Université Abou Bekr Belkaid
Tlemcen Algérie
جامعة أبي بكر بلقايد
تلمسان الجزائر
République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Laboratoire STIC

THESE

Présentée

A L'UNIVERSITE DE TLEMCEN
FACULTE DE TECHNOLOGIE

Pour l'obtention du diplôme de

DOCTORAT

Spécialité : " Télécommunications"

Par

Mme ABDELMALEK SLIMANE Zohra

CONTRIBUTION A LA MODELISATION DES RESEAUX NEMO

Soutenue en 2012 devant le Jury:

CHIKH Mohamed Amine.	Pr, Université de Tlemcen	Président
HAFFAF Hafid	Pr, Université d'Oran	Examinateur
KECHAR Bouabdellah.	MCA, Université d'Oran	Examinateur
FEHAM Mohammed	Pr, Université de Tlemcen	Directeur de Thèse

À mes parents, à mon mari et à mes filles.

Remerciements

Ce travail a été réalisé au laboratoire des Systèmes et Technologies de l'Information et de la Communication STIC de la faculté de technologie, université de Tlemcen. Cet environnement propice à la conduite de recherches amont m'a permis de m'impliquer pleinement sur un sujet passionnant et de bénéficier d'un encadrement et d'interlocuteurs dont les qualités scientifiques et pédagogiques sont pour beaucoup dans l'aboutissement de ce travail.

Je tiens tout d'abord à remercier le professeur Mohammed FEHAM directeur du laboratoire STIC de m'avoir accueilli au sein de l'équipe Réseaux et Services Associés RSA, et d'avoir dirigé mon travail. Son suivi régulier de l'évolution de mon travail, ses conseils et ses encouragements m'ont permis de réaliser ce mémoire dans d'excellentes conditions de travail.

Je suis particulièrement sensible à l'honneur que me font Messieurs les membres du jury en acceptant de lire et de juger ce mémoire. Je tiens à remercier tout particulièrement le professeur CHIKH Mohamed Amine d'avoir accepté de présider ce jury, ainsi que le professeur HAFFAF Hafid de l'Université d'Oran, et Monsieur KECHAR Bouabdellah Maitre de conférences de l'Université d'Oran. Je les remercie sincèrement pour le temps qu'ils ont consacré à la lecture, à l'évaluation de mon travail et à la rédaction des rapports d'expertise.

Mes remerciements s'adressent aussi à mon mari pour son soutien et pour la confiance qu'il m'a témoignée. Son enthousiasme, sa rigueur et sa passion pour la recherche, ont rendu nos nombreuses discussions scientifiques très enrichissantes.

Bien entendu, il me serait impossible de terminer sans adresser une pensée chaleureuse à mes parents pour leur soutien et leurs encouragements pendant de longues années, sans qui je n'aurais pu arriver à ce niveau d'études.

Résumé

La gestion de la mobilité des réseaux constitue aujourd'hui un véritable challenge dans l'Internet nouvelle génération. Avec la prolifération des terminaux mobiles et des réseaux d'accès sans fil tels que IEEE 802.11, IEEE 802.16, 3GPP et 3GPP2, on affiche un désir croissant 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, tramway, métro, train, bus,…) sont un environnement typique. Le protocole NEMO Support Basic (BS) est l'une des quelques solutions qui ont été largement acceptées dans le monde académique et l'industrie pour supporter la mobilité d'un réseau mobile. Cependant, la performance du handover du protocole NEMO BS avec les améliorations existantes n'est toujours pas suffisante pour les besoins des applications temps réel et exigeantes en QoS, d'autres optimisations sont donc nécessaires. Dans cette thèse, nous proposons deux nouvelles approches de handover NEMO indépendantes de l'infrastructure, combinant le multihoming et le handover Make-Before-Break intelligent, assurant ainsi une connectivité sans couture avec zéro délai et zéro perte. Pour les deux solutions, nous nous basons sur l'appui des services MIH IEEE 802.21. Dans la première approche, nous proposons une nouvelle architecture d'un réseau NEMO multihomed avec plusieurs MRs domiciliés dans différents HAs. Cette architecture est basée sur l'introduction de la notion de routeur primaire et routeur secondaire, et l'intégration d'une nouvelle entité nommée MNPx (Mobile Network Proxy) au sein du réseau mobile, dont la tâche principale est la gestion intelligente de la mobilité et du trafic d'une manière transparente pour les MNNs. Dans la deuxième approche, nous avons adressé le cas du modèle NEMO multihomed (1.1.1) où un seul MR multi-interfaces est employé. Basé sur l'estimation du délai du handover requis, les handovers L2 et L3 sont lancés en utilisant des triggers MIH efficaces et opportuns, réduisant ainsi le temps d'anticipation et augmentant la probabilité de prédiction. Nous avons étendu les services de MIH pour fournir l'établissement et la commutation de tunnel avant la rupture du lien courant. Ainsi, le handover est exécuté dans le background sans latence et sans perte de paquet tandis que le scénario de ping-pong est évité, et le coût et la consommation d'énergie sont minimisés. Des expériences de simulation sous le simulateur de réseau NS2 ont été conduites pour identifier les valeurs appropriées des paramètres des modèles validant nos propositions.

Mots clés : *réseau mobile, NEMO, Multihoming, routeur mobile, Handover sans couture, IEEE 802.21, MIH triggers, modèle de propagation, NS, PHD, MTM, MNPx*

Abstract

Network mobility management constitutes today a true challenge for the Internet next generation. With the proliferation of mobile devices, and wireless access network such as IEEE 802.11, IEEE 802.16, 3GPP and 3GPP2, one posts an increasing desire on behalf of the users to be profited from ubiquitous Internet access, i-e without discontinuity anywhere at any time during their displacements, so that we have whole networks made up of mobile devices moving together and wishing this quality of service. Public transportation systems (plane, boat, TGV, tram, subway, train, bus …) are typical environments. NEMO Basic Support (BS) protocol is one of the few solutions that have been widely accepted in the academic world and the industry for supporting the mobility of moving network. However, Handoff performance of NEMO BS protocol with existent improvement proposals is still not sufficient for real time and QoS-sensitive applications and further optimizations are needed. In this thesis, we propose two new Infrastructure independent NEMO handoff approaches combining multihoming and intelligent Make-Before-Break Handoff achieving seamless connectivity with no handoff latency and no handoff packet loss. For both solutions, we rely on the support of MIH IEEE 802.21 services. In the first approach, we propose a new architecture of a multihomed NEMO network with several MRs domiciled in different HAs. This architecture is based on the introduction of the concept of primary and secondary routers, and the integration of a new entity named MNPx (Mobile Network Proxy) within the mobile network, whose principal task is the intelligent management of mobility and traffic transparently for MNNs. In the second approach, we addressed the case of multihomed NEMO model (1,1,1) where a single multi-interfaces MR is used. Based on required Handoff time estimation, L2 and L3 handoffs are initiated using effective and timely MIH triggers, reducing so the anticipation time and increasing the probability of prediction. We extended MIH services to provide tunnel establishment and switching before link break. Thus, the handoff is performed in background with no latency and no packet loss while ping-pong scenario is almost avoided and cost and power consumption are saved. We provide implementation and simulation experiments under Network Simulator NS2 to identify appropriate model parameter values validating our proposals.

Keywords : *Network mobility, NEMO, Multihoming, Mobile Router, seamless handoff, IEEE 802.21, MIH triggers, path loss model, NS, PHD, MTM, MNPx*

Table des matières

CHAPITRE II

Analyse du Handover du protocole NEMO Support Basique et ses Extensions

CHAPITRE III

Le Multihoming dans les Réseaux NEMO Standard IEEE 802.21

CHAPITRE IV

Handover sans Coutures basé sur le Modèle NEMO Multihomed (n,n,1)

CHAPITRE V

Handover Sans Coutures basé sur le Modèle NEMO multihomed (1,1,1)

Liste des figures

Figures **page**

Figures **page**

Figures **page**

Liste des tableaux

Acronymes

3GPP	3rd Generation Partnership Project
3GPP2	3rd Generation Partnership Project 2
ACK	Acknowledgment
AP	Access Point
AR	Access router
BAck	Binding Acknowledgement
BER	Bit Error Rate
BID	Binding Identification Number
BU	Binding Update
CBR	Continuous Bit Rate
CN	Correspondent Node
CoA	Care of Address
CoT	Care-of Test
CoTI	Care-of Test Initiate
DAD	Duplicate Address Detection
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol for IPv6
EDC	Environment Detector Component
EIF	Egress Interface
FA	Foreign Agent
Fast RA	Fast Router Advertisement
FBack	Fast Binding Acknowledgement
FBU	Fast Binding Update
FHMIPv6	Fast Hierarchical Mobile IPv6
FMIPv6	Fast Mobile IPv6
FNA	Fast Neighbor Advertisement
GPS	Global Positionning System
HA	Home Agent
HAck	Handover Acknowledge
HI	Handover Initiate
HiMIP-NEMO	Hierarchical backhaul packet forwarding architecture
HIP	Host Identity Protocol
HMIPv6	Hierarchical Mobile IPv6
HNI	Heterogeneous Network Information
HoA	Home Address
HoT	Home Test
HoTI	Home Test Initiate

HPD	Handover Policy Decision
ICE	Intelligent Control Entity
ICMP	Internet Control Message Protocol
IE	Information Element
IEEE	Institute of Electrical and Electronics Enginneers
IETF	Internet Engineering Task Force
IF	Interface
IIF	Ingress Interface
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	IP security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IS	Information Server
L2	Layer 2
L3	Layer 3
LBA	Local Binding Acknowledgement
LBU	Local Binding Update
LCoA	Local CoA
LD	Link_Down
LFN	Local Fixed Node
LGD	Link_Going_Down
LMA	Local Mobility Anchor
LMAA	LMA Address
LMN	Local Mobile Node
LSI	Link_switch_Imminent
MAC	Media Access Control
MAG	Mobile Access Gateway
MAP	Mobility Anchor Point
MCoA	Multiples Care of Addresses
MICS	Media Independent command Service
MIES	Media Independent Event Service
MIH	Media Independent Handover
MIHF	Media Independent Handover Function
MIIS	Media Independent Information Service
MIPv4	Mobile IPv4
MIPv6	Mobile IPv6
MMRCFH	Multiple Mobile Router Cooperation Fast Handover
MN	Mobile Node
MN-HNP	Mobile Node's Home Network Prefix
MN-HoA	Mobile Node's Home Address
MN-Id	Mobile Node Identifier
MNN	Mobile Network Node
MNP	Mobile Network Prefix
MNPx	Mobile Network Proxy
MR	Mobile Router
mSCTP	mobile Stream Control Transmission Protocol
MTM	Mobility and Trafic Management

NA	Neighbour Advertisement
NAP	Next Access Point
NAR	Next Access Router
NCoA	Next Care-of Address
NEMO	Network Mobility
NEMO BS	NEMO Basic Support
NEMO-WG	NEMO Working Group
NIST	National Institute of Standards and Technology
NS	Neighbour Solicitation
NS2	Network Simulator 2
NUD	Neighbor Unreachability Detection
ODAD	Optimistic Duplicate Address Detection
OSI	Open System Interconnection
PAD	Padding
PAN	Personal Area Network
PAR	Previous Access Router
PBA	Proxy Binding Acknowledgement
PBU	Proxy Binding Update
PCoA	Previous Care of Address
PDC	Policy Decision Component
PDU	Packet Data Unit
PHY	Physical Media
PMIPv6	Proxy Mobile IPv6
PoA	Point of Attachment
Proxy-CoA	Proxy Care-of Address
PrRtAdv	Proxy Router Advertisement
QoS	Quality of Service
RA	Router Advertisement
RCoA	Regional CoA
RFC	Request for Comment
RO	Route Optimization
RS	Router Solicitation
RSS	Received Signal Strength
RSSI	Received Signal Strength Indicator
RtSolPr	Router Solicitation for Proxy Advertisement
RTT	Round Trip Time
SA	Security Association
SINEMO	Seamless IP diversity based NEtwork MObility
SIP	Session Initiation Protocol
TCP	Transport Control Protocol
UDP	User Data Protocol

Introduction générale

Contexte

Les possibilités de se connecter à l'Internet aujourd'hui se multiplient avec le déploiement à grande échelle de réseaux d'accès sans fil variés (e.g WiFi, WiMAx, UMTS, LTE, LTE-Advanced…). Cet environnement de réseaux hétérogènes et chevauchés offre un accès Internet omniprésent. Avec la prolifération des produits sans fils et des services réseaux mobiles, on affiche un désir croissant de la part des usagers à bénéficier d'un accès Internet sans discontinuité de leurs applications réseaux habituelles 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 (socket TCP) et de localisation dans la topologie Internet, ne permet pas une connectivité sans interruption des services. Lors de son changement de réseau d'accès, 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.

Nous distinguons deux types de mobilité de point de vue de l'entité mobile : la mobilité d'un terminal et la mobilité d'un réseau entier.

Pour le premier cas, plusieurs solutions de gestion de la mobilité ont été développées à différents niveaux du modèle OSI (SIP, HIP, TCP-Migrate, mSCTP, MIPv6, PMIPv6, …). Cependant, seules les

solutions au niveau de la couche réseau L3 (MIPv6, FMIPv6, HMIPv6, PMIPv6, …) permettent de gérer la mobilité d'une façon transparente pour les applications et pour les technologies sous-jacentes. Dans les différentes architectures proposées, les décisions de gestion de la mobilité sont soit laissées à la discrétion du terminal mobile, soit prises par le réseau d'accès.

Pour le second cas, le problème de la gestion de la mobilité au niveau de la couche L3 peut être résolu en utilisant les protocoles développés au sein de l'IETF dans le contexte d'IPv6 pour le cas d'un terminal mobile (e.g MIPv6), ceci exigerait d'une part que chaque dispositif soit capable du protocole MIPv6, et d'autre part que chaque dispositif exécute les fonctionnalités du protocole MIPv6 conduisant ainsi à une surcharge de trafic. Une autre solution basée sur l'extension de MIPv6 a été proposé récemment par le groupe de travail NEMO WG de l'IETF sous le nom de NEMO Basic Support Protocol (NEMO BS). Dans l'architecture de NEMO, le réseau mobile est contrôlé par un routeur mobile dont la principale tâche est la gestion de la mobilité d'une manière transparente pour les équipements embarqués dans le réseau mobile. Plusieurs déploiements de NEMO BS sont réalisés au sein de grands projets publics ou par des industriels tels que: ICAR, Nautilus6, DAIDALOS, OVERDRIVE, eMOTION, etc.

En dehors des travaux de l'IETF, d'autres solutions sont proposées également (SINEMO, HiMIP-NEMO, SIP-NEMO, HIP-NEMO).
Le travail de cette thèse se limite au protocole NEMO BS, dont plusieurs issues sont encore ouvertes à la recherche, nous citons les problèmes d'optimisation du routage, de la sécurité, de la multi-domiciliation et des performances du handover.

Problématique

Les performances du handover à travers les réseaux hétérogènes jouent un rôle crucial pour les applications sensibles au QoS et les services temps réel. Bien que le protocole NEMO BS ait le mérite de permettre dès aujourd'hui le déploiement et l'expérimentation de services sans contraintes temporelles, sans que ceux-ci n'aient à fonctionner dans un mode dégradé, ses performances (latence élevée, perte de paquet élevée et le coût de signalisation important) sont clairement non optimales et par conséquent il est considéré non approprié pour des applications à contraintes de temps.
Plusieurs architectures et mécanismes ont été proposés pour optimiser les performances du handover de NEMO BS. Cependant, ces optimisations restent insuffisantes pour répondre aux besoins des applications à performance critique. Nous admettons que pour le cas d'un réseau mobile géré par un seul routeur mobile, il existerait toujours une limite inférieure pour le délai du handover qui dans le meilleur des cas, sera réduit au temps d'interruption dû à la réassociation au niveau liaison (L2).
Une approche multihoming peut résoudre le problème. Les solutions proposées dans ce contexte souffrent de plusieurs limitations. D'une part, elles sont dépendantes soit de l'infrastructure réseau soit

de l'application NEMO déployée. D'autre part, les performances réalisées sont assujetties à certains paramètres de l'environnement.
Dans le travail de cette thèse, nous adressons le problème des performances du handover NEMO en proposant deux solutions indépendantes de l'infrastructure basées sur l'approche multihoming et s'appuyant sur les services MIH du standard IEEE 802.21.

Contributions

Les travaux que nous avons réalisés au cours de cette thèse ont fait l'objet des publications suivantes :

- Z. Slimane, M. Feham and A. Abdelmalek. A Seamless and Transparent MN-Proxy based Mobility Support For (n,n,1) Multihomed NEMO Model. International Journal of Computer Science and Network Security, Vol.10, No.4, PP.306–313, April 2010.

- Z. Slimane, M. Feham and A. Abdelmalek. Seamless Infrastructure independent MultiHomed NEMO Handoff Using Effective and Timely IEEE 802.21 MIH triggers. To appear in International Journal of Wireless and Mobile Networks (IJWMN), Vol.4, No.3, 2012.

Organisation de la thèse

La suite de ce manuscrit est organisée de la façon suivante :

Le premier chapitre présentera un état de l'art des différentes solutions proposées pour la gestion de la mobilité dans les deux cadres d'un terminal mobile et d'un réseau mobile. Nous nous focaliserons en particulier sur la mobilité des réseaux NEMO, leurs usages et leurs issues.

Le second chapitre présentera une étude analytique des différents composants du handover NEMO BS, mettant en évidence les limites de ses performances. Nous survolerons ensuite quelques propositions d'extensions du protocole NEMO BS ayant trait en particulier à l'optimisation du handover.

Le troisième chapitre est divisé en deux parties, la première est consacrée aux différents aspects de la multi-domiciliation (multihoming) dans les réseaux NEMO, leurs bénéfices et leurs issues. La seconde partie introduira le standard IEEE 802.21 dont les spécifications ont pour objectif d'assister et de faciliter le handover dans un environnement hétérogène.

Le quatrième chapitre présentera en détails notre première proposition de gestion de la mobilité d'un réseau NEMO multihomed dans le cas où plusieurs routeurs mobiles sont déployés. Une approche proactive consistant à exécuter des handovers soft (Make Before Brake) est adoptée, conduisant à la disponibilité de plusieurs tunnels simultanément qui seront utilisés suivant les besoins de gestion de la

mobilité ou du trafic. Une évaluation des performances sous NS2 permettant de valider le modèle proposé est prévue à la fin du chapitre.

Le cinquième chapitre décrit notre seconde proposition de gestion de la mobilité d'un réseau NEMO multihomed dans le cas où un seul routeur mobile multi-interfaces est déployé. Cette approche repose sur deux mécanismes : (i) la préparation du handover, (ii) et l'anticipation du handover avant la rupture du lien. Cette solution garantit une connectivité sans couture avec économie de coût et d'énergie. Des tests et des résultats de simulation sous NS2 seront présentés pour l'identification des valeurs appropriées des paramètres utilisés permettant de valider le modèle proposé.

Enfin, en conclusion générale de cette thèse, nous rappellerons les principales contributions réalisées au cours de nos travaux et énoncerons leurs principales perspectives.

CHAPITRE 1

Supports de Mobilité dans les Réseaux IP

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 [1]-[4], 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 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. Des recherches ont été menées également dans ce sens.

Le problème de la mobilité peut se décomposer en deux sous-problèmes distincts:

- La localisation (ou joignabilité) : l'équipement mobile doit avoir une adresse qui lui permet d'être joignable quelque soit sa localisation dans la topologie Internet.

- La continuité des services en cours de déplacement : lors de changement de réseaux d'accès, les sessions ouvertes doivent être maintenues d'une manière transparente pour les utilisateurs mobiles.

Deux alternatives sont possibles pour résoudre les problèmes introduits par la mobilité. La première d'entre-elles consiste à ne rien changer au niveau de la couche IP et à laisser les couches supérieures gérer le problème. La seconde consiste à modifier les principes de l'adressage. Des propositions existent pour définir deux espaces d'adressage. Le premier serait dédié à la localisation et le second à l'identification.

Dans la suite de ce chapitre, nous présenterons le problème de dualité de l'adressage IP, les types de mobilité et les solutions existantes de la gestion de la mobilité. Nous détaillerons en particulier, les protocoles liés à la couche réseau aussi pour un terminal mobile que pour un réseau entier en déplacement.

II.2 Dualité d'Identification / Localisation de l'adresse IP

Lors de son changement de réseau d'accès, un nœud mobile change de point d'attachement (le routeur d'accès), son adresse IP change également, il n'est plus joignable par ses correspondants et ses sessions actives sont interrompues. Ce problème lié à la localisation des nœuds mobiles dans le réseau Internet reste difficile à résoudre à cause de la dualité des fonctions d'une adresse IP à savoir l'identification et la localisation. Une adresse IP identifie de manière unique un nœud sur le réseau Internet [5,8]. Elle permet aussi de localiser ce 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. Malheureusement son identification change aussi ce qui pose des problèmes aux couches supérieures. En effet, le protocole TCP [6] utilise les paramètres suivants pour identifier une connexion : l'adresse IP source, l'adresse IP destination, le port source et le port destination. Lorsqu'un de ces éléments change, il ne s'agit plus pour lui de la même session et les communications en cours sont interrompues. Un des objectifs de la gestion de la mobilité serait la séparation de l'identité de la machine et de sa localisation.

II.3 Types de mobilité et de Handovers

Le terme de mobilité Internet peut être défini comme la capacité d'accéder tout en se déplaçant et quelle que soit la localisation à l'ensemble des services Internet. Nous distinguons deux types de mobilité de point de vue de l'entité mobile :

- Mobilité de station (terminal) : concerne tout simplement le déplacement dans la topologie

Internet d'un équipement de type ordinateur, PDA, SmartPhone, Laptop, etc. Ces entités sont généralement appelées nœuds mobiles (ou Mobile Nodes, MNs).

- Mobilité de réseau : la notion de mobilité peut s'étendre aux réseaux eux-mêmes. La mobilité de réseau désigne alors le déplacement d'un réseau tout entier dans lequel sont déployés des équipements capables de communiquer à travers internet, à titre d'exemple nous citons le cas des systèmes de transport en commun où les passagers désirent bénéficier d'un accès Internet.

Par ailleurs, 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 :

- Link-Mobilité (ou mobilité intra-lien) : désigne une mobilité entre deux points d'accès sans fil d'un même réseau d'accès. Aucune reconfiguration d'adresse IP n'est nécessaire (handover L2).

- Micro-mobilité (ou mobilité locale) : désigne une mobilité à l'intérieur d'un même réseau d'accès mais qui implique des mécanismes de changement d'adresse IP (handover L3). La gestion de la mobilité est locale.

- Macro-mobilité (ou mobilité globale) : désigne une mobilité entre différents réseaux d'accès impliquant une reconfiguration d'adresse IP (handover L3), sans tenir compte du type de technologie.

La gestion de la mobilité fait intervenir des mécanismes de handovers. Le handover se produit lorsqu'un nœud mobile (MN) désire changer son point d'attachement au réseau Internet (changement de cellule). Le handover peut être donc défini comme étant le processus de changement de point d'attachement. Nous avons deux grandes catégories de handover suivant qu'il se déroule au niveau liaison (handover L2) ou au niveau réseau (handover L3), dont plusieurs types sont possibles :

- Hard Handover : désigne un handover qui arrive suite à la perte du lien d'accès avec le réseau d'accès (Break-Before-Make). Ce type de handover a un impact très fort sur les applications (les sessions ouvertes seront interrompues).

- Soft Handover : Dans ce cas, le mobile est multi-domicilié, c'est-à-dire admettant deux ou plusieurs interfaces par les quelles il est capable de communiquer simultanément avec plusieurs points d'attachements, ce qui lui permet d'exécuter un handover avec l'une de ses interfaces sans interrompre les communications sur l'interface active (Make-Before-Break).

- Smooth Handover : désigne un handover sans pertes.

- Handover sans coutures ou Seamless handover : dans ce cas, le handover est sans effet sur l'application (un minimum de délai de handover et de pertes sont exigés pour réponde aux besoins de l'application).

II.4 Solutions de la gestion de la mobilité

Plusieurs solutions pour la gestion de la mobilité dans Internet ont été proposées à différents niveaux du modèle OSI [9]-[18]. Les solutions qui gèrent la mobilité au niveau L3+ (c'est-à-dire au-dessus du niveau IP) ont l'avantage de ne modifier que les extrémités impliquées dans une connexion, indépendamment de l'infrastructure IP qui reste inchangée, elles permettent d'éviter le passage par un routage triangulaire et fonctionnent aussi bien avec IPv4 [5] ou IPv6 [8]. Au niveau L3,5 entre la couche réseau et la couche transport, l'architecture HIP (Host Identity Protocol) [16] propose la mise en place d'une couche intermédiaire permettant de séparer l'identification et la localisation d'un nœud mobile. Malheureusement, la mise en place d'une telle solution nécessiterait des changements importants au niveau des systèmes d'exploitation et des modifications au niveau de chaque application utilisant Internet.
Au niveau transport, la plupart des solutions concernent le protocole TCP, nous citons à titre exemple TCP-Migrate [17] et mSCTP (mobile Stream Control Transmission Protocol) [18]. L'inconvénient de ces solutions est qu'elles permettent seulement de gérer le maintien des communications qui utilisent effectivement le protocole associé à la solution. Au niveau application, le protocole SIP (Session Initiation Protocol) [19] est proposé pour gérer la mobilité. Une des fonctionnalités de base de SIP est de pouvoir gérer la localisation de ses utilisateurs. Cependant, tout comme les solutions de mobilité de niveau transport, la mobilité basée sur SIP permet seulement de gérer la mobilité des applications contrôlées par SIP lui-même.

Contrairement aux couches supérieures, la position de la couche réseau dans le modèle OSI permet d'une part de conserver la connectivité d'un nœud mobile indépendamment de la technologie qu'il utilise et d'autre part de faire basculer les communications de façon transparente pour les couches supérieures. Ainsi, un grand nombre de protocoles de gestion de la mobilité ont été proposés au niveau L3. Nous citons MIPv4 (Mobile IPv4) [9], MIPv6 (Mobile IPv6) [10] et ses améliorations FMIPv6 (Fast Mobile IPv6) [11] et HMIPv6 (Hierarchical Mobile IPv6) [12]. Une gestion orientée réseau (PMIPv6) [14] est aussi proposée pour permettre à des nœuds mobiles de ne pas implémenter eux-mêmes les mécanismes de mobilité. En outre, pour la gestion de la mobilité d'un réseau mobile nous avons le protocole NEMO (Network Mobility) [15] qui fait l'objet d'extensions dans cette thèse.
Dans la suite de ce chapitre, nous décrirons uniquement les solutions au niveau L3.

II.4.1 Solutions de la gestion de la mobilité au niveau L3 d'un terminal

II.4.1.1 Mobile IPv4 - Support de mobilité pour IPv4

Mobile IPv4 (MIPv4) a fait l'objet de la RCF 3344 [9] publié en 2002, il a été développé comme protocole de gestion de la mobilité au niveau L3 d'un terminal mobile. Il résout en quelques sortes le problème discuté plus haut de la dualité des fonctions de l'adresse IP d'identification et de localisation, pour fournir un service Internet sans discontinuité et un maintien des sessions actives lors d'un changement de points d'attachement à Internet (changement de routeurs d'accès).

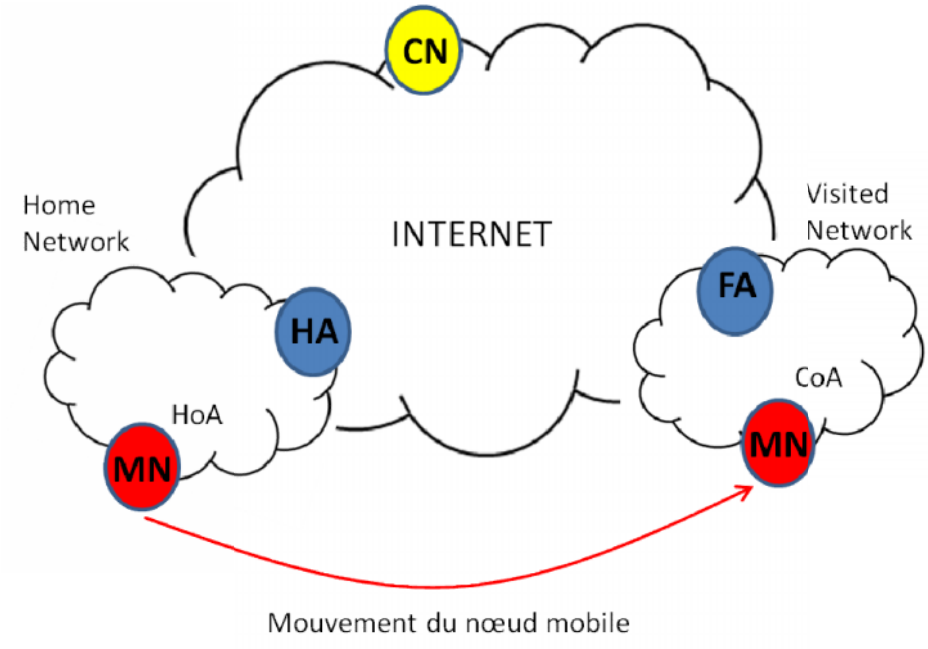

Fig. 1.1- Composants de base de l'architecture MIPv4

a) Terminologie

MIPv4 introduit de nouvelles entités fonctionnelles dans le réseau avec une terminologie nouvelle :

- Mobile Node (MN) ou nœud mobile : un terminal mobile ou un routeur mobile qui change son point d'attachement d'un réseau à un autre.
- Home Network ou réseau mère : c'est le réseau auquel est attaché initialement un MN.
- 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 MN.
- Foreign Network ou réseau visité : n'importe quel réseau autre que le réseau mère auquel le MN est connecté.
- Foreign Agent (FA) ou agent visité : un routeur d'accès dans le réseau visité qui fournit au MN un service de routage des paquets qui lui sont destinés par le HA.

- Home Address (HoA) ou adresse mère : est l'adresse IP du MN sur son réseau mère. Elle fournit l'identification du MN pour tous ses correspondants.
- Care-of Address (CoA) ou adresse temporaire : est l'adresse IP de localisation du MN, obtenue au réseau visité, et qui lui permet d'envoyer et recevoir des paquets sur ce réseau.
- Correspondant Node (CN) ou nœud correspondant : est un terminal en communication avec le MN. Un CN peut être fixe ou mobile.

b) Fonctionnement du protocole MIPv4

Lorsqu'un MN est attaché à son réseau mère, il communique de la même manière que n'importe quel nœud sur Internet en utilisant son HoA comme adresse source (Fig. 1.1). Lorsque le MN se déplace dans un réseau visité, il récupère une CoA dont le préfixe sera celui du réseau visité. Pour pouvoir continuer à communiquer à travers ce réseau, il doit donc utiliser cette adresse temporaire comme adresse source dans ce réseau. Pour cela le MN doit être capable de détecter les changements de réseau, d'obtenir cette nouvelle CoA, et informer l'agent mère et les correspondants de sa nouvelle localisation. L'ensemble de ces opérations sont regroupées dans le handover L3 de MIPv4 (Détection de mouvement, Configuration de l'adresse CoA, Enregistrement et Tunneling).

b.1) Détection de mouvement

Dans la première phase du handover L 3, le MN cherche à détecter son mouvement par rapport au réseau auquel il est attaché et ce par la découverte des agents mobiles HA ou FA (Mobile Agent Discovery). Pour détecter le changement de réseau, le MN utilise les informations contenues dans les messages « Agent Advertisement » diffusés périodiquement par les agents mobiles. Ces informations englobent entre autres l'adresse de l'agent mobile, le préfixe du réseau, les services supportés (enregistrement au FA obligatoire, type de tunnel supporté, etc) et la durée de vie du message diffusé.
La RFC 3344 définit deux mécanismes pour la détection de mouvement :

- La première méthode utilise l'information de la durée la vie du message « Agent Advertisement ». La valeur de la durée de vie est triple de la période de diffusion des messages « Agent Advertisement ». Si le MN n'a reçu aucun message « Agent Advertisement » de l'agent courant pendant cette durée de vie, le MN envoie un message «Agent Solicitation » sur le lien du nouveau réseau pour trouver les agents mobiles (FA) actifs rapidement et procéder au Handover L3.
- La seconde méthode utilise les informations de préfixe de réseau. A partir de l'adresse source du nouveau message « Agent Advertisement » reçu, le MN peut détecter son mouvement ; Si le préfixe contenu dans le nouveau message diffère du préfixe du réseau courant auquel est attaché le MN, celui-ci conclue qu'il a changé de réseau.

Pour la procédure (Mobile Agent Discovery), MIPv4 se sert des messages existants « Router Advertisement » et « Router Solicitation » définis pour ICMP (Router Discovery) [7], en y ajoutant des extensions.

b.2) Configuration de l'adresse CoA

Le protocole MIPv4 permet au MN d'utiliser deux différents types de CoA:

- Configuration avec une adresse privée : L'agent visité (FA) attribue une adresse IP privée au MN pour le localiser sur son réseau. L'adresse IP publique du FA est utilisée comme CoA du MN. L'agent FA reçoit les paquets envoyés par le HA et les redirige au MN, il fonctionne donc comme un relais entre le HA et le MN.
- Configuration avec une adresse publique : Le MN obtient une CoA grâce à un serveur DHCP sur le réseau visité. Le MN utilise cette adresse publique temporaire sur le réseau visité, donc le HA n'envoie plus les paquets vers son agent visité, mais les envoie directement vers le MN en utilisant son CoA.

b.3) Enregistrement

Dés que le MN a obtenu une CoA propre ou d'un FA, il entame la phase d'enregistrement auprès de son HA. L'enregistrement dans MIPv4 fournit un mécanisme flexible pour les MNs pour communiquer leurs localisations courantes à leurs HAs. C'est la méthode par laquelle un MN peut demander les services d'expédition en visitant un réseau étranger, informer son HA de sa nouvelle CoA, remplacer un enregistrement qui doit expirer, ou de-enregistrer quand il retourne au réseau mère. MIPv4 définit deux procédures différentes d'enregistrement, soit par l'intermédiaire du FA qui joue le rôle de relais entre le MN et le HA dans le cas où le MN enregistre la CoA du FA, soit directement du MN vers le HA si le MN enregistre sa CoA. Les deux procédures d'enregistrement comportent l'échange des messages « Registration Request » et « Registration Reply » encapsulés par UDP avec le port 434.
Le HA maintient une table d'associations entre la HoA et la CoA du MN qu'il gère. Cette table d'associations doit être réactualisée à chaque fois que le MN change de réseaux.

Si le MN utilise la CoA du FA, il envoie d'abord le message « Registration Request » à son FA. Dans ce cas, le MN utilise comme adresse source l'adresse privée fourni par le FA. Ensuite, le FA vérifie la validité du message, met à jour sa table d'associations et retransmet ce message au HA en utilisant son CoA comme adresse source. Le HA reçoit ce message, réactualise sa table d'associations et envoie un message « Registration Reply » au MN via son FA courant.
Si le MN utilise une CoA autre que celle du FA, il échange directement les messages avec le HA sans impliquer le FA. Dans ce cas, le MN utilise comme adresse source son CoA. Tous les messages d'enregistrement doivent être authentifiés pour pouvoir être validés.

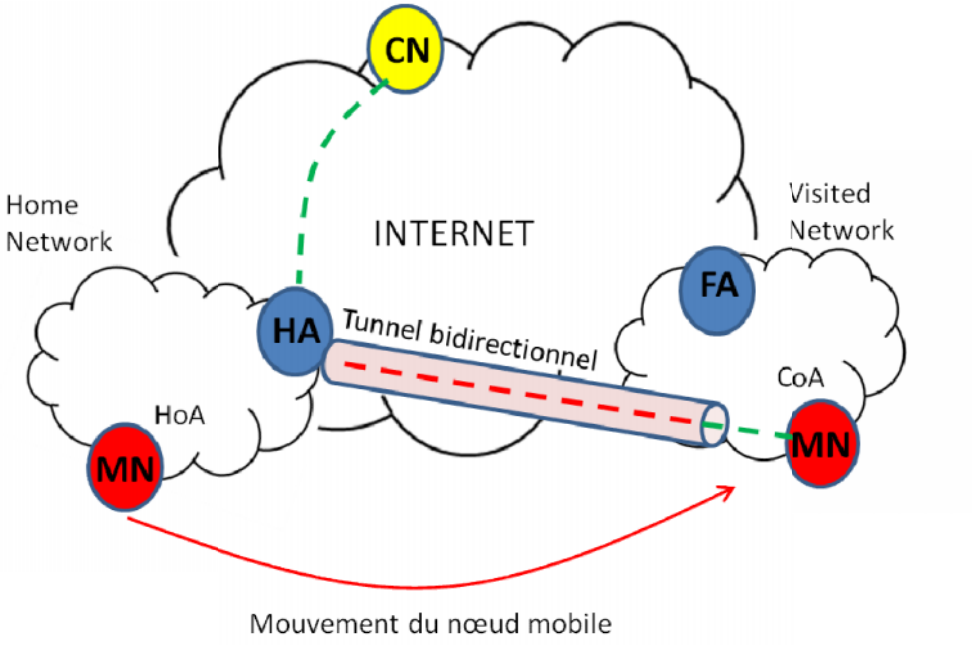

Fig. 1.2- Tunneling de MIPv4 dans le cas ou le MN enregistre sa propre CoA

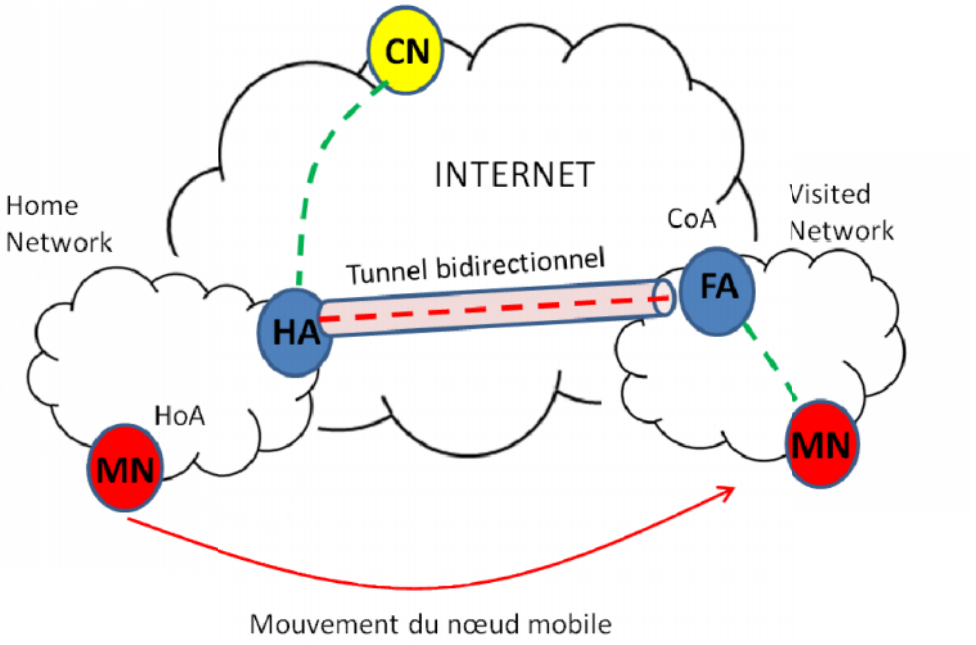

Fig. 1.3- Tunneling de MIPv4 dans le cas ou le MN utilise la CoA du FA

b.4) Tunneling

Le tunneling consiste à utiliser un tunnel IP-in-IP entre le MN/FA et le HA. Les paquets issus du MN à destination de son correspondant CN sont encapsulés suivant les cas, soit par le MN lui-même (Fig. 1.2) soit par le FA (Fig. 1.3) et envoyés au HA, qui à son tour les dés-encapsule et les envoie vers le CN. De l'autre côté, les paquets issus du CN à destination du MN sont interceptés par le HA qui les encapsule et les envoie vers le MN/FA.

c) Limitations de MIPv4

La gestion de la mobilité par le protocole MIPv4 implique plusieurs problèmes de performances:

- Adressage publique : MIPv4 ne considère pas les adresses privées puisqu'il suppose que tous les nœuds mobiles ont des adresses publiques par les quelles ils peuvent être atteints de l'Internet. Ceci limite donc les environnements dans lesquels MIPv4 peut être utilisé.
- Encapsulation : la taille des paquets est augmentée à cause d'encapsulation des paquets par le HA ou par le MN, cela provoque la perte de bande passante en réseau;
- Routage triangulaire : les paquets doivent suivre un chemin triangulaire pour être acheminé à destination, cela ajoute un délai d'acheminement supplémentaire significatif.
- Filtrage d'entrée (Ingress Filtering) : Beaucoup de routeurs emploient le filtrage d'entrée pour tout trafic sortant pour contrecarrer les attaques de « address spoofing ». Ceci signifie que les routeurs acceptent uniquement les paquets avec des adresses IP sources topologiquement correctes (une adresse dans le sous-réseau correct), et ils bloquent les paquets des MNs avec des adresses d'autres sous-réseaux. Si le MN désire envoyer des paquets au CN en utilisant un routage direct, il doit utiliser comme adresse source son adresse HoA au lieu de son adresse CoA. Le filtrage d'entrée rejette ces paquets, et par conséquent le routage n'est pas optimisé.

II.4.1.2 Mobile IPv6 - Support de mobilité pour IPv6 (MIPv6, RFC 3775, 2004)

La conception du protocole mobile IPv6 (MIPv6) présenté dans la RFC 3775 [10] a tiré des avantages des deux expériences acquises du développement du support MIPv4 et des nouvelles fonctionnalités fournis par le protocole IPv6. Les mécanismes d'IPv6 résolvent un certain nombre de problèmes qu'avaient à résoudre le support MIPv4. Ainsi, le mécanisme de configuration sans état (stateless) permet à un nœud mobile MN en déplacement d'acquérir une adresse IPv6 globale topologiquement valide. Il peut dès lors communiquer sans contrainte. Le mécanisme d'annonce des routeurs « Router Advertissement » facilite quant à lui la détection du mouvement qui est essentielle à la gestion de la mobilité.

MIPv6 mobile est donc conçu pour contrôler les mouvements d'un nœud mobile (MN) entre les réseaux IPv6. La même terminologie que MIPv4 est utilisée pour MIPv6, sauf que pour ce dernier, le concept de Foreign Agent (FA) ou agent visité n'existe pas. Au lieu de cela, dans un réseau visité un

routeur d'accès (Access Router, AR) joue un rôle semblable à celui d'un FA dans MIPv4. Le routeur AR par contre, n'a pas besoin d'assigner son adresse IP pour être l'adresse CoA du MN. A la différence du protocole MIPv4, le protocole MIPv6 permet en outre de réaliser un routage optimisé des paquets évitant le routage triangulaire. Ainsi, lorsque le MN se trouve sur un réseau visité, il peut communiquer directement avec le CN sans passer par le HA.

a) Fonctionnement du protocole MIPv6

Les opérations du handover L3 conduites par MIPv6 peuvent être classées en trois phases :

- La phase de Détection de mouvement
- La phase d'Auto-configuration de l'adresse temporaire CoA
- La phase de binding update

Cette dernière phase est décomposée également en trois phases :

- la phase de binding update avec le HA
- la phase de routabilité de retour (return Routability)
- la phase de binding update avec le CN

1) Détection de mouvement

La Détection de mouvement est la première phase de la procédure du handover L3, elle a pour objectif de détecter le changement de réseau.
MIPv6 définit trois méthodes pour détecter son mouvement sur la base des événements suivants :

- Non accessibilité du routeur d'accès : Si le MR ne reçoit pas des acquittements aux messages TCP qu'il a émis, il entame la procédure de détection de voisins non joignables (Neighbor Unreachability Detection, NUD). Pour ce faire, il émet un message « Neighbor Solicitation » au routeur pour solliciter la réponse « Neighbor Advertisement » du routeur. Si le MN ne peut pas recevoir la réponse pendant un délai égal à une seconde (par défaut), il déduit que le routeur n'est plus accessible, et devrait lancer la procédure de Découverte de nouveaux routeurs d'accès (requête « Router Solicitation (RS)» qui permet de déclencher le l'envoi du message « Router Advertisement (RA)» de la part des routeurs).

- Absence de réception du message « Router Advertisement » : Le message « Router Advertisement (RA) » est émis périodiquement par les routeurs ou en réponse à la requête « Router Solicitation (RS)». Il permet d'indiquer entre-autres quel est le préfixe utilisé sur le lien. Le message RA contient un champ appelé « délai de retransmission » qui donne la

période entre deux émissions non sollicitées de ce message (minimum 3 secondes). Il est plus fréquent qu'un routeur émette d'une manière régulière ses messages RA afin d'informer les nœuds de la prolongation de validité de préfixes annoncés. Toutefois, si le MN ne reçoit aucun message RA de son routeur pendant trois fois cet Intervalle, il considère que ce routeur n'est plus accessible. Le MN devrait lancer la procédure de Découverte de routeur pour trouver un nouveau routeur.

- Déclenchement du handover L2 : MIPv6 propose d'utiliser le protocole de découverte de voisins (Neighbor Discovery) à la suite du déclenchement du handover L2 pour confirmer le déclenchement du handover L3. Le MN envoie le message « Neighbor Solicitation » et attend la réponse « Neighbor Advertisement » du routeur afin de vérifier l'accessibilité du routeur. Si le routeur n'est pas accessible, le MN lance la procédure de Découverte de routeur pour trouver un nouveau routeur accessible. Cette méthode peut donc identifier le lancement du handover de niveau 3, mais le délai de vérification d'accessibilité du routeur est au moins d'une seconde.

2) Auto-configuration de l'adresse temporaire CoA

Une fois que le MN détecte le changement de réseau, il doit lancer la phase d'Auto-configuration d'adresses pour générer une nouvelle adresse IP sur le nouveau réseau.A la réception d'un message « Router Advertisement (RA) » sur le nouveau réseau, il peut découvrir le préfixe du réseau et configurer une adresse globale appartenant à ce préfixe qui sera la nouvelle adresse temporaire (CoA). Le mobile doit ensuite effectuer un test d'unicité de l'adresse acquise, en utilisant 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, sinon elle est considérée dupliquée et une autre auto-configuration est reprise.

3) Binding Update

- Binding Update avec le HA : Dès que le MN finit la phase d'Auto-configuration d'adresses, il envoie le message Binding Update (BU) au HA pour mettre à jour le Binding Cache du HA.

  Le binding cache du HA permet d'associer les adresses HoA avec les adresses CoA correspondantes.

  Lorsque le HA reçoit le message BU, il actualise son cache et envoie un message Binding Ack (BAck) au MN en guise de réponse au message BU. Les messages BU/BAck entre le MN et son HA doivent être authentifiés par IPsec [15, 23] ; le MN établit préalablement un tunnel IPsec avec son HA en créant une association de sécurité (SA) avec son HA par le biais du protocole IKE (Internet Key Exchange, [82]). En absence d'optimisation de routage, les

paquets échangés entre le MN et le CN seront sont transmis à travers le tunnel mis en place entre le HA et le MN (Fig. 1.5).

- Routabilité de retour (Return Routability) : Pour pouvoir utiliser le mécanisme d'optimisation de routage, non seulement le MN et le HA doivent supporter le protocole MIPv6, mais le CN doit aussi supporter le protocole MIPv6. Si le CN ne supporte pas le protocole MIPv6, la communication entre le MN et le CN doit passer par le HA, comme pour MIPv4. Similairement au HA, Le MN doit opérer un binding update au niveau du CN. Pour s'assurer que c'est le bon MN qui a envoyé le message du binding update, une méthode appelée procédure de routabilité de retour (Return Routability) est employée (Fig. 1.4). Elle a pour but d'établir la preuve au CN que le MN est accessible à son adresse mère HoA et à son adresse temporaire CoA. Seulement avec cette assurance que le CN est capable d'accepter les binding updates du MN pour pouvoir ensuite diriger les paquets de ce MN directement à son adresse CoA.

  Quatre messages sont utilisés dans cette procédure :

  - Home Test Init (HoTI) : envoyé par le MN au CN via le tunnel MN-HA
  - Care-of Test Init (CoTI) : envoyé par le MN au CN directement (sans passer par le HA)
  - Home Test (HoT) : réponse à HoTI envoyé par le CN au MN via le tunnel MN-HA
  - Care-of Test (CoT) : réponse à CoTI envoyé par le CN au MN directement

  La procédure est constituée de deux phases préliminaires, dont l'une teste l'adresse HoA (HoTi puis HoT) et l'autre teste l'adresse CoA (CoTi puis CoT). Ensuite toute demande de binding update sera subordonnée à l'exécution correcte de ces deux phases préliminaires. Les deux phases sont menées parallèlement l'une et l'autre, à l'initiative du MN. Le CN répond aux deux requêtes indépendamment l'une de l'autre en y ajoutant respectivement un « home keygen token » et un « care-of keygen token » à partir desquels le MN peut générer une clé appelée « Binding Management Key (Kbm) », qui lui permet de s'authentifier lors de l'échange BU/BAck effectué avec le CN.

- Binding Update avec le CN : Le MN et le CN utilisent la clé Kbm générée dans la phase de routabilité de retour pour authentifier les messages BU/BAck. Lorsque le CN reçoit le message BU du MN, il met à jour son binding cache et envoie le message BAck au MN. Le MN et le CN peuvent ensuite communiquer en utilisant le routage optimisé de paquets (Fig. 1.5).

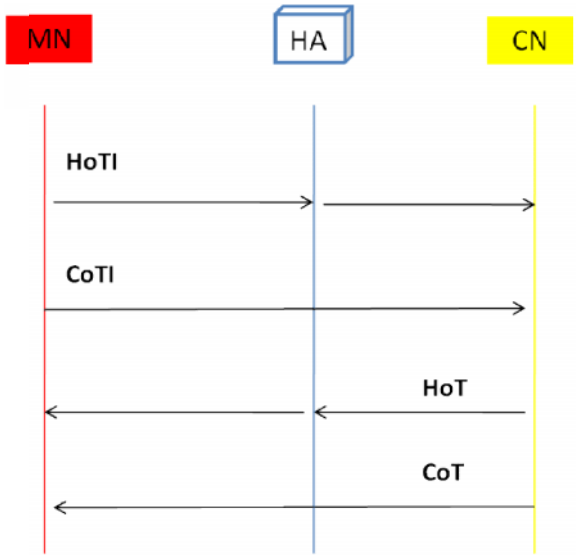

Fig. 1.4- Procédure de retour de Routabilité

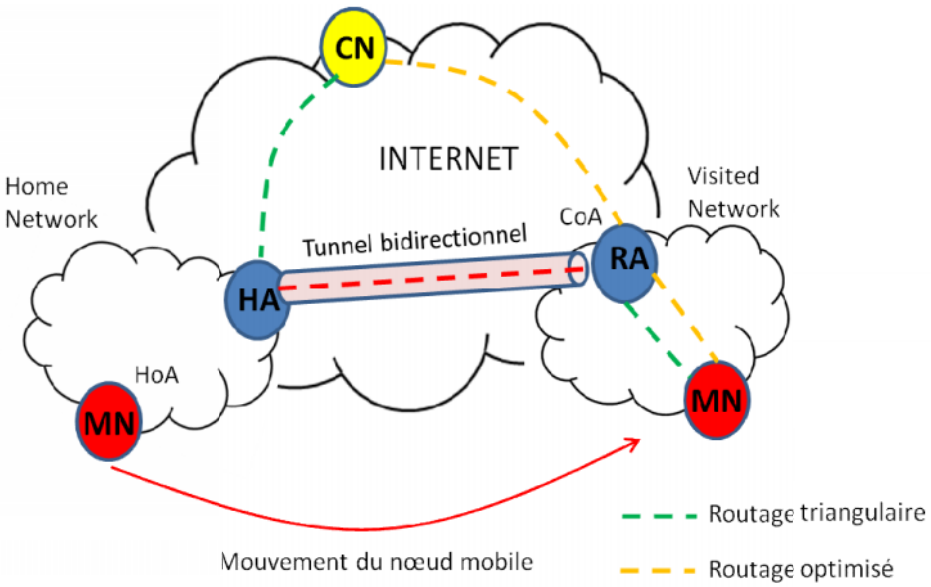

Fig. 1.5- Composants de base de l'architecture MIPv6
(Routage triangulaire et Routage optimisé)

b) Format des messages de signalisation utilisés

MIPv6 définit un en-tête d'extension de mobilité pour IPv6 pour transporter les messages de signalisation, dont le format est le suivant : (Fig. 1.6)

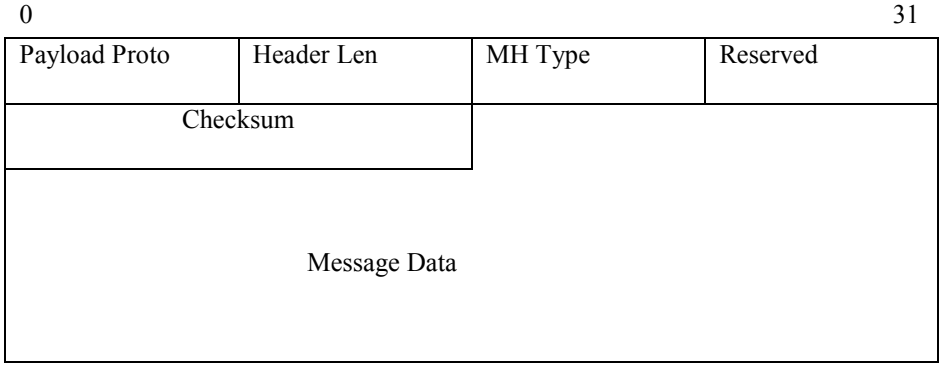

Fig. 1.6- Format de l'en-tête d'extension de mobilité d'IPv6

- Payload Proto : a la même fonction que celui de l'en-tête IPv6. Il identifie le prochain en-tête d'extension. Dans le cas du message de signalisation de MIPv6, il doit valoir 59, c'est-à-dire qu'il n'y a pas d'en-tête d'extension suivant.
- Header Length : représente la longueur d'en-tête d'extension de mobilité. Il ne prend pas en compte les 8 premiers octets de l'en-tête.
- MH Type : décrit les types des messages de mobilité (voir Tableau 1.1).

MH Type	Type de message de mobilité
1	Home Test Init (HoTI)
2	Care-of Test Init (CoTI)
3	Home Test (HoT)
4	Care-of Test (CoT)
5	BU
6	BAck

Tableau 1.1- Exemples de messages de signalisation de MIPv6

Nous donnons ici uniquement les formats des messages BU et BAck dont nous aurons besoin au niveau de la présentation du protocole de mobilité de réseau (NEMO), pour les formats des autres messages utilisés par MIPv6, voir [10].

Format du message BU :

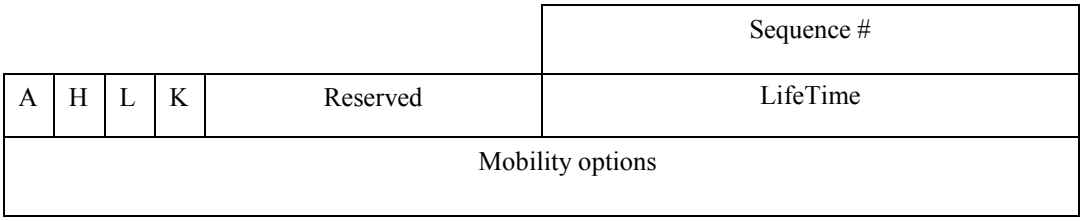

Fig. 1.7- Format du message BU de MIPv6

bits:

- Acknowledge (A): demande d'accusé de réception.
- Home Registration (H) : demande de traitement du BU par le HA du MN.
- Link-Local Address Compatibility (L): la HoA utilise le même identifiant que l'adresse du lien locale.
- Key Management Mobility Capability (K): utilisation manuelle d'IPsec.

Mobility options : contient les options de mobilité telle que la CoA.

Format du message BAck :

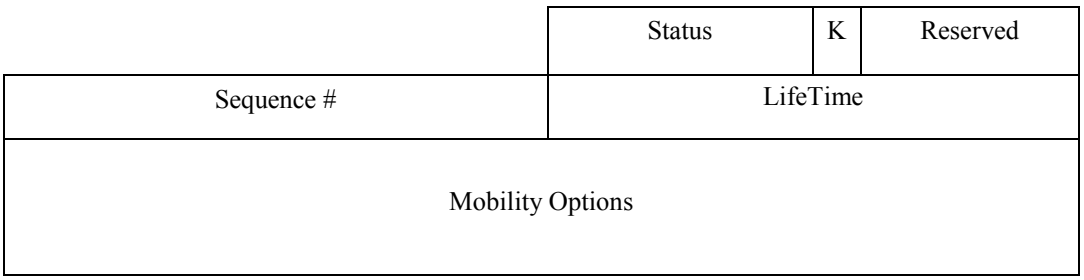

Fig. 1.8- Format du message BAck de MIPv6

- Status (8 bits) : permet d'indiquer le résultat du traitement du message BU.
  La valeur à indique BU accepté, les valeurs supérieures ou égal à 128 indiquent que le BU est rejeté.

c) Limites de performance de MIPv6

Bien que MIPv6 Mobile permette de résoudre le problème du routage triangulaire, il souffre encore de plusieurs faiblesses liées à ses performances. Le délai du handover de MIPv6 est long. Particulièrement, le délai de la phase de Détection de mouvement, celui de la phase d'auto-configuration et celui de la phase de binding update sont très long pour les applications en temps réel.

Les pertes de paquets pendant le handover peuvent être importantes. Le protocole MIPv6 n'a pas proposé une solution pour réduire ces pertes.

Pour faire face à ces limites, plusieurs solutions ont été proposées. Parmi les différentes propositions, nous présentons un aperçu sur deux principales solutions : le protocole Fast MIPv6 (FMIPv6) et le protocole MIPv6 Hiérarchique (HMIPv6).

II.4.1.3 Fast Mobile IPv6 (FMIPv6, RFC 4068, 2005)

FMIPv6 publié initialement dans la RFC 4068 puis dans les RFC 5268 et 5568 [11], est une extension de MIPv6 dont le but est de réduire le délai du handover en comblant les lacunes de MIPv6. Les améliorations apportées se résument dans les points suivants :

- Réduction du délai de détection du mouvement du MN
- Réduction du délai d'enregistrement de la nouvelle CoA.

L'idée de FMIPv6 est d'utiliser les informations de préfixe sur les liens d'accès pour prédire ou répondre rapidement à un événement de handover. Le protocole FMIPv6 pratique une l'anticipation du mouvement du MN pour prévoir et se préparer au prochain handover à l'avance.

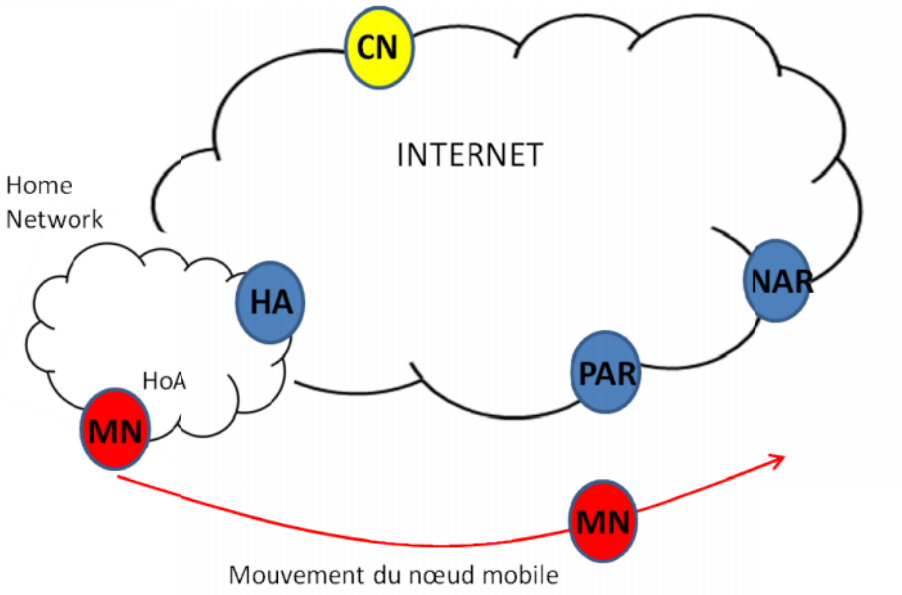

Fig. 1.9- Composants de base de l'architecture de FMIPv6

Une nouvelle terminologie est définie pour FMIPv6 :

- PAR (Previous Access Router) : le routeur d'accès précédent
- NAR (New Access Router) : le nouveau routeur d'accès
- PCoA (Previous CoA) : l'adresse temporaire CoA précédente

- NCoA (New CoA) : nouvelle adresse temporaire CoA

Le protocole FMIPv6 définit également de nouveaux messages :

- 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).
- FBAck (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' acquittement 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 FBAck.

a) Opérations du protocole FMIPv6

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. le MR envoie ensuite un message FBU contenant le NCoA proposé. Le MN envoie le message FBU sur le lien du PAR toutes les fois que l'anticipation" du handover est faisable. Quand l'anticipation n'est pas

faisable ou quand il n'a pas reçu un message FBAck, le MR envoie le message FBU immédiatement après l'attachement au lien du NAR.

FMIPv6 définit deux modes opératoires: le mode prédictif et le mode réactif.

i) **mode prédictif :** Dans ce mode (Fig. 1.10), 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.

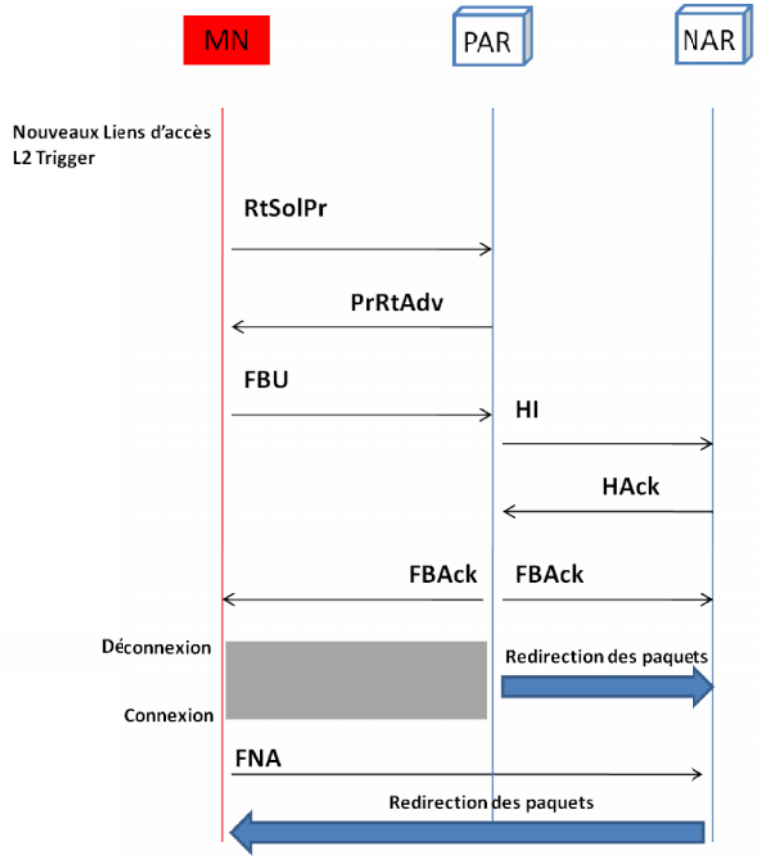

Fig. 1.10- Procédure du mode prédictif de FMIPv6

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. 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.

mode réactif : Dans ce mode (Fig. 1.11), 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.

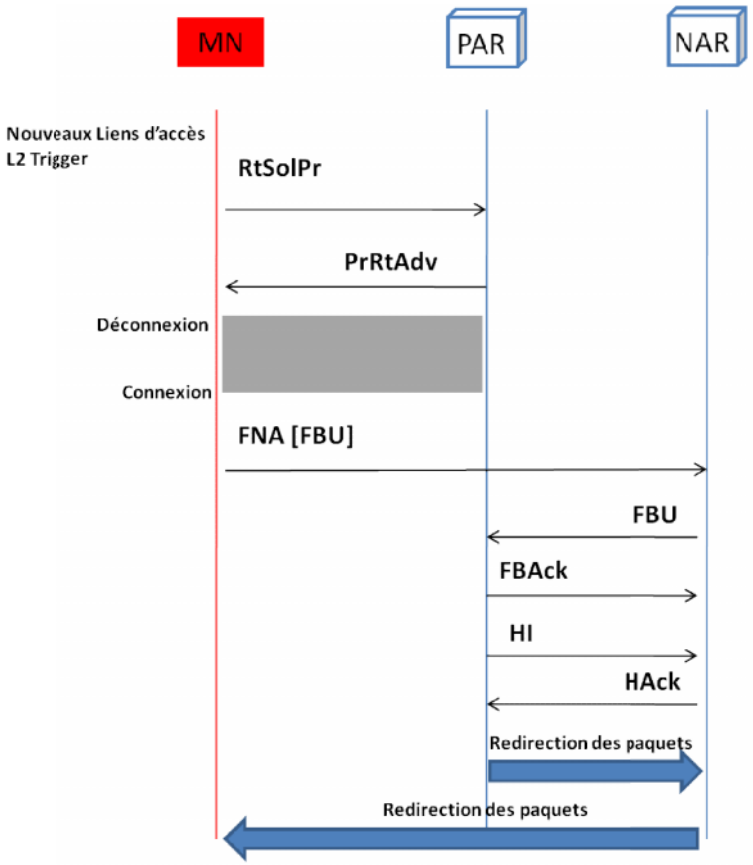

Fig. 1.11- Procédure du mode réactif de FMIPv6

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 tunneler 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 Advertissement au MN.

b) Conclusion sur FMIPv6

Le protocole FMIPv6 est une solution assisté par le réseau qui permet de réduire considérablement le délai du handover et par conséquent les pertes de paquets. Cependant, dans le meilleur des cas, le temps d'interruption global peut être réduit au temps d'interruption dû à la réassociation au niveau L2, donc un délai et une perte de paquets résiduels existeront toujours pour cette solution, qui risque de ne pas répondre à certaines applications exigeantes en QoS.

II.4.1.4 Hierarchical Mobile IPv6 (HMIPv6, RFC 4140, 2005)

Le protocole HMIPv6 [12] est une extension du protocole MIPv6, dont l'objectif est de réduire la quantité des messages de signalisation du protocole MIPv6. Les messages de signalisation sont les messages de la phase de binding update avec le HA, les messages liés avec la phase de routabilité de retour et les messages de la phase de binding update avec les CNs. En fait, le protocole HMIPv6 permet également de réduire le délai de ces trois phases, donc de réduire le temps d'interruption des communications entre le MN et ses correspondants.

Le protocole HMIPv6 (Fig. 1.12) introduit une nouvelle entité appelée MAP (Mobility Anchor Point). Le réseau global est découpé en différents domaines qui sont indépendants des réseaux IP. Chaque MAP contrôle un domaine et la taille de ce domaine est définie par l'opérateur de télécommunications. Le MAP joue le rôle d'un HA local pour le MN. Il permet de masquer le mouvement du MN dans son domaine au HA et aux CNs.
Lorsqu'un MN entre dans un domaine qui est contrôlé par le MAP, il reçoit le message « Router Advertissement ». Ce message contient l'information concernant le MAP qui contrôle ce domaine, telle que l'adresse du MAP, le préfixe du réseau où le MAP se trouve, etc.
Ensuite, le MN s'auto-configure avec deux adresses temporaires : une adresse temporaire régionale RCoA (Regional CoA) et une adresse temporaire locale LCoA (Local CoA).

- L'adresse RCoA est une adresse composée par le préfixe du réseau où ce MAP se trouve et par l'identifiant d'interface du MN. Le MN ne change pas cette adresse RCoA tant qu'il reste dans ce domaine.

- L'adresse LCoA est une adresse du réseau où le MN s'attache au fur et à mesure. Le MN change cette adresse LCoA quand il passe d'un réseau à un autre.

Après l'accomplissement de l'auto-configuration de ces deux adresses, le MN envoie un message LBU (Local Binding Update) au MAP pour créer une association entre son adresse RCoA et son adresse LCoA. Quand le MAP reçoit ce message, il doit effectuer la procédure DAD pour vérifier l'unicité d'adresse RCoA. S'il n'y a pas de conflit d'adresse, le MAP envoie le message LBA (Local Binding Acknowledgement) au MN. Cela signifie que la phase de binding update avec le MAP est réussie. Ensuite, le MN effectue la phase de binding update avec le HA et les CNs en utilisant son adresse RCoA comme sa nouvelle adresse temporaire.

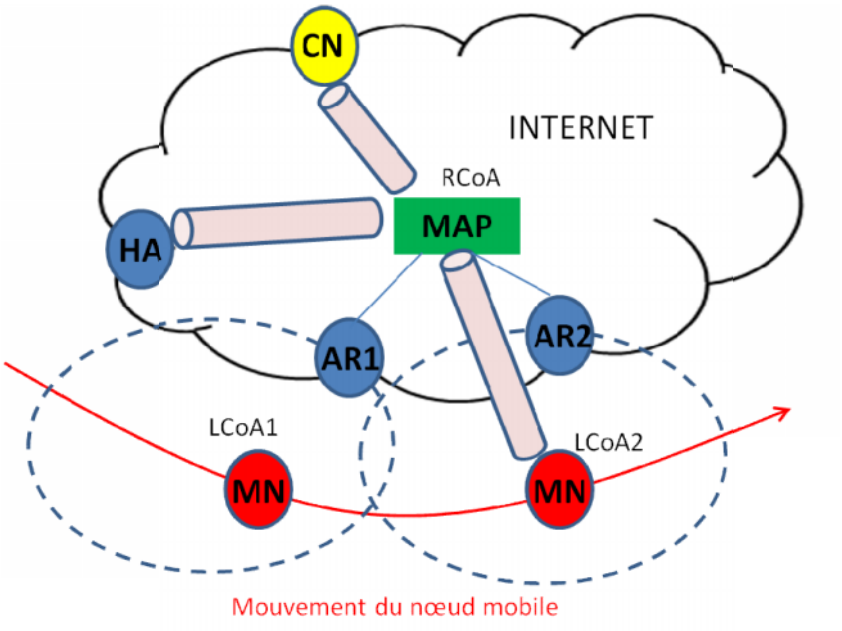

Fig. 1.12- Principe de fonctionnement de HMIPv6

Le HA et les CNs mettent à jour leurs binding caches avec l'adresse RCoA et envoient les paquets vers l'adresse RCoA du MN. Dans le même temps, un tunnel bidirectionnel est crée entre le MN et le MAP. Les paquets des CNs sont envoyés à l'adresse RCoA du MN, le MAP intercepte ensuite ces paquets, les encapsule et les retransmet à l'adresse LCoA du MN en traversant le tunnel.

De même, les paquets du MN sont envoyés à l'adresse RCoA en traversant le tunnel, le MAP intercepte ensuite ces paquets et les retransmet aux CNs. Enfin, le MAP, le MN et les CNs transfèrent les paquets de données de la même façon que dans le cas du protocole MIPv6. Par conséquent, lorsque le MN se déplace dans un domaine, il lui suffit de mettre à jour son LCoA avec le MAP. Le MN n'a pas besoin d'effectuer la phase de binding update avec le HA et les CNs quand il n'a pas changé son adresse RCoA. Le MAP masque ainsi le mouvement du MN dans son domaine au HA et aux CNs.

On appelle souvent la micro-mobilité le mouvement du MN à l'intérieur d'un domaine MAP et la macro-mobilité le mouvement du MN entre des domaines MAP. Pour la micro-mobilité, le protocole HMIPv6 apporte les avantages présentés ci-dessus, mais il provoque ainsi un délai supplémentaire pour le traitement des paquets. Pour la macro-mobilité, le MN doit obtenir non seulement l'adresse RCoA et effectue la phase de Mise à jour d'association avec le MAP, mais aussi effectuer la phase de

Mise à jour d'association avec le HA et les CNs. Le délai de ces procédures est plus long que celui du protocole MIPv6. Un choix adéquat du domaine est nécessaire pour éviter la macro-mobilité fréquente du MN. Une solution (FHMIPv6) [13] combinant FMIPv6 et HMIPv6 a été proposée également.

II.4.1.5 Proxy Mobile IPv6 (FMIPv6, RFC 5213, 2008)

PMIPv6 [14] propose une solution de gestion de la mobilité d'un nœud mobile entièrement réalisée par le réseau. Le besoin pour une telle solution s'explique par le fait qu'elle permette à n'importe quel nœud mobile de se déplacer entre différents réseaux d'accès sans avoir besoin d'implémenter lui-même des solutions de mobilité spécifiques.

PMIPv6 est prévu donc pour fournir à un nœud mobile la gestion de mobilité basée totalement sur le réseau, sans exiger la participation du MN à n'importe quelle signalisation reliée à la mobilité. Les entités de mobilité dans le réseau poursuivent le mouvement du MN et déclenchent la signalisation requise.

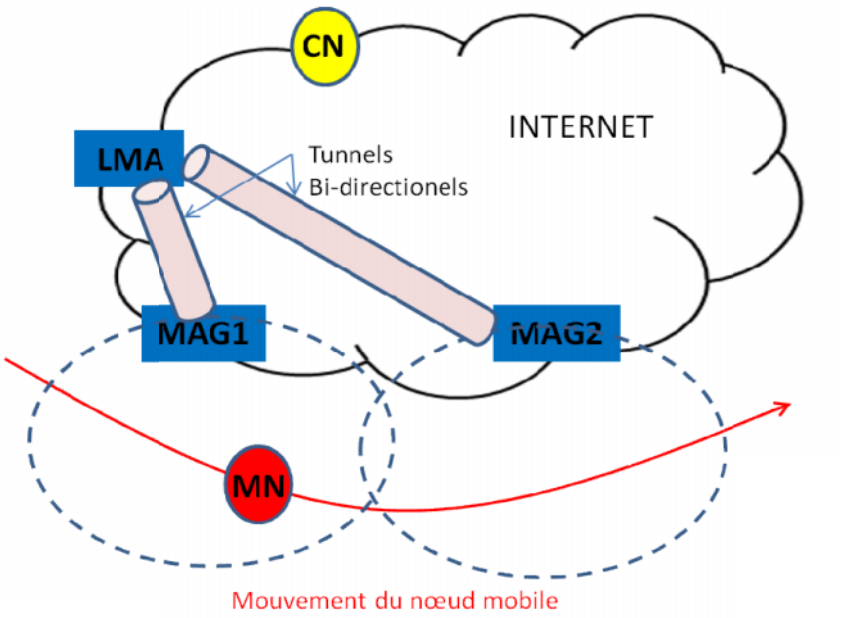

Fig. 1.13- Composants de base de l'architecture de PMIPv6

a) Terminologie

- PMIPv6-domain : le domaine PMIPv6 désigne le réseau où la gestion de la mobilité IPv6 d'un nœud mobile est manipulée à l'aide du protocole PMIPv6.
- LMA (Local Mobility Anchor) : joue le rôle d'un Home Agent (HA) dans le domaine PMIPv6.

- MAG (Mobile Access Gateway) : est une fonction sur un routeur d'accès qui gère la signalisation liée à la mobilité d'un MN qui est attaché à ce MAG.
- MN-HNP (Mobile Node's Home Network Prefix) : est un préfixe assigné au lien entre le nœud mobile et la LMA.
- MN-HoA (Mobile Node's Home Address) : est l'adresse HoA du MN obtenue àpartir du préfixe HNA attribué par le LMA et annoncé au MN par le MAG.
- MN-Id (Mobile Node Identifier) : c'est l'identité du MN dans le domaine PMIPv6
- Policy Profile : est un terme abstrait pour designer un ensemble de paramètres de configuration qui sont configurés pour un nœud mobile donné. Les entités de mobilité dans le domaine PMIPv6 exigent l'accès à ces paramètres pour fournir la gestion de la mobilité à un nœud mobile donné.
- Proxy-CoA (Proxy Care-of Address): est l'adresse de l'interface externe du MAG. Cette adresse sera utilisée pour établir un tunnel entre le LMA et le MAG.
- LMAA (LMA Address) : adresse du LMA.
- Proxy Binding Update (PBU) : est un message de binding update envoyé par le MAG au LMA.
- Proxy Binding Acknowledgement (PBA) : est la réponse au message PBU, envoyé par LMA au MAG.

b) Operations du protocole PMIPv6

PMIPv6 définit la notion de domaine PMIPv6 dans lequel la mobilité est gérée par ce protocole. Un MN localisé à l'intérieur d'un domaine PMIPv6 est lié à un LMA qui joue le rôle de son HA. De plus, lorsqu'il se déplace, le MN s'attache à des MAG successifs qui jouent le rôle de routeurs d'accès responsables de la signalisation liée à sa mobilité (Fig. 1.13).

Le principe de PMIPv6 est d'émuler le fait que le MN se trouve toujours dans son réseau mère en lui assignant un HNP, celui-ci étant uniquement assigné à ce MN. Le MN considère donc le domaine PMIPv6 comme un seul lien.

Lorsqu'un MN arrive dans un domaine PMIPv6 (le domaine géré par le MAG1 sur la figure 1.14, il doit tout d'abord se rattacher au réseau d'accès dans lequel il se trouve. Le MAG1 peut alors détecter l'arrivée de ce MN et déterminer à partir de son identifiant ou MN-Id si celui-ci est autorisé à utiliser les services de mobilité ou pas. Si oui, le MAG1 envoie un PBU au LMA, incluant l'identifiant du MN. Le LMA alloue alors au MN un HNP, met à jour son binding cache et met en place un tunnel bidirectionnel jusqu'à l'adresse Proxy-CoA1 du MAG1 qu'il voit comme étant l'adresse temporaire CoA courante du MN. Le LMA répond alors au MAG1 par un PBA incluant le HNP du MN. Le

MAG1 réalise lui aussi les mécanismes nécessaires à la mise en place du tunnel vers l'adresse du LMA (LMAA) et au transfert des paquets vers le MN. Le MAG1 envoie alors un message « Router Advertisement » dans lequel il indique au MN son HNP, le préfixe IPv6 que le MN doit utiliser pour configurer son adresse HoA. Dès lors, tous les paquets à destination de ce préfixe seront routés par le LMA vers le MAG1 qui, à son tour, les transmettra au MN. Les paquets envoyés par le MN suivront le même trajet.

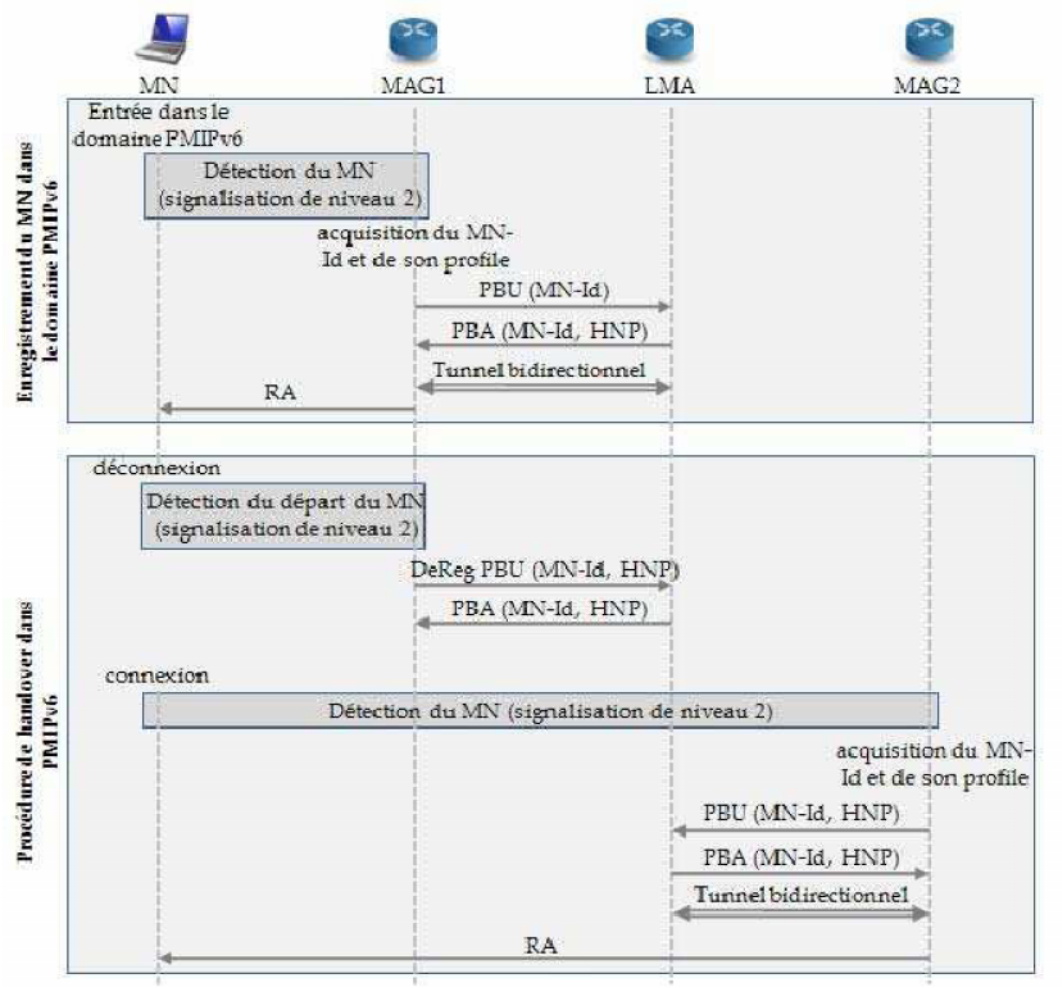

Fig. 1.14- Procédure du handover dans un domaine PMIPv6

Lorsque le MN change de réseau et donc de MAG de rattachement, le MAG1 détecte la déconnexion et lance une procédure de dé-enregistrement auprès du LMA par l'échange des messages PBU/PBA. Le LMA lance alors un timer à la fin duquel il supprime le binding entre le HNP et la Proxy-CoA1. Une fois que le MN s'est attaché au MAG2, un tunnel bidirectionnel entre le LMA et le MAG2 est mis en place de la même manière que précédemment et toutes les communications depuis et vers le MN passent par ce nouveau tunnel.

II.4.2 Gestion de la mobilité d'un réseau mobile - Protocole NEMO

Si les travaux dans le domaine de la mobilité au niveau L3 se sont dans un premier temps exclusivement consacrés à la mobilité des stations, le besoin de fournir un accès Internet permanent 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) créé en octobre 2002. Ces travaux ont abouti à l'édition de la RFC 3963 [15] qui spécifie des fonctionnalités semblables à celles de MIPv6 dédiées aux routeurs mobiles (protocole NEMO BS). A noter que d'autres solutions pour la gestion de la mobilité au niveau L3 d'un réseau NEMO existent aussi, nous citons particulièrement SINEMO [20] et HiMIP-NEMO [21]. Cette thèse se limite au protocole NEMO BS [15] standardisé par l'IETF.

II.4.2.1 Réseaux NEMO

Un réseau mobile ou réseau NEMO peut être défini comme un réseau /sous-réseau en déplacement, connecté à Internet par l'intermédiaire d'un ou plusieurs routeurs qui changent leurs points d'attachements dans la topologie Internet. La gestion de la mobilité des réseaux NEMO doit assurer d'une manière transparente la continuité des services Internet pour les stations ou terminaux embarqués. De nombreuses applications des réseaux NEMO sont envisagées (Fig. 1.15). Celles-ci incluent en particulier [22]:

- Réseaux de capteurs et systèmes embarqués: déployés dans les trains, voitures, bateaux et avions. 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. Nous pouvons citer encore les capteurs de santé permettant le contrôle en temps réel de l'état de santé d'un patient.

- les réseaux d'accès à Internet : déployés dans les transports publics (bus, Metro, tramway, TGV, trains et taxis) et permettent d'offrir un accès Internet aux passagers. Un exemple démonstratif est celui d'une compagnie de transport offrant un accès Internet sans interruption de service à ses passagers en utilisant les appareils proposés par la compagnie ou leurs propres laptops ou téléphones.

Fig. 1.15- Exemples d'applications des réseaux NEMO

- Les réseaux PAN (Personal Area Network) : les PANs sont des réseaux constitués d'un ensemble d'appareils électroniques de petite taille (cardio-fréquencemètre, téléphone cellulaire, assistant personnel, appareil photo digital, etc.) portés par les personnes. De nombreux scénario d'utilisation des PANs peuvent être imaginés, notamment pour des applications liées à la sécurité civile (police, pompiers), à la médecine et éventuellement à l'armée.

II.4.2.2 Protocole NEMO Support Basique (NEMO BS) [RFC 3963, 2005]

Le protocole NEMO BS [15] est une extension de MIPV6 [10] pour supporter la mobilité d'un réseau entier (réseau NEMO) qui change son point d'attachement à Internet. NEMO BS assure d'une manière transparente la continuité des sessions ouvertes pour tous les nœuds dans le réseau mobile NEMO.

Cette transparence est possible grâce à l'introduction d'un routeur appelé routeur mobile (Mobile Router, MR) au niveau du réseau NEMO. Le réseau NEMO est attaché au réseau mère/réseau visité par le biais du routeur mobile (MR) qui contrôle son mouvement.

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

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.

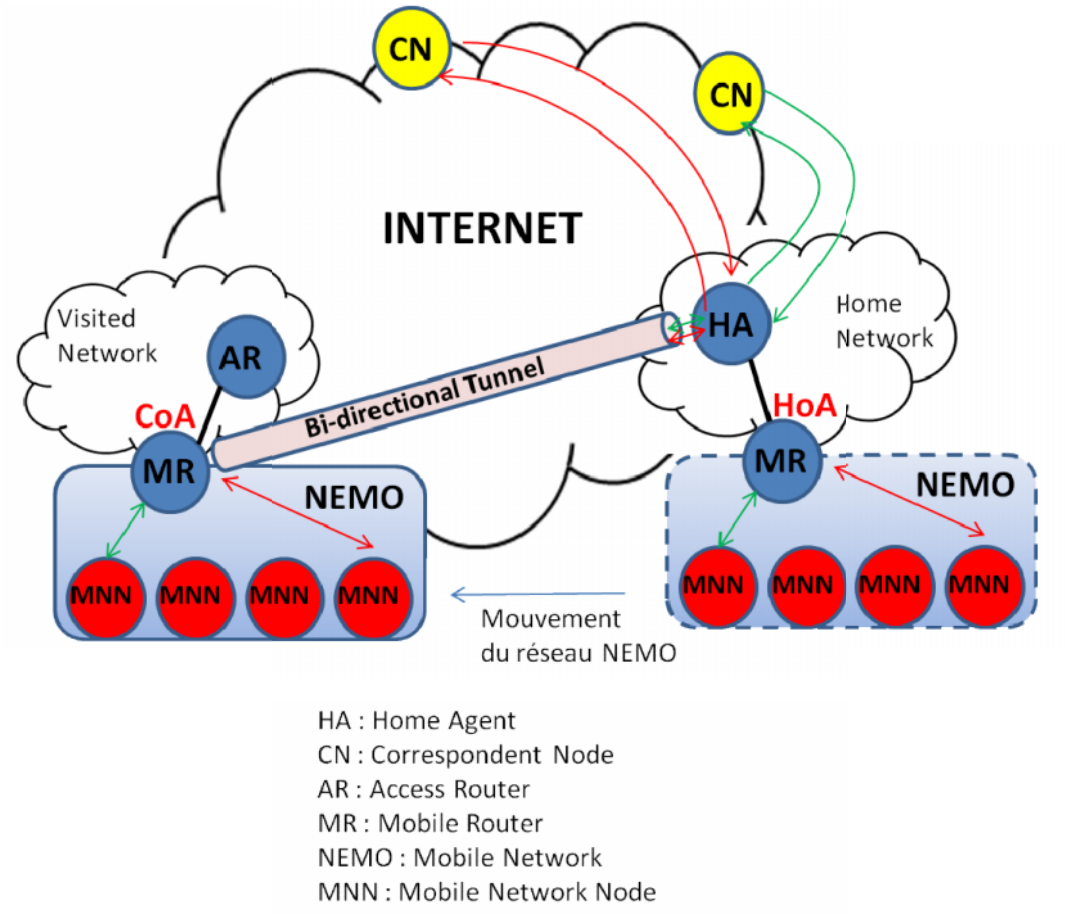

Fig 1.16 – Fonctionnement de base du protocole NEMO BS

a) Opérations du protocole NEMO BS

Les mêmes opérations conduites par MIPv6 sont valables pour NEMO BS, à l'exception des procédures de retour de routabilité (Return Routability) et le binding update avec les CNs. En effet, NEMO BS ne supporte pas l'optimisation de routage.

Donc, quand le MR s'éloigne du réseau mère et s'attache à un nouveau routeur d'accès (Access Router, AR), 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 entré indiquant la nouvel adresse CoA de l'actuel point d'attachement du MR.

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 un dans le message BU (Fig. 1.17). Il inclut également les informations sur le préfixe du réseau mobile de sorte que le HA peut expédier les paquets destinés aux nœuds MNNs du réseau mobile NEMO.

Quand le HA reçoit le message binding update (BU) 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 [23].

Une fois le processus de mise à jour est terminé, un tunnel IP-in-IP [24] 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 l'adresse CoA du MR comme point d'entrée du tunnel 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 ce dernier 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'assuré que le trafic proviens bien d'un des nœuds du réseau mobile sinon il rejette le paquet.

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.

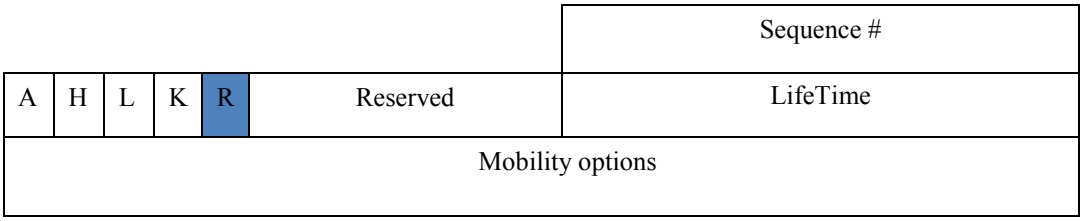

Fig. 1.17- Changement dans le message BU pour le support NEMO

Option du préfixe

NEMO ajoute une option de préfixe (Fig. 1.18) dans le champ « Mobility Options » du message BU de MIPv6.

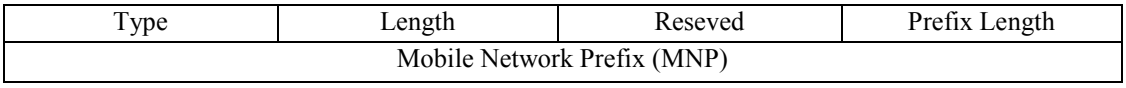

Fig. 1.18- Option du préfixe pour le support NEMO

- Type : valeur égal à 6
- Length (8 bits) : indiquant la longueur en octets de l'option, à l'exception des champs « Type » et « Length ».
- Reseved : 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 (Fig ; 1.19) 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.

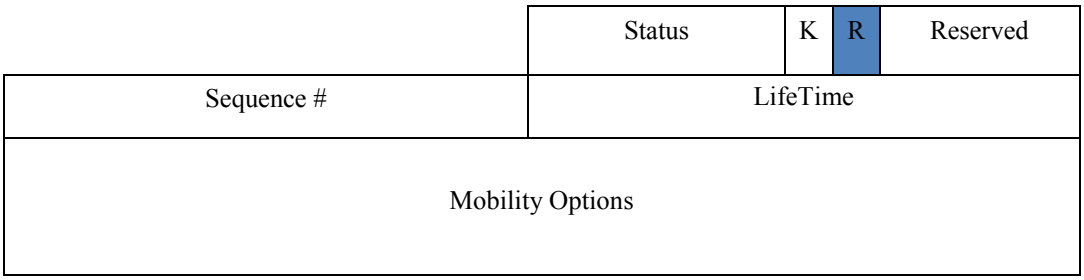

Fig. 1.19- Changement dans le message BAck pour le support NEMO

II.4.2.3 Issues du protocoles NEMO BS

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. Néanmoins, 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. Parmi ces issues, 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 [25] pour documenter ces problèmes liés au RO. Jusqu'à présent aucune solution n'est standardisée.

- **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 [26], mais les performances obtenues restent encore insuffisantes [27]. Rappelons que l'objet de cette thèse est d'adresser particulièrement ce problème.

- **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 [28] dans laquelle les issues du multihoming sont analysées. Le développement de support de mobilité dans le contexte du multihoming est une issue ouverte.
Par ailleurs, nos propositions dans cette thèse sont basées principalement sur le multihoming, de ce fait nous avons consacré une bonne partie du chapitre 3 aux problèmes liés à cette fonctionnalité.

- **Sécurité :**

NEMO hérite certain inconvénient de MIPv6 tels que les menaces de sécurité. Dans [70] diverses attaques (redirection attacks, traffic hijacking, denial of service) contre NEMO ont été décrites et ont mené à l'adoption d'IPSec [23] pour protéger le trafic d'arrivée (inbound) et le trafic de départ (outbound) de NEMO.
Dans l'architecture NEMO, la mobilité est masquée au MNNs (MNNs unaware of mobility), il est donc important que NEMO fournit la sécurité quand le réseau mobile est attaché à un réseau étranger. 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 dans [15] comment les issues d'autorisation et d'authentification [29] 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 [30], [70]-[77]. Malheureusement, avec ces propositions, les menaces de sécurité ne sont pas toutes maitrisées et le problème de sécurité dans NEMO reste toujours ouvert.

II.5 Conclusion

Dans ce chapitre, nous avons présenté un état de l'art des solutions de gestion de la mobilité dans les réseaux IP. Nous nous sommes intéressés particulièrement aux solutions transparentes aux applications, c'est-à-dire celles qui opèrent au niveau L3, et nous avons considéré aussi les supports développés pour le cas d'un réseau tout entier mobile que pour un terminal mobile. Ces solutions se basent sur la séparation entre l'adresse IP d'identification et celle de localisation, et nécessitent quelques changements dans l'infrastructure réseau. Pour maintenir la connectivité à Internet, les entités mobiles doivent exécuter les procédures de détection de mouvement, d'auto-configuration et de

mise à jour de localisation, ces opérations impliquent des délais d'interruption de sessions plus ou moins importants induisant des pertes de paquets (MIPv4 et MIPv6).
Les différentes améliorations ont permis de limiter le temps de handover en améliorant les mécanismes de détection de mouvement et d'enregistrement de la nouvelle adresse (FMIPv6) et de limiter la signalisation de mobilité à des domaines réduits (HMIPv6). Une gestion orientée infrastructure a été proposée également pour supporter la mobilité des nœuds mobiles n'implémentant aucun mécanisme de mobilité. La figure 1.20 récapitule l'ensemble des solutions de gestion de mobilité proposées dans ce chapitre.

Le protocole NEMO BS, extension logique de MIPv6 fût développé pour la gestion de la mobilité d'un réseau entier. Cependant, le protocole est basique nécessite des développements complémentaires, ainsi plusieurs issues sont encore ouvertes pour la recherche, la performance du handover est l'une d'entres-elles et fait l'objet de cette thèse. En effet, NEMO BS a hérité les limites de performance de MIPv6, de sorte qu'il n'est pas approprié pour les applications temps réel et de qualité de service. Dans le chapitre suivant, à travers une étude analytique nous mettons en évidence les limites de ses performances. Nous présenterons ensuite quelques extensions permettant de réduire l'impact négatif du handover NEMO sur les communications en cours.

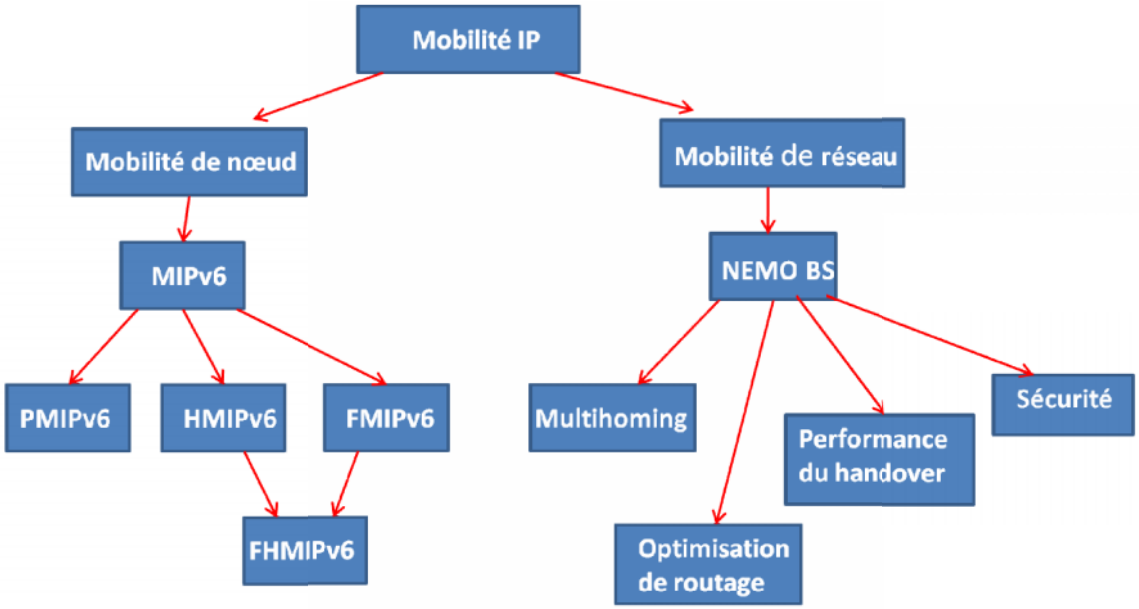

Fig. 1.20- Classification des supports de gestion de la mobilité au niveau IP

CHAPITRE 2

Analyse du Handover du protocole NEMO Support Basique et ses Extensions

II.1 Introduction

Le protocole de NEMO BS conçu par IETF pour la gestion de la mobilité de réseau, est une extension du protocole MIPv6. Le handover de NEMO BS hérite ainsi des inconvénients de MIPv6.
Les performances du handover hard (Brake-Before-Make) du protocole NEMO ont été analysées dans la littérature [31-35]. Les résultats prouvent que le support de mobilité tel qu'il est défini ne permet pas d'assurer une connectivité sans couture (Seamless connectivity). Pour surmonter les limitations du protocole NEMO BS, beaucoup d'optimisations ont été proposées. Les solutions proposées se fondent sur l'optimisation de chaque composant du handover, en utilisant la conception inter-couche (cross-layer design), l'assistance de réseau, le multihoming, etc. L'objectif de ce chapitre est de présenter une analyse des composants du handover du protocole NEMO BS (ou MIPv6-NEMO) et décrire ses extensions d'optimisation.

II.2 Analyse du délai du handover NEMO

Le protocole NEMO BS [15] proposé par IETF fournit un support de mobilité pour un réseau mobile entier 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 (Fig. 2.1).

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.

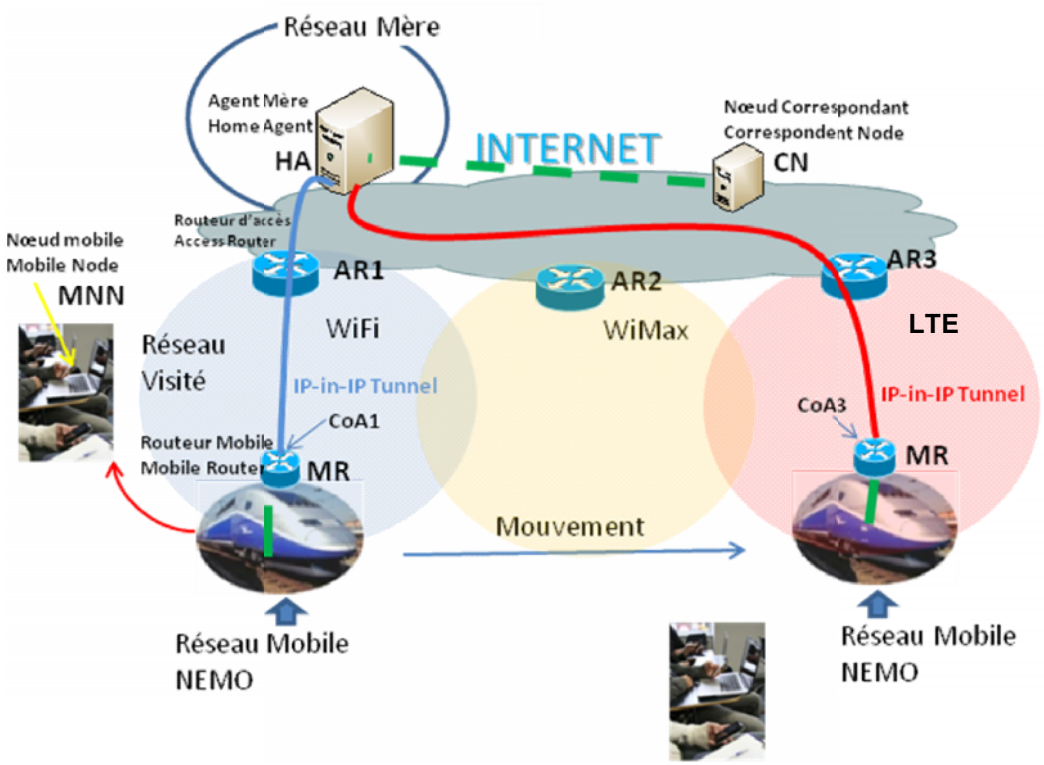

Fig. 2.1 – Composants de base du protocole NEMO BS

II.2.1 Délai du Handover L2

Puisque les handovers 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 :

$$T_{HO} = T_{L2} + T_{L3} \quad \textbf{(2.1)}$$

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 [4, 19, 20, 21].

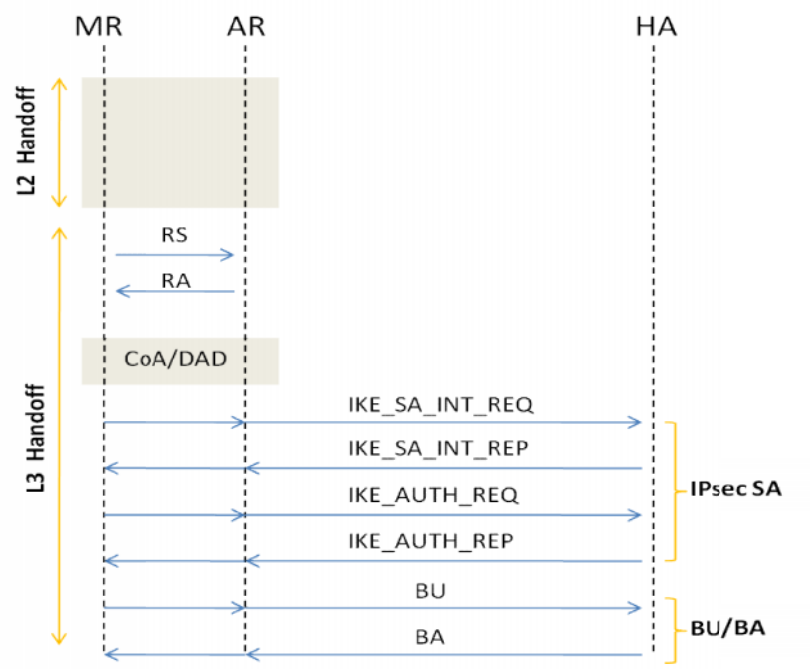

Fig. 2.2 – Procédures du handover NEMO BS

Il s'en suit :

$$T_{L2} = T_{scan} + T_{auth} + T_{ass} \quad \textbf{(2.2)}$$

Le handover L2 est déclenché par l'événement de lien Link_Down (voir chapitre III) correspondant à la condition suivante:

$$P_{rx} < P_{th} \quad \textbf{(2.3)}$$

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.2.2 Délai du Handover L3

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

1. Détection de Mouvement (Movement Detection , MD) : après avoir été déconnecté de l'ancien routeur d'accès (old AR, oAR), le MR détecte son mouvement grâce à l'information de préfixe contenue dans les messages reçus « Router Advertisement (RA) » [3] annoncés périodiquement par le nouvel AR (new AR, nAR). Le MR peut agir d'une façon proactive en envoyant des messages « Router Solicitation (RS) » [3] pour obtenir les messages RA des routeurs voisins. Le MR détecte son mouvement si le routeur oAR est inaccessible, i-e : aucun message RA provenant du oAR n'est reçu).

2. Assignation d'adresse CoA et test DAD : sur la réception de l'information de préfixe du nAR, le MR procède à la configuration automatique stateless [3] (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) [3]. 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, sinon 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 prés de son HA. Toutefois, comme indiqué par [10], tous les messages de signalisation entre le MR et le HA doivent être authentifiés par IPsec [15, 23]; 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) [82].

4. Enregistrement BU/BACK : Dès que le MR s'est auto-configurer avec une nouvelle et unique adresse CoA et qu'une association de sécurité est crée 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 :

$$T_{L3} = T_{MD} + T_{DAD} + T_{Reg} \quad \textbf{(2.4)}$$

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 :

$$T_{MD} = T_{RS} + T_{RA} \quad \textbf{(2.5)}$$

$$T_{Reg} = T_{SA} + T_{BU} + T_{BA} \quad \textbf{(2.6)}$$

Où:

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

En nous référant à la figure 2.2, nous pouvons exprimer T_{L3} en fonction de RTT_{MR-AR} et RTT_{AR-HA} , (RTT est le délai aller-retour : Round Trip Time) :

$$T_{L3} = 4\,RTT_{MR-AR} + T_{DAD} + 3RTT_{AR-HA} \quad \textbf{(2.7)}$$

II.2.3 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 2.3, 2.4 et 2.5.

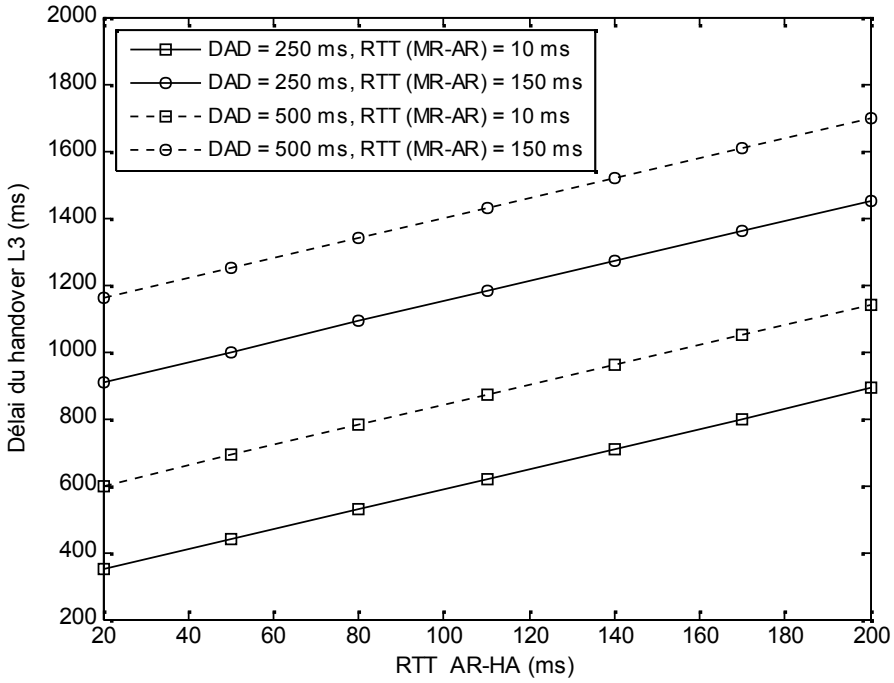

Fig. 2.3 – Délai du handover NEMO (handover L3)

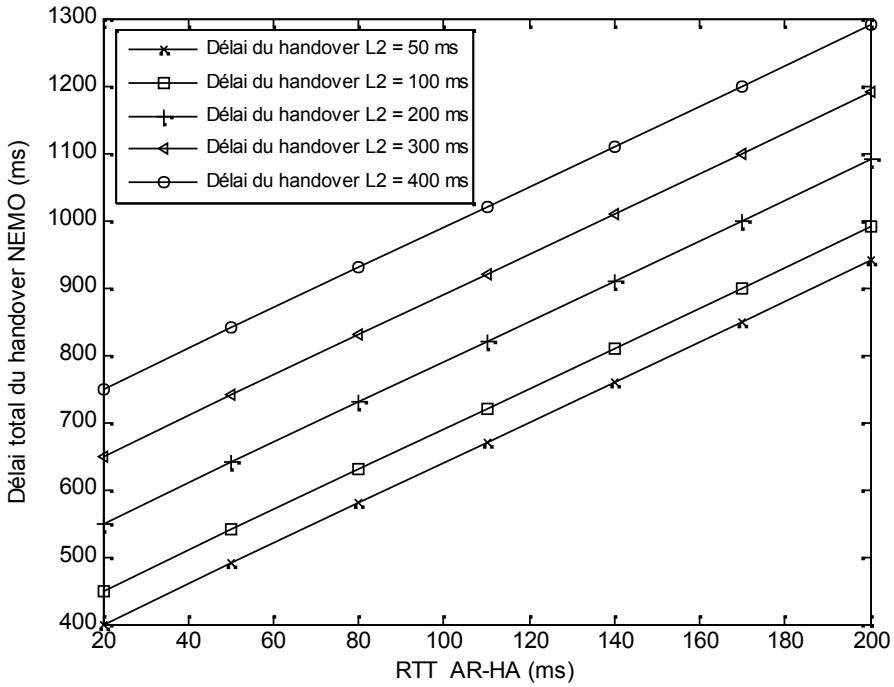

Fig. 2.4 – Délai total du handover NEMO (handover global)

La figure 2.3 représente le délai partial du handover NEMO concernant le niveau L3.
Pour le paramètre RTT_{MR-AR} , 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 RTT_{AR-HA} (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 [3].

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 2.4, 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 RTT_{MR-AR} 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 2.5 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.

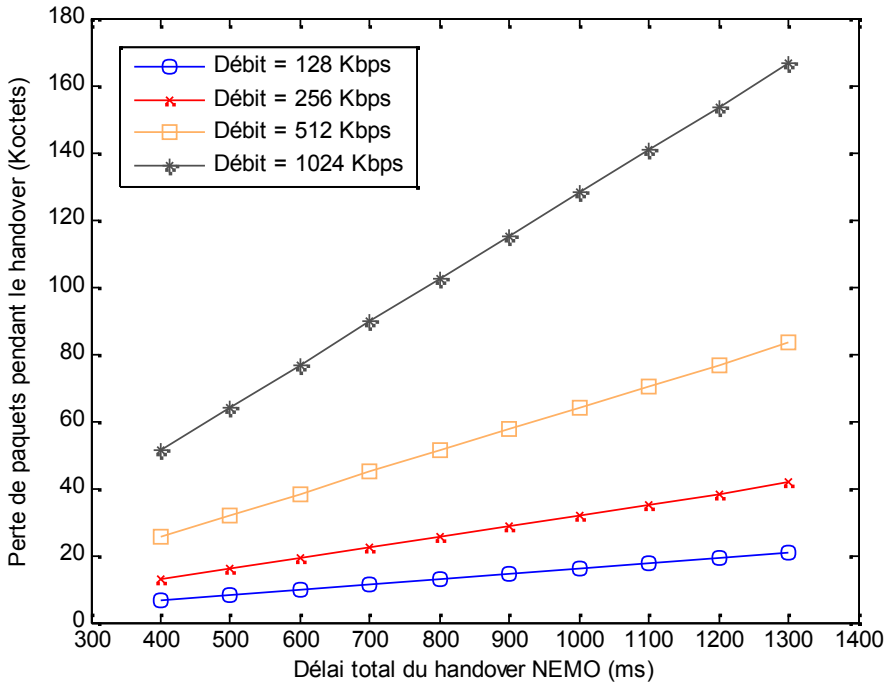

Fig. 2.5 – Perte de paquet pendant le handover NEMO

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 les quelles 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.3 Solutions proposées pour l'optimisation de NEMO BS

Les résultats que nous avons exposés plus haut montrent que le protocole NEMO BS [15] tel qu'il a été défini ne permet pas de fournir une continuité des services sans perturbation, causée notamment par un délai de handover et des pertes de paquets non négligeables.

Pour réduire l'impact de ce problème, plusieurs propositions d'optimisation de NEMO ont été faites. Dans ce qui suit, nous présentons les plus pertinentes.

II.3.1 RA rapides (Fast Router Advertisement) [36,37]

La détection du mouvement dans le protocole NEMO BS est réalisée lors de la réception d'un message « Router Advertisement, RA ». Le message RA est envoyé par les routeurs d'accès périodiquement sur le lien local ou en réponse à un message « Router Solicitation, SA ».

Dans le cas d'un RA non sollicité, le temps nécessaire à la détection dépend de la fréquence à laquelle le message RA est envoyé, cette fréquence est déterminée par le « délai de retransmission » qui donne la période entre deux émissions non sollicitées de ce message. Le protocole Neighbor Discovery d'IPv6, RFC 4861 [69] définit un minimum (MIN_DELAY_BETWEEN_RAS) de 3 secondes pour le « délai de retransmission », ce qui n'est pas adapté à une gestion rapide de la mobilité. Le protocole MIPv6 (et donc NEMO) suggère d'augmenter cette fréquence entre 0.030 s et 0.070 secondes, mais précise que ces valeurs ne doivent pas être utilisées par défaut afin de ne pas charger le lien. Avec une telle fréquence, il faut donc en moyenne 50 ms pour détecter le nouveau lien IPv6.

Pour le cas d'un RA sollicité, le routeur adressé doit retarder la réponse à un message « Router Solicitation » par un temporisateur aléatoire prédéfini [69], la valeur de celui-ci est de 0 à (MAX_RA_DELAY_TIME = 0.5) secondes.

L'impact de ce retard sur la détection de mouvement peut être sérieux. Même si en utilisant des triggers L2 une fois que le MR arrive à un nouveau sous-réseau pour déclencher immédiatement un message RS plutôt que d'attendre le prochain RA non sollicité, le RA sollicité est retardé. Un nouveau mécanisme [37] est proposé pour tenir compte des temps de réponse plus rapides dans le traitement des messages « Router Solicitation ». Un routeur d'accès est désigné sur chaque lien pour répondre immédiatement à la demande du MR. L'utilisation d'un seul routeur en tant que répondant rapide assure que les collisions ne se produisent pas. Le message « Router Advertisement » directement envoyé à l'adresse du MR sans délai est désigné sous le nom Fast Router Advertisement.

II.3.2 DAD optimisé (Optimistic Duplicate Address Detection, ODAD) [38]

Dans la phase d'auto-configuration sans état (stateless autoconfiguration) du handover NEMO, le MR combine le préfixe de réseau obtenu à partir du message RA avec un suffixe produit à partir de l'adresse MAC de son interface pour construire une nouvelle adresse. Cette adresse non testée est désignée sous le nom d'adresse tentative (Tentative Address). Le MR doit vérifier au préalable que cette adresse est unique sur le lien avant de pouvoir l'utiliser. Pour ce faire, il execute le test DAD (Duplicate Address Detection) en envoyant un message NS (Neighbor solicitation) avec comme adresse destination l'adresse tentative. Par défaut lors du DAD, un terminal émet un unique NS. Si au bout d'une seconde (valeur par défaut) il n'a pas reçu de NA (Neighbor Advertisement) lui indiquant que sa nouvelle adresse est déjà attribuée, il conclut qu'elle est unique sur le lien et peut désormais l'utiliser pour communiquer. Dans le meilleur des cas, le processus DAD introduit donc un délai supplémentaire d'une seconde.

Une nouvelle solution appelée ODAD (Optimistic Duplicate Address Detection) [38] est proposée pour supprimer les délais engendrés par le DAD. Cette proposition se base sur le fait que les adresses IPv6 ont de très faibles probabilités d'être dupliquées lorsqu'elles ont été obtenues par des mécanismes automatiques tels que l'auto-configuration d'adresses sans état du protocole IPv6. Le principe d'ODAD est donc d'autoriser les terminaux à utiliser directement leurs nouvelles adresses IPv6 tout en réalisant le DAD en parallèle. Appliqué au protocole NEMO, cela permet aux MRs d'envoyer un BU au HA dès la création des nouvelles adresses temporaires CoAs.

II.3.3 FMIPv6-NEMO [26]

Dans le travail intitulé ''Optimized FMIPv6 using IEEE 802.21 MIH Services in Vehicular Networks'' [26], les auteurs étudient le potentiel d'appliquer FMIPv6 dans les environnements véhiculaires, et en y apportant des optimisations en employant les services MIH IEEE 802.21 locaux et à distance avec les réseaux d'accès du voisinage.
Ils proposent d'employer un cache spécial au niveau du MR pour réduire le temps d'anticipation dans FMIPv6 et d'augmenter ainsi la probabilité du mode de fonctionnement prédictif. En outre, ils proposent un mécanisme inter-couche (cross-layer design) pour prendre des décisions intelligentes de handover dans FMIPv6.

Un container appelé « Heterogeneous Network Information (HNI) » est défini au niveau du MR pour stocker les informations L2 et L3 statiques et dynamiques des réseaux d'accès voisins obtenu par les services IEEE 802.21 MIIS remote.
Ces informations sont obtenues à partir d'un serveur d'information (IS : Information Server) situé sur le réseau d'accès (il s'agit d'une nouvelle entité proposé par les auteurs pour être intégré au sein de

l'infrastructure réseau). Une partie des informations du HNI maintenu par l'IS est répliquée au niveau des ARs afin de permettre à ces derniers de résoudre les informations L2 correspondant aux préfixes de sous-réseaux. Ceci élimine le besoin pour les ARs d'échanger l'information entre eux.

Le container HNI contient entre-autres les informations suivantes :
Le type de l'interface physique du RA (PoA PHY Type), l'adresse MAC du RA (PoA MAC Address), les canaux radio utilisés (PoA Channel Range), le type du réseau (Network Type), les tarifs (Costs), la sécurité du réseau (Network Security), le préfixe du sous-réseau du RA (PoA Subnet Prefix), etc. (PoA signifie Point of Attachement, c'est le router d'accès AR).

Les opérations du handover proposé sont comme suit :

- les messages RtSolPr/PrRtAdv prévus dans FMIPv6 ne sont plus utilisés, ils sont remplacés par les messages « MIH_Get_Information request/reply » (voir chapitre III).
- La procédure précédente est déclenché avant le déclenchement du trigger « MIH_Link_Going_Down » (i-e : chute du signal reçu et lien sur le point d'être rompu).
- Une fois que le trigger « MIH_Link_Going_Down » est déclenché, le MR explore son cache HNI et select un RA approprié pour y effectuer le handover.

Le délai du handover provoquée par la découverte des liens radio dans FMIPv6 peut être éliminé en ayant l'information L2. En outre, avec l'information L3, le MR apprendra les préfixes de sous-réseau du NAR et forment le NCoA avant le handover. Ceci élimine le temps de découverte des routeurs d'accès et optimise le délai du handover L3 dans FMIPv6.

A travers des résultats analytiques et de simulation, les auteurs montrent que leur proposition permet d'augmenter la probabilité du mode de fonctionnement prédictif et de réduire le délai global (L2 et L3) du handover. Un délai total du handover d'environ 250 ms est obtenu quand le véhicule a un mouvement lent (18 Km/s) et cette valeur augmente jusqu'à 350 ms quand la vitesse de véhicule atteint 90 Km/h.

II.3.4 ICE based NEMO [39]

Les auteurs de cette solution proposent une optimisation du handover dans le cas de configurations de réseaux NEMO multihomed grâce à une collaboration des différents routeurs. Les différents MRs qui sont situés à différentes positions dans le même réseau NEMO, peuvent exécuter le handover à des instants différents lorsque le réseau NEMO se déplace. Un MR qui n'est pas entrain d'exécuter le handover peut transporter le trafic adressé à autre MR exécutant le handover.
Une nouvelle entité appelée ICE (Intelligent Control Entity) est introduite dans l'infrastructure réseau pour la gestion du handover et des ressources réseau (les ARs). Les auteurs définissent un domaine

ICE qui contient un ICE et plusieurs ARs (Fig. 2.6). L'ICE collecte les informations concernant les routeurs d'accès ARs telles que l'adresse du RA, sa capacité, sa charge actuelle, les identités de ses APs et les adresses des MRs qui lui sont associés. L'ICE utilise ces informations pour déterminer le meilleur AR à servir un MR si celui-ci en détecte plusieurs. L'ICE collecte également des informations concernant les MRs afin de pouvoir choisir le meilleur MR (cas où plusieurs MRs sont candidats) pour transporter le trafic d'un autre MR pendant son handover.

En outre, les auteurs affirment que le handover sans couture (zéro délai et pertes très faibles) peut être réalisé si certains paramètres sont correctement configurés, à savoir la distance X entre deux MRs, la distance Y de la zone de recouvrement et la vitesse du réseau NEMO. En particulier, la distance (X+Y) doit être grande, ce qui restreint le champ d'application de la proposition.

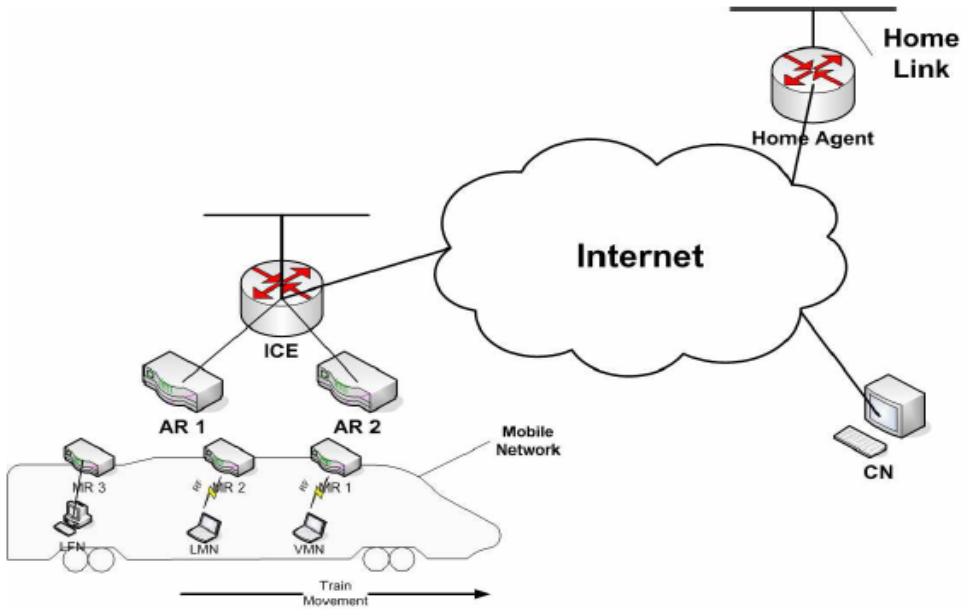

Fig. 2.6 – Architecture d'un domaine ICE [39]

II.3.5 Fast handover for a train-based mobile network [40]

Dans cette approche nommée MMRCFH (Multiple Mobile Router Cooperation Fast Handover) [40], les auteurs considèrent un réseau mobile NEMO multihomed de type train (train-based). Le réseau possède plusieurs MRs qui sont interconnectés d'une manière sécurisée. Les auteurs utilisent la terminologie de FMIPv6, mais leur approche est tout à fait différente. Quand un MR quitte un sous-réseau d'un routeur d'accès (AR) et entre dans un autre sous-réseau d'un autre AR, le premier est appelé PAR (Previous AR) et le second NAR (New AR). Les adresses temporaires CoA associées respectivement avec le PAR et le NAR sont notées PCoA et NCoA.

L'objectif de MMRCFH est d'obtenir l'adresse NCoA avant le handover et de permettre au MRs de recevoir pendant la période du handover les paquets par un autre MR. Pour cela, il utilise les caractéristiques du transport par les voies ferroviaires (les lignes ferroviaires sont fixes et le

mouvement du train est régulier). Aussitôt qu'un MR (MR1 sur la figure 2.7) a détecté qu'il s'est déplacé par rapport à un PAR, il informe le PAR via l'autre MR (MR2 toujours connecté au PAR). de rediriger ses paquets vers MR2. Lorsque le MR1 complète son handover, il aide MR2 à exécuter un handover sans pertes au NAR. Avec cette proposition, les auteurs ont réalisé une amélioration du délai du handover à environ 230 ms.

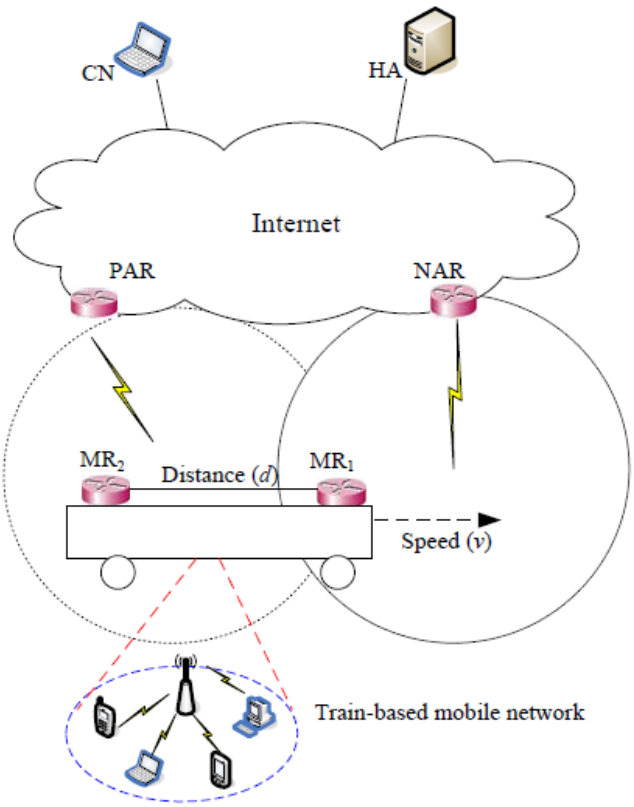

Fig. 2.7 – Principe de base de MMRCFH

II.3.6 GPS Aided Predictive Handover [41]

Dans cette approche, les auteurs proposent d'utiliser le GPS [67] pour assister un réseau mobile NEMO multihomed à prédire les handovers. L'idée est la suivante : pendant que le réseau se déplace le long d'un chemin, il enregistre dans une base de données toutes les données reliées aux réseaux d'accès.

La prochaine fois que, quand le réseau se déplace le long du même chemin, l'information stockée peut être employée pour prévoir et préparer les handovers. L'information, qui devrait être stockée, comprend : le type du réseau d'accès, son identificateur et l'information concernant le préfixe utilisé.

Ainsi, en se basant sur des coordonnées GPS réelles et des données précédemment enregistrées, un système multihomed peut prévoir l'apparition des réseaux et se préparer aux handovers.

Sur la base de résultats expérimentaux, les auteurs affirment que la solution proposée a permis d'éliminer presque totalement le délai du handover [41]. L'approche utilisée par les auteurs est intéressante, cependant son application est restreinte aux scénarios de mouvements répétés.

II.7 Conclusion

Dans ce chapitre, dans un premier temps, nous avons mis en évidence les limites de performance du handover NEMO BS notamment par son délai et ses pertes de paquets élevés et inappropriés pour les applications à contraintes de temps. L'étude analytique que nous avons menée des différents composants du protocole NEMO BS à savoir la détection de mouvement, l'acquisition d'une adresse temporaire CoA valide et l'enregistrement au niveau du HA, a montré que ce protocole cause à lui seul un délai de handover minimal d'environ 350 ms. En cumulant les délais des handovers L2 et L3, le délai minimal du handover global est estimé à 400 ms (pris pour des conditions extrêmement favorables), le délai moyen étant de 1250 ms. Les pertes qui en découlent dépendront du débit du transfert des données de l'application.

Ceci étant, nous avons survolé dans un second temps, quelques propositions d'extensions du protocole NEMO BS ayant trait en particulier à l'optimisation du handover. Les premières améliorations faites d'ailleurs pour MIPv6, ont porté sur les phases de détection de mouvement et d'auto-configuration (Fast RA, ODAD). [42] considère que le handover de NEMO même avec ces optimisations n'est pas suffisant pour les applications à performances critiques.
Ensuite, il ya eu d'autres optimisations qui sont dépendantes soit de l'infrastructure réseau (ajout de nouvelles entités pour assistance du handover) soit des applications NEMO déployées. La plus pertinente de ces proposition nous semble-t-il est celle correspondant à l'extension de NEMO avec les fonctionnalités de FMIPv6 et l'appui des services MIH 802.21. Toutefois, les performances atteintes demeurent toujours insuffisantes pour garantir un handover sans couture.
Le chapitre suivant présentera le multihoming, une approche incontournable pour répondre aux besoins de performance de handover pour les applications temps réel et exigeantes en QoS, et introduira le standard IEEE 802.21.

CHAPITRE 3

Le Multihoming dans les Réseaux NEMO Standard IEEE 802.21

III.1 Introduction

Pour assurer une connectivité permanente à Internet, à tout moment et en tout lieu, un réseau mobile NEMO est de préférence meilleur s'il est connecté via plusieurs interfaces et à travers plusieurs technologies à des réseaux d'accès distincts, ceci est traduit par le concept de multi-domiciliation (multihoming) [28].

Dans un sens général, le multihoming est une technique de fiabilité et d'accroissement de performance par des liens redondants. En vertu de NEMO, le multihoming prend la forme de multiples HAs, de multiples MRs, de multiples préfixes MNPs, ou des combinaisons d'eux. Le multihoming a le potentiel pour assurer l'équilibrage de charge, la tolérance aux pannes et la bande passante accrue [28].

Le protocole NEMO BS [15] est une extension de MIPv6 [10] pour la prise en charge de la mobilité d'un réseau NEMO desservi par un seul routeur mobile (MR), il ne supporte pas donc le multihoming.

Le développement de supports de mobilité pour les réseaux NEMO multihomed est un champ de recherches largement exploré en raison de son importance dans les applications d'un internet omniprésent. Toutefois, le multihoming est un problème difficile à résoudre en raison des nombreux cas complexes de multihoming.

Le Groupe de travail NEMO-WG a analysé ces complexités dans un projet Internet [28], mais laisse la solution comme travail en dehors de la portée du groupe de travail.

Le multihoming se rapporte donc à la situation dans laquelle un nœud a plusieurs adresses IP permettant de fournir ses localisations dans la topologie Internet. Dans le contexte NEMO, cette situation est possible si le réseau NEMO peut être simultanément relié à l'Internet par l'intermédiaire de plusieurs routeurs mobiles, ou par l'intermédiaire d'un seul routeur mobile multi-interfaces (disposant de plusieurs interfaces, de même technologie ou de technologies différentes). Les différentes interfaces (cas de plusieurs routeurs ou un seul routeur) peuvent être en activité simultanément. Cela permet de pallier aux pannes, de partager les charges, de mettre en place des préférences ou plus simplement de garantir un meilleur accès à l'Internet en faisant appel à plusieurs technologies. Ce dernier cas de figure est très intéressent dans la mesure où il nous permettra d'exécuter des handovers soft, pour maintenir les sessions ouvertes et assurer par conséquent une connectivité sans couture (le temps d'interruption et les pertes de paquets dus au handover peuvent être fortement réduits). La fonctionnalité de multihoming nécessite donc de considérer les aspects de changement d'interface et de changement de routeur mobile.

Ce chapitre décrit d'une part le multihoming dans le contexte de réseaux NEMO, ses bénéfices et les issues qui en découlent. Comme il y a beaucoup de situations dans lesquelles les réseaux NEMO peuvent être multihomed, une taxonomie est proposée afin de classifier les configurations de multihoming possibles, parmi lesquelles nous choisirons deux pour développer nos propositions de handovers sans couture pour les applications temps réels et exigeantes en QoS. D'autre part, nous examinerons les spécifications du standard MIH IEEE 802.21 [68], celui-ci nous permettra d'optimiser le handover dans un environnement d'accès hétérogène pour un routeur mobile multihomed supportant les technologies (IEEE 802.11 [43], IEEE 802.16 [44], 3GPP [45] et 3GPP2 [46]).

III.2 Bénéfices du multihoming

Les avantages pour un réseau mobile supportant les fonctionnalités du multihoming [28] peuvent être brièvement résumées comme suit :

III.2.1 Tolérance aux pannes/Redondance

La tolérance aux pannes/Redondance (Fault-Tolerance/Redundancy) est définie comme le comportement dans le quel les fonctionnalités du réseau sont assurées par les composants secondaires du système lorsque le composants primaire devient hors service.

Ceci est probablement l'avantage le plus important dans le sens ou l'investissement dans une solution de multihoming fera gagner au moins ce bénéfice. La forme la plus simple de la tolérance aux pannes à utiliser un lien d'accès pendant l'opération normale et la migration du trafic à un autre quand le lien devient inutilisable.

Ainsi, quand le réseau NEMO est multihomed et au moins deux tunnels avec les Homes Agents sont disponibles, si l'un d'eux échoue, le trafic est pris en charge par un autre et la continuité de connexion pour les MNNs est garantie.

III.2.2 Partage de charge

Le partage de charge (Load Sharing) est défini comme la répartition des trafics émis et reçus par les Nœuds MNNs sur plusieurs tunnels ouverts simultanément. Dans le cas du protocole NEMO BS, la charge du trafic du réseau est totalement émise sur un itinéraire. Malheureusement, quand cette charge est trop lourde à manipuler par une seule interface, cela aurait comme conséquence une congestion élevée et une perte énorme de données.
Cependant, avec l'appui du multihoming, plusieurs interfaces peuvent être employées pour écouler le trafic du réseau NEMO. Le partage de charge exige l'établissement de plusieurs tunnels qui seront utilisés simultanément. Il peut être établi statiquement ou dynamiquement.

III.2.3 Politique de routage

La politique de routage (Routing Policy/Path selection/Preference Settings) : est définie comme la capacité d'un utilisateur ou une application à choisir la technologie de transmission ou le réseau d'accès préféré sur la base du coût, de la bande passante, du délai, du RTT ou d'une politique prédéfinie. Ceci peut être établi statiquement ou dynamiquement, et initié par le MR, le HA ou même le MNN.

III.2.4 Agrégation de bande passante

L'agrégation de bande passante (Aggregate Bandwidth) permet de fournir à l'utilisateur ou à l'application plus de largeur de bande. Les interfaces multiples qui sont reliées à différents réseaux d'accès peuvent augmenter la bande passante totale disponible.

III.2.5 Bicasting

Le Bi-casting peut être utilisé pour réduire typiquement pour le trafic en temps réel, les pertes de paquets et les délais de livraison provoqués par les congestions. Le bi-casting fait une duplication d'un flux de données particulier et les envoie simultanément par différents itinéraires (tunnels).

III.3 Classification des configurations multihoming possibles

Comme il y a plusieurs configurations dans lesquelles les réseaux mobiles sont multihomed, il est nécessaire de les classer en taxonomie clairement définie. Cela peut être fait de différentes manières :

- Taxonomie orientée Propriétés (Ownership-Oriented Approach)
- Taxonomie orientée Problèmes (Problem-Oriented Approach)
- Taxonomie orientée Configurations (Configuration-Oriented Approach)

Seule la taxonomie orientée Configurations est décrite dans cette section. Les deux autres peuvent être consultés dans la RFC 4980 [28].

Il y a différentes configurations d'un réseau mobile multi-domicilié, selon le nombre de routeurs mobiles MRs présents, selon le nombre d'interfaces externes (egress interfaces) et d'adresses mères (HoAs) dont le routeur dispose et selon les préfixes de sous-réseau MNPs annoncées pour les nœuds MNNs.
Trois principaux paramètres de différenciation des configurations multihoming possibles sont identifiés. Avec ces paramètres, nous pouvons nous référer à chaque configuration par le triplet (x,y,z) où les paramètres x, y et z sont définis comme suit:

- x indique le nombre de MRs, où: x = 1 implique que le réseau mobile NEMO n'a qu'une seul MR multi-interfaces, et x = n signifie que le réseau a plus d'un MR.
- y indique le nombre de de HAs, où: y = 1 implique qu'un HA unique est attribué au réseau mobile NEMO pour la gestion des binding updates, et y = n signifie que plusieurs HAs sont affectées au réseau mobile.
- z indique le nombre de préfixes MNPs attribués au réseau mobile NEMO, où: z = 1 indique que seule une MNP est disponible dans le réseau NEMO, et z = n implique que plusieurs MNPs sont disponibles dans le réseau NEMO.

III.3.1 Configuration (1,1,1)

Dans cette configuration, le réseau NEMO admet un seul MR associé à un seul HA et un seul MNP est délégué au MR (Fig. 3.1). Ce cas est l'un des configurations les plus typiques. Le réseau NEMO est multihomed si son MR est multihomed, c'est-à-dire si le MR admet plusieurs interfaces. Chaque interface est liée à une adresse CoA. Un tunnel doit être établi entre chaque Interface (CoA) et le HA.

D'un point de vue d'extension du protocol NEMO, les issues suivantes sont à considérer :

1. Enregistrement de multiples CoAs au niveau du même HA. La RFC 5648 [47] a apporté une solution à ce problème (MCoA : Multiple Care-of Addresses Registration).
2. Support pour l'activation et/ou la commutation des tunnels.
3. Des mécanismes efficaces de détection de rupture de liens sont également nécessaires. A ce sujet, les mécanismes développés dans le standard IEEE 802.21 [68] conviennent parfaitement à ce cas de figure (voir section III.5). Nous reviendrons sur ce cas dans notre proposition de handover sans couture basé sur le modèle (1,1,1) présentée au chapitre 5.

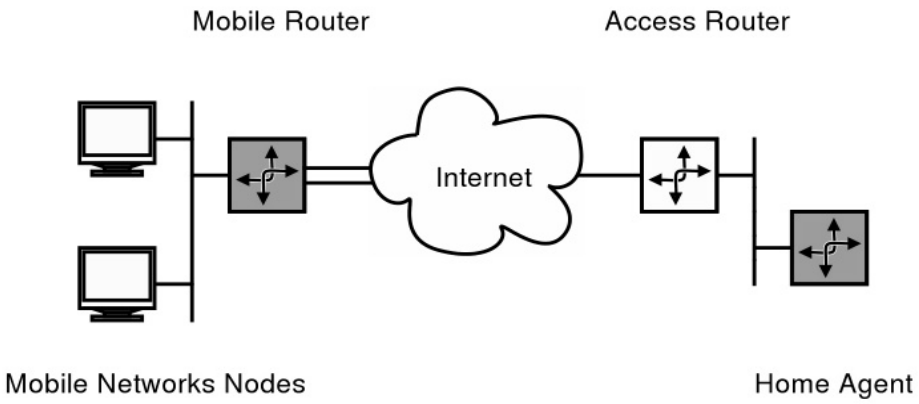

Fig. 3.1 – Configuration (1,1,1) : un MR, un HA et un MNP

III.3.2 Configuration (n,1,1)

Dans cette configuration, le réseau NEMO présente plusieurs MRs, un seul HA et un seul MNP (Fig. 3.2).

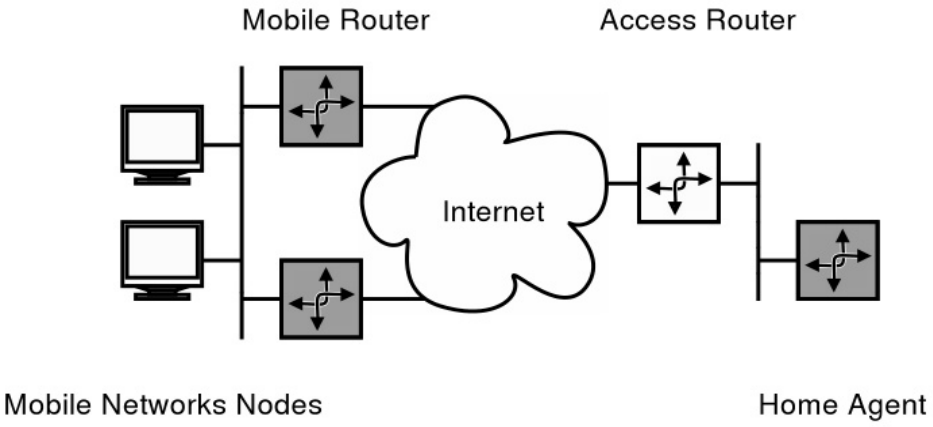

Fig. 3.2 – Configuration (n,1,1) : multiple MR, un HA et un MNP

Un tunnel bi-directionnel doit être établi entre chaque MR et le HA. D'un point de vue de mobilité de réseau, ce cas est semblable au précédent, ainsi les mêmes recommandations s'appliquent sauf pour le mécanisme (MCoA) qui n'est pas nécessaire. Cependant, la présence d'une entité au sein du réseau NEMO pour gérer les MRs et leurs tunnels est nécessaire. Cette entité sera soit intégrée à un des MRs ou soit complètement indépendante.

III.3.3 Configuration (1,n,1)

Cette configuration implique seulement un seul MR, et un seul MNP est disponible dans le réseau NEMO. Cependant, le MR est associé à de multiples HAs (Fig. 3.3). Le groupe de travail NEMO WG considère uniquement le cas où les HAs appartiennent au même domaine, cela facilite que le même MNP soit annoncé. Le MR doit donc être multihomed (plusieurs interfaces externes). Il doit établir un tunnel avec chaque HA à travers chacune de ses interfaces. En plus des points 2 et 3 présentés pour la configuration (1,1,1) qui sont recommandés, un module d'extension de NEMO au niveau du MR pour la gestion des différents tunnels avec les HAs est nécessaire.

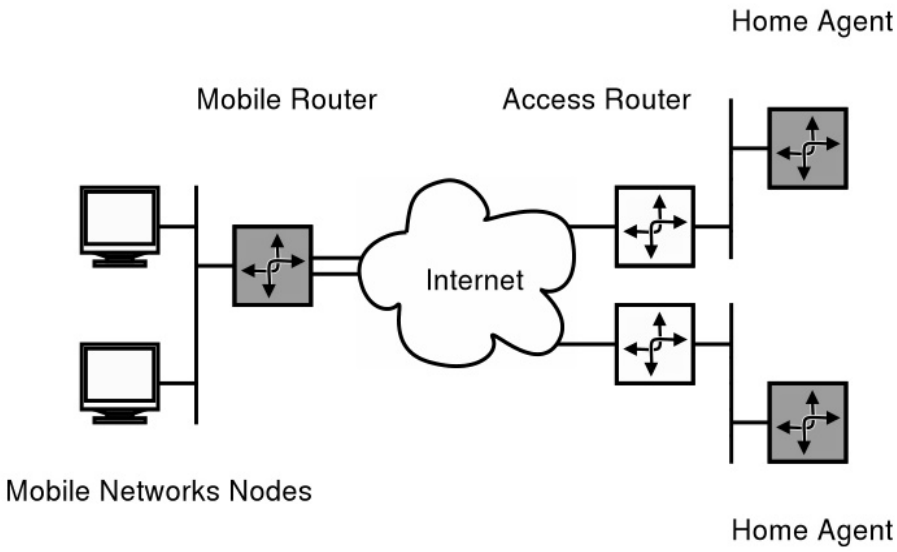

Fig. 3.3 – Configuration (1,n,1) : un MR, multiple HAs et un MNP

III.3.4 Configuration (n,n,1)

Dans cette configuration, plusieurs MRs desservent le réseau NEMO, chaque MR admet son HA, et un seul MNP est disponible dans le réseau NEMO (Fig. 3.4). Ce cas est semblable au précédent sauf que les HAs peuvent appartenir à différents domaines.

Les mêmes recommandations sont donc valables, en plus une entité pour gérer les MRs et leurs tunnels est nécessaire. Nous reviendrons sur ce cas dans notre proposition de handover sans couture basé sur le modèle (n,n,1) présentée au chapitre 4.

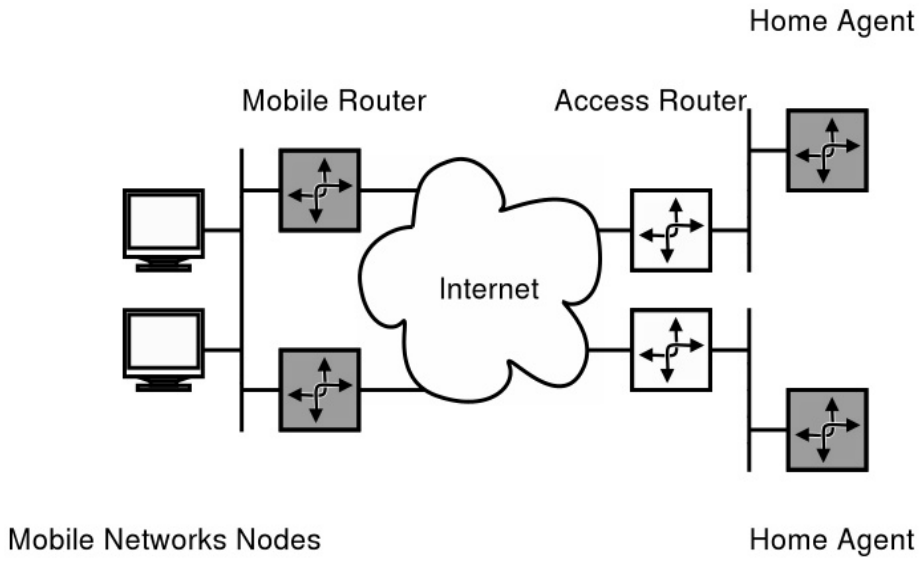

Fig. 3.4 – Configuration (n,n,1) : multiple MRs, multiple HAs et un MNP

III.3.5 Configuration (1,1,n)

Dans cette configuration, le réseau NEMO a un seul MR qui est associé à un seul HA, mais deux MNPs ou plus sont disponibles dans le réseau NEMO (Fig. 3.5).

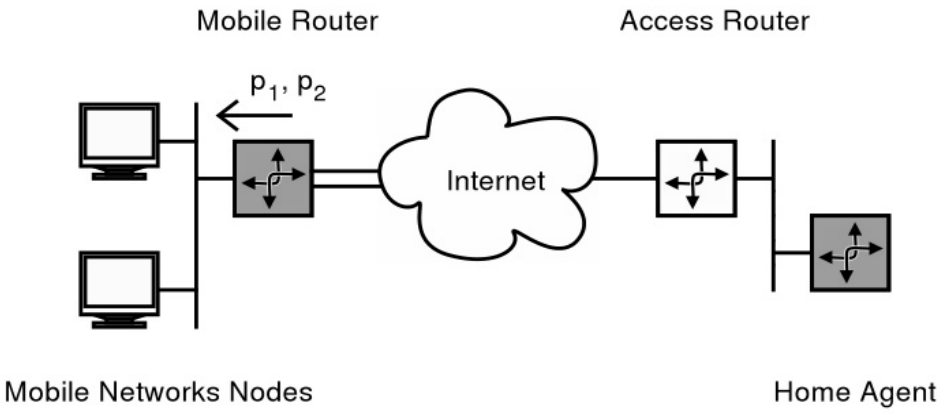

Fig. 3.5 – Configuration (1,1,n) : un MR, un HA et multiple MNPs

Le MR doit être multihomed. Ce cas est très similaire au cas (1,1,1), les mêmes recommandations donc sont valables. Considérant les MNNs dans le réseau NEMO, ils sont multihomed au vu de l'annonce de plusieurs MNPs. Ils s'auto-configurent alors avec une adresse globale de chaque MNP disponible sur leur lien (MR). Les MNNs peuvent maintenir leurs adresses IP sources lors d'un changement de tunnel puisque tous les MNPs sont annoncés par le même MR et délégués par le même HA.

III.3.6 Configuration (n,n,n)

Ce cas de figure est plus complexe, nous notons la présence de plusieurs MRs, plusieurs HAs et plusieurs MNPs. Les cas complexes incluent également les configurations (n,1,n) et (1,n,n). En dépit de l'utilisation du multihoming, ces configurations ne permettent pas de garantir le maintien des sessions. Les problèmes qui en sont les causes sont liés à :

- Mécanisme de filtrage d'entrée (Ingress filtering) : les adresses sources sont filtrées par les routeurs d'accès ARs, par les HAs et même par les MRs. En conséquence, chaque tunnel ne pourra véhiculer que les trafics correspondant à un seul préfixe MNP.

- La sélection des adresses sources par les MNNs : si un tunnel est rompu, un autre doit être utilisé, et puisque les préfixes MNPs sont soit annoncés par déférents MRs ou délégués par différents HAs, les MNNs doivent changer leurs adresses IP sources, ce qui a pour conséquence des interruptions de sessions déjà établies.

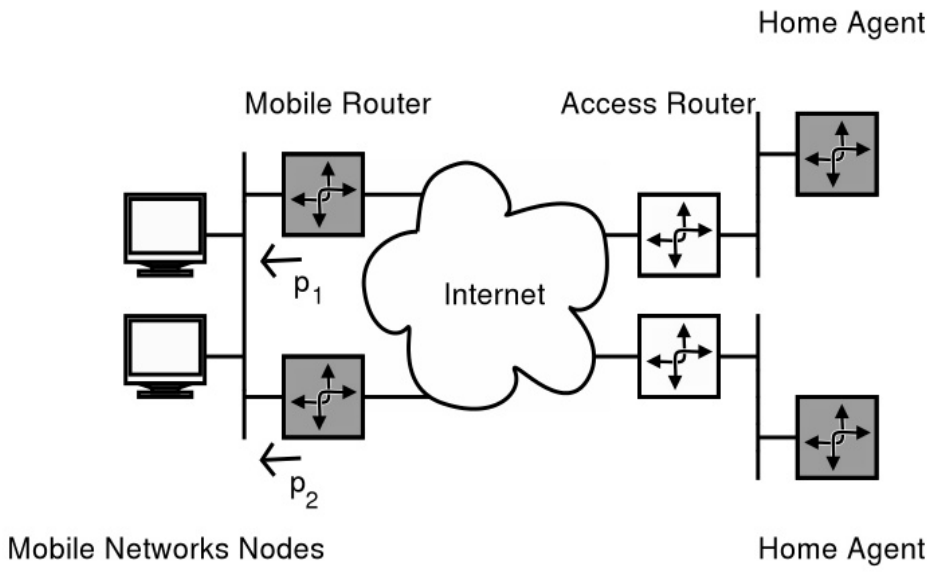

Fig. 3.6 – Configuration (n,n,n) : multiple MRs, multiple HAs et multiple MNPs

III.4 Issues du Multihoming

III.4.1 Détection de rupture de tunnel (Failure Detection)

En raison de l'utilisation de liens radio, les ruptures de tunnels sont majoritairement causées par les ruptures des liens d'accès. D'où, des mécanismes efficaces de détection de pannes et de rupture de liens sont nécessaires au niveau du réseau NEMO. Le standard IEEE 802.21 [68] apporte une solution à ce problème dans le cas d'un routeur mobile multihomed utilisant les technologies (IEEE 802.11, IEEE 802.16, 3GPP et 3GPP2). D'autres mécanismes doivent être élaborés suivant les cas de déploiement de réseaux NEMO multihomed et qui pourront éventuellement s'appuyer sur la norme IEEE 802.21.

III.4.2 Exploration de chemins (Path Exploration)

Une fois un échec dans le chemin actuellement utilisé est détecté, des chemins alternatifs doivent être explorés afin d'identifier ceux qui sont disponibles. Cela peut se faire par exemple en maintenant des caches pour les chemins alternatifs et l'exécution d'un test keepalive (test de survivabilité) permettant de mettre à jour l'état des tunnels disponibles.

III.4.3 Sélection de chemin (Path selection)

Un mécanisme de sélection de chemin est exigé pour choisir parmi les multiples chemins disponibles. Selon la configuration multihoming de NEMO impliquée, les différences entre les chemins peuvent affecter uniquement la partie entre le MR et le HA, ou elles peuvent affecter le chemin de bout en bout.
En outre, selon la configuration, la sélection de chemin peut être exécutée par le HA, le MR, ou les MNNs eux-mêmes par le choix d'adresse source.

III.4.4 Re-Homing

Après qu'une panne ait été détectée et un chemin alternatif disponible a été identifié, un aiguillage des communications existantes sur le nouveau chemin choisi doit se faire. Ce procédé change fortement selon la configuration multihoming de NEMO.

Pour les configurations (*, *, 1), le procédé de re-homing implique seulement le MR et le HA. L'échange de messages additionnels autres que les BU est nécessaire. Nous verrons plus dans les chapitres 4 et 5, pour les configurations respectivement (n,n,1) et (1,1,1) les mécanismes d'activation et de commutation des tunnels que nous avons développés et utilisés pour l'aiguillage des communications courantes lorsqu'une panne ou une rupture de lien est détectée.
Pour les cas (*, *, n), en plus des mécanismes précédents, des mécanismes de bout en bout peuvent être exigés. De tels mécanismes peuvent impliquer une certaine forme de signalisation de bout en

bout ou tout simplement reposer sur l'emploi d'adresses sources différentes pour les communications en cours.

III.4.5 Filtrage d'entrée (Ingress Filtering)

Le principe du filtrage d'entrée (Network ingress filtering [48]) est relativement simple, les filtres d'entrée sont placés sur les routeurs de bordure de l'ensemble des ISP (Internet Service Provider). Lorsqu'un paquet avec une adresse IP source ne correspondant pas à l'adresse du réseau desservi tente d'accéder à l'extérieur via ce routeur, il est bloqué par le filtre. Il est bien évident que pour être efficace, cette méthode doit être appliquée par l'ensemble des acteurs du réseau Internet.

Donc, les mécanismes de filtrage d'entrée peuvent agir sur les paquets sortants quand les tunnels bidirectionnels multiples finissent vers des HAs différents. Ceci pourrait en particulier se produire si des préfixes MNPs différents sont manipulés par des MRs différents. Si un paquet avec une adresse IP source configurée d'un MNP spécifique est envoyé sur un tunnel à un HA qui ne manipule pas ce MNP, le paquet peut être rejeté par le HA ou par un routeur de bordure dans le réseau mère.

L'issue de filtrage d'entrée dépend fortement des configurations multihoming de NEMO. Pour le cas (*, *, 1), il n'y a pas une telle issue, puisqu'il y a un seul MNP. La même constatation est faite pour les cas (1, 1, *) et (n, 1, 1), il n'y a pas un tel problème, puisqu'il y a un seul HA acceptant tout le MNPs.

Le problème par contre se pose pour les configurations (n,1, n) et (*, n, n).

III.4.6 Source Address Selection

Dans les configurations (*, *, n), les MNNs seraient configurées avec plusieurs adresses issues de différents MNPs. Les mécanismes de choix d'adresses de source sont nécessaires. C'est une issue générale qui concerne n'importe quel nœud quand des préfixes multiples sont offerts. Cependant, les mécanismes actuellement disponibles de choix d'adresses sources ne pas permettre pas aux MNNs d'acquérir l'information suffisante pour choisir leurs adresses sources intelligemment. Le choix d'adresse appropriée peut être influencé par beaucoup de paramètres : préférences d'utilisateur, filtrage d'entrée, préfixe de destination, type d'interface, caractéristiques de lien, etc…Un mécanisme de choix d'adresse est donc nécessaire.

III.4.7 Support MCoA (Multiple Bindings/Registrations)

Quand un MR multihomed obtient plusieurs adresses CoAs multiple, il est souvent nécessaire pour lui de lier ces CoAs au même MNP. C'est une issue de mobilité générique, les nœuds IPv6 mobiles font face au même problème. Le protocole NEMO BS ne supporte pas donc cette fonctionnalité.

A noter que les solutions comme MCoA proposée par [47] peuvent résoudre ce problème. D'ailleurs, notre proposition présentée dans le chapitre 5 s'appuie sur ce dernier mécanisme.

III.5 Standard IEEE 802.21 : Vue d'ensemble

La norme IEEE 802.21 a été récemment mise au point pour le traitement des handovers dans les réseaux hétérogènes, également appelé Media-Independent Handover (MIH) [68]. La norme devrait permettre aux nœuds mobiles multihomed de tirer pleinement parti des chevauchements et de la diversité des réseaux d'accès. Elle fournit pour les nœuds multi-interfaces (IEEE 802.11 a/b/g/n, IEEE 802.16, 3GPP/3GPP2), un cadre pour la découverte des réseaux dans le voisinage de manière efficace et pour l'exécution de handovers hétérogènes intelligents entre ces différents réseaux en fonction de leurs capacités respectives et les conditions actuelles des liens.

III.5.1 Architecture générale du MIH

L'élément de noyau de l'architecture de MIH est la MIHF (MIH Function) qui est une interface logique entre la couche L2 et les couches plus élevées (Fig. 3.7). La MIHF qui peut être vu comme une couche L2.5 aide dans le choix de prise de décision de handover et de sélection de lien par la couche L3 et les couches supérieures en leur fournissant des services abstraits. Les couches supérieures (y compris les modules de gestion de mobilité tels que MIPv6 et NEMO, IP, protocoles de transport et applications) sont des MIH Users. Les MIH Users communiquent avec le MIHF par l'intermédiaire de MIH_SAP (Media Independent Service Access Points). D'autre part, Le MIHF interagit avec les couches L1/L2 via MIH_LINK_SAP spécifique pour chaque technologie (Fig. 3.8). Les MIHF locale et distante communiquent via MIH_NMS_SAP.

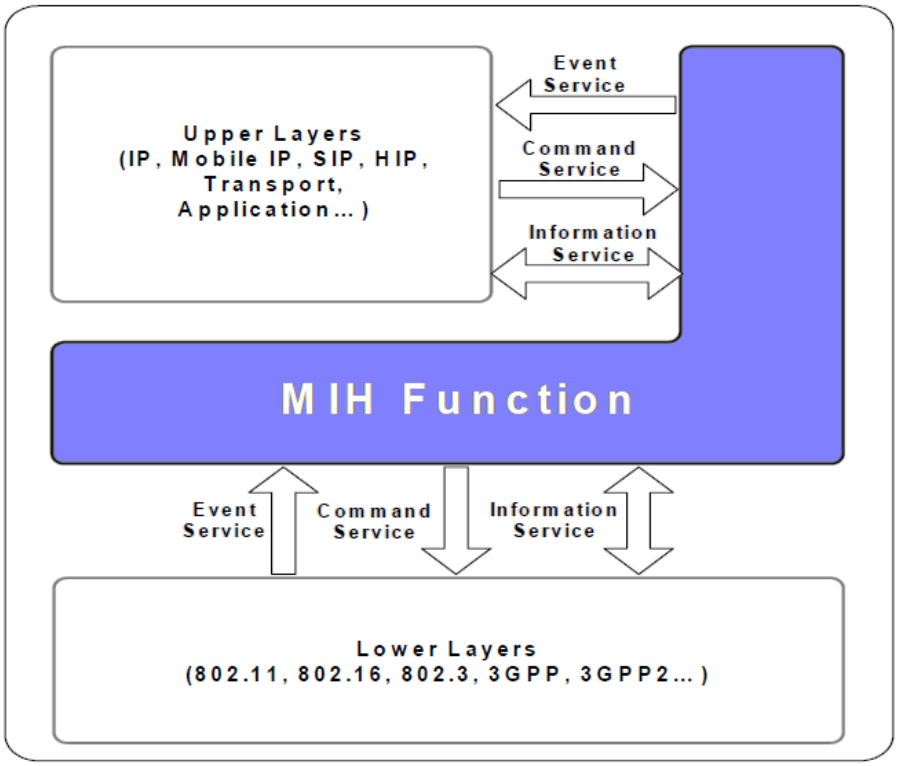

Fig. 3.7 – Architecture générale de la MIH IEEE 802.21 [68]

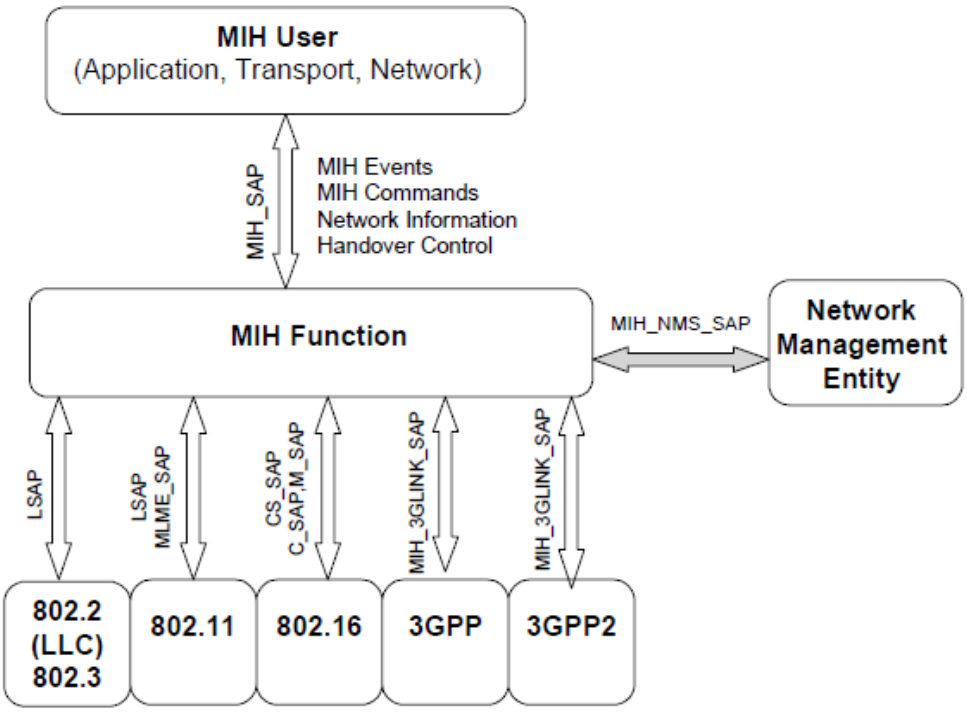

Fig. 3.8 – Interaction inter-couches (Service Access Points) [68]

III.5.2 Services MIH

La MIHF fournit trois types de services qui facilitent les handovers à travers les réseaux hétérogènes :

- Les services d'événements : MIH Event Services (MIES)
- Les services de commande : MIH Command Services (MICS)
- Les services d'information : MIH Information Services (MIIS)

Cette section fournit une description générale de ces services.

III.5.2.1 MIES - Media Independent Event Service

En général les handovers peuvent être initiés soit par le dispositif mobile (MN ou MR) ou par le réseau. Les événements qui peuvent déclencher le handover peuvent provenir de la couche MAC, de la couche PHY ou de la MIHF du mobile ou du point d'attachement. Ainsi, la source de ces événements peut être locale ou à distance (remote).

Le service d'événement ES peut être globalement divisé en deux catégories (Fig. 3.9) : événements de lien (Link Event) et événements MIH (MIH Event).

Les deux événements de lien et MIH traversent typiquement d'une couche inférieure à une couche plus élevée. Les événements de lien sont définis comme événements qui commencent de la source d'événement les entités au-dessous de MIHF et se terminent typiquement à MIHF.

Au niveau de MIHF, les événements de lien peuvent être encore propagés, avec ou sans traitement additionnel, aux entités des couches supérieures qui se sont inscrites à l'événement spécifique. Les événements qui sont propagés par le MIHF aux couches supérieures sont définis comme événements MIH.

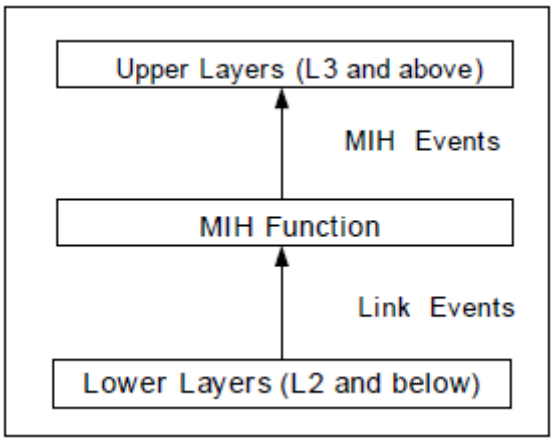

Fig. 3.9 – Evénement de lien et événement MIH [68]

III.5.2.1.1 Types d'événements

Le service MIES peut supporter plusieurs types d'événements :

- Evénements de changement d'état MAC et PHY (MAC and PHY State Change events)
- Evénements des paramètres de lien (Link Parameter events) : Ces événements sont dus au changement des paramètres du lien.
- Evénements de prédiction (Predictive events) : Les événements prédictifs expriment la probabilité du changement des propriétés à l'avenir basées sur les conditions passées et présentes.
- Evénement de synchronisation de lien (Link Synchronous events) : Ces événements donnent des indications aux couches supérieures au sujet des activités de la couche liaison
- (non relié à tout changement d'état de MAC/PHY) qui sont appropriés dans la gestion de mobilité par les couches supérieures.
- Evénements de transmission de lien (Link Transmission events) : Ces événements indiquent le statut de transmission (par exemple, succès ou échec) d'un paquet par la couche de liaison.

III.5.2.1.2 Evènement Local/Remote

Les événements locaux sont propagés à travers différentes couches dans la pile locale d'un dispositif. Tous les événements sont locaux en nature. Les événements à distance sont des indications qui traversent le réseau d'une MIHF à une autre MIHF. Les événements MIH peuvent être locaux ou à distance. Les événements à distance MIH commencent au niveau de la MIHF distante. Ils traversent le support vers la MIHF locale et puis ils sont expédiés au MIH Users qui ont souscrit pour ces événements dans la pile locale.

III.5.2.1.3 Liste des événements

Les événements de lien et MIH définis sons résumés dans le tableau (Tableau 3.1).

No	Type	Nom	Local/ Remote	Description
1	Lien MIH Changement d'état	Link Up MIH Link Up	L,R	La connexion L2 est établie et le lien est disponible pour l'usage
2	Lien MIH Changement d'état	Link Down MIH Link Down	L,R	La connexion L2 est rompue et le lien n'est pas disponible pour l'usage
3	Lien MIH Prédiction	Link Going Down MIH Link Going Down	L,R	L'état de lien dégrade et la perte de connexion est imminente
4	Lien MIH Changement d'état	Link Detected MIH Link Detected	L,R	Un nouveau lien a été détecté
5	Lien MIH Changement de paramètres	MIH Link Parameters Change MIH Link Parameters Report	L,R	Les paramètres de lien ont croisé seuil spécifié
6	Lien MIH Administratif	Link Event Rollback MIH Link Event Rollback	L,R	L'événement précédent doit être ignoré
7	Lien MIH Transmission de lien	Link SDU Transmit Status MIH Link SDU Transmit Status	L	Indiquer le statut de transmission des segments PDU (Packet Data Unit)
8	Lien MIH Synchronisation de lien	Link Handover Imminent MIH Link Handover Imminent	L,R	Le handover L2 est imminent basé sur des changements des états de lien
9	Lien MIH Synchronisation de lien	Link Handover Complete MIH Link Handover Complete	L,R	Le handover L2 à un nouveau point d'attachement a été accompli

Tableau 3.1 – Liste des événements

III.5.2.2 MICS - Media Independent Command Service

Le service MICS se rapporte aux commandes envoyées des couches plus élevées aux couches inférieures. Les commandes sont passées soit du MIHF à la couche L2, soit du MIH User à la MIHF.

Les services de commande sont utilisés pour déterminer le statut de liens et contrôler le nœud multihomed pour des performances optimales.

Un certain nombre de commandes ont été définies pour permettre aux couches supérieures de configurer, commander, et obtenir l'information des couches inférieures afin de faciliter le handover et optimiser son exécution.

III.5.2.2.1 Liste des commandes MIH : Voir Tableau 2.2

No	Nom de la commande	Local/ Remote	Description
1	MIH Get Status	L,R	Obtenir l'état des liens
2	MIH Switch	L,R	Commuter les liens
3	MIH Configure	L,R	Configurer un lien
4	MIH Configure Link Thresholds	L,R	Configure des seuils pour des événements de lien
5	MIH Scan	L,R	Scanner un lien
6	MIH Handover Initiate	L,R	Le réseau lance le handover et envoie une liste de réseaux suggérés et points d'attachement associés
7	MIH Handover Prepare	L,R	Cette commande est envoyée par l'entité MIHF courante pour viser l'entité MIHF cible afin de tenir compte de la ressource demandée et la préparation du handover
8	MIH Handover Commit	L,R	Cette commande est envoyée par un nœud pour un engagement de handover en incluant le réseau choisi et le point d'attachement associé.
9	MIH Handover Complete	L,R	Notification d'accomplissement de handover,
10	MIH Network Address Information	L,R	Cette commande est envoyée par l'entité MIHF courante à MIHF cible pour obtenir l'adresse du client sur le réseau cible

Tableau 3.2 – Liste des commandes

III.5.2.3 MIIS - Media Independent Information Service

Le service d'information (MIIS) fournit un cadre par lequel la MIHF soit dans le nœud mobile ou dans le réseau peut découvrir et obtenir les informations sur les réseaux d'accès du voisinage. L'objectif est d'acquérir une vue globale de tous les réseaux hétérogènes dans le secteur pour faciliter des handovers sans couture.

Le service MIIS inclut un support pour divers éléments d'information (IE : Information Element).
Les éléments d'information fournissent les informations qui sont essentielles pour qu'un module de handover prenne la décision intelligente de handover.

III.5.2.3.1 Liste des éléments d'information (IE) : (voir Tableau 2.3)

No	IE	Description
1.1	TYPE_IE_LIST_OF_NETWORKS	Liste des réseaux d'accès voisins (type de liens)
1.2	TYPE_IE_NUMBER_OF_OPERATORS	Nombre d'opérateurs distincts pour chaque type de lien disponible
1.3	TYPE_IE_LIST_OF_OPERATORS	Liste d'opérateurs pour chaque type de lien
2.1	TYPE_IE_NUMBER_POA	Nombre de point d'attachements (PoA) pour un réseau d'accès spécifique
2.2	TYPE_IE_OPERATOR_IDENTIFIER	Opérateur du réseau d'accès
2.3	TYPE_IE_COST	Indication de coût
2.4	TYPE_IE_NETWORK_SECURITY	Caractéristiques de sécurité du lien
2.5	TYPE_IE_QOS	Caractéristiques QoS du lien
3.1	TYPE_IE_POA_ADDRESS	Adresse MAC du point d'attachement (POA)
3.2	TYPE_IE_POA_LOCATION	GPS Localisation du POA
3.3	TYPE_IE_POA_DATA_RATE	Le minimum et le maximum de la valeur du débit soutenu par le lien d'un PoA donné
3.4	TYPE_IE_POA_PHY_TYPE	Le type de média PHY
4.1	TYPE_IE_POA_SUBNET_INFORMATION	Informations sur les sous-réseaux soutenus par un PoA

Tableau 3.3 – Liste des éléments d'information (IE)

III.5.3 Protocole MIH

IEEE802.21 la MIHF dans le nœud mobile et dans le réseau. Le protocole MIH permet à des paires d'entités MIHF locale et distante d'interagir par l'échange de services MIH.

Le protocole MIH définit des formats de trames pour échanger des messages entre les entités paires MIHF. Ces messages sont basés sur les primitifs qui font partie des services MIES, des services MICS et des services MIIS.

III.5.3.1 Format de la trame utilisée

La trame MIH définie peut être encapsulée avec la technologie Ethernet et également avec d'autres technologies radio 802 telles que 802.11 et 802.16. Le format de la trame MIH utilisée en Ethernet est représenté à la figure 3.10. Un autre mode d'encapsulation est possible, sur un protocole transport (TCP/UDP) avec un port bien défini pour MIH. Ce mode n'a pas fait d'objet de spécification particulière par le standard IEEE 802.21.

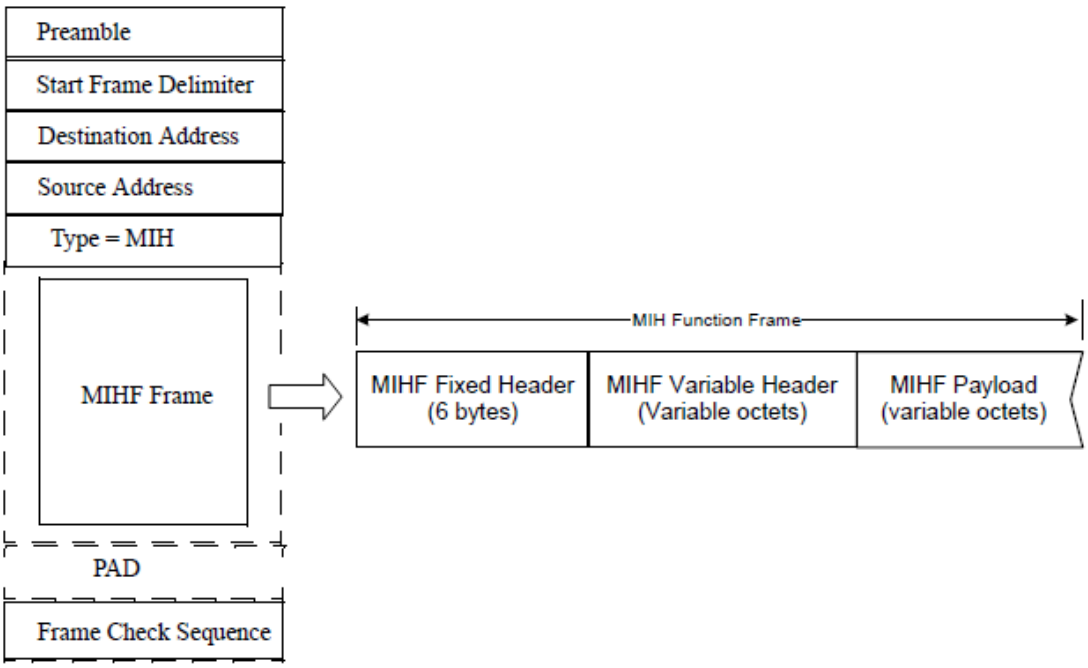

Fig. 3.10 – Exemple de format de trame MIH pour Ethernet

La trame MIH est constituée des trois champs suivants :

- MIH Fixed Header (6 àctets) : contient l'identifiant du message MIH
- MIH Variable Header (longueur variable) : contient des identifiants additionnels qui aident à analyser et coordonner le la charge de la trame soit la 'MIHF payload'**.**
- MIHF payload (longueur variable) : charge de la trame MIH

Le tableau suivant résume quelques messages du protocole MIH :

No	Identifiant du message MIH	Type du message	Identifiant du service MIH
1	MIH Event Register	Request, Response	MIES
2	MIH Link Detected	Indication	MIES
3	MIH Link Up	Indication	MIES
4	MIH Link Down	Indication	MIES
5	MIH Link Going Down	Indication	MIES
6	MIH Get Status	Request, Response	MICS
7	MIH Switch	Request, Response	MICS
8	MIH Configure Link Thresholds	Request, Response	MICS
9	MIH Scan	Request, Response	MICS
10	MIH Get Information	Request, Response	MIIS

Tableau 3.4 – Liste des messages MIH

III.6 Conclusion

Ce chapitre a été divisé en deux parties, la première a été consacrée au multihoming dans le contexte d'un réseau NEMO où des tunnels bidirectionnels multiples sont établis entre des pairs de MRs et HAs. Après avoir montré quelques bénéfices du multihoming, une classification des configurations de multihoming possibles a été présentée et les issues impliquées ont été expliquées. Cette analyse nous est très utile dans la mesure où elle nous permettra de faire des choix pour des extensions du protocole NEMO BS avec des mécanismes multihoming connexes.

Dans la seconde partie, nous avons présenté un aperçu des services du standard IEEE 802.21 Media-Independent Handover. Après avoir montré les motivations et les besoins d'une norme pour faire face aux handovers de réseaux hétérogènes, nous avons introduit le modèle de référence IEEE 802.21 et les services MIH. Nous avons ensuite brièvement présenté le protocole MIH.

Dans les chapitres suivants, nous allons développer des mécanismes de handover sans couture en traitant deux configurations de multihoming avec l'appui des services MIH présentés précédemment.

CHAPITRE 4

Handover sans Coutures basé sur le Modèle NEMO Multihomed (n,n,1)

IV.1 Introduction

La multi-domiciliation (Multihoming) [28] est une solution prometteuse pour fournir un service Internet omniprésent et quelques autres avantages tels que le partage de charge (Load-Sharing) [49, 50, 51], la tolérance aux pannes/redondance (Fault-Tolerance/Redundancy) [52] et les Stratégies de routage (Policy-based Routing) [53-55]. Le multihoming dans les réseaux NEMO constitue à l'heure actuelle une issue de recherche importante dont l'objectif est de fournir des solutions de gestion de la mobilité permettant d'assurer une connectivité permanente à Internet, à tout moment et en tout lieu, sans interruption de service. Le support NEMO combiné au multihoming constitue donc la pièce manquante qui va nous permettre d'être en permanence accordé à Internet même en déplacement. L'objectif de ce chapitre est la proposition d'un nouveau support (extension du protocole NEMO BS) basé sur le multihoming permettant la gestion de la mobilité et le trafic dans le contexte d'un modèle n,n,1) de réseau NEMO multihomed [84].

Rappelons que la configuration (n, n, 1) signifie que le réseau NEMO dispose de plusieurs routeurs mobiles (MR) dont chacun présente une seule interface externe et admet un Home Agent (HA), mais où un seul préfixe MNP est utilisé.
Notre objectif est de développer une solution indépendante de l'infrastructure des réseaux d'accès.

Pour cela, nous nous orientons vers une intelligence au centre du réseau NEMO lui-même. Pour prendre l'ensemble des décisions de mobilité, nous introduisons une entité centrale (routeur intelligent) au sein du réseau NEMO, et qui jouera le rôle de passerelle (Gateway) entre les MNNs embarqués et les MRs. Nous avons nommé cette entité MNPx (Mobile Network Proxy), elle est responsable de la gestion des handovers et la distribution du trafic entre les MRs d'une façon transparente pour les MNNs à l'intérieur du réseau NEMO. Tous les trafics (émis et reçus) des MNNs transitent par le MNPx, Tous les routeurs mobiles du réseau NEMO sont reliés au MNPx avec des liens filaires ou sans fil. Le MNPx dispose donc de multiples interfaces, nous ferons appel au standard IEEE 802.21 en utilisant particulièrement les services MIH à distance pour gérer les MRs.

Nous adoptons dans la solution proposée, une approche proactive consistant à exécuter des handovers soft (Make Before Brake), conduisant à la disponibilité de plusieurs tunnels simultanément. Ainsi, la rupture d'un lien actif pour un MR donné provoque uniquement un basculement du trafic via un autre MR disposant d'un tunnel déjà établi.

IV.2 Choix de la Configuration (n,n,1)

Quand nous traitons un réseau NEMO multihomed basé sur plusieurs routeurs mobiles, le choix de la configuration (n, n, 1) au lieu de la configuration (n, n, n) est essentiel en raison de ses possibilités pour réaliser les avantages du multihoming d'une manière transparente pour les couches transports et les couches applications.

Dans le modèle (n, n, n), chaque MR possède son préfixe MNP. Il existe deux types de solutions pour les mécanismes de gestion de la mobilité. Les premières solutions emploient les niveaux d'encapsulation multiples en considérant un modèle de réseau mobile niché (nested) [56, 57, 58] sans changement aux adresses IP déjà assignées pour MNNs). Ceci mène à une complexité accrue et un délai relativement plus lent.

D'autres solutions recommandent de configurer les MNNs avec de nouvelles adresses IP du préfixe MNP délégué au MR substituant qui fournira le nouveau chemin à l'Internet. Malheureusement, changer ces adresses endommagera plus les applications. C'est ainsi parce que les applications et les protocoles courants des couches transport, telles que le TCP et le UDP, identifient les points extrémités d'une communication par les adresses IP des nœuds impliqués, impliquant que les adresses IP choisies au temps d'établissement de communication doivent demeurer invariables pour la vie de la communication. Ainsi, tout changement des adresses IP sources mènera à une latence élevée et cause le rétablissement des sessions de transport.

Cependant, la configuration (n,n,1) nous permet d'éviter ces dégradations de performance. Toutefois, la gestion de la mobilité doit être réalisée d'une manière optimisée et sans couture. Dans la configuration (n,n,1), chaque MR maintient indépendamment son propre tunnel bidirectionnel. Quand une rupture dans le chemin actuellement utilisé se produit, il doit être détecté, afin de changer le tunnel

endommagé. Par conséquent, des mécanismes pour la détection des ruptures des liens et pour la vérification du maintien des tunnels (keepalive test) sont nécessaires. D'autre part, une fois un échec dans le chemin actuellement utilisé est détecté, les chemins alternatifs doivent être explorés afin d'identifier ceux qui sont disponibles. Un autre problème qui doit être résolu est lié à l'optimisation du délai de ces opérations. En effet, le délai total pour détecter l'échec du tunnel courant, découvrir et choisir d'autres chemins et configurer l'un d'eux serait relativement élevé. Les mécanismes rapides sont donc nécessairement très recommandés.

Par ailleurs, des mécanismes pour contrôler la distribution du trafic sortant (outbound traffic) pour les services de partage de charge et de stratégie de routage sont exigés. A noter que les mécanismes pour la configuration (n, 1, 1) se déduisent de la configuration (n, n, 1).

IV.3 Description du support de mobilité proposé

Pour surmonter le manque de support de multihoming dans le protocole NEMO BS, nous présentons une nouvelle approche pour la mobilité de réseau en proposant un routeur proxy comme passerelle centrale à l'intérieur du réseau mobile pour assurer la gestion de la mobilité et du trafic.

En outre, en raison des délais de la détection des ruptures des liens et des opérations de basculement de chemins, les paquets destinés au réseau NEMO peut être retardés ou perdus pendant la période du handover. À cet effet, nous présentons d'autres mécanismes pour améliorer notre solution.

IV.3.1 Passerelle MNPx

Dans notre proposition, le routeur proxy (MNPx) sera l'unique passerelle par défaut pour tous les MNNs. Tout le trafic sortant (outbound) des MNNs comme le trafic destiné (inbound) aux MNNs doit passer par le MNPx (Fig. 4.1).

Le réseau mobile NEMO admet un routeur mobile MR primaire et un ou plusieurs MRs secondaires. Le Home Agent (HA) du MR primaire est appelé HA primaire.

Le préfixe MNP délégué au MR primaire est également communiqué à MNPx qui doit l'annoncer aux nœuds MNNs. A l'intérieur du réseau NEMO, les routeurs MRs ne peuvent communiquer qu'avec le routeur MNPx (ils ne doivent pas communiquer entre eux ni avec les MNNs). Une fois un échec dans le chemin actuellement utilisé à l'Internet est détecté, un des MRs déjà enregistré et possédant un tunnel avec le Home Agent du routeur mobile primaire devra remplacer le MR dont le lien avec le réseau d'accès est rompu (le MR de remplacement est appelé substituant).

La passerelle MNPx a la responsabilité exclusive de choisir et de designer le routeur MR substituant sur la base des informations qu'elle maintient au sujet de tous les MRs. En outre, le MNPx est chargé également de gérer le trafic sortant (outbound). En conséquence, nous prévoyons un module à implémenter au niveau du MNPx que nous avons appelé MTM (Mobility and Trafic Management) deux composants principaux (dont les détails sont présentés ci-dessous):

(i) le composant de détection d'environnement EDC (Environment Detector Component)

(ii) le composant de décision de politique PDC (Policy Decision Component)

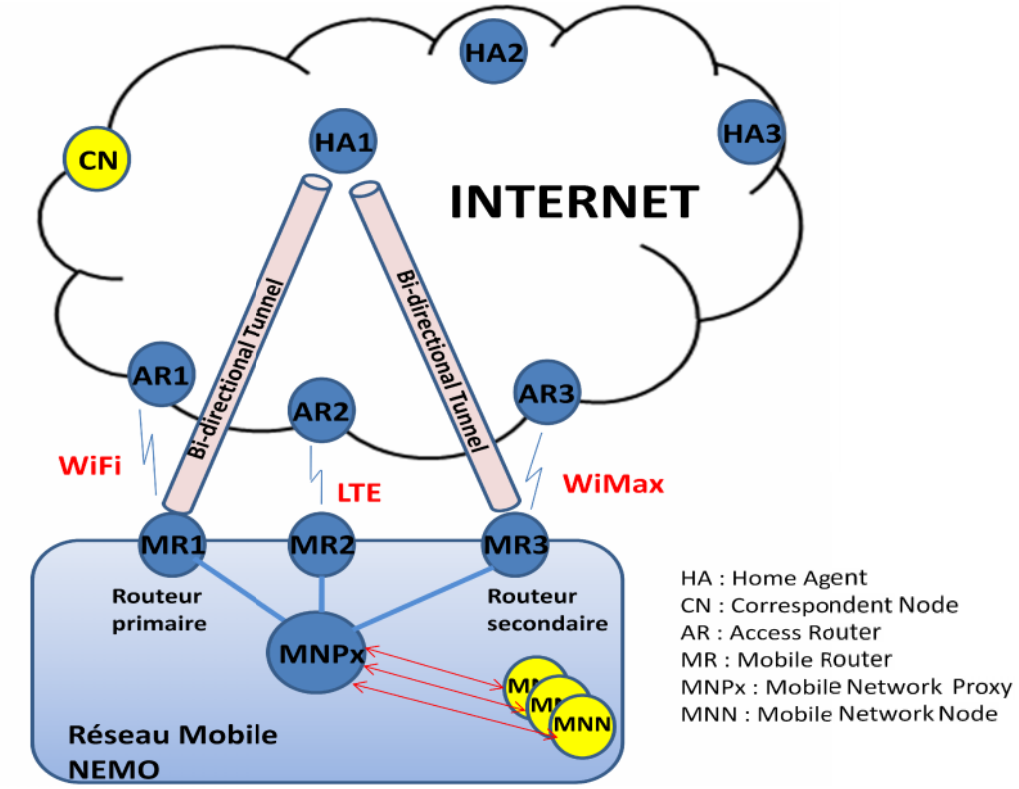

Fig. 4.1 – Architecture du schéma pour le support de mobilité proposé

IV.3.2 Détection d'environnement (EDC)

Ce composant a la responsabilité de détecter les changements qui pourraient se produire au niveau des routeurs mobiles notamment les événements ayant lien avec le handover. À ce stade, nous sommes confrontés à divers problèmes : quelle information le détecteur d'environnement devrait détecter, comment obtenir cette information et comment l'employer. Cependant, aborder toutes ces questions est hors de la portée de cette thèse. Nous nous concentrons ici seulement sur l'information nécessaire pour le besoin de gestion de la mobilité et du trafic (partage de charge, stratégie de routage), particulièrement ceux relié à la détection d'échec de tunnel et aux caractéristiques des liens d'accès.

Au niveau du réseau NEMO, la détection des échecs de tunnel entre le HA primaire et les MRs devraient se fonder sur les messages « Router Advertisement » émis par les routeurs d'accès aux MRs, ou sur d'autres mécanismes aux niveaux L1/L2 permettant de détecter des ruptures de liens et générer des triggers.

Lorsqu'un événement de type rupture de lien (par exemple) se produit au niveau d'un MR, celui-ci doit transmettre une notification à la passerelle MNPx. Cependant, ce mécanisme souffre de la latence en particulier quand le MR lui-même ou son interface d'entrée (ingress interface) tombe en panne.

Pour s'affranchir de cet obstacle et réaliser des détections plus rapides, une possible solution proactive serait l'utilisation d'un mécanisme de test keepalive ordonné périodiquement par le détecteur d'environnement. Ce dernier réalise aux périodes très courtes le test keepalive avec tous les MRs pour voir si les tunnels établis avec le HA primaire sont encore ouverts. Le détecteur d'environnement devrait également envoyer aux MRs des demandes d'informations périodiques sur les liens d'accès pour les besoins de gestion du trafic sortant (outbound).

Les informations collectées par le composant détecteur d'environnement sont automatiquement expédiées au composant de décision de politique qui les utilisera pour la gestion de la mobilité ou du trafic.

IV.3.3 Utilisation des services MIH IEEE 802.21

Dans ce travail, nous nous basons sur les mécanismes définies et spécifiés dans le standard IEEE 802.21 [68] (présenté dans le chapitre 3) pour développer notre proposition. Les services MIH de ce standard nous permettent d'assister le composant EDC dans ses tâches de détection d'environnement.

Nous allons utiliser les services MIES et MICS locaux et remote (à distance) au niveau de chaque routeur mobile MR et au niveau du MNPx.

Les services locaux permettent de détecter les changements des états de liens des MRs, de déclencher les triggers associés. Les services MIES à distance permettent au MRs de notifier la passerelle MNPx des évènements associée aux liens se produisant à leurs niveaux ; d'autres parts le MNPx pourra utiliser les services MICS à distances pour obtenir les informations désirées sur les états des liens des MRs et leurs qualités et caractéristiques.

Le tableau 4.1 résume les services MIES et MICS utilisés dans cette approche et les paramètres correspondants.

- Service MIH_Link_Down : en local, ce service par les MRs et le MNPx pour notifier les MIHF locales d'une rupture de lien interne. Le MNPx utilisera ce service local pour détecter les MRs inaccessibles ou hors service. En remote, les MRs utilisent ce service pour informer la MIHF du MNPx de la rupture du lien externe.

- Service MIH_Link_Going_Down : utilisé uniquement en remote par les MRs pour notifier le MIHF du MNPx qu'un lien externe est sur le point de tomber.

Primitive	Service	Local/ Remote	Paramètres
MIH_Link_Down	MIES	L/R	MR IF MAC Addr, MAC addr of new PoA, Reason Code
MIH_Link_Going_Down	MIES	L/R	MR IF MAC Addr, MAC Addr of Curent PoA, TimeInterval, ConfidenceLevel
MIH_Get_Status	MICS	L/R	NETWORK_ID , CHANNEL_ID , CHANNEL_QUALITY , LINK_SPEED
MIH_Get_Information	MICS	L/R	Information Element IE Type : PHY_TYPE, DATA_RATE, …

Tableau 4.1 – Services MIH utilisés (première approche)

- Service MIH_Get_Status : utilisé uniquement en remote par le MNPx pour demander au MIHF d'un MR l'état de son lien externe.

- Service MIH_Get_Information : est employé en remote par le MNPx pour demander au MIHF d'un MR des informations liées à une interface spécifique. Le type d'information demandée est spécifié par le paramètre IE (Information Element).

IV.3.3 Décision de politique (PDC)

Le composant de décision de politique a la charge de gérer d'une part la mobilité du réseau NEMO et d'autre part le trafic sortant provenant des nœuds MNNs. Il doit donc prendre les décisions intelligentes de handover soft et de choix de chemins de routage compte tenu des exigences des applications en QoS et les caractéristiques des liens disponibles. Nous définissons à l'intérieur de ce composant deux modules, un pour la gestion de la mobilité et l'autre pour la gestion du trafic.

IV.3.3.1 Gestion de la mobilité

L'idée principale derrière notre proposition est, si possible, d'enregistrer et d'établir des tunnels à l'avance entre chaque MR secondaire et le HA du MR primaire et de les employer quand le MR primaire (ou un MR secondaire) avec un tunnel ouvert opérationnel devient hors service ou perd la connectivité de son lien au réseau d'accès (Fig. 4.2).

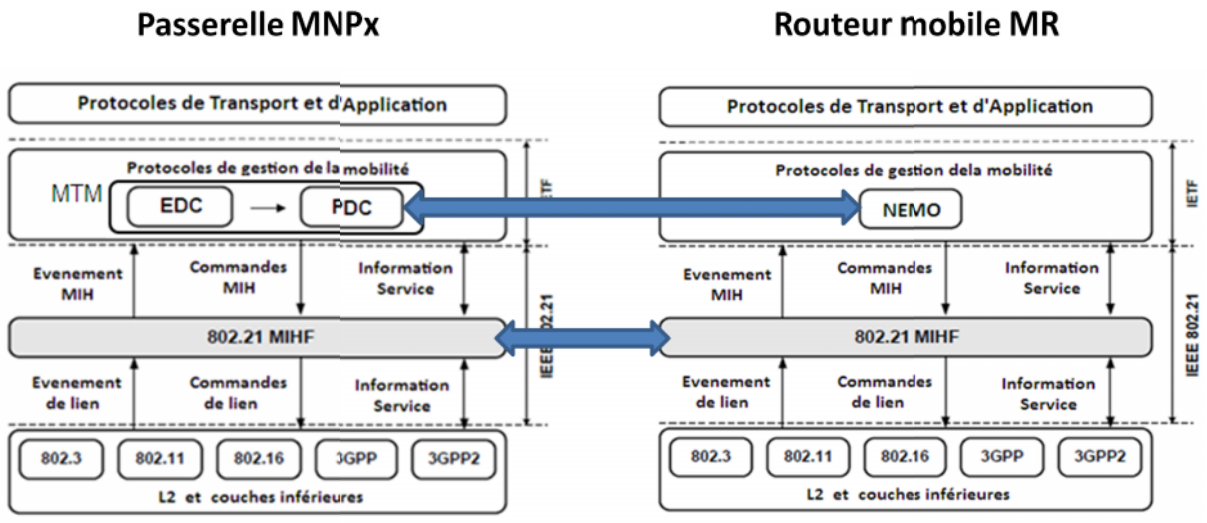

Fig. 4.2 – Architecture de la pile de mobilité proposée pour les MRs et le MNPx

Nous précisons ici que tous les MRs appartenant au réseau NEMO sont enregistrées au niveau du MNPx (par exemple par les adresses physiques) et leurs interfaces internes (ingress interfaces) sont configurées avec des adresses IP du préfixe MNP délégué, de sorte qu'elles soient facilement authentifiées.

Nous avons défini au niveau du MNPx un cache appelé MR_Data cache (Tableau 4.2) pour maintenir les informations nécessaires concernant tous les MRs du réseau NEMO. Chaque entrée du cache contient les champs suivants :

MAC MR	MRType	HoA	CoA	Tunnel Status	Active	Bandwidth	Packet Loss Rate	Round Trip Time (RTT)	Service Cost
MAC MR1	1	HoA1	MR1 CoA	1	1				
MAC MR2	0	HoA2	MR2 CoA	0	0				
MAC MR3	0	HoA3	MR3 CoA	1	0				

Tableau 4.2 – Cache MR_Data au niveau du MNPx

- Champ MAC MR : l'identifiant du MR (par exemple l'adresse physique de son interface interne (ingress interface)
- Champ MRType : MR primaire (valeur 1) ou MR secondaire (valeur 0)
- Champ HoA : Home Address du MR
- Champ CoA : l'adresse CoA obtenu par le MR (qui définit sa localisation actuelle)
- Champ Tunnel Status : valeur 1 pour tunnel établi ou valeur 0 pour tunnel non encore établi
- Champ actif : indique si le tunnel est actuellement actif (valeur 1) ou non (valeur 0)
- Les autres champs : tels que la largeur de bande, le taux de perte de paquet et le délai RTT représentent quelques informations nécessaires sur les liens d'accès pour la gestion éventuelle du trafic sortant.

IV.3.3.2 Gestion du trafic

Puisque plusieurs chemins à l'Internet à travers les différents MRs seront disponibles simultanément, des mécanismes de stratégie de routage et de partage de charge peuvent être assurés par le MNPx si les informations nécessaires sont collectées par le composant de détection d'environnement.
Ainsi, sur la base de ces informations et les préférences des applications des utilisateurs le MNPx peut choisir le chemin approprié pour expédier le trafic sortant (outbound) des MNNs. Le développement de ces mécanismes sort du cadre de cette thèse mais reste une des perspectives de ce travail.

IV.4 Opérations du support de mobilité proposé

IV.4.1 Procédure d'enregistrement d'un nouveau MR substituant

Considérons l'exemple de la figure 4.3 où le réseau mère (Home network) est le réseau WiFi et MR1 est le routeur primaire. Supposant que le routeur mobile secondaire MR3 a obtenu une adresse temporaire CoA sur le réseau d'accès WiMax et a établi un tunnel avec son Home Agent HA3. Le routeur mobile MR3 notifie alors le MNPx de l'établissement de ce tunnel en utilisant un message authentifié comprenant les informations suivantes :

- L'adresse du MR3 dans son réseau mère (soit HoA3)
- L'adresse CoA obtenue
- un Nonce (un nombre entier aléatoire) utilisés comme un contrôle de retour de routabilité (return routability)

Pour cette notification, nous utilisons le message New_tunnel_Notification qui est envoyé par le module de gestion de la mobilité NEMO au niveau de MR3 au composant PDC au niveau du MNPx.

Le message New_tunnel_Notification est traité différemment par MNPx suivant que la source est un MR primaire ou secondaire. Nous expliquons tout de suite le traitement pour le cas ou l'émetteur est un MR secondaire, le cas ou l'émetteur est le MR primaire sera expliqué plus loin.

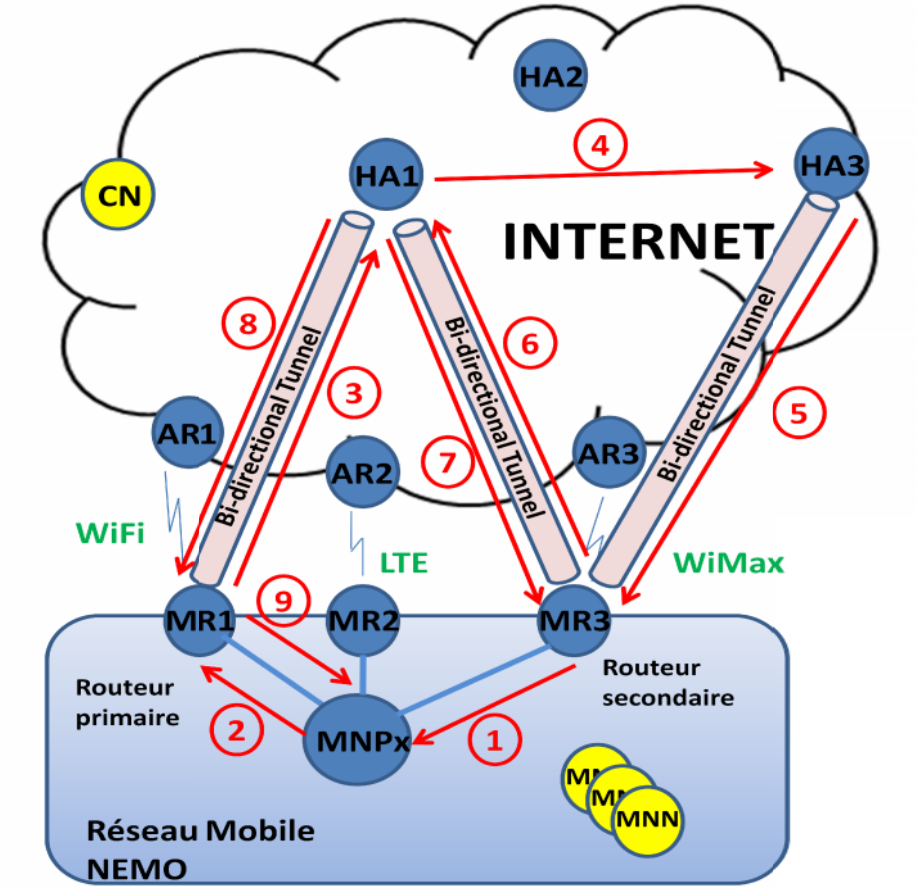

Fig. 4.3 – Principes du support de mobilité basé sur MNPx

1	New_tunnel_Notification	6	Substitute_ BU
2	New_Sub_Reg	7	Substitute_BACK
3	Sub_Reg_Request	8	Substitute_Reg_Notification
4	Sub_Reg_Invite	9	Substitute_Reg_Confirmation
5	Sub_Reg_Invite		

Donc à la réception et la validation du message New_tunnel_Notification envoyé par MR3, le MNPx mis à jour l'entrée MR3 de son cache MR_Data. Ensuite, il transmit à MR1 les informations obtenus de MR3 en le sollicitant de les communiquer à son Home Agent pour procéder à l'enregistrement de MR3 en tant que substituant de MR1. Cette requête se fait par l'envoie d'un message New_Sub_Reg du PDC (MNPx) au module NEMO de MR1.

Le routeur MR1 à son tour émis à son Home Agent HA1 un message Sub_Reg_Request contenant les informations envoyés par le MNPx. À la réception de ce message, le HA1 envoie à MR3 un message d'invitation pour l'enregistrement Sub_Reg_Invite.
Ce message inclut les informations suivantes :

- le préfixe MNP délégué à MR1
- Le nonce généré par MR3
- Un nonce généré cette fois-ci par HA1

Ce message arrive à MR3 via son Home Agent HA3.
MR3 vérifie la validité du message. Si le message est valide, il répond à HA1 avec un message Substitute_ BU (substitute Binding Update) comprenant :

- Son adresse temporaire CoA
- Le préfixe MNP
- Le nonce généré par HA1

Après vérification de la validité de ce message, HA1 enregistre MR3 comme un substituant pour MR1 dans son binding cache et envoie à MR3 un message Substitute_BACK (substitute Binding Acknowledgement). HA1 envoie parallèlement un message Substitute_Reg_Notification à MR1 pour l'informer que MR3 a été enregistré comme substituant. Cette information est immédiatement translatée par le biais d'un message Substitute_Reg_Confirmation à MNPx qui met à jour son cache MR_Data. Ce procédé est illustré sur la figure 4.4.
Les tunnels établis avec HA1 ont soit l'état ouvert (open) ou l'état fermé (close) suivant que le tunnel est actuellement utilisé pour véhiculer le trafic ou non. Le nouveau tunnel établi entre MR3 et HA1est mis initialement dans l'état fermé, en attente d'un ordre de commutation qui le ferra basculé dans l'état ouvert.
Un scenario possible est le cas où le routeur primaire MR1 n'a pas de lien avec les réseaux d'accès, et que le réseau NEMO est desservi par un de ses routeurs mobiles secondaires. Dans ce cas, lorsque MR1établit un nouveau tunnel avec HA1, ce tunnel est mis automatiquement à l'état ouvert par HA1. Le message New_tunnel_Notification envoyé par MR1 au MNPx entraine simplement l'aiguillage par MNPx du trafic sortant (outbound) sur MR1.
À moins qu'une politique de routage soit implémentée au niveau du HA1, ce dernier devrait toujours utiliser par priorité le tunnel HA1-MR1 (tunnel primaire).
Le tunnel déjà ouvert avec le MR secondaire peut être soit utilisé simultanément avec le tunnel primaire soit tout simplement fermé.

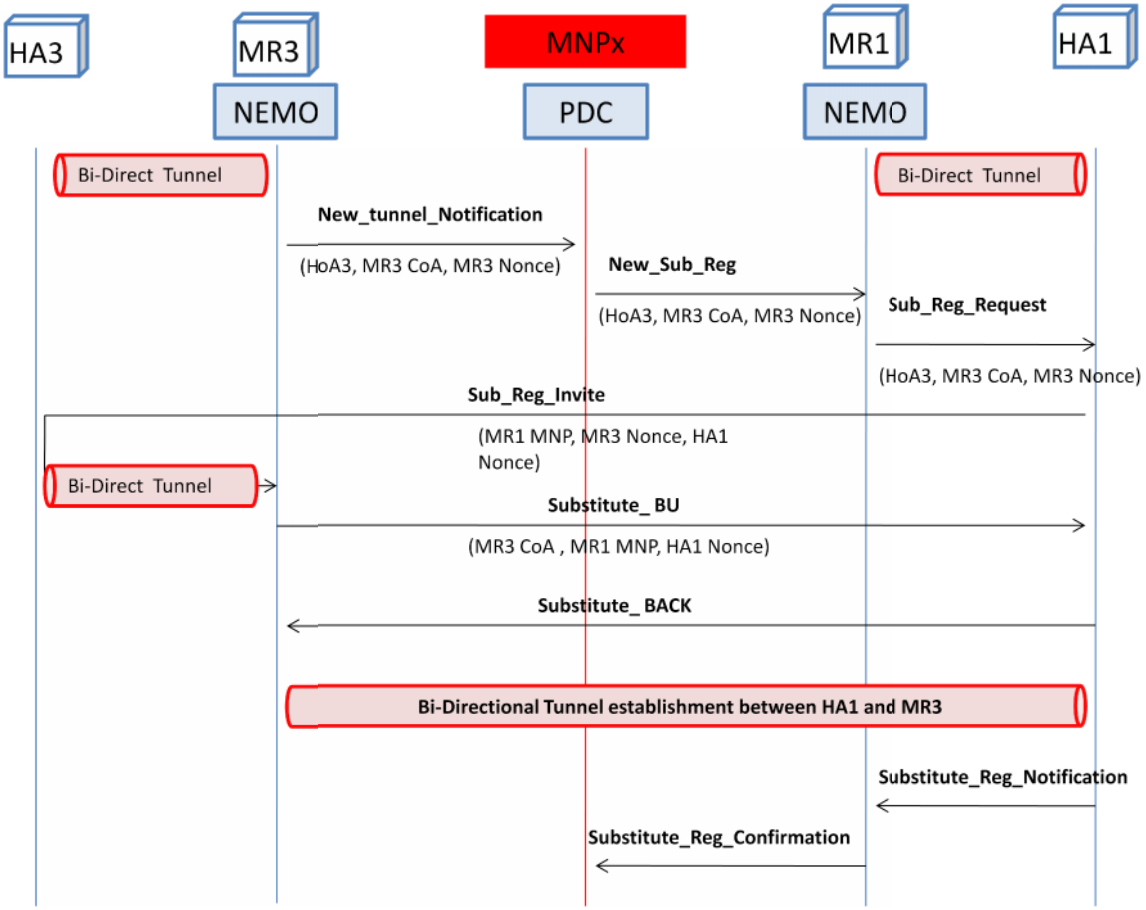

Fig. 4.4 – Procédure d'enregistrement du MR substituant

IV.4.2 Changements au niveau du Binding Cache

Dans la version NEMO support basique [15], un routeur mobile ne peut enregistrer qu'une seule adresse CoA au prés de son HA. Par conséquent, l'enregistrement de CoAs multiples avec une seule adresse HoA n'est pas possible. Afin de palier ce problème et permettre aux routeurs mobiles secondaires de s'enregistrer au prés du HA1 du routeur mobile primaire, nous avons modifié la structure du binding cache de HA1 pour tenir compte des informations sur les routeurs mobiles substituant possibles.

Nous avons ajouté trois champs (Tableau 4.3) :

- MR-type : indique si le MR enregistré est primaire (valeur 1) ou secondaire (valeur 0).
- Tunnel : indique si ce tunnel est ouvert (open) ou fermé (close) au trafic de données. Une fois établi, le tunnel est par défaut ouvert au trafic de signalisation et fermé au trafic de données.
- ExpireTime : indique le temps d'expiration de la disponibilité du tunnel. La valeur de ce champ est obtenue par l'équation suivante ExpireTime = CurrentTime + LifeTime
  où CurrentTime est l'instant courant et LifeTime est la durée de vie du tunnel.

Prefix	CoA	MRType	Tunnel	ExpireTime
MNP	MR1 CoA	1	Opened	-
MNP	MR3 CoA	0	Closed	-
---	---	---	---	---

Tableau 4.3 – Nouveau Binding Cache pour le support d'enregistrement de CoAs multiples

IV.4.3 Détection de rupture de lien

Nous proposons deux approches pour détecter les ruptures des liens du MR présentant des tunnels ouverts avec le HA primaire.

a) Approche basée sur le service MIH_Link_Down

Si un événement Link_Down (trigger LD) est généré par l'interface externe d'un MR, le MIHF du MR transmet cet évènement (remote MIH_Link_Down) vers le MIHF du MNPx. Ce dernier notifie immédiatement le composant EDC (module MTM). Cet événement sera traité suivant la politique défini au niveau du PDC (module MTM). A noter que cette approche conduit à des délais de déconnexion et des pertes de paquets non nuls. Nous reviendrons sur ce problème plus loin.

Rappelons que l'événement LD est déclenché si :

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

Ou P_{rx} est la puissance du signal reçu (RSS : Received Signal Strength)

P_{th} est la puissance seuil en dessous de la quelle le lien est considéré rompu (Down).

b) Approche basée sur le service MIH_Link_Going_Down

Dans cette approche, afin d'activer le tunnel d'un MR substituant avant le déclenchement du trigger LD, nous utilisons l'événement Link_Going_Down (trigger LGD) permettant la prédiction de la rupture des liens. Le trigger LGD sera utilisé avec un seuil prédéfini :

$$P_{rx} < \alpha_{LGD} P_{th}$$

Ou α_{LGD} le coefficient LGD légèrement supérieur à 1 (valeurs typiques : 1.05, 1.01, …)

Donc, de la même manière, si un événement LGD est généré par l'interface externe d'un MR, le MIHF du MR transmet cet évènement (remote MIH_LinkGoing_Down) vers le MIHF du MNPx qui notifie immédiatement le composant EDC (module MTM).

Un scenario de mise hors service du MR peut se produire empêchant ainsi la propagation des événements qui seraient déclenchés à son niveau vers le MNPx, ce qui peut être catastrophique pour la garantie de la continuité des sessions ouvertes (seamless connectivity). Pour éviter ce problème, nous avons proposé d'utiliser conjointement un test proactif effectué par le MNPx périodiquement permettant d'obtenir le status des liens (avec tunnel établi avec le MR primaire). Le test repose sur l'utilisation du service MIH_Get_Status (remote) envoyé par le MNPx aux MRs.

IV.5 Format des messages utilisés

- **Message New_Tunnel_Notification**
  Source : un MR ayant établi un nouveau tunnel avec son HA (module NEMO)
  Destination : MNPx (PDC module MTM)
  Description : message de notification d'établissement du nouveau tunnel.
  Format : voir figure 4.5.

<table>
<tr><td></td><td>Type</td><td>Code</td><td>Length</td></tr>
<tr><td>Tunnel ID</td><td colspan="2">Sequence Number</td><td>LifeTime</td></tr>
<tr><td colspan="4">MAC Address of MR's ingress interface</td></tr>
<tr><td colspan="4">IP Address of MNPx</td></tr>
<tr><td colspan="4">HoA</td></tr>
<tr><td colspan="4">CoA</td></tr>
<tr><td colspan="4">MR's Nonce</td></tr>
</table>

Fig. 4.5 – Format du message New_Tunnel_Notification

- Type (4 bits) : spécifie le type du message (valeur 0 pour la catégorie New_Tunnel)
- Code (4 bits) : donne le code du message (valeur 1 pour New_Tunnel_Notification)
- Length (1 octet) : longueur du paquet en octets
- Tunnel ID (2 octets) : identifiant du tunnel, le MR assigne un identifiant différent pour chaque nouveau tunnel établi.
- Sequence Number (1 octet) : numéro de séquence du message envoyé.

- LifeTime (1 octet) : durée de vie de la notification, au bout de ce délai si le MR est un secondaire et il ne reçoit aucune réponse (message Sub_Reg_Invite) il retransmit le message avec le numéro de séquence suivant.
- MAC Adresse of MR's ingress interface: l'adresse MAC de l'interface interne du MR. directement connecté au MNPx.
- IP Address of MNPx: adresse IPv6 du MNPx obtenu à partir du préfixe MNP délégué au routeur primaire.
- HoA : l'adresse HoA du MR.
- CoA : l'adresse temporaire CoA obtenue par le MR.
- MR's Nonce (4 octets) : un nombre aléatoire choisi par le MR.

- **Message New_Sub_Reg**

  Source : MNPx (PDC module MTM)

  Destination : le MR dont le tunnel avec le HA primaire est actuellement ouvert pour le trafic (module NEMO).

  Description : message de demande d'enregistrement d'un nouveau MR secondaire candidat pour la substitution.

  Format : voir figure 4.6.

	Type	Code	Length
IP Address of MNPx			
HoA			
CoA			
MR's Nonce			

Fig. 4.6 – Format du message New_Sub_Reg

- Type (4 bits) : spécifie le type du message (valeur 1 pour la catégorie New_Sub)
- Code (4 bits) : donne le code du message (valeur 1 pour New_Sub_Reg)
- Length (1 octet) : longueur du paquet en octets

Les autres champs sont les mêmes que ceux du message New_Tunnel_Notification.

- **Message Substitute_Reg_Confirmation**

  Source : le MR dont le tunnel avec le HA primaire est actuellement ouvert pour le trafic (module NEMO).

  Destination : MNPx (PDC module MTM)

  Description : message de confirmation d'enregistrement du nouveau MR secondaire substituant.

  Format : le même format que celui de la figure 4.6, avec un Type = 1 et un Code = 2.

- **Message Sub_Reg_Request**

  Source : Le MR ayant reçu le message New_Sub_Reg_Confirmation (module NEMO).

  Destination : Le HA primaire (module NEMO).

  Description : requête pour l'enregistrement du MR substituant au niveau du HA primaire.

  Format : nous avons défini ce message conformément aux messages de signalisation NEMO [2], voir figure 4.7.

  - MH Type : Le type d'entête de mobilité pour ce message est fixé à 55.
  - Les champs HoA, CoA et MR's Nonce sont similaires à ceux du message New_Tunnel_Notification.

Payload Proto	Header Len	MH Type = 55	Reserved
Checksum		Sequence ID	LifeTime
HoA			
CoA			
MR's Nonce			
options			

Fig. 4.7 – Format du message Sub_Reg_Request

- **Message Substitute_Reg_Notification**

  Source : Le HA primaire (module NEMO).

  Destination : Le MR ayant émis le message Sub_Reg_Request (module NEMO).

  Description : notification de l'enregistrement du MR substituant au niveau du HA primaire.

  Format : même format que celui de la figure 4.7 avec un champ MHType = 56.

- **Message Sub_Reg_Invite**

  Source : Le HA primaire (module NEMO).

  Destination : Le MR secondaire candidat à la substitution (module NEMO) via son HA (l'adresse HoA est utilisée comme adresse IP destination).

Description : invitation à la procédure binding update.

Format : voir figure 4.8.

Payload Proto	Header Len	MH Type = 57	Reserved
Checksum		Sequence ID	LifeTime
MNP			
MR's Nonce			
HA's Nonce			
options			

Fig. 4.8 – Format du message Sub_Reg_Invite

- MNP : préfixe délégué au MR primaire.
- MR's Nonce : le Nonce généré par le MR secondaire candidat à la substitution
- MR's Nonce : un Nonce généré par le HA primaire pour le test de « return routability » .
-

- **Message Substitute_BU**

  Source : Le MR secondaire candidat à la substitution (module NEMO)

  Destination : Le HA primaire (module NEMO).

  Description : message de binding update.

  Format : nous avons gardé le même format utilisé par le protocole NEMO BS avec de légers modifications, voir figure 4.9.

Payload Proto	Header Len	MH Type = 5	Reserved
Checksum		Sequence ID	LifeTime
		Sequence #	
	T	Reserved	LifeTime
CoA			
MNP			
HA's Nonce			

Fig. 4.9 – Format du message Substitute_BU

- Flag T (1 bit): ce nouveau drapeau est ajouté pour indiquer au HA si le message BU vient d'un MR primaire (valeur 1) ou d'un MR secondaire (valeur 0).
- CoA : est l'adresse temporaire CoA obtenue par le MR secondaire candidat à la substitution.
- Les autres champs sont les mêmes que ceux du message Sub_Reg_Invite.

- **Message Substitute_BACK**

  Source : Le HA primaire (module NEMO).

  Destination : Le MR secondaire candidat à la substitution (module NEMO)

  Description : ACK au message de binding update Substitute_BU .

  Format : le même format utilisé par le protocole NEMO BS est repris avec adjonction du flag T, voir figure 4.10.

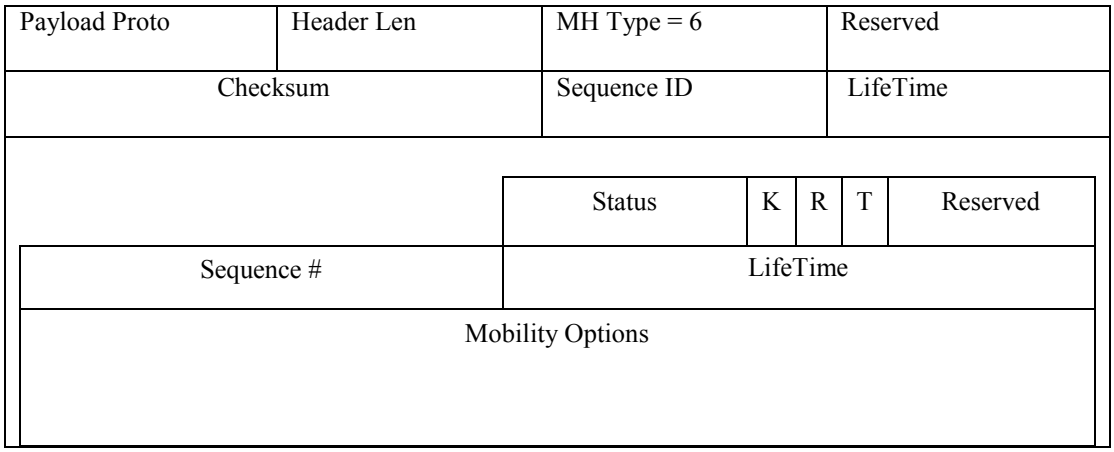

Fig. 4.10 – Format du message Substitute_BACK

- **Message Tunnel_Activation_Request**

  Source : MNPx (PDC module MTM)

  Destination : Le MR substituant (module NEMO)

  Description : message de demande d'activation du tunnel pour le trafic de données

  Format : voir figure 4.11.

- Type (4 bits) : spécifie le type du message (valeur 2 pour la catégorie Tunnel_Activation)
- Code (4 bits) : donne le code du message (valeur 1 pour Tunnel_Activation_Request)
- Length (1 octet) : longueur du paquet en octets
- Motif : donne le motif de la requête, valeur 200 pour la gestion de mobilité (rupture du lien, la CoA correspondante au lien rompu est spécifiée dans le champ options), valeur 250 pour la gestion du trafic.

	Type	Code	Length
IP Address of MNPx			
MAC Address of MR's ingress interface			
HoA			
CoA			
Motif			
Options			

Fig. 4.11 – Format du message Tunnel_Activation_Request

Les autres champs sont les mêmes que ceux du message New_Tunnel_Notification

- **Message Tunnel_Activation_Replay**
  Source : Le MR substituant (module NEMO) ayant reçu le message Tunnel_Activation_Request
  Destination : MNPx (PDC module MTM)
  Description : réponse au message Tunnel_Activation_Request
  Format : voir figure 4.12.

	Type	Code	Length
IP Address of MNPx			
MAC Address of MR's ingress interface			
HoA			
CoA			
Response Code			

Fig. 4.12 – Format du message Tunnel_Activation_Replay

- Type (4 bits) : spécifie le type du message (valeur 2 pour la catégorie Tunnel_Activation)
- Code (4 bits) : donne le code du message (valeur 2 pour Tunnel_Activation_Replay)
- Length (1 octet) : longueur du paquet en octets
- Response Code : successful (code 240), failure (code 244)

Les autres champs sont les mêmes que ceux du message Tunnel_Activation_Request

- **Message Tunnel_Opening_Request**

  Source : Le MR substituant (module NEMO)

  Destination : Le HA primaire (module NEMO).

  Description : message de demande d'ouverture de tunnel pour le trafic de données.

  Format : voir figure 4.13.

Payload Proto	Header Len	MH Type = 63	Reserved
Checksum		Sequence ID	LifeTime
MNP			
CoA			
Motif			
Options			

Fig. 4.13 – Format du message Tunnel_Opening_Request

- Motif : donne le motif de la requête, valeur 6300 pour la gestion de mobilité (rupture du lien, la CoA correspondante au lien rompu est spécifiée dans le champ options), valeur 3250 pour la gestion du trafic.

- **Message Tunnel_Opening_Replay**

  Source : Le HA primaire (module NEMO).

  Destination : Le MR substituant (module NEMO) ayant émis la requête Tunnel_Opening_Request

  Description : message de demande d'ouverture de tunnel pour le trafic de données.

  Format : voir figure 4.14.

Payload Proto	Header Len	MH Type = 64	Reserved
Checksum		Sequence ID	LifeTime
MNP			
CoA			
Motif			
Response Code			

Fig. 4.14 – Format du message Tunnel_Opening_Replay

Les champs MNP, CoA et Motif sont copiés du message Tunnel_Opening_Request.

- Response Code (4 octets) : donne le code de la réponse au message Tunnel_Opening_Request, les codes suivants sont définis :

  - 6400 pour Successful Operation
  - 6401 pour Tunnel Already Open
  - 6402 pour Mobile Router Operation not permitted
  - 6403 pour Invalid Prefix
  - 6404 pour Not Authorized for Prefix

- **Message Tunnel_Suppression**

  Source : MNPx (PDC module MTM)

  Destination : un MR ayant un tunnel ouvert avec le HA primaire (module NEMO).

  Description : message de demande de suppression du tunnel du binding cache du HA primaire.

  Format : voir figure 4.15

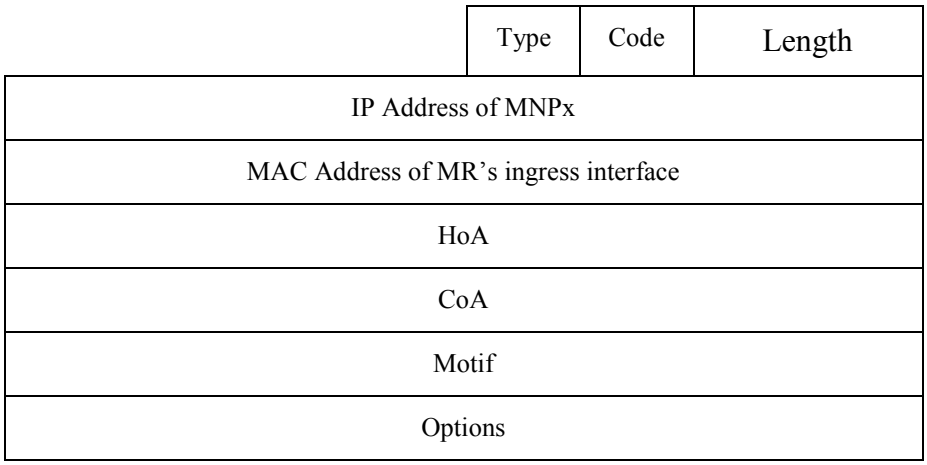

Fig. 4.15 – Format du message Tunnel_Suppression

- Type (4 bits) : spécifie le type du message (valeur 3 pour la catégorie Tunnel_Suppresion)
- Code (4 bits) : donne le code du message (valeur 1 pour Tunnel_Suppression)
- Length (1 octet) : longueur du paquet en octets
- Motif : donne le motif de la requête, valeur 300 pour rupture du lien.

Les autres champs sont les mêmes que ceux du message New_Tunnel_Notification (Type = 1).

- **Message Tunnel_Suppression_Confirmation**

  Source : Le MR ayant reçu du HA primaire le message Tunnel_Dereg_Replay (module NEMO)

  Destination : MNPx (PDC module MTM)

  Description : message de confirmation de suppression du tunnel du binding cache du HA primaire.

  Format : voir figure 4.16.

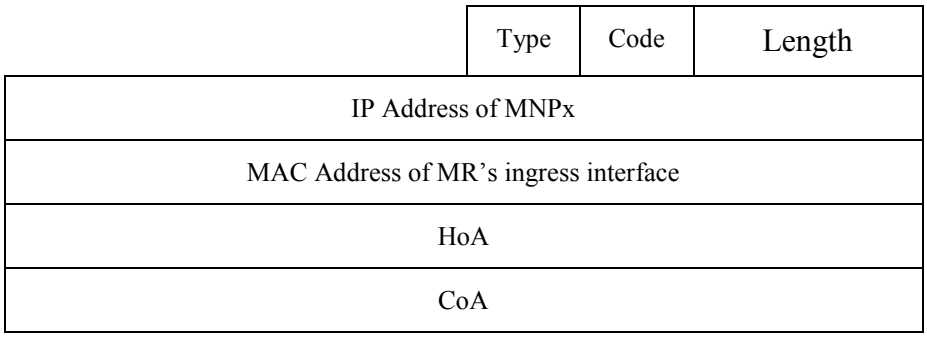

Fig. 4.16 – Format du message Tunnel_Suppression_Confirmation

- Type (4 bits) : spécifie le type du message (valeur 3 pour la catégorie Tunnel_Suppresion)
- Code (4 bits) : donne le code du message (valeur 2 pour Tunnel_Suppression_Confirmation)
- Length (1 octet) : longueur du paquet en octets

Les autres champs sont les mêmes que ceux du message Tunnel_Suppresion.

- **Message Tunnel_Dereg_Request**

  Source : Le MR ayant reçu du MNPx le message Tunnel_Suppression

  Destination : Le HA primaire (module NEMO).

  Description : message de demande de dé-registration du tunnel du binding cache du HA primaire.

  Format : voir figure 4.17.

- CoA of MR (originating message): adresse CoA du MR qui transmet la requête
- Motif : rupture du lien (code 6000), MR hors service (code 6001), …
- CoA of target MR : adresse CoA du MR dont le lien est rompu.

Payload Proto	Header Len	MH Type = 60	Reserved
Checksum		Sequence ID	LifeTime
MNP			
CoA of MR (originating message)			
Motif			
Options (CoA of target MR)			

Fig. 4.17 – Format du message Tunnel_Dereg_Request

- **Message Tunnel_Dereg_Replay**
  Source : Le HA primaire (module NEMO).
  Destination : Le MR ayant émis le message Tunnel_Dereg_Request.
  Description : réponse au message de Tunnel_Dereg_Request.
  Format : voir figure 4.18

Payload Proto	Header Len	MH Type = 61	Reserved
Checksum		Sequence ID	LifeTime
CoA of MR (originating message)			
CoA of target MR			
Reason Code			

Fig. 4.18 – Format du message Tunnel_Dereg_Replay

- Reason Code :
  6100 pour Successful Operation
  6101 pour Rejected Operation
  6102 pour Tunnel Does not exist
  6403 pour Mobile Router Operation not permitted

- **Message Tunnel_Alive_Request**
  Source : Le HA primaire (module NEMO).
  Destination : MR cible du test de survivabilité de tunnel
  Description : message de test de survivabilité de tunnel.
  Format : voir figure 4.19.

Payload Proto	Header Len	MH Type = 59	Reserved
Checksum		Sequence ID	LifeTime
Source : IPv6 Adresse of Primary HA			
Destination : CoA of MR			
Payload Data			

Fig. 4.19 – Format du message Tunnel_Opening_Replay

- Payload Data : une séquence binaire de 16 octets choisi aléatoirement par le HA primaire.

- **Tunnel_Alive_Replay**
  Source : MR cible du test de survivabilité de tunnel
  Destination : Le HA primaire (module NEMO).
  Description : réponse au message Tunnel_Alive_Request.
  Format : voir figure 4.20.

Payload Proto	Header Len	MH Type = 60	Reserved
Checksum		Sequence ID	LifeTime
Source : CoA of MR			
Destination : IPv6 Adresse of Primary HA			
Payload Data			

Fig. 4.20 – Format du message Tunnel_Opening_Replay

- Payload Data : reproduction de la même séquence binaire de 16 octets envoyée par le HA primaire.

IV.6 Procédures du handover soft (commutation de tunnel)

Considérons à nouveau l'exemple de la figure 4. 3. Admettons que le déplacement du réseau NEMO fait que son MR primaire MR1 perd ou est sur le point de perdre la connectivité à son réseau d'accès actuel (l'évènement considéré dépendra du service MIH utilisé, soit MIH_Link_Down ou

MIH_Link_Going_Down, ou même MIH_Get_Status). Quand le MNPx détecte cet évènement au moyen du composant de détection d'environnement EDC, il regarde immédiatement dans son cache MR_Data les MRs substituants disponibles (Tunnel Status = 1, Active = 0), il en sélectionne un suivant une politique prédéfinie (par exemple suivant la bande passante, ou le plus récent, …) et lui envoie un message Tunnel_Activation_request l'invitant à demander au HA1 (HA primaire) l'ouverture du tunnel associé (Fig. 4.21).

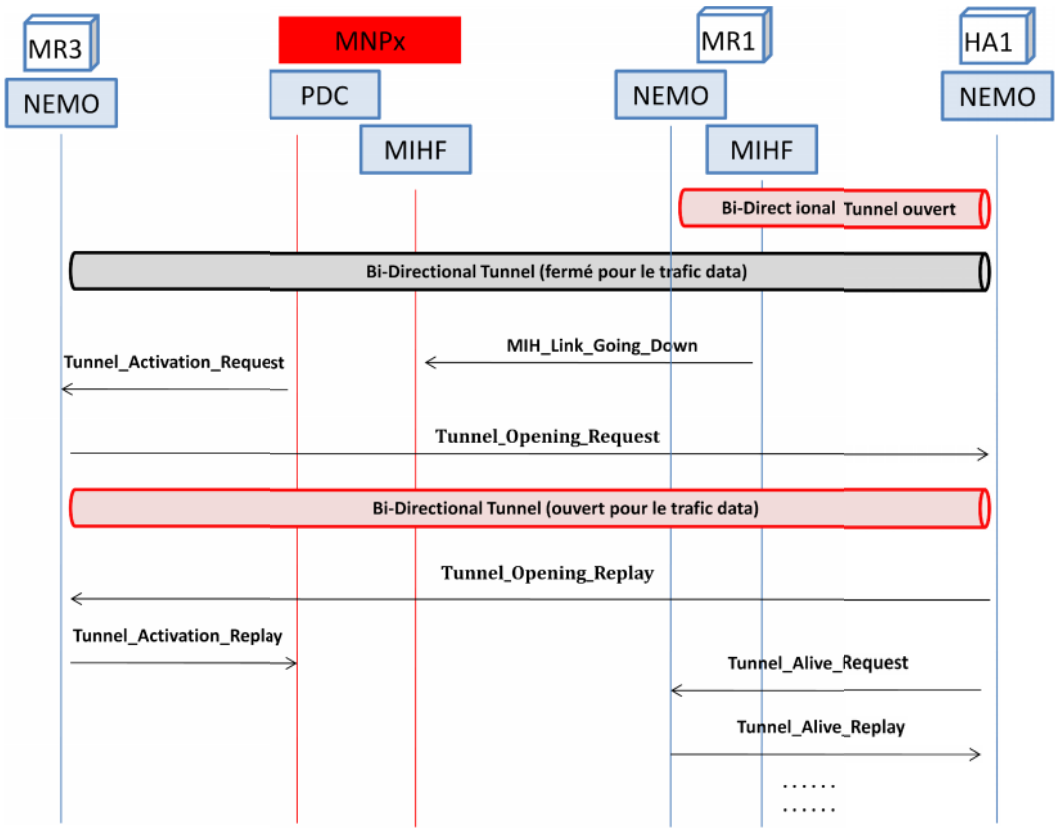

Fig. 4.21 – Procédure d'ouverture de tunnel pour le trafic de données

Supposons que MNPx choisit MR3 pour remplacer MR1. Le MNPx envoie donc le message Tunnel_Activation_Request à MR3, celui-ci envoie à son tour un message Tunnel_Opening_Request à HA1 lui indiquant les paramètres et le motif de cette demande (tunnel MR1_HA1 inaccessible). À la réception et la validation de ce message,

- HA1 ouvre le tunnel HA-MR3 dans les deux directions par lequel le trafic en provenance ou à destination du réseau NEMO est immédiatement véhiculé.
- HA1 transmet à MR3 une réponse Tunnel_Opening_Replay

Une fois que MR3 a reçu un message Tunnel_Opening_Replay avec la valeur du champ 'Response Code' = 6400 (Successful Operation), il répond au MNPx par un message Tunnel_Activation_Replay (Response Code = 240).

Le HA1 utilisera simultanément les tunnels HA1-MR1 et HA1-MR3 jusqu'à confirmation de la rupture du tunnel HA1-MR1. HA1 emploiera un procédé spécial de test de survivabilité du tunnel, il envoie au MR1 un message Tunnel_Alive_Request. Si le MR1 n'a pas perdu son lien avec le réseau d'accès, il répondra par le message Tunnel_Alive_Replay.

Le HA1 répétera ce test pendant un délai prédéfini que nous avons appelé AliveTestDelay (par défaut 30 s). La période de répétition est fixée à 3s. Si à l'expiration de ce délai, le MR1 répond toujours, alors le HA1 maintient le tunnel HA1-MR1et peut fermer ou non le tunnel HA1-MR3 suivant les stratégies de routage implémentées au niveau de HA1 (bicasting, partage de charge, préférences des applications,…). Si au contraire, avant l'expiration du délai AliveTestDelay le routeur HA1 ne reçoit pas successivement trois messages Tunnel_Alive_Replay, il conclue que MR1 à perdu son lien avec le réseau d'accès ; HA1 supprime donc l'entrée correspondante au MR1 de son binding cache. Les figures 4.22, 4.23 et 4.24 donnent, en notation Abstract Protocol Notation [83], les algorithmes exécutés respectivement par un MR (module NEMO), le HA primaire (module NEMO) et le MNPx (module MTM) dans le cadre de la présente extension.

```
 1 : bool newTunnel;
 2 : integer MRType; ( Mr primaire : MRTYpe=1, MR secondaie: MRType=0)

 3 : newTunnel →
 4 : send New_Tunnel_Notification to MNPx

 5 : receive Sub_Reg_Invite from primary HA→
 6 :    if (MRType==1) then
 7 :       discard message;
 8 :    else
 9 :       if (message valide) then
10 :          send Substitute_BU to primary HA ;
11 :       else
12 :          discard message;
13 :       fi
14 :    fi

15 : receive Substitute_BACK from primary HA→
16 :    if (MRType==1) then
17 :       discard message;
18 :    else
19 :       establish bi-directional tunnel with primary HA;
20 :    fi

21 : receive New_Sub_Reg from MNPx →
22 :    send Sub_Reg_Request to primary HA ;

23 : receive Substitute_Reg_Notification from primary HA→
24 :    send Substitute_Reg_Confirmation to MNPx ;

25 : receive Tunnel_Activation_Request from MNPx →
26 :    if (MRType==1) then
27 :       discard message;
28 :    else
29 :       send Tunnel_Opening_Request to primary HA ;
30 :    fi

31 :    receive Tunnel_Opening_Replay from primary HA →
32 :    if (MRType==1) then
33 :       discard message;
34 :    else
35 :       send Tunnel_Activation_Replay to MNPx ;
36 :    fi

37 : receive Tunnel_Alive_Request from primary HA →
38 :    send Tunnel_Alive_Replayt to primary HA ;
```

Fig. 4.22 – Algorithme exécuté par un MR (module NEMO)

```
1 :  receive Sub_Reg_Request from  MRi→
2 :     generate HA's Nonce;
3 :     send  Sub_Reg_Invite to MRj  (using HoAj);

4 :  receive Substitute_BU from  MRj→
5 :        if (message valide) then
6 :           update binding cache;
7 :           send Substitute_BAck to MRj  (using CoAj);
8 :           send Substitute_Reg_Notification to MRi ;
9 :        else
10 :          discard message;
11 :       fi

12 :  receive Tunnel_Opening_Request  from  MRj→
13 :     open MRj for data traffic;
14 :     send Tunnel_Opening_Replay to MRj ;
15 :     start survivability test;
```

Fig. 4.23 – Algorithme exécuté par le HA primaire (module NEMO)

```
1 :  bool  primaryMR; (MR primaire : PrimaryMR=true, MR secondaire: PrimaryMR=false)
2 :
3 :  receive New_Tunnel_Notification from  MRi→
4 :     if (PrimaryMR) then
5 :        switch traffic to primary MR;
6 :     else
7 :        lookup in  MR_data cache for Active Tunnel (say MRj);
8 :        send New_Sub_Reg to MRj ;
9 :     fi

10 :  receive Substitute_Reg_Confirmation from  MRj→
11 :     update MR_data cache;

12 :  receive remote MIH_Link_Going_Down  from MRi →
13 :     lookup in MR_data cache for available tunnels (Tunnel status=1);
14 :     select the most recent tunnel (say MRi);
15 :     send Tunnel_Activation_Request to MRi;

16 :  receive Tunnel_Activation_Replay from MRi→
17 :     update MR_data cache;
18 :     forward outbound traffic via MRi;
```

Fig. 4.24 – Algorithme exécuté par le MNPx (module MTM)

IV. 7 Implémentation et Evaluation

IV. 7.1 Implémentation sous NS2

L'implémentation est faite sur la version NS-2.29 [80] intégrant le package MIH de NIST [81]. D'une part, nous avons créé un agent C++ MTMAgent héritant de la classe Agent de NS-2 [79], pour supporter la gestion de la mobilité au niveau de l'entité MNPx. Les messages implémentés sont : New_Sub_Reg, Tunnel_Activation_request et Tunnel_Activation_Replay.

D'autre part, nous avons porté des modifications sur les agents NEMO implémentés au niveau du MR et du HA pour supporter les mécanismes d'enregistrement des CoAs multiples de routeurs secondaires et de commutation de tunnel, nous avons modifié le cache du HA et ajouté les messages suivants : New_tunnel_Notification, Sub_Reg_Request, Substitute_BU, Substitute_BACK, Substitute_Reg_Notification et Substitute_Reg_Confirmation.

IV. 7.2 Simulations

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

La topologie du réseau simulé est présentée à la figure 4.25, où un adressage hiérarchique [79] est adopté :

- Le nœud 0 : Un routeur (0.0.0) présentant quatre interfaces filaires.
- Le nœud 1 : Un nœud correspondant CN (3.0.0).
- Le nœud 2 : Le Home Agent HA1 (4.0.0) du routeur primaire MR1.
- Le nœud 3 : Une station de base IEEE 802.11 (routeur d'accès AR1 (1.0.0)) avec une couverture de 100 m.
- Le nœud 4 : Une station de base IEEE 802.16 (routeur d'accès AR2 (2.0.0)) avec une couverture de 1000 m.
- Le nœud 5 : Le routeur mobile primaire MR1 (4.1.0) présentant deux interfaces : une interface externe (802.11) et une interface interne (802.3) reliée au MNPx.
- Le nœud 6 : Un routeur mobile secondaire MR2 (4.2.0) présentant deux interfaces : une interface externe (802.16) et une interface interne (802.3) reliée au MNPx.
- Le nœud 7 : Le routeur MNPx (4.3.0) présentant trois interfaces filaires (802.3).
- Le nœud 8 : un MNN (4.3.1) relié directement au MNPx.

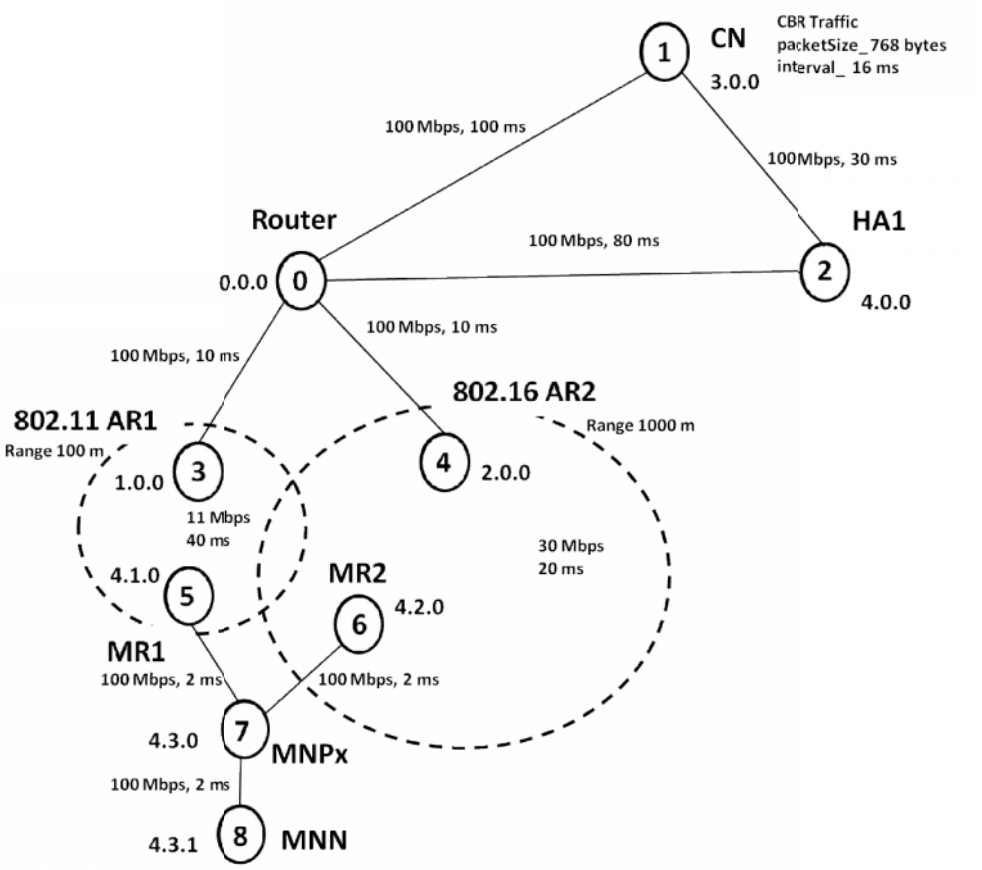

Fig. 4.25 – Topologie du réseau NEMO (n,n,1) simulé

Les caractéristiques des liens notamment la bande passante et le délai sont reportés sur la figure 4.25. Un trafic streaming CBR est émis par le CN à destination d'un nœud MNN du réseau NEMO (longueur des paquets = 768 octets, intervalle entre les paquets = 16 ms). Le temps de simulation est fixé à 20 s.
Le simulateur NS-2 ne supporte pas la mobilité d'un réseau entier, pour cette raison nous avons émulé le mouvement du réseau NEMO en réduisant la puissance d'émission de la station de base IEEE 802.11 (routeur d'accès AR1 (1.0.0)). Suivant l'importance de la chute de puissance ainsi provoquée on déclenche ou bien le trigger LGD ou le trigger LD.

Nous considérons le scénario de simulation suivant :

Au début de la simulation (de t=0 jusqu'à t = 5 s), le réseau NEMO dispose d'un seul lien avec le réseau Internet, le lien avec la station de base 802.11 (AR1). La station de base 802.16 étant désactivée. Par conséquent un seul tunnel est disponible, celui établi entre le MR1 (routeur primaire) et son HA.

A t = 5 s, la station de base 802.16 est activée, un second tunnel est établi entre le routeur secondaire MR2 et le HA, MR2 s'enregistre au près du HA comme substituant de MR1.

A t = 10 s, nous déclenchons le trigger Link_Goig_Down au niveau du MR1, et ceci en réduisant convenablement la puissance d'émission de la station de base IEEE 802.11.

Puis à des instants t = 10 s, t = 10.05 s, t = 10.1 s, t = 10.15 s, t = 10.2 s, …., t = 10.5 s, de la même manière que précédemment nous déclenchons le trigger Link_Down, et cela pour balayer la fourchette [0,500 ms] des valeurs possibles pour le paramètre TimeInterval associé au trigger LGD. Cette manipulation nous permettra de déterminer le seuil pour lequel il est possible d'assurer une connectivité sans couture.

IV. 7.3 Résultats

Nous avons représenté sur la figure 4.26, le temps d'interruption de services en fonction du paramètre TimeInterval. Il est déterminé par le temps écoulé entre la réception du dernier paquet de données (Trafic CBR) via MR1 et la réception du premier paquet de données via MR2.
Il est tout à fait clair que ce délai de déconnexion est inversement proportionnel au temps TimeInterval, plus ce dernier augmente plus nous aurons la chance de terminer les opérations de commutation de tunnels avant que le lien courant tombe.

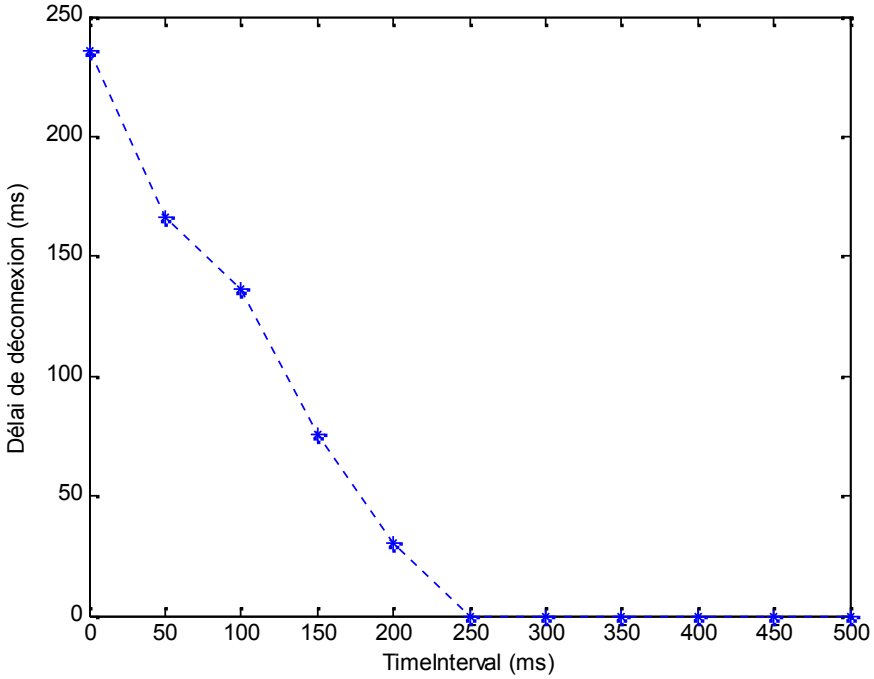

Fig. 4.26 – Délai d'interruption de services en fonction du paramètre TimeInterval (LGD trigger)

Une valeur 0 pour TimeInterval signifie que le trigger utilisé pour déclencher la commutation de tunnels est le Link_Down, c'est-à-dire qu'on a affaire un handover hard.

Nous notons la valeur seuil de 250 ms pour TimeInterval, pour laquelle le délai de déconnection est nul. Pour les applications telles que la visioconférence et la voix sur IP (VoIP) un délai de 50 ms est tolérable [63], ainsi un seuil de 200 ms pour TimeInterval peut être retenu. Noter que nous avons utilisé la valeur maximale du RTT entre AR2 et HA donnée par la référence [66], soit 200 ms.

La figure 4.27 représente le nombre de paquets perdus en fonction de TimeInterval. Nous pouvons le déterminer en faisant la différence entre le numéro de séquence (paquet TCP) du premier paquet de données reçu après rétablissement de la connexion et le numéro de séquence du dernier paquet de données reçu avant déconnexion. Un exemple est illustré sur la figure 4.28.

On note une perte maximale de 15 paquets pour le cas TimeInterval = 0. Si nous faisons une comparaison avec le protocole NEMO BS [15], avec la même application CBR (PacketSize = 768 octets, Interval = 16 ms), un handover de celui-ci d'une durée moyenne de 1250 ms engendrera une perte d'environ 78 paquets.

La représentation du débit du trafic reçu (Throughput) mesuré au niveau du MNN est donnée à la figure 4.29 pour les valeurs de TimeInterval : 0, 100 ms et 250 ms. Les allures des courbes de cette figure confirment les résultats obtenus précédemment.

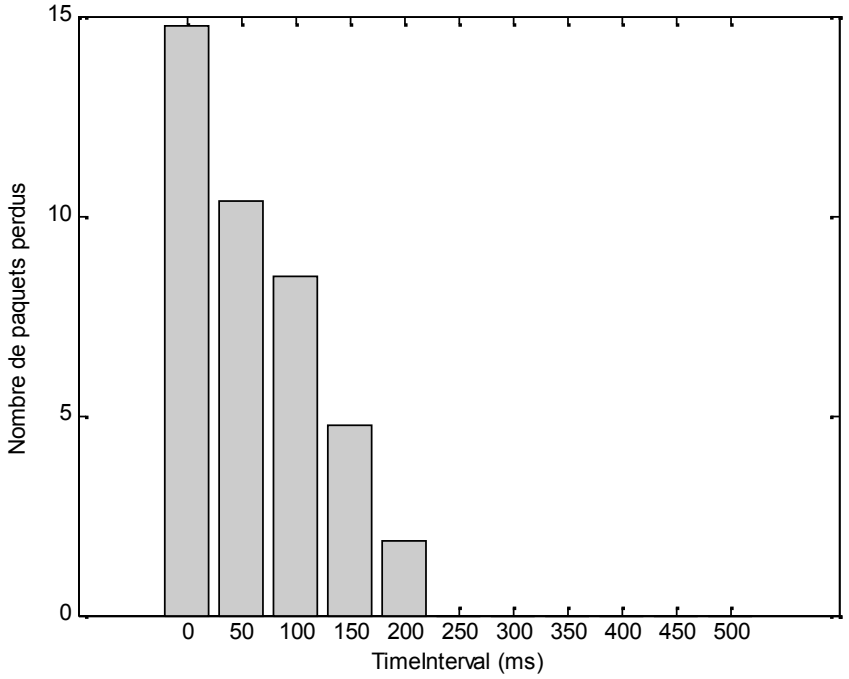

Fig. 4.27 – Pertes de paquets en fonction du paramètre TimeInterval (LGD trigger)

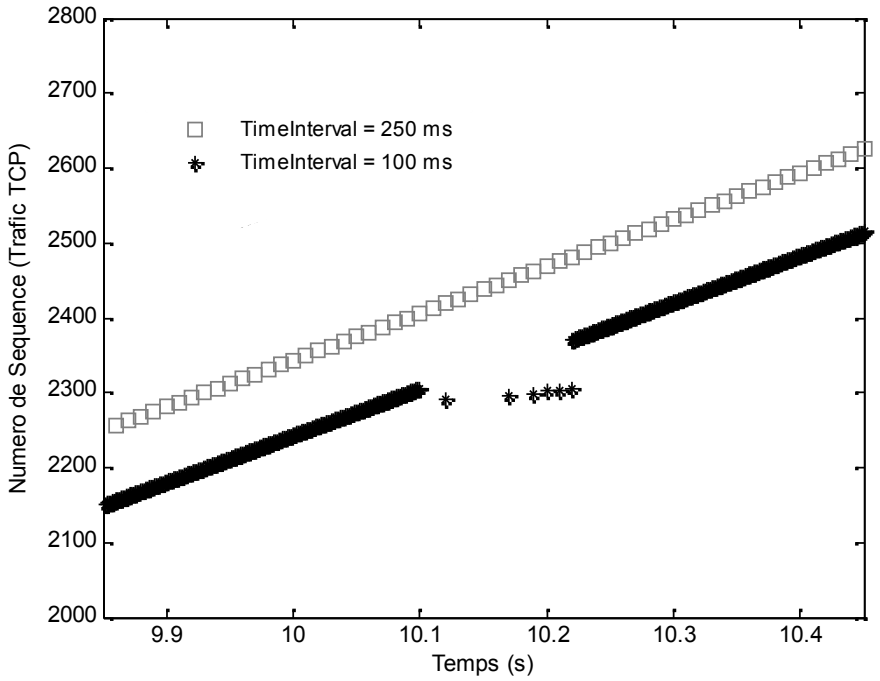

Fig. 4.28 – Mise en évidence des interruptions par Numéros de séquence TCP

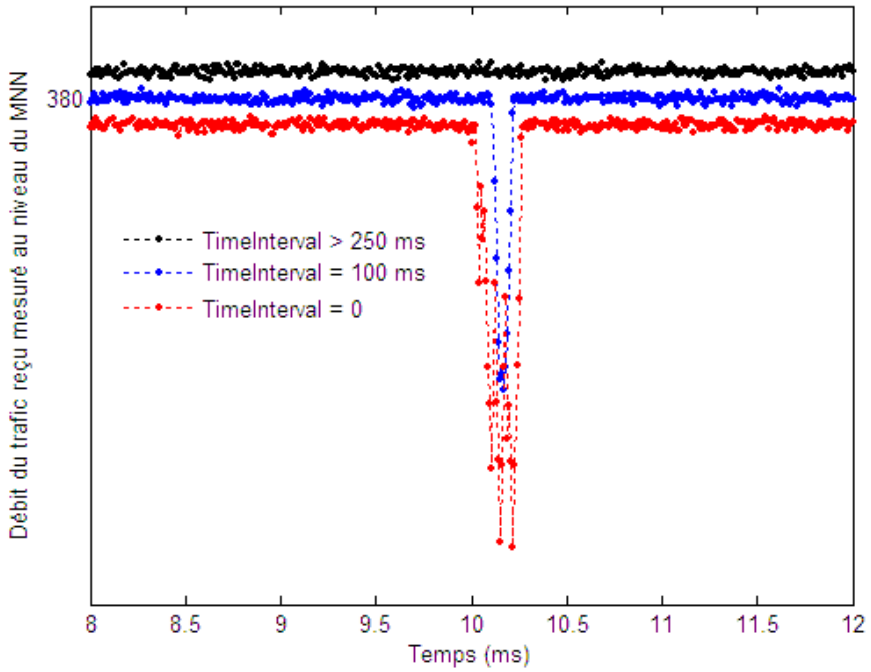

Fig. 4.29 – Débit du trafic CBR reçu en fonction du paramètre TimeInterval (LGD trigger)

IV.8 Conclusion

Nous avons décrit dans ce chapitre une nouvelle approche pour la gestion de mobilité dans le contexte NEMO multihomed (n, n, 1), indépendante de l'infrastructure réseau, ne nécessitant par conséquent aucun changement dans l'architecture Internet. La solution proposée permet de garantir une connectivité sans couture (seamless connectivity) pour répondre aux besoins des applications temps réel et exigeantes en QoS. Nous avons introduit l'entité centrale MNPx jouant le rôle de passerelle entre les MNNs embarqués et les MRs, et dont la tâche principale est la gestion intelligente des handovers et du trafic, avec l'appui des services MIH IEEE 802.21 locaux et remote.

Nos contributions dans cette partie de la thèse se résument dans les points suivants :

(i) Proposition d'une nouvelle architecture d'un réseau NEMO multihomed avec plusieurs MRs domiciliés dans différents HAs. Cette architecture est basée sur l'introduction de la notion de routeur primaire et routeur secondaire, et l'intégration d'une nouvelle entité nommée MNPx (Mobile Network Proxy) au sein du réseau mobile pour la gestion des handovers et la distribution du trafic entre les MRs d'une façon transparente pour les MNNs.

(ii) Conception d'un module MTM (Mobility and Trafic Management) constitué de deux composants : un premier composant nommé EDC (Environment Detector Component)

pour la détection d'environnement et un second composant nommé PDC (Policy Decision Component) pour prendre les décisions intelligentes de handover et de gestion de trafic.

(iii) Définition des mécanismes de Détection de rupture de lien basés sur les services Remote MIH IEEE 802.21.

(iv) Extension du protocole MIPv6-NEMO par le support d'enregistrement des CoAs multiples de routeurs secondaires (MRs substituant), et le support de commutation de tunnel.

(v) Définition des messages et élaboration des procédures du nouveau support de mobilité proposé.

(vi) Implémentation et simulation des mécanismes proposés sous NS2.

CHAPITRE 5

Handover Sans Coutures basé sur le Modèle NEMO multihomed (1,1,1)

V.1 Introduction

Dans ce chapitre, nous traitons le cas d'un réseau NEMO multi-domicilié (multihomed) où l'utilisation simultanée des liens multiples disponibles n'est pas nécessaire voir même non recommandée. Cela, peut être par exemple dans le cas où aucune politique de partage de charge ou de sélection de chemins n'est désirée, ou par exemple pour des raisons d'optimisation du coût de connexion ou de la consommation d'énergie. En effet, la disponibilité au sein d'un réseau NEMO de plusieurs interfaces de communication sans fil pose nécessairement la question de leur gestion et de la consommation d'énergie. L'activation d'une interface pour son attachement à un réseau d'accès a un coût énergétique et peut avoir un coût monétaire suivant le type de réseau. Cela ne devrait donc être fait que pour répondre à un besoin. Dans la suite, nous nous focalisons sur le cas d'un réseau NEMO pourvu d'un seul routeur mobile MR à plusieurs interfaces supportant IEEE 802.21, et nous nous proposons de développer un mécanisme permettant d'avoir une connectivité sans couture (seamless connectivity) précisément avec zéro délai et zéro paquets de perte, tout en minimisant le temps d'activation simultanée des interfaces de communication sans fils. Ce mécanisme devra offrir la continuité des sessions d'une façon transparente pour les utilisateurs embarqués dans le réseau NEMO. Pour ce faire, nous allons adopter une approche proactive consistant à une préparation du handover (attachement aux réseaux d'accès disponibles, enregistrement de la nouvelle CoA au niveau du Home

Agent, établissement d'un tunnel entre le MR et le HA), et puis à une anticipation du handover (commutation de tunnel) suite à une prédiction de l'évènement Link_Down. Pour remplir les objectives signalés plus haut, la commutation du tunnel doit impérativement se terminer avant le trigger LD. A cet effet, le trigger Link_Going_Down (LGD) est utilisé pour la préparation du handover et un nouveau trigger que nous avons appelé Link_switch_Imminent (LSI) est défini pour le déclenchement de l'anticipation du handover. Le seuil du trigger LGD est calculé sur la base du temps nécessaire estimé pour le handover NEMO. Le seuil du trigger LSI est déterminé en fonction du temps nécessaire estimé pour la commutation d'un tunnel MR-HA. Ces temps sont estimés à partir des informations récupérées des réseaux d'accès disponibles. La détermination des seuils des triggers est possible grâce un modèle de propagation déterminé qui implique la vitesse de déplacement du réseau NEMO. Originalement, les seuils des triggers MIH ont des valeurs fixes prédéfinies. Cependant, cette approche n'est pas appropriée pour des environnements dynamiques et trouve très vite sa limite lorsqu'on cherche par exemple à optimiser le temps d'anticipation du handover. Dans notre proposition, une configuration dynamique et adaptative de ces seuils est effectuée en fonction des paramètres de l'environnement.
Avec cette manière de procéder, nous pouvons assurer une probabilité de prédiction du handover évitant ainsi les scénarios de ping-pong.

V.2 Modèle de mobilité

Dans cette partie, nous supposons un modèle NEMO multihomed (1, 1, 1) restreint à : un seul routeur mobile MR, un seul Home Agent HA et un seul préfixe MNP (Mobile Network Prefix, [28], § chapitre III). Nous considérons donc un MR unique intégrant des interfaces multiples. Ces interfaces peuvent être issues de technologies différentes (e.g IEEE 802.11, IEEE 802.16, 3GPP, 3GPP2) ou de même technologie. Le déplacement entre deux réseaux ayant la même technologie d'accès ne peut être réalisé que si le MR possède deux interfaces de cette technologie d'accès. De ce fait, des interfaces similaires seront utilisées pour réaliser des handovers soft vers des réseaux d'accès cibles de même technologie que le réseau d'accès courant sur le point d'être inaccessible.

A noter qu'une seule interface de technologie donnée ne permet pas l'exécution d'un handover sans interruption de services ; une rupture du lien courant (Link_Down event) est indispensable pour l'association au nouveau réseau. D'un autre côté, pour la facilité de gestion des interfaces multiples nous imposons au MR d'être compatible avec la norme IEEE 802.21, mais dans le but de réaliser un schéma de handover indépendant de l'assistance de l'infrastructure réseau, seuls les services MIH locaux sont utilisés. D'un autre coté, le HA doit supporter l'enregistrement d'adresses CoA multiples (MCoA, [47], § chapitre III). Nous proposons donc la pile de gestion de la mobilité de la figure 5.1, intégrant les trois entités suivantes :

- Le module MIHF (Media Independent Handover Function) : dont le rôle principal est d'assister les modules de gestion de la mobilité (niveau L3) pour le support d'interfaces multiples et l'exécution des handovers.

- Le module NEMO+MCoA : module du protocole de la gestion de la mobilité NEMO modifié pour prendre les nouvelles fonctionnalités telles que l'enregistrement de multiples CoAs (MCoA) et la commutation de tunnels.

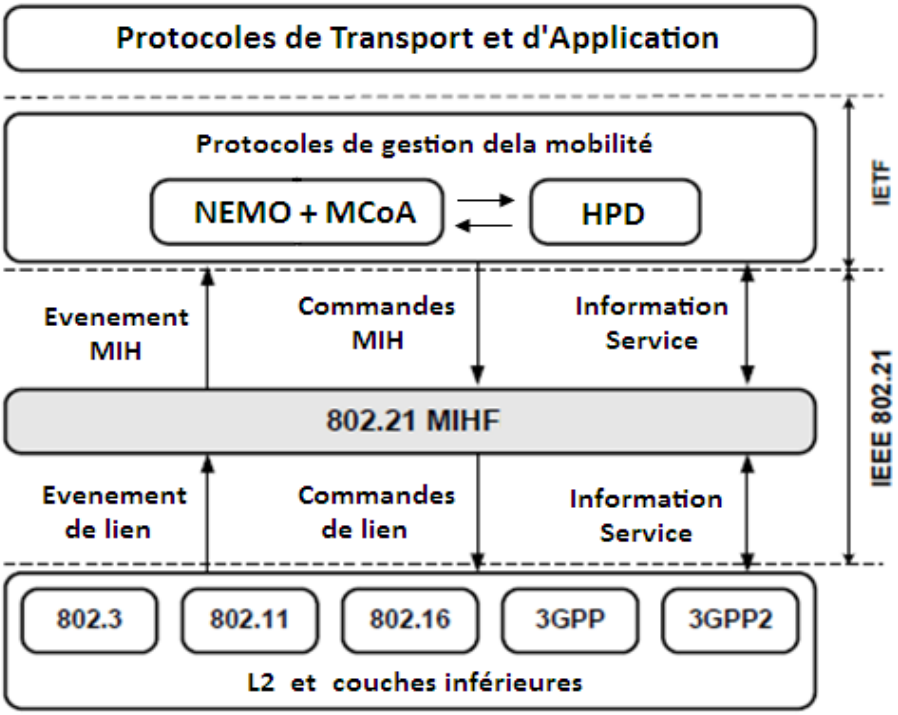

Fig. 5.1- Architecture de la pile de gestion de la mobilité proposée

- Le module HPD (Handover Policy Decision) : un nouveau module implémenté au niveau L3 pour gérer les handovers d'une manière intelligente. Le HPD échange les primitives avec le MIHF et le module NEMO, il est responsable également de la maintenance de deux caches, un pour les liens détectés (*AvailableLinkCache*) et un autre pour les chemins alternatifs disponibles (*AlternativePathCache*) qui seront détaillés plus loin.

  Primitives échangées avec le MIHF (voir section V.3) :

  - MIH_Link_Detected
  - MIH_Configure_Link_Threshold
  - MIH_Link_Going_Down
  - MIH_Link_Connect
  - MIH_Link_UP

- Link_Switch_Imminent
- MIH_Switch

Primitives échangées avec le Module NEMO (voir section V.6) :

- HPD_L3_Soft_Handover_Initiate (link ID, IF)
- HPD_L3_Soft_Handover_Complete
- HPD_Tunnel_Switch_Req (link ID, IF, CoA)
- HPD_Tunnel_Switch_Rep

V.3 Services MIH utilisés

Nous utilisons un sous-ensemble des services MIH existantes ainsi que de nouveaux services que nous avons proposés pour faciliter la prise de décision du handover. Le tableau 5.1 présente ces services (primitives) et les paramètres correspondants.

Primitive	Service	Paramètres
MIH_Link_Detected	MIES	MR IF MAC Addr, MAC addr of new PoA, MIH capability, Link Type
MIH_Link_Up	MIES	MR IF MAC Addr, MAC addr of new PoA, Link ID
MIH_Link_Down	MIES	MR IF MAC Addr, MAC addr of new PoA, Reason Code
MIH_Link_Going_Down	MIES	MR IF MAC Addr, MAC Addr of Curent PoA, TimeInterval, ConfidenceLevel
MIH_Link_Switch_Imminent	MIES	MR IF MAC Addr, MAC Addr of Curent PoA, TimeInterval, ConfidenceLevel
MIH_Link_Event_Rollback	MIES	MR IF MAC Addr, Event ID
MIH_Configure_Link_Threshold	MICS	LinkParameter, nitiateActionThreshold, RollbackActionThreshold, ExecuteActionThreshold
MIH_Switch	MICS	Old Link ID, New Link ID

Tableau 5.1 – services MIH utilisés

Lorsqu'une seule interface est utilisée, le MR ne peut être associé simultanément avec plus d'un routeur d'accès AR. Par conséquent, avant d'établir une connexion avec un nouvel AR, il est obligé de rompre ses communications avec l'ancien AR (Hard handover). Ainsi, dans le protocole MIPv6-NEMO le processus du handover est déclenché par l'événement Link_Down (LD) ; Cependant dans l'approche FMIPv6-NEMO [26], l'anticipation du handover est réalisée avec l'assistance du réseau en utilisant le trigger Link_Going_Down (LGD) à seuil fixe.

Dans notre proposition basée sur le multihoming, le processus du handover doit s'achever avant le l'événement Link_Down du lien courant. Donc, au lieu d'utiliser le trigger LD, nous avons prévu l'utilisation de deux triggers : Link_Going_Down (LGD) et Link_Switch_Imminent (LSI). Le premier trigger LGD est utilisé pour déclencher la préparation du handover, il est généré sur la base du temps nécessaire estimé pour le handover NEMO ; Contrairement à FMIPv6-NEMO, le seuil correspondant n'est pas fixé. Le second trigger LSI étant utilisé pour le déclenchement de l'anticipation du handover, il est généré sur la base du temps nécessaire estimé pour la commutation d'un tunnel MR-HA. La figure 5.2 montre la correspondance des niveaux de seuils de puissances reçues (RSS: Received Signal Strength) pour chaque événement.

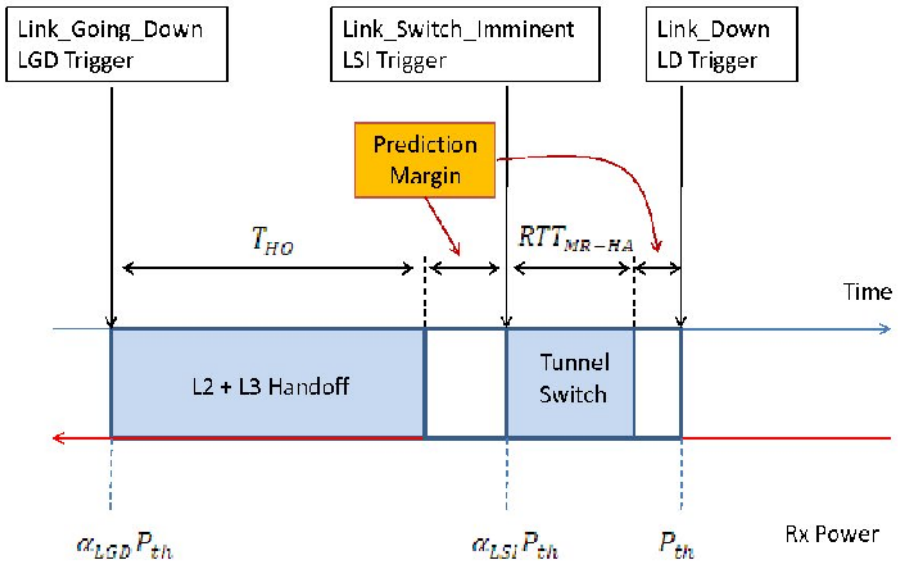

Fig. 5.2- Génération des Triggers LGD et LSI

α_{LGD} et α_{LSI} sont les coefficients des niveaux seuils de la RSS respectivement pour le trigger LGD et le trigger LSI ($\alpha_{LGD} > \alpha_{LSI} > 1$).

Le trigger LGD dans [68] et qui est utilisé d'ailleurs dans MIPv6-NEMO [26], est basé sur un coefficient α_{LGD} prédéfini. Si la valeur mesurée de RSS descend en dessous de $\alpha_{LGD}P_{th}$ alors le trigger LGD est déclenché. Dans la présente proposition, les coefficients α_{LGD} et α_{LSI} sont configurés dynamiquement à partir des informations récoltées des réseaux de voisinage. La primitive MIH_Configure_Link_Threshold est utilisée à cette fin.

V.4 Estimation des temps nécessaires pour le handover NEMO et la commutation de tunnel

Le temps nécessaire T_{HO} pour le handover NEMO et le temps nécessaire T_{TS} pour la commutation d'un tunnel MR-HA sont des facteurs importants pour le déclenchement des triggers de lien associés. Le trigger LGD doit être déclenché avant l'événement LD par au moins le temps requis pour préparer et exécuter un handover. Le trigger LSI doit être déclenché au minimum T_{TS} avant l'événement LD. Dans notre schéma, le calcul de la valeur de α_{LGD} est basé sur le temps total T_{LGD} suivant:

$$T_{LGD} = T_{HO} + \Delta T_{HO} + T_{TS} + \Delta T_{TS} \quad \textbf{(5.1)}$$

Où :

T_{HO} est donnée par **(2.1)**

ΔT_{HO} et ΔT_{TS} sont des marges de sécurité

$$\Delta T_{HO} = \gamma_1 \% T_{HO} \quad \textbf{(5.2)}$$

$$\Delta T_{TS} = \gamma_2 \% T_{TS} \quad \textbf{(5.3)}$$

γ_1 et γ_2 sont des pourcentages pouvant prendre apriori des valeurs entre 0 à 20.

Equation **(5.1)** peut être écrite sous la forme suivante:

$$T_{LGD} = T_{L2} + T_{L3} + \Delta T_{HO} + RTT_{MR-HA} + \Delta T_{TS} \quad \textbf{(5.4)}$$

Et de la même manière, nous avons pour α_{LSI} :

$$T_{LSI} = RTT_{MR-HA} + \Delta T_{TS} \quad \textbf{(5.5)}$$

Pour estimer le temps du handover (L2+L3) et celui de la commutation de tunnel, nous utilisons :

- Le type du nouveau lien détecté pour estimer le temps du handover L2 et le delai aller-retour RTT_{MR-nAR} du MR vers le nouveau AR.
- Le lien courant pour estimer le temps du handover L3 et le temps de la commutation du tunnel en mesurant les délais RTT_{MR-oAR} et RTT_{HA-oAR} .

V.5 Détermination des valeurs des seuils des triggers LGD et LSI

Etant donné un modèle de propagation [59], une méthode analytique peut être utilisée pour extraire les valeurs des coefficients α_{LGD} et α_{LSI} [60, 61].

Supposons un modèle de propagation logarithmique (log-distance path loss model [59]) représenté par l'équation **(5.6) :**

$$\left[\frac{P_{rx}(d)}{P_{rx}(d_0)}\right]_{dB} = -10\beta\log\left(\frac{d}{d_0}\right) \quad \textbf{(5.6)}$$

Où d est la distance entre l'émetteur et le récepteur exprimée en mètres, $P_{rx}(d)$ représente la puissance du signal reçu à la distance d exprimée en watts, β est l'exposant de l'affaiblissement, et $P_{rx}(d_0)$ est la puissance reçue à une distance de référence d_0, et qui peut être déterminée en utilisant le modèle de propagation en espace libre avec par exemple $d_0 = 1\ m$.

En admettant que le réseau mobile NEMO a une vitesse de déplacement constante v , les coefficients α_{LGD} et α_{LSI} peuvent être déterminés comme suit :

$$\alpha_{LGD} = \left|\frac{1}{1-\frac{v.T_{LGD}}{d_0}\left(\frac{P_{th}}{P_{rx}(d_0)}\right)^{\frac{1}{\beta}}}\right|^{\beta} \quad \textbf{(5.7)}$$

$$\alpha_{LSI} = \left|\frac{1}{1-\frac{v.T_{LSI}}{d_0}\left(\frac{P_{th}}{P_{rx}(d_0)}\right)^{\frac{1}{\beta}}}\right|^{\beta} \quad \textbf{(5.8)}$$

P_{th} est le niveau de puissance seuil correspondant au trigger LD (§ chapitre II).

Notons que la vitesse v peut etre estimée par l'approche suivante:

Supposons que la puissance reçue à l'instant t_i est $P_{rx}(d_i)$, et la puissance reçue à l'instant t_{i+1} est $P_{rx}(d_{i+1})$, alors à partir de l'équation **(5.6)** nous avons :

$$v = \frac{d_{i+1}-d_i}{t_{i+1}-t_i} \quad \textbf{(5.9)}$$

Ensuite:

$$v = \frac{d_0}{t_{i+1}-t_i}\left|\left(\frac{P_{rx}(d_0)}{P_{rx}(d_{i+1})}\right)^{\frac{1}{\beta}} - \left(\frac{P_{rx}(d_0)}{P_{rx}(d_i)}\right)^{\frac{1}{\beta}}\right| \quad \textbf{(5.10)}$$

Les figures 5.3et 5.4, respectivement les figures 5.5 et 5.6, montrent les variations des coefficients α_{LGD} et α_{LSI} pour différentes valeurs de β et différentes vitesses de déplacement. Les deux coefficients augmentent avec β, v et le temps nécessaire correspondant (T_{LGD} ou T_{LSI}). A titre indicatif, nous avons représenté sur la figure 5.7 les variations de α_{LGD} en fonction de β pour une valeur moyenne de 1.25 s du temps T_{LGD} .

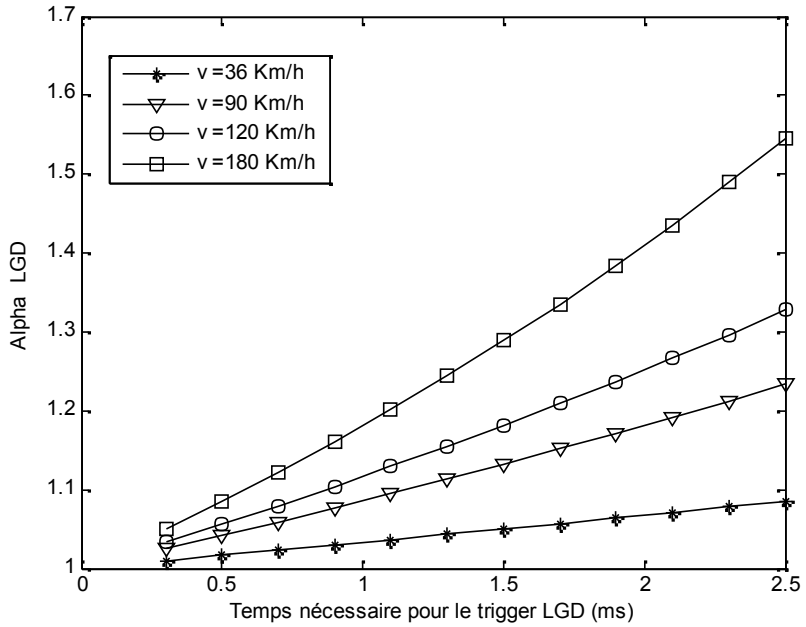

Fig. 5.3- Evolution de α_{LGD} en fonction de T_{LGD} ($\beta = 3$)

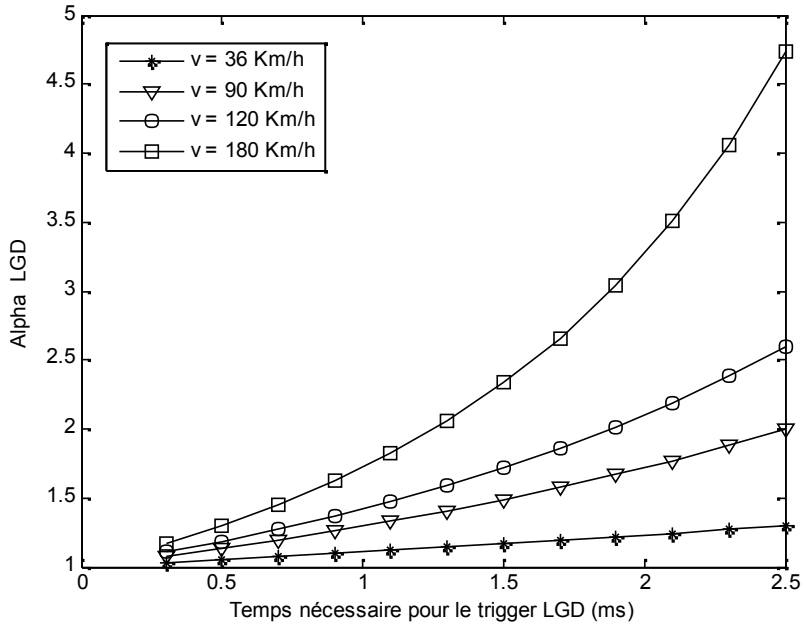

Fig. 5.4- Evolution de α_{LGD} en fonction de T_{LGD} ($\beta = 3.5$)

Cependant, pour réaliser un modèle de propagation plus réaliste, nous devons tenir compte des effets du shadowing résultants des obstacles et des multi-trajets.

Un composant additionnel $X_\sigma\,(dB)$ est introduit dans l'expression **(5.6)** du modèle logarithmique (log-distance path loss model) [59] :

$$\left[\frac{P_{rx}(d)}{P_{rx}(d_0)}\right]_{dB} = -10\beta \log\left(\frac{d}{d_0}\right) + X_\sigma \qquad \textbf{(5.11)}$$

X_σ est une variable aleatoire de distribution gaussienne à moyenne nulle et de variance σ.
Ce modèle est connu sous le nom de log-normal shadowing model [59].

Lorsque le composant $X_\sigma\,(dB)$ devient significatif, une moyenne de la puissance du signal reçu est nécessaire pour produire des mesures stables; Nous utilisons pour cela le simple estimateur récursif [62] défini par l'équation **(5.12) :**

$$\overline{P_{rx}}\,(i) = \delta\, P_{rx}(i) + (1-\delta)\overline{P_{rx}}\,(\text{i-1}) \qquad \textbf{(5.12)}$$

Où $P_{rx}(i)$ est la puissance du signal reçu à l'instant i, $\overline{P_{rx}}\,(i)$ est sa puissance moyenne au même l'instant i, et δ est un facteur de pondération.

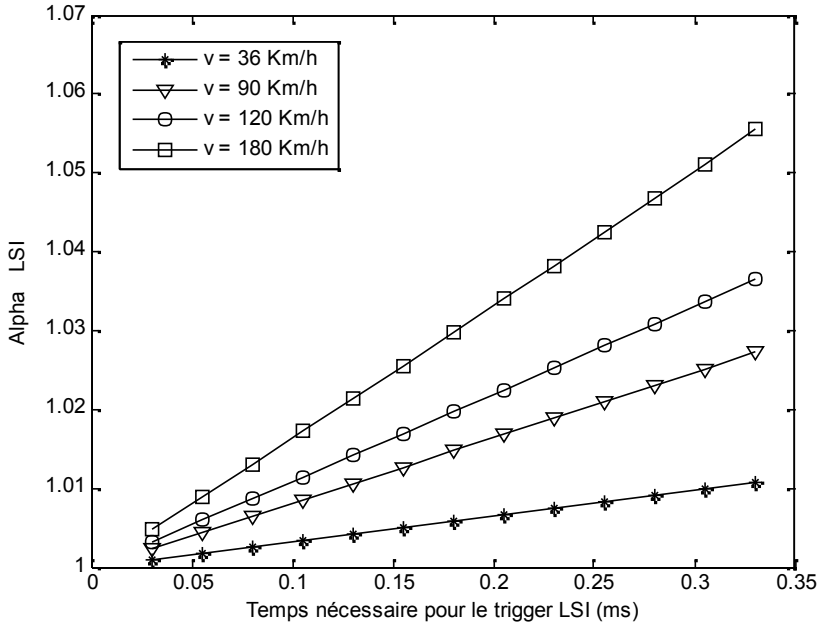

Fig. 5.5- Evolution de α_{LSI} en fonction de T_{LSI} ($\beta = 3$)

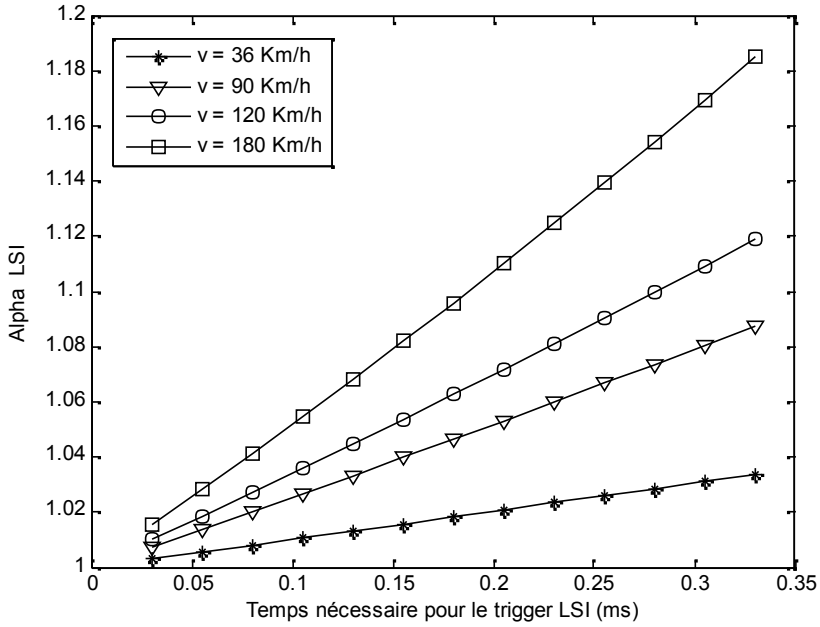

Fig. 5.6- Evolution de α_{LSI} en fonction de T_{LSI} ($\beta = 3.5$)

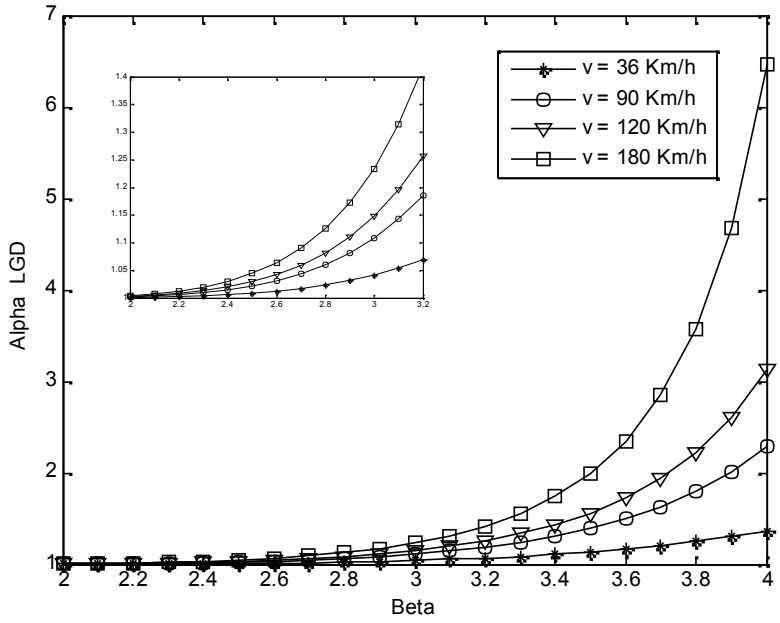

Fig. 5.7- Evolution de α_{LGD} en fonction de β ($T_{LGD} = 1.25\ s$)

V.6 Détails des opérations du handover soft proposé

Cette section définit les outils nécessaires (caches, messages, services, …) et décrit l'exécution des procédures de traitement des événements engendrés par le handover Make-Before-Brake intelligent proposé.

V.6.1 Hypothèses

Nous admettons que le réseau mobile NEMO est déjà connecté à un réseau d'accès, et qu'un tunnel est déjà établi et opérationnel entre le HA et le MR via une de ses interfaces multiples. Désignons par IF-1 cette interface active. Lorsque le réseau NEMO se déplace, le MR peut entrer dans une zone de couverture d'un autre réseau d'accès. Nous admettons que l'ancien et le nouveau réseau ont une zone de chevauchement commune dans laquelle le passage du réseau NEMO est suffisamment long pour permettre la configuration de la nouvelle interface et éventuellement la mise à jour de la localisation du MR.

V.6.2 Traitement d'une détection de lien

Si un événement Link_Detected est généré par une autre interface (soit par exemple IF-2) correspondante à la technologie du réseau d'accès cible, alors le MIHF translate cet événement au HPD (Fig. 5.8). Le HPD maintient pour les liens détectés un cache que nous avons appelé *AvailableLinkCache* (Tableau 5.2) :

Adresse MAC Interface MR	Adresse MAC Nouveau AR	Compatibilité MIH	Type Lien	Temps Expiration
IF-2				
IF-3				

Tableau 5.2 – Cache des liens disponibles (*AvailableLinkCache*)

Ce cache compte cinq champs que sont : l'adresse MAC de l'interface du MR concernée par le lien détecté, l'adresse MAC du routeur d'accès/point d'accès, la compatibilité MIH supportée ou non, le type du lien (IEEE 802.11, IEEE 802.16, 3GPP, 3GPP2, …) et enfin le temps d'expiration du lien (calculé en fonction de la période du scan de la technologie correspondante au type de lien).

Lorsque le HPD reçoit l'événement MIH_Detected_Link, il entame les deux procédures suivantes :

(i) Il fait la mise de son cache *AvailableLinkCache.*

(ii) Il envoie une requête au MIHF pour générer la primitive MIH_Configure_Link_Threshold permettant de configurer les seuils des triggers LGD et LSI pour l'interface IF-1.

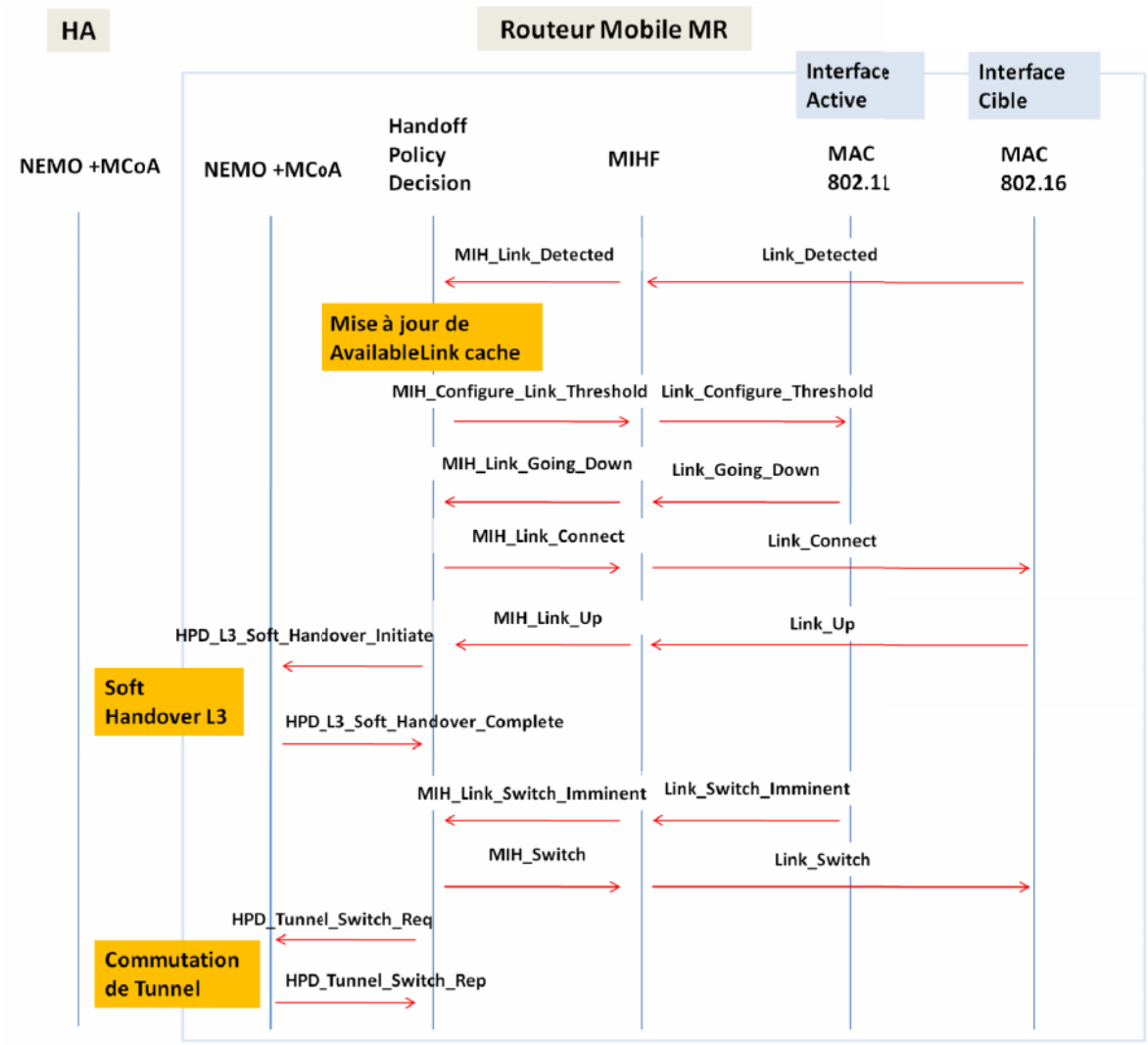

Fig. 5.8- Procédures du handover proposé : préparation et anticipation

V.6.3 Traitement d'un événement Link_Going_Down

Par suite d'un dépassement de seuil LGD, un événement Link_Going_Down est généré par l'interface IF-1, le MIHF translate cet événement au HPD qui procède comme suit :

(i) Il fait un scan des entrées de son cache *AvailableLinkCache* afin de choisir le lien approprié candidat à une nouvelle association et activer l'interface correspondante (Supposons que cette interface est IF-2).

(ii) Il envoie à MIHF une requête MIH_link_Connect pour activer l'interface IF-2; ceci est équivalent à un handover soft L2).

Si un événement Link_Up est reçu par MIHF de la part de l'interface IF-2, le HPD est notifié en conséquence, il sollicite alors le support de mobilité NEMO à faire une mise à jour de localisation, en quelque sorte un handover soft L3 (acquisition d'une adresse CoA, enregistrement au niveau du HA et établissement d'un nouveau tunnel MR-HA).

Pendant cette phase de traitement de l'événement Link_Going_Down, si la puissance reçue $\overline{P_{rx}}$ excède à nouveau le seuil $\alpha_{LGD}.P_{th}$ alors un événement MIH_Link_Event_Rollback est généré pour stopper les opérations du handover entamées.

Pour établir un nouveau tunnel entre le MR et le HA, le support d'extension MCoA [28] est utilisé. Nous avons modifié au niveau du HA la structure du cache « binding cache » (Tableau 5.3) afin d'assurer l'enregistrement de multiples CoA.

Tout tunnel établi entre le MR et le HA présente un des deux états : actif ou standby. Le HA ne peut avoir qu'un seul tunnel en état actif, les autres devront être à l'état standby. Le tunnel actif est le seul tunnel ouvert pour l'écoulement du trafic entre le MR et le HA et vice versa. Les tunnels en mode standby sont des tunnels fermés, en attente d'un ordre de commutation à l'état actif, déclenché par un message Tunnel_Switch_Request envoyé par le MR et validé par le HA.

HoA	BID	CoA	Etat du tunnel	Temps Expiration
HoA1	BID1	CoA1	active	-
HoA1	BID2	CoA2	standby	-

Tableau 5.3 – Binding Cache du Home Agent (support de MCoA)

Pour le maintient des chemins alternatifs disponibles pour le MR (liens ou tunnels), nous avons défini au niveau du HPD un cache appelé *AlternativePathCache* (Tableau 5.4).

Link ID	IF	Type du handover	CoA	Etat	Temps Expiration
Link #	IF2	Horizontal/Vertical	CoA2	ready	-

Tableau 5.4 – Cache au niveau du MR pour les chemins alternatifs disponibles

L'état « ready » indique que le chemin entre le MR et le HA à travers l'interface en question est déjà établi et est prêt à être utilisé pour le trafic. Le temps d'expiration est calculé en fonction de T_{LGD} (voir paragraphe V.6.5).

V.6.4 Traitement d'un un événement Link_Switch_Imminent

Lorsqu'un événement Link_Switch_Imminent est généré par exemple par IF-1, le HPD fait un scan du cache *AlternativePathCache* pour trouver un chemin alternatif prêt à utilisation. Donc tout va dépendre du type du handover, si c'est un type horizontal le HPD ordonne uniquement une commutation du lien (MIH_Switch), si c'est un type vertical le HPD doit demander un MIH_Switch et une commutation de tunnel (la requête est dirigée vers le support de gestion de la mobilité NEMO).

Afin de permettre au protocole NEMO de réaliser des commutations de tunnels, nous avons défini deux nouveaux messages de signalisation NEMO conformément à [2] :

- Le message Tunnel_Switch_Request dont le type d'entête de mobilité MH Type = 9, (Fig. 5.9) ; ce message envoyé par le MR au HA est une demande de commutation d'un tunnel donné de l'état standby à l'état actif avec fermeture du tunnel en court d'activité.
- Le message Tunnel_Switch_Replay dont le type d'entête de mobilité MH Type = 10 est la réponse par le HA au message Tunnel_Switch_Request (Fig. 5.10).

Payload Proto	Header Len	MH Type = 9	Reserved
Checksum		Sequence ID	Time
HoA			
BID1 of active tunnel		BID2 of target tunnel	
IPv6 care-of address (CoA) of active tunnel			
IPv6 care-of address (CoA) of target tunnel			
options			

Fig. 5.9- Format du paquet du message Tunnel_Switch_Request

Payload Proto	Header Len	MH Type = 10	Reserved
Checksum		Sequence ID	Time
Replay Code			

Fig. 5.10- Format du paquet du message Tunnel_Switch_Replay

V.6.5 Quelques Considérations

Pour les raisons d'optimisation du coût de connexion ou de la consommation d'énergie évoquées au début de ce chapitre, nous proposons le mécanisme suivant :

```
1 :  receive MIH_Link_Detected from IFj →
2 :     update AvailableLinkCache ;
3 :     compute α_LGD and α_LSI ;
4 :     send MIH_Configure_Link_Threshold to IFi (active interface);

5 :  receive MIH_Link_Going_Down from IFi →
6 :     start HPD_Timer ;
7 :     lookup in AvailableLinkCache for an available link;
8 :     select the most recent link (say IFj);
9 :     send MIH_Link_Connect to IFj;

10 :  receive MIH_Link_Up from IFj →
11 :    send HPD_L3_Soft_Handover_Initiate to NEMO Module

12 :  receive HPD_L3_Soft_Handover_Complete from NEMO Module →
13 :    update AlternativePathCache ;

14 :  receive MIH_Link_Switch_Imminent from IFi →
15 :    stop HPD_Timer ;
16 :    lookup in AlternativePathCache for an available tunnel;
17 :    select the most recent tunnel (say IFj tunnel);
18 :    send HPD_Tunnel_Switch_Req to NEMO Module ;

19 :  receive HPD_Tunnel_Switch_Rep from NEMO Module →
20 :    send MIH_Switch to MIHF ;

21 :  timeout (HPD_Timer) →
22 :    send MIH_Link_Connect to IFj;
23 :    remove IFj tunnel from AlternativePathCache;
24 :    return;
```

Fig. 5.11- Algorithme exécuté par le MR (module HPD)

A l'expiration d'un délai égal au double de T_{LGD} compté à partir de l'instant de déclenchement de l'évènement Link_Going_Down, si aucun évènement Link_Switch_Imminent n'est généré alors l'interface IF-2 est déconnecté, le chemin alternatif correspondant est effacé du cache *AlternativePathCache* et le tunnel correspondant est retiré du binding cache au niveau du HA. La figure 5.11 représente en notation Abstract Protocol Notation [83] l'algorithme exécuté par le MR (module HPD).

Dans tous les cas, si un évènement Link_Down est généré alors le HPD prend la décision de commuter vers un chemin alternatif disponible, sinon de procéder à un handover vers un lien alternatif disponible, sinon de faire un scan à la recherche d'un nouveau réseau d'accès.

V.7 Implémentation et Evaluation des performances

Dans cette section, nous présentons une implémentation sous NS2 du modèle de handover soft proposé ci-dessus et les résultats de simulation permettant de valider le modèle et évaluer ses performances.

V.7.1 Implémentation sous NS2

Pour valider le modèle proposé et évaluer ses performances, nous avons implémenté les mécanismes décrits précédemment sous NS2-29 [80] avec le package de mobilité de NIST [81]. Des modifications ont été apportées au code C++ des modules NEMO implémentés au niveau du HA et du MR pour supporter les mécanismes d'enregistrement MCoA et la commutation de tunnels. Un nouvel agent

C++ HPDAgent [78] est créé au niveau du MR supportant les mécanismes proposés pour la gestion du handover.

V.7.2 Simulations

Sur la base du code de l'implémentation décrite dans le paragraphe précédent, nous avons réalisé une série de simulations sous NS2 pour déterminer les valeurs appropriées des paramètres utilisés dans le modèle et conduire une évaluation des performances.

Le scenario illustré à la figure 5.12 a été utilisé à cette fin. La topologie du réseau est constituée de six nœuds utilisant l'adressage hiérarchique [79]:

- Le nœud 0 : Un routeur (0.0.0) présentant quatre interfaces filaires.
- Le nœud 1 : Un nœud correspondant CN (3.0.0).
- Le nœud 2 : Le Home Agent HA (4.0.0).
- Le nœud 3 : Une station de base IEEE 802.11 (routeur d'accès AR1 (1.0.0)) avec une couverture de 100 m.
- Le nœud 4 : Une station de base IEEE 802.16 (routeur d'accès AR2 (2.0.0)) avec une couverture de 1000 m.
- Le nœud 5 : Le routeur mobile (4.1.0) présentant deux interfaces externes (802.11 et 802.16) pour se connecter aux réseaux d'accès, et une interface interne (802.11) pour connecter un MNN, la portée est fixée à 20 m. Le MR se déplace à la vitesse v de la cellule de AR1 vers la cellule de AR2.
- Le nœud 6 : un MNN (4.1.1) suivant le même mouvement que le MR.

Les caractéristiques des liens notamment la bande passante et le délai sont reportés sur la figure 5.12.

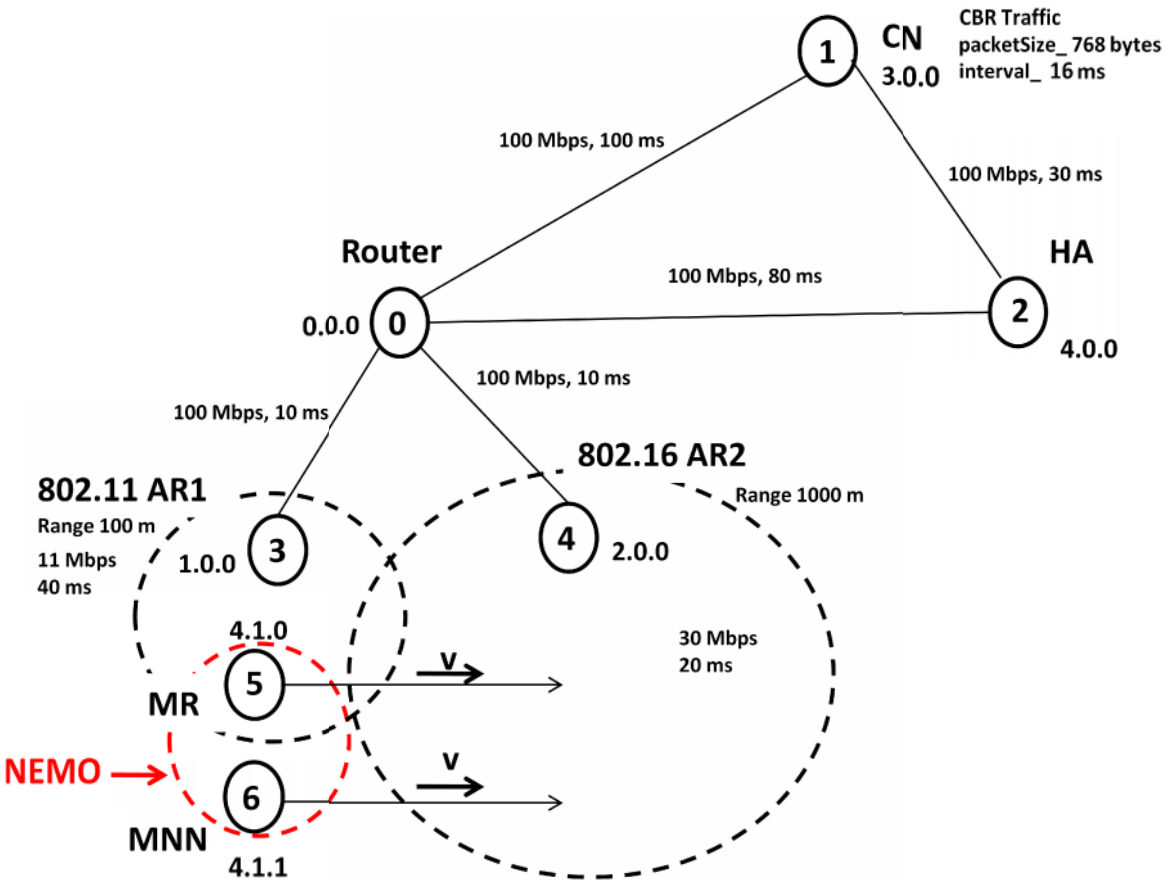

Fig. 5.12- Topologie du réseau NEMO (1, 1, 1) simulé

Le modèle du shadowing utilisé pour le lien radio 802.11 présente les paramètres suivants :

σ	4
β	3
Puissance transmise	14 dBm
P_{th}	-75 dBm

Un trafic streaming CBR est émis par le CN à destination d'un nœud MNN du réseau NEMO dont la mobilité est supportée par le MR (longueur des paquets = 768 octets, intervalle entre les paquets = 16 ms). Le temps de simulation est fixé à 60 s.

V.7.3 Résultats

Dans cette section, nous présentons les résultats de simulations permettant d'une part d'identifier les valeurs appropriées des paramètres du modèle conduisant à sa validation, et d'autres parts de mettre en évidence ses performances vis-à-vis d'autres approches (MIPv6-NEMO et FMIPv6-NEMO).

V.7.3.1 Détermination de la valeur appropriée de δ

Dans un premier temps, nous avons mené des simulations à la recherche des valeurs appropriées de δ pour la meilleure estimation de la puissance du signal reçu. En faite, δ dépend du paramètre du shadowing σ. La figure 5.13 montre les variations possibles du RSS (Received Signal Strength) pour différentes valeurs de δ et un modèle de shadowing avec $\sigma = 4$.

Sans l'application d'une moyenne, les oscillations des variations sont assez grandes alors qu'une valeur de δ= 0.1 semble être tout à fait acceptable pour stabiliser l'estimation. Il est important d'obtenir cette stabilité afin de réduire la probabilité de l'effet ping pong. Notons que le système devient moins réactif aux changements rapides lorsqu'une sur moyenne (δ= 0.01) est appliquée.

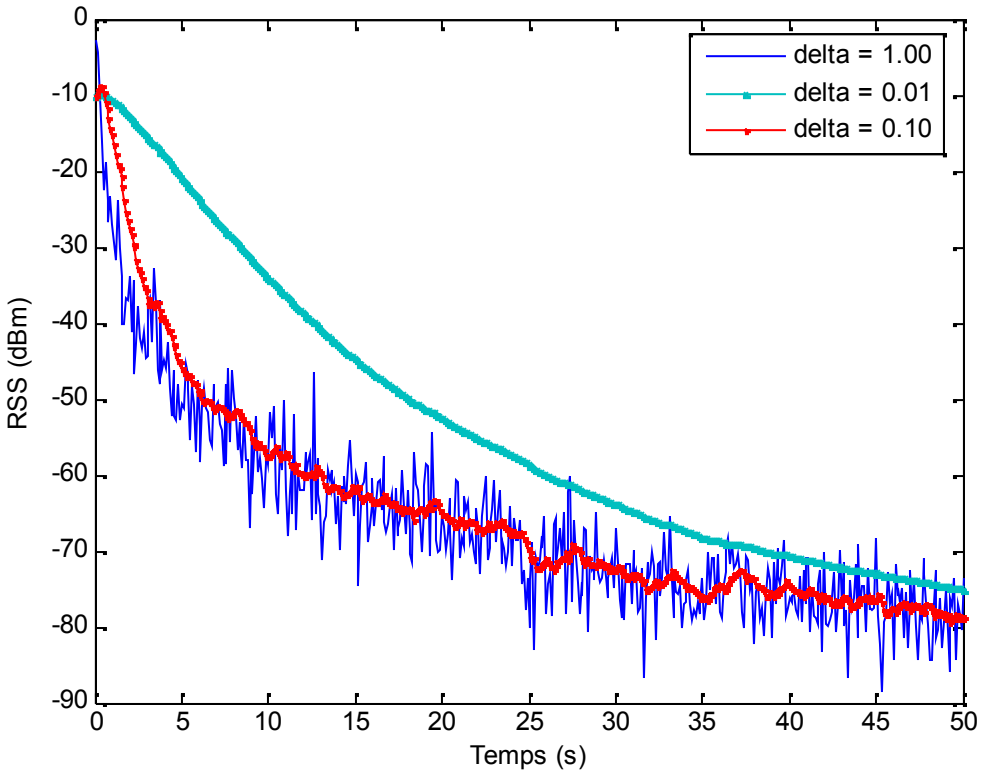

Fig. 5.13- Puissance RSS moyenne pour les valeurs de δ de 1, 0.01 et 0.10.
($\sigma = 4, \beta = 3, v = 90$ *Km/h*)

V.7.3.2 Niveaux de confidence pour l'évènement Link_Down

Le niveau de confidence spécifié dans la primitive MIH_Link_Going_Down donne une estimation sur la probabilité que lien fasse une rupture dans l'intervalle de temps spécifié. Plus ce niveau s'approche de l'unité plus la prédiction du handover est bonne.
Nous avons représenté sur les figures 5.14 et Fig. 5.15 le niveau de confidence respectivement pour les triggers LGD et LSI en fonction des coefficients α_{LGD} et α_{LSI} et la puissance reçue RSS.

Pour les deux cas LGD et LSI, et pour une puissance RSS donnée, le niveau de confidence croît d'une façon logarithmique avec les valeurs des coefficients α_{LGD} et α_{LSI}.

V.7.3.3 Impact de l'erreur d'estimation de β sur T_{LGD}

Le choix du paramètre β du modèle de propagation influe considérablement sur la précision des valeurs des coefficients α_{LGD} et α_{LSI} nécessaires respectivement pour la préparation et l'anticipation du handover. La valeur de β utilisée pour la détermination de ces coefficients doit donc se confondre avec la valeur du modèle de propagation réel. Dans cette partie des simulations, nous avons déterminé l'impact de l'erreur d'estimation sur β sur la détermination de la valeur du seuil du trigger LGD pour des modèles réels admettant comme paramètre $\beta = 2, 3$ et 4. Les résultats sont reportés sur la figure 5.16. Nous constatons qu'une erreur positive conduit à une augmentation pour le temps de préparation du handover, et donc à une diminution de la probabilité de prédiction. Cette augmentation est d'autant plus importante que le paramètre β du modèle réel est faible. En contre partie, une erreur négative conduit à une diminution pour le délai de préparation du handover, et donc un risque de ne pas terminer la préparation à temps pour anticiper le handover avant la rupture du lien (Link_Down).
A titre indicatif, sur la courbe correspondant à β = 3, pour une erreur par défaut sur β de 1% , on note une déviation du temps LGD d'environ 297 ms, soit une déviation relative d'environ 23%. C'est la raison pour laquelle nous avons recommandé des valeurs entre 0 à 20 de γ_1 et γ_2 dans les équations **(5.2) et (5.3)**.

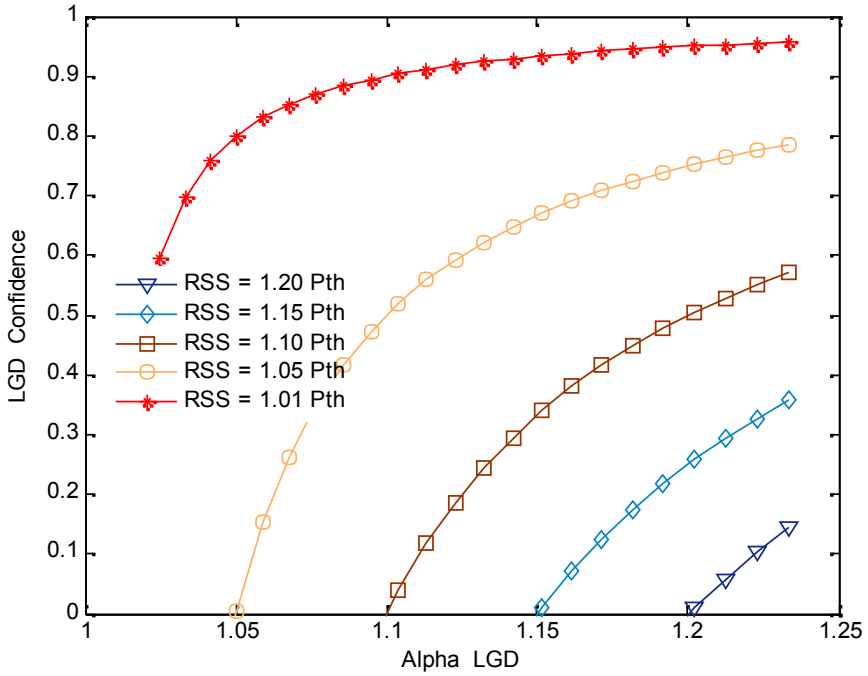

Fig. 5.14- Niveau de confidence pour l'évènement LD lorsque l'évènement LGD est déclenché

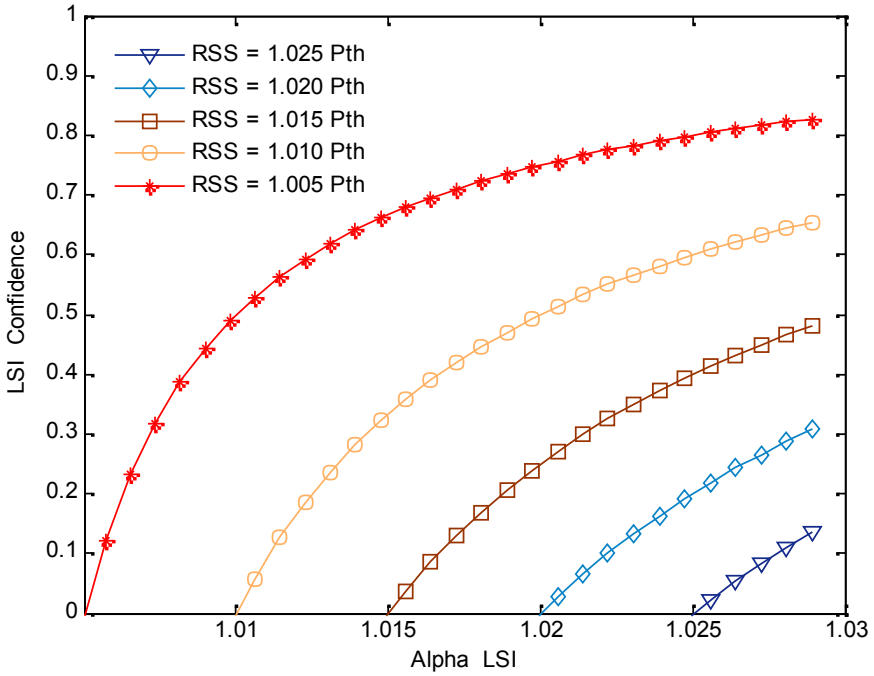

Fig. 5.15- Niveau de confidence pour l'évènement LD lorsque l'évènement LSI est déclenché

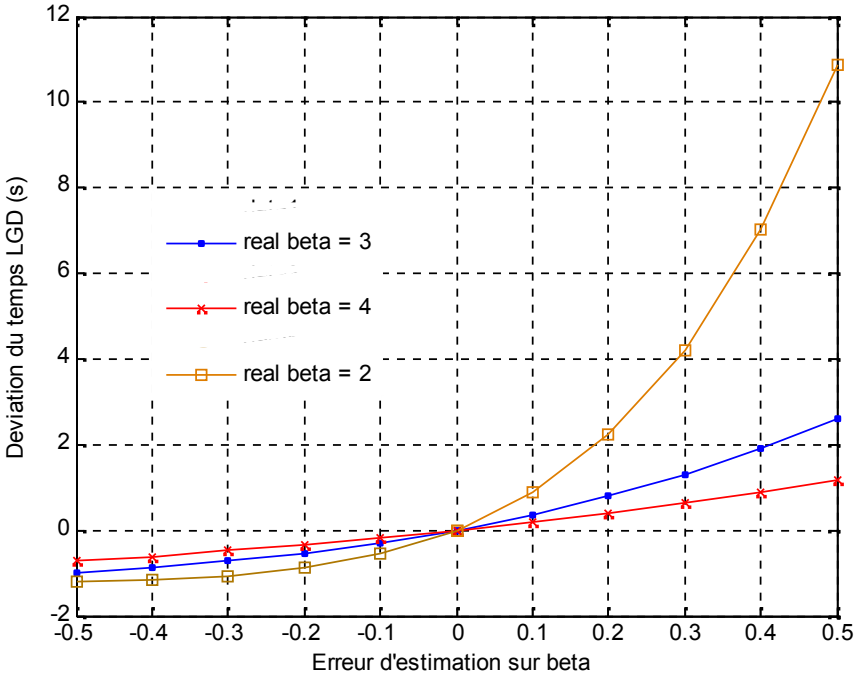

Fig. 5.16- Impact de l'erreur d'estimation de β sur le temps de préparation du handover

V.7.3.4 Validation du modèle

Nous présentons dans la figure 5.17 le débit instantané du trafic CBR reçu au niveau du MR pour le scénario décrit dans le paragraphe (V.7.2) avec une vitesse moyenne de déplacement du réseau NEMO de 90/Km. Le modèle du handover est utilisé sans erreur d'estimation sur β ($\Delta\beta$=0), avec un facteur de pondération δ= 0.1 pour l'estimation du RSS. Les paramètres de transmission et du modèle de propagation radio sont ceux du paragraphe (V.7.2).

Le résultat est comparé au protocole MIPv6-NEMO [15] dont le handover est déclenché par le trigger LD, et au protocole FMIPv6-NEMO [26] dont le handover anticipé est déclenché par le trigger LGD avec un coefficient α_{LGD} prédéfini (égal à 1.05).

L'événement Link_Down se produit à l'instant 38.512 s. Pour l'approche FMIPv6-NEMO, l'évènement Link_Going_Down (LGD) est déclenché à l'instant 37.893 s, soit uniquement 619 ms avant la rupture du lien. Ce qui ne permet pas d'assurer une connectivité sans couture même avec l'assistance du réseau, l'existence d'un délai et d'un taux de pertes résiduels demeure toujours possible.

Pour notre approche, l'évènement LGD est déclenché à 37.146, soit 1.366 s avant le Link_Down. Ce qui laisse le temps de préparer le handover en background. L'évènement LSI est déclenché à 38.396 s, soit 116 ms avant le Link_Down, laissant ainsi le temps de commuter le tunnel établi entre le MR et le HA.

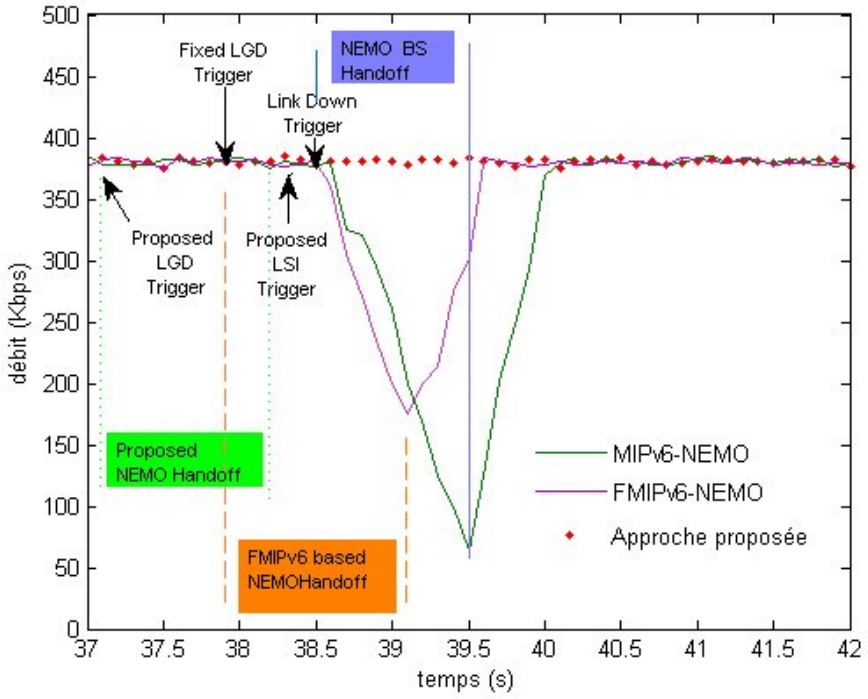

Fig. 5.17- Débit du trafic reçu mesuré au niveau du MNN

Alors que le protocole MIPv6-NEMO et son amélioration FMIPv6-NEMO affichent tous les deux des valeurs finies de délais de handover et de taux de pertes de paquets, notre approche fournit un support de mobilité permettant d'assurer une connectivité sans couture avec précisément un délai et un taux de perte nuls.

V.7.3.5 Performance de l'approche proposée

Dans ce paragraphe, nous abordons les performances de notre approche de handover sans couture. Nous utilisons pour cela les deux métriques suivantes : le délai du handover et le taux de perte des paquets pendant le handover.

Les figures 5.18 et 5.19 représentent respectivement ces deux métriques en fonction de la vitesse du réseau NEMO et l'erreur par défaut sur β. Nous constatons que la vitesse a peu d'impact sur les résultats, tandis qu'une augmentation sur l'erreur par défaut sur β fait augmenter le délai du handover et les pertes de paquets.

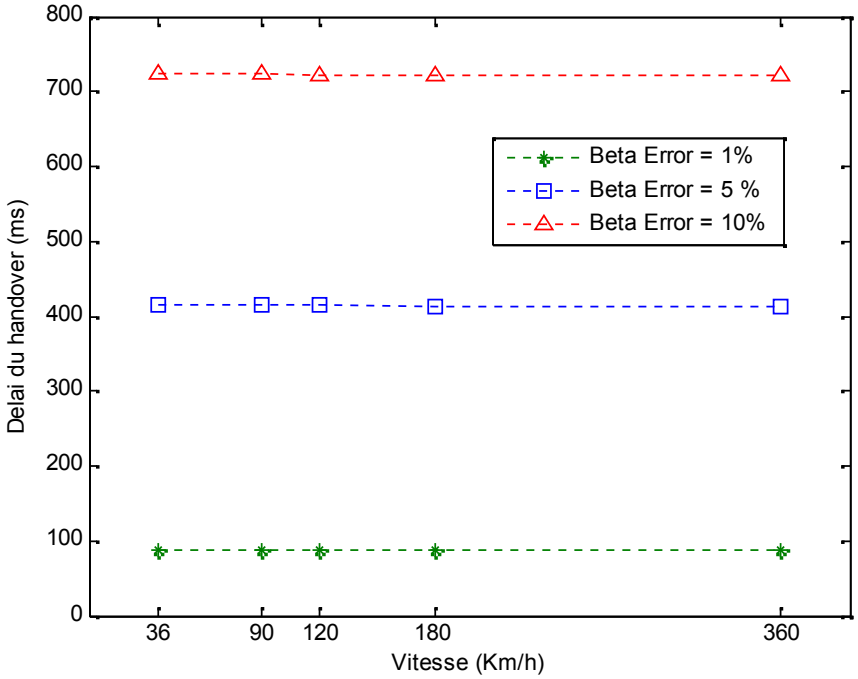

Fig. 5.18- Délai du handover en fonction de la vitesse et de l'erreur par défaut sur β

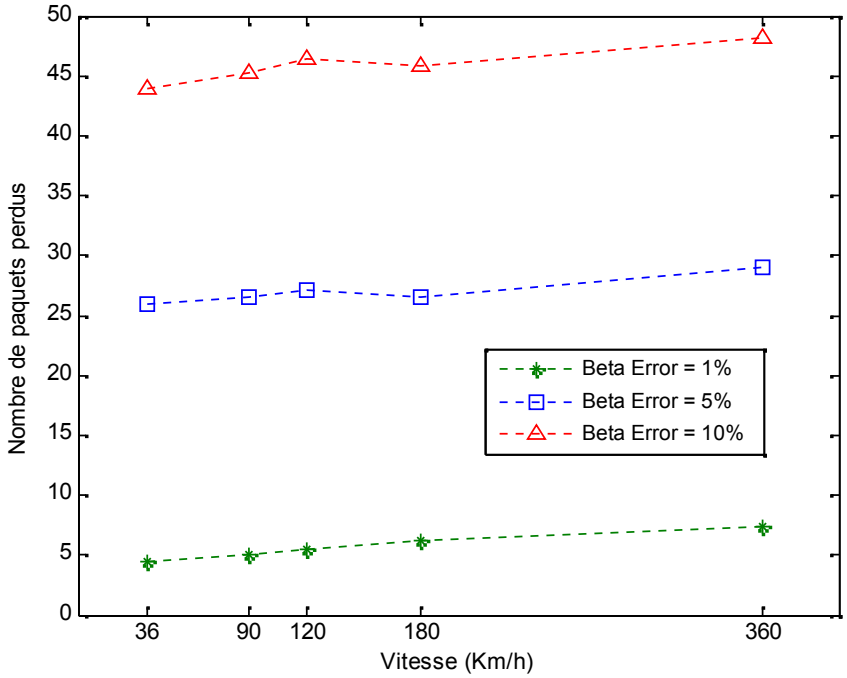

Fig. 5.19- Pertes des paquets durant le handover en fonction de la vitesse et de l'erreur par défaut sur β

V.8 Conclusion

Dans ce dernier chapitre de la thèse, nous avons examiné la combinaison de la fonctionnalité de multihoming et du handover soft intelligent pour aboutir à une solution de support de mobilité permettant de garantir dans le contexte de réseaux NEMO une connectivité sans couture (seamless handover) pour les applications temps réel et exigeantes en QoS. Nous avons adressé le cas du modèle NEMO multihomed (1,1,1) avec l'assistance des services locales MIH IEEE 802.21MIH. L'approche proposée est donc indépendante de l'infrastructure réseau, ne nécessitant par conséquent aucun changement dans l'architecture Internet. Le mécanisme de handover proposé doit être exécuté avant l'événement Link_Down du lien actuel suivant le principe Make-Before-Brake. A cette fin, nous avons utilisé des triggers dynamiques, LGD pour la préparation du handover calculé sur la base du temps nécessaire estimé du handover NEMO, et LSI pour l'anticipation du handover calculé sur la base du temps nécessaire estimé pour la commutation d'un tunnel entre le routeur mobile et son Home Agent. Les seuils de ces triggers sont configurés d'une façon dynamique et adaptative au changement des paramètres de l'environnement (modèle de propagation, vitesse de déplacement du réseau NEMO, nature et état des liens d'accès et le délai aller-retour entre le MR et le HA). Nos contributions dans cette partie de la thèse se résument dans les points suivants :

(i) la conception d'un nouveau composant MIH_User que nous avons nommé HPD (Handoff Policy Decision) pour l'accomplissement du handover soft intelligent utilisant les informations collectés des réseaux d'entourage et les états des liens et chemins disponibles.

(ii) La définition d'un nouveau service MIH (MIH_Link_Switch_imminent) pour le déclenchement de la commutation du tunnel MR-HA.

(iii) Proposition d'une méthode de génération et configuration dynamique des seuils des triggers utilisés.

(iv) Extension du protocole MIPv6-NEMO avec le support de commutation de tunnel utilisé conjointement avec l'enregistrement MCoA.

(v) Implémentation et simulation des mécanismes proposés sous NS2.

Les résultats des tests de simulation que nous avons conduit sous NS2 pour le mécanisme proposé sont comparés à ceux de la littérature pour le cas MIPv6-NEMO [15] et FMIPv6-NEMO [26] et montrent une amélioration significative des performances du handover en terme de délai et de pertes de paquets. Les tests ont permis par ailleurs d'identifier les valeurs appropriées des paramètres utilisés dans notre modèle permettant ainsi de valider l'approche proposée [85].

Conclusion générale

La gestion de la mobilité d'un réseau mobile entier embarquant plusieurs équipements capables de communiquer avec l'Internet a suscité un grand intérêt pour les chercheurs et les industriels qui désirent déployer de tels réseaux dans les systèmes de transport publics par exemple.
Le problème peut être résolu en utilisant MIPv6 par exemple ou l'une de ses améliorations, ceci exigerait d'une part que chaque dispositif soit capable du protocole MIPv6, et d'autre part que chaque dispositif embarqué exécute les fonctionnalités du protocole MIPv6 conduisant ainsi à une surcharge de trafic. Une autre solution basée sur l'extension de MIPv6 a été proposé récemment par le groupe de travail NEMO WG de l'IETF sous le nom de NEMO Basic Support Protocol. Cette solution basique ne prend pas en charge malheureusement toutes les fonctionnalités de mobilité et plusieurs issues tels que l'optimisation de routage (RO), le multihoming, les performances du handover et la sécurité ont été soulevés par l'IETF.

L'optimisation du handover, tant en termes de protocoles que d'algorithmes décisionnels, reste toujours un sujet d'actualité. Dans la spécification de base du protocole NEMO, le routeur mobile ne peut utiliser qu'une seule adresse IPv6 pour s'attacher aux réseaux d'accès. Le problème se résume au fait qu'au cours d'un changement de réseau, le routeur mobile doit exécuter un handover hard de sorte qu'une coupure de service est inévitable. Ce genre de problème n'est pas du tout acceptable dans le cas d'un trafic temps-réel sensible au délai. La totalité des travaux de recherche visant à améliorer les performances du handover NEMO BS, est restée inefficace pour répondre aux besoins des applications à contraintes temporelles.

Dans cette thèse, nous avons adressé cette problématique conjointement avec celle du multihoming visant à réduire au minimum le délai du handover et éliminer également les pertes de paquets pendant l'opération du handover. Nous avons apporté deux solutions simples, immédiates et à moindre coût pour la gestion de la mobilité dans le contexte d'un réseau NEMO multi-domicilié (multihomed).

Nos solutions sont indépendantes de l'infrastructure, ne nécessitant ainsi aucun changement dans l'architecture de base du protocole NEMO BS.
Etant donné, l'importance cruciale des algorithmes de décision et d'exécution du Handover, qui restent spécifiques à chaque configuration de NEMO multihomed, nous avons proposé pour les cas que nous avons traités des mécanismes adaptés permettant d'assurer des handovers sans coutures (zéro délai et zéro perte de paquets).

Notre première contribution est réalisée autour du modèle NEMO multihomed (n,n,1) dans lequel plusieurs MRs domiciliés dans différents HAs sont déployés, et qu'un seul préfixe est délégué. Notre idée pour réaliser un handover sans couture, consiste à établir et maintenir au préalable des tunnels de substitution entre les MRs et le HA déléguant le préfixe. Le trafic de données est basculé sur un tunnel substituant avant la rupture du tunnel courant.
Nous avons introduit une passerelle MNPx au sein du réseau NEMO, dont les principaux rôles sont l'interconnexion des MNNs et les différents MRs, et la gestion intelligente du handover et du trafic. Pour ce faire, nous nous sommes appuyés sur les services MIES spécifiés par le standard IEEE 802.21 pour la génération des triggers L2, et le module MTM (Mobility and Traffic Management) que nous avons développé nous même pour, dans un premier temps, la prise de décision et l'exécution du handover. De plus, nous avons fait l'extension du protocole NEMO BS avec les deux supports : d'enregistrement multiple des CoAs des routeurs substituants et de commutation de tunnel. Des procédures pour ces mécanismes, impliquant de nouveaux messages ont été élaborées en conséquence.

Dans notre seconde contribution, nous nous sommes focalisés sur le modèle NEMO multihomed (1,1,1) où un seul MR multi-interfaces est déployé et un seul préfixe est délégué. Dans cette configuration, l'enregistrement de multiples CoAs au près du HA n'est plus vraiment une issue à partir du moment que la RFC 5648 a été publiée. L'objectif de cette partie était la réalisation d'un handover sans couture avec la contrainte d'économie d'énergie et éventuellement de coût. Dans cette approche, nous avons fait également appel aux services MIH. Nous avons adopté une approche proactive consistant à une préparation du handover (attachement aux réseaux d'accès disponibles, enregistrement de la nouvelle CoA au niveau du Home Agent, établissement d'un tunnel entre le MR et le HA), et puis à une anticipation du handover (commutation de tunnel) suite à une prédiction de l'évènement Link_Down. Deux triggers L2 ont été utilisés pour la préparation et l'anticipation du handover respectivement Link_Going_Down et Link_Switch_Imminent.
Afin de minimiser le temps d'activation simultanée de plusieurs interfaces de communication sans fils, nous avons opté pour une configuration dynamique et adaptative des seuils de ces triggers en fonction des paramètres de l'environnement (caractéristiques des liens d'accès, localisation du réseau mobile dans la topologie internet, vitesse du réseau mobile, modèle de propagation, …). Avec cette manière de procéder, nous avons pu assurer une grande probabilité de prédiction du handover évitant ainsi les scénarios de ping-pong.

Les résultats obtenus sont excellents et permettent d'envisager des expériences pratiques.
Toutefois, dans ce mémoire nous n'avons pas adressé le problème de la gestion du trafic dans les configurations multihoming proposées, le prolongement immédiat de ce travail serait la définition d'une politique de routage, de partage de charge ou même d'agrégation de bande passante dans le cas où plusieurs tunnels sont ouverts simultanément.
Une autre perspective comme continuité à ce travail serait le développement d'algorithmes décisionnels de handover reposant sur les qualités des liens d'accès, les capacités des réseaux d'accès et les préférences des utilisateurs. A ce sujet on pourra introduire de nouveaux métriques pour la décision du handover telles que le BER, la bande passante, le RTT, la couverture du réseau, le coût, la sécurité, etc.
Dans notre seconde approche, nous avons considéré un seul modèle de propagation, comme perspective il serait intéressant d'étudier l'impact d'autres modèles de propagation tels que Longley-Rice, Durkin's, Okumura et Hata, appliqués aux différentes technologies d'accès IEEE 802.11, IEEE 802.16, 3GPP et 3GPP2, et de développer des techniques d'estimation n'impliquant pas des paramètres fortement dynamiques telle que la vitesse du réseau NEMO.

Enfin, rappelons que les issues d'optimisation de routage et de sécurité demeurent toujours des issues ouvertes pour le cas des réseaux NEMO multi-domiciliés.

Bibliographie

[1] C. Perkins, “ IP Mobility Support,” RFC 2002, October 1996.

[2] M. Stemm .”Vertical Handoffs inWireless Overlay Networks”. ACM Journal of Mobile Networks and Applications (MONET), Vol. 3, No. 4, pages 335-350. 1998.

[3] N. Montavont and T. Noel. Handover Management for Mobile Nodes in IPv6 Networks. IEEE Communications Magazine, August 2002.

[4] P. Vidales, L. Patanapongpibul and R. Chakravorty .Ubiquitous Networking in Heterogeous Environments.. In Proceedings of the 8th IEEE Mobile Multimedia Communications (IEEE MoMuC'2003), October 2003.

[5] Internet Protocol, IETF RFC 791, September 1981.

[6] Transmission Control Protocol, IETF RFC 793, September 1981.

[7] J. Postel. Internet control Message Protocol, IETF RFC 792, September 1981.

[8] S. Deering and R. Hinden, “Internet Protocol, Version 6 (IPv6) Specification”, IETF RFC 2460, December 1998.

[9] C. Perkins, “IP Mobility Support for IPv4”, RFC 3344, IETF, 2002.

[10] D. Johnson, C. Perkins & J. Arkko, “Mobility Support in IPv6”, RFC 3775, IETF, 2004.

[11] R. Koodli, "Mobile IPv6 Fast Handovers", IETF RFC 5568, July 2009.

[12] H. Soliman, C. Castelluccia, K. El Malki and L. Bellier, “Hierarchical Mobile IPv6 (HMIPv6) Mobility Management”, RFC 5380, IETF, October 2008.

[13] Y-G.Hong, M-K.Shin and H-J.Kim, “ Fast Handover for Mobile IPv6 using Access Router Based Movement Detection and CoA Configuration,” 2004.

[14] S. Gundavelli, K. Lung, V. Devarapalli, K. Chowdhury and B. Patil, “Proxy Mobile IPv6”, IETF RFC 5213, August 2008.

[15] V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol," IETF, RFC 3963, January 2005.

[16] R. Moskowitz and P. Nikander, “Host Identity Protocol (HIP) Architecture”, IETF, RFC 4423, May 2006.

[17] A.C. Snoeren and H. Balakrishnan, "An End-to-End approach to Host Mobility," 6th ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom'00), Boston, MA, pp. 155 - 166, August 2000.

[18] R. Stewart, Q. Xie, M. Tuexen, S. Maruyama and M. Kozuka, "Stream Control Transmission Protocol (SCTP) Dynamic Address Reconfiguration", IETF RFC 5061, September 2007.

[19] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley and E. Schooler "SIP: Session Initiation Protocol", IETF RFC 3261, June 2002.

[20] P. K. Chowdhury, M. Atiquzzaman, and W. Ivancic. SINEMO: An IP-diversity based approach for network mobility in space, Second International Conference on Space Mission Challenges for Information Technology (NASA SMC-IT), Pasadena, CA, pp 109-115, 2006.

[21] C-W Lee, Y-S. Sun and M-C Chen, HiMIP-NEMO: Combining Cross-layer Network Management and Resource Allocation for Fast QoS-Handovers. Proceedings of the 67th IEEE Vehicular Technology Conference, Singapore, 2008.

[22] T. Ernst, Le support des réseaux mobiles dans IPv6, RSTI - TSI. Volume 25 – no 5, pages 573 à 597, 2006.

[23] S. Kent, K. Seo, "Security Architecture for the Internet Protocol", IETF RFC 4301, 2005.

[24] W. Simpson, "IP in IP Tunneling", IETF RFC 1853, October 1995.

[25] C. Vogt and J. Arkko, "A Taxonomy and Analysis of Enhancements to Mobile IPv6 Route Optimization", IETF RFC 4651, February 2007.

[26] 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.

[27] E. Perera, V. Sivaraman, A. Seneviratne, "Survey on Network Mobility Support", Mobile Computing and Communications Review, Volume 8, Number 2, 2004.

[28] C. Ng, E. Paik, T. Ernst, M. Bagnulo, "Analysis of Multihoming in Network Mobility Support," IETF, RFC 4980, October 2007.

[29] S. Jung, F. Zhao, S. Felix Wu, H. Kim, "Threat analysis on network mobility (NEMO)", Information and Communications Security, 6th International Conference, pp. 331-342, 2004.

[30] Lei Zhao, Xiaoping Li, Qingkuan Dong, Lei Shi," An IKEv2 Based Security Authentication Scheme for Mobile Network", Advances in information Sciences and Service Sciences(AISS) ,Vol.3, No.9, pp. 191-198, October 2011.

[31] H. Petander, E. Perera, K.C. Lan, A. Seneviratne. "Measuring and improving the performance of network mobility management in ipv6 networks". IEEE Journal on Selected Areas in Communications, 24(9), pp 1671-1681. 2006.

[32] Shayla Islam and al., “Mobility Management Schemes in NEMO to Achieve Seamless Handoff: A Qualitative and Quantitative Analysis”. Australian Journal of Basic and Applied Sciences, 5(6) pp 390-402. 2011.

[33] N. Montavont and T. Noël,” Handover Management for Mobile Nodes in IPv6 Networks”, IEEE Communications Magazine • August 2002.

[34] K. ZHU, D. NIYATO, P. WANG, E. HOSSAIN, D. I. KIM, “Mobility and Handoff Management in Vehicular Networks: A Survey”, WIRELESS COMMUNICATIONS AND MOBILE COMPUTING, Wiley InterScience 2009.

[35] Pack SH, Shen XS, Mark JW, Pan JP. A comparative study of mobility management schemes for mobile hotspots. Proceedings of IEEE WCNC, 2007; 3850–3854.2007.

[36] G. Daley, B. Pentland, R. Nelson, “Movement Detection Optimization in Mobile IPv6,” *ICON2003*. pp.687-692. 2003.

[37] J. Kempf, M. Khalid, and B. Pentland, “IPv6 fast router advertisement,”draft-mkhalil-ipv6-fastra-05.txt, July 2004.

[38] N. Moore, “Optimistic Duplicate Address Detection for IPv6,” IETF RFC 4429, April 2006.

[39] H. Lin, H. Labiod. Hybrid handover optimization for multiple mobile routers-based multihomed NEMO networks, in: Proceedings of IEEE International Conference on Pervasive Service, Istanbul. 2007.

[40] Z. Huang, Y. Yang, H. Hu and K. Lin. A fast handover scheme based on multiple mobile router cooperation for a train-based mobile network Int. J. Modelling, Identification and Control, Vol. 10, No. 3/4, pp 202-212. 2010.

[41] G. Jeney, L. Bokor and Z. Mihaly. GPS aided predictive handover management for multihomed NEMO configurations. 9th International Conference on Intelligent Transport Systems Telecommunications, pp 69-73. 2009.

[42] H. Petander, E. Perera, K.C. Lan, A. Seneviratne, “Measuring and Improving the Performance of Network Mobility Management in IPv6 Network,” IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 24, NO.9, pp.1671-1681, September 2006.

[43] IEEE 802.11 WG, “IEEE Standard for Local and metropolitan area networks. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications”. IEEE Std. 802.11-1999.

[44] IEEE 802.16 WG, “IEEE Standard for Local and Metropolitan Area Networks. Part 16: Air Interface for Fixed Broadband Wireless Access Systems,” IEEE Std. 802.16-2004, October 2004.

[45] 3rd Generation Partnership Project (3GPP). http://www.3gpp.org/specifications.

[46] 3rd Generation Partnership Project 2 (3GPP2). http://www.3gpp2.org/public_html/specs/index.cfm

[47] R. Wakikawa, V. Devarapalli, G. Tsirsis and T. Ernst and K. Nagami, (2009), "Multiple Care-of Addresses Registration," IETF, RFC 5648.

[48] Ferguson P., Senie D., “Network ingress Filtering: Defeating Denial of Service Attacks which Employ IP Source Address Spoofing”, RFC 2267, IETF, January 1998.

[49] E. K. Paik, H. S. Cho, T. Ernst and Y. H. Choi, "Load sharing and session preservation with multiple mobile routers for large scale network mobility," The proceedings of AINA 2004: Page(s):393 - 398 Vol.1.2004.

[50] F. Guo, J. Chen, W. Li, and T. Chiueh, ”Experiences in Building A Multihoming Load Balancing System,” Proc. of IEEE INFOCOM 2004, Mar 2004.

[51] S. H. Cho, J. K. Na and C. K. Kim, "A dynamic load sharing mechanism in multihomed mobile networks," ICC 2005 16-20 May 2005 Page(s):1459 - 1463 Vol. 3. 2005.

[52] R. Kuntz and J. Lorchat. Building Fault Tolerant Networks using a multihomed Mobile Router: a Case Study. In Asian Internet Engineering Conference (AINTEC) 2006, Bangkok,Thailand, November 2006.

[53] K. Mitsuya, K. Tasaka, and R. Wakikawa. A Policy Data Set for Flow Distribution. Internet Draft draft-mitsuya-monami6- flow-distribution-policy-02.txt, October 2006.

[54] C. Park, N. Choi, E. Paik, T. Kwon and Y. Choi, “Multiple Interface/Prefix Selection for Virtual Mobile Networks”, ICACT, February 2008.

[55] IETF, Internet Draft, Feb. 2004.Q. Wang, R. Atkinson, and J.Dunlop, “Towards Always Best Connected Multi-Access: the MULTINET Approach”, IWCMC '08. August 2008.

[56] N. Montavont, T. Ernst, and T. Noel, “Multihoming in Nested Mobile Networks”, In International Symposium on Applications and the Internet (SAINT)-IPv6: Technology and Deployment Workshop”, Tokyo, Page(s):184 – 189. January 2004.

[57] P. Rawat, J-M Bonnin, and L. Toutain. An end-2-end tunnel header compression solution for nested mobile networks. In ICLAN’07 (International Conference on the Latest Advances in Networks), Paris, France, December 2007.

[58] M. Sabeur, B. Jouaber and D. Zeghlache "Low Latency Handoff for Nested Mobile Networks" CCNC 2006.

[59] Theodore S. Rappaport. Wireless Communication: Principles and Practice. Personal Education International. 2nd edition, 2002

[60] S. Woon, N. Golmie, A. Sekercioglu. Effective Link Triggers to Improve Handover Performance. Proceedings of 17th Annual IEEE Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC'06), Helsinki, Finland, pp 11-14. 2006.

[61] S. J. Yoo, D. Cypher, and N. Golmie, , “LMS predictive link triggering for seamless handovers in heterogeneous wireless networks,” in Proc. MILCOM, Orlando, FL, Oct. 28–30, pp 1-7. 2007.

[62] Maurice Bellanger. Traitement numérique du signal. 6e édition, Dunod, Paris, 1998.

[63] Neal seitz, ITU-T QoS Standards for IP-based Networks. Standards Report, IEEE Communications magazine, June 2003.

[64] Y. Young An, B. Ho Yae, K. Won Lee, Y. Ze Cho, and W. Young Jung, "Reduction of Handover Latency Using MIH Services in MIPv6", Proceedings of the 20th International Conference on Advanced Information Networking and Applications (AINA'06), 2006.

[65] V. Vassiliou and Z. Zinonos, "Analysis of the Handover Latency Components in Mobile IPv6", JOURNAL OF INTERNET ENGINEERING, VOL. 3, NO. 1, DECEMBER 2009.

[66] Details for North Americ Internet Traffic Report. 2012 http://www.internettrafficreport.com/namerica.htm

[67] Guochang Xu. GPS: Theory, Algorithms and Applications. Springer 2007-09-14 , ISBN: 3540727140, 2007.

[68] IEEE 802.21-2008, Media Independent Handover Services. 2008.

[69] E. Nordmark, W. Simpson and H. Soliman. "Neighbor Discovery for IP version 6 (IPv6)", IETF, RFC 4861, September 2007.

[70] A. Petrescu, A. Olivereau, C. Jeanneteau, H.-Y. Lech, "Threats for basic network mobility support (NEMO threats)", IETF Internet Draft: draft-petrescu-nemo-threats-01.txt, 2004

[71] L. Tian-fu, C. Chichao, H. Tzonelih, "Private authentication techniques for the global mobility network", Wireless Personal communications, Vol.35, No.4, pp.329-336, 2005.

[72] H. Fathi, S. Shin, K. Kobara, Shyam S. Chakraborty, H. Imai, R. Prasad, "LR-AKE-Based AAA for network mobility (NEMO) over wireless links", IEEE Journal on Selected Areas in Communications, Vol. 24, No.9, pp.1725-1736, 2006.

[73] Y. Qiu, F. Bao, Y. Wu, Y. Yang, "A lightweight fast handover authentication scheme in mobile networks", IEEE International Conference on Communications, pp.122-127, 2009.

[74] C. Wan, A. Hu, J. Zhang, "Managing Handover Authentication in Big-domain Wireless Environment", Journal of JCIT, Vol. 4, No. 3, pp.86-93, 2009.

[75] J-D Koo, S-H Oh, D-C Lee, "Authenticated route optimization scheme for network mobility (NEMO) support in heterogeneous networks", International Journal of Communication Systems, Vol. 23, No. 9, pp. 1252–1267, 2010.

[76] J. Choi, S. Jung. "A handover authentication using credentials based on chameleon hashing", IEEE Communications Letters, Vol.14, No. 1, pp.54-56, 2010.

[77] L. Tian-Fu, H. Tzonelih, "Provably secure and efficient authentication techniques for the global mobility network", Journal of Systems and Software, Vol. 84, No.10, pp.1717-1725, 2011.

[78] F. J. Ros, P. M. Ruiz. Implementing a New Manet Unicast Routing Protocol in NS2. Dept. of Information and Communications Engineering University of Murcia, December, 2004.

[79] The VINT Project. The ns Manual. http://www.isi.edu/nsnam/ns/ns-documentation.html.

[80] NS-2 Network Simulator, http://www.isi.edu/nsnam/ns

[81] The Network Simulator NS-2 NIST add-on—IEEE 802.21 model (based on IEEE P802.21/D03.00), National Institute of Standards and Technology (NIST), January 2007.

[82] C. Kaufman, Ed., “Internet Key Exchange (IKEv2) Protocol”, IETF RFC 4306, 2005.

[83] M. G. Gouda, “Elements of Network Protocol Design,” John Wiley and Sons, 1998.

[84] Z. Slimane, M. Feham and A. Abdelmalek. A Seamless and Transparent MN-Proxy based Mobility Support For (n,n,1) Multihomed NEMO Model. International Journal of Computer Science and Network Security, Vol.10, No.4, PP.306–313, April 2010.

[85] Z. Slimane, M. Feham and A. Abdelmalek. Seamless Infrastructure independent MultiHomed NEMO Handoff Using Effective and Timely IEEE 802.21 MIH triggers. Accepté pour publication dans “International Journal of Wireless and Mobile Networks (IJWMN)”, Vol.4, No.3, 2012.

Publications

1. Z. Slimane, M. Feham and A. Abdelmalek. A Seamless and Transparent MN-Proxy based Mobility Support For (n,n,1) Multihomed NEMO Model. International Journal of Computer Science and Network Security, Vol.10, No.4, PP.306–313, April 2010.

2. Z. Slimane, M. Feham and A. Abdelmalek. Seamless Infrastructure independent MultiHomed NEMO Handoff Using Effective and Timely IEEE 802.21 MIH triggers. To appear in International Journal of Wireless and Mobile Networks (IJWMN)", Vol.4, No.3, 2012.

A Seamless and Transparent MN-Proxy based Mobility Support For (n,n,1) Multihomed NEMO Model

Zohra Slimane [1], Mohamed Feham [1] and Abdelhafid Abdelmalek [1,2]

(1) STIC Laboratory, University of Tlemcen, Algeria
(2) LAMIH Laboratory, University of Valenciennes and Hainaut Cambrésis, France

Summary
Multihomed Network Mobility is a research field being widely explored because of its importance in military and vehicular applications. Multihoming is a promising solution for providing ubiquitous Internet and some other benefits such as Load-Sharing and Policy-based Routing. Unfortunately, extensions of NEMO Basic Support proposed for the purpose of managing multihomed NEMO are still sub-optimal and too immature for standardization. Indeed, the proposed solutions are partial and don't benefit from all advantages offered by multihoming. Further design, implementation and evaluation are still needed to obtain powerful, secure and flexible solutions. In this paper, we propose a new solution for both mobility and traffic management in the context of (n,n,1) multihomed NEMO networks. The proposed approach relies on beforehand Mobile Routers registration and unidirectional tunnels establishment. A Router-Proxy is also introduced inside the Mobile Network as a central entity to mange mobility and traffic. NS2-Mobiwan simulation results show excellent performance improvement in terms of handoff delay and packet loss rate, proving a really transparency and seamless Internet connectivity.

Key words:
Network mobility, NEMO, Multihoming, Mobile Router, Handover.

1. Introduction

Network mobility management constitutes today a true challenge for the Internet fourth-generation. With the proliferation of wireless devices and mobile network services, one posts an increasing desire on behalf of the users to be profited from ubiquitous Internet access, i-e without discontinuity anywhere at any time during their displacements, so that we have whole networks made up of mobile devices moving together and wishing this quality of service. Public transportation systems (train, tram, subway, buses …) are typical environments.

Network mobility cannot be enough served by MIPv6 [1] (including improved versions, Hierarchical Mobile IPv6 (HMIPv6) [2], Fast Handover for MIPv6 (FMIPv6) [3] and Proxy based Mobile IPv6 (PMIPv6) [4]), because MIPv6 manages only host mobility and has some limitations of supporting Network Mobility. The main problem is that it could only possible to forward packets addressed to a mobile router, but not those nodes behind the mobile router in the mobile network. The deployment scenario of MIPv6 by hosts individually requires also, on one hand that each device support MIPv6, and on the other hand, that each device carries out when handover is involved the functionalities of the protocol MIPv6 leading thus to an increased signaling traffic overhead.

These issues were actively investigated in NEMO (Network Mobility) WG in IETF which has extended MIPv6 protocol to support a collective mobility of an entire single-homed mobile network by introducing mobile router and prefix binding update option. The NEMO Basic Support protocol specified by the NEMO WG [5] is designed so that network mobility is transparent to the nodes inside the mobile network. The mobile network is viewed and managed as a single unit, which changes its point of attachment to the Internet through the mobile router. However, the most interesting NEMO scenario that will practically provide ubiquitous internet is the multihoming. A mobile network is considered as multihomed when either it is simultaneously connected to the Internet via multiple mobile routers, or via only one mobile router which has more than one egress interface. Different interfaces may indeed be active simultaneously; a mobile network must be able to deal with both horizontal and vertical handover. A taxonomy for classifying the potential multihomed configurations and the associated issues is described in [6] and [7] in the context of NEMO-IPv6. Multihoming yields some benefits like Fault-Tolerance/Redundancy, Load Sharing and Policy-based Routing. NEMO Basic Support protocol unfortunately does not specify any particular mechanism to manage multihoming and must be improved to deal with multihomed networks, as it suffers from some problems such as ingress filtering mechanisms, session interruptions during handover, registration procedure latency, multiple Care-of-Addresses registration and Home Agents

Manuscript received April 5, 2010
Manuscript revised April 20, 2010

synchronization. Recently, much work dealing with multihoming has been made to solve these issues, and several seamless mobility approaches have been proposed but they still remain sub-optimal because of their relatively longer handoff delays and higher packet-loss rates.

The multihoming analysis draft [7] classifies multihomed mobile networks using (x, y, z) notation. Variables x, y, and z respectively mean the number of Mobile Routers intended to connect the mobile network to Internet, the number of Home Agents, and the number of Mobile Network Prefix. In this paper, we propose a new solution for mobility and traffic management in the context of multihomed NEMO networks. Our special interesting is concentrated on the (n,n,1) multihomed NEMO configuration. We introduce a new entity called Mobile Network Proxy (MNPx) at the Mobile Network level to manage Handoffs and traffic distribution between the multiple Network Routers ensuring transparently to nodes inside the Mobile Network.

The remainder of this article is organized as follows. In Section 2, we provide essential background about network mobility and multihoming. In section 3 we re-examine multihoming capabilities and issues for the (n,n,1) NEMO configuration. Section 4 presents our Mobile Network Proxy based multihoming solution and describes its behavior in a common scenario. We show performance evaluation in section 5. Finally, section 6 concludes the paper.

2. Related Work

NEMO Basic Support protocol is an extension of MIPv6 to support mobility for a whole Mobile Network (MN) that changes its point of attachment to internet, in such a way that session continuity is maintained transparently for every Mobile Network Node (MNN) within the MN. The MN is attached to the Home Network/Visited Network via Mobile Router (MR) to which an IPv6 Mobile Network Prefix (MNP) is delegated to advertise to MMNs inside the MN.

The MR has at least two interfaces: ingress (IIF) and egress (EIF). The IIF is configured with an IP from MNP whereas the EIF will be configured with the Home Address (HoA) when the MR is attached to the Home Network. This HoA is the permanent address of the MR used as an identifier. When the MN moves away from the Home Network and the MR attaches to a new Access Router (AR) belonging to the Visited Network, the MR acquires a temporal address called Care-of-Address (CoA) used as a locator with which it configures its EIF (Fig. 1).

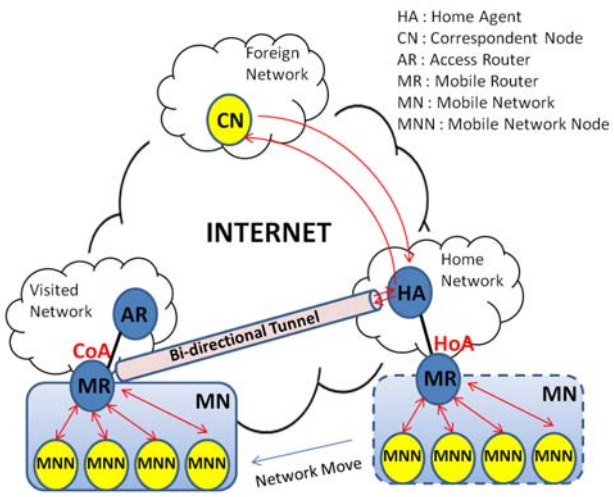

Fig. 1. NEMO Support Mobility

The NEMO protocol relies on a pair of Binding Update (BU) and Binding Acknowledgement (BA) messages exchanged between MR and its Home Agent (HA) to establish a bidirectional tunnel between them. All IPv6 traffic to and from MR is sent through this tunnel using IP-in-IP encapsulation.

When a MR attaches to a new AR and acquires a CoA, it sends a router BU (Mobile Router Flag (R) set) including MNP information to its HA. When the HA receives this Binding Update, it creates a cache entry binding the Mobile Router's HoA to its CoA. Then, if a successful BA is received the MR initiate the establishment of a bidirectional tunnel MR-HA. All packets exchanged between a MNN and a Correspondent Node (CN) in the Foreign Network pass through this tunnel.

The NEMO mechanism described above concerns only the simple case (1,1,1) i.e single MR, single HA and single MNP. Although its advantages compared to MIPv6, NEMO Basic Support still present weaknesses when dealing with multihomed networks. Some of the proposed methods to solve these problems are available in literature, but still there is considerable requirement of effort to build a powerful, secure and flexible solution.

Paik et al. [9] addressed many issues in multihomed NEMO and analyzed the influence of mobility on load sharing and session preservation when deploying multiple MRs. In [10], Cho and al. considered multiple MRs and HAs multihomed mobile networks to provide HA-based dynamic load sharing. A neighbor MR authentication and registration mechanism was also introduced. Choi et al. have proposed then a transparent failover mechanism (TFM) to provide seamless Internet services by introducing a “peer” relationship among the multiple MRs of the same NEMO [11]. Wang et al. [12] proposed the MULTINET approach: a policy-based multi-access

support for NEMO multihoming using a single Mobile Router with multiple egress interfaces. This approach exploits the multiple care-of addresses extension (MCoA) [8]. A Host Identity Protocol (HIP) extension called HIP-NEMO was introduced by Novaczki et al. [13] to provide secure and efficient multihoming NEMO solution. Park et al. introduced in [14] a novel concept of a virtual mobile network in the context of multihomed NEMO based on single MR with multiple egress interfaces. The MR can advertise information of access networks to its subnet so that each MNN can select appropriate access network to forward the MNN's traffic. Recently, a solution to support multihoming in NEMO based on Proxy Mobile IPv6 (PMIPv6) [4] was proposed by Li et al. [15].

Although the improvement brought by these contributions to NEMO BS protocol, the multihoming issues are still open. Further design, implementation and evaluation are still needed for standardization. In the remainder of this paper, we investigate the (n,n,1) multihoming NEMO configuration and propose a new transparent and seamless approach to manage mobility and traffic at the Mobile Network level.

3. Multihoming Capabilities and Issues for the Configuration case (n,n,1)

When dealing with Multiple Mobiles Routers based multihomed NEMO, the choice of (n,n,1) multihoming configuration instead of (n,n,n) configuration is essential because of its capabilities to achieve multihoming benefits in a transparent fashion with respect to transport and application layers. In the (n,n,n) model, each MR has its MNP. There are two solutions for multihoming mechanisms. The first solutions use multiple encapsulation levels by considering a Nested Mobile Network model [16] and leave configured IP addresses unchanged (i.e there will be no change in already assigned IP addresses for MNNs). This leads to more complexity and relatively higher delays. Other solutions recommend configuring MNNs with new IP addresses from the MNP delegated to the substitute MR that will provide the new path to internet. Unfortunately, changing these addresses will cause more damages to applications. This is so because current applications and transport layers, such as TCP and UDP, identify the endpoints of a communication through the IP addresses of the nodes involved, implying that the IP addresses selected at the communication establishment time must remain invariant through the lifetime of the communication. So, any change in the source addresses will lead to a high latency and causes the re-establishment of the transport sessions. The (n,n,1) configuration however allows us to avoid these performance degradations.

Though, the mobility must be achieved in an optimized and a seamless fashion. In the (n,n,1) configuration , each MR independently maintains its own bidirectional tunnel. When a failure in the currently used path occurs, it must be detected, in order to change the tunnel that has failed. Hence mechanisms to detect failures and check tunnel keepalive are needed. On the other hand, once a failure in the currently used path is detected, alternative paths have to be explored in order to identify an available one.

Another issue that has to be solved is related to the optimization of the latency of these operations. Indeed, the overall delay to detect the failure of the current tunnel, discover and select others paths and configure one of them would be relatively high. Fast mechanisms are so needed.

Moreover, a mechanism to manage the distribution of outbound traffic for Load-Sharing and Policy-Routing is required.

4. Proposed Multihoming Mobility Support

To overcome the lack of multihoming support in NEMO BS, we introduce a new approach for network mobility by proposing a Router-Proxy as a central gateway inside the Mobile Network to perform mobility and traffic management and by using unidirectional HA-MR tunnel instead of bidirectional ones.

Furthermore, because of failure detection delay and multihoming operation, packets destined to the MN network may be delayed or lost during handoff period. To this end, we introduce other mechanisms to improve our solution.

4.1 Unidirectional HA-MR Tunnel

One of the main drawbacks of NEMO Basic Support that affect the efficiency of the protocol is the bidirectional tunnel. Indeed, the NEMO BS does not allow direct routing between MR and CN. Outbound traffic has to be sent to the HA first, and then forwarded to the CN, even when a much more efficient route exists between the CN and the MR. Sending outbound traffic via the MR-HA tunnel is not really necessary.

This triangular routing mechanism takes in general much more time than the direct routing because of the operations of encapsulation and decapsulation, leading hence to increased transmission delay. To overcome this weakness, we propose to use only a unidirectional tunnel from HA to MR for inbound traffic as illustrated in (Fig. 2). On the other hand, outbound traffic will be forward directly to the correspondent node using routing optimization. Obviously, this policy routing must be implemented at the Mobile Router level.

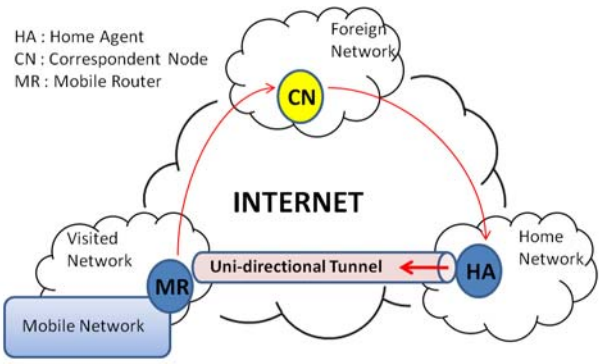

Fig. 2. MNN-CN Communication via Ha->MR Unidirectional Tunnel

4.2 Mobile Network Proxy (MNPx)

In our proposal, the Mobile Network Proxy (MNPx) will be the unique default gateway for all MNNs. All outbound traffic from MNNs as well as inbound traffic to MNNs must pass through MNPx. (Fig. 3)

A MN has one primary MR and one or more secondary MRs. The MNP delegated to the primary MR is also communicated to MNPx which has to advertise it to MNNs. Inside the MN, MRs can only communicate with MNPx and have not to communicate to each other nor to MNNs. Once a failure in the currently used path to Internet is detected one of the registered MRs that have already tunnels with the primary MR's Home Agent must replace the failed MR.

The MNPx has the exclusive responsibility to choose and to designate the substitute MR on the basis of information it holds about all MRs. As a result, we define in our approach two principal components to be implemented in the MNPx: (i) the Environment Detector Component and (ii) the Policy Decision Component which are detailed below.

4.2.1 Environment Detector Component

This component has the responsibility of detecting all the changes which could occur on the level of mobiles routers and from which some triggering events are created. At this stage, we are confronted with various problems: which information the Environment Detector should detect, how to get this information and how to use it. However, addressing all these issues is out of the scope of this paper. We focus here only on necessary information for Mobility/Traffic management purpose, especially those related to tunnel failure detection and access links capabilities.

At the MN level, the detection of tunnel failures between the primary MR's HA and MRs should rely on Router Advertisements from Access Routers to MRs, or other L2 trigger mechanisms to detect faults. The MR then transmits a notification about the failure to MNPx. However, this mechanism suffers enough from latency particularly when MR itself or its ingress interface fails.

To expect fast detection, we propose the use of a proactive keepalive test mechanism handled periodically by the Environment Detector. This latter performs at very short periods the keepalive test with all its MRs to see whether the established tunnels with the primary MR's HA are still alive. Likely, the Environment Detector should generate periodic requests to ask MRs for access links capabilities. Information collected by the Environment Detector Component is automatically forwarded to the Policy Decision Component who must trigger consequently the appropriate events and update its *MR_Data Cache* (see Table 1).

4.2.2 Policy Decision Component

a) Mobility management

The main idea behind our proposal is, when possible, to register and establish tunnels in advance between each secondary MR and the primary MR's HA and use them when the primary MR fails or loses link connectivity. We point out here that all MRs belonging to the MN are registered at the MNPx (e.g. by physical addresses) and their ingress interfaces are IP configured by MNPx from the delegated MNP, so that they are easily authenticated.

MR_Data Cache at MNPx: MNPx maintains an information Cache (called MR_Data Cache) for all MRs belonging to the Mobile Network. Each entry in the MR_Data Cache Table contains the following fields:

MR field: the MR identifier (e.g. its ingress interface physical address)

MRType field: primary MR (1) or secondary MR (0)

HoA field: MR Home Address

CoA field: acquired CoA

Tunnel Status field: established (1) or not yet (0)

Active field: indicates whether the tunnel is active (1) at this time or not (0)

Other fields: Bandwidth, Packet Loss Rate and Round Trip Time (RTT) represent some necessary information about the actual access links that should be used for eventual traffic management.

Table 1 : MR_Cache Table at MNPx

MR	MRType	HoA	CoA	Tunnel Status	Active	Bandwidth	Packet Loss Rate	Round Trip Time (RTT)	Service Cost	Others Fields
MR1	1	HoA1	MR1 CoA	1	1					
MR2	0	HoA2	MR2 CoA	0	0					
MR3	0	HoA3	MR3 CoA	1	0					

b) Traffic management

Since several paths to internet through the different MRs will be available at the same time, path selection and load sharing can provided by the MNPx if necessary information of access networks is gathered by the Environment Detector. Then, on the basis of this information and user application preferences MNPx can select appropriate path to forward the MNN's outbound traffic independently from the downlink tunnels. In this paper, we focus only on mobility management. The traffic management issue will be addressed in further work.

4.3 Multihoming Mobility Mechanisms

Let us consider the example of (Fig. 3) where MR1 is the primary MR. Assume that the secondary MR3 has obtained a CoA and established a tunnel with its Home Agent HA3. MR3 then notifies MNPx with an authenticated message including the MR3 home Address HoA3, the acquired CoA and a Nonce (a random integer) used as a return routability check, instead of using the long return routability procedure of IPv6.

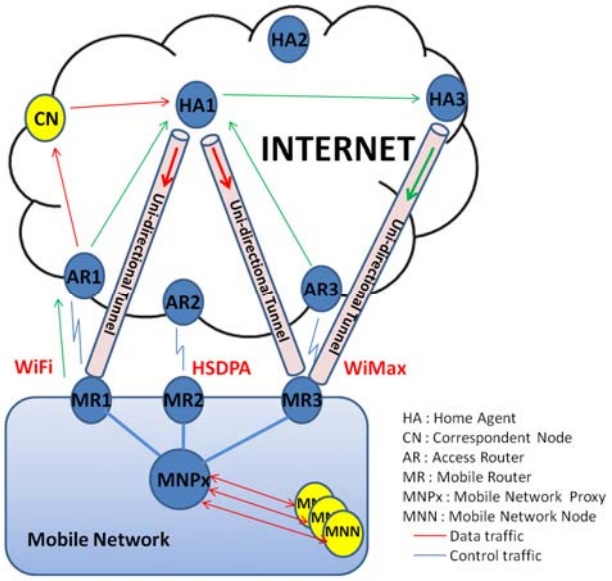

Fig. 3. Principe of the MNPx based Support Mobility

MNPx first updates MR_Data cache entry for MR3 then it communicates information sent by MR3 to MR1 and orders it to request its Home Agent HA1for registering MR3 as a substitute for MR1. Then MR1 sends to HA1 a substitute registration request message including the information it receives from MNPx. On receiving this message, HA1 sends an invitation message to MR3 to register. This message includes the MNP of MR1, the MR3's Nonce and another Nonce generated this time by HA1. The message arrives at MR3 via its Home Agent HA3. MR3 checks the validity of the message, if so it replies to HA1 with a substitute Binding Update (SBU) message including the acquired CoA, MNP and HA1's Nonce. After checking the validity of this message, HA1 then register MR3 as a substitute for MR1 in its binding cache and sends a Binding ACK to MR3.

To provide fast handover, a unidirectional tunnel between HA and MR3 is established in advance and will be used when needed. Then, HA1 sends a notification message to MR1 to inform it that MR3 has been registered as a substitute. This information is immediately forward to MNPx which consequently updates its MR_Data Cache. This procedure is illustrated at (Fig. 4).

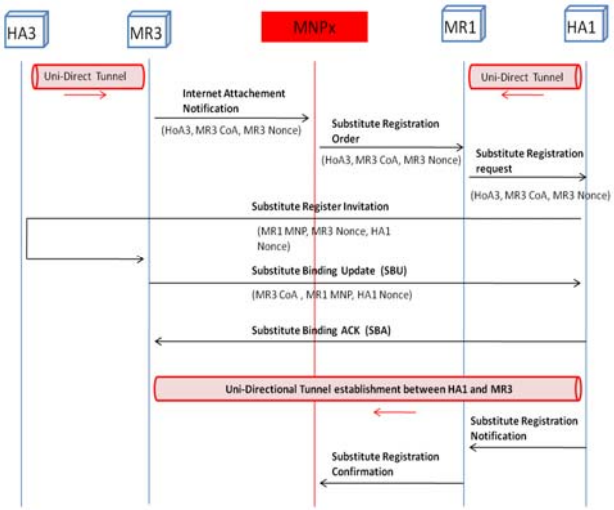

Fig. 4. Substitute MR Registration

4.3.1 Change in BU Message Format

A new MR Type Flag (T) is included in the Binding Update (Fig. 5) to indicate to the Home Agent whether the Binding Update is coming from a primary Mobile Router or a secondary Mobile Router. The BU message must include also another field for the HA1's Nonce value.

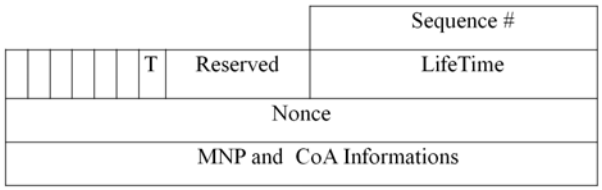

Fig. 5. Substitute BU Message Format

4.3.2 Change in Binding Cache Table at HA1

With MIPv6 basic support [1], a Mobile Node can register only one CoA with its HA. Hence, the registration of multiple CoAs with a single HoA is not possible. To accommodate multiple binding registrations at the HA1, we modify the binding cache structure of the HA1 to take into account information about possible substitute Mobile Routers. We add three fields (Table 2):

- MR-type Field: indicates whether the registered MR is a primary MR (value set to 1) or a secondary one (value set to 0).
- Tunnel Field: indicates whether this tunnel is active (opened) or not (closed).
- ExpireTime: indicates the time at which this tunnel is considered unavailable. The value of this field is obtained by the following equation (1):

  ExpireTime = CurrentTime + LifeTime (1)

Table 2: Binding Cache Table at HA1

Prefix	CoA	MRType	Tunnel	ExpireTime
MNP	MR1 CoA	1	Opened	-
MNP	MR3 CoA	0	Closed	-
---	---	---	---	---

4.3.3 Transparent and Seamless Session Continuity

When the MNPx detects the MR1 failure by means of the Environment Detector Component, it immediately looks in its MR_Data Cache for the available substitute MRs (Tunnel status = 1), chooses one according to a predefined policy and orders it to request HA1 to open the associated tunnel. Let's again consider the example of (Fig. 3). Assume that MNPx chooses MR3 to replace the failed MR. MR3 requests HA1 to open its tunnel for traffic destined to the MN indicating a MR1 failure. On receiving this message, HA1 opens the HA1-MR3 tunnel through which traffic destined for the MN is immediately forward. HA1 will use both HA1-MR1 and HA1-MR3 tunnels simultaneously until it confirms that MR1 has failed. HA1 will use a special check procedure to see whether MR1 is alive or not (this test include the path until MNPx). If MR1 has effectively failed, HA1 removes the MR1 entry from its binding cache Table, otherwise it maintains the HA1-MR1 tunnel opened and closes the HA1-MR3 tunnel. Except if a routing policy is implemented at HA1, this latter should always forward incoming packets toward the MN, in priority through the tunnel established with the primary MR.

We propose that HA1 maintains a copy of the last forwarded packets toward the MN (the size of this cache depends on the overall delay for tunnel change operation (failure detection, choice of the substitute MR and tunnel change request). When, HA1 receives a tunnel change request, it will retransmit them through the new tunnel. Thus, no packet loss can be achieved.

Since we do not use any tunnel for outbound traffic, on MR1 failure the outbound traffic is immediately and directly routed by the selected substitute MR without being buffered. However, a cache of the last forwarded packets by The MNPx will also prevent packet loss delay.

Thus, MNNs are not involved in this process and the transparency is guaranteed.

5. Performance Evaluation

Simulation experiments were performed using the network simulator NS-2 [17] with Mobiwan [18] extensions to evaluate the performance of our proposed mechanisms in terms of handover latency and packet loss. Our results are compared to the NEMO BS solution.

We implemented the MNPx based mobility support within NS-2 by creating new three types of Agent inheriting from Agent class: ProxyPolicyAgent, MRMobilityAgent and HAMobilityAgent. In our simulation, a MNPx is a Node attached with a ProxyPolicyAgent, a MR is a Node attached with a MRMobilityAgent and a HA is a Node attached with a HAMobilityAgent.

5.1 Simulation Topology and Parameters

(Fig. 6) describes our simulation network topology. According to Mobiwan extensions we have created a Wide Area IPv6 network that represents the core of internet and two Base Stations BS1 and BS2 to be used as Access Routers. The Mobile Network consists of four 802.11

mobile nodes: two Mobile Routers, MR1 as primary and MR2 as secondary, the proxy MNPx and a MNN (A). The protocol AODV was used, although any routing protocol can be used. The wireless transmission range was set to 100 m. The topology is designed in such a way that BS1 can reach only MR1, BS2 can reach only MR2, and MNPx covers all mobile nodes inside the MN, but no one of the mobile nodes can reach the others.

The simulation time was set to 60 seconds. We create a CBR traffic source and attach it to a UDP agent at the Correspondent Node (B) level. This traffic is directed from B toward A at the data rate of 200Kbps. Packet size was set to 1500 bytes. Internet latency is supposed random following a uniform distribution in the interval [50ms, 250 ms]. We start the simulation with the tunnel established with MR1. At t= 20 s, we intentionally make MR1 failure and reactivate it at t=40 s.

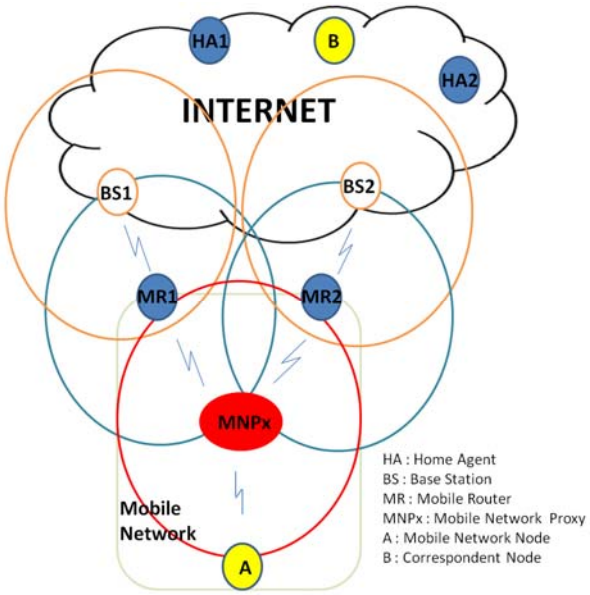

Fig. 6. Proposed Simulation Topology

5.2 Simulation Results

We first compare the performance of our proposed MNPx based support to NEMO BS. (Fig.7) show measured throughput at node A. Because of the lack of multihoming support, at t=20s once MR1 fails the throughput for NEMO BS falls to zero and stay equal to zero until the MR1 is again registered. Notice that even if MR1 is activated at t=40s few seconds are needed before the tunnel is again available.

However, in MNPx based support, the substitute mobile router MR2 provides an alternative tunnel almost immediately after detecting the failure achieving hence a seamless Internet service. The multihoming Handoff is performed in less than one second. This delay can also be improved by a good parameter setting of keepalive test period.

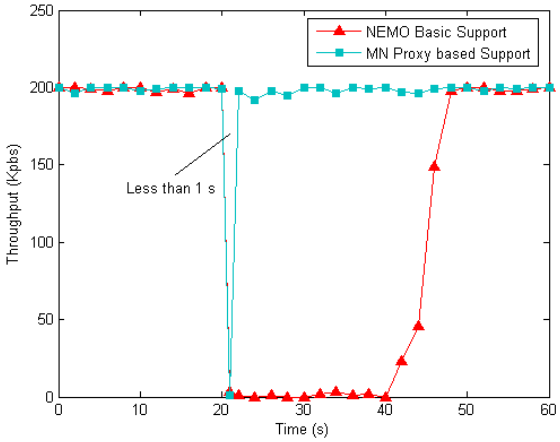

Fig. 7. Throughput over time (Failure Detection Delay=500 ms)

In the second simulation experiment we examine the impact of Failure Detection Delay (FDD) and Last Forwarded Packet (LFP) cache size on Packet Loss. It was observed that Packet Loss increases with FDD and decreases with LFP (Fig. 8). Packet Loss can be totally eliminated if these parameters are rightly configured.

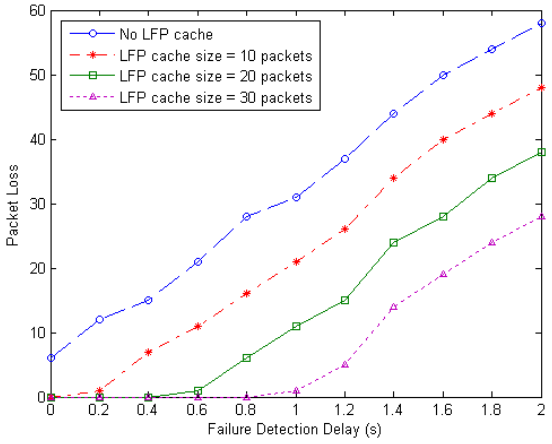

Fig. 8. Packet Loss vs Failure Detection Delay (vs LFP cache size)

6. Conclusion

In this paper, we have proposed a novel network mobility support in the context of (n,n,1) model based multihomed NEMO networks. Our approach uses MRs registration at

the Home Agent delegating the Mobile Network Prefix and beforehand establishment of unidirectional tunnels. We introduced also a Mobile Network Proxy to manage mobility and outbound traffic at the mobile network level. Simulation results show that our proposition provides excellent performance in terms of Handoff delay and Packet Loss. Our improving mechanisms for the proposed architecture are very efficient and make it possible to achieve a really transparent and seamless connectivity as well as routing optimization.

References

[1] D.Johnson, C.Perkins, and J.Arkko, "Mobility Support in IPv6," IETF, RFC 3775, June 2004.

[2] H. Soliman, C. Castelluccia, K.-E. Malki, and L. Bellier, "Hierarchical mobile IPv6 mobility management," IETF, RFC 4140, Aug. 2005.

[3] R. Koodli, Ed."Fast Handovers for Mobile IPv6", IETF, RFC 4068, July 2005.

[4] S. Guidiville, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil (2008). "Proxy Mobile IPv6," IETF, RFC 5213, August 2008.

[5] Devarapalli, V., Wakikawa, R., Petrescu, A., and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol," IETF, RFC 3963, January 2005.

[6] N. Montavont, T. Noel and T. Ernst, "Multihoming in nested mobile networking," SAINT 2004 Workshops on 26-30 Jan. 2004 Page(s):184 – 189.

[7] C. Ng, E. Paik, T. Ernst, M. Bagnulo, "Analysis of Multihoming in Network Mobility Support," IETF, RFC 4980, October 2007.

[8] R. Wakikawa, V. Devarapalli, G. Tsirsis and T. Ernst and K. Nagami, "Multiple Care-of Addresses Registration," IETF, RFC 5648, October 2009.

[9] E. K. Paik, H. S. Cho, T. Ernst and Y. H. Choi, "Load sharing and session preservation with multiple mobile routers for large scale network mobility," The proceedings of AINA 2004: Page(s):393 - 398 Vol.1.

[10] S. H. Cho, J. K. Na and C. K. Kim, "A dynamic load sharing mechanism in multihomed mobile networks," ICC 2005 16-20 May 2005 Page(s):1459 - 1463 Vol. 3.

[11] N. Choi, J. Ryu, E. Paik, T. Kwon, and Y. Choi, Senior, "A Transparent Failover Mechanism for a Mobile Network with Multiple Mobile Routers", IEEE COMMUNICATIONS LETTERS, VOL. 11, NO. 7, JULY 2007.

[12] Q. Wang, R. Atkinson, and J.Dunlop, "Towards Always Best Connected Multi-Access: the MULTINET Approach", IWCMC '08. August 2008.

[13] S. Novaczki, L. Bokor, G. Jeney, and S. Imre, "A HIP based network mobility protocol," JOURNAL OF NETWORKS, VOL. 3, NO. 1, JANUARY 2008

[14] C. Park, N. Choi, E. Paik, T. Kwon and Y. Choi, "Multiple Interface/Prefix Selection for Virtual Mobile Networks", ICACT, February 2008

[15] Y. Li, D. Kum, and Y. Cho, "Multihoming Support Scheme for Network Mobility Based on Proxy Mobile IPv6", ISECS International Colloquium ICCCM'08, August 2008.

[16] N. Montavont, T. Ernst, and T. Noel, "Multihoming in Nested Mobile Networks", In International Symposium on Applications and the Internet (SAINT)-IPv6: Technology and Deployment Workshop", Tokyo, January 2004.

[17] The Network Simulator manual, The NS2 homepage http://www.isi.edu/nsnam/ns

[18] T. Ernst. MobiWan: NS-2 extensions to study mobility in Wide-Area IPv6 networks http://www.inrialpes.fr/planete/mobiwan/

Zohra Slimane received her Engineering Diploma in Telecommunication in 2006, and her Magister Diploma in SRT Telecommunication Systems and Networks in 2008 from Tlemcen University (Algeria). Since 2008, she has been a system engineer at Sonatrach Aval Research Group and a PhD student researcher at STIC Laboratory (Tlemcen Algeria). Her research interests include networking, information systems, mobile networks, ubiquitous internet and fourth-generation networks.

Mohammed Feham received his Dr. Eng. degree in optical and microwave communication from the University of Limoges (France) in 1987, and his PhD in Science from the University of Tlemcen (Algeria) in 1996. Since 1987, he has been an Assistant Professor and Professor of microwave and communication engineering. He has served on the Scientific Council and other committees of the Electronics and Telecommunication Departments of the University of Tlemcen. His research interests include telecommunication systems and mobile networks and services.

Abdelhafid Abdelmalek received the Laurea degree in Telecommunication Engineering from Institute of Telecommunications Oran (Algeria) in 1991, and Diploma of deepened studies in optoelectronic at Nancy (France) in 1993. From 1994 to 2000, he worked as engineer in charge of design and management of ISDN networks at Algerie Telecoms Company. In 2002, he received a Magister Diploma in Signals and systems at Tlemcen University, Algeria. From 2004, he is a PhD researcher. His research interests include data communications, Mobile networks, security, protocols and next generation networks.

To appear in IJWMN Vol.4, No.3 2012

Seamless Infrastructure independent MultiHomed NEMO Handoff Using Effective and Timely IEEE 802.21 MIH triggers

Zohra Slimane, Mohamed Feham and Abdelhafid Abdelmalek

STIC Laboratory University of Tlemcen Algeria
{ z_slimani, m_feham, a_abdelmalek }@mail.univ-tlemcen.dz

ABSTRACT

Handoff performance of NEMO BS protocol with existent improvement proposals is still not sufficient for real time and QoS-sensitive applications and further optimizations are needed. When dealing with single homed NEMO, handoff latency and packet loss become irreducible all optimizations included, so that it is impossible to meet requirements of the above applications. Then, How to combine the different Fast handoff approaches remains an open research issue and needs more investigation. In this paper, we propose a new Infrastructure independent handoff approach combining multihoming and intelligent Make-Before-Break Handoff. Based on required Handoff time estimation, L2 and L3 handoffs are initiated using effective and timely MIH triggers, reducing so the anticipation time and increasing the probability of prediction. We extend MIH services to provide tunnel establishment and switching before link break. Thus, the handoff is performed in background with no latency and no packet loss while ping-pong scenario is almost avoided. In addition, our proposal saves cost and power consumption by optimizing the time of simultaneous use of multiple interfaces. We provide also NS2 simulation experiments identifying suitable parameter values used for estimation and validating the proposed model.

Keywords

NEMO, multihoming, seamless handoff, IEEE 802.21, MIH triggers, path loss model, NS2

1. INTRODUCTION

It is now possible to deploy, in moving networks such as vehicle and aircraft networks, applications implying communications with the infrastructure or with other moving networks while profiting surrounding heterogeneous wireless capacities of communication (e.g ieee 802.11, ieee 802.16, 3GPP, 3GPP2). Network Mobility [1] NEMO Basic Support (BS) is one of the few solutions that have been widely accepted in the academic world and the industry for supporting the mobility of moving networks. NEMO allows an entire IP network to perform a layer 3 (L3) handoff. Transparent service continuity is achieved using a mobile router for mobility management on behalf of the transported mobile network devices. Handoff performance plays a crucial role in QoS-sensitive applications and real-time services in heterogeneous networks. Although NEMO BS has the merit to allow as of today the deployment and the experimentation of no time constraints services without having to function in a degraded mode, its performance (high latency, high packet loss and high signaling cost) is thus clearly considered as suboptimal and is not appropriate for time constraints applications.
Therefore, there have already been a number of studies and a large set of optimizations that try to address these issues ([6]-[17]). The proposed solutions rely on the optimization of each component of the handoff, using cross layer design, network assistance, multihoming, etc. However, minimal reached values of handoff latency and packet loss still do not fill real time and QoS-sensitive applications requirements. Consequently, NEMO with the above optimizations is still not sufficient for such applications and further improvements or solutions are needed.

In this paper, we propose a new multihoming based NEMO handoff scheme achieving seamless connectivity (precisely with zero latency and zero packet loss). Our cross layer design uses timely and effective MIH triggers (such as Link_Going_Down, Link_switch_Imminent) and required handoff time based adaptative MIH command services such as Link_Configure_Thresholds. We provide proactive surrounding networks attachment, home registration, tunnel establishment and then tunnel switching if necessary just before Link Down event. With this manner of executing the anticipation, we increase the probability of prediction avoiding ping-pong scenario and we save also cost and power consumption.
The rest of the paper is organized as follows. Section 2 introduces the related works on NEMO optimizations. Section 3 provides NEMO handoff components analysis and numerical evaluation. Section 4 gives an overview of IEEE802.21 STD and MIH services. In Section 5, we describe the details of our proposal and associated algorithms. In Section 6, NS2 implementation and simulation results are presented, and the performance of the proposed scheme is discussed. Finally, conclusions are stated in Section 7.

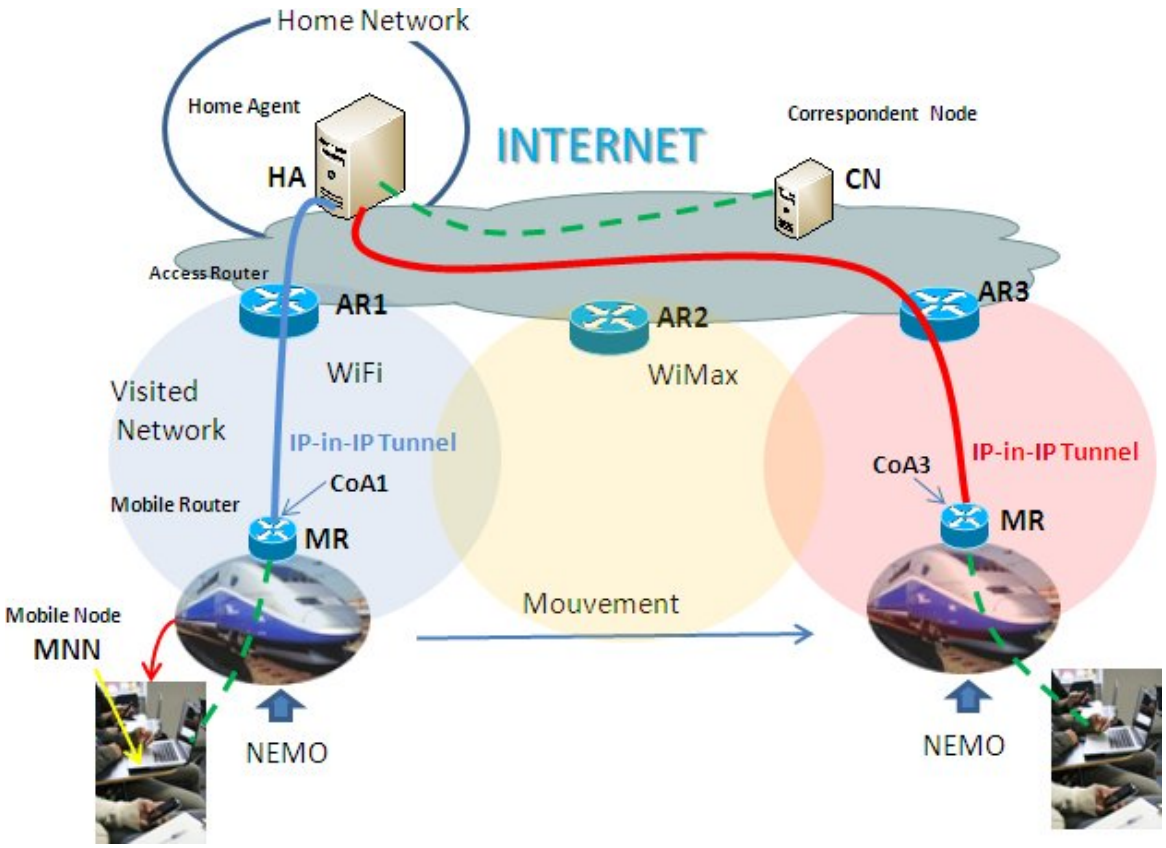

Figure 1. Basic Components of NEMO BS Protocol

2. Related Work

NEMO BS Protocol [1] designed by IETF to manage network mobility (Figure 1) is an extension of the MIPv6 [2] protocol. The NEMO BS handoff inherits so the drawbacks of MIPv6. It is composed of the link layer handoff followed by the new network attachment and then the home registration. Brake-Before-Make handoff performance (latency, packet loss and signaling overhead) of NEMO BS were analyzed in the literature [3, 4, 5,

8, 9, 18]. The results show that the mobility support does not provides seamless connectivity. To overcome the limitations of NEMO BS protocol, many optimizations were proposed. To reduce the new network attachment for MIPv6-NEMO, delay Optimistic Duplicate Address Detection (ODAD) [6] and Fast Router Advertisements [3,7] were proposed. Besides, Many Infrastructure based mobility supports were proposed to address handoff efficiency in NEMO. Cross layer design scheme [8] using IEEE 802.21MIH services and addressing movement prediction and handoff timing algorithms was proposed on FMIPv6 to anticipate L3 handoff. HiMIP-NEMO [9] proposes the use of Foreign Mobility Agent (FMA) to achieve QoS handoff with reduced latency and packet loss. An extension of Proxy MIPv6 (PMIPv6) called N-NEMO [10] was proposed to provide mobility support for NEMO context. The scheme is based on tunnel splitting, global tunnel between LMA and MAG, and local tunnel between MR and MAG, leading to reduced signaling cost.

Many other works based on multihoming were investigated to improve seamless handoff. In [11] a new entity ICE (Intelligent Control Entity) is introduced in NEMO architecture to improve handoff for multiple MRs-based multihomed NEMO. Another protocol called SINEMO [12] using IP diversity and soft handoff was proposed to reduce Handoff signaling cost for a single multihomed MR based NEMO. Other GPS Aided Predictive Handover Management solutions using Make Before Brake handoff were proposed to improve handoff performance but they are rather more suitable for multihomed train-based NEMO [13, 14, 15].

Higher layer Extensions such as SIP-NEMO [16] and HIP-NEMO [17] based respectively on Session Initiation Protocol (SIP) and Host Identity Protocol (HIP) were also proposed. However, in addition to being not transparent to all applications these schemes suffer from additional signaling overhead.

The handoff performance of NEMO BS with above optimization is still not sufficient for QoS-sensitive applications. Latency of link layer handoff and NEMO signaling overhead (precisely from the round trip time RTT between the Mobile Router and the Home Agent) affect the overall performance of mobility management significantly.

3. NEMO handoff Latency Analysis

NEMO Basic Support (BS) protocol proposed by IETF provides mobility support for an entire mobile network moving across different heterogeneous access networks Continuous and uninterrupted internet access to the Mobile Network Nodes (MNN) inside the mobile network is provided by the Mobile Router (MR) which manages the movement (Figure 1). The MR is identified by its Home Address (HoA) through which it is accessible in its home network, and it is localized by its Care-of-Address (CoA) acquired at visited network. The Home Agent (HA) located at the home network assists the MR to support mobility management. To change its point of attachment to a new access network (i-e to a new access router AR), the MR must process in general a vertical Handoff including both L2 and L3 Handoff (Figure 2).

Since L2 and L3 Handoff are independent in NEMO BS protocol (L3 Handoff occurs after L2 Handoff), the overall handoff latency can be expressed by the following equation:

$$T_{HO} = T_{L2} + T_{L3} \quad (1)$$

Where T_{L2} is the Link layer (L2) Handoff latency (the time required to establish a new association by the physical interface) and T_{L3} is the IP layer (L3) Handoff latency (the time to register the new CoA at the Home Agent (HA) and to be able to receive the first data packet at this new localization).
L2 Handoff procedure includes in general scanning (T_{scan}), authentication (T_{auth}) and association (T_{ass}) which are very dependent on technology and exhibit great variation. The published values of T_{L2} are between 50 ms and 400 ms [4, 19, 20, 21].

Then:

$$T_{L2} = T_{scan} + T_{auth} + T_{ass} \quad (2)$$

The L2 Handoff is triggered by the link event:

$$P_{rx} < P_{th} \quad (3)$$

Where P_{rx} is the received signal power corresponding to the received signal strength indication (RSSI) and P_{th} is the predefined threshold power below which the Link status is considered down.

L3 Handoff procedure is composed of four distinct phases:

- Movement Detection (MD): after disconnecting from the old AR (oAR), the MR detects its movement thanks to prefix information contained in received Router Advertisement (RA) messages broadcasted periodically by the new AR (nAR). The MR may proactively send Router Solicitation (RS) messages to obtain the RA message from the nAR (The MR detects its movement if the oAR is unreachable, i-e no RA messages from the oAR).
- Duplicate Address Detection (DAD): Upon receiving prefix information from the nAR, the MR proceeds to the stateless auto-configuration; it configures itself with a new CoA (constructed from new prefix) and must check its uniqueness with the DAD process.

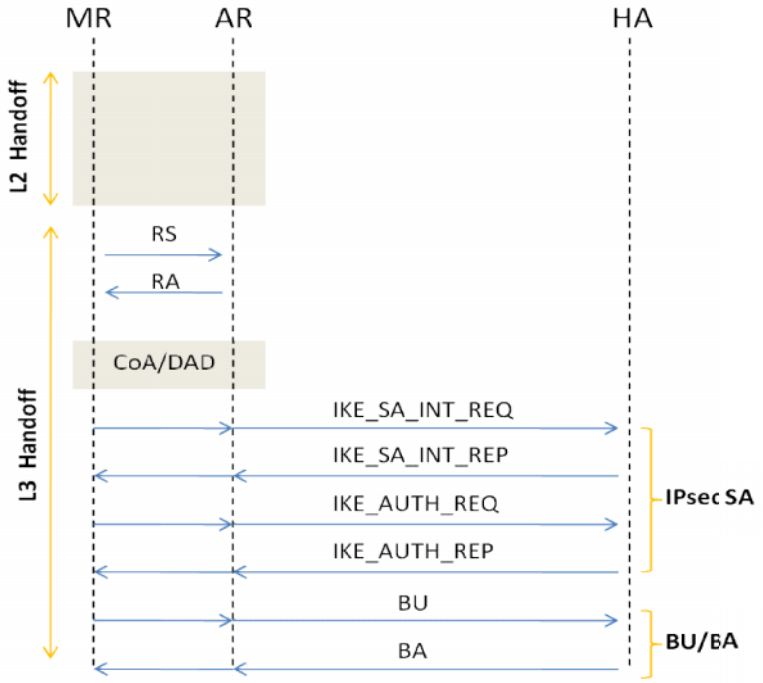

Figure 2. NEMO BS Protocol handoff procedure

- New CoA Registration and MR-HA Tunnel establishement (Reg): As soon as the MR acquires a new CoA, it immediately sends a Binding Update (BU) to its Home Agent (HA). Upon receiving this message, the

HA registers the new CoA in its binding cache and acknowledges by sending a Binding Acknowledgement (BA) to the MR. As stated by [1], all signaling messages between the MR and the HA must be authenticated by IPsec. Once the binding process finishes, a bi-directional IP-in-IP tunnel is established between the MR and its HA. The tunnel end points are the MR's CoA and the HA's address. Either IPsec or other IP-in-IP protocol could be used for this purpose.

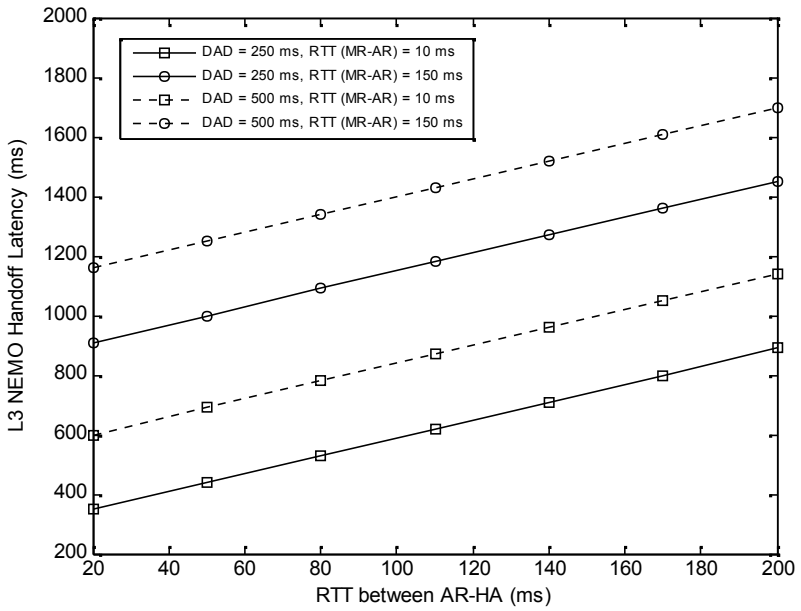

Figure 3. L3 NEMO Handoff latency vs. RTT_{AR-HA}

Thus, The L3 Handoff latency can analytically be computed as:

$$T_{L3} = T_{MD} + T_{DAD} + T_{Reg} \tag{4}$$

Where T_{MD} , T_{DAD} and T_{Reg} are respectively Movement Detection phase delay, DAD process delay and registration delay.
Additionally, we have in the explicit form:

$$T_{MD} = T_{RS} + T_{RA} \tag{5}$$

$$T_{Reg} = T_{SA} + T_{BU} + T_{BA} \tag{6}$$

Where:
T_{RS} : delay of Router Solicitation
T_{RA} : delay of Router Advertisement
T_{SA} : delay of creating an IPsec Security Association (SA)
T_{BU} : delay of Binding Update
T_{BA} : delay of Binding Ack

Then, according to (Figure 2) we can compute T_{L3} as function of RTT_{MR-AR} and RTT_{AR-HA} , where RTT is the Round Trip Time.

$$T_{L3} = 4\,RTT_{MR-AR} + T_{DAD} + 3RTT_{AR-HA} \tag{7}$$

(Figure 3) and (Figure 4) show respectively L3 NEMO Handoff Latency and Overall NEMO Handoff Latency (L2+L3). For RTT_{MR-AR} , we use a minimum value of 10 ms and a maximum value of 150 ms. For RTT_{AR-HA} (twice time the delay of internet) we use the measured data from [22].
Two values of DAD (250, 500 ms) are used to take account of optimistic DAD. We can easily see that the minimum value of the Total NEMO Handoff Latency exceeds 400 ms, and this minimum values are carried out only under very special conditions.

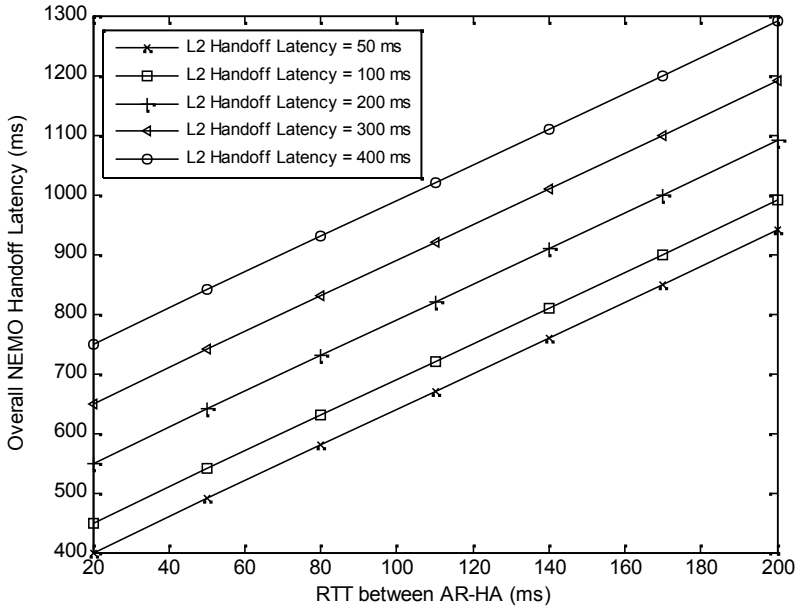

Figure 4. Overall NEMO Handoff latency vs. RTT_{AR-HA}
(only the minimum value 10 ms of RTT_{MR-AR} is considered)

(Figure 5) shows the Packet Loss during Handoff increasing with both the overall NEMO Handoff latency and the data rate. The results provided by [8] for example for NEMO Handoff improvements experienced for vehicular networks based on MIH assisted FMIPv6 show an overall NEMO Handoff latency of about 250 ms when vehicle has a slow movement (18 Km/s) and this value increases to 350 ms when vehicle speed reaches 90 Km/h. Consequently, these results show that single homed NEMO even improved is not appropriate for real time and QoS-sensitive applications.

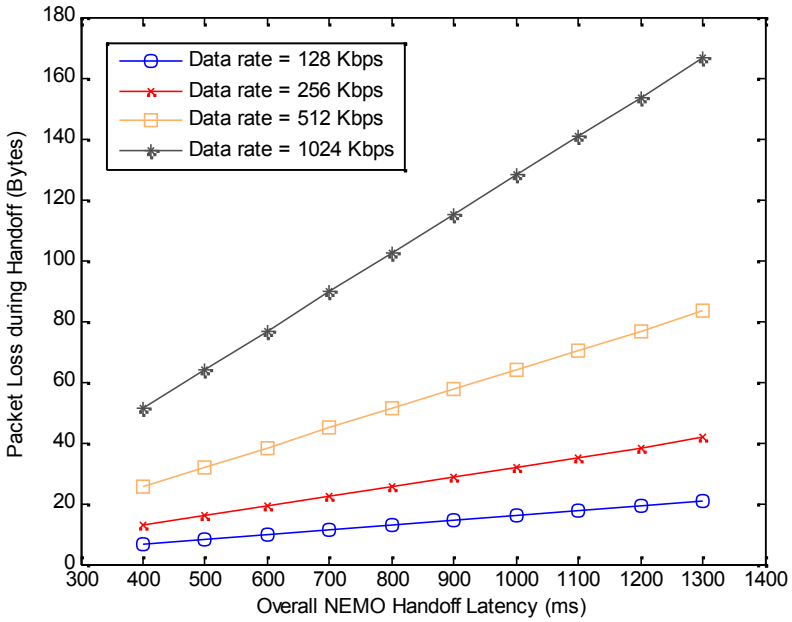

Figure 5. Packet loss during NEMO Handoff

4. IEEE 802.21 Media Independent Handover Services

The main aim of the IEEE 802.21 MIH standard [23] is the specification of generic SAPs and primitives that provide generic link layer intelligence and some network information to upper layers to optimize handovers between heterogeneous media such as IEEE 802.11 a/b/g/n, IEEE 802.16, 3GPP/3GPP2 etc. IEEE 802.21 provides a framework (a logical interface) that allows higher levels (users in the mobility-management protocol stack) to interact with lower layers to provide session continuity without dealing with the specifics of each technology. The handover process is typically conditioned by measurements and triggers supplied by the link layers on the mobile devise (either a MN or a MR).

4.1. MIH architecture

The core element of the MIH architecture is the MIH Function (MIHF) which is a logical interface between L2 and higher layers (Figure 6). MIHF which can be seen as a L2.5 layer helps in handover decision making and link selection by L3 and Upper layers by providing them with abstracted services. Upper layers (including mobility manager such as MIPv6 and NEMO, IP, transport protocols and applications) are the MIH Users. The MIH Users communicate with the MIHF via MIH_SAP (a media independent Service Access Points). The MIHF, on the other hand, interacts with L2/L1 layers via the MIH_LINK_SAP.

4.2. MIHF services

MIHF defines three main services that facilitate handovers between heterogeneous networks: MIH Event Services (MIES), MIH Command Services (MICS) and MIH Information Services (MIIS).

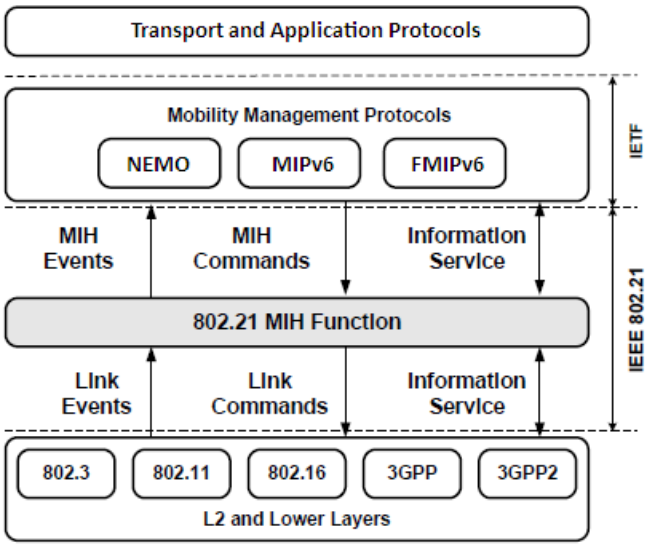

Figure 6. IEEE 802.21 General Architecture

4.2.1. MIES - Media Independent Event Service

MIH capable devices use MIES to generate L1/L2 events indicating state and parameters changes occurring on the link to the upper layers. Two types of events are possible: Link Events exchanged between L1/L2 layers and the MIHF, and the MIH Events between the MIHF and the MIH Users. The defined events include Link Up, Link Down, Link Going Down, Link Detected, Link Parameters Change, Link Event Rollback, etc.

4.2.2. MICS - Media Independent Command Service

MICS refers to the commands sent from the higher layers to the lower layers to control their behavior. Two types of commands are possible: Link Commands issued by the MIHF to the lower layers such as Link Configure Thresholds and MIH Commands issued by MIH Users to the MIHF such as Get status, Switch, Configure, Configure Link Thresholds, Scan, Handover Initiate, Handover Terminate, etc.

4.2.3. MIIS - Media Independent Information Service

MIH Users rely on The MIIS to obtain information from remote MIHF about neighboring access networks. Potential target networks and their capabilities could be discovered to facilitate handovers by making more accurate decisions. MIIS includes support for various Information Elements (IEs) which includes information about network such as Identifier, cost, QoS and security, and information about Point of Attachment (PoA) such as location, Link-layer address, subnet, data rate, etc.

5. Proposed MIH assisted Multihomed NEMO Handoff

In this section, we will describe our proposed scheme for managing mobility with NEMO when a multihomed MR is used. First, we present our model, then we explain the MIH services to be used, and finally the procedure of Handoff is detailed.

5.1. Mobility Management Model

In our proposed, we suppose a (1,1,1) Multihomed NEMO model (i-e: one MR, one HA and one MNP-Mobile Network Prefix) [27]; we consider so a mobile network with a single MR integrating multiple interfaces. These interfaces should be from different technologies or from same technology. Duplicate interface will be used in soft handoff to gain access to new network using same technology as current network becoming unreachable. The MR has a unique HoA and may obtain different CoA simultaneously. The MR is IEEE 802.21 compliant, and to provide an infrastructure independent scheme only local MIH services are used. Therefore, the HA must support multiple CoA (MCoA) registration [28]. Our scheme relies on three entities in the mobility management stack: MIHF, the Handoff Policy Decision entity (HPD) and NEMO protocol, the two last entities are MIH Users.

5.2. MIH services used in our Scheme

We utilize a subset of existing MIH services and new proposed ones to facilitate handoff decision making. (Table 1) lists these services (primitives) with corresponding parameters.

Table 1. Used MIH services in the proposed approach.

Primitive	Service	Parameters
MIH_Link_Detected	MIES	MR IF MAC Addr, MAC addr of new PoA, MIH capability, Link Type
MIH_Link_Up	MIES	MR IF MAC Addr, MAC addr of new PoA, Link ID
MIH_Link_Down	MIES	MR IF MAC Addr, MAC addr of new PoA, Reason Code
MIH_Link_Going_Down	MIES	MR IF MAC Addr, MAC Addr of Curent PoA, TimeInterval, ConfidenceLevel
MIH_Link_Switch_Imminent	MIES (new)	MR IF MAC Addr, MAC Addr of Curent PoA, TimeInterval, ConfidenceLevel
MIH_Link_Event_Rollback	MIES	MR IF MAC Addr, Event ID
MIH_Configure_Link_Threshold	MICS	LinkParameter, nitiateActionThreshold, RollbackActionThreshold, ExecuteActionThreshold
MIH_Switch	MICS	Old Link ID, New Link ID

When using a single interface, the MR cannot be associated simultaneously with more than one PoA and therefore has to break its communication with its current PoA (hard handoff) before establishing a connection with a new one. Hence, the handoff process is triggered by the Link_Down (LD) event. In our proposed scheme based on multihoming, Handoff process should be finished before the Link_Down event of the current link. So, instead of using LD trigger, we provide Link_Going_Down (LGD) and Link_Switch_Imminent (LSI) events which are fired using required Handoff time and required tunnel switching time. (Figure 7) shows corresponding received power threshold (RSS) of each event.

α_{LGD} and α_{LSI} are respectively the LGD power level threshold coefficient and the LSI power level threshold coefficient ($\alpha_{LGD} > \alpha_{LSI} > 1$). We use LGD event to trigger a soft handoff, and LSI event to switch tunnel before LD event. LSI event is used also to increase the probability of prediction and to avoid ping-pong scenario.

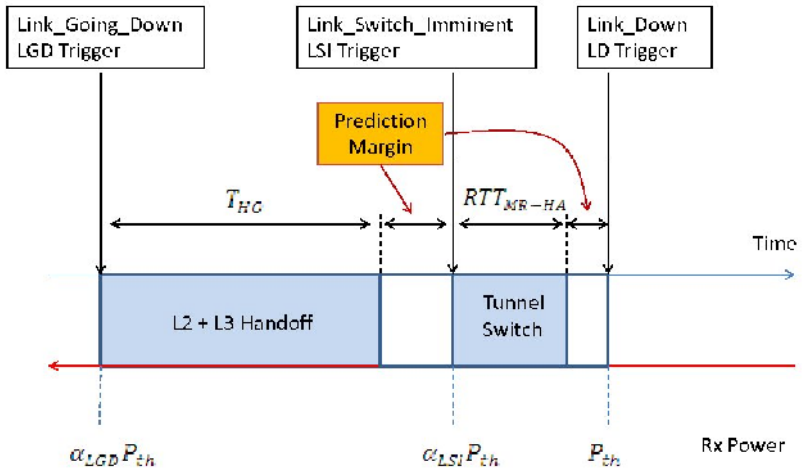

Figure 7. Generated Link triggers to prepare and perform Handoff before Link_Down event

LGD trigger in [23] is based on pre-defined threshold associated with the received signal strength (RSS). If the measured value of RSS crosses threshold $\alpha_{LGD}P_{th}$, then the LGD trigger is generated and the handover process starts.
In our proposal α_{LGD} and α_{LSI} coefficients are adaptively configured using information gathered from neighboring access networks (we use for this purpose MIH_Configure_Link_Threshold primitive).

5.3. Required Handoff Time and Tunnel switching Time Estimation

The required handoff time T_{HO} and tunnel switching time T_{TS} are important factors for timely link triggering. The LGD trigger should be invoked prior to an actual LD event by at least the time required to prepare and execute a handoff. LSI trigger should be generated T_{TS} before LD event. In our scheme, the setting $\alpha_{LGD}$is based on the following total time T_{LGD}:

$$T_{LGD} = T_{HO} + \Delta T_{HO} + T_{TS} + \Delta T_{TS} \quad (8)$$

Where :
T_{HO} is given by (1)
ΔT_{HO} and ΔT_{TS} are added as security margin.

$$\Delta T_{HO} = \gamma_1 \% T_{HO} \quad (9)$$

$$\Delta T_{TS} = \gamma_2 \% T_{TS} \quad (10)$$

γ_1 and γ_2 are between 0 and 20.

Equation (10) can be written in the following form:

$$T_{LGD} = T_{L2} + T_{L3} + \Delta T_{HO} + RTT_{MR-HA} + \Delta RTT_{MR-HA} \quad (11)$$

In the same way, we get for α_{LSI} :

$$T_{LSI} = RTT_{MR-HA} + \Delta RTT_{MR-HA} \quad (12)$$

To estimate (L2+L3) handoff time and tunnel switching time, we use:

- New detected link to get L2 handoff time estimation and RTT_{MR-nAR} based on link type information.

- Current link to get L3 handoff time estimation and tunnel switching time estimation by measuring RTT_{MR-oAR}.

5.4. Setting LGD and LSI triggers Thresholds

Given a path loss model, an analytical method can be used for effectively setting α_{LGD} and α_{LSI} coefficients [24, 25]. Let's assume the log-distance path loss model [26] for example shown in (13).

$$\left[\frac{P_{rx}(d)}{P_{rx}(d_0)}\right]_{dB} = -10\beta \log\left(\frac{d}{d_0}\right) \quad (13)$$

where d is the distance between the receiver and the transmitter expressed in meters, $P_{rx}(d)$ denotes the received signal power level in watts at distance d , β is the path loss exponent, and $P_{rx}(d_0)$ is the received power at the close-in reference distance , d_0, and can be determined using the free space path loss model (take for example $d_0 = 1\ m$).

Assuming the Mobile Network (NEMO) moving at speed v, then α_{LGD} and α_{LSI} coefficients can be determined as:

$$\alpha_{LGD} = \left\lfloor \frac{1}{1-\frac{vT_{LGD}}{d_0}\left(\frac{P_{th}}{P_{rx}(d_0)}\right)^{\frac{1}{\beta}}} \right\rfloor^{\beta} \quad (14)$$

$$\alpha_{LSI} = \left\lfloor \frac{1}{1-\frac{vT_{LSI}}{d_0}\left(\frac{P_{th}}{P_{rx}(d_0)}\right)^{\frac{1}{\beta}}} \right\rfloor^{\beta} \quad (15)$$

Figures 8 and 9 respectively 10 and 11 show α_{LGD} and α_{LSI} variations for different β values and different moving speeds. Both α_{LGD} and α_{LSI} increase with β, v and required time for their setting. For example, we plot in Figure 12 the α_{LGD} variations versus β for a mean value of T_{LGD} equal to 1.25 s.

Note that speed v can be estimated using the following approach:

Assume that at instant time t_i the received signal power level is $P_{rx}(d_i)$ and at t_{i+1} we receive $P_{rx}(d_{i+1})$, from (13) we get:

$$v = \frac{d_{i+1} - d_i}{t_{i+1} - t_i} \tag{16}$$

Therefore:

$$v = \frac{d_0}{t_{i+1} - t_i} \left| \left(\frac{P_{rx}(d_0)}{P_{rx}(d_{i+1})} \right)^{\frac{1}{\beta}} - \left(\frac{P_{rx}(d_0)}{P_{rx}(d_i)} \right)^{\frac{1}{\beta}} \right| \tag{17}$$

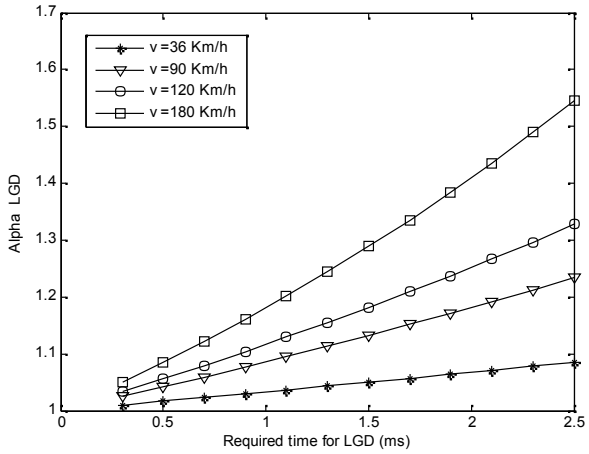

Figure 8. α_{LGD} vs. T_{LGD} (for $\beta = 3$)

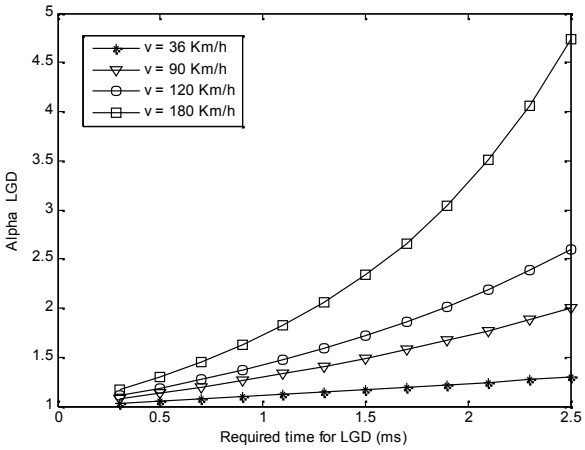

Figure 9. α_{LGD} vs. T_{LGD} (for $\beta = 3.5$)

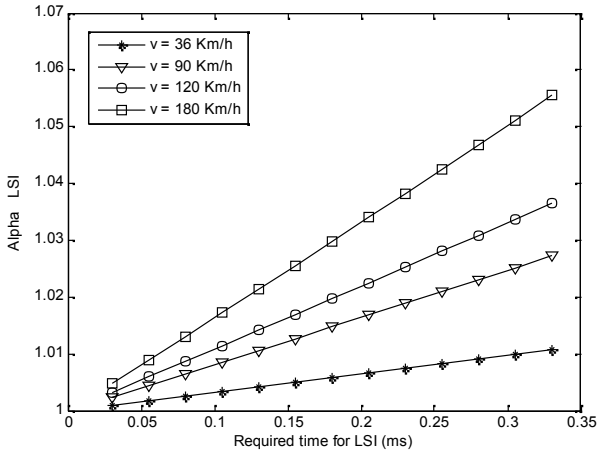

Figure 10. α_{LSI} vs. T_{LSI} (for $\beta = 3$)

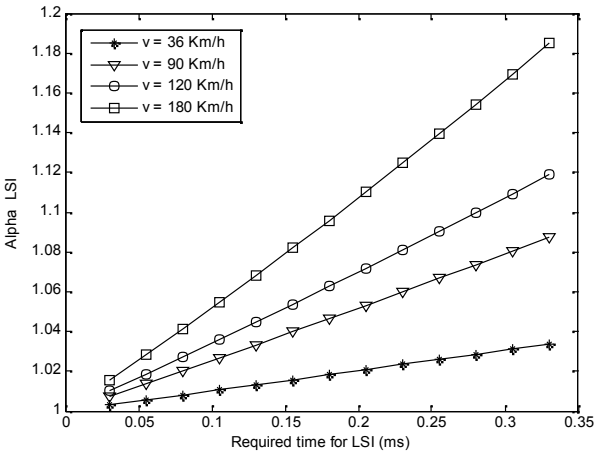

Figure 11. α_{LSI} vs. T_{LSI} (for $\beta = 3.5$)

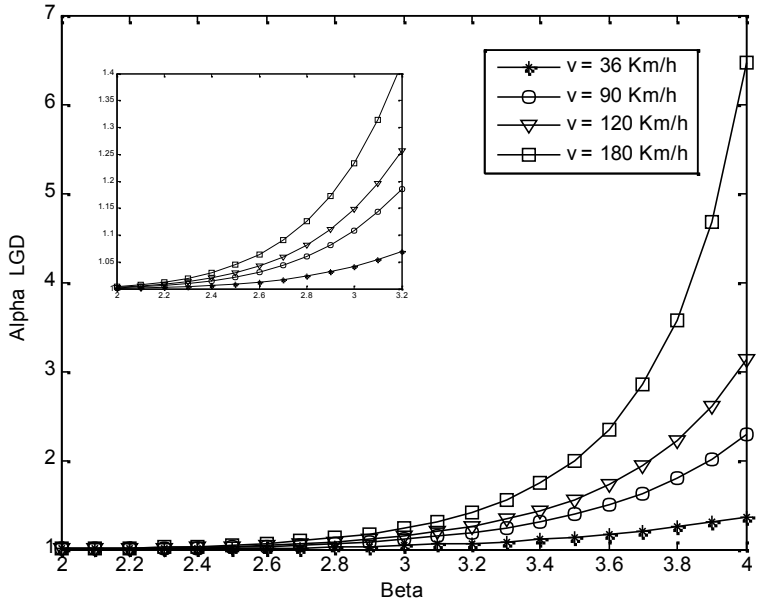

Figure 12. α_{LGD} vs. β (for $T_{LGD} = 1.25\ s$)

However, to achieve a more realistic path loss model we have to take into account the shadowing effects which may affect the propagation model. An additional component $X_\sigma\ (dB)$ is introduced in the log-distance path loss model shown in (13) leading to the model known as the log-normal shadowing [26]:

$$\left[\frac{P_{rx}(d)}{P_{rx}(d_0)}\right]_{dB} = -10\beta \log\left(\frac{d}{d_0}\right) + X_\sigma \tag{18}$$

X_σ is a zero-mean Gaussian distributed random variable with a standard deviation of σ.

When the shadowing component becomes significant, it is important to include a weighted averaging mechanism to produce a stable signal strength measure. We use for this purpose a simple recursive estimator:

$$\overline{P_{rx}}\ (i) = \delta\, P_{rx}(i) + \ (1-\delta)\overline{P_{rx}}\ (\text{i-1}) \tag{19}$$

where $\overline{P_{rx}}\ (i)$ is the average received signal power at instant i, $P_{rx}(i)$ is the received signal power at instant i and δ is the weighting factor.

5.5. Handoff operation and Tunnel switching

We suppose that the mobile network (NEMO) is already connected to an access network, and that a tunnel is already operational between the HA and the MR through one of its multiple interfaces. Let's denote this active interface IF-1. When the MR moves it could be covered by another access network. So, if a Link_Detected event is generated, by another interface (say IF-2), the MIHF translate this event to the HPD (Figure 13). This latter maintains a cache for detected links called *AvailableLinkCache* (Table 2).

So, when the HPD receives the MIH_Detected_Link event, it updates its cache and requests MIHF to generate MIH_Configure_Link_Threshold to set LGD and LSI triggers Thresholds for IF-1. Then, if a Link_Going_Down event is generated by IF-1, the HPD scans the entries in *AvailableLinkCache,* chooses the appropriate link to connect to (assume it is IF-2 link), and send a MIH_link_Connect request to MIHF to set this connection (L2 soft Handoff). Upon receiving a Link_Up from IF-2, the HPD solicits the NEMO mobility support to perform if required CoA acquisition and registration and tunnel establishment (L3 soft Handoff).

Table 2. Mobile Router Available Links Cache

MR IF MAC Addr	MAC addr of new PoA	MIH capability	Link Type	Expire Time
IF-2				
IF-3				

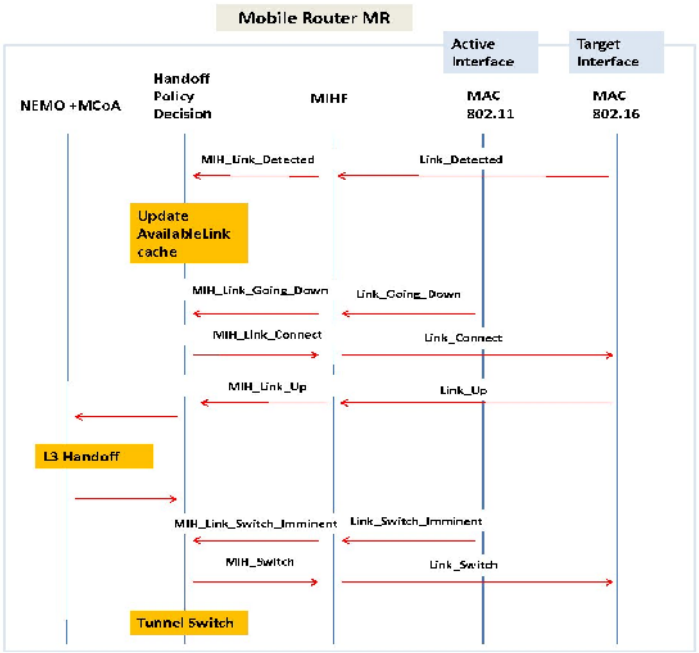

Figure 13. Proposed Handoff preparation and execution procedures

When processing Link_Going_Down event, if the received signal power $\overline{P_{rx}}$ goes up $\alpha_{LGD} \cdot P_{th}$ MIH_Link_Event_Rollback is generated.

To establish a second tunnel between MR and HA, MCoA [28] is used; we modify the binding cache structure of the HA (Table 3) to accommodate multiple binding registrations at the HA. The second established tunnel

remains in status “standby” until it is switched to active mode when a Tunnel_Switch_Request message is received from the MR and validated by the HA.

Table 3. Home Agent Binding Cache

HoA	BID	CoA	Tunnel Status	Expire Time
HoA1	BID1	CoA1	active	-
HoA1	BID2	CoA2	standby	-

Note that new available paths (links or tunnels) for the MR are stored at the HPD level also in a cache called *AlternativePathCache* (Table 4).
Then if a Link_Switch_Imminent event is generated by IF-1, the HPD scans the *AlternativePathCache* to look for an available alternative path. Depending on “Handoff Type” field in *AlternativePathCache* , the HPD will request only link switching (MIH_Link_Switch) or both link switching and tunnel switching (request to NEMO).

Table 4. Mobile Router Alternative Paths Cache

Link ID	IF	Handoff Type	CoA	Status	Expire Time
Link #	IF2	Horizontal/Vertical	CoA2	ready	-

To allow NEMO to perform tunnel switching, we define two new NEMO signaling messages with MH Type = 9 (Tunnel_Switch_Request message, see Figure 14) and MH Type = 10 (Tunnel_Switch_Replay message, see Figure 15) in the Mobility Header of NEMO protocol [2].

Payload Proto	Header Len	MH Type = 9	Reserved
Checksum		Sequence ID	Time
HoA			
BID1 of active tunnel		BID2 of target tunnel	
IPv6 care-of address (CoA) of active tunnel			
IPv6 care-of address (CoA) of target tunnel			
options			

Figure 14. Packet Format of Tunnel_Switch_Request message

Payload Proto	Header Len	MH Type = 10	Reserved
Checksum		Sequence ID	Time
Replay Code			

Figure 15. Packet Format of Tunnel_Switch_Replay message

After a period time twice the time T_{LGD} from the time a Link_Going_Down event is generated, if neither a Link_Switch_Imminent event nor a Link_Down event is generated, the IF-2 is disconnected, the alternative path is deleted from *AlternativePathCache* and the tunnel is removed from the binding cache at the HA level.
In any case, if a Link_Down event is generated, the HPD takes the decision to switch to an alternative path if available, otherwise to Handoff to an alternative link if available, otherwise to scan for new access networks.

6. Simulation Results

The scenario illustrated in Figure 16 was simulated using the NS-2 simulator together with the NIST mobile package to verify and evaluate the extended NEMO model described previously. The network topology is constituted of six nodes using hierarchical addressing, a router (0.0.0), two access routers: the base station 802.11 AR1 (1.0.0) with coverage of 100 m and the base station 802.16 AR1 (2.0.0) with coverage of 1000 m, the mobile router MR (4.1.0) moving at speed 90 Km/h from AR1 cell to AR2 cell, the Home Agent HA (4.0.0) and the correspondent node CN (3.0.0). Link characteristics namely the bandwidth and the delay are shown are also shown on the figure. Simulation time is set to 60 s. A Constant Bit Rate (CBR) traffic stream with a packet size of 768 bytes at 0.016 second intervals is sent from CN to MR. A shadowing model was used for the 802.11 radio link with $\sigma = 4$, $\beta = 3$, a transmit power of 14 dBm and a predefined threshold power P_{th} equal to -75 dBm.

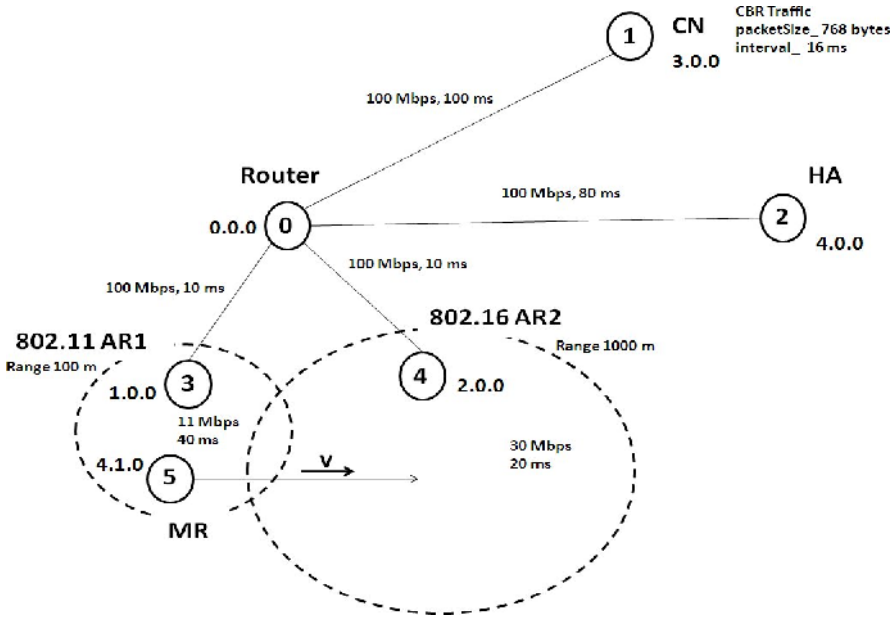

Figure 16. Simulated Network topology

First, we investigate appropriate value for δ for accurate estimation of received signal power. δ will largely depend on the amount of signal variation σ. Figure 17 shows the possible signal strength variations for different δ values for a shadowing model with $\sigma = 4$. The variation swing can be seen to be quite large without any averaging applied, while a value of δ= 0.1 stabilizes the estimation quite acceptably. It is important to obtain stability to reduce the probability of a ping pong effect. Note that when more averaging is applied (δ= 0.01) the system becomes less responsive to rapid changes.

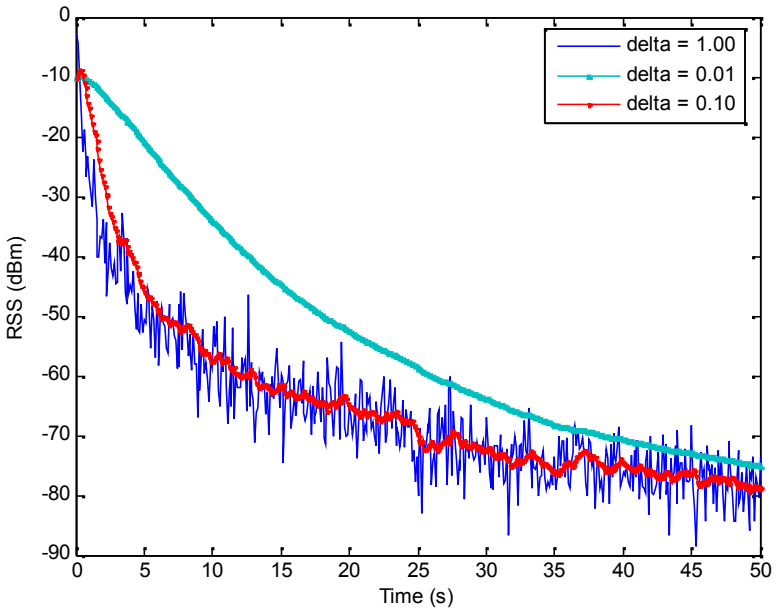

Figure 17. Average received signal strength (RSS) for δ values of 1, 0.01 and 0.10. ($\sigma = 4, \beta = 3, v = 90\ Km/h$)

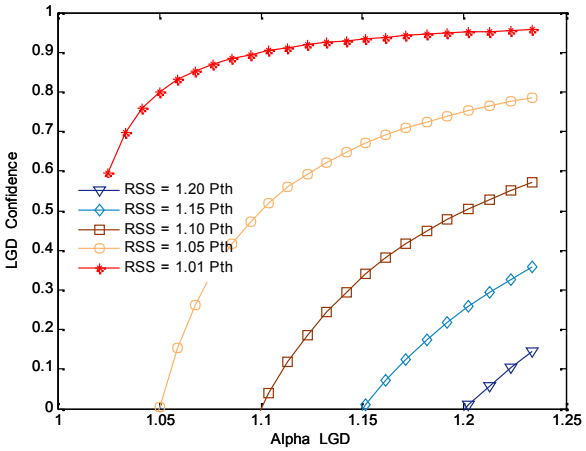

Figure 18. Confidence level for LD event when LGD event is triggered

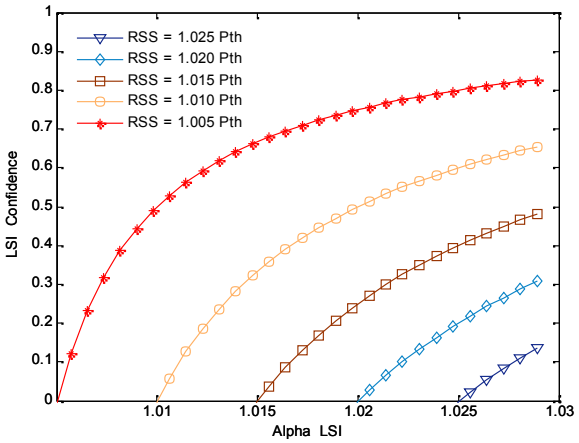

Figure 19. Confidence level for LD event when LSI event is triggered

In Figures 18 and 19 we present the confidence level for link to go down within the specified time interval for respectively LGD and LSI triggers. For a given RSS, the confidence level increases for both LGD and LSI triggers when the corresponding threshold factor increases.

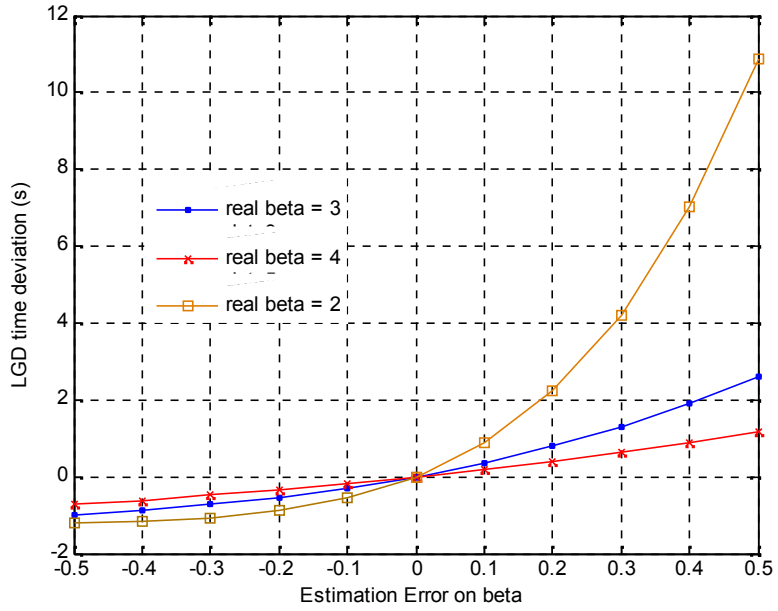

Figure 20. impact of β estimation error on T_{LGD}

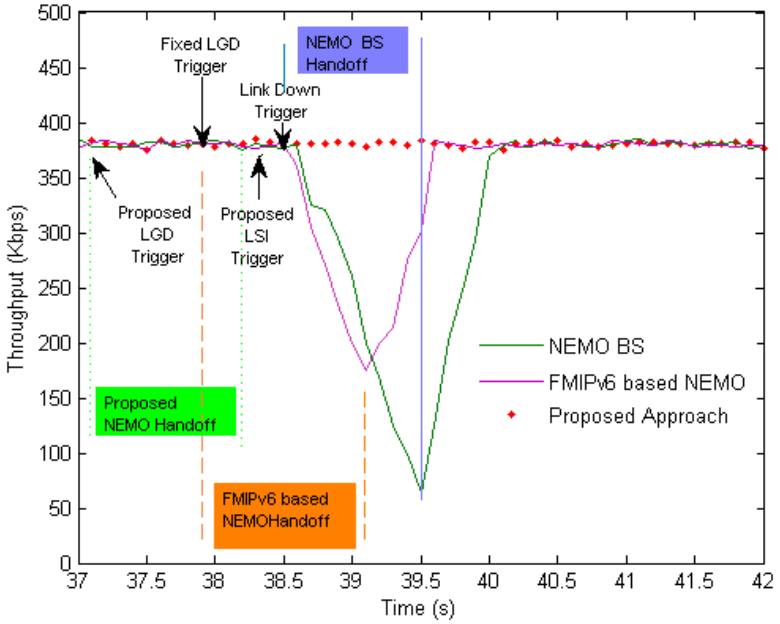

Figure 21. Throughput of received CBR Traffic

We also determined the impact of estimation error on the parameter model β on Setting LGD trigger Threshold. The results are shown in Figure 20 when the real path loss model involves a value of $\beta = 2, 3$ or 4. We notice that positive (negative) error leads to increasing (decreasing) in Handoff anticipation time.
Figure 21 shows the throughput of the CBR traffic at the MR level for the scenario presented in Figure 16. The model was used without β estimation error ($\Delta\beta$=0) and a value of δ= 0.1 for RSS estimation. The result is compared with MIPv6-NEMO (Handoff triggered by LD) and FMIPv6-NEMO (Handoff anticipation triggered by LGD with fixed $\alpha_{LGD} = 1.05$). The LD occurs at time 38.512 s. For FMIPv6-NEMO, the LGD event is triggered at 37.893 s. For our proposal, the LGD is triggered at 37.146 s and LSI is triggered at 38.396 s
While MIPv6-NEMO and FMIPv6-NEMO achieve both finite Handoff delay and finite packet loss, our proposal provides seamless connectivity with no Handoff latency and no packet loss.

7. CONCLUSIONS

In this paper, we have investigated the combination of multihoming and intelligent soft handoff to achieve seamless connectivity for real time and QoS-sensitive applications in the context of NEMO networks. We addressed the case of (1,1,1) multihomed NEMO model with the assistance of IEEE 802.21MIH services. The proposed Handoff mechanism must be executed before the Link_Down event of the current link. For this purpose, we used LGD trigger (fired using required NEMO Handoff time) for Handoff preparation and LSI trigger (fired using required tunnel switching time) for Handoff anticipation. Our contributions are the design of a new MIH user (HPD: Handoff Policy Decision) for intelligent soft Handoff decisions based on information gathered from surrounding networks, the definition of new MIH service to provide LSI trigger and the extension of the NEMO BS protocol to support tunnel switching when MCoA registration is used. The tests we performed show that our solution makes it possible to achieve a really seamless handover when the suitable model and parameters are chosen. Our proposed Handoff approach is infrastructure independent and can provide both no packet loss and no Handoff delay as well.

REFERENCES

[1] V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert, (2005), "Network Mobility (NEMO) Basic Support Protocol," Internet Engineering Task Force (IETF), RFC-3963.

[2] D. Johnson, C. Perkins, and J. Arkko, (2004) "Mobility Support in IPv6,"Internet Engineering Task Force (IETF), RFC-3775.

[3] H. Petander, E. Perera, K.C. Lan, A. Seneviratne, (2006). Measuring and improving the performance of network mobility management in ipv6 networks. IEEE Journal on Selected Areas in Communications, 24(9), pp 1671-1681.

[4] V.Vassiliou and Z. Zinonos, (2009) "An Analysis of the Handover Latency Components in Mobile IPv6," Journal of Internet Engineering, vol. 3(1), pp 230-240.

[5] Shayla Islam and al, (2011). Mobility Management Schemes in NEMO to Achieve Seamless Handoff: A Qualitative and Quantitative Analysis. Australian Journal of Basic and Applied Sciences, 5(6) pp 390-402.

[6] Moore N, (2005). Optimistic duplicate address detection for ipv6. IETF draf.

[7] Kempf J, Khalid M, Pentland B, (2004). Ipv6 fast router advertisement. IETF draft.

[8] Q.B Mussabbir, W. Yao, (2007). Optimized FMIPv6 using IEEE 802.21 MIH Services in Vehicular Networks. IEEE Transactions on Vehicular Technology. Special Issue on Vehicular Communications Networks.

[9] C-W Lee, Y-S. Sun and M-C Chen, (2008). HiMIP-NEMO: Combining Cross-layer Network Management and Resource Allocation for Fast QoS-Handovers. Proceedings of the 67th IEEE Vehicular Technology Conference, Singapore.

[10] Z. Yan, H. Zhou and I. You, ( ). N-NEMO: A Comprehensive Network Mobility Solution in Proxy Mobile IPv6 Network. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, vol. 1, No. 2/3, pp 52-70.

[11] H. Lin, H. Labiod, (2007). Hybrid handover optimization for multiple mobile routers-based multihomed NEMO networks, in: Proceedings of IEEE International Conference on Pervasive Service, Istanbul.

[12] P. K. Chowdhury, M. Atiquzzaman, and W. Ivancic, (2006). SINEMO: An IP-diversity based approach for network mobility in space,. Second International Conference on Space Mission Challenges for Information Technology (NASA SMC-IT), Pasadena, CA, pp 109-115.

[13] Z. Huang, Y. Yang, H. Hu and K. Lin, (2010). A fast handover scheme based on multiple mobile router cooperation for a train-based mobile network Int. J. Modelling, Identification and Control, Vol. 10, No. 3/4, pp 202-212.

[14] G. Jeney, L. Bokor and Z. Mihaly, (2009). GPS aided predictive handover management for multihomed NEMO configurations. 9th International Conference on Intelligent Transport Systems Telecommunications, pp 69 – 73.

[15] A. Mitra, B. Sardar and D. Saha, (2011). Efficient Management of Fast Handoff in Wireless Network Mobility (NEMO). Working paper series WPS No. 671.

[16] S. Pack, X. Shen, J. Mark and J. Pan, (2007). A comparative study of mobility management schemes for mobile hotspots. In Proceedings of IEEE WCNC, pp 3850–3854.

[17] S. Herborn, L. Haslett, R. Boreli, and A. Seneviratne, (2006). Harmony HIP mobile networks. In Proceedings of IEEE VTC 2006-Spring, vol. 2, pp 871–875.

[18] K. Zhu, D. Niyato, P. Wang, E. Hossain, and D. Kim, (2009). Mobility and Handoff Management in Vehicular Networks: A Survey. Wireless Communications and Mobile Computing, Wiley InterScience, pp 1-20.

[19] Y. Y. An, et.al, (2006), "Reduction of Handover Latency Using MIH Services in MIPv6", in Proc. of the 20th International Conference on Advanced Information Networking and Applications (AINA'06) – Vol.02, pp 229-234.

[20] R. Koodli, et al., (2008), "Mobile IPv6 Fast Handovers", RFC 5268, Internet Engineering Task Force.

[21] D-H Kwon, Y-S Kim, K-J Bae, and Y-J Suh, (2005), "Access Router Information Protocol with FMIPv6 for Efficient Handovers and Their Implementations", IEEE GLOBECOM 2005.

[22] Details for North Americ Internet Traffic Report. http://www.internettrafficreport.com/namerica.htm

[23] IEEE 802.21-2008, Media Independent Handover Services.

[24] S. Woon, N. Golmie, A. Sekercioglu (2006). Effective Link Triggers to Improve Handover Performance. Proceedings of 17th Annual IEEE Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC'06), Helsinki, Finland, pp 11-14.

[25] S. J. Yoo, D. Cypher, and N. Golmie, (2007), "LMS predictive link triggering for seamless handovers in heterogeneous wireless networks," in Proc. MILCOM, Orlando, FL, Oct. 28–30, pp 1–7.

[26] Theodore S. Rappaport (2002). Wireless Communication: Principles and Practice. Personal Education International.

[27] C. Ng, E. Paik, T. Ernst, and M. Bagnulo, (2007), "Analysis of Multihoming in Network Mobility Support," IETF, RFC 4980.

[28] R. Wakikawa, V. Devarapalli, G. Tsirsis and T. Ernst and K. Nagami, (2009), "Multiple Care-of Addresses Registration," IETF, RFC 5648.

Résumé

Dans cette thèse, nous proposons deux nouvelles approches de handover NEMO indépendantes de l'infrastructure, combinant le multihoming et le handover Make-Before-Break intelligent, assurant ainsi une connectivité sans couture avec zéro délai et zéro perte. Pour les deux solutions, nous nous basons sur l'appui des services MIH IEEE 802.21. Dans la première approche, nous proposons une nouvelle architecture d'un réseau NEMO multihomed avec plusieurs MRs domiciliés dans différents HAs. Cette architecture est basée sur l'introduction de la notion de routeur primaire et routeur secondaire, et l'intégration d'une nouvelle entité nommée MNPx (Mobile Network Proxy) au sein du réseau mobile, dont la tâche principale est la gestion intelligente de la mobilité et du trafic d'une manière transparente pour les MNNs. Dans la deuxième approche, nous avons adressé le cas du modèle NEMO multihomed (1.1.1) où un seul MR multi-interfaces est employé. Basé sur l'estimation du délai du handover requis, les handovers L2 et L3 sont lancés en utilisant des triggers MIH efficaces et opportuns, réduisant ainsi le temps d'anticipation et augmentant la probabilité de prédiction. Nous avons étendu les services de MIH pour fournir l'établissement et la commutation de tunnel avant la rupture du lien courant. Ainsi, le handover est exécuté dans le background sans latence et sans perte de paquet tandis que le scénario de ping-pong est évité, et le coût et la consommation d'énergie sont minimisés. Des expériences de simulation sous le simulateur de réseau NS2 ont été conduites pour identifier les valeurs appropriées des paramètres des modèles validant nos propositions.

Mots clés : *réseau mobile, NEMO, Multihoming, routeur mobile, Handover sans couture, IEEE 802.21, MIH triggers, modèle de propagation, NS2, PHD, MTM, MNPx*

Abstract

In this thesis, we propose two new Infrastructure independent NEMO handoff approaches combining multihoming and intelligent Make-Before-Break Handoff achieving seamless connectivity with no handoff latency and no handoff packet loss. For both solutions, we rely on the support of MIH IEEE 802.21 services. In the first approach, we propose a new architecture of a multihomed NEMO network with several MRs domiciled in different HAs. This architecture is based on the introduction of the concept of primary and secondary routers, and the integration of a new entity named MNPx (Mobile Network Proxy) within the mobile network, whose principal task is the intelligent management of mobility and traffic transparently for MNNs. In the second approach, we addressed the case of multihomed NEMO model (1,1,1) where a single multi-interfaces MR is used. Based on required Handoff time estimation, L2 and L3 handoffs are initiated using effective and timely MIH triggers, reducing so the anticipation time and increasing the probability of prediction. We extended MIH services to provide tunnel establishment and switching before link break. Thus, the handoff is performed in background with no latency and no packet loss while ping-pong scenario is almost avoided and cost and power consumption are saved. We provide implementation and simulation experiments under Network Simulator NS2 to identify appropriate model parameter values validating our proposals.

Keywords : *Network mobility, NEMO, Multihoming, Mobile Router, seamless handoff, IEEE 802.21, MIH triggers, path loss model, NS2, PHD, MTM, MNPx*

ملخص

نقترح في هذه الأطروحة منهاجين جديدين مستقلين عن البنية الأساسيّة لشبكة الأنترنيت في سياق للشبكة المتحركة (NEMO)، لتحقيق عدم انقطاع الاتصال مع عدم وجود كمون ولا خسارة في الهندوفر(handover). إعتمدنا في ذلك على قضية طرق الاتصال المتعددة (multihoming) و الهندوفر السلس (Make-Before-Break) بالإضافة إلى خدمات MIH IEEE 802.21. في المقاربة الأولى، إقترحنا هيكلية جديدة لشبكة NEMO بعدة MRs و عدة HAs. تستند هذه الهيكلية على إدخال مفهوم التوجيه الابتدائي والثانوي, والدمج بذاتية جديدة بإسم توكيل الشبكة المتحرّكة (MNPx) ضمن الشبكة المتحرّكة NEMO, بحيث تكون مهمتها الرئيسيّة الإدارة الذكيّة للتحركية و نقل البيانات بشكل شفاف بالنسبة للأجهزة المتنقلة داخل الشبكة المتحركة. في المقاربة الثانية، تناولنا النموذج (1,1,1) في شبكة NEMO حيث يتم استخدام MR واحد يحتوي على عدة وصلات للشبكة. إعتمادا على تقدير الوقت الضروري لعملية الهندوفر, يتم تشغيل الهندوفر L2 و L3 بإستخدام أزندة MIH بالشكل الفعال و في الوقت المناسب، و بهذه الطريقة يتم الحد من وقت التوقع وزيادة احتمال التنبؤ. مدّدنا خدمات MIH بحيث يتم إنشاء النفق والتبديل قبل انقطاع الرابط. هكذا, ينجز الهندوفر في خلفيّة بلا حالة كمون ولا ربط خسارة بينما يتم تفادي سيناريو ping-pong ويتم حفظ التكاليف واستهلاك الطاقة. نقدم في الأخير نتائج التجارب تحت NS2 لتحديد قيم المعالم المناسبة للنموذج للتحقق من صحة مقترحاتنا.

الكلمات المفاتيح : الشبكة المتحركة، طرق الاتصال المتعددة، الهندوفر, *PHD, IEEE 802.21, NEMO,multihoming, MTM, NS2, MNPx,*