées pour développer des solutions de gestion de la mobilité, ces solutions avaient pour principal objectif la continuité des services en cours de déplacement d'un terminal mobile. D'autres part, les sociétés de transport désirant offrir un service de connexion à leurs clients en déplacement et aux fabricants de véhicules, qui interconnectent de plus en plus d'équipements à bord, envisagent la question de la mobilité d'un réseau entier et non plus uniquement celle d'équipements isolés. Des recherches ont été menées également dans ce sens. [6]

Dans ce chapitre, nous allons citer les types de mobilité et définir le phénomène de Handover, aussi détailler les phases de ce mécanisme, suivi d'une description de différents types de Handover .finalement, une présentation d'analyse des composants du Handover du protocole NEMO BS (ou MIPv6-NEMO).

II.2. Types de mobilité:

Les protocoles de mobilité interviennent généralement au cours du Handover.

Il existe plusieurs niveaux de mobilité faisant référence au modèle OSI. [10]

Nous nous intéressons plus particulièrement à savoir si un changement d'adresse IP est nécessaire lors d'un scénario de mobilité (qu'il soit intra-technologie ou inter-technologies). Nous nous basons donc sur ce critère pour distinguer les différents types de mobilité. [6]

II.2.1. Micro-mobilité :

Le niveau de mobilité le plus bas, est le niveau 2 (Layer 2, L2) qui correspond à la couche liaison du modèle OSI. Ce niveau de mobilité est connu sous le nom Micro Mobilité ou la mobilité locale. Par définition, la Micro Mobilité concerne le déplacement d'une station mobile entre deux points d'attachement situés sur le même réseau sans changement de son adresse IP courante. [10]

II.2.2. Macro-mobilité :

La mobilité de niveau réseau (Layer 3, L3) est connue également sous le nom Macro-Mobilité ou la mobilité globale. Il s'agit de gérer le déplacement d'un utilisateur mobile entre deux réseaux d'accès différents. Ce déplacement nécessitera une mise à jour de l'adresse IP courante de la station mobile.

II.3. Définition de Handover :

Le Handover (HO) ou le transfert intercellulaire est l'ensemble des fonctions et des opérations mises en œuvre entre une ou plusieurs stations de service et une station mobile, pour permettre à cette dernière de changer son point d'attachement au réseau Internet (changement de cellule) et de bénéficier des services d'une autre cellule au lieu de l'ancienne. La station mobile aura la possibilité de continuer sa communication en cours avec un minimum d'interruption [10], sachant que les deux cellules impliquées sont gérées soit par un même réseau (Handover horizontal) soit par les différents réseaux (Handover vertical).

II.4. Les raisons pour exécuter un Handover :

Les raisons les plus communes pour qu'un HO soit exécuter sont en raison de manque de qualité de signal ou du niveau du trafic pour une station de base.

II.4.1. Qualité de signal :

Si le rapport de signal/bruit diminue au-dessous d'un certain niveau (Seuil) c'est-à-dire la diminution de la qualité de signal qui est indiqué par le système, le HO doit être exécuté. [11]

II.4.2. Le trafic :

Chaque cellule a un certain niveau de charge, en effet quand la quantité du trafic dépasse le niveau maximum de la capacité d'une cellule, les utilisateurs de cette cellule sont remis à une autre cellule qui a une capacité plus disponible. De cette façon, les ressources radio sont utilisées d'une façon uniforme. Les HOs sont également adaptés au comportement de l'utilisateur mobile. D'une façon générale, lorsqu'un utilisateur mobile accélère, un Handover peut être effectué d'une microcellule à une macro-cellule et s'il ralentit, un Handover sera favorable à une pico-cellule. [11]

II.5. Les différentes phases du Handover :

II.5.1. Phase de découverte :

La notion de découverte est importante car elle pose de nombreuses difficultés. La procédure de Handover suppose un grand nombre de mesures pour un mobile afin de découvrir son environnement et les points d'accès auxquels, il peut potentiellement s'attacher. Ces mesures sont :

- la puissance du signal reçu (qui est un indicateur de qualité).
- le taux d'erreur binaire.
- la distance entre le mobile et le point d'attachement.

Dans cette phase, le Handover vertical doit être utilisé en conjonction avec les mesures (signal reçu, taux d'erreur,...). Les éléments sont les suivants :

- Type de service : On peut avoir différents types de services qui demandent des qualités de services différentes.
 - Le coût : Il s'agit d'un élément très important pour l'utilisateur, car les opérateurs vont utiliser des stratégies de taxation qui vont déterminer son choix.
 - Paramètres réseau : Des paramètres de réseau comme le trafic, la bande passante disponible.
 - Performance du système : On peut inclure ici des paramètres de canal comme la BER, l'interférence.
- La batterie peut avoir aussi une influence dans le handover.

II.5.2. Phase de décision :

Lorsque des paramètres mesurés sur l'accès courant franchissent certains seuils (puissance de signal, taux de perte), le mécanisme de HO est déclenché.

La phase de décision qui vient une fois que le mobile a déjà acquis son environnement, et qui consiste à choisir parmi la liste des AR disponibles le prochain AR auquel il va s'attacher. Ce choix peut être fait par le mobile ou par une entité dans le réseau. La seconde approche est souvent utilisée pour préparer l'attachement avant que le changement de AR ne soit commencé afin de réduire le temps d'interruption.

En fonction du niveau de la pile réseau auquel on se place, les informations utilisées pour prendre la décision ne sont pas de même nature.

De plus en plus, les approches cherchent à s'affranchir la séparation stricte en couche dont on n'est plus très sûr qu'elle soit bien adaptée à la gestion de la mobilité. Elle limite, en effet, l'acheminement des données utiles au déclenchement du Handover puis à la sélection du prochain AR, surtout en environnement hétérogène où chaque niveau de liaison ne dispose que des informations relatives à sa technologie d'accès et ne voit pas les AR d'autres technologies présents dans la zone.

II.5.3. Phase d'exécution du Handover :

La phase d'exécution comprend l'attachement au nouvel AR, c'est-à-dire l'ensemble des actions que le mobile doit entreprendre pour être capable de communiquer à travers le nouvel AR. Une fois l'attachement effectué, il est nécessaire de faire la publicité de la nouvelle localisation pour permettre aux nouveaux correspondants de joindre le mobile en fonction d'une identité qu'ils connaissent. Il s'agit donc d'avertir le réseau et/ou les correspondants courants ou potentiels de la nouvelle position du mobile. Il faut ensuite diriger le trafic vers la nouvelle position. Dans le cas de la mobilité IP les deux dernières actions sont combinées lors des mises à jour d'association qui informe l'agent mère (ou Home Agent) ou les correspondants pour qu'ils envoient leur trafic vers la nouvelle position.

II.6. Types de Handover :

Un mécanisme de Handover qu'il est proactif lorsque tout ou partie de la phase d'exécution peut être préparée avant le changement effectif du point d'attachement. Il sera réactif lorsque l'ensemble des phases sont effectués après. Nous avons deux grandes catégories de handover suivant ce qu'il se déroule au niveau liaison (handover L2) ou au niveau réseau (handover L3), dont plusieurs types sont possibles :

II.6.1. Hard Handover :

Le mécanisme du Hard Handover est appliqué généralement dans le cas d'une mobilité relativement lente ou moyenne. Durant le Handover, ce mécanisme oblige la station mobile à interrompre la connexion avec l'ancienne station de base avant d'établir la connexion avec la nouvelle station de base (mécanisme Break-Before-Make). [10]

Ce type de Handover est utilisé dans les systèmes cellulaires, où chaque cellule a une bande de fréquences différentes. Quand l'utilisateur entre dans une nouvelle cellule, il entraîne la démolition de la connexion existante avant qu'une nouvelle connexion utilisant une autre fréquence soit établie dans la cellule visitée. L'algorithme de ce type de handover est assez simple ; la station mobile effectue un Handover lorsque la puissance du signal d'une cellule voisine dépasse la puissance du signal de la cellule actuelle à un seuil donné. [11]

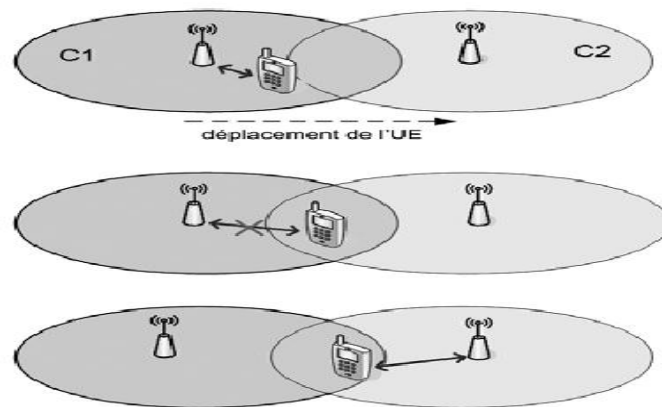


Figure II.9 : Hard Handover.

Le problème majeur du hard Handover c'est la coupure de communication causé par la non disponibilité des ressources. Ce problème peut être résolu par l'introduction d'un critère de priorité concernant l'allocation des ressources. Dans une cellule donnée, la demande des ressources pour le Handover est prioritaire par rapport aux nouvelles demandes. Cette idée mène à une mauvaise efficacité spectrale puisque, pour une cellule donnée, on aura des ressources non utilisées lorsqu'il n'y a pas de demandes de Handover vers cette cellule ce qui implique un blocage pour les nouvelles demandes.[11]

Ce mécanisme est bénéfique du point de vue de l'allocation des ressources, mais en cas d'échange du trafic temps-réel de volume important, ou dans le cas du déplacement du mobile avec une vitesse

importante, ce mécanisme provoque une interruption de service au cours du Handover, ce qui n'est pas bon pour le trafic temps-réel. [10]

Le Handover du GSM est un Hard Handover car le circuit est complètement relâché avant qu'un nouveau soit établi. Aussi le réseau WIMAX utilise ce type de Handover.

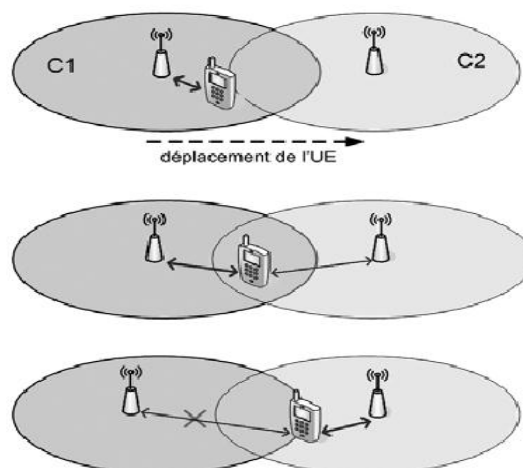
Le réseau de mobilité (NEMO) a été normalisé par IETF pour faciliter la connectivité Internet continue à hôtes dans un tel réseau. Le routeur mobile est l'élément clé dans un réseau mobile, il fournit la connectivité Internet à tous les nœuds de réseaux mobiles.

Le protocole NEMO Basic permet à MR de se connecter au réseau d'accès via une interface physique qui est moins fiable. Au cours de la période du Handover, le MR doit briser la connexion avec l'ancien réseau d'accès avant d'établir une connexion (break-before-make) avec le nouveau réseau d'accès, résultant l'augmentation du temps de Handover et la perte de paquets. Le problème majeur du hard Handover dans le réseau mobile c'est la coupure de communication qui effectue le retard des applications sensibles par exemple la voix sur IP, la vidéo à la demande. Donc le fonctionnement de NEMO est une mauvaise. [12]

II.6.2. Soft Handover :

Le soft-Handover (SHO) est une technique qui permet au mobile de se déplacer d'un routeur d'accès à un autre routeur d'accès sans déconnexion. Ainsi, le mobile a toujours une connectivité de bonne qualité avec le réseau de cœur : les pertes de paquets induites par le Handover sont inexistantes, et la gigue induite par la dégradation du signal radio est minime. [13]

Le soft-Handover est réalisable, si le mobile est capable de communiquer simultanément avec plusieurs routeurs d'accès (mécanisme make-before-Break), c'est-à-dire, soit le mobile dispose de plusieurs interfaces sans-fil (homogènes ou hétérogènes), soit la technologie d'accès permet la connexion du mobile vers plusieurs routeurs d'accès (802.11 en mode ad-hoc, ou WCDMA).



Rapport-gratuit.com

LE NUMERO 1 MONDIAL DU MÉMOIRES

Rapport-gratuit.com

LE NUMERO 1 MONDIAL DU MÉMOIRES

Figure П.10 : Soft Handover.

Il propose deux techniques : le MDHO et le FBSS.

II.6.2.1. MDHO :

Durant le Handover, le MDHO (Macro Diversity Handover) permet à la MN de se connecter aux routeurs d'accès voisins appartenant à une liste des ARs (Diversity Set) maintenue par la MN avant d'interrompre la connexion avec l'ancien routeur d'accès (mécanisme Make-Before-Break). Dans ce cas le mobile communique avec plusieurs routeurs d'accès en même temps.

Contrairement au Hard Handover, ce mécanisme utilise beaucoup de ressources radio vu qu'il se connecte à plusieurs ARs en même temps, mais il permet d'éviter l'interruption du service au cours du Handover. [10]

II.6.2.2. FBSS :

Le FBSS (Fast Base Station Switching) est très proche du MDHO dans son principe (Make-Before-Break). Il ajoute une technique qui se résume dans le fait que le mobile peut choisir parmi les ARs avec lesquelles, il est connecté une seule qui sera appelée AR ancre (Anchor AR). Il va échanger avec cette AR ancre tous ses données ainsi que les messages de signalisation. La MS aura le droit de changer de l'AR ancre quand elle le voudra, à condition qu'elle choisisse un nouvel AR ancre parmi la liste des ARs appartenant à son Diversity Set avec lesquelles, elle est connectée. Généralement, la MN change de AR ancre quand cette dernière n'est plus disponible en nombre de connexions ou en ressources, ou bien encore quand le signal d'une autre AR candidate deviendra meilleur que celui de son AR Ancre courante. [10]

Ce type de Handover est utilisé à partir de l'UMTS et dans les générations suivantes puisqu'il maintient la connexion lors du Handover, même le réseau WIMAX utilise le soft Handover.

Le Soft Handover permet plus de deux liens sans fil pour réduire les pertes de paquets, et aussi pour éviter d'injecter plusieurs copies de paquets dans le LFN lorsque les deux paquets dupliqués sont livrés avec succès. En comparaison avec le make-before-Break transfert, la différence significative est de savoir si le même paquet est distribué sur deux liaisons sans fil ou non à certains moments. Cela signifie que les utilisateurs peuvent compter sur les deux liaisons pendant un temps donné, dans le cas de NEMO-SHO, alors que le make-before-Break oblige les utilisateurs à s'appuyer soit sur le lien actuel ou sur le nouveau lien.

II.6.3. Fast Handover :

Le Fast Handover a été accepté comme une solution efficace de Handover pour résoudre les problèmes de latence de Handover et de perte de paquets. Cette solution assure une latence de handover beaucoup plus courte et moins de perte de paquets par une détection rapide du mouvement et réduction du délai d'enregistrement de la nouvelle CoA.

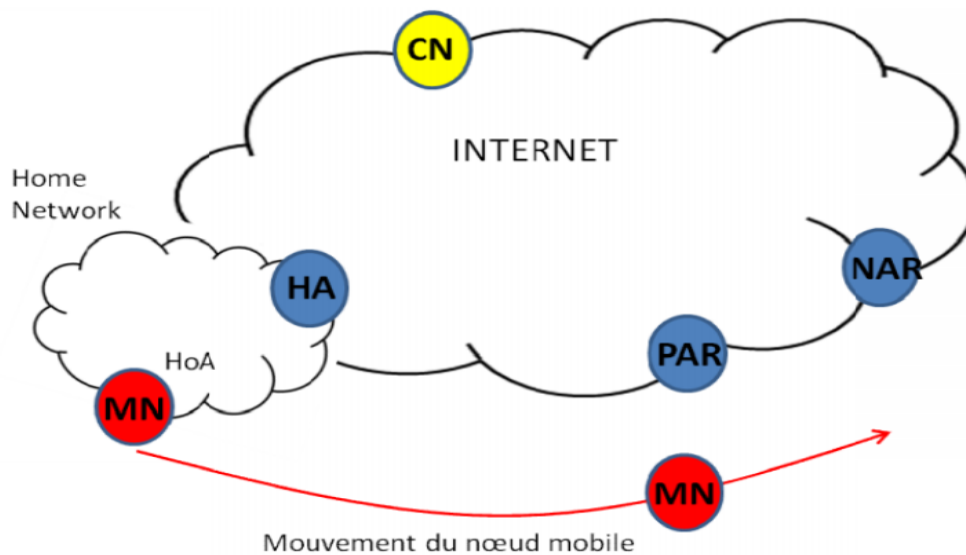


Figure П. 11: Fast Handover

Où :

1. PAR (Previous Access Router) : le routeur d'accès précédent.
2. NAR (New Access Router) : le nouveau routeur d'accès.
3. NCoA (New CoA) : nouvelle adresse temporaire CoA.
4. PCoA (Previous CoA) : l'adresse temporaire CoA précédente.

Le Fast Handover utilise les messages suivants :

- RtSolPr (Router Solicitation for Proxy Advertisement) : ce message est envoyé par le MN à son PAR pour demander les informations concernant un Handover potentiel.
- PrRtAdv (Proxy Router Advertisement) : ce message est envoyé par le PAR au MN pour fournir les informations concernant les liens d'accès des réseaux voisins, facilitant ainsi la détection rapide de mouvement.
- FBU (Fast Binding Update) : ce message est envoyé par le MN à son PAR. Il a pour objet de permettre au PAR de lier l'adresse temporaire précédente PCoA à la nouvelle adresse temporaire NCoA et de rediriger les paquets destinés à l'adresse temporaire précédente (PCoA) à sa nouvelle adresse temporaire (NCoA).
- FBBack (Fast Binding Acknowledgement) : ce message est envoyé par le PAR au MN et au NAR pour indiquer la création d'un tunnel.
- HI (Handover Initiate) : ce message est envoyé par le PAR au NAR pour le Handover du MN.
- HAck (Handover Acknowledge) : ce message d'acquiescement du Handover est envoyé par le NAR au PAR pour répondre au message HI.
- FNA (Fast Neighbor Advertisement) : ce message est envoyé par le MN à son NAR pour annoncer son attachement sur ce réseau. Il est aussi utilisé pour assurer la possibilité d'utilisation de la nouvelle adresse temporaire (NCoA) si le MN n'a pas reçu le message FBBack.[6]

Après avoir découvert un ou plusieurs liens d'accès, le MR envoie un message RtSolPr au PAR afin d'obtenir les informations de préfixe des routeurs d'accès associés à ces nouveaux liens. L'envoi de ce message peut être déclenché par un trigger L2. A la réception du message RtSolPr, le PAR répond au MN en envoyant le message PrRtAdv qui contient les informations concernant les routeurs d'accès, tels que le préfixe, l'adresse IP et l'adresse MAC. Une fois que le message PrRtAdv est reçu par le MN, il peut s'auto-configurer avec une nouvelle adresse temporaire NCoA qui est potentiellement utilisable dans le nouveau réseau.[6]

II.6.3.1. Mode prédictif :

Le MN envoie sa nouvelle adresse (NCoA) au PAR au moyen du message FBU du réseau du PAR. Le PAR doit assurer la possibilité d'utilisation de la nouvelle adresse temporaire NCoA pour le MN dans le nouveau réseau avant d'envoyer la réponse FBack au MN. Il envoie le message HI qui contient l'adresse MAC, l'adresse PCoA et l'adresse NCoA du MN au NAR. Le NAR approuve l'utilisation de cette adresse NCoA ou propose une nouvelle adresse NCoA en envoyant le message Hack au PAR. A la réception du message Hack, le PAR envoie le message FBack au MN et au NAR pour répondre au message FBU.

Si le NAR propose une nouvelle adresse NCoA, le PAR doit informer le MN au moyen du message FBack. Ainsi, le MN pourra utiliser sa nouvelle adresse NCoA dans le nouveau réseau puisqu'il a reçu le message FBack avant de changer le réseau. Dès que le MN s'attache au nouveau réseau, il envoie le message FNA au NAR pour annoncer son attachement à ce nouveau réseau. [6]

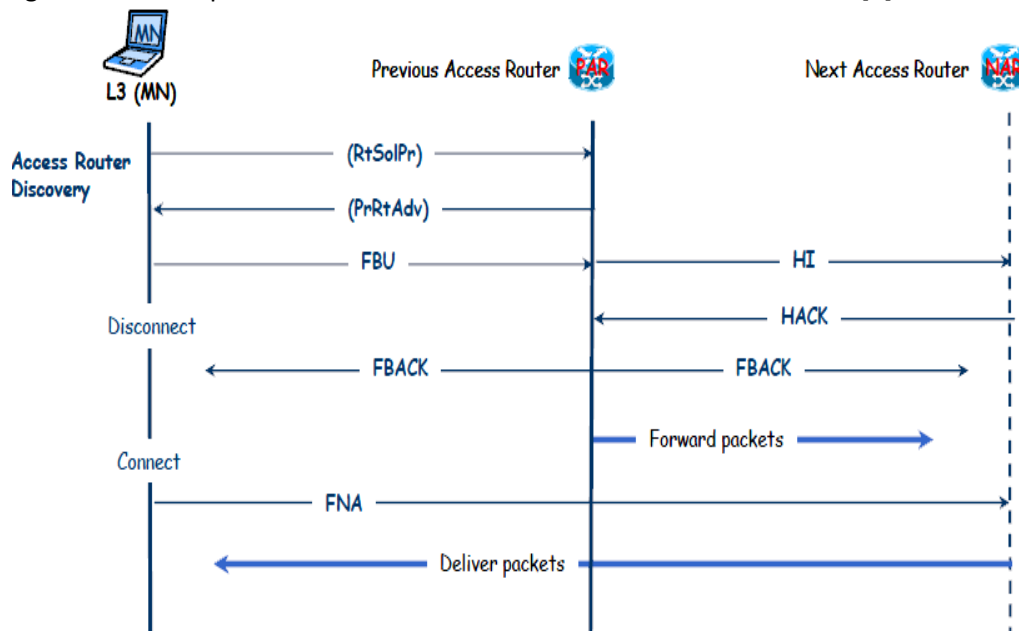


Figure П. 12: Procédure du mode prédictif de FHO.

Le PAR crée le tunnel entre l'AR précédent et le NAR et redirige les paquets du MN à sa nouvelle adresse NCoA. Par conséquent, le MN peut envoyer et recevoir les paquets via ce tunnel pendant la phase de Mise à jour d'association. [6]

II.6.3.2. Mode réactif :

Le MN n'a pas pu envoyer le message FBU ou n'a pas pu recevoir le message FBack avant de changer de réseau. Donc, le MN ne peut pas assurer qu'il peut utiliser la nouvelle adresse NCoA. Le PAR peut créer une association entre l'adresse PCoA et l'adresse NCoA. Une fois que le MN s'attache au nouveau réseau, il utilise son adresse NCoA comme l'adresse source du message FNA.

Le message FBU est encapsulé dans le message FNA. Ce message FNA est envoyé au NAR.

Si le NAR approuve l'utilisation de la nouvelle adresse NCoA, il envoie le message FBU au PAR. En réponse au message FBU, le PAR crée l'association et le tunnel entre l'adresse PCoA et l'adresse NCoA. Ensuite, les messages HI/HACK sont échangés de la même manière que dans le mode prédictif. Le PAR peut alors tunnelier le FBack ainsi que les paquets à destination du MN en passant par le NAR. Dans le cas contraire, le NAR soit propose une nouvelle adresse NCoA au MN, soit lui demande de générer une nouvelle tout en envoyant un message Router Advertisement au MN. [6]

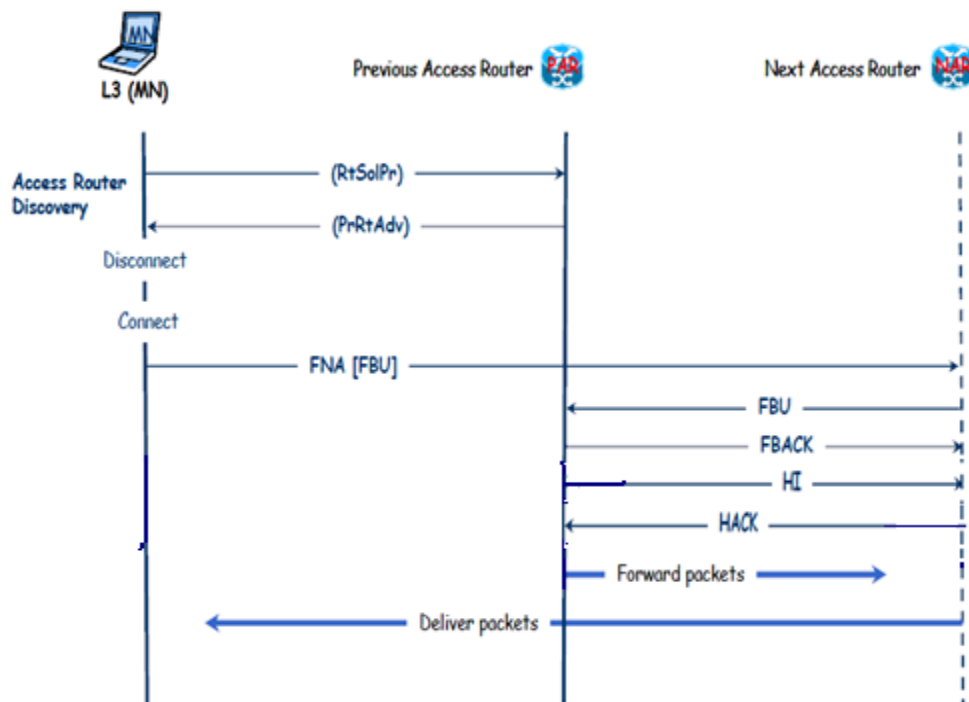


Figure Π. 13: Procédure du mode réactif de FHO.

II.6.4. Smooth Handover :

Le MN change le routeur d'accès (AR) à un autre AR. Ce changement d'AR est considéré comme un Handover. Lors de Handover et avant, le HA reçoit la nouvelle CoA de MR, en lui envoyant des paquets où certains d'eux sont probablement perdus [14].

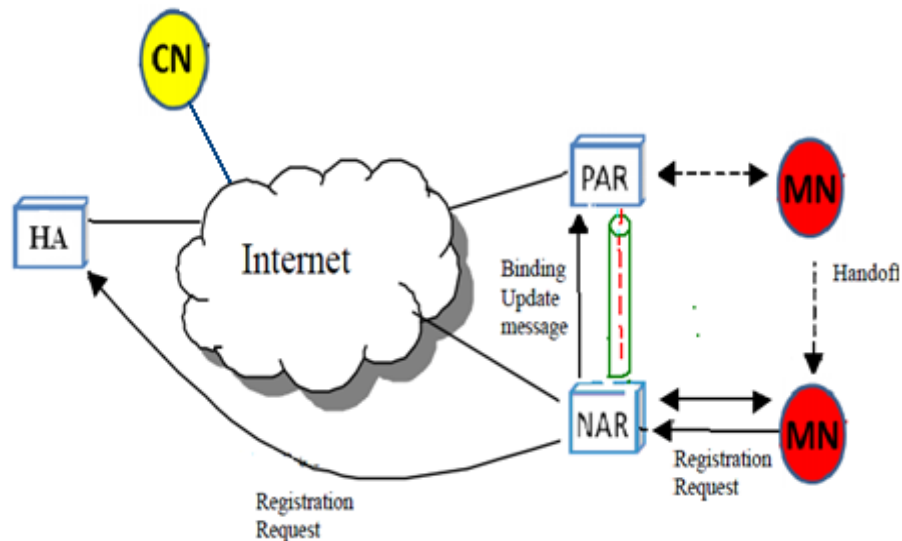


Figure П. 14: Principe de fonctionnement Smooth Handover.

Le smooth Handover est une technique qui réduit le nombre de pertes de paquets IP, en moment de Handover. Pour réduire ces pertes, il fait appel à un mécanisme de sauvegarde dans PAR. Le PAR effectue une copie de tous les paquets qu'il transmet au mobile avant, pendant et après la déconnexion. [13]

Nous partons du principe qu'il n'existe pas des chevauchements entre deux éléments AR, ce qui signifie que le MN est toujours à l'intérieur de la cellule d'au moins une AR. Cependant, il peut y avoir des chevauchements entre les cellules adjacentes qui couvrent les ARs, ce qui signifie que le MN pourrait recevoir des agents advertissements de plusieurs ARs. Les solutions différentes sur lesquelles AR à utiliser .la solution est basée sur la force du signal et qu'il y a un certain chevauchement entre les cellules de AR adjacentes. Comme le MN commence à se déplacer, il remarque que les signaux reçus par le MN sont en train de s'affaiblir. [14]

Le MN commence alors à chercher un autre AR. Quand il reçoit un agent avertissements de NAR, (l'étape initiale de Handover), le MN envoie le Registration Request à NAR qui la transmet au HA. Si le MN obtient son nouvelle localisation et son NCoA, le NAR demande à PAR d'envoyer les paquets mémorisés au MN à cette NCoA, le NAR doit informer le PAR au moyen du message binding update. Le PAR répond par le message Binding Ack (Back) au NAR. [14]

Le NAR établit un tunnel IP avec le PAR et ce dernier indique la présence de MN. A cet instant, le PAR transmet au mobile, et à travers le tunnel, tous les paquets précédemment sauvegardés. Le NAR décapsule alors ces paquets et les transmet au MN. Les paquets dupliqués et sauvegardés lors de la déconnexion sont récupérés localement. [13]. Lorsque le HA reçoit la demande d'enregistrement, il traite la requête puis envoie le registration reply à NAR qui le transmet au MN. Le Registration reply contient les informations indiquant si la demande a été acceptée ou rejetée. [14].

II.6.5. Handover sans coutures ou Seamless Handover :

Le Seamless Handover est une extension du Fast Handover, dont l'objectif est la réduction du protocole de signalisation i.e. la quantité de message de signalisation. En fait, le Seamless Handover permet également d'obtenir un temps de latence de Handover similaire à celle du retard de Handover L2 (l'ordre de plusieurs dizaines de millisecondes), donc de réduire le temps d'interruption des communications entre le MN et ses correspondants. Celui-ci permet de Minimiser la perte de paquets.

Le mécanisme de Seamless Handover ajout une nouvelle entité dénommée decision engine (DE). Comme dans la hiérarchique, il introduit une entité appelée MAP (Mobility Anchor Point) qui découpe le réseau global en différents domaines pour gérer la mobilité [15]. La Decision engine (DE) contrôle la procédure de Handover dans son domaine de réseau, et prendre les décisions de Handover. Lorsque les nœuds mobiles peuvent déplacer au domaine de réseau, la DE poursuit ces nœuds mobiles afin d'identifier les modes de déplacement. Cela peut se faire par le biais de messages périodiques des routeurs d'accès. Pour minimiser les pertes des paquets, on utilise le processus SPS (Synchronized-Packet-Simulcast) qui permet de transmettre les paquets en même temps au routeur d'accès précédent et au routeur d'accès potentiel où le nœud mobile se déplace [15].

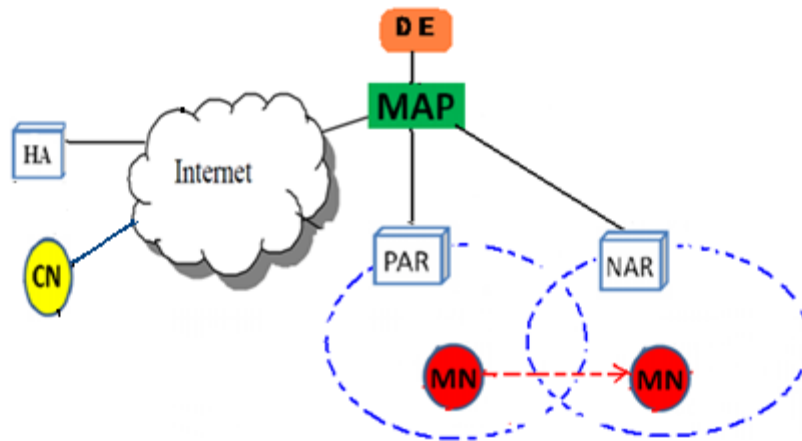


Figure П.15: Principe de fonctionnement Seamless Handover.

Ce type de Handover ajoute six nouveaux messages aux messages de Fast Handover :

- CTS (Current Tracking Status): ce message est envoyé par le MN à DE pour donner des informations de localisation.
- CLS (Carrying Load Status) : ce message est envoyé par les ARs au DE pour fournir les informations concernant le nombre de nœuds mobiles géré actuellement par le AR.
- HD (Handover Decision) : ce message est envoyé par DE à AR, ce message contient la décision de Handover par DE, donc déterminer le AR avec lequel, le MN peut attacher avec lui.
- HN (Handover Notification) : ce message est envoyé par PAR à MN pour fournir les informations concernant le NAR.
- Scast (Simulcast) : ce message est envoyé par PAR à MAP Pour démarrer le processus de SPS.
- Soff (Simulcast Off) : ce message est envoyé par NAR à MAP. Ce message arrête le processus de SPS.

Le Seamless Handover commence lorsque le nœud mobile veut passer à un nouveau réseau, il recevra des messages beacon advertisement du nouveau routeur d'accès. Au début de Handover, le MN envoie un message RtSolPr à PAR. A la réception du message RtSolPr, le PAR transmet le message HI à tous les NARs potentiels avec lesquels le MN lui demande dans le message RtSolPr. Ce message contient la nouvelle adresse NCoA et l'ancienne adresse PCoA.

Tous les NARs répondent par un message Hack qui indique l'acceptation ou la récusation de NCoA. Dans le cas où le NAR accepte la nouvelle CoA, le PAR établit un tunnel temporaire à la NCoA. Dans l'autre cas, le PAR établit un tunnel des paquets à NAR, qui transmet temporairement au MN. En réponse de RtSolPr, le MN reçoit un message PrRtAdv de PAR [15].

Le MN envoie un message CTS à DE quand il reçoit un message beacon advertisement d'un nouveau routeur d'accès. Le message CTS contient des informations sur la puissance du signal du nouveau routeur d'accès. Cette information sera utilisée pour la localisation, les NARs transmettent un message CLS à chaque seconde jusqu'à ce qu'il reçoit un message HD de DE. Le message CLS indique le nombre de nœuds mobiles qui ont été connectés au routeur d'accès et leurs adresses IP. Le DE analyse le message CLS et le message CTS afin de suivre le mouvement de nœud mobile pour un courte période (moins de trois second), puis le DE donne la décision et envoie un message HD à tous les NARs participants. Ensuite, le PAR envoie un message HN avec le PrRtAdv au MN indiquant exactement par quel NAR, le MN devrait passer [16].

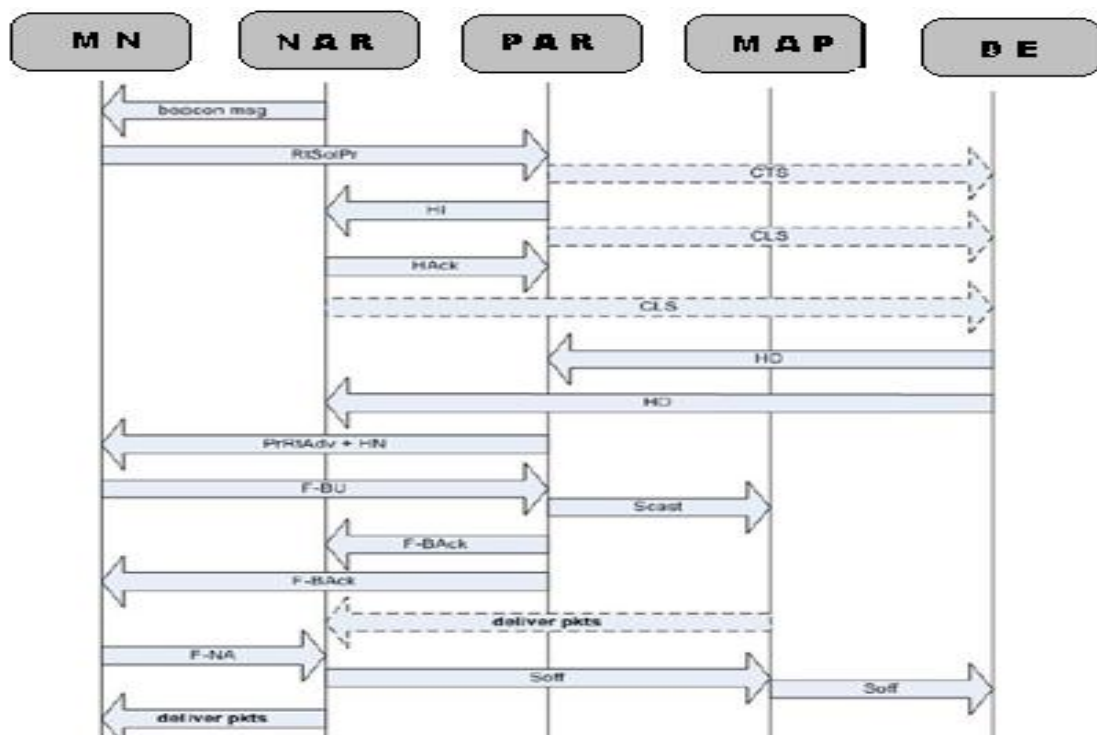


Figure 11.16: Procédure de Seamless Handover. [15]

Le mode de mouvement de Seamless Handover suit trois procédures :

II.6.5.1. La procédure du mode de mouvement stochastique :

L'utilisation de message HD pour informer les NARs à l'anticipation de mode. Dans ce mode, le MN ne veut pas être associé à NAR. Le MN prépare une liaison avec le NAR pour que le MN retourne à ce NAR. Cela permet d'éviter l'utilisation des ressources inutiles et réduire le temps. Le PAR transmet au MN le message HN qui indique que le MN est capable de passer au réseau. Une fois la force du signal est diminuée jusqu'à un certain seuil prédéfini, Le DE envoie un autre message HD aux NARs participants, dans le cas où il a déterminé qu'ils ne sont plus nécessaires dans l'anticipation de mode [16].

II.6.5.2. La procédure du mode de mouvement stationnaire :

Le MN sera l'état stationnaire entre deux zones de couverture NARs. Le DE utilise le message HD pour établir plusieurs liaisons entre le MN et NARs. Ces derniers permettent au MN d'utiliser plusieurs CoAs en même temps.

II.6.5.3. La procédure du mode de mouvement linéaire:

Le message HD contient les informations du NAR où le MN peut se déplacer. Un autre message HD inclut le reste des informations d'autres NARs qui ne sont pas sélectionnés par le DE [15].

Ensuite, le MN transmet le message FBU à PAR, après il reçoit le message HN et forme la NCoA, afin d'associer entre le PCoA et le NCoA. La procédure SPS est lancée au moyen de message Scast qui est envoyé au MAP par PAR, ce qui signifie la duplication d'envoi des paquets à PAR et à NAR en même temps. Le PAR envoie le message Fback au MN et NAR.

Après réception du message FNA qui démontre que le MN est arrivée au nouveau réseau, le NAR transmet des paquets au MN. Pendant ce temps, le PAR est également transmis les paquets au NAR. Ce dernier envoie tous les paquets sur le canal sans fil pour assurer la réception par le nœud mobile dans le cas où il n'a pas changé de réseau immédiatement. Puis, le NAR envoie un message Soff à MAP après il transmet tous les paquets qui sont envoyés par PAR au MN pour la mise à jour de la liaison entre la nouvelle adresse du MN et son adresse régionale. Le message Soff sera transmis à la DE, qui ne permettra pas au nœud mobile d'exécuter un autre Handover avant que la procédure de Handover en cours est terminée [15].

Le tableau ci-dessous indique le type de Handover utilisé dans le réseau adéquat.

	Hard Handover	Soft Handover	Fast Handover	Handover sans coutures	Smooth Handover
WIFI					
GSM	x				
UMTS		x			
WIMAX	x	x			
GPRS	x				
NEMO	x	x	X	x	X

Tableau II.1: les types de handover de différents réseaux

II.7. Les paramètres de qualité de service :

Comme la Qualité de Service (QoS) est un point important dans tous les réseaux (informatique et télécom.), il semble intéressant d'étudier les moyens permettant d'introduire cette notion dans les réseaux NEMO où les terminaux sont en mouvement les uns par rapport aux autres.

La QoS peut être apportée à différents niveaux : couche application, couche transport, couche réseau, couche MAC, etc.

La qualité de service possède quatre paramètres de performance qui sont :

II.7.1. Le délai (Delay) :

Il correspond au temps que met un paquet pour traverser le réseau d'un point d'entrée à un point de sortie [17].

II.7.2. La gigue (jitter) :

Elle représente la variation des délais d'acheminement des paquets dans le réseau.

II.7.3. Le taux de perte de paquets (paquet loss) :

Les pertes de paquets sont dues à des phénomènes de congestion sur le réseau ou à une mauvaise qualité de liaison.

II.7.4. Le débit :

Il désigne le nombre de bits transmis par seconde.

II.8. Analyse du délai du Handover NEMO :

Le protocole NEMO BS proposé par IETF fournit un support de mobilité pour un réseau mobile entier en se déplaçant à travers différents réseaux d'accès hétérogènes. L'accès continu et non interrompu à Internet aux nœuds (MNN) à l'intérieur du réseau mobile NEMO est fourni par le routeur mobile (MR) qui contrôle le mouvement du réseau NEMO.

Le MR est identifié par son adresse (HoA) par laquelle, il est accessible dans son réseau mère, et il est localisé par son adresse (CoA) acquise au réseau visité. L'agent mère (Home Agent : HA) situé au réseau mère aide le MR dans la gestion de mobilité du réseau NEMO. Pour changer son point d'attachement à un nouveau réseau d'accès (i-e : attachement à un nouveau routeur d'accès AR), Le MR doit exécuter en général un handover vertical comprenant les deux Handovers L2 et L3.

II.8.1. Délai du Handover L2 :

Puisque les Handover L2 et L3 sont indépendants dans le protocole de NEMO BS (le Handover L3 se produit après le Handover L2), le délai global du Handover T_{HO} peut être exprimé par l'équation suivante :

$$T_{HO} = T_{L2} + T_{L3}$$

Où :

- T_{L2} est le délai du Handover de la couche L2 (le temps requis pour établir une nouvelle association par l'interface physique)
- T_{L3} est le délai du Handover de la couche L3 ou niveau IP (c'est le délai pour enregistrer une nouvelle adresse CoA auprès du Home Agent (HA) et recevoir le premier paquet de données à cette nouvelle localisation)

La procédure du Handover L2 inclue en général les trois phases suivantes qui dépendent de la technologie d'accès et affichent une grande variation :

1. Le scanning introduisant un délai T_{scan}
2. L'authentification T_{auth}
3. L'association T_{ass}

Les valeurs publiées du délai T_{L2} sont entre 50 ms et 400 ms :

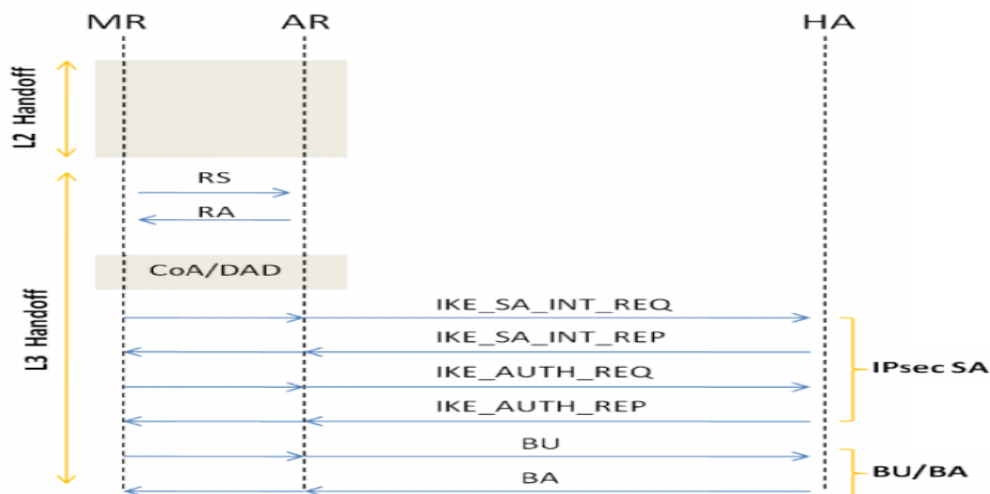


Figure П.17: Procédures du Handover NEMO BS.

Il s'en suit :

$$T_{L2} = T_{scan} + T_{auth} + T_{ass}$$

Le Handover L2 est déclenché par l'évènement de lien Link Down correspondant à la condition suivante:

$$P_{rx} < P_{th}$$

Où :

- P_{rx} : est la puissance du signal reçu correspondant à l'indication RSSI (Received Signal Strength Indication).
- P_{th} : est la puissance de seuil prédéfinie en-dessous de laquelle le statut de lien est considéré rompu (Link_Down).

II.8.2. Délai du Handover L3 :

La procédure du Handover L3 est composée de quatre phases distinctes :

1. Détection de Mouvement (Movement Detection , MD) : Si le MR change l'AR et que ce nouvel AR appartient à un réseau différent, le changement d'AR entraîne un changement de réseau. Dans ce cas, le MR doit effectuer la procédure du Handover de niveau 3 pour pouvoir maintenir sa connexion avec ses correspondants. Pour cela, le MR doit d'abord détecter le changement de réseau avant d'auto-configurer sa nouvelle adresse IP. Le MR détecte son mouvement grâce à l'information de préfixe contenue dans les messages reçus « Router Advertisement (RA) » annoncés périodiquement par le nouvel AR (new AR, NAR). Le MR peut agir d'une façon proactive en envoyant des messages « Router Solicitation (RS) » pour obtenir les messages RA des routeurs voisins. Le MR détecte son mouvement si le routeur PAR est inaccessible, (i-e : aucun message RA provenant du PAR n'est reçu).
2. Assignation d'adresse CoA et test DAD : Après la réception de l'information de préfixe du NAR, le MR procède à la configuration automatique state less (dont le délai est négligeable); le MR s'auto-configure avec une nouvelle adresse CoA (construite à partir du nouveau préfixe) et doit vérifier son unicité avec le processus DAD (Duplicate Address Detection). Le processus DAD consiste à diffuser sur le lien une requête de recherche de nœuds possédant la même adresse IP choisie. Si au bout d'une seconde (valeur par défaut) aucune réponse n'est reçue alors l'adresse IP choisie est considérée unique ; si non, elle est considérée dupliquée et une reconfiguration est obligatoire.
3. Association de sécurité IPsec (IPsec Security Association, SA) : Une fois que le MR a obtenu une adresse CoA unique, il doit s'enregistrer au près de son HA. Toutefois, comme indiqué par, tous les messages de signalisation entre le MR et le HA doivent être authentifiés par IPsec ; le MR doit donc établir préalablement un tunnel IPsec avec son HA ; pour ce faire, le MR crée une association de sécurité (SA) avec son HA en utilisant le protocole IKE (Internet Key Exchange).
4. Enregistrement BU/BACK : Dès que le MR s'est auto-configuré avec une nouvelle et unique adresse CoA et qu'une association de sécurité est créée entre le MR et son HA, le MR envoie immédiatement un binding update (BU) à son HA. A la réception de ce message, le HA enregistre la CoA dans son binding cache et renvoie un binding ACK (BACK) au MR.

Ainsi, le délai du Handover L3 peut être calculé analytiquement par :

$$T_{L3} = T_{MD} + T_{DAD} + T_{Reg}$$

Où:

- T_{MD} : est le délai de la procédure de détection de mouvement.
- T_{DAD} : est le délai du test DAD.
- T_{Reg} : est le délai de l'enregistrement d'une adresse CoA, y compris le délai de l'association de sécurité IPsec.

Sous la forme explicite, nous avons :

$$T_{MD} = T_{RS} + T_{RA}$$

$$T_{Reg} = T_{SA} + T_{BU} + T_{BA}$$

Où:

- T_{RS} : est le délai du 'Router Solicitation'
- T_{RA} : est le délai du 'Router Advertisement'
- T_{SA} : est le délai de la création d'une association de sécurité IPsec (SA)
- T_{BU} : est le délai du Binding Update
- T_{BA} : est le délai du Binding Ack

En référant à la figure Π.9, nous pouvons exprimer T_{L3} en fonction de RTT_{MR-AR} et RTT_{AR-HA} , (RTT est le délai aller-retour : Round Trip Time) :

$$T_{L3} = 4 RTT_{MR-AR} + T_{DAD} + 3RTT_{AR-HA}$$

II.8.3 .Evaluation numérique.

Pour mettre en évidence les performances du Handover NEMO BS, nous avons conduit des tests numériques sous Matlab. Les résultats sont représentés dans les figures Π.10, Π.11 et Π.12.

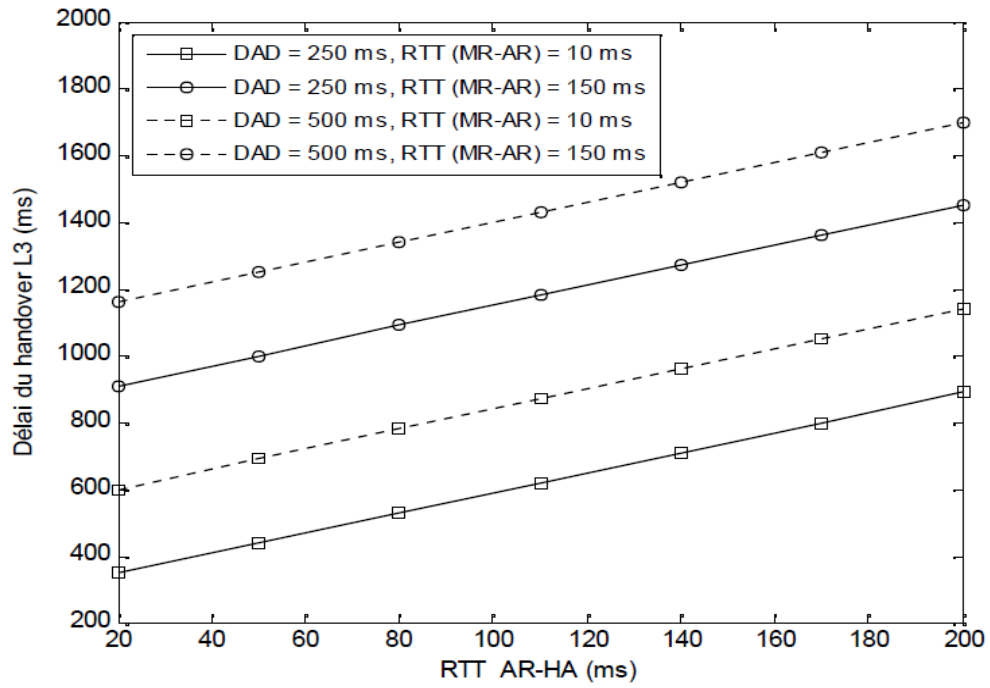


Figure П.18: Délai du Handover NEMO (Handover L3).

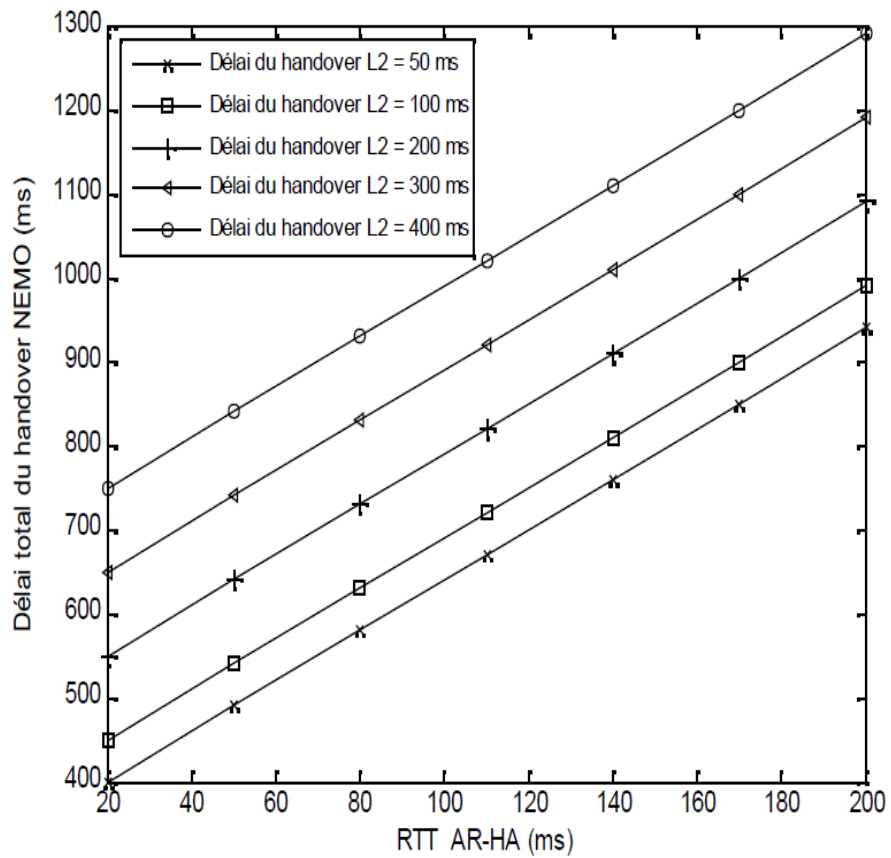


Figure П. 19: Délai total du Handover NEMO (Handover global).

La figure (П.10) représente le délai partiel du Handover NEMO concernant le niveau L3.

Pour le paramétrer, nous avons utilisé comme valeur minimale 10 ms et comme valeur maximale 150 ms. Cette plage regroupe toutes les valeurs possibles pour les différentes technologies (IEEE 802.11, IEEE 802.16, 3GPP et 3GPP2). Pour le (double délai de l'internet), nous avons utilisé les données publiés par [66], soit la plage [20 ms, 200 ms]. Deux valeurs pour le délai DAD (250 ms et 500 ms) sont utilisées pour prendre en compte la variation du délai DAD.

Nous constatons que le délai du Handover L3 est compris entre une valeur minimale d'environ 350 ms et une valeur maximale de 1.7 s.

Sur la figure П.11, nous avons représenté le délai total du Handover NEMO regroupant celui de L2 et celui de L3. Nous avons retenu pour cette représentation les valeurs minimales de et du délai DAD soit respectivement 10 ms et 250 ms. Pour le délai du Handover L2 qui dépend énormément de la technologie radio utilisée [64, 65], nous avons pris la plage [50 ms, 400 ms]. Nous pouvons facilement voir que la valeur minimale du délai total du Handover NEMO excède la valeur 400 ms, et ce dans les conditions très spéciales décrites précédemment.

La figure П.12 montre que les pertes de données exprimées en Koctets pendant le Handover augmentant avec le délai total du Handover NEMO et le débit de l'application utilisée.

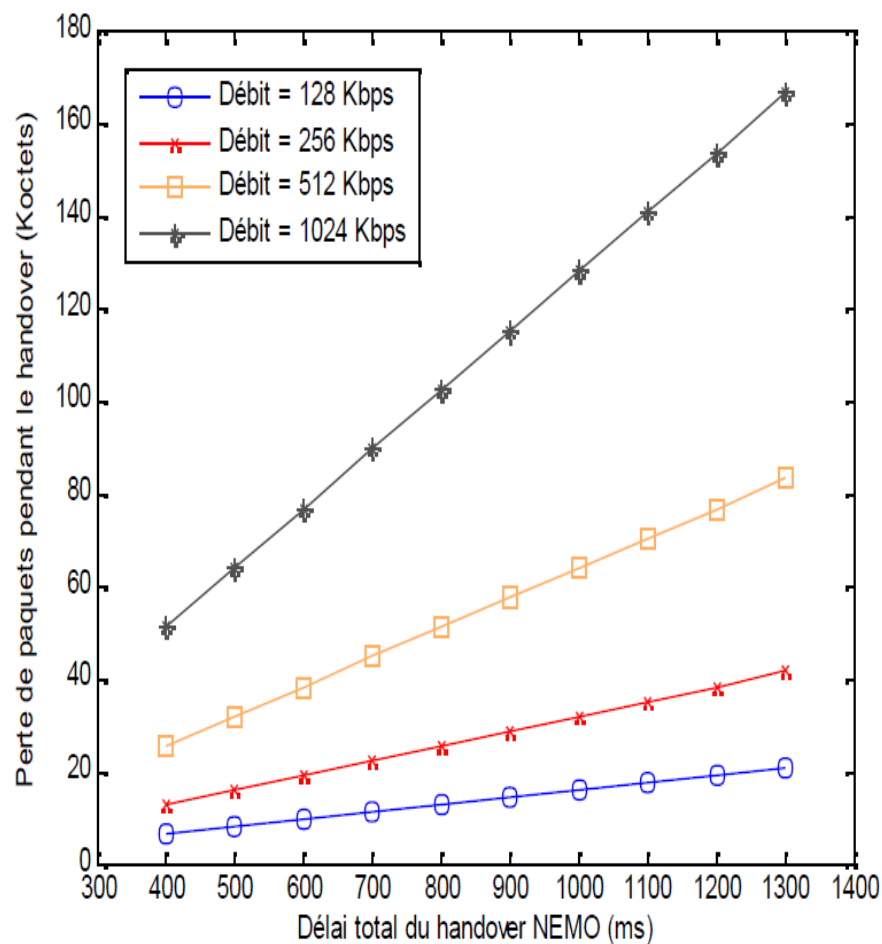


Figure П.20: Perte de paquet pendant le Handover NEMO.

Prenons l'exemple d'une application audio admettant un débit de transfert de 128 Kbps avec des paquets de longueur 80 octets chacun, si nous nous mettons dans les conditions les plus favorables pour lesquelles le délai total du Handover NEMO est minimal, soit 400 ms, alors le nombre de paquets perdus est environ 82, ce qui est inacceptable pour une telle application.

II.9. Conclusion :

Dans ce chapitre, nous avons focalisé sur la gestion de mobilité et nous sommes intéressés aux spécificités du Handover en détaillant ses phases et ses types sans oublier d'étudier le handover dans le cadre de réseau NEMO.

Dans le troisième chapitre, nous envisagerons l'analyse de résultats de simulation obtenus après l'exécution du scénario étudié.

Chapitre3 :

Simulation & Résultats

III.1. Introduction :

Dans ce chapitre, nous implémentons les mécanismes de handover qui se comporte comme l'opération effectuée par un terminal qui change de station de base de service vers une station de base cible. Cela peut se produire quand le terminal se déplace et souhaite conserver un signal de bonne qualité, ou si le terminal voit qu'une autre station de base peut lui fournir une meilleure QoS. Ce handover peut engendrer ou non un handover des couches supérieures selon que les stations de base sont sur le même lien réseau ou non.

Nous avons choisi le logiciel NS (Network simulator) qui est un outil de simulation de réseaux car il se comporte comme un bon outil dans le domaine de la recherche, et du développement de nouveaux protocoles pour différents types de réseaux. Ce simulateur a la caractéristique d'être en accord avec le réel pour la plupart des points suivants : délai, bande passante, durée de vie ; et pour faire de la qualité de service.

III.2. Présentation de logiciel :

III.2.1. Définition de NS2 :

NS2 est un outil de simulation de réseaux de données. Il est bâti autour d'un langage de programmation appelé Tcl dont il est une extension. Du point de vue de l'utilisateur, la mise en œuvre de ce simulateur se fait via une étape de programmation qui décrit la topologie du réseau et le comportement de ses composants, puis vient l'étape de simulation proprement dite et enfin l'interprétation des résultats. Cette dernière étape peut être prise en charge par un outil annexe, appelé nam qui permet une visualisation et une analyse des éléments simulés.

NS2 est en réalité un programme relativement complexe écrit en C++ et interfacé via Tcl. Pour modifier le comportement d'objets existants, il est donc nécessaire de modifier le code C++ qui en réalise l'implantation.

TCL (Tool Command Language) est un langage de commandes qui sert à contrôler les applications. C'est essentiellement un langage de scripts offrant des structures de programmation telles que les boucles, les procédures ou les notions de variables.

III.2.2. Composants :

Le simulateur NS actuel est particulièrement bien adapté aux réseaux à commutation de paquets et à la réalisation de simulations de grande taille (le test du passage à l'échelle). Il contient les fonctionnalités nécessaires à l'étude des algorithmes de routage unicast ou multicast, des protocoles de transport, de session, de réservation, des services intégrés, des protocoles d'application comme FTP. A titre d'exemple la liste des principaux composants actuellement disponibles dans NS par catégorie est :

- application : Web, ftp, telnet, générateur de trafic (CBR...) ;

- transport : TCP, UDP, RTP, SRM ;
- routage unicast : Statique, dynamique (vecteur distance) ;
- routage multicast : DVMRP, PIM ;
- gestion de file d'attente : RED, DropTail, Token bucket.

III.2.3. Organisation du simulateur :

NS-2 est un interpréteur de commandes Otcl qui comporte un ordonnanceur d'événements et une bibliothèque des composants réseaux .l'utilisation de NS-2 se fait en trois temps comme montre la figure suivant :

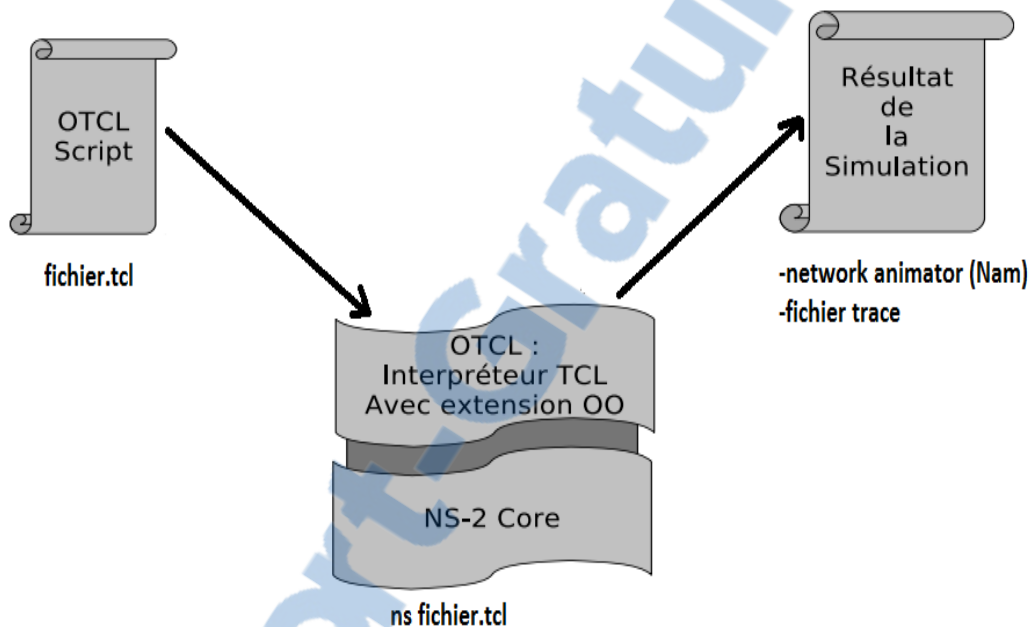


Figure III.1 : Flot de simulation avec NS-2.

- 1- L'utilisateur écrit un script Otcl pour définir la topologie du réseau, pour instancier les différents modules du réseau et pour décrire les scénarios de trafic.
- 2- NS-2 interprète le script et exécute la simulation .les résultats sont stockés dans des fichiers en fonction des commandes du simulateur utilisé.
- 3- Une fois la simulation terminée. les résultats peuvent être analysés directement avec l'outil de visualisation NAM et un fichier de trace.

3-1- Nam : c'est l'outil de visualisation des simulations. L'interface permet de visualiser le déroulement des communications en plaçant la topologie dans l'espace et en simulant les échanges dans le temps.

3-2-fichier Trace : l'exécution d'un fichier .tcl donne un fichier trace contient un événement (d'émission, de réception ou de suppression), le temps simulé auquel chaque événement est arrivé, le type et la taille du paquet.

III.2.4. Architecture du réseau :

NS-2 permet de construire des réseaux fonctionnant sur le principe de la commutation de paquets. Le paquet est l'élément d'information qui circule sur un réseau. Il comporte un en-tête avec les paramètres spécifiques au protocole utilisé. Il contient également un espace qui modélise les données échangées entre les composants du réseau.

Pour définir un réseau, il faut assembler les différents composants suivants :

- **Nœuds** : endroits où est généré le trafic, ou nœuds de routage.
- **Liens** de communication entre les réseaux.
- **Agents** de communication, représentant les protocoles de niveau transport (TCP, UDP); ces agents sont attachés aux nœuds et connectés l'un à l'autre, ce qui représente un échange de données (connexion TCP, flux UDP).
- **Applications** qui génèrent le trafic de données selon certaines lois, et se servent des agents de transport.

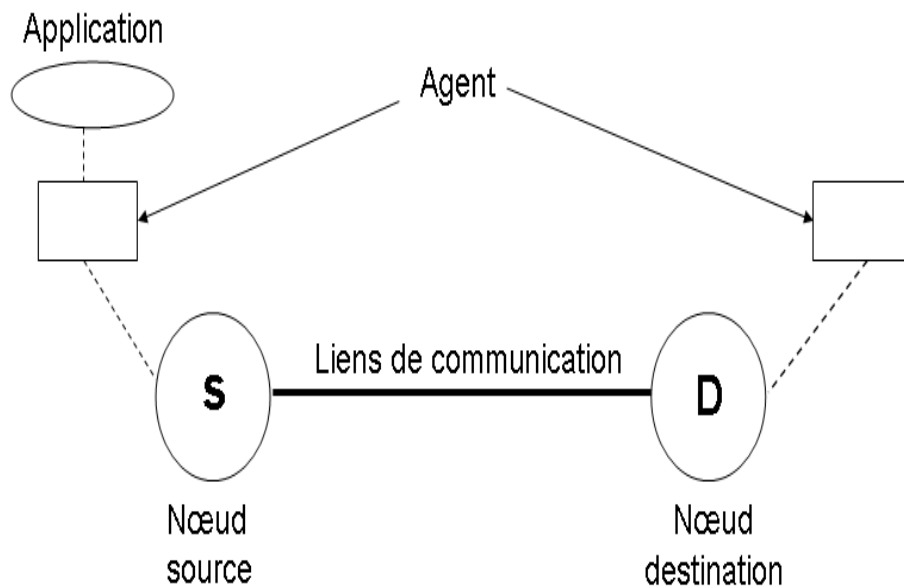


Figure III.2 : Composants d'un modèle de réseaux en NS.

III.2.5. Création d'un scénario :

Pour décrire un réseau et son trafic, il faut définir dans l'ordre :

1. la topologie du réseau : les nœuds et les liaisons.

2. la couche transport (UDP, TCP, ...) entre des pairs de nœuds.
3. la couche application qui va fournir les données.
4. des temporisateurs précisant les instants auxquels les transferts vont démarrer.

III.2.6. Les modules nécessaires pour la simulation :

Le Neighbor Discovery (ND), le module Media Independent Handover (MIH) et le module de gestion de mobilité (MIPv6) sont les éléments clés utilisés dans le code de simulation.

III.2.6.1. Module de découverte voisin :

Le module ND est utilisé pour fournir la détection de mouvement de la couche 3. Dans le réseau, la BS envoie périodiquement des messages RAs (Router Advertisement) pour informer les MR au sujet du préfixe de réseau. L'agent de ND situé dans le MR reçoit ces RAs et détermine si le message contient un nouveau préfixe et informe le directeur d'interface. Un temporisateur est associé au préfixe. Quand le préfixe est expiré, un avis est envoyé au directeur d'interface. L'implémentation supporte également RS (Router Solicitation) pour permettre à un MR de découvrir une nouvelle BS après un Handover.

III.2.6.2. Le service MIH (Media Independent Handover):

Afin d'assurer une continuité de service entre réseaux hétérogènes, IEEE a proposé IEEE802.21 qui définit le mécanisme du MIH permettant l'optimisation du handover entre différents réseaux de la famille IEEE802, 3GPP et 3GPP2.

Le groupe de travail IEEE 802.21 a pour cela créé une architecture de base qui définit une fonction MIHF « Media Independent Handover Function » qui va aider les systèmes mobiles à effectuer un handover sans couture entre des réseaux d'accès hétérogènes tels que IEEE 802.3 (réseau local filaire), IEEE 802.11x (réseau local sans fil), IEEE 802.16e (réseau WiMAX mobile), GPRS et UMTS (réseau mobile 3G).

III.2.6.2.1. Présentation du standard IEEE802.21 :

Le standard IEEE 802.21 [18] consiste en l'élaboration d'une architecture qui permet la continuité de service de manière transparente lorsque le routeur mobile (MR) passe entre deux réseaux hétérogènes au niveau liaison de données.

Un ensemble de fonctions permettant l'optimisation du Handover est défini dans la pile protocolaire de gestion de mobilité MME (Mobility Management Entity) des éléments du réseau et il y a une

création d'une nouvelle entité appelée MIHF (Media Independent Handover Function). Cela fonctionne sur la couche 3 et peut communiquer entre les interfaces locales et à distance. Les interfaces à distance peuvent être entrées en contact par l'intermédiaire d'un autre MIHF. Ceci est illustré sur la figure ci-dessous.

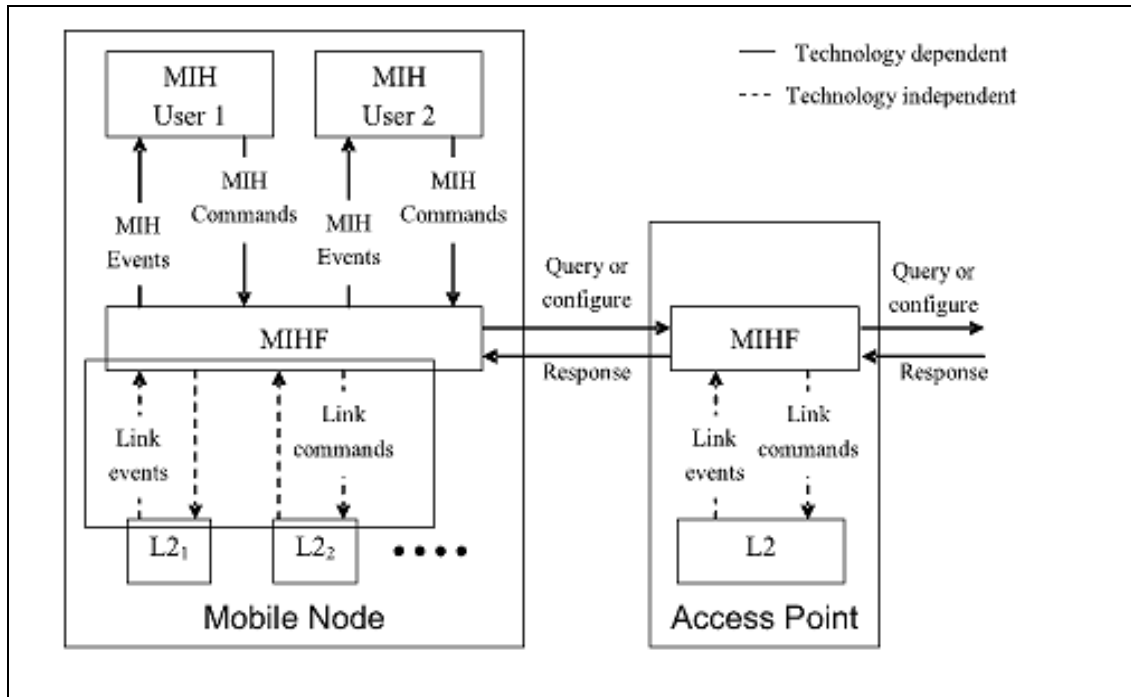


Figure III.3 : Vue d'ensemble de conception de MIHF.

III.2.6.3. La gestion de mobilité MIPv6 :

Le MIPv6 décrit un moyen de gérer la mobilité de terminaux IPv6. Cette mobilité permet qu'un terminal IPv6 soit toujours joignable quelle que soit sa localisation dans l'Internet et que ses connexions en cours restent actives malgré ses déplacements.

La figure ci-dessous comportant plusieurs acteurs :

- Le routeur mobile (MR) : est le terminal IPv6 pouvant se déplacer ;
- L'agent mère (Home Agent, HA) : est un équipement de réseau qui gère la mobilité à la manière d'un HLR dans les réseaux cellulaires ;
- Terminal correspondant (Correspondent Node, CN) : est un terminal IPv6 avec qui MR a ou aura une connexion active ;

On distingue deux types de réseaux sur lesquels MR peut venir se connecter :

Réseau mère : est le réseau d'origine de MR, ou il est adressable par son adresse mère (HA : Home adress).

Réseau visité : est le réseau où se déplace MR. Lors de son arrivée dans ce type de réseau, MR récupère grâce au mécanisme d'auto-configuration d'IPv6 [21] une adresse IPv6 topologiquement correcte appelée adresse temporaire (Care-of Address).

Le principe de base de Mobile IPv6 est que MR est toujours adressable par son adresse mère, qu'il soit sur son réseau mère ou sur un réseau visité.

Dans le cas où MR est dans son réseau mère, le routage des paquets s'effectue de manière standard, en se basant sur les tables des routeurs. MR n'est ni plus ni moins qu'un terminal IPv6 "fixe".

Dans le cas où MR effectue un mouvement pour aller sur un réseau visité **①**, celui-ci récupère une adresse temporaire sur ce réseau ; c'est-à-dire appartenant au préfixe utilisé sur ce lien du réseau. Il enregistre sa nouvelle position auprès de l'agent mère **②**, grâce à un message appelé Binding Update (BU) comportant à la fois son adresse mère et son adresse temporaire, et attend une confirmation de sa part **③** sous la forme d'un message appelé Binding Acknowledgment (BA). L'agent mère joue alors le rôle de proxy et intercepte tous les paquets à destination de l'adresse mère pour les orienter vers la nouvelle position de MR - c'est-à-dire son adresse temporaire « primaire ».

MR signale sa nouvelle position **④** aux correspondants avec lesquels il était en communication, toujours grâce aux messages BU et BA, afin d'optimiser les communications (les communications ne seront plus envoyées à l'adresse mère puis orientées par l'agent mère vers l'adresse temporaire "primaire", mais directement envoyées du correspondant vers le mobile).

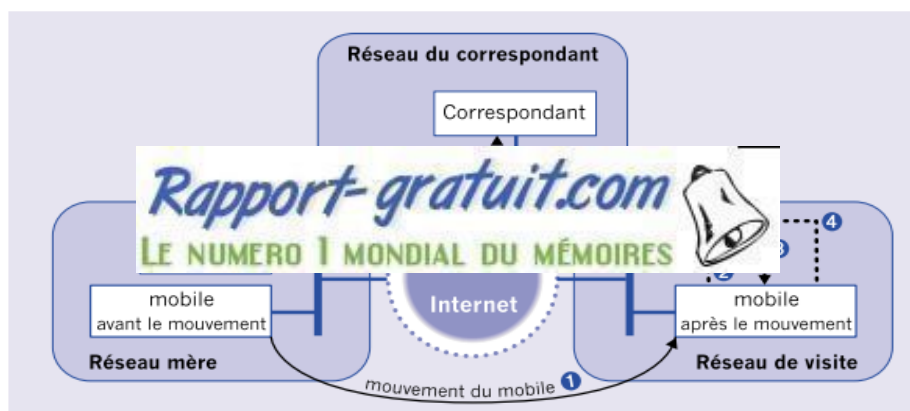


Figure III.4 : Mécanisme de base de mobilité IPv6.

La figure III.5 montre le déroulement de la connexion optimisée. Si un autre correspondant CN veut communiquer avec MR, il envoie son premier paquet à l'adresse mère de MR **①**, où le HA joue son rôle de proxy et transfère le paquet vers le MR **②**. Voyant arriver un paquet transféré, ce dernier peut choisir de signaler au correspondant sa position actuelle **③**, permettant ainsi une communication directe entre CN et MR **④**.

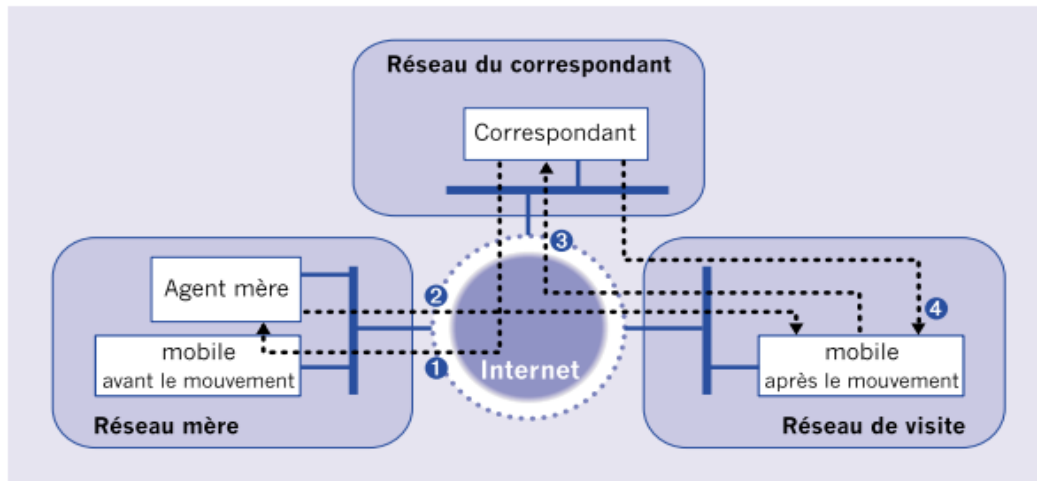


Figure III.5 : Optimisation du routage entre le correspondant et le mobile.

III.2.7. Paramétrage et configuration du réseau :

Avant de pouvoir utiliser le simulateur, la topologie du réseau et le besoin de chaque nœud doivent être décrits dans un fichier TCL qui sera ensuite lu par le simulateur.

Les paramètres et les configurations définies au niveau de ce fichier sont les suivants :

III.2.7.1. Les paramètres de simulation :

Paramètres	Signification
Temps de départ	0 le début de simulation
Trafic _ start	5 le début de trafic
Temps de mouvement	9 le début de mouvement
Trafic _ stop	70 la fin de trafic
simulation _ stop	70 la fin de simulation

Tableau III.1 : Les paramètres de simulation.

III.2.7.2. Les paramètres de réseau Wifi :

Paramètres	Signification
Channel/wirelessChannel	Type de canal : sans fils
Propagation/TwoRayGround	Modèle de propagation radio
Phy/wirelessPhy	Type d'interface du réseau

Mac/802_11	Type de couche MAC
Queue/DropTail/PriQueue	Type d'interface de la file d'attente
LL	Link layer type
Antenna/OmniAntenna	Modèle d'antenne
50	Taille maximale des files d'attente
Adhocrouting	Le protocole de routage utilisé . dans ce cas DSDV
50	La fréquence pour max paquets
5000	Dimension de x dans la topographie
5000	Dimension de y dans la topographie

Tableau III.2 : Les paramètres de réseau WiFi.

III.2.7.3. Configuration du point d'accès :

Paramètres	Signification
WiFi Coverage	potée de la station de base fixée à 20 m de rayon
Pt_	=0.025w : puissance du signal transmis de la station de base
freq_	=2412 e+6 : fréquence de 2.4GHz
RXThresh_	=1.12277e-10w: seuil de réception de puissance
CSThresh_	= [expr 0.9*[Phy/WirelessPhy set RXThresh_]] w:seuil de détection de porteuse

Tableau III.3 : Les paramètres du point d'accès WiFi.

III.2.7.4. Paramètres du réseau WiMAX :

Paramètres	Signification
Channel/WirelessChannel	type de canal : sans fils
Propagation/TwoRayGround	modèle de propagation radio : 802.16
Phy/WirelessPhy /OFDM	type d'interface du réseau : 802.16

Mac/802_16	type de couche MAC 802.16
Queue/DropTail/PriQueue	type d'interface de la file d'attente
LL	Link layer type 802.16
Antenna/OmniAntenna	modèle d'antenne
50	taille maximale des files d'attente
Adhocrouting	le protocole de routage utilisé. Dans ce cas DSDV

Tableau III.4 : Les paramètres du réseau WiMAX.

III.2.7.5. Configuration de la station de base (WiMAX1) :

Paramètres	Signification
Pt_	=0.25w : puissance du signal transmis de la station de base
RXThresh_	=1.26562e-13w : seuil de réception de puissance
CSThresh_	= [expr 0.9*[Phy/WirelessPhy set RXThresh_]] w : seuil de détection de porteuse

Tableau III.5 : Les paramètres de la station de base WiMAX1.

III.2.7.6. Configuration de la station de base (WiMAX2) :

Paramètres	Signification
Pt_	=0.025w : puissance du signal transmis de la station de base
RXThresh_	=1.26562e-13w : seuil de réception de puissance
CSThresh_	= [expr 0.8*[Phy/WirelessPhy set RXThresh_]] w : seuil de détection de porteuse

Tableau III.6 : Les paramètres de la station de base WiMAX2.

III.3. Simulations :

Les simulations sont conduites sous NS2 pour évaluer les performances et valider le support de mobilité proposé.

La topologie du réseau simulé sous NS2 est présentée à la figure III.6, où un adressage hiérarchique est adopté :

- Le nœud 0 : Un nœud (0.0.0) présentant CN d'interface filaire.
- Le nœud 1 : Un routeur (1.0.0) présentant quatre interfaces filaires.
- Le nœud 2 : Le nœud (2.0.1) présentant une interface externe de 802.11.
- Le nœud 3 : Une station de base IEEE 802.11 (routeur d'accès AR1 (2.0.0)).

- Le nœud 4 : Le routeur mobile MR (2.1.0) supportant plusieurs technologies (Multi-interface).
- Le nœud 5 : Le nœud MN1 (2.0.2) présentant un nœud mobile attaché au routeur mobile.
- Le nœud 6 : Le nœud MN2 (2.0.3) présentant un nœud mobile attaché au routeur mobile.
- Le nœud 7 : Une station de base IEEE 802.16 (routeur d'accès AR2 (3.0.0)).
- Le nœud 8 : Le nœud (3.0.1) présentant une interface externe de 802.16
- Le nœud 9 : Une station de base IEEE 802.161 (routeur d'accès AR3 (4.0.0)).
- Le router 10: Le nœud (4.0.1) présentant une interface externe de 802.16.

III.3.1. La topologie de réseau sous NS2 :

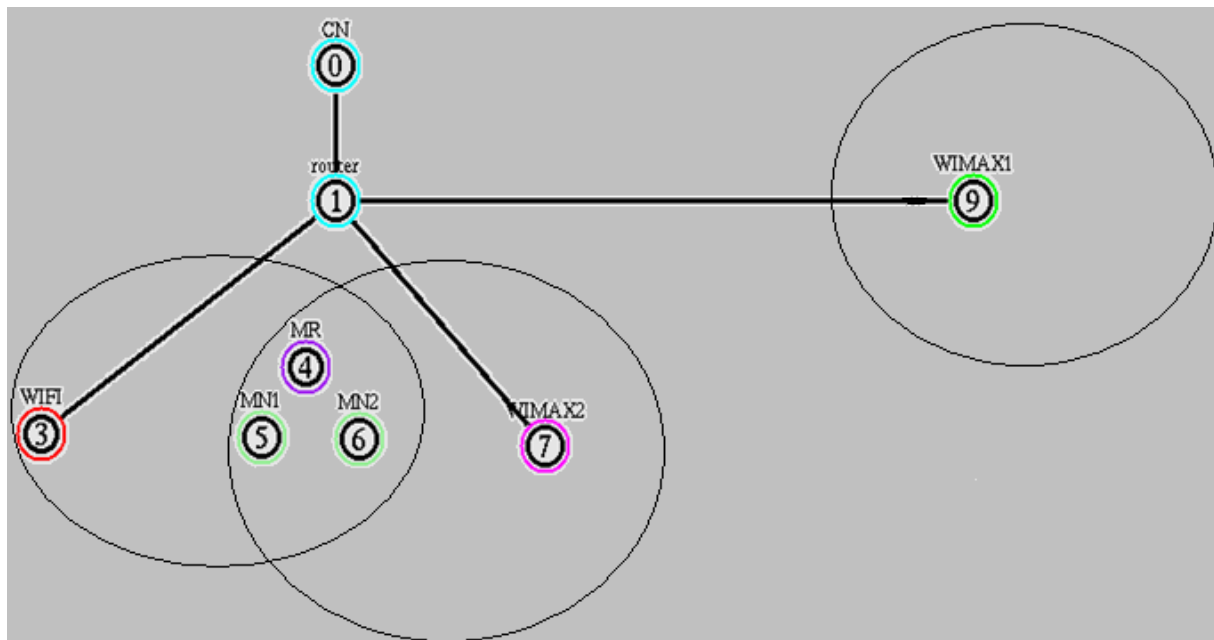


Figure III.6 : topologie de réseau NEMO.

Le scénario simulé consiste à véhiculer le trafic relatif à l'application entre le nœud CN (Correspondant Node) et le Routeur mobile (MR) avec lequel ils s'attachent les nœuds MN1 et MN2. Le MR se déplace linéairement du réseau WiMAX1 vers la région commune entre les réseaux WiMAX2 et WiFi avec une vitesse donnée (en Km/h) où il va choisir le meilleur réseau des deux à base de leurs qualités de service (voir figure III.6).

Nous allons présenter l'évolution du débit, le taux des paquets perdus et le délai de transmission des paquets en fonction du temps de la simulation pour différentes vitesses du routeur mobile. Ainsi, nous pouvons interpréter les résultats obtenus.

III.3.2. Débit :

La figure (III.7) illustre l'évolution du débit en fonction du temps de la simulation pour des différentes vitesses.

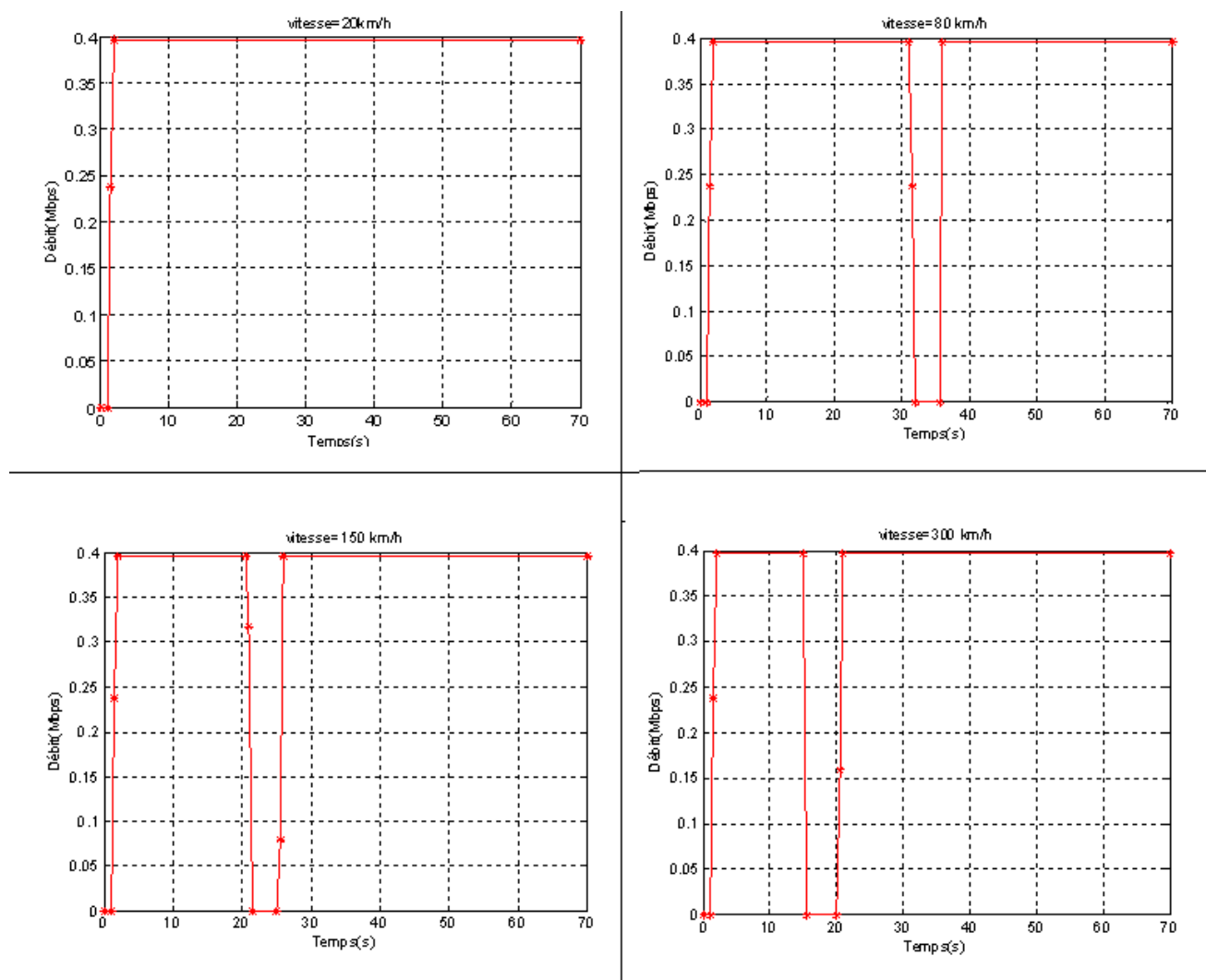
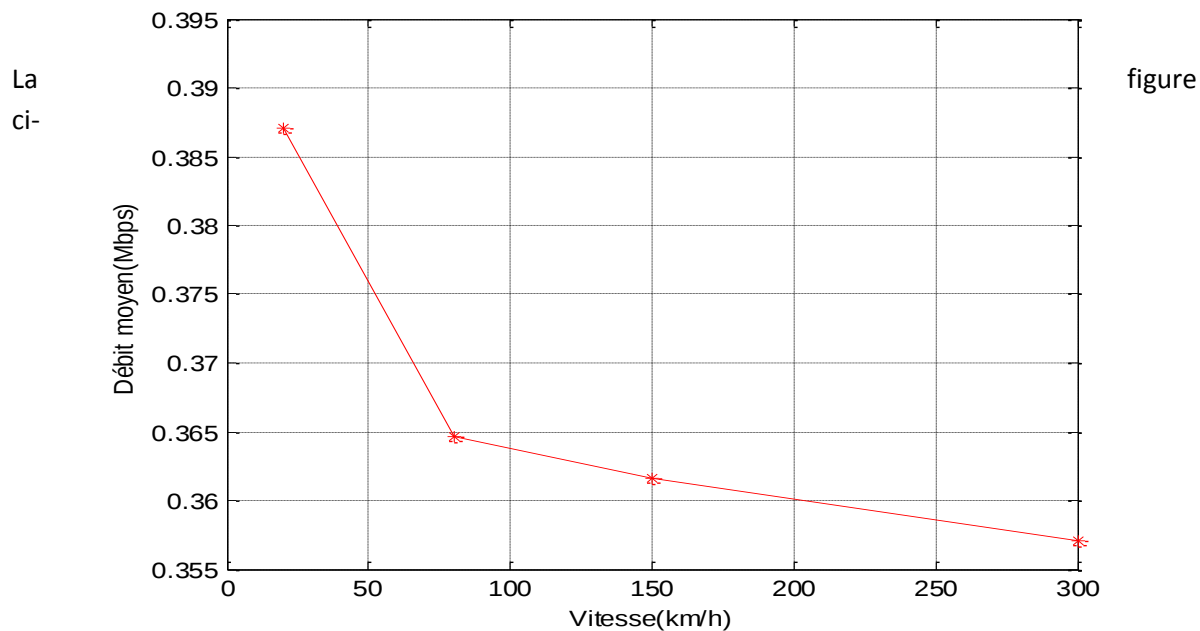


Figure III.7 : Evolution du débit en fonction du temps.

D'après cette figure, on déduit qu'avec une vitesse faible, le débit reste important (élevé).

Au moment du handover, on remarque que le débit chute considérablement car à ce moment, le mobile ne peut ni recevoir, ni émettre un trafic IP.



dessous illustre le débit moyen en fonction de la vitesse du routeur mobile.

Figure III.8 : Evolution du débit moyen en fonction de la vitesse.

A partir de cette figure, on peut déduire que le débit moyen diminue avec la vitesse ce qui correspond au taux des paquets perdus important.

III.3.3. Nombre des paquets perdus :

La figure III.9 montre l'évolution du nombre de paquets perdus en fonction du temps de la simulation pour des différentes vitesses.

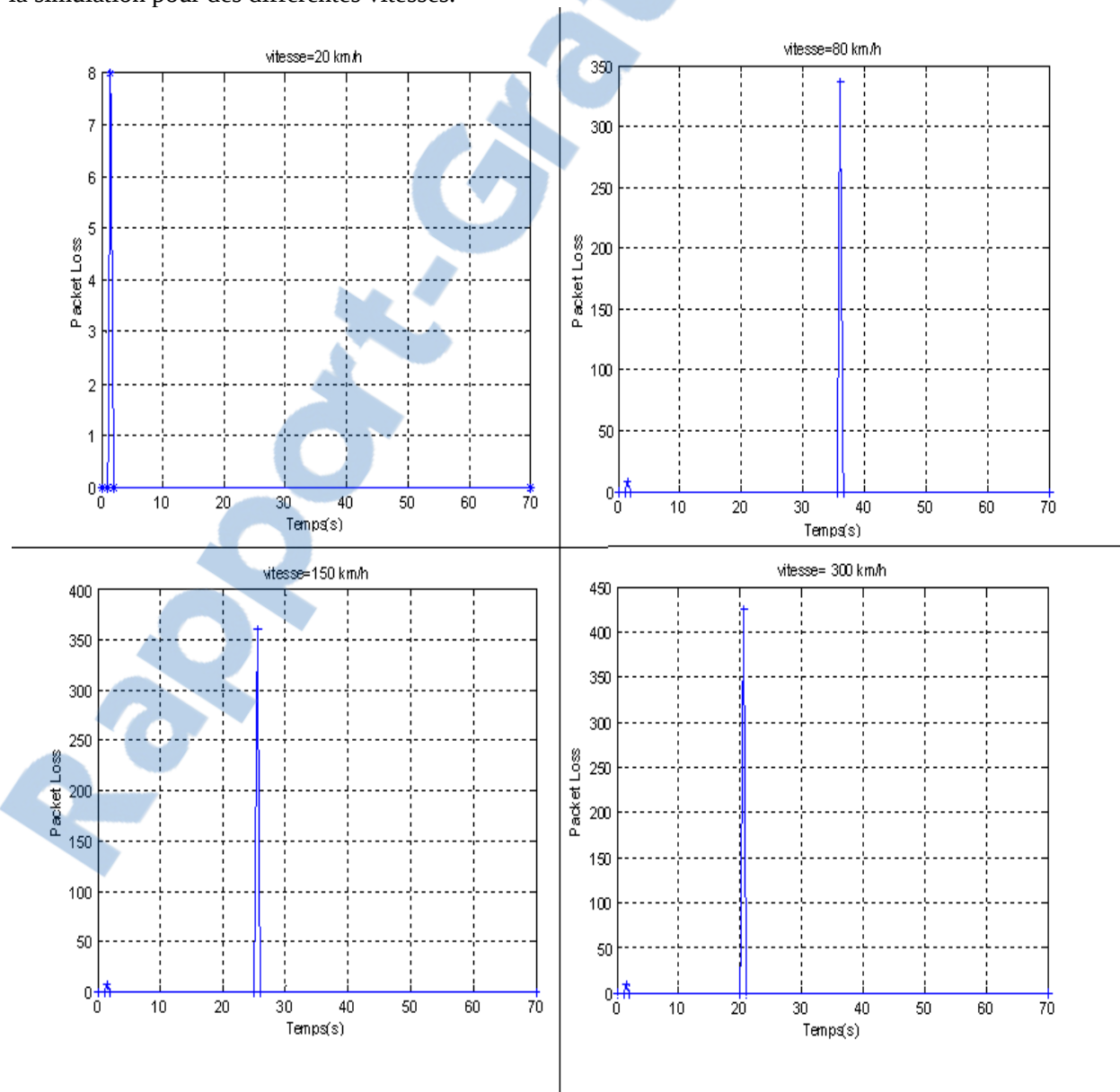


Figure III.9 : Evolution du nombre de paquets perdus en fonction du temps.

D'après cette figure nous déduisons que :

- Pour une faible mobilité, les performances du handover sont satisfaisantes. En effet, pour une vitesse de 20 Km/h, le nombre de paquets perdus est inférieur à 8. Par contre, pour une vitesse de 300 Km/h, il atteint une valeur de 425 paquets perdus, ce qui prouve que pour des vitesses élevées les performances du handover chutent considérablement.
- La variation du nombre de paquets perdus se comporte d'une façon similaire avant et après l'exécution du handover pour les deux réseaux.

La figure suivante représente la variation du taux des paquets perdus moyen en fonction de la vitesse du routeur mobile.

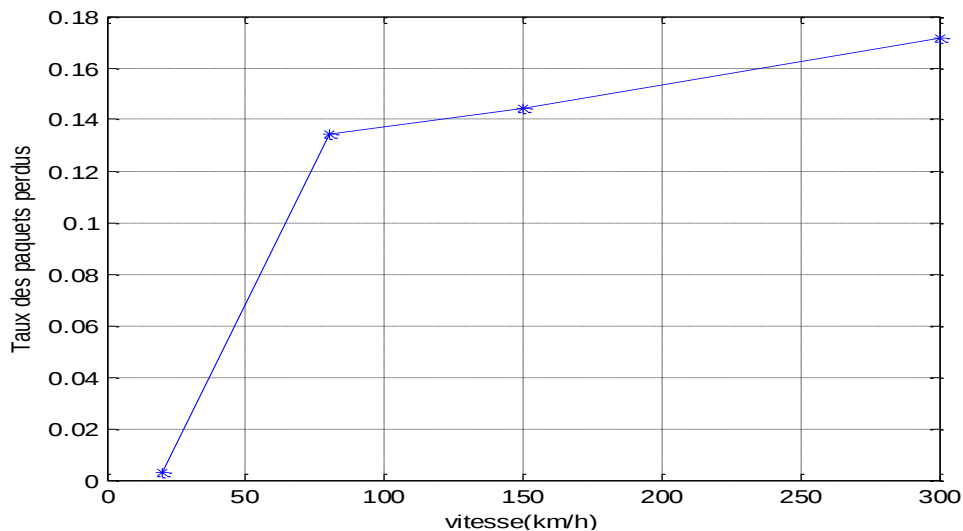


Figure III.10 : Taux de paquets perdus en fonction de la vitesse.

D'après cette figure, on remarque que le taux des paquets perdus augmente avec la vitesse. Donc, on peut dire qu'avec une forte mobilité, ce paramètre de performance est devenu important.

III.3.4. Délai de transmission :

La figure (III.11) illustre l'évolution du délai de transmission en fonction du temps de la simulation pour des différentes vitesses.

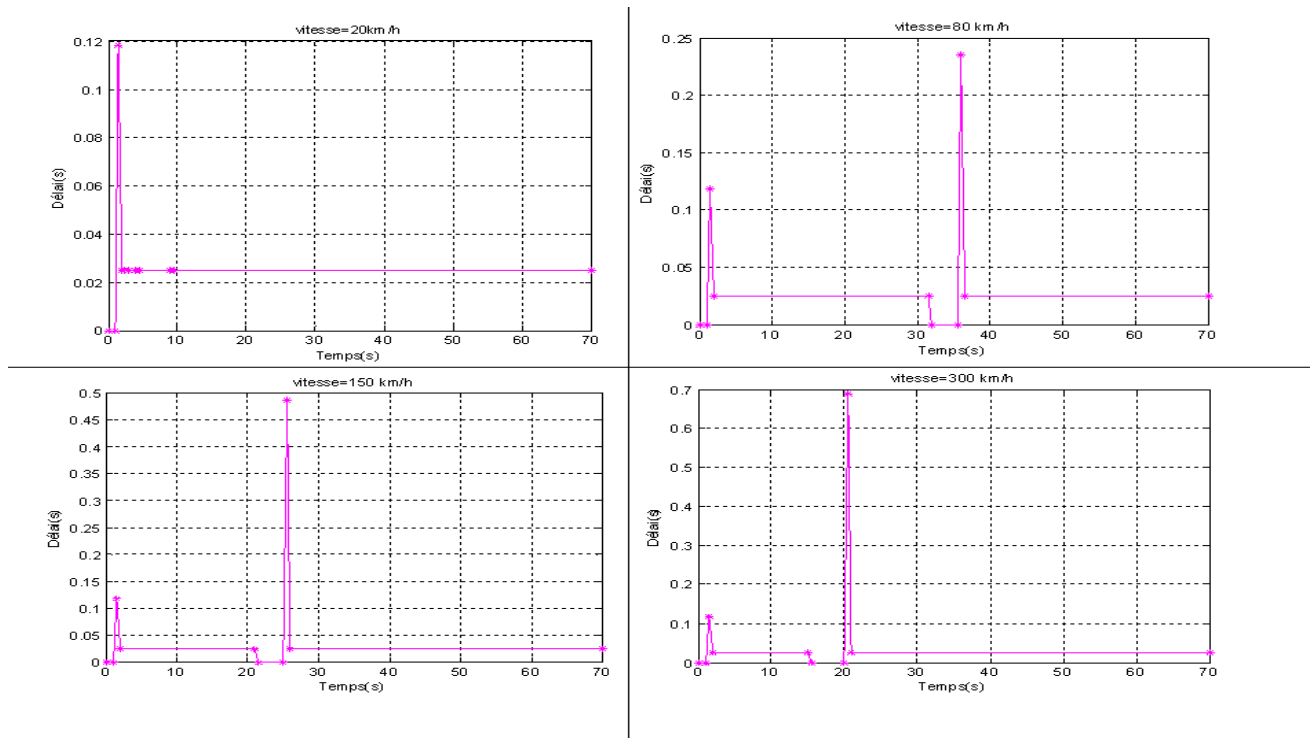


Figure III.11 : Evolution du délai de transmission du temps.

Cette figure montre :

- L'augmentation du délai implique que le lien radio se comporte mal, ainsi certains paquets vont être retransmis, d'où la nécessité du HO.
- Le délai de transmission des paquets augmente avec l'exécution du handover et légèrement avec la vitesse.

La figure ci-dessous illustre le délai moyen en fonction de la vitesse du routeur mobile.

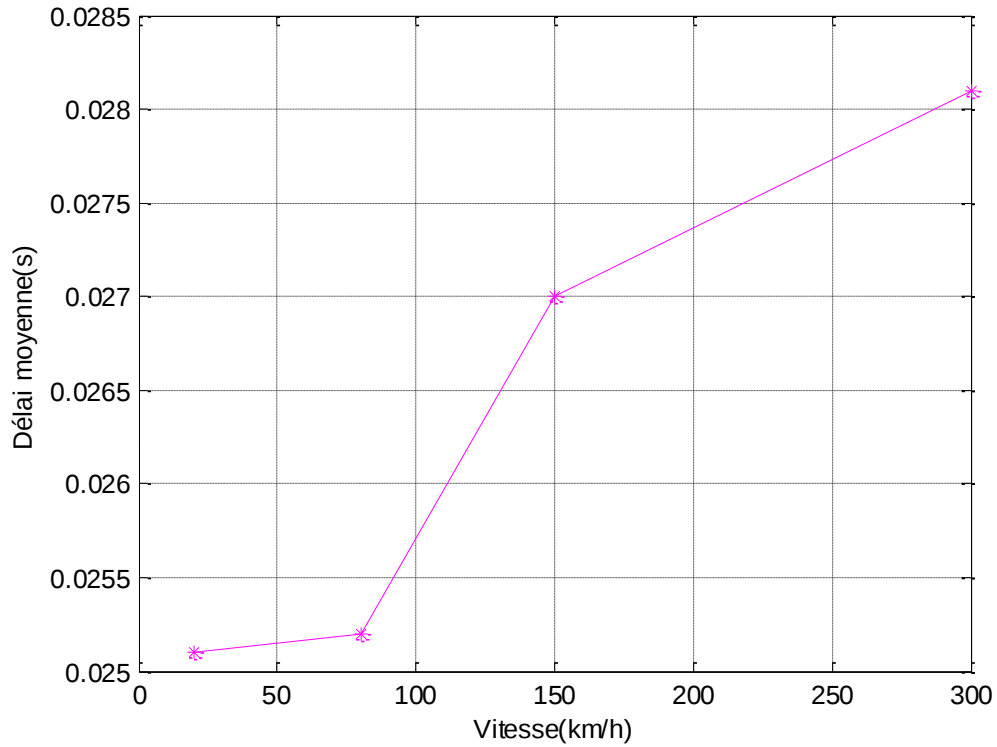


Figure III.12 : Le délai moyen en fonction de la vitesse.

D'après cette figure, on remarque que le délai moyen de transmission augmente avec la vitesse. Ce qui signifie qu'avec une forte mobilité, le lien radio se comporte mal, d'où la nécessité de retransmission de certains paquets.

III.4. Conclusion :

Dans ce chapitre, nous avons présenté tout d'abord, l'outil de simulation, nous avons décrit également les modifications rajoutées au simulateur pour le support des mécanismes de handover entre des réseaux hétérogènes. Ensuite, nous avons présenté notre modèle de simulation, paramétrer et configurer les nœuds nécessaires du réseau. Enfin, nous avons illustré le cadre de notre travail de simulation pour passer finalement à l'évaluation des performances du handover dans le réseau NEMO.

Conclusion générale

La problématique de notre projet d'étude se rapporte à la définition d'une architecture logicielle capable de faciliter la mobilité d'un réseau entier et de supporter le changement de leur point d'attachement entre les réseaux hétérogènes (le handover vertical).

Dans notre travail, nous avons présenté le principe de la mobilité des réseaux, leurs applications leur problématique et leur prise en charge dans IPv6.

La mobilité des réseaux a ouvert une brèche dans la gestion habituelle de la mobilité et mis à jour de nouveaux problèmes qui nécessiteront de plus amples travaux de recherche. En effet, le besoin de déplacer des réseaux est perçu depuis un certain temps, mais aucun travail significatif ne leur avait été consacré avant les premiers travaux introduits à l'IETF qui ont comblé ce manque. Les problèmes qui leurs sont propres n'ayant pas été abordés, donc suffisamment bien détaillés, les premières discussions à l'IETF ont eu pour résultat une certaine prise de conscience, assez faible dans un premier temps, mais grandissante depuis, dans les rangs de la communauté, qui a abouti avec la création du groupe de travail NEMO. Le support des réseaux mobiles est à présent un sujet qui intéresse de nombreux industriels, allant des fournisseurs d'équipement réseau ou d'électronique grand public jusqu'aux fabricants d'automobiles, en passant par les opérateurs de téléphone et de transport public.

Le support de la mobilité des réseaux permet de développer l'idée d'un Internet omniprésent, à tout instant, à tout endroit, avec n'importe qui. Les applications multimédia seront les premières à bénéficier de ce type d'environnement. En effet, la mobilité des réseaux rend en pratique possible la mobilité de tout équipement, ce qui implique aussi que toute application doit être en mesure de fonctionner dans un environnement mobile. Ceci nécessitera des mécanismes de changement d'interface et de routeur mobile, et la prise en considération d'un certain nombre de paramètres, en particulier le changement de qualité de service, de bande passante, de règles d'usage (pare-feu) en fonction des technologies accessibles à un instant donné et du réseau d'accès. La gestion de la mobilité des réseaux mobiles doit faire face à de nombreuses contraintes.

L'étude que nous venons de mener se caractérise essentiellement par l'utilisation d'un simulateur (logiciel NS-2) pour évaluer et analyser les performances du handover et la gestion de la mobilité d'un réseau entier en implémentant le module MIH (module développé par IEEE 802.21) et MIPv6 (module de la gestion de mobilité) au lieu d'utiliser le package Mobiwan réservé spécialement au réseau NEMO.

En perspective, nous conseillons d'interconnecter plusieurs réseaux hétérogènes et utiliser plusieurs routeurs mobiles (avec lesquels s'attachent d'autres terminaux) supportant ces différentes technologies afin d'étudier la gestion de la mobilité. On pourrait aussi illustrer l'effet de la charge des routeurs mobiles sur les performances du handover vertical entre ces différents réseaux.

Conclusion générale

La problématique de notre projet d'étude se rapporte à la définition d'une architecture logicielle capable de faciliter la mobilité d'un réseau entier et de supporter le changement de leur point d'attachement entre les réseaux hétérogènes (le handover vertical).

Dans notre travail, nous avons présenté le principe de la mobilité des réseaux, leurs applications leur problématique et leur prise en charge dans IPv6.

La mobilité des réseaux a ouvert une brèche dans la gestion habituelle de la mobilité et mis à jour de nouveaux problèmes qui nécessiteront de plus amples travaux de recherche. En effet, le besoin de déplacer des réseaux est perçu depuis un certain temps, mais aucun travail significatif ne leur avait été consacré avant les premiers travaux introduits à l'IETF qui ont comblé ce manque. Les problèmes qui leurs sont propres n'ayant pas été abordés, donc suffisamment bien détaillés, les premières discussions à l'IETF ont eu pour résultat une certaine prise de conscience, assez faible dans un premier temps, mais grandissante depuis, dans les rangs de la communauté, qui a abouti avec la création du groupe de travail NEMO. Le support des réseaux mobiles est à présent un sujet qui intéresse de nombreux industriels, allant des fournisseurs d'équipement réseau ou d'électronique grand public jusqu'aux fabricants d'automobiles, en passant par les opérateurs de téléphone et de transport public.

Le support de la mobilité des réseaux permet de développer l'idée d'un Internet omniprésent, à tout instant, à tout endroit, avec n'importe qui. Les applications multimédia seront les premières à bénéficier de ce type d'environnement. En effet, la mobilité des réseaux rend en pratique possible la mobilité de tout équipement, ce qui implique aussi que toute application doit être en mesure de fonctionner dans un environnement mobile. Ceci nécessitera des mécanismes de changement d'interface et de routeur mobile, et la prise en considération d'un certain nombre de paramètres, en particulier le changement de qualité de service, de bande passante, de règles d'usage (pare-feu) en fonction des technologies accessibles à un instant donné et du réseau d'accès. La gestion de la mobilité des réseaux mobiles doit faire face à de nombreuses contraintes.

L'étude que nous venons de mener se caractérise essentiellement par l'utilisation d'un simulateur (logiciel NS-2) pour évaluer et analyser les performances du handover et la gestion de la mobilité d'un réseau entier en implémentant le module MIH (module développé par IEEE 802.21) et MIPv6 (module de la gestion de mobilité) au lieu d'utiliser le package Mobiwan réservé spécialement au réseau NEMO.

En perspective, nous conseillons d'interconnecter plusieurs réseaux hétérogènes et utiliser plusieurs routeurs mobiles (avec lesquels s'attachent d'autres terminaux) supportant ces différentes technologies afin d'étudier la gestion de la mobilité. On pourrait aussi illustrer l'effet de la charge des routeurs mobiles sur les performances du handover vertical entre ces différents réseaux.

- [1] <http://livre.g6.asso.fr/index.php/Mobilit%C3%A9Bis>, 11 December 2009.
- [2] http://livre.g6.asso.fr/index.php/Support_de_la_Mobilit%C3%A9_des_R%C3%A9seaux, 2006.
- [3] Florent Kaisser, << Communications dans les réseaux fortement dynamiques>>, PDF, 2010.
- [4]] AIT SALEM Noureddine,<<NEMO La gestion de la mobilité des réseaux>>,PPT,2011.
- [5] Thierry Ernst, << Le support des réseaux mobiles dans IPv6>>, PDF, 2006.
- [6] Abdelmalek Slimane Zohra, << contribution à la modélisation des réseaux nemo>>, THESE DOCTORANT, 2012.
- [7] S. Kent, K. Seo, <<Security Architecture for the Internet Protocol>>, IETF RFC 4301, 2005.
- [8] W. Simpson, <<IP in IP Tunneling>>, IETF RFC 1853, October 1995.
- [9] Q.B Mussabbir, <<W. Yao. Optimized FMIPv6 using IEEE 802.21 MIH Services in Vehicular Networks. IEEE Transactions on Vehicular Technology. Special Issue on Vehicular Communications Networks >>, 2007.
- [10] Tarek BCHINI, <<Gestion de la Mobilité, de la Qualité de Service et Interconnexion de Réseaux Mobiles de Nouvelle Génération>>, PDF, 10/06/2010.
- [11] Addou Mohammed Adnana**Seladji Salim, <<Etude et modilisation du handover inter-système UMTS-WIMAX>>, MEMOIRE, juillet 2010.
- [12] Md. Shohrab Hossain**Mohammed Atiquzzaman, <<Performance Comparison between Multihomed Network Mobility Protocols >>, PDF, 2012.
- [13] Farouk Belghoul ** Yan Moret **Christian Bonnet, <<Mécanismes de handover pour les réseaux IP sans-fil>>, PDF ,2002

- [14] Babak Ayani, << Smooth Handoff in Mobile IP>>, PDF, 14/05/2002.
- [15] Khalid Eltayb Aldalaty, <<Mobile IP Handover Delay Reduction Using Seamless Handover Architecture>>, PDF, 2009.
- [16] Robert Hsieh** Zhe Guang Zhou**Aruna Seneviratne, <<S-MIP: A Seamless Handoff Architecture for Mobile IP>>, PDF, 2003.
- [17] badr benmammar, <<la gestion dynamique de la qualité de service dans les réseaux IP mobiles>>, PDF, 12/05/2006.

