Optimisation du Handover dans le protocole IPv6 mobile avec la méthode E-HCF

Guozhi Wei

THESE
PRESENTEE EN VUE D'OBTENIR
LE GRADE DE DOCTEUR DE L'UNIVERSITE PARIS XII

SPECIALITE : SCIENCES INFORMATIQUES

PAR
GUOZHI WEI

OPTIMISATION DU HANDOVER DANS LE PROTOCOLE IPV6 MOBILE AVEC LA METHODE E-HCF

Soutenu publiquement le date 2007 devant le jury composé de :

Directeur de thèse :	Gérard DUPEYRAT Professeur à l'Université de PARIS XII - Val de Marne
Co-directrice de thèse :	Anne WEI Maître de Conférences et HDR à l'Université de PARIS XII - Val de Marne
Rapporteur :	Jean-Louis DEWEZ Professeur au Conservatoire National des Arts et Métiers
Rapporteur :	Houda LABIOD, Enseignant-chercheur et HDR à l'Ecole Nationale Supérieure des Télécommunication
Examinateurs :	Benoît GELLER Enseignant-chercheur et HDR à l'Ecole Nationale Supérieure de Techniques Avancées
Examinateur :	Éric GRESSIER-SOUDAN Professeur au Conservatoire National des Arts et Métiers

Résumé

Les réseaux sans fil sont en plein développement du fait de la flexibilité de leur interface, qui permet aux utilisateurs de se communiquer directement entre eux ou de se connecter facilement à Internet en onde radio sans mettre en place préalablement d'infrastructures lourdes, telles que des câbles filaires. Parmi les différentes technologies de réseaux sans fil, l'IEEE 802.11/Wi-Fi est devenu une technologie plus connue et plus utilisée pour construire des réseaux sans fil à haut débit dans une zone à forte concentration d'utilisateurs, telle que les aéroports, les campus ou les sites industriels. L'engouement pour les réseaux sans fil et notamment pour les réseaux Wi-Fi a fait émerger de nouvelles nécessités, tel que se déplace dans les réseaux sans fil tout en restant connecté à Internet.

Dans les réseaux sans fil, le déplacement d'un utilisateur implique parfois un changement de Point d'accès (AP) au réseau. On désigne généralement ce fait un handover de niveau 2, du fait que le changement d'AP n'implique que les deux premières couches du modèle OSI. Si les deux APs se situent dans des réseaux différents, le changement d'AP implique aussi le changement de réseau pour cet utilisateur. On dénomme généralement cette situation un handover de niveau 3, par le fait que cet utilisateur devrait changer son réseau d'attachement et son adresse IP pour maintenir la connexion à Internet et que ce changement intervient sur la couche réseau du model OSI.

La procédure du handover de niveau 2 dans les réseaux Wi-Fi est gérée par la norme IEEE 802.11 et celle de niveau 3 est gérée par le protocole IP Mobile. Le protocole IP Mobile est un protocole standardisé par l'IETF qui permet à l'utilisateur de maintenir ses communications en cours et de rester connecté à Internet tout en masquant d'une manière transparente le changement de réseau. Ainsi, l'utilisateur peut se déplace dans les réseaux Wi-Fi tout en maintenant les communications en cours et restant connecté à Internet grâce à la norme IEEE 802.11 et au protocole IP Mobile. Cependant, le délai introduit par ces deux procédures du handover est trop long, les communications en cours sont interrompus pendant ces procédures, naturellement, cela ne peut pas répondre aux exigences qualitatives des applications temps réel comme la vidéo conférence ou la voix sur IP.

Diverses propositions qui ont été faites pour réduire le délai de ces procédures du handover et améliorer leur performance. Cependant, ces propositions sont soit imparfaites, soit non-implémentables à cause de leur complexité.

En partant du principe que les réseaux Wi-Fi et les routeurs d'accès sont déjà massivement implantés dans le monde universitaire et dans les entreprises, nous proposons d'ajouter une nouvelle fonctionnalité, appelé E-HCF (Extended Handover Control Function) dans un routeur sans modifier les autres équipements du réseau. Le routeur pourvu de cette fonctionnalité est dénommé le routeur E-HCF. Pour réduire le délai des procédures du handover, la fonctionnalité E-HCF permet au routeur de générer une topologie des APs en utilisant la théorie des graphes de voisinage et de maintenir un pool d'adresses IP disponibles dans sa base de données. Quand le Nœud mobile (MN) a besoin de changer son AP, le routeur E-HCF peut proposer au MN une liste des APs potentiellement utilisables qui sont choisis et classés par un algorithme de sélection et de classement que nous avons élaboré dans la thèse. Si le changement d'AP implique un changement de

réseau, le MN doit changer d'adresse IP. Dans ce cas, le routeur E-HCF peut attribuer une adresse IP unique à ce MN. Le MN peut donc utiliser cette adresse sans exécuter la phase d'Auto-configuration d'adresses ni exécuter la procédure de Détection d'adresse dupliquée. Avec cette nouvelle fonctionnalité E-HCF, nous pouvons réduire le délai des procédures du handover de quelques secondes à une centaine de millisecondes.

Pour réduire la perte de paquets due aux procédures du handover, nous proposons de modifier le protocole IPv6 Mobile. Le MN met fin à l'association entre son adresse mère et son adresse temporaire avec l'Agent mère (HA) et le Nœud correspondant (CN) avant de procéder la procédure du handover. Par ce moyen, le HA peut intercepter les paquets destinés à l'adresse mère du MN et les garder dans son mémoire tampon. Une fois le MN met à jour l'association entre son adresse mère et sa nouvelle adresse temporaire avec le HA, le HA peut envoyer les paquets stockés dans son mémoire de tampon au MN. Il intercepte et redirige également les paquets du CN ou du MN vers la nouvelle adresse temporaire du MN ou vers les adresses du CN respectivement pendant la phase de mise à jour d'association. Avec cette méthode, nous pouvons limiter la perte de paquets et garantir un délai acceptable.

Pour étayer notre proposition, nous avons utilisé le simulateur OPNET pour simuler le déroulement des procédures du handover dans les réseaux Wi-Fi géré par la méthode E-HCF et celui géré par le protocole IPv6 Mobile. Les résultats obtenus montrent qu'avec notre méthode E-HCF, nous pouvons garantir un délai acceptable et limiter la perte des paquets.

Ensuite, nous avons également validé notre méthode E-HCF avec la norme IEEE 802.11e qui supporte la Qualité de Service (QoS). Avec le support de QoS, les résultats obtenus par simulation illustrent les améliorations des performances significatives pour les communications de bout en bout dans les réseaux chargés.

Nos travaux de recherche ont donné lieu à trois publications dans les conférences internationales et un article dans la revue internationale (Voir Index).

Mots Clés

IEEE 802.11/Wi-Fi, IPv6, IPv6 Mobile, Handover, Méthode E-HCF, QoS

Abstract

Wireless networks are in full development because of the flexibility of their interfaces, which allow users to be easily connected to the Internet. Among various technologies of wireless networks, IEEE 802.11/Wi-Fi technology is becoming better known and more used to construct high speed wireless networks in areas with high concentration of users, such as airports, campuses or industrial sites. The passion for wireless networks and in particular for Wi-Fi networks has given rise to new uses of the Internet, such as moving in wireless networks while still being connected.

In Wi-Fi networks, the user's movement may sometimes lead to a change of Access Points (APs) to the network. This fact is generally named the handover of layer 2 because this change involves only the first two layers of the OSI model. If the two APs are located in different networks, the change of AP would entail a change of network for the user. This situation is generally termed, the handover of layer 3 because the user should change his network and his IP address to maintain connection to the Internet. Therefore, this change intervenes on the network layer of the OSI model.

The process of the handover of layer 2 is handled by the IEEE 802.11 standard and that of layer 3 is controlled by the Mobile IP protocol. The Mobile IP protocol is a protocol standardized by IETF, which allows users to change network, while maintaining their actual connection to the Internet. Consequently, users can connect to the Internet, while keep moving in Wi-Fi networks in control of the IEEE 802.11 standard and the Mobile IP protocol. However, the delay induced by these procedures of handover is too long. As such, this generally leads to the cut-off of current communications, hence impacting adversely on the qualitative requirements of real-time applications, such as video conferencing or voice over IP.

Various proposals have been made to reduce the delay of handover procedures and to improve their performances. However, these proposals are either imperfect, or non-implementable because of their complexity.

Based on the premise that Wi-Fi networks and access routers are already massively implanted in academia and in industry, we propose to add a new functionality, called E-HCF (Extended Handover Control Function) in routers, without modifying other network equipments. A router equipped with this functionality is called an E-HCF router. To reduce the delay of handover procedures, the E-HCF functionality allows a router to generate a topology of APs by using the neighbourhood graph theory and to maintain a pool of available IP addresses in its database. When a Mobile Node (MN) needs to change its AP, the E-HCF router may propose to the latter a list of potentially usable APs, which are selected and classified by an algorithm of selection and classification that we developed in the thesis. If the change of APs involves a change of network, the MN must change its IP address. In this case, the E-HCF router can assign a unique IP address to this MN. The MN can thus use this address without engaging in the process of Stateless Address Autoconfiguration or the procedure of Duplicate Address Detection. With this new E-HCF functionality, we can reduce the delay of handover procedures from a few seconds to one hundred milliseconds.

To reduce packet loss, incurred due to handover procedures, we propose to modify the Mobile IPv6 protocol. In general, the MN terminates the binding between its home address and its care-of address with its Home Agent (HA) and its Correspondent Node (CN) before proceeding with the handover procedures. Consequently, we can use the HA to intercept and redirect the packets of the CN or the MN respectively to the new care-of address of the MN or to the addresses of the CN during the complete binding process. With this method, we can limit packet loss and guarantee an acceptable delay.

To support our proposal, we used the OPNET simulator to simulate the handover procedures in Wi-Fi networks as defined by the E-HCF method and by the Mobile IPv6 protocol. The results obtained show that we can guarantee an acceptable delay and limit packet loss with our E-HCF method.

We also validated our method with the standard IEEE 802.11e that supports Quality of Service (QoS). With the support of QoS, the simulation results demonstrate significant performance improvements for end-to-end communications in the loaded networks.

Our research has resulted in three publications in international conferences and an article in an international journal (see index).

Keywords

IEEE 802.11/Wi-Fi, IPv6, Mobile IPv6, Handover, E-HCF Function, QoS

Remerciements

Je tiens tout d'abord à remercier Monsieur Gérard DUPEYRAT, Professeur à l'Université de Paris XII - Val de Marne, mon directeur de thèse, pour son encadrement, ses nombreux conseils et son soutien. J'adresse aussi mes remerciements à Madame Anne WEI, Maître de Conférences et HDR à l'Université de Paris XII - Val de Marne, ma co-directrice de thèse. Les conseils, la motivation et la confiance qu'elle m'a prodigués me furent très précieux pour mener à bien cette thèse.

Je remercie très sincèrement Monsieur Jean-Louis DEWEZ, Professeur au Conservatoire National des Arts et Métiers (CNAM) et Madame Houda LABIOD, Enseignant-chercheur et HDR à l'Ecole Nationale Supérieure des Télécommunications Paris (ENST Paris) pour avoir accepté d'évaluer ce travail en assurant la tâche de rapporteur.

J'exprime ma profonde reconnaissance à Monsieur Benoît GELLER, Enseignant-chercheur et HDR à l'Ecole Nationale Supérieure de Techniques Avancées (ENSTA) et à Monsieur Éric GRESSIER-SOUDAN, Professeur au Conservatoire National des Arts et Métiers (CNAM) pour leur participation à mon jury de thèse. Un remerciement particulier au dernier, qui m'a offert une condition de travail très agréable, a corrigé l'intégrité de cette thèse et m'a donné les commentaires précieux.

Je tiens à remercier Madame Marie-Christine COSTA, Professeur et Directrice du laboratoire Cédric du CNAM, et Monsieur Stéphane NATKIN, Professeur et Responsable d'équipe RSM du laboratoire Cédric du CNAM pour m'avoir accueilli au Cédric et fournir les moyens de préparer ma thèse pendant les deux dernières années.

J'exprime ma plus sincère reconnaissance à Olivier BOURSIN, Amelie LAMBERT, Laurent DEHOEY, Patrice KRZANIK, Jean-Paul ETIENNE, Julien CORDRY, Jose PLUQUET, Jean-Frédéric ETIENNE, Fouad KEYRILLOS, Leila HARFOUCHE, Didier EREPMOC pour les corrections de la thèse, les conseils, les discussions, les joies partagées. Je suis reconnaissant à Monsieur Joël BERTHELIN, Madame Safia SIDER, Madame Viviane GAL pour des aides et des soutiens qu'ils m'ont apportés.

Finalement, je dois remercier ma famille. Merci pour vos encouragements et votre soutien pendant ces dernières années plus difficiles dans ma vie.

À mes parents

You've got to find what you love.

— Steve JOBS

Table des matières

Introduction

Les réseaux sans fil sont en plein développement du fait de la flexibilité de leur interface qui permet aux utilisateurs de se communiquer directement entre eux ou de se connecter facilement à Internet en onde radio, sans mettre en place préalablement d'infrastructures lourdes, telles que des câbles filaires. Ces différents technologies de réseaux sans fil ont une portée de quelques mètres à une centaine kilomètres et atteignent des débits de plusieurs kilobits par seconde à plusieurs centaines de mégabits par seconde. Plusieurs gammes de technologies sont actuellement commercialisées, tels que l'IEEE 802.15/Bluetooth pour les petits réseaux personnels avec une dizaine de mètres de portée et un débit de 723,2Kbits/s, l'IEEE 802.11/Wi-Fi pour les réseaux local avec plusieurs centaines de mètres de portée et un débit allant jusqu'à 54Mbits/s, l'IEEE 802.16/WiMax pour les réseaux métropolitains avec plus de dix kilomètres et un débits de 74 Mbits/s, et l'IEEE 802.22/WRAN pour les réseaux régionaux avec un débit de 18Mbits/s.

Parmi ces différentes technologies de réseaux sans fil, l'IEEE 802.11/Wi-Fi est la plus connue et la plus utilisée pour construire un réseau sans fil à haut débit dans une zone à forte concentration d'utilisateurs, telle que les aéroports, les gares, les campus ou le site industriel. Le succès de Wi-Fi est non seulement dû à ses performances, mais aussi au coût des matériels plus acceptable et à son implantation simple et rapide. Naturellement, les utilisateurs qui se servent de réseaux Wi-Fi souhaitent pouvoir se déplace dans les réseaux tout en restant connecté à Internet.

Dans les réseaux Wi-Fi, le déplacement d'utilisateur implique parfois un changement de Point d'accès (AP). On désigne généralement ce fait un handover de niveau 2, du fait que ce changement n'implique que les deux premières couches du modèle OSI. Si les deux APs se situent dans des réseaux différents, le changement d'AP implique ainsi le changement de réseau pour cet utilisateur. On dénomme généralement cette situation un handover de niveau 3, par le fait que cet utilisateur devrait changer son réseau d'attachement et son adresse IP pour maintenir la connexion à Internet et que ce changement intervient sur la couche réseau du model OSI. La gestion du handover de niveau 3 est beaucoup plus compliqué que la gestion du handover de niveau 2, parce que l'utilisateur doit changer son adresse IP pour maintenir la connexion à Internet, cependant, s'il change son adresse IP, les communications en cours avec ses correspondants ne peuvent plus être maintenues du fait du changement d'adresse IP.

En effet, le protocole IP identifie un nœud sur Internet d'une manière unique grâce à son adresse IP. L'adresse IP se compose de deux parties : le préfixe qui détermine le réseau sur lequel le nœud se trouve et l'identifiant du nœud sur son réseau. Comme Internet est un réseau à grande échelle, c'est pourquoi chaque routeur ne peut mémoriser qu'une route vers tous les nœuds qui y sont attachés directement. Les tables de routage agrègent dans une même entrée l'adresse d'un réseau qui regroupe un ensemble de réseaux partageant un préfixe commun

suivant le principe d'un routage hiérarchique confondue aux principes de CIDR (Classless Inter-Domain Routing). Pour un Nœud Mobile (*en anglais Mobile Node – MN*) qui change de réseaux d'attachement, s'il ne change pas son adresse IP, il ne pourra pas recevoir les paquets qui lui sont destinés. Pour qu'un MN puisse changer de réseaux et garder la communication, il doit changer d'adresse IP à chaque fois qu'il change de réseaux. Mais une fois que le MN change son adresse IP, il ne peut pas conserver ses connexions au niveau de la couche transport et perturber donc ses applications.

Pour que le MN puisse maintenir les communications en cours tout en se déplaçant d'un réseau vers l'autre, le protocole IPv6 Mobile propose de gérer la mobilité du MN au niveau IP. Il permet ainsi au MN d'utiliser deux adresses IP et un mécanisme de Mise à jour d'association (*en anglais Binding Update*) pour masquer le changement d'adresse concernant les applications utilisées entre le MN et ses correspondants. Par conséquent, les communications en cours sont maintenues.

Bien que le protocole IPv6 Mobile résolve le problème de mobilité dans IPv6, ce protocole ne peut pas supporter les applications en temps réel qui sont sensibles au délai ou à la perte de paquets. C'est parce que la procédure du handover gérée par le protocole IPv6 Mobile peut souvent prendre plusieurs secondes quand un MN se déplace entre les réseaux. Cette latence signifie que quand le MN est déconnecté d'un réseau, il perd la communication avec son Nœud Correspondant (*en anglais Correspondant Node – CN*) jusqu'à ce qu'il réussit à se connecter avec succès à un autre réseau et pouvoir communiquer avec son CN. Pendant ces moments, les paquets destinés au MN seront perdus, étant donné que le MN est inaccessible et que le MN ne peut envoyer aucun paquet.

Ainsi, les travaux présentés dans cette thèse ont pour objectif d'améliorer la performance du handover dans les réseaux sans fil. Le handover considéré ici est non seulement le handover de niveau 2, mais aussi le handover de niveau 3. Après l'étude des problématiques du handover, de la norme IEEE 802.11, du protocole IP Mobile et des différentes propositions, nous proposons une méthode E-HCF. En s'appuyant sur cette méthode, nous pouvons garantir un délai acceptable et limiter la perte de paquets due au handover. Nous obtenons ainsi une amélioration significative de la performance du handover dans les réseaux Wi-Fi. Nous pouvons aussi appliquer notre méthode E-HCF dans les autres types de réseaux sans fil, tel que WiMax.

Le chapitre 1 présente les différents types de réseaux sans fil. Une grande partie est consacrée à la présentation des réseaux IEEE 802.11/Wi-Fi et particulièrement à l'explication de la procédure du handover de niveau 2 gérée par la norme IEEE 802.11/Wi-Fi dans ce réseau. Les différentes propositions qui visent à améliorer la procédure du handover dans le réseau Wi-Fi sont aussi citées.

Le chapitre 2 présente les protocoles IPv4 et IPv6, ainsi que les protocoles IPv4 Mobile et IPv6 Mobile. Nous détaillons dans ce chapitre le mécanisme d'Auto-configuration d'adresses proposé par le protocole IPv6. Le protocole IPv6 Mobile utilise l'auto-configuration d'adresses sans état pour permettre au MN d'avoir une nouvelle adresse sur le nouveau réseau. Nous décrivons ainsi en détail la procédure du handover de niveau 3 gérée par le protocole IPv6 Mobile, telle que la Détection de mouvement, la Mise à jour d'association, etc. Pour améliorer la performance de la procédure du handover, de

nombreuses propositions ont été faites, parmi lesquelles, le Fast handover pour IPv6 Mobile (FMIPv6) et le IPv6 Mobile Hiérarchique (HMIPv6) sont plus connus. Mais le protocole FMIPv6 se concentre seulement sur l'exécution du protocole, il n'a pas proposé comment découvrir les APs du réseau Wi-Fi et les routeurs d'accès potentiellement utilisables. Le protocole HMIPv6 n'a pas proposé une solution pour réduire le temps de la détection de mouvement et le temps d'auto-configuration d'adresses.

Nous proposons une méthode E-HCF dans le chapitre 3. Nous voulons apporter le minimum de changement pour les infrastructures existantes. Nous ajoutons simplement une nouvelle fonctionnalité E-HCF dans le routeur de réseaux, sans modifier les routeurs d'accès, et les APs. Le routeur qui est équipé de la fonctionnalité E-HCF peut générer une topologie des APs en utilisant la théorie des graphes de voisinage et de maintenir un pool d'adresses IP disponibles. Quand le MN a besoin de changer son AP, le routeur pourvu de cette fonctionnalité peut proposer au MN une liste d'APs potentiellement utilisables qui sont choisis et classés par un algorithme de sélection et de classement que nous avons élaboré dans la thèse. Le routeur E-HCF peut aussi attribuer une adresse IP unique au MN si le changement d'AP implique un changement de réseau. Avec cette nouvelle fonctionnalité, nous pouvons réduire le délai des procédures du handover de quelques secondes à une centaine de millisecondes. Pour réduire la perte de paquets due aux procédures du handover, nous proposons de modifier le protocole IPv6 Mobile. Le MN met fin à l'association entre son adresse mère et son adresse temporaire avec l'Agent mère (HA) et le Nœud correspondant (CN) avant de procéder la procédure du handover. Par ce moyen, le HA peut intercepter les paquets destinés à l'adresse mère du MN et les garder dans son mémoire tampon. Une fois le MN met à jour l'association entre son adresse mère et sa nouvelle adresse temporaire avec le HA, le HA peut envoyer les paquets stockés dans son mémoire tampon au MN. Il intercepte et redirige également les paquets du CN ou du MN vers la nouvelle adresse temporaire du MN ou vers les adresses du CN respectivement pendant la phase de mise à jour d'association. Avec cette méthode, nous pouvons limiter la perte de paquets et garantir un délai acceptable.

Le chapitre 4 présente nos simulations. Nous utilisons OPNET pour simuler et appuyer notre proposition. Nous utilisons trois différents types d'applications pour simuler les comportements des utilisateurs qui se déplacent dans les réseaux Wi-Fi.

Dans le dernier chapitre, nous proposons d'ajouter le contrôle de la qualité de service dans le handover de réseaux et d'observer une amélioration des performances significatives.

Cette thèse se termine par une conclusion sur ce travail, suivi des perspectives. Nos travaux de recherche apportent trois publications dans les conférences internationales et un article dans une revue internationale.

1 Réseaux sans fil

Un réseau sans fil est un type de réseau qui permet des communications via les ondes radioélectriques et se substitue aux habituels câbles. A cette fin, des bornes sont installées pour délimiter une zone de couverture. Les utilisateurs peuvent en profiter à condition de disposer d'un adaptateur pour émettre et recevoir des données sur ce réseau. Cet adaptateur peut prendre la forme d'un boîtier, d'une carte PCI ou encore, pour les ordinateurs portables, d'une carte au format PCMCIA. Comme les réseaux sans fil permettent à des utilisateurs de communiquer sans mettre en place d'infrastructures lourdes, telles que des réseaux filaires, ils répondent bien à la demande des utilisateurs qui veulent se connecter facilement à Internet à n'importe quel endroit. Ces dernières années, grâce aux avancées de l'électronique, du traitement du signal, et de coût d'utilisation plus abordable, les réseaux sans fil se développent très rapidement et représentent un marché énorme.

Parmi différentes technologies de réseaux sans fil, IEEE 802.11/Wi-Fi [802.11] [PEYR05] permettent de relier des ordinateurs portables, des ordinateurs de bureau, des assistants personnels (*en anglais Personal Digital Assistant – PDA*) ou tout type de périphérique à une liaison haut débit (54Mbit/s ou supérieur) sur un rayon théorique de plusieurs dizaines de mètres en espace clos à plusieurs centaines de mètres en environnement ouvert. Ainsi, IEEE 802.11/Wi-Fi devient une technologie plus connue et plus utilisée pour construire un réseau sans fil à haut débit dans une zone à forte concentration d'utilisateurs, telle que les aéroports, les gares, les campus ou les sites industriels.

Dans ce chapitre, nous commencerons par décrire les différentes technologies de réseaux sans fil. Pour la raison que notre recherche se concentre sur l'amélioration des performances des procédures du handover dans les réseaux Wi-Fi, nous détaillerons par la suite la norme IEEE 802.11/Wi-Fi, particulièrement la procédure du handover gérée par cette norme.

1.1 Différents Types de réseaux sans fil

Plusieurs technologies de réseaux sans fil existent, les caractéristiques principales des différentes technologies sont la fréquence d'émission utilisée, la modulation, la puissance et la sensibilité du signal radio, le débit et la portée du réseau. Pour l'instant, les principales technologies des réseaux sans fil sont : IEEE 802.15.1/Bluetooth, IEEE 802.15.3/UWB, IEEE 802.11/Wi-Fi, et IEEE 802.16/WiMax. Puisque les différents organismes de normalisation et les différents constructeurs tentent chacun d'imposer leur technique, ces différentes technologies ne sont pas compatibles entre elles. Leurs débits de transmission vont de 1Mbit/s (Bluetooth) à 480 Mbit/s (UWB).

Nous pouvons classer ces réseaux en fonction de leurs portées, comme le montre la figure 1.

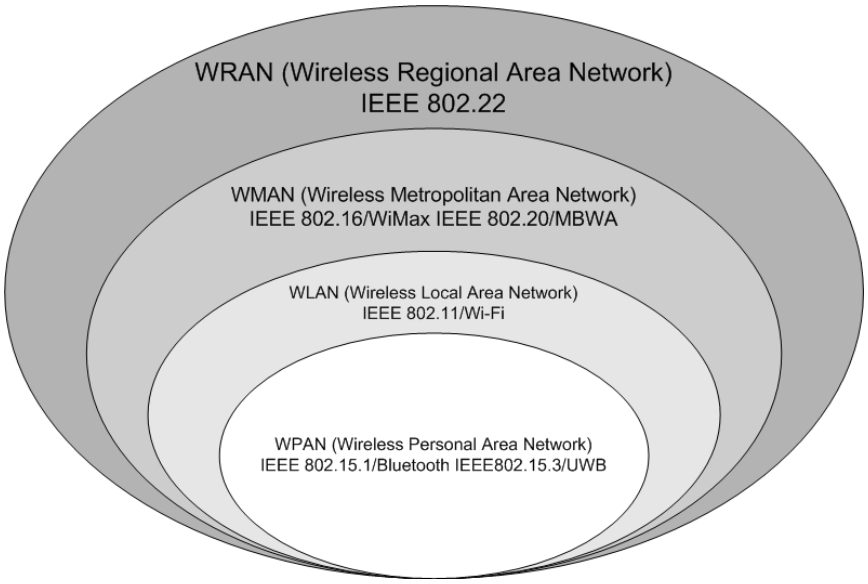


Figure 1: Catégories de Réseaux sans fil

1.1.1 Réseau Personnel sans fil – WPAN (Wireless Personal Area Network)

Ce sont des réseaux avec une portée d'une dizaine de mètres. Un réseau personnel sans fil est principalement constitué d'équipements, comme des ordinateurs portables, des imprimantes, des appareils numériques, des téléphones portables ou des PDAs, appartenant à un même utilisateur et distants de quelques mètres. Ce type de réseaux réalise des connexions entre les équipements. Les principales normes sont IEEE802.15.1/Bluetooth et IEEE 802.15.3/UWB(Ultra-Wide Band).

IEEE 802.15. 1/Bluetooth

Lancée par Ericsson en 1994, IEEE 802.15.1/Bluetooth [802.15.1] [B04] a été conçue avant tout pour permettre la réalisation de petits réseaux personnels de quelques mètres entre les appareils numériques (PDA, téléphone, appareil photo, portable...). Elle utilise une technologie radio courte distance destinée à simplifier les connexions entre les appareils numériques. Les fréquences utilisées sont comprises entre 2400 et 2483,5MHz. Cette bande de fréquence ne demande pas de licence d'exploitation. La puissance de transmission du Bluetooth peut atteindre 100mW, ce qui permet une émission sur plusieurs dizaines de mètres. Il est possible de réduire cette puissance entre 1 et 2,5 mW pour atteindre une portée de quelques mètres.

Pour la réalisation des connexions entre les terminaux dans ce petit réseau, une appellation, Piconet, a été définie par les normalisateurs, un Piconet est un mini réseau qui se crée de manière instantanée et automatique quand plusieurs terminaux Bluetooth sont dans un même rayon, un terminal fonctionne comme un maître, et les autres fonctionnent comme les esclaves. Le terminal maître gère les communications avec les différents esclaves. La communication entre deux terminaux esclaves transite obligatoirement par le terminal

maître. Le réseau Piconet peut prendre en charge jusqu'à 7 terminaux esclaves actifs et 255 terminaux esclaves en mode inactifs [CAPONE01].

Les périphériques esclaves peuvent avoir plusieurs maîtres, les différents Piconet peuvent donc être reliés entre eux. Le réseau ainsi formé est appelé un Scatternet (littéralement réseau chaîné).

La figure 2 présente le schéma de connexion de terminaux Bluetooth.

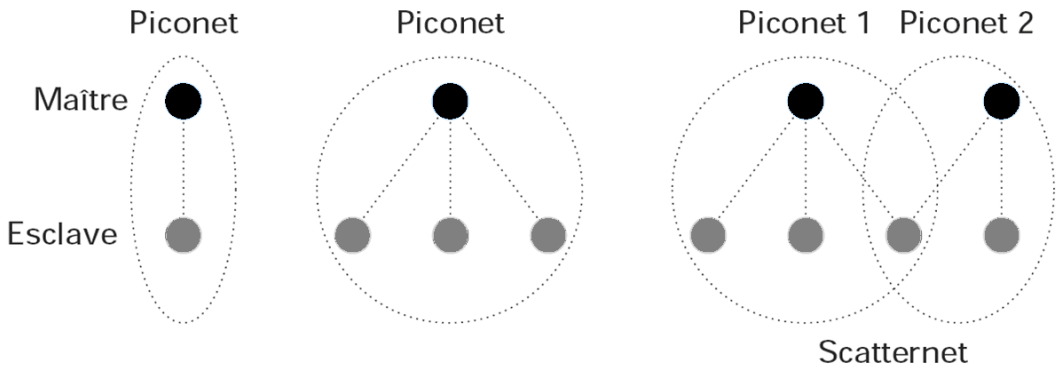


Figure 2 : Schéma de connexion de terminaux Bluetooth

Les communications sur une liaison Bluetooth entre deux terminaux peuvent être de deux types : asynchrone ou synchrone. Une communication synchrone permet un débit synchrone de 64 Kbit/s, une communication asynchrone peut atteindre un débit de 723,2 Kbit/s.

802.15.3/UWB (Ultra-Wide Band)

IEEE802.15.3/UWB [802.15.3] [PH03] a pour objet de réaliser un environnement sans fil à très haut débit pour un réseau personnel. Il est utilisé en particulier pour la mise en œuvre d'un port similaire à un USB sans fil en offrant des débits de 480Mbit/s.

IEEE802.15.3/UWB utilise une technique de modulation radio qui est basée sur la transmission d'impulsions de très courtes durées, souvent inférieures à la nanoseconde. Ainsi, la bande passante atteint de très grandes valeurs. UWB utilise des modulations de signaux en position d'impulsions avec deux modes : en modulation temporelle, en modulation biphasée. Il peut utiliser la bande classique des 2,4Ghz pour atteindre une vitesse de 54Mbit/s où il peut utiliser l'ensemble de la bande passante entre 3,1 et 10,7 GHz, mais à une puissance très faible. En dépit de la très faible puissance utilisée, la bande passante de plus de 7 GHz permet d'obtenir un débit situé entre 110Mbit et 480Mbit/s en fonction des perturbations externes. La topologie du réseau UWB est en tout point similaire à celle des réseaux Bluetooth, avec des Piconets et des Scatternets.

1.1.2 Réseau Local sans fil – WLAN (Wireless Local Area Network)

Ce sont des réseaux avec une portée d'une centaine de mètres. La principale norme est IEEE802.11/Wi-Fi. L'IEEE 802.11/Wi-Fi sera présenté dans la section suivante.

IEEE802.11/Wi-Fi (Wireless-Fidelity)

IEEE 802.11/Wi-Fi est aujourd'hui promu par l'alliance WECA (Wireless Ethernet Compatibility Alliance). La norme IEEE802.11/Wi-Fi sera détaillée dans le paragraphe 1.2.

1.1.3 Réseau Métropolitain sans fil – WMAN (Wireless Metropolitan Area Network)

Ce sont des réseaux avec une portée de 2 à 50 kilomètres, l'envergure d'une ville. Cette technologie est destinée principalement aux opérateurs de télécommunication. Les principales normes sont IEEE802.16/WiMax et IEEE 802.20/MBWA.

IEEE 802.16/WiMax (World Interoperability for Microwave Access)

IEEE 802.16/WiMax [MW06] [Wi05] est avant tout une famille de normes, définissant les connexions à haut débit par voie hertzienne. WiMax est également un nom commercial pour ces normes, comme l'est Wi-Fi pour 802.11 (la Wi-Fi Alliance est en cela comparable au WiMax Forum).

WiMax décrit des technologies hertziennes destinées principalement à des architectures point-multipoint : à partir d'une antenne centrale, plusieurs répéteurs propagent les signaux vers des terminaux pour leur donner un accès. La connexion avec les terminaux s'effectue en deux temps en passant par un répéteur, il est toutefois possible d'avoir une liaison directe entre les terminaux et l'antenne centrale. Les réseaux basés sur la technologie IEEE 802.16 ont une portée de l'ordre de quelques dizaines de kilomètres.

Le but premier du WiMax était de permettre la création de réseaux métropolitains fixes à très hauts débit. La norme 802.16e, publiée le 24 Juin 2004, utilise une fréquence entre 2 et 6 GHz et offre un taux de transmission théorique pouvant atteindre 74 Mbit/s. Elle apporte aussi un certain niveau de mobilité au WiMax : Les utilisateurs peuvent se déplacer jusqu'à 60km/h en conservant un débit de 15 Mbit/s.

IEEE 802.20/MBWA (Mobile Broadband Wireless Access)

IEEE 802.20/MBWA [FL05] est un standard en cours de développement permettant plus de mobilité que le WiMax et plus de débit que l'UMTS. Cette technologie utilise des fréquences inférieures à 3,5 GHz avec une cellule d'un rayon de 2,5Km et peut offrir 1 Mbits/s par utilisateur. Des versions utilisant un canal plus large de 5 MHz pourraient permettre des débits de 4 Mbit/s en descente et 1,2 Mbit/s en montée pour chaque utilisateur.

Le MBWA autorise des déplacements pouvant aller jusqu'à 250km/h avec un débit d'1 Mbit/s.

1.1.4 Réseau Régional sans fil – WRAN (Wireless Regional Area Network).

Ce sont des réseaux sans fil à haut débit couvrant une large zone géographique. Les principales normes sont IEEE 802.22.

IEEE 802.22/WRAN

La norme IEEE 802.22 [Cord05] vise à créer des réseaux sans fil dont la zone de couverture est comprise entre 40 et 100 km, en utilisant la bande de fréquence VHF/UHF (Very High Frequency/Ultra High Frequency) entre 54 et 862 MHz (fréquence de télévision). Pour éviter des interférences avec les canaux utilisés par la télévision, il utilise seulement les fréquences qui ne sont pas attribuées aux chaînes de télévision. 802.22 utilise un canal de 6, 7 ou 8 MHz et peut avoir un débit de 18Mbit/s pour un canal de 6MHz.

Voici un schéma comparatif de débits et de portées des différentes normes de réseaux sans fil que nous venons de décrire [Bour07]:

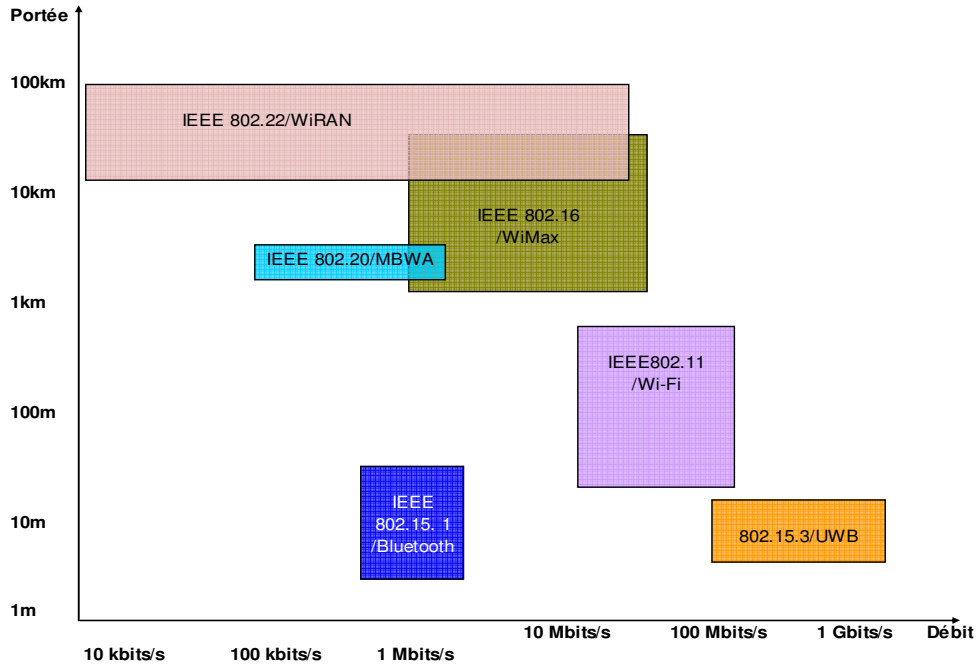


Figure 3 : Schéma débits portée des réseaux sans fil

1.2 Réseau local sans fil – IEEE 802.11/Wi-Fi

En 1997, l'organisme de standardisation IEEE (*Institute of Electrical and Electronics Enginneers – IEEE*) publie le premier standard international IEEE 802.11 [802.11 99] décrivant les caractéristiques d'un réseau local sans fil (en anglais *Wireless Local Area Network –WLAN*). La norme IEEE 802.11 définit les deux premières couches (la couche physique et la couche liaison de données) du modèle OSI pour une liaison sans fil utilisant des ondes électromagnétiques. La première version de la norme IEEE 802.11 ne proposait que des débits maxima de l'ordre de 2Mbits/s dans la bande de fréquence libre des 2,4 GHz. En raison des problèmes liés aux faibles débits proposés, les principales modifications ont porté sur la couche physique et proposent des débits supérieurs et une connectivité plus robuste. En septembre 1999 et en 2003, trois versions de la norme – 802.11a [802.11a 99], 802.11b [802.11b 99] et 802.11g [802.11g 03] sont ratifiées respectivement. Les normes 802.11b et 802.11g utilisent la bande de fréquence des 2,4GHz et proposent des débits théoriques allant respectivement jusqu'à 11Mbits/s et 54Mbits/s. La norme 802.11a propose également un débit maximal de 54Mbits/s mais utilise la bande de fréquence des 5GHz. Les versions 802.11b et 802.11g étant interopérables, un équipement 802.11b peut communiquer avec un équipement 802.11g et inversement. Par contre, un équipement 802.11a ne pourra établir une liaison radio qu'avec un autre équipement 802.11a en raison des bandes de fréquences différentes. La norme 802.11a étant moins répandue, nous allons par la suite plus particulièrement nous intéresser aux versions 802.11b et 802.11g.

Dans les paragraphes suivants, nous introduirons d'abord l'architecture de Wi-Fi, ensuite, nous parlerons de l'architecture du protocole, et de son fonctionnement.

1.2.1 Architecture IEEE 802.11/Wi-Fi

La norme IEEE 802.11 dispose de deux modes de fonctionnement distincts, qui correspondent à des architectures différentes : le mode infrastructure avec Point d'accès (*en anglais Access Point – AP*) et le mode réseau Ad-hoc.

Mode Infrastructure avec Point d'accès

Le mode infrastructure avec Point d'accès implique l'existence d'une station particulière, appelée Point d'accès, qui fédère autour d'elle les stations sans fil à portée radio. Cet AP est généralement relié à un réseau filaire. Il permet à une station sans fil de communiquer avec une autre station sans fil, qu'elles dépendent ou non du même AP et qu'elles se trouvent ou non dans le même type de réseau.

L'ensemble des stations sans fil à portée d'AP et cet AP lui-même constituent une cellule qui est appelée BSS (*Basic Service Set*) (Figure 4). Chaque BSS est identifiée par un BSSID (*Basic Service Set Identifier*), un identifiant de 6 octets (48 bits). Dans le mode infrastructure, le BSSID correspond à l'adresse MAC d'AP. Dans un BSS, il n'existe qu'un AP, et tout le trafic passe obligatoirement par cet AP. Du fait que la communication au sein

d'un BSS ne peut utiliser que le lien radio IEEE 802.11, toutes les stations d'un BSS sont à portée de l'AP. La zone de couverture d'un BSS est donc restreinte à la zone de portée radio autour de cet AP.

L'AP est une station qui possède, outre les services de communication sans fil, les services du système de distribution. Donc, il est possible de relier plusieurs BSS entre eux par un système de distribution ou DS (*Distribution System*). Le système DS correspond en règle générale à un réseau Ethernet filaire. Un groupe de BSS interconnectées par un système de distribution constitue un ensemble de services étendu ESS (*Extended Service Set*). Le système de distribution est responsable du transfert des trames entre différents BSS d'un même ESS.

L'ESS peut fournir une passerelle d'accès vers un réseau fixe, tel qu'Internet. Cette passerelle permet de connecter le réseau 802.11 à un autre réseau. Un ESS est repéré par un ESSID (*Extended Service Set Identifier*), un identifiant de 32 caractères (au format ASCII) servant de nom pour le réseau. L'ESSID, souvent abrégé SSID, est le nom du réseau et représente en quelque sorte un premier niveau de sécurité même s'il est très fragile dans la mesure où la connaissance du SSID est nécessaire pour qu'une station mobile se connecte au réseau étendu.

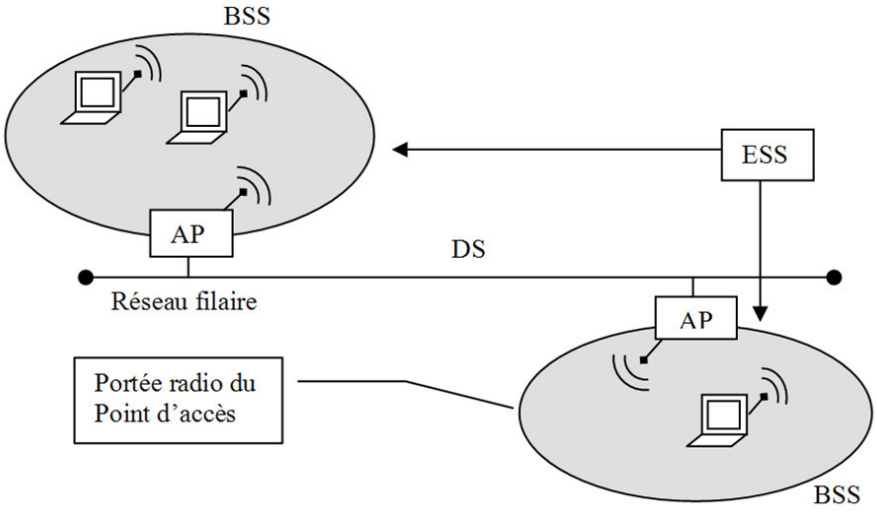


Figure 4 : Mode Infrastructure avec Point d'Accès

On peut dire que le mode infrastructure est, de fait, le mode par défaut. Compte tenu de la base installée des réseaux locaux filaires, l'utilisateur souhaite naturellement utiliser IEEE 802.11 pour communiquer avec des stations filaires disposées dans un réseau Ethernet. Une telle configuration implique le fonctionnement en mode infrastructure.

Mode Ad-hoc

Dans ce mode, il n'existe pas de station particulière, le réseau fonctionnant de façon totalement distribuée, les stations sans fil se connectent les unes aux autres afin de constituer un réseau point-à-point, c'est-à-dire un réseau dans lequel chaque station joue en même temps le rôle de client et le rôle de point d'accès.

L'ensemble des stations sans fil à portée radio mutuelle est appelé IBSS (*Independent Basic Service Set*) et fournit un ensemble de services de base indépendants. Un IBSS est ainsi un réseau sans fil éphémère constitué au minimum de deux stations et permettant à des personnes situées dans une même salle d'échanger des données. Il est identifié par un SSID. A la différence du mode infrastructure, le SSID est généré aléatoirement.

Dans un réseau Ad Hoc, si deux stations du réseau sont hors de portée l'une de l'autre, elles ne pourront pas communiquer, même si elles ont une autre station commune (problème du nœud caché). En effet, contrairement au mode Infrastructure, le mode Ad Hoc ne propose pas de système de distribution capable de transmettre les trames d'un nœud à un autre.

De plus, il n'est pas possible pour une station sans fil ad-hoc d'accéder à un quelconque réseau filaire. Ce mode est donc limité à de petits réseaux.

La figure 5 présente l'architecture du réseau Ad-hoc

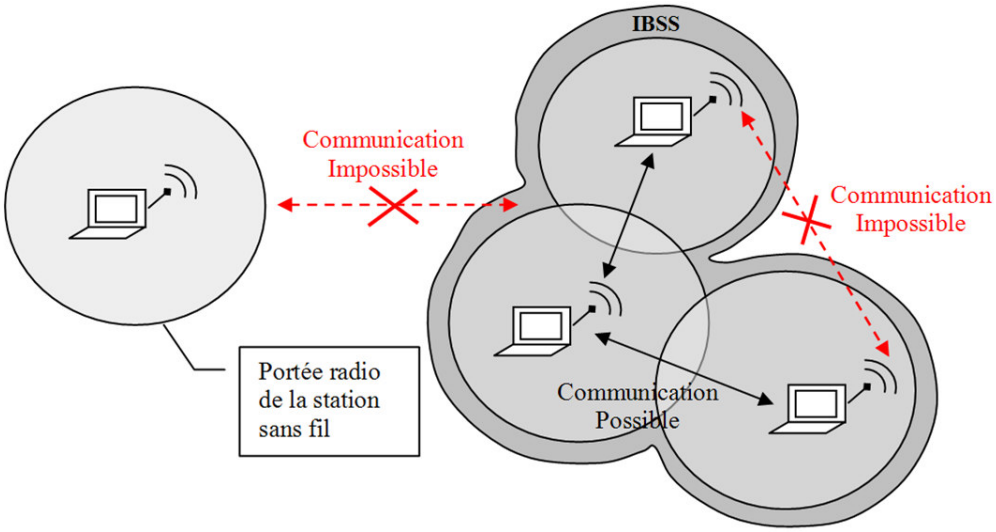


Figure 5 : Architecture du réseau ad-hoc

1.2.2 Architecture de protocoles IEEE 802.11/Wi-Fi

Comme décrit dans le tableau 1, la norme 802.11 définit les deux premières couches du modèle de référence OSI – la couche physique et la couche liaison de données.

Tableau 1: Architecture de protocoles IEEE 802.11/Wi-Fi

Couche liaison de données	LLC (Logical Link Control) 802.2
	MAC (Medium Access Control) 802.11
Couche physique	PLCP (Physical Layer Convergence Protocol)
	PMD (Physical Medium Dependent)

1.2.2.1 La couche physique

La couche physique définit la modulation des ondes radioélectriques et les caractéristiques de la signalisation pour la transmission de données. La couche physique de l'IEEE 802.11 assure les fonctions suivantes :

- Codage/décodage des signaux (par exemple, PSK (Phase Shift Keying), QAM, etc.) ;
- Génération/suppression de préambules (à des fins de synchronisation) ;
- Transmission/réception des bits.

Comme certaines normes IEEE 802, la couche physique de 802.11 est aussi subdivisée en sous–couches. IEEE 802.11 comprend deux sous–couches physiques : une sous–couche de convergence physique – PLCP (Physical Layer Convergence Protocol) et une sous–couche dépendante du support – PMD (Physical Medium Dependent).

- La sous-couche PLCP définit une méthode qui sert à convertir des unités de données de protocole MAC ou MPDU (MAC Layer Protocol Data Unit) de 802.11 en un format de trame adapté à l'émission et la réception de données utilisateur et d'informations de gestion, entre deux stations ou plus, à l'aide de la sous–couche PMD associée.

- La sous-couche PMD définit les caractéristiques des données utilisateur ainsi que la méthode utilisée pour leur transmission et leur réception à travers le support sans fil entre deux stations ou plus.

Les diverses normes pour IEEE 802.11, telles que 802.11, 802.11a, 802.11b, 802.11g, sont développées et elles utilisent différentes modulations et techniques d'étalement de spectre.

La modulation est une technique de transposition du spectre, son but est de transposer le signal dans une bande de fréquences adéquate pour obtenir une meilleure qualité de transmission. Elle nécessite l'utilisation d'une porteuse de haute fréquence qui est plus favorable à la transmission et susceptible de se propager sur des distances importantes. Les modulations les plus utilisées dans 802.11 sont la modulation par variation de fréquence FSK (Frequency Shift Keying), la modulation par variation de phase PSK et la modulation d'amplitude en quadrature QAM (Quadrature Amplitude Modulation [PAUL02].

Les techniques d'étalement de spectre SS (*Spread Spectrum*) sont largement employées dans beaucoup de systèmes de communication sans fil modernes tolérant la présence de plusieurs utilisateurs exploitant les mêmes ressources (temps et fréquence). Le principe de l'étalement de spectre consiste à étaler la densité spectrale de puissance sur toute la largeur de la bande de fréquences. Pour cela, une séquence pseudo aléatoire connue des deux communicants est utilisée pour l'étalement des données binaires (codage) à transmettre sur le canal et le désétalement des informations reçues au niveau du récepteur (décodage). Les trois techniques principales d'étalement de spectre couramment utilisées pour IEEE 802.11 sont décrites dans le tableau 2 : l'étalement de spectre par séquence directe DSSS (*Direct*

Sequence Spread Spectrum) et l'étalement de spectre par sauts de fréquences FHSS (*Frequency Hopping Spread Spectrum*) ; le multiplexage par fréquences orthogonales OFDM (*Orthogonal Frequency Division Multiplexing*) – [Rice00] [Stallings].

Tableau 2: Caractéristiques des normes de la couche physique IEEE 802.11

	802.11	802.11a	802.11b	802.11g
Couche physique IEEE 802.11	PLCP (Physical Layer Convergence Protocol)			
	2,4–2,4835GHz DSSS, FHSS	5,15 – 5,35GHz OFDM 5,725 – 5,825GHz OFDM	2,4–2,4835GHz DSSS	2,4–2,4835GHz DSSS, OFDM

1.2.2.2 La couche liaison de données

La couche liaison de données de 802.11 définit l'interface entre le bus du nœud et la couche physique, notamment une méthode d'accès proche de celle utilisée dans le standard Ethernet et les règles de communication entre les différentes stations. Elle est composée essentiellement de deux sous-couches – LCC (Logical Link Control ou le contrôle de la liaison logique) et MAC (Media Access Control, ou le contrôle d'accès au médium).

La sous-couche LLC utilise les mêmes propriétés que la sous-couche LLC de 802.2. Il est de ce fait possible de relier un WLAN à tout autre réseau local appartenant à un standard de l'IEEE.

La sous-couche MAC est spécifique de 802.11, son rôle est assez similaire à celui de la couche MAC 802.3 du réseau Ethernet filaire en termes de méthode d'accès. Cependant, la sous-couche MAC 802.11 intègre les fonctionnalités nécessaires pour réaliser un accès sur une interface radio.

Les stations sans fils de 802.11 utilisent un même canal radio pour communiquer. Si ces stations sans fil tentent d'accéder à ce canal en même temps, il y aura probablement une collision et une perte de trames. Pour que les stations sans fil puissent partager une même ressource de communication sans provoquer de collision, deux méthodes d'accès fondamentalement différentes au niveau de la sous-couche MAC sont utilisées dans IEEE 802.11 : l'accès à compétition et l'accès contrôlé.

- La méthode d'accès à compétition propose de ne pas contrôler le premier accès à la ressource de communication, en acceptant un accès aléatoire au medium. Mais si plusieurs stations utilisent le canal simultanément et entrent en collision, le protocole organise une retransmission pour que les stations en collision puissent achever leur envoi avec succès. Ce faisant, le protocole résout la collision. L'ancêtre de ces protocoles est Aloha [Abr73] et le protocole plus connu est CSMA

(Carrier Sense Multiple Access) – l'accès multiple avec écoute préalable de la porteuse [Stallings].

- La méthode d'accès contrôlé consiste à organiser à l'avance l'accès à la ressource de communication. L'ancêtre de cette technique est le multiplexage temporel statique, ou TDMA (Time Division Multiple Access).

La norme IEEE 802.11 met à profit ces deux méthodes d'accès en offrant comme mode par défaut l'accès à compétition – DCF (Distributed Coordination Function) et comme mode optionnel l'accès contrôlé – PCF (Point Coordination Function).

1.2.2.3 DCF (Distributed Coordination Function)

DCF a été conçu pour permettre des transferts de données asynchrones en best-effort, dans lequel toutes les stations qui veulent transmettre des données ont une chance égale d'accéder au support. DCF utilise aussi la technique d'accès à compétition pour contrôler des stations à l'accès au medium. Or, dans les réseaux Wi-Fi, la technique CSMA/CD ne peut pas être utilisée par DCF, même si elle est très efficace dans le cas d'un réseau local filaire LAN (Local Area Network). Cela s'explique par le fait que la détection de collisions n'est pas possible dans un système radio.

La technique CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) – l'accès multiple avec écoute préalable de la porteuse/évitement de collision est une variante du CSMA/CD, qui permet à la méthode CSMA de fonctionner lorsque la détection des collisions n'est pas possible dans le hertzien. Son principe de fonctionnement consiste à résoudre la contention avant que les données soient transmises en utilisant des accusés de réception – ACK(Acknowledgement) et des temporisateurs – IFS (Inter-Frame Spacing). Le DCF s'appuie sur cette technique.

Tout message reçu doit être au plus vite acquitté par le récepteur. Un accusé de réception ACK doit être envoyé par le récepteur pour confirmer que les données sont reçues de manière intacte, le non–retour d'un accusé de réception ACK, au bout d'un intervalle de temps prédéterminé, permet à l'émetteur de détecter s'il y a eu collision.

Les stations désirant émettre testent le canal à plusieurs reprises afin de s'assurer qu'aucune activité n'est détectée. Dans le Wi-Fi, le temps est découpé en tranches, qui correspondent chacune à un slot_time. Le slot_time est utilisé pour définir la taille des IFS (Inter-Frame Spacing – Espace Inter-Trame). IFS correspond à l'intervalle de temps entre la transmission de deux trames. Les intervalles IFS sont des périodes d'inactivité sur le support de transmission. L'accès au support est contrôlé par l'utilisation d'IFS (Inter-Frame Spacing). Les valeurs des différent IFS sont prédéterminées par la norme et exécutées par la couche physique.

La norme définit trois inter-trames de tailles différentes, utilisées pour leurs différentes propriétés. Plus l'inter-trame est courte pour une station, plus son accès est prioritaire.

- L'inter-trame courte SIFS (*Short Inter Frame Spacing*) est la plus courte, permet à ACK de précéder toute autre transmission qui souhaiterait débuter en même temps. De la sorte, ACK est assuré d'être transmis avant tout autre paquet en attente de retransmission.

- L'Inter-trame pour l'accès contrôlé PIFS (*Point Coordination Inter-Frame Spacing*) est intermédiaire est utilisée par le Point d'Accès (appelé Point Coordinateur dans ce cas) pour l'envoi des paquets en mode PCF. Le fait que l'inter-trame PIFS soit plus courte que l'inter-trame DIFS montre que les paquets envoyés dans le mode PCF sont prioritaires sur les paquets envoyés en mode DCF. La valeur de PIFS est la valeur de SIFS plus un temps, ou time_slot, défini dans l'algorithme de backoff.

- L'inter-trame pour l'accès distribué DIFS (*Distributed Inter-Frame Spacing*) est la plus longue, est utilisée pour l'envoi d'un paquet courant dans le mode d'accès DCF.

Dans les réseaux Wi-Fi, les terminaux d'un même BSS peuvent écouter l'activité de toutes les stations qui s'y trouvent. Lorsque la station source transmet ses données, les autres stations l'entendent et, pour éviter une collision, mettent à jour un temporisateur, appelé NAV (Network Allocation Vector). NAV permet de retarder toutes les transmissions prévues. NAV détermine l'instant auquel la trame peut être transmise avec succès, en incluant le temps de transmission de la trame de données, le SIFS et l'ACK. Les autres stations n'ont la capacité de transmettre qu'après la fin du NAV.

Afin d'éviter les collisions lorsque plusieurs stations veulent transmettre des données en même temps, l'algorithme de backoff est introduit dans le réseau Wi-Fi. Quand une station voulant transmettre des données écoute le support, si aucune activité n'est détectée pendant une période de temps correspondant à un DIFS, et en plus la valeur de son NAV est égale à 0, la station doit encore patienter pendant une durée déterminée par l'algorithme de backoff pour pouvoir envoyer les trames. La durée de la procédure de backoff est communément appelée CW (Contention Window) – en français la fenêtre de contention. L'algorithme de backoff choisi une valeur aléatoire X dans l'intervalle [0; CW], où CW est une variable entière.

La durée de l'attente pour la station est donnée par la formule suivante :

Attente = alea_uni(CW) * Timeslot où alea_uni(n) fournit un entier entre 1 et n-1.

La valeur numérique du paramètre CW dépend des caractéristiques du médium CW_{min} et CW_{max} et est restreinte par la relation $CW_{min} \leq CW \leq CW_{max}$. A la première tentative d'émission d'une donnée, le paramètre CW est positionné à CWmin. A chaque retransmission de cette donnée (en raison de l'occupation du canal), le paramètre CW est séquentiellement positionné à la puissance de 2 supérieure moins 1 jusqu'à atteindre CW_{max} (voir figure 6).

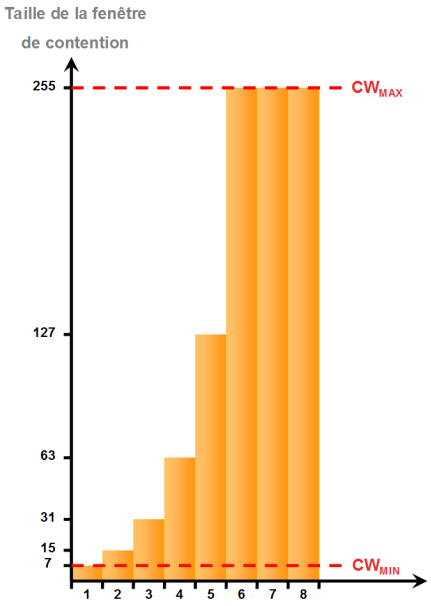


Figure 6 : Exemple de l'incrémentation du paramètre CW

Dès la sélection de X, la station décrémente la valeur de X et continue d'écouter le support. Lorsque le médium est à nouveau occupé avant que la valeur X atteigne la valeur 0, la station attend qu'il soit à nouveau libre et qu'il reste libre pendant DIFS avant de continuer à décrémenter X. Dès que X atteint la valeur 0 et si le support est toujours libre, alors l'émission peut commencer. Si le support est occupé, elle continue de l'écouter jusqu'à ce qu'il soit libre. Quand le support devient disponible, elle retarde encore sa transmission en utilisant l'algorithme de backoff avant de transmettre ses données.

Elle transmet ses données à l'instant. Si les données envoyées sont reçues intactes, la station de destination attend pendant un temps équivalent à un SIFS et émet un ACK pour confirmer leur bonne réception. Si l'ACK n'est pas détecté par la station source ou si les données ne sont pas reçues correctement ou encore si l'ACK n'est pas reçu correctement, on suppose qu'une collision s'est produite, et la trame est retransmise.

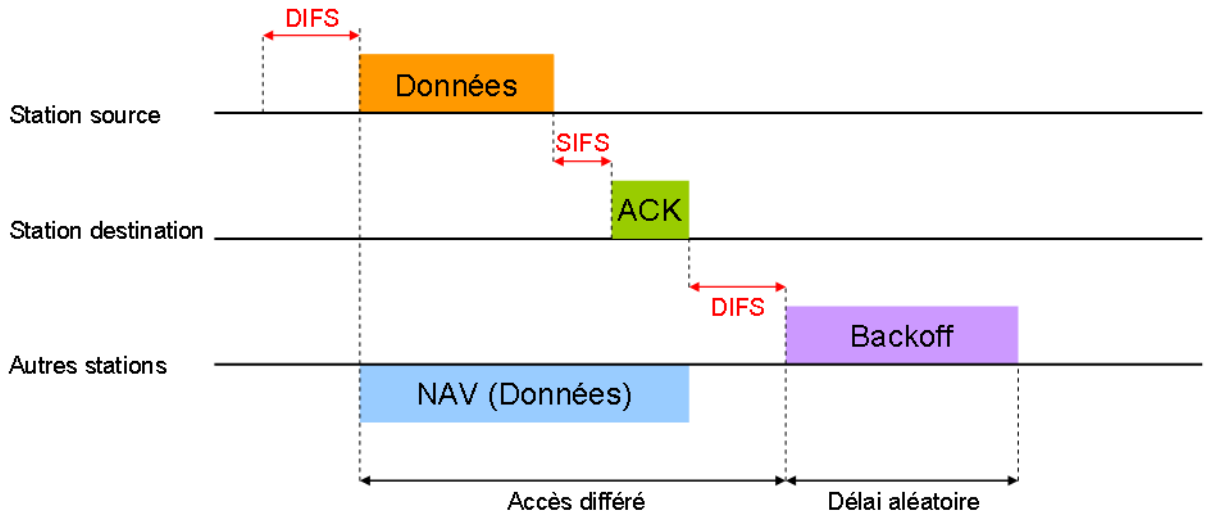


Figure 7 : Processus de Transmission des Trames

Mécanisme RTS/CTS

Bien que la méthode DCF permette de partager la ressource radio tout en évitant les collisions, il reste un problème propre aux réseaux sans fil. En effet, il manque encore un mécanisme tenant compte des problèmes liés à la station cachée.

Comme rappelé ci-dessus, lorsque la station source s'accapare le médium et transmet une trame, les autres stations se trouvant dans la portée radio de la station source d'un même BSS peuvent aussi recevoir cette trame. Cette trame inclue une valeur NAV. NAV est utilisé pour interdire toutes les autres stations sauf la station source de transmettre des données pendant le temps de NAV. Mais il est possible que des stations d'un même BSS/ (associés au même AP ou utilisant le même canal radio) n'entendent pas cette trame en raison de leurs portées radio et imaginent le médium libre et transmettent une donnée au même moment. Ces émissions simultanées peuvent provoquer des collisions au niveau de l'AP. Afin de remédier à ces problèmes, la norme propose un mécanisme de réservation du médium. Avant une transmission, la station source envoie à l'AP une trame RTS (Request To Send) indiquant qu'il va transmettre une trame de données et la durée de la transmission. La durée de la transmission (NAV) est marquée dans le champ TTL du RTS. En retour, l'AP envoie une trame CTS (Clear To Send) comme la réponse qui contiendra aussi l'information sur la durée. Cette trame notifie aux stations se trouvant dans la portée radio de l'AP de ne pas utiliser le médium pendant la durée de NAV car une émission est imminente.

Toutes les stations recevant soit le RTS, soit le CTS, déclencheront leur indicateur NAV (Network Allocation Vector) pour une certaine durée, et utiliseront cette information pour écouter le support.

Ce mécanisme réduit la probabilité de collisions par une station "cachée " de l'émetteur dans la zone du récepteur à la courte durée de transmission du RTS, parce que la station entend le CTS et considère le support comme occupé jusqu'à la fin de la transaction.

Lorsque la station source reçoit la trame CTS, le canal est réservé et il peut transmettre sa trame de données.

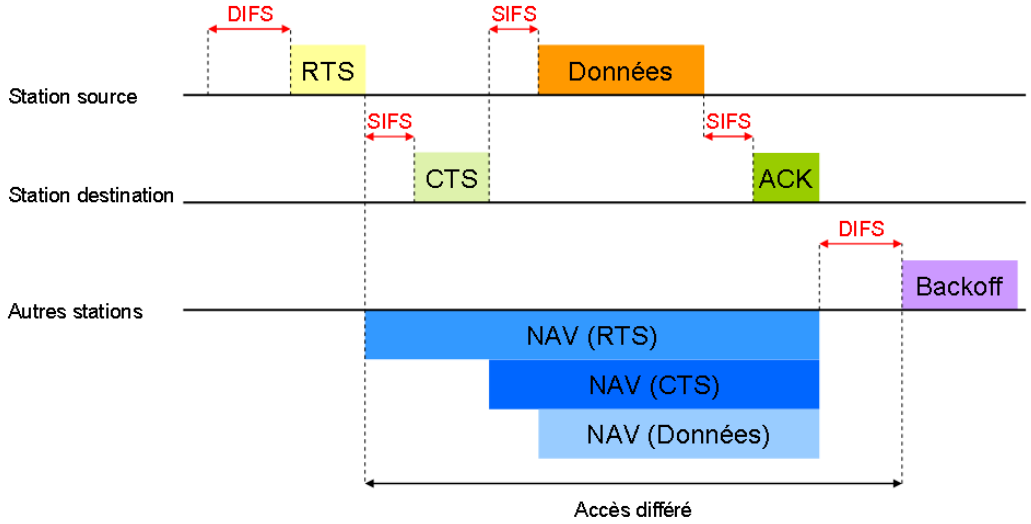


Figure 8: Transmission en utilisant les trames RTS/CTS

La procédure RTS/CTS est cependant un mécanisme optionnel, dont l'utilisation est déterminée par le paramètre RTSThreshold.

Trois comportements sont définis par la norme :

- ne jamais effectuer de procédure RTS/CTS pour l'émission de trames de données.
- toujours effectuer une procédure RTS/CTS avant l'émission d'une trame de données.
- effectuer une procédure RTS/CTS pour une trame de données dépassant une certaine taille.

Sur les équipements sans fil actuel, c'est généralement la troisième solution qui est utilisée par défaut afin de limiter les retransmissions des grandes trames de données.

1.2.2.4 PCF (Point Coordination Function)

PCF (*Point Coordination Function*) utilise le mode accès contrôlé et favorise la prise en charge de données isochrones, comme la voix ou la vidéo. Ce mode garantit une transmission à un rythme régulier, ce qui permet de synchroniser des flux.

PCF consiste à contrôler les échanges dans le réseau par un Point de coordination (*en anglais Point Coordinator*). Le Point de Coordination, généralement représenté par l'AP, permet d'avoir une coordination centralisée de l'accès au médium pendant la période dite CFP (*Contention Free Period*) durant laquelle la méthode PCF est utilisée. Cette période CFP est alternée par une trame permettant de synchroniser les terminaux avec une autre période dite CP (*Contention Period*) pendant laquelle la méthode DCF peut être utilisée. Utilisant des intervalles de temps PIFS (*PCF Inter-Frame Space*) plus courts que ceux utilisés par les terminaux, l'AP est donc privilégié.

Pendant la période CFP, l'AP balaye tour à tour les stations et donne les autorisations d'envoyer les données, ce processus est appelé polling [Stallings].

1.2.3 Gestion des Associations

Les fonctions de gestion permettent de structurer, de faire fonctionner et de gérer le réseau Wi-Fi. Elles incluent la fonction d'association qui est nécessaire pour bâtir le réseau, la fonction désynchronisation qui est indispensable pour le niveau physique à saut de fréquence, et la fonction de gestion d'énergie qui permet à des stations de fonctionner en mode économie d'énergie. Dans notre recherche, nous nous concentrons sur la fonction d'association.

Lorsque les stations se déplacent dans le réseau Wi-Fi, c'est-à-dire lorsqu'elles changent de BSS, ou qu'elles sortent d'un mode d'économie d'énergie ou juste après allumage, avant de pouvoir communiquer, elles doivent choisir un AP d'un BSS, et s'associer à cet AP. Cette procédure de découverte des APs et consistant à s'associer avec un AP est appelée la procédure d'association. Les stations qui se déplacent dans les réseaux se déconnectent avec l'AP courant, et lancent la procédure d'association et se reconnectent à un nouveau AP. Cette procédure du changement d'AP dans les réseaux sans fil est appelé handover de couche liaison ou le handover de niveau 2 (en anglais *Layer 2 Handover – L2 handover*).

La procédure d'association est à l'initiative des stations et est décomposée en trois phases : phase de découverte, phase d'authentification et phase de réassociation. Elle est réalisée à l'aide des trames de gestion des associations sous la forme des échanges de type hand-check : requête puis réponse à la requête. Avant la fin de la procédure d'association, les stations ne peuvent ni recevoir les trames des données, ni envoyer les trames des données.

Phase de découverte

La première étape d'une procédure d'association consiste à découvrir un Point d'Accès. Le choix d'un Point d'Accès est lié à un certain nombre de critères, tels que la puissance du signal, le taux d'erreur des paquets ou la charge du réseau.

Un mécanisme, défini dans la norme 802.11b/g pour mesurer la puissance du signal reçu – RSSI (Received Signal Strength Indication) avec une valeur variable entière entre [0,255], est utilisé pour représenter la puissance du signal. Si le RSSI avec l'AP courant descend au–dessous d'un seuil, la station doit lancer la phase de découverte pour chercher un autre Point d'Accès plus approprié.

La recherche du meilleur Point d'Accès passe par l'écoute du support. Elle peut se faire de deux manières différentes : scan actif et scan passif, selon des critères tels que les performances ou la consommation d'énergie.

- Scan actif: La station mobile sonde tous les canaux radio consécutivement en envoyant une trame, appelée Probe Request Frame. Lorsqu'un AP reçoit cette trame, il répond à la station source en envoyant une trame, appelée Probe Response

Frame. Cette trame contenant les différents paramètres, tels que des informations de configuration réseau comme le SSID et le mécanisme de sécurité adopté, le taux des transmissions supporté, etc. S'il existe plusieurs APs à proximité utilisant un même canal radio, l'envoi d'une Probe Request peut engendrer de multiples Probe Response, envoyées par ces différents APs. Lorsque la station reçoit une Probe Response, il enregistre les différents paramètres de l'AP contenus dans cette trame. Ensuite, il continue de sonder les canaux radio suivants (ou une liste de canaux radio). Apres avoir sondé tous les canaux, la station sélectionne un AP parmi ceux qu'il a découverts et passe à la phase d'authentification.

Il est possible que la station ne puisse pas recevoir une Probe Response après l'envoi d'une Probe Request sur un canal. En effet, une collision s'est produite lorsque l'envoi de Probe Request, quand il n'y a pas d'AP à proximité opérant sur ce canal sondé peut causer une non-réception de Probe Response. Pour éviter que la station attende la Probe Response trop longtemps sans pouvoir sonder le canal suivant, la station doit lancer un compteur du temps Probe Timer après l'envoi d'un Probe Request sur un canal radio. La norme définit deux temps d'attente lors du scan d'un canal : MinChannelTime et MaxChannelTime. Apres l'émission de la première Probe Request sur un canal, la station initie le compteur Probe Timer. S'il n'y a pas d'activité détectée sur le canal, et lorsque le compteur Probe Timer atteint MinChannelTime et si pendant ce temps la station n'a pas reçu de Probe Response, il en déduit qu'aucun AP n'opère sur ce canal et passe au canal suivant. Si la station détecte que le canal n'est pas à vide, elle doit attendre Probe Response d'AP jusqu'à ce que le compteur Probe Timer atteigne MaxChannelTime et passer au canal suivant. La norme ne définit que la relation MinChannelTime < MaxChannelTime sans donner de valeurs numériques à ces paramètres. Comme nous allons le constater par la suite, ces paramètres peuvent fortement varier suivant le modèle de l'équipement sans fil. Une mesure empirique [Ram05] montre que MinChannelTime vaut environ 20ms et MaxChannelTime vaut environ 40 ms. Pour sonder tous les canaux, la limite du délai de scan actif peut être calculée comme :

$$N \times T_{min} \leq T_{scan} \leq N \times T_{Max,}$$

Où N est le nombre de canaux qui peuvent être sondés lors du scan actif, le T_{min} est MinChannelTime, le T_{Max} est MaxChannelTime, et T_{scan} correspond à tout le délai de scan actif mesuré.

- Scan Passif : La norme 802.11b/g spécifie également une méthode de recherche passive. Les APs diffusent périodiquement une trame balise (*en anglais Beacon Frame*) pour annoncer leur présence. Afin de découvrir les APs sur un canal, il suffit pour les stations de basculer sur ce canal et d'intercepter des trames balises provenant des APs. La trame balise est généralement envoyée toutes les 100 millisecondes environs. Pour la norme 802.11b/g qui a 11 canaux. La station doit prendre 100 ms ×11 ≈ 1 seconde à sonder tous les canaux et découvrir les APs disponibles. Puisque le scan passif nécessite toujours une plus longue latence que le scan actif, la plupart des stations utilisent le scan actif pour découvrir les APs disponibles.

Phase d'authentification

Lorsqu'une station a sélectionné un nouveau AP suite à la phase de découverte, elle doit s'authentifier avec l'AP choisi. Deux méthodes d'authentification sont définies dans la norme. La méthode ouverte ne nécessite qu'une séquence de deux messages (requête/réponse) car chaque station est systématiquement autorisée à accéder au réseau. Par contre, la méthode à clé partagée est décomposée en une séquence de quatre messages. La station commence par envoyer son identité à l'AP. Celui-ci demande alors à la station de répondre à un texte de défi permettant de vérifier si la station possède le secret partagé. Après vérification de la réponse au texte de défi, l'AP communique à la station le résultat de l'authentification (réussie ou non).

Phase de réassociation

La phase de réassociation constitue la dernière étape de la procédure d'association et se décompose en deux messages. Suite à une authentification réussie, la phase d'association permet à la station et à l'AP de s'accorder sur les différents paramètres qu'ils vont utiliser pour leurs communications à venir. Une station est capable de transmettre et de recevoir des données dès la fin de la phase d'association.

La figure 9 illustre les différentes phases introduites précédents.

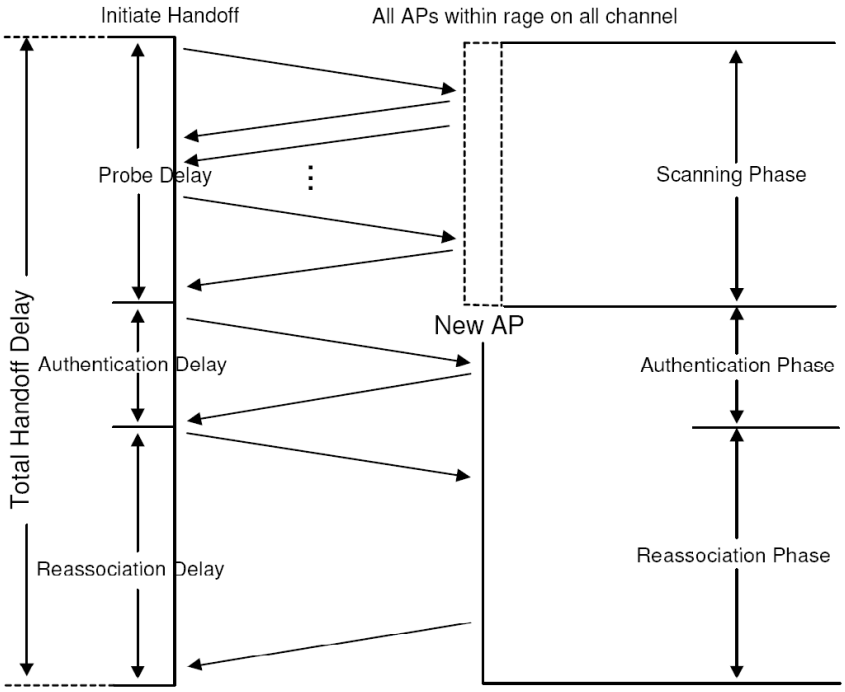


Figure 9: Processus d'associations

Selon les trois phases, le délai total est décomposé en trois parties : délai de découverte, délai d'authentification et délai de réassociation. Parmi lesquels, le délai le plus important est le délai de la phase de découverte, il représente 90% du délai total [Mish03]. La phase d'authentification et la phase de réassociation ne nécessitent généralement que quelque millisecondes.

Comme dit précédemment, la station ne peut ni transférer ni recevoir les données avant la fin de la procédure d'association. Le délai est assez significatif pour affecter la qualité de service pour beaucoup d'applications.

Etant donné que la station doit par défaut scanner tous les canaux consécutivement dans le mode scan actif ou le mode scan passif, pour réduire le délai, la meilleure solution est de scanner le moins de canaux possible. Si la station sait préalablement sur quel canal les APs disponibles fonctionnent avant la phase de découverte, elle ne scannera que ces canaux.

L'auteur de [Shin04] propose de scanner tous les canaux et d'enregistrer les résultats dans le cache de la station, baptisé AP cache. Quand la station se déplace dans un endroit déjà visité auparavant, elle sait sur quel canal il y a les APs disponibles par vérification de son AP cache. Donc, elle ne scanne que ces canaux et les canaux 1, 6, 11 en plus. Mais s'il n'y a pas d'AP cache correspondante ou une AP cache erronée, la station doit re-scanner tous les canaux et le délai de la phase de découverte est le même que le scan total.

L'autre de [Mish03] propose de procéder périodiquement la phase de découverte pendant MinChannelTime temps et sur un seul canal, ensuite la station se reconnecte à son AP courant pour reprendre son communication en cours. Par ce moyen, la station construit une liste des APs disponibles à sa portée avant de changer d'AP. Mais cette méthode nécessite un temps plus long, de plus, il doit se reconnecter chaque fois à son AP courant, cela provoque la perte de paquets et est compliqué à réaliser.

Dans [Hua06], l'auteur utilise l'AP pour enregistrer l'information des APs voisines dans la base de données de chaque AP. L'AP informe la station correspondant à un canal sur lequel il existe les AP voisines, la station ne scanne que les canaux proposés. Mais l'inconvénient est qu'il n'est pas facile de construire et mettre à jour le graphe de voisins, puisque tous les APs doivent mettre à jours leur cache et surtout lorsque cette méthode est employée dans un réseau sans fil à grande échelle.

L'auteur de [Ram05] propose une méthode – SyncScan pour réduire le délai de la phase de découverte. Il assume pouvoir synchroniser tous les APs à proximité pour que ils puissent diffuser des trames balises avec un intervalle préconfiguré. La station lance un scan passif et change les canaux justement avant l'arrivée des trames balises provenant des APs de chaque canal. Cette méthode peut réduire le délai d'une seconde à quelques centaines de milliseconde, mais il est impossible d'ajouter cette fonctionnalité dans tous les APs et de les synchroniser dans un réseau sans fil à grande échelle.

1.3 Conclusion

Dans ce chapitre, nous avons présenté différents technologies de réseaux sans fil, en particulier les réseaux IEEE 802.11/Wi-Fi. Une grande partie est consacrée pour décrire la procédure du handover de niveau 2 gérée par la norme Wi-Fi. Vu que le délai de la procédure du handover de niveau 2 gérée par la norme Wi-Fi et la perte de paquets provoqués par la procédure du handover de niveau 2 gérée par la norme Wi-Fi ne peuvent pas répondre à la demande des applications temps réel, plusieurs approches sont proposées pour réduire ce délai, cependant, elles ne sont pas complètes ou suffisantes. Par conséquent, nous présenterons notre méthode, baptisé E-HCF dans le chapitre 3, qui a pour l'objet d'améliorer la performance du handover dans les réseaux Wi-Fi.

2 Protocole IP et Protocole IP Mobile

Le protocole IP (*Internet Protocol – IP*) [RFC 791] est un protocole standardisé par l'organisation de standardisation des protocoles de l'Internet (en anglais *Internet Engineering Task Force – IETF*) dans les années 70. Il définit une manière selon laquelle les ordinateurs peuvent communiquer par les équipements intermédiaires du réseau. Le principal intérêt du protocole IP est son adoption quasi universelle. Avec le développement et le succès d'Internet, la majorité des applications ont été développées et conçues pour utiliser ce protocole. En effet, celui-ci offre à un ordinateur la possibilité d'être à la fois relié à son réseau local, mais également de pouvoir dialoguer avec n'importe quels autres ordinateurs sur Internet.

Dans ce contexte favorable, il a été naturellement envisagé d'utiliser des terminaux mobiles sur Internet. Comme le protocole IP devient un standard de communication réseau, il a donc été nécessaire d'enrichir le protocole IP afin que celui-ci permette le support de la mobilité des terminaux mobiles. Un nouveau protocole IP Mobile, le protocole de gestion de la mobilité dans Internet Nouvelle Génération, a donc vu le jour [RFC 3220]. Ce protocole est aussi normalisé par l'IETF et est une surcouche du protocole IP. L'objectif de celui-ci est de masquer la mobilité d'un terminal mobile à ses correspondants et d'offrir la possibilité de maintenir une connexion au réseau tout en effectuant son déplacement.

Il existe deux générations du protocole IP - IPv4 (IP Version 4) [RFC 791] et IPv6 (IP version 6) [RFC 2460]. IPv4 est la première version du protocole IP à avoir été largement déployée et forme encore la base d'Internet. Mais les limitations d'IPv4, surtout la pénurie des adresses IPv4, conduit à la transition d'IPv4 vers IPv6 [CAR05]. Le protocole IP Mobile se décline aussi en deux normes - IPv4 Mobile [RFC 3220] et IPv6 Mobile [RFC 3775]. Le premier standard IPv4 Mobile a été défini pour le support de la mobilité dans les réseaux IPv4. Le protocole IPv6 Mobile est en cours de normalisation pour l'utilisation des terminaux mobiles sur IPv6.

Dans ce chapitre, nous présentons d'abord les deux générations du protocole IP – IPv4 et IPv6. Ensuite, nous décrivons le protocole IPv4 Mobile et IPv6 Mobile, où nous insisterons sur la procédure du handover quand un terminal mobile se déplace d'un réseau vers l'autre. En raison des problématiques provoquées par la procédure du handover gérée par le protocole IP Mobile, telles que le délai, la perte de paquets, les diverses propositions qui ont été faites pour résoudre ces problématiques et améliorer la performance du handover. Nous les présentons dans ce chapitre et présentons notre méthode E-HCF dans le chapitre suivant.

2.1 Le Protocole IP

Selon l'architecture de systèmes de communication définie dans le modèle de référence : OSI (*Open Systems Interconnection – OSI*), le protocole IP est un protocole routable qui fonctionne au niveau de la couche réseau.

Le protocole IP se charge de sélectionner et d'établir le meilleur chemin à travers les réseaux pour acheminer les données sous forme de paquets (ou datagrammes) vers la destination. L'envoi de ces paquets est réalisé en fonction des adresses de réseaux qu'ils contiennent. Cependant le protocole IP n'apporte aucune garantie pour l'acheminement correct des données ou pour la qualité de service (en anglais *Quality of Service – QoS*). Il se contente de faire de son mieux. On dit que le protocole IP est un protocole "best effort". Les paquets peuvent emprunter différents chemins, être perdus, arriver dans le désordre ou erronés. Le protocole IP est un protocole non fiable mais robuste. Ce sont les couches situées au dessus de la couche réseau qui sont en charge de fiabiliser la communication, de gérer les erreurs et de réordonnancer les paquets si nécessaire.

Comme nous l'avons décrit, il existe deux normes du protocole IP. Nous présentons d'abord le protocole IPv4, ensuite, le protocole IPv6 dans les paragraphes suivants.

2.1.1 Protocole IP version 4

Le protocole IPv4 a été standardisé en 1981 et s'adressait initialement à la communauté militaire et scientifique. Il utilise une adresse IP sur 32 bits, c'est-à-dire que 4 294 967 296 adresses sont possibles.

Le protocole IPv4 n'a pas été conçu pour assurer la QoS, ni l''auto-configuration d'adresses, ni le multicast, ni la sécurité. Il est évident que le protocole IPv4 ne peut plus répondre à la demande des utilisateurs. Les diverses solutions ont été trouvées pour assurer les fonctions ci-dessus, mais elles l'alourdissent l'ensemble des couches supplémentaires. Par exemple:

- Le protocole NAT (en anglais *Network Address Translation – NAT*) qui permet de résoudre la pénurie d'adresses IPv4, a pour effet de compliquer la gestion des adresses IP privées et publiques, d'alourdir les chemins de routage, de surcharger les tables de routage et de ralentir le développement des applications temps réel qui fonctionnent de bout en bout.

- Vu que le protocole IPv4 n'est pas prévu à l'origine pour permettre à un terminal d'auto-configurer son adresse IP dans un réseau, il faut les configurer manuellement ou utiliser un serveur doté du protocole DHCP (en anglais *Dynamic Host Configuration Protocol – DHCP*) qui supporte la fonction d'auto-configuration d'adresses pour les terminaux.

- La fonction de diffusion, qui s'est développée aujourd'hui dans le protocole IPv4, monopolise une classe complète d'adresses et n'est pas une fonction native d'IPv4.

- Le protocole IPSec est utilisé comme une option dans IPv4. En outre, le NAT complique l'utilisation du protocole IPSec.

2.1.2 IP version 6

Comme expliqué ci-dessus, IPv4 ne peut pas répondre aux besoins engendrés par la croissance très forte d'Internet, ni aux besoins induits par de nouvelles applications. Toutes les limitations d'IPv4 conduisent à la transition d'IPv4 vers IPv6. IPv6 a été conçu dans la continuité d'esprit d'IPv4, sans réelle rupture technologique. Cependant, le nouveau protocole IPv6 n'en reste pas moins différent et l'interopérabilité entre les deux versions IP n'est pas naturelle.

La caractéristique la plus importante d'IPv6 est qu'il supporte des adresses plus longues qu'en IPv4. L'augmentation de la taille des adresses conduit à une taille d'en-tête de 40 octets pour le paquet IPv6, le double de l'en-tête IPv4 sans les options. En outre, le format d'en-tête IPv6 est simplifié et amélioré pour permettre aux routeurs de meilleures performances dans leurs traitements de paquets.

Les principales améliorations de l'en-tête IPv6 sont les suivantes:

- L'en-tête ne contient plus le champ checksum parce que l'en-tête devait être ajustée par chaque routeur en raison de la décrémentation du champ durée de vie. Par contre, pour éviter qu'un paquet soit erroné, tous les protocoles des couches supérieures doivent mettre en œuvre un mécanisme de checksum de bout en bout.

- La taille d'en-tête est fixée. Ainsi le routeur peut facilement déterminer où commence la zone de données utiles.

- Les options ont été retirées de l'en-tête et remplacées par des extensions qui peuvent être facilement ignorées par les routeurs intermédiaires.

- Les champs sont alignés sur des mots de 64 bits, ce qui optimise leur traitement, surtout avec les nouvelles architectures à 64 bits.

- La fonction de fragmentation a été retirée des routeurs intermédiaires. IPv6 utilise un mécanisme de découverte du PMTU (en anglais *Path Maximum Transfer Unit – PMTU*) pour éviter d'avoir recours à la fragmentation par les routeurs. Si la fragmentation s'avère nécessaire, une extension est prévue.

Le format d'en-tête d'un paquet IPv6 est montré dans la figure 10 [RFC 2474]. L'en-tête du paquet IPv6 est fortement simplifié par rapport à l'en-tête IPv4 (7 champs au lieu de 14). Une extension est ajoutée pour les fonctionnalités optionnelles, telles que la sécurité, le routage, la mobilité, etc.

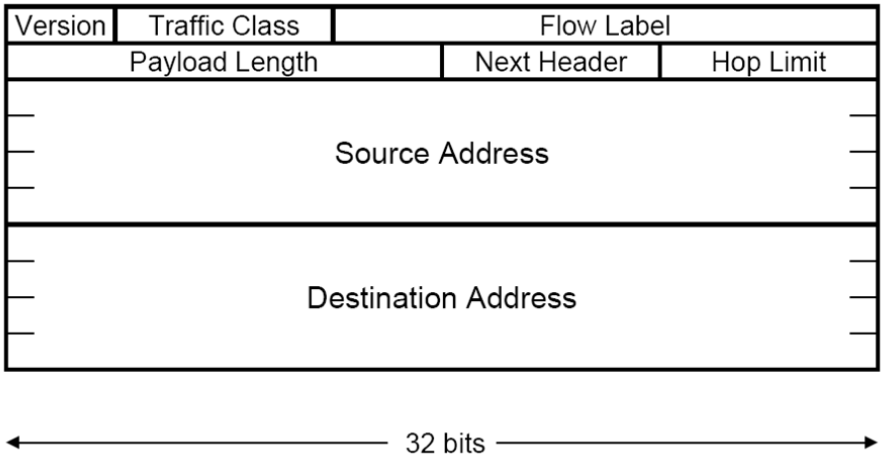


Figure 10 : Format d'en-tête IPv6

- Version : est sur 4 bits. Le champ version est le seul champ qui occupe la même place dans l'en-tête IPv6 et dans l'en-tête IPv4.

- Classe de trafic (en anglais *Traffic Class*) : est sur 8 bits. Les six premiers bits de ce champ constituent un label DSCP (*en anglais Differentiated Services Code Point - DSCP*) qui indique un niveau de classe de service qui peut éventuellement refléter de priorités et permet de traiter les paquets plus ou moins rapidement dans les équipements intermédiaires du réseau. Les deux autres bits de ce champ sont réservés pour ECN (*en anglais Explicit Congestion Notification - ECN*) [RAM01] qui se sert à informer à l'avance le protocole de transport de la cogestion sur le chemin prennent les paquets. Ce champ est semblable au champ "Type of Service" d'IPv4.

- Etiquette de flot (en anglais *Flow Label*) : est sur 20 bits. C'est un nouveau champ qui permet de transporter une référence (en anglais *label*). Avec cette référence, il est capable de préciser le flux auquel appartiennent les paquets et donc d'indiquer la QoS exigée par les informations transportées. Cette référence permet également aux routeurs de prendre des décisions adaptées. Grace à ce nouveau champ, le routeur peut traiter de façon spécifique les paquets IPv6, autorisant ainsi la prise en compte de diverses contraintes.

- Longueur du contenu (en anglais *Payload Length*) : est sur 16 bits. Contrairement à IPv4, ce champ ne contient que la taille des données utiles, sans prendre en compte la longueur d'en-tête IPv6 qui n'est pas nécessaire.

- En-tête d'extension (en anglais *Next Header*) : est sur 8 bits. Ce champ a une fonction similaire au champ Protocole d'IPv4. Il identifie l'en-tête d'extension qui peut s'agir d'un protocole (de niveau supérieur ICMP, UDP, TCP...) ou de la désignation d'extensions.

- Limite nœuds (en anglais *Hop Limit*) : est sur 8 bits. Comme le champ TTL (en anglais *Time to Live – TTL*) de l'en-tête IPv4, cette valeur indique le nombre maximum de nœuds par lesquels peut transiter le paquet. La valeur inscrite dans ce champ est décrémentée à chaque nœud. Le paquet est détruit lorsque cette valeur atteint 0.

- Adresse source (en anglais *Source Address*) : sur 128 bits.

- Adresse de destination (en anglais *Destination Adresse*) : sur 128 bits. Elle n'est pas forcement le destinataire final si un en-tête d'extension est présent.

A part la simplification et l'amélioration de l'en-tête d'un paquet IPv6, le protocole IPv6 a ajouté de nouvelles fonctionnalités pour résoudre les problématiques du protocole IPv4 et pour mieux répondre à la demande de nouvelles applications d'Internet.

Les principales caractéristiques d'IPv6 sont :

1. Adressage hiérarchique et capacité augmentée
2. Auto-configuration d'adresses IPv6
3. En-tête d'extension IPv6 pour optimiser le routage
4. Sécurité
5. Qualité de Service (QoS)

Nous présentons précisément ces principales caractéristiques ci-après:

1. Adressage hiérarchique et capacité augmentée

- **L'espace d'adresses IPv6**

IPv6 dispose d'une adresse sur 128 bits, donc il propose un immense espace d'adresses IPv6 (2^{128} adresses). IPv6 permet ainsi d'éviter l'utilisation du NAT et donc peut promouvoir l'utilisation et le développement des applications temps réels, telles que la Vidéo conférence, la voix sur IP (*en anglais Voice Over Internet Protocol - VoIP*) ou les jeux multi-joueurs, qui fonctionnent mieux de bout-en-bout.

- **Syntaxe des adresses IPv6**

Les adresses IPv4 sont représentées en format décimal à points. L'adresse sur 32 bits est divisée en quatre fois 8 bits. Chaque groupe de 8 bits est converti en son équivalent décimal et séparé par des points. Pour IPv6, l'adresse sur 128 bits est divisée en frontières 16 bits, et chaque bloc de 16 bits est converti en un nombre hexadécimal à 4 chiffres et séparé par deux-points.

Donc, la syntaxe d'adresse IPv6 est la suivante : FE80 : 0 : 0 : 0 : 02AA : 00FF : FE28 : 9C5A

Certains types d'adresses contiennent de longues séquences de zéros. Pour simplifier la représentation d'adresse IPv6, une séquence contiguë de 0 par blocs de 16 bits sont mis à zéro dans le format hexadécimal "deux point" pour être compressée en ":: ".

Par exemple : l'adresse FE80 : 0000 : 0000 : 0000 : 02AA : 00FF : FE28 : 9C5A peut être compressée en FE80 :: 02AA : 00FF : FE28 : 9C5A.

❖ **Préfixes IPv6**

Le préfixe IPv6 est la partie de l'adresse qui indique les bits ayant des valeurs fixes, ou qui représente l'identifiant de réseau. Les préfixes pour IPv6 sont exprimés de la même manière que pour IPv4. Un préfixe IPv6 s'écrit sous la forme "adresse/longueur de préfixe".

Par exemple : le préfixe FE80 :: /64 représente l'adresse lien-local, l'adresse FE80 :: 02AA : 00FF : FE28 : 9C5A est une adresse lien-local (en anglais *Link local Address*).

❖ **Différents types d'adresses IPv6**

Il y a trois types d'adresses IPv6: unicast, multicast et anycast qui sont caractérisées par leur préfixe [RFC 3513].

- Une adresse de type **unicast** désigne une interface unique de réseau IPv6. Un paquet envoyé à une telle adresse sera donc remis à l'interface ainsi identifiée. L'adresse unicast peut être une adresse globale ou une adresse lien-local. Nous les présentons plus tard dans ce paragraphe.

- Une adresse de type **multicast** désigne un groupe d'interfaces qui en général appartiennent à des nœuds différents. Ces différents nœuds peuvent être situés n'importe où dans Internet. Lorsqu'un paquet a pour destination une adresse de type multicast, il est acheminé par le réseau à toutes les interfaces qui sont membres de ce groupe. Son préfixe est FF00 :: /8.

  Par exemple, FF02:0:0:0:0:0:0:1 représente le groupe de tous les nœuds d'un lien-local et FF02:0:0:0:0:0:0:2 représente le groupe de tous les routeurs d'un lien-local.

- Une adresse de type **anycast** désigne un groupe d'interfaces, la différence avec une adresse de type multicast étant que lorsqu'un paquet a pour destination une telle adresse, il est acheminé à un des éléments du groupe et non pas à tous. Son adresse est composée par une partie préfixe et une partie identifiant anycast. La partie préfixe est la même que celle utilisée pour les adresses unicast, et la partie identifiant anycast n'est pas encore complètement définie. Pour l'instant, 0x7E est utilisé pour l'agent mère du protocole IPv6 Mobile. Cette adresse est principalement expérimentale.

Parmi les adresses unicast, on peut distinguer celles qui auront une portée globale, c'est-à-dire désignant sans ambiguïté un nœud sur tous les réseaux IPv6 et celles qui auront une

portée locale, ces dernières ne pourront pas être routées sur Internet. Donc, cette première est appelée l'adresse globale et la deuxième est appelée l'adresse lien-local.

- L'adresse globale, proposée dans le [RFC 3587], précise la structure d'adresse IPv6 définie dans le [RFC 3513] en précisant les tailles de chacun des blocs. Une adresse globale peut être décomposée en plusieurs parties, chaque partie définissant un niveau de hiérarchie différent (Voir la figure 11).

    1. Une topologie publique codée sur 48 bits, allouée par le fournisseur d'accès;

    2. Une topologie de site codée sur 16 bits, ce champ permet de coder les numéros de sous-réseau;

    3. Un identifiant d'interface (64 bits) distinguant les différents nœuds sur le lien.

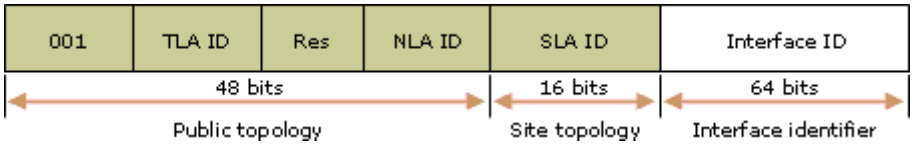


Figure 11 : Adresse globale

Ce modèle hiérarchique a un impact très important sur le routage, car il permet de faire de l'agrégation d'adresses suivant la même hiérarchie. L'utilisation de la hiérarchie au sein des adresses unicast simplifie la structure du réseau et les tables de routage en permettant une agrégation aisée des différentes adresses d'une même organisation.

- L'adresse lien-local est une adresse dont la validité est restreinte à un lien, c'est-à-dire l'ensemble des interfaces directement connectées sous un routeur intermédiaire : par exemple des nœuds branchés sur un même lien Ethernet. L'adresse lien-local peut être configurée automatiquement à l'initialisation de l'interface et permet la communication entre les nœuds voisins sur ce lien. L'adresse est obtenue en concaténant le préfixe FE80 :: /64 aux 64 bits de l'identifiant d'interface. Cette adresse est utilisée par les protocoles d'auto-configuration d'adresses, de Découverte de voisin (en anglais *Neighbor Discovery*) et de Découverte de routeur (en anglais *Router Discovery*) [RFC 4861]. L'adresse lien-local est unique sur un lien. La procédure de Détection d'Adresse Dupliquée (en anglais *Duplicate Address Detection – DAD*) [RFC 4429] [RFC 4862] permet de s'en assurer. Par contre, la duplication d'une adresse lien-local entre deux liens différents ou entre deux interfaces d'un même nœud est autorisée. Un routeur ne doit en aucun cas retransmettre un paquet ayant pour adresse source ou adresse destination une adresse de type lien-local.

L'adresse globale et l'adresse lien-local utilisent toutes les deux un identifiant d'interface sur 64 bits pour désigner un nœud sur un lien. Afin de faciliter l'auto-configuration d'adresses IPv6 et de disposer d'un identifiant unique au niveau d'Internet pour chaque l'interface, plusieurs techniques ont été élaborées. La plus répandue est la proposition de

IEEE qui permet de construire un identifiant d'interface sur 64 bits en utilisant l'adresse MAC du nœud [EUI-64]. Pour créer un identifiant d'interface du format EUI-64, une valeur 0XFFFE sur 16bits est insérée dans l'adresse MAC entre l'identifiant du constructeur sur 24 bits et l'identifiant du numéro de séries sur 24 bits, les 2 bits u (septième bit du premier octet) et g (huitième bit du premier octet) ont les valeurs 1 et 0 respectivement. La figure 12 présente la transformation d'adresse MAC en identifiant d'interface selon la méthode EUI-64. Pour mieux montrer cette transformation, les 2 bits u et g sont marqués comme 0 dans l'adresse MAC dans la figure.

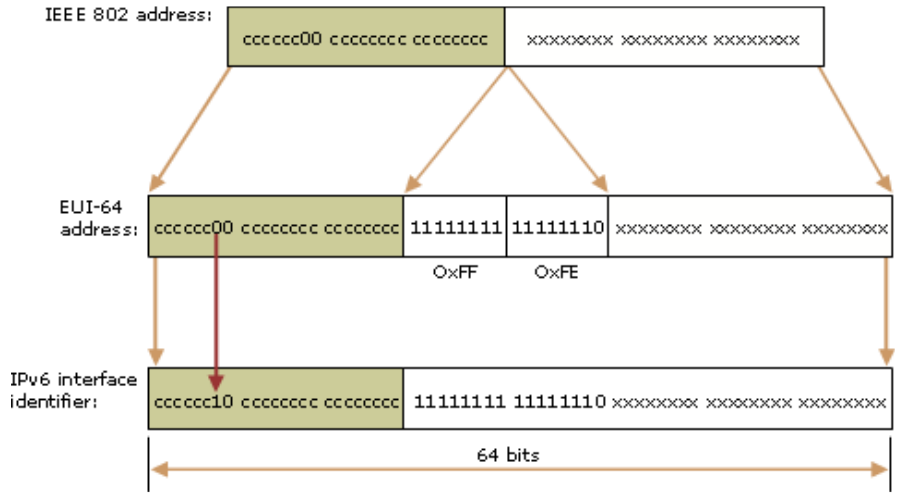


Figure 12 : Transformation d'adresse MAC en Identifiant d'Interface

La méthode EUI-64 permet de réduire à une valeur proche de zéro la probabilité de conflits d'adresse dans un réseau. Mais il existe le problème de sécurité pour cette méthode. L'adresse MAC d'un nœud peut être déduite de son adresse IPv6. De plus, si le nœud ne possède aucune adresse MAC, il ne peut pas utiliser cette méthode pour créer un identifiant d'interface.

En dehors de cette méthode, on peut également choisir une valeur aléatoire pour garantir plus de confidentialité ou au contraire la dériver d'une clé publique pour mieux authentifier le nœud.

2. Auto-configuration d'adresses IPv6

Le protocole IPv6, contrairement au protocole IPv4, prévoit la possibilité pour un nœud d'auto-configurer son adresse dans un réseau.

IPv6 spécifie deux méthodes d'auto-configuration d'adresses globale : l'auto-configuration d'adresses avec état et l'auto-configuration d'adresses sans état.

- L'auto-configuration d'adresses avec état (en anglais *Stateful Address Autoconfiguration*): Son fonctionnement s'appuie sur le protocole DHCPv6 (en anglais *Dynamic Host Configuration Protocol for IPv6*) [RFC 3315], qui est construit sur une architecture client/serveur. C'est le serveur DHCP qui procure les paramètres de configuration, tels que les adresses, le routage, le DNS, aux clients

lorsque ces derniers en font la demande. Avec ces informations, les clients peuvent configurer leur interface réseaux et communiquer. Il est important de noter que l'ensemble des échanges DHCP sont toujours à l'initiative des clients. Le serveur ne fait que répondre à des demandes, il n'est jamais l'initiateur d'un échange. L'auto-configuration d'adresses avec état est retenue lorsqu'un site demande un contrôle strict de l'attribution des adresses. Mais la procédure DHCP nécessite plusieurs échanges de messages de signalisation entre le serveur et le client. De plus, le client doit parfois avoir une adresse lien-local et procéder la procédure DAD pour vérifier l'unicité de son adresse lien-local avant d'envoyer la requête auprès du serveur DHCP, en outre, le client doit aussi procéder la procédure DAD pour vérifier l'unicité d'adresse globale attribuée par le serveur DHCP avant de pouvoir l'utiliser [LI07]. Tout cela n'est pas adaptable pour les clients mobiles qui s'accommodent mal de ces lourdes procédures. En effet, lorsqu'un client mobile vient de changer de réseau, il doit obtenir et utiliser aussitôt que possible une adresse temporaire CoA (en anglais *Care-of Address – CoA*) dans ce nouveau réseau pour maintenir ses communications en cours.

- L'auto-configuration d'adresses sans état (en anglais *Stateless Address Autoconfiguration*) [RFC 4862]: Elle consiste pour le client d'un réseau à obtenir une adresse IP de manière autonome, sans la nécessité d'une intervention humaine ou d'un serveur DHCP. La procédure se décompose en trois parties: la création d'une adresse lien-local, la vérification de son unicité et la détermination d'une adresse globale à l'aide du message – Annonce de routeur (en anglais *Router Advertisement*) [RFC 4861]. L'auto-configuration d'adresses sans état est typiquement utilisée quand la gestion administrative des adresses attribuées n'est pas nécessaire au sein d'un réseau. Grâce à sa simplicité et son autonomie, l'auto-configuration d'adresses sans état est choisie par le protocole IP Mobile pour que le client mobile puisse auto-configurer aussitôt que possible son adresse temporaire dans un nouveau réseau. Nous décrivons le protocole IP Mobile dans le paragraphe suivant.

Avant d'expliquer la procédure d'auto-configuration d'adresses sans état, nous vous rappelons la structure d'adresse IPv6 globale décrite dans le paragraphe précédent. L'adresse IPv6 globale sur 128 bits est divisée en deux parties de 64 bits chacune. La première partie est le préfixe du réseau qui identifie le réseau sur lequel le nœud se trouve, et la deuxième partie est l'identifiant d'interface qui identifie l'interface d'un nœud dans le réseau. L'adresse IPv6 globale d'un nœud sur un réseau consiste à marier le préfixe de ce réseau avec son identifiant d'interface.

Auto-configuration d'adresses sans état

La procédure d'auto-configuration d'adresses sans état est décomposée en trois phrases: la phase de création d'adresse lien-local, la phase de vérification de l'unicité d'adresse lien-local et la phase de détermination d'adresse globale :

Quand un nœud se connecte à un nouveau réseau ou est à l'initialisation de son interface, le nœud génère un identifiant pour l'interface. Cet identifiant d'interface est construit généralement par la méthode EUI-64. Grace à cet identifiant d'interface, l'adresse lien-local

de ce nœud est constituée. Pourtant, le nœud ne peut pas encore l'utiliser, car il ne sait pas si cette adresse lien-local est déjà utilisée par un autre nœud de ce même réseau ou non. Cette adresse possède un état provisoire, puis le nœud doit vérifier l'unicité de son adresse lien-local dans son réseau par le moyen de la procédure DAD avant de pouvoir l'utiliser [RFC 4862]. L'adresse est qualifiée d'adresse provisoire pendant l'exécution de la procédure DAD et ce jusqu'à la confirmation de son unicité.

La procédure DAD est réalisée à l'aide du protocole Découverte de voisins pour IPv6 (en anglais *Neighbor Discovery for IPv6*) [RFC 4861]. Elle utilise les messages de type ICMPv6 – Sollicitation de voisin (en anglais *Neighbor Solicitation – NS*) et Annonce de voisin (en anglais *Neighbor Advertisement – NA*) pour prouver l'unicité d'adresse lien-local dans un réseau.

Le nœud envoie un message "Sollicitation de voisin" avec l'adresse multicast de l'adresse provisoire dans le champ de l'adresse de destination, l'adresse indéterminée dans le champ de l'adresse source et son adresse provisoire dans le champ de l'adresse ciblée de l'en-tête d'extension. Le nœud envoie DupAddrDetectTransmits fois (par défaut 1 fois) le message "Sollicitation de voisin" pour exécuter la procédure DAD. L'intervalle entre les messages consécutifs est de RetransTimer milliseconde (par défaut 1000 milliseconde) si DupAddrDetectTransmits est plus que 1. Par ailleurs, RetransTimer est aussi le temps qu'un nœud doit attendre après l'envoi du dernier message "Sollicitation de voisin" et avant d'achever la procédure DAD [RFC 4862].

Il faut noter que le nœud doit joindre le groupe d'adresse multicast de tous les nœuds et le groupe d'adresse multicast de l'adresse provisoire avant d'envoyer le message "Sollicitation de voisin"[RFC 3513]. Le premier s'assure que le nœud reçoit le message "Annonces de Voisin" des autres nœuds qui utilisent déjà cette adresse; et le dernier s'assure que deux nœuds essayant d'utiliser la même adresse simultanément devraient détecter la présence de chacun. Pour joindre le group de l'adresse multicast, le nœud doit envoyer typiquement un message – Découverte d'auditeur multicast (en anglais *Multicast Listener Discovery – MLD*) [RFC3810] pour l'adresse multicast au routeur de son réseau. Cependant, ce message ne peut pas être envoyé immédiatement quand le nœud vient de se connecter à un nouveau réseau ou que son interface vient d'être initialisée. Un délai doit être respecté avant l'envoi de ce message. Ceci sert à alléger la congestion lorsque beaucoup de nœuds sont allumés sur un réseau en même temps, comme après une panne de courant. Cela peut aussi aider à éviter d'avoir plus d'un nœud essayant de solliciter la même adresse en même temps. Le délai est choisi aléatoirement entre *(0, MAX_RTR_SOLICITATION_DELAY). MAX_RTR_SOLICITATION_DELAY* est une variable, sa valeur est de 1 seconde par défaut [RFC 4861].

Une fois que le message "Sollicitation de voisin" est envoyé par le nœud, trois possibilités se présentent :

- Si l'adresse provisoire est utilisée comme une adresse validée par un autre nœud, un message "Annonce de voisin" sera reçu par ce nœud. Donc, le nœud réalise que son adresse lien-local n'est pas unique et qu'il ne peut pas l'utiliser. Par conséquent, la procédure d'auto-configuration d'adresses sans état s'arrête et une intervention manuelle est nécessaire.

- Si un autre nœud veut aussi utiliser cette adresse provisoire, c'est-à-dire que l'adresse provisoire est également une adresse provisoire pour un autre nœud, un message "Sollicitation de voisin" dans le cadre d'une procédure DAD est aussi reçu par ce nœud. L'adresse provisoire ne peut être utilisée par aucun des nœuds.

- Si rien n'est reçu au bout de 1000 millisecondes (la valeur de RetransTimer par défaut) [RFC 4861], cela signifie que l'adresse provisoire est unique. Cette adresse passe de l'état de provisoire à celui de valide et elle est assignée à l'interface de ce nœud. Le nœud peut utiliser cette adresse.

La première phase de l'auto-configuration d'adresses sans état est achevée. Le nœud a auto-configuré son adresse lien-local et a utilisé la procédure DAD pour vérifier l'unicité de son adresse lien-local. Toutefois, la procédure DAD n'offre pas une fiabilité absolue, notamment lorsque le lien est coupé.

La phase suivante a pour objectif d'obtenir le préfixe du réseau et les autres paramètres de configuration afin de constituer une adresse globale. Le nœud acquiert ces informations au moyen du message – Annonce de routeur (en anglais *Router Advertisement – RA*) envoyé par le routeur de ce réseau [RFC 4861].

Il y a deux types de messages "Annonce de routeur" – l'Annonce de routeur non-sollicitée et l'Annonce de routeur sollicitée.

- L'Annonce de routeur non-sollicitée : c'est le routeur qui diffuse un message "Annonce de Routeur" périodiquement sans la demande des nœuds dans le réseau.

- L'Annonce de routeur sollicitée : c'est le routeur qui diffuse un message "Annonce de routeur" à la demande des nœuds dans le réseau. Le nœud envoie un message "Sollicitation de routeur" au routeur pour lui demander d'envoyer le message "Annonce de routeur" au plus vite.

Le nœud doit recevoir le message "Annonce de routeur" pour auto-configurer son adresse globale. Mais l'envoi du message "Annonce de routeur" ne peut pas se faire à tout moment. Chaque routeur doit utiliser son propre temporisateur pour envoyer le message "Annonce de routeur non-sollicitée". Le temporisateur choisit une valeur aléatoire uniformément distribuée entre (*MinRtrAdvInterval*, *MaxRtrAdvInterval*) seconde. L'expiration du temporisateur donne lieu à l'envoi du message "Annonce de routeur non-sollicitée". Une fois que le message "Annonce de routeur non-sollicitée" est envoyée, le temporisateur doit choisir une nouvelle valeur aléatoire pour le prochain envoi. L'intervalle entre les envois est aléatoire afin de réduire la probabilité de synchronisation avec les messages "Annonce de routeur" envoyés par d'autres routeurs sur le même lien. Par contre, lorsque le routeur vient d'être initialisé, le délai de premier envoi du message "Annonce de routeur non sollicitée" ou l'intervalle entre les *MAX_INITIAL_RTR_ADVERTISEMENTS* fois envois consécutifs ne peut pas dépasser *MAX_INITIAL_RTR_ADVERT_INTERVAL* seconde (la valeur par défaut est de 16 secondes) [RFC 4861]. Cette limite est pour que le routeur puisse être découvert par les nœuds aussitôt qu'il devient disponible dans le réseau. Les

descriptions des paramètres – *MinRtrAdvInterval*, *MaxRtrAdvInterval* vont être présentées dans le paragraphe suivant.

Généralement, l'intervalle entre les messages "Annonce de routeur non-sollicitée" successifs est plus long que le temps qu'un nœud pourrait attendre [RFC 4861]. Donc, le nœud peut envoyer le message "Sollicitation de routeur" (en anglais *Router Solicitation – RS*) au routeur pour lui demander d'envoyer le message "Annonce de routeur" au plus vite. Le message envoyé par le routeur à la demande du nœud est dénommé "Annonce de routeur sollicitée". En outre, dès l'instant que le nœud se connecte à un nouveau réseau ou que son initialisation est accomplie, il doit attendre un délai aléatoire tiré entre *(0, MAX_RTR_SOLICITATION_DELAY)* seconde avant d'envoyer son premier message "Sollicitation de routeur"[RFC 4861]. Ceci sert à alléger la congestion quand beaucoup de nœuds sont allumés sur un réseau en même temps. Toutefois, si le nœud a déjà passé un délai après son (re)initialisation (par exemple, la procédure DAD), il peut envoyer son premier message "Sollicitation de routeur" sans tarder. De plus, le nœud ne peut pas envoyer plus de *MAX_RTR_SOLICITATIONS* fois le message "Sollicitations de routeur". L'intervalle entre ces envois ne peut pas être plus court que *RTR_SOLICITATION_INTERVAL* seconde. Une fois que le nœud reçoit le message "Annonce de routeur", il s'arrête d'envoyer le message "Sollicitation de routeur". Cependant, si le nœud a déjà envoyé plus de *MAX_RTR_SOLICITATIONS* fois le message "Sollicitations de routeur" et qu'il a déjà attendu *MAX_RTR_SOLICITATION_DELAY* seconde après l'envoi du dernier message "Sollicitation de routeur" et qu'il n'a toujours pas reçu le message "Annonce de routeur", il peut conclure qu'il n'y a aucun routeur dans le réseau et qu'il ne peut pas créer une adresse globale.

Quant au routeur, il doit retarder un délai aléatoire tiré entre *(0, MAX_RA_DELAY_TIME)* seconde avant d'envoyer le message "Annonce de routeur sollicitée". De plus, le routeur se permet d'envoyer le message "Annonce de routeur sollicitée" avec un intervalle plus court que celui décidé par le paramètre *MinRtrAdvInterval*. Pourtant, le message "Annonce de routeur non-sollicitée" ne peut pas être envoyé avec un intervalle plus court que celui décidé par *MinRtrAdvInterval*. En tous cas, l'intervalle de tous les types de message "Annonce de routeur" ne peut pas être inférieur à *MIN_DELAY_BETWEEN_RAS* seconde.

D'ailleurs, étant donné qu'un routeur retarde parfois l'envoi du message "Annonce de routeur" de quelques secondes, le délai de la procédure d'auto-configuration d'adresses peut être excessivement long dans le cas où toutes les phases sont exécutées étape par étape. Pour accélérer la procédure d'auto-configuration d'adresses sans état, un nœud peut générer son adresse lien-local et vérifier son unicité tout en attendant le message "Annonce de routeur" pour créer son adresse globale.

Comme nous le décrivons ci-dessus, pour auto-configurer une adresse globale, le délai total nécessaire pour le nœud est le suivant:

$$\mathbf{T_{Total} = T_{joint} + T_{DAD} + T_{\text{délai de la réception du message "Annonce de routeur"}}}$$

Dont,

$\mathbf{T_{joint}}$: est le délai que le nœud doit attendre pour joindre un groupe de multicast. Elle est une valeur aléatoire tirée entre (0, 1) seconde.

$\mathbf{T_{DAD}}$: est le délai de la procédure DAD. La valeur minimum est de 1 seconde.

$\mathbf{T_{\text{délai de la réception du message "Annonce de routeur"}}}$: est le délai de la réception du message "Annonce de Routeur". Le délai minimum est de 0 seconde dans le cas où nous considérons que le nœud reçoit le message "Annonce de Routeur non-sollicitée" pendant la procédure DAD. Le délai maximum est la valeur maximum entre (*MIN_DELAY_BETWEEN_RAS* – le temps passé depuis le dernier envoi du message "Annonce de routeur") et *MAX_RA_DELAY_TIME* dans le cas où nous considérons que le nœud envoie le message "Sollicitation de routeur" sans attendre un délai aléatoire tiré entre (0, 1) seconde après la procédure DAD. Si nous supposons que le routeur a envoyé le message "Annonce de routeur" justement avant de recevoir le message "Sollicitation de routeur", la valeur *MIN_DELAY_BETWEEN_RAS* est de 3 secondes, donc, le délai maximum est de 3 secondes.

Nous avons le délai total de la procédure d'auto-configuration d'adresses sans état :

$\mathbf{T_{Total}}$ (min) = $\mathbf{T_{joint}} + \mathbf{T_{DAD}} + \mathbf{T_{\text{délai de la réception du message "Annonce de routeur"}}}$ = 0 + 1 + 0 seconde = 1 seconde
$\mathbf{T_{Total}}$ (max) = $\mathbf{T_{joint}} + \mathbf{T_{DAD}} + \mathbf{T_{\text{délai de la réception du message "Annonce de routeur"}}}$ = 1 + 1 + 3 secondes = 5 secondes

Nous constatons que $\mathbf{T_{DAD}}$ représente un délai important et non-compressible pour la procédure d'auto-configuration d'adresses sans état et que le délai de la réception du message "Annonce de routeur" est parfois trop long.

Plusieurs propositions sont faites pour éviter la procédure DAD ou réduire le temps de la phase d'Auto-configuration d'adresses. [RFC 4429] permet au nœud d'utiliser l'adresse avant d'achèvement de la procédure DAD. Si l'adresse est déjà utilisée, le nœud doit changer son adresse immédiatement. Cette méthode est basée sur la faible probabilité de duplication d'adresse. Cependant, cela pénalise tous les deux nœuds en cas de collision d'adresse. [Han04] permet au routeur de maintenir un pool d'adresse unique et d'attribuer une adresse au nœud lorsque le dernier s'attaché au réseau. Le nœud diffuse une requête – "Sollicitation de routeur" et devrais attendre un temps pour avoir la réponse – "Annonce de routeur" du routeur. Ce temps est négligeable.

3. En-tête d'extension IPv6 pour optimiser le routage

En raison que le format d'en-tête IPv6 est simplifié, le protocole IPv6 définie les en-têtes d'extension IPv6 pour supporter les nouvelles fonctionnalités d'IPv6. Ces en-têtes d'extension peuvent être vus comme un prolongement de l'encapsulation d'un paquet IP dans un paquet IP.

Un en-tête d'extension a une taille multiple de 64 bits. Le champ d'en-tête suivant de l'en-tête IPv6 définit le type d'en-tête d'extension : un autre en-tête d'extension ou un protocole de la couche supérieur. Le tableau 4 présente les différentes valeurs du champ l'en-tête

suivant et ses correspondances. Les différents en-têtes d'extension sont décrits dans [RFC 2460]. À part que l'en-tête d'extension de proche-en-proche et l'en-tête d'extension de routage de type 0 sont traités par tous les routeurs intermédiaires, les autres en-têtes d'extension ne sont pris en compte que par le récepteur des paquets.

Tableau 3 : Valeurs du champ en-tête suivant

Valeur	En-tête d'extension	Valeur	Protocole
0	Proche-en-proche	4	IPv4
43	Routage	6	TCP
44	Fragmentation	17	UDP
50	Confidentialité	41	IPv6
51	Authentification	58	ICMPv6
59	Fin des en-têtes	132	SCTP
60	Destination	135	Mobilité

4. Protocole de sécurité utilisé dans le protocole IPv6

Il y a plusieurs protocoles de sécurité normalisés et utilisés dans le réseau qui fonctionne aux différentes couches de l'architecture d'ISO. Les protocoles plus connus sont [VAN05]:

- Le protocole SSL, spécifié pour le web à la couche Transport.
- Le protocole S-RTP, assure l'application temps réel à la couche Transport.
- Le protocole IPSec, introduit des mécanismes de sécurité à la couche Réseau.
- Le protocole L2TP, offre un tunnel à la couche Liaison.

Parmi ces différents protocoles de sécurité, le protocole IPSec est plus répandu et plus utilisé parce qu'il est le seul protocole qui peut répondre aux diverses applications, accepter les deux protocoles de transport UDP et TCP et assurer les services de sécurité complets (confidentialité, authentification, intégralité). IPSec propose également différents mécanismes (AH ou ESP) et modes de fonctionnement (transport ou tunnel) correspondant aux différents niveaux de sécurité [NOR03].

L'utilisation des propriétés d'IPSec est optionnelle dans IPv4 et obligatoire dans IPv6. De plus, grâce à la disparition des NAT, IPSec peut être utilisé pour une sécurité de bout en bout dans IPv6.

5. QoS

IPv6 présente également plusieurs avantages permettant de mieux gérer la QoS mais qui ne sont pas encore significatifs. De manière générale, la QoS est gérée de la même façon sous IPv6 que ce que aujourd'hui sous IPv4. Cependant, les applications temps réel, telles que la Vidéo conférence, la VoIP, pourraient trouver un réel intérêt dans IPv6, du fait de son nombre d'adresses qui permet d'éviter d'avoir recours au NAT qui nuisent à ce type de services. Nous allons présenter la QoS dans le chapitre 5.

Comme nous avons présenté, le protocole IPv6 apporte un certain nombre d'améliorations fonctionnelles par rapport au protocole IPv4. Surtout, les nouvelles fonctions, telles que l'auto-configuration d'adresses et la découverte de voisin, permettent de simplifier la gestion du réseau. De plus, le nouveau format d'en-tête IPv6 permet d'optimiser le routage et permet aussi aux routeurs d'avoir de meilleures performances dans leurs traitements des paquets.

2.2 Protocole IP Mobile

Le protocole IP identifie un nœud sur Internet d'une manière unique grâce à son adresse IP. L'adresse IP est composée de deux parties : le préfixe qui détermine le réseau sur lequel le nœud se trouve, et l'identifiant de ce nœud sur son réseau. Internet est un réseau à grande échelle, c'est la raison pour laquelle que chaque routeur ne peut mémoriser qu'une route vers tous les nœuds qui y sont attachés. Les routeurs ne stockent que des entrées correspondant à des réseaux en considérant que des paquets destinés à des nœuds ayant le même préfixe seront tous routés d'une manière identique.

Dans ce contexte, la mobilité du nœud introduit un nouveau problème de routage : le Nœud Mobile (en anglais *Mobile Node – MN*) se déplace d'un réseau vers un autre réseau. S'il ne change pas son adresse IP, il aura un différent préfixe sur ce nouveau réseau. Cependant, le nœud doit être situé sur un réseau avec le même préfixe indiqué par son adresse IP afin de pouvoir recevoir les paquets qui lui sont destinés. Pour qu'un MN puisse changer de réseau et garder la connexion à Internet, il doit changer d'adresse IP à chaque fois qu'il change du réseau. Mais une fois que le MN change son adresse IP, il ne peut plus conserver les communications en cours au niveau de la couche transport ou des couches supérieures.

Pour qu'un MN puisse maintenir les communications en cours et garder la connexion à Internet tout en se déplaçant d'un réseau vers l'autre, le protocole IP Mobile propose de gérer la mobilité du MN au niveau IP. Il permet au MN d'utiliser deux adresses IP et un mécanisme de Mise à jour d'association (en anglais *Binding Update – BU*) pour masquer le changement d'adresses IP aux applications exécutées entre le MN et ses correspondants. Par conséquent, les communications en cours peuvent être maintenues lorsque le MN change du réseau.

Avant d'expliquer le fonctionnement du protocole IP Mobile, nous présentons d'abord son architecture et ses composants.

La figure 13 présente l'architecture du protocole IP Mobile:

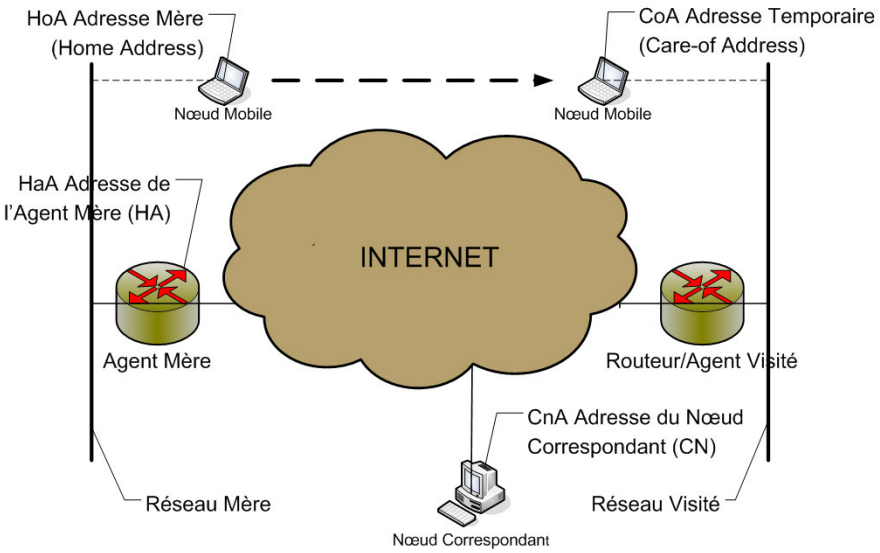


Figure 13 : Architecture du protocole IP Mobile

- Nœud Mobile (en anglais *Mobile Node – MN*) : un terminal qui peut changer de point d'attachement d'un réseau à un autre.

- Adresse Mère (en anglais *Home Address – HoA*) : est l'adresse IP du MN sur son réseau mère. Elle permet d'identifier le MN de façon unique sur tous les réseaux.

- Adresse Temporaire (en anglais *Care-of Address – CoA*): permet de localiser le MN sur un réseau visité afin de lui permettre d'envoyer et recevoir des paquets sur ce réseau.

- Agent Mère (en anglais *Home Agent – HA*) : correspond à un routeur particulier situé dans le réseau mère. Il est chargé d'assurer l'association entre l'adresse mère et l'adresse temporaire du MN lorsque celui-ci est attaché à un réseau visité. Cet agent est également chargé de rediriger les paquets IP à destination de l'adresse mère du MN vers son adresse temporaire sur son réseau visité.

- Nœud Correspondant (en anglais *Correspondant Node – CN*) : est un terminal qui communique avec le MN.

- Réseau Mère : est un réseau auquel le MN et son HA s'attachent.

- Réseau Visité : est un réseau autre que le réseau mère pour un MN. Le MN aura une adresse temporaire quand il s'attache à ce réseau.

- Agent Visité (en anglais *Foreign Agent – FA*) : correspond à un routeur du réseau visité auquel le MN est attaché. Il fournit des services de routage au MN lorsque le MN est enregistré auprès de lui. Il est utilisé uniquement dans le protocole IPv4 Mobile.

Par la suite, nous présentons le fonctionnement du protocole IPv4 Mobile et du protocole IPv6 Mobile dans les paragraphes suivants. Nous détaillons assez précisément le protocole IPv4 Mobile, parce que le protocole IPv6 Mobile en est issu.

2.2.1 Protocole IPv4 Mobile

Quand un MN se trouve sur son réseau mère, il communique de la même manière que n'importe quel nœud sur Internet en utilisant son adresse mère comme son adresse source. Les paquets qui lui sont destinés comprennent son adresse mère comme son adresse de destination et sont routés en fonction du préfixe du réseau mère. Le HA est inactif pour le MN.

Lorsque le MN est attachée à un réseau visité, il devrait d'abord obtenir une adresse temporaire. Le protocole IPv4 Mobile permet au MN d'utiliser deux différents types d'adresses temporaires:

- Le MN utilise l'adresse IP publique de l'agent visité comme son adresse temporaire. L'agent visité attribue une adresse IP privée au MN pour le localiser sur son réseau. L'agent visité fonctionne comme un relais entre le HA et le MN. C'est lui qui reçoit les paquets envoyés par le HA et les redirige au MN. Ce mécanisme peut être comparé au système de translation d'adresses (en anglais *Network Address Translation – NAT*). L'utilisation de ce type d'adresse temporaire est préférable dans le protocole IPv4 Mobile car elle permet aux nombreux MNs de partager une même adresse temporaire publique et qu'elle évite d'allouer les nouvelles adresses IP publiques aux MNs à cause de la pénurie des adresses IPv4 publiques.

- Le MN auto-configure son adresse temporaire publique avec le serveur DHCP. Le MN utilise cette adresse publique sur le réseau visité, donc le HA n'envoie plus les paquets vers son agent visité, mais les envoie directement vers son adresse temporaire publique. Dans ce cas, l'agent visité fonctionne comme un routeur d'accès (en anglais *Access Router – AR*). L'utilisation de ce type d'adresse temporaire permet au MN de fonctionner sans l'agent visité, mais elle demande toutefois la réservation d'un pool d'adresses IP publiques pour les MNs et elle pose un problème au niveau de l'espace d'adresses d'IPv4.

Une fois que le MN a eu l'adresse temporaire, il doit mettre à jour l'association entre son adresse mère et son adresse temporaire avec le HA. En fait, le HA maintient une table d'associations contenant l'association entre l'adresse mère et l'adresse temporaire 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 l'adresse de l'agent visité, il envoie d'abord le message – Requête d'enregistrement (en anglais *Registration Request*) à son agent visité. Ensuite, l'agent visité vérifie la validité du message "Requête d'enregistrement", met à jour sa table d'associations et retransmet ce message au HA. Le HA reçoit ce message, réactualise sa table d'associations et envoie un message – Réponse d'enregistrement (en anglais *Registration*

Reply) au MN via l'agent visité. Si le MN utilise une adresse temporaire publique, il échange directement les messages avec le HA sans impliquer l'agent visité.

Quelle que soit l'adresse temporaire utilisée par le MN, dès que le HA reçoit le message "Requête d'enregistrement", il diffuse une requête ARP (en anglais *Address Resolution Protocol – ARP*) sur son réseau. Ceci permet au HA d'associer son adresse MAC avec l'adresse mère du MN afin de pouvoir intercepter tous les paquets destinés à l'adresse mère du MN.

Les figures 14, 15, 16,17 sont présentées pour expliquer le mécanisme de routage de paquets triangulaire géré par le protocole IPv4 Mobile lorsque le MN utilise une adresse temporaire publique dans le réseau visité.

La figure 14 présente la situation dans laquelle le MN est connecté à un réseau visité et a obtenu une adresse temporaire publique sur ce nouveau réseau visité et que le CN continue d'envoyer les paquets à l'adresse mère du MN.

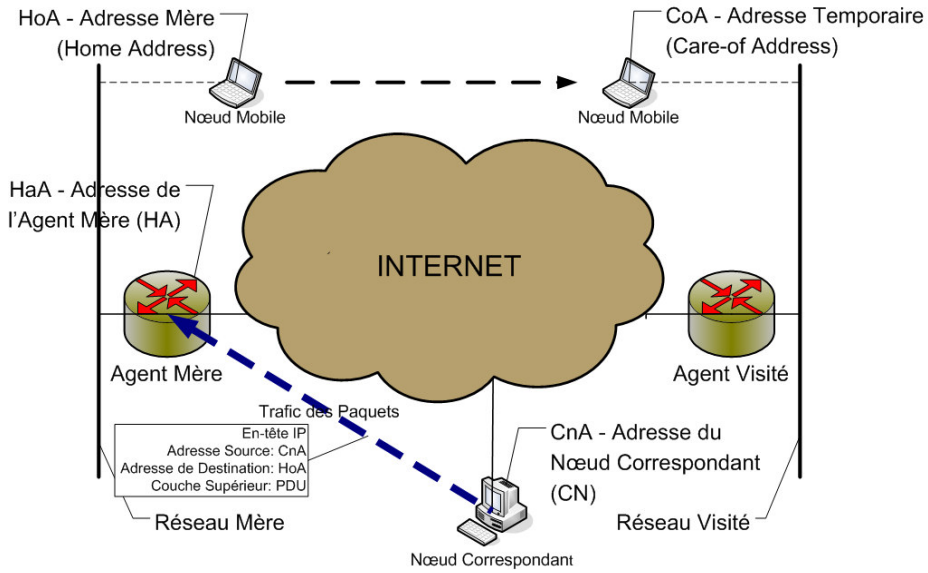


Figure 14 : Paquets envoyés par le CN à l'adresse mère du MN

La figure 15 présente la situation dans laquelle le HA encapsule les paquets interceptés et les redirige à l'adresse temporaire publique du MN via le tunnel IPSec. Le tunnel IPSec est créé d'une manière optionnelle pour protéger les paquets transmis. Comme il est inconcevable que le HA modifie les paquets interceptés, les paquets d'origine sont justement encapsulés en ajoutant un nouvel en-tête IP devant l'en-tête existant. Le nouvel en-tête contient l'adresse du HA comme adresse source, et l'adresse temporaire du MN comme adresse destinataire. Le paquet encapsulé peut atteindre le réseau visité puisque l'adresse temporaire a un préfixe comme celui du réseau visité. Ce procédé permet de continuer à utiliser le mécanisme de routage IP conventionnel tout en permettant une redirection des paquets.

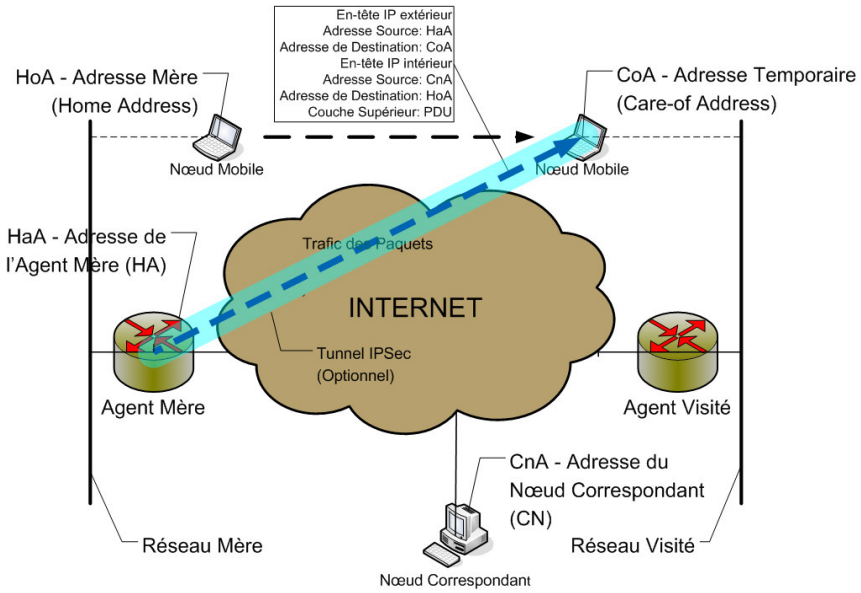


Figure 15 : Paquets interceptés, encapsulés et redirigés par le HA au MN via le tunnel IPSec

Les paquets issus du MN sur un réseau visité et à destination du CN utilisent un principe similaire. Les paquets IP d'origine comportent comme adresse source l'adresse mère du MN et comme adresse destination celle du CN. Ensuite les paquets IP d'origine sont encapsulés par le MN lui-même, l'adresse source de l'en-tête extérieure est l'adresse temporaire du MN et l'adresse destination de l'en-tête extérieure est l'adresse du HA. Les paquets transmis entre le MN et le HA sont aussi protégés par le protocole IPSec, ils traversent les routeurs intermédiaires jusqu'au HA. Ce processus est présenté dans la figure 16.

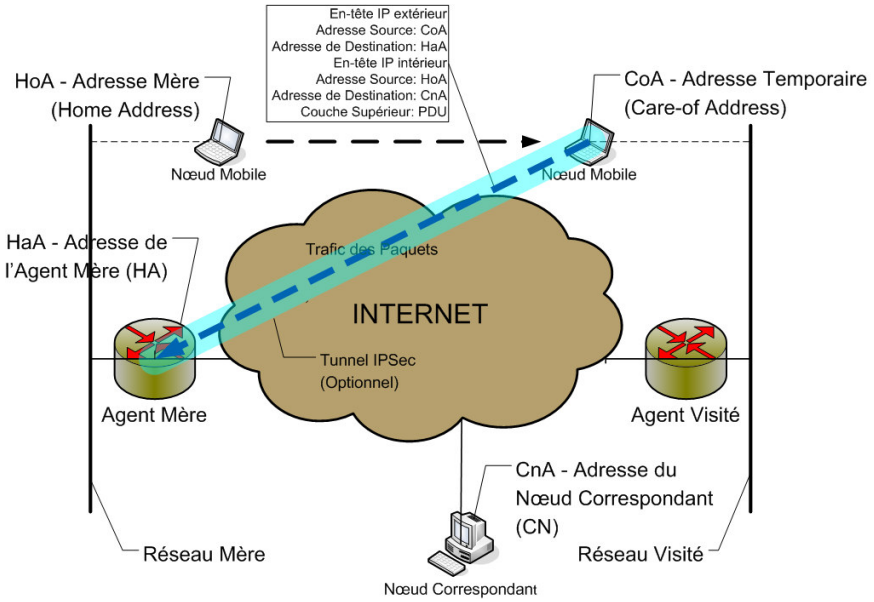


Figure 16 : Paquets encapsulés et envoyés par le MN au HA via tunnel IPSec

Une fois que le HA a reçu les paquets, il supprime l'en-tête extérieur des paquets et redirige les paquets au CN. Le CN reçoit les paquets du MN comme si le MN était dans le réseau mère.

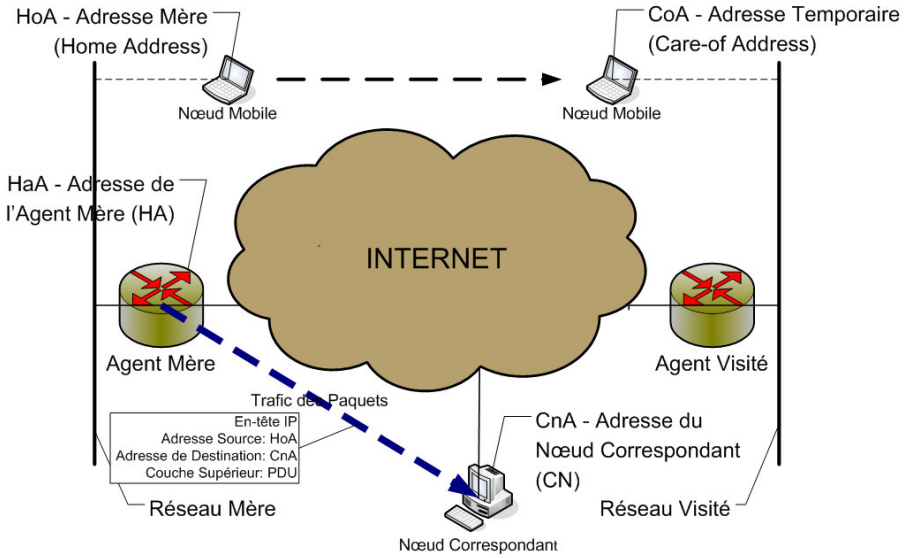


Figure 17 : Paquets désencapsulés et redirigés par le HA au CN

Les figures ci-dessus présentent la situation dans laquelle le MN a acquis une adresse temporaire publique par le mécanisme DHCP. Il se trouve lui-même à l'extrémité du tunnel et décapsule les paquets qui traversent le tunnel et arrivent à lui. Si le MN utilise l'adresse de l'agent visité comme son adresse temporaire, c'est donc l'agent visité qui est à l'extrémité du tunnel. Lorsque l'agent visité reçoit les paquets tunnelés, il les décapsule et remet le paquet d'origine au MN.

En conclusion de notre description, grâce à l'utilisation du protocole IPv4 Mobile, le MN peut se déplacer sur le réseau sans interrompre la communication en cours, cependant, la gestion de la mobilité par le protocole IPv4 Mobile implique des problèmes de performances: 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; les paquets doivent suivre un chemin triangulaire pour être acheminé à destination, cela ajoute un délai d'acheminement supplémentaire significatif. Par conséquent, il est difficile de garantir la qualité de service requise pour les applications temps réel.

D'ailleurs, comme nous l'avons décrit dans le premier chapitre, le déplacement d'un MN dans le réseau Wi-Fi entraine parfois un changement d'AP, plus précisément, le MN se déconnecte d'abord de son AP précédent, cherche ensuite les nouveaux APs disponibles qui sont à sa portée et se connecte finalement à un nouveau AP, avec lequel il a une meilleure réception du signal. Le fait qu'un MN change physiquement son point d'accès au réseau est baptisé le handover de niveau 2. Si les deux points d'accès se situent sur des réseaux différents, le changement d'AP provoque aussi un changement de réseau pour le MN, on dénomme généralement cette situation, le handover de niveau 3, en fait, le MN devrait changer son réseau d'attachement et son adresse IP pour maintenir la connexion à Internet. La procédure du handover de niveau 2 est gérée par la norme IEEE 802.11, cependant celle de niveau 3 est gérée par le protocole IP Mobile. Parce que le handover de

niveau 2 n'implique pas forcement le handover de niveau 3, un mécanisme pour détecter le changement de réseau devrai être implémenté pour repérer le déclenchement du handover de niveau 3. Cependant, le protocole IPv4 Mobile n'a pas défini ce type de mécanisme.

2.2.2 Protocole IPv6 Mobile

Le protocole IPv6 Mobile est proposé pour résoudre les problèmes cités ci-dessus en utilisant les nouvelles fonctionnalités du protocole IPv6. Le mécanisme de Détection de mouvement permet au MN de détecter le changement de réseau. Le mécanisme d'Auto-configuration d'adresses sans état permet au MN d'acquérir une adresse IPv6 globale aussitôt qu'il s'attache à un nouveau réseau visité. Le support du mécanisme de Mise à jour d'association pour CN et l'utilisation du nouvel en-tête IPv6 permet au MN et au CN de pouvoir communiquer directement sans passer par le HA. Nous expliquons en détail dans le paragraphe suivant comment le protocole IPv6 Mobile gère mieux la mobilité des MNs dans les réseaux IPv6.

Nous présentons d'abord les nouveaux messages de signalisation du protocole IPv6 Mobile, ensuite nous expliquons la gestion de la mobilité par ce protocole.

2.2.2.1 Messages de signalisation du protocole IPv6 Mobile

Le protocole IPv6 Mobile définit un en-tête d'extension de mobilité pour les nouveaux messages de signalisation, tels que le Mise à jour d'association (en anglais *Binding Update – BU*), l'Acquittement de mise à jour d'association (en anglais *Binding Acknowledgement – BA*), l'Initialisation de test d'adresse mère (en anglais *Home Address Test Init – HoTI*), etc. La valeur du champ d'en-tête suivant de l'en-tête IPv6 est défini comme 135, c'est-à-dire il y a un en-tête d'extension de mobilité dans le paquet IPv6.

Le format général d'en-tête d'extension de mobilité est donné dans la figure 18 [RFC 3775]:

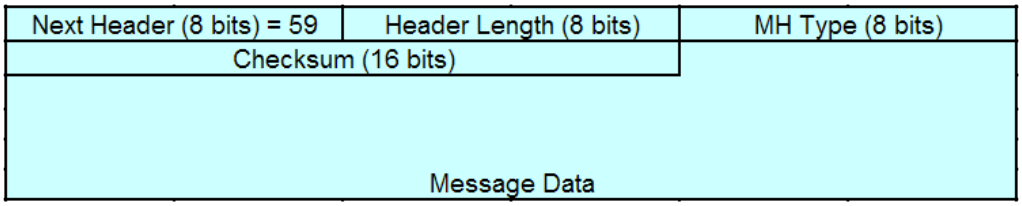


Figure 18: Format d'en-tête d'extension de mobilité

- Le champ en-tête suivant (en anglais *Next Header*) : 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 d'IPv6 Mobile, il doit valoir 59, c'est-à-dire qu'il n'y a pas d'en-tête d'extension suivant).

- Le champ longueur d'en-tête (en anglais *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.

- Le champ type d'en-tête de mobilité (en anglais *MH Type*) décrit les types des messages de mobilité.

Le tableau 4 présente les différents types des messages de mobilité.

Tableau 4 : Différents types des messages de mobilité

Type d'en-tête	Type de message de mobilité
0	Demande de rafraîchissement de mise à jour d'association (en anglais *Binding Refresh Advice*)
1	Initialisation de test d'adresse mère (*HoTI*)
2	Initialisation de test d'adresse temporaire (en anglais *Home Address Test Init – CoTI)*
3	Test d'adresse mère (en anglais *Home Test – HoT*)
4	Test d'adresse temporaire (en anglais *Care-of Test – CoT*)
5	Mise à jour d'association (*BU*)
6	Acquittement de mise à jour d'association (*BA*)
7	Erreur de mise à jour d'association

Le protocole IPv6 Mobile a également utilisé deux nouveaux en-têtes d'extensions pour le mécanisme de routage de paquets optimisés – l'en-tête d'extension de destination et l'en-tête d'extension de routage de type 2. La valeur du champ d'en-tête suivant de l'en-tête IPv6 est de 60 pour signifier l'en-tête d'extension de destination et de 43 pour représenter l'en-tête d'extension de routage de type 2.

2.2.2.2 Gestion de la mobilité par le protocole IPv6 Mobile

La procédure du handover de niveau 3 gérée par le protocole IPv6 Mobile se décompose en trois phases – la phase de Détection de mouvement, la phase d'Auto-configuration d'adresses et la phase de Mise à jour d'association. La phase de Mise à jour d'association est décomposée également en trois phases : la phase de Mise à jour d'association avec le HA, la phase de Routabilité de retour et la phase de Mise à jour d'association avec le CN.

1. Détection de mouvement

La phase de Détection de mouvement est la première phase de la procédure du handover de niveau 3, elle a pour objectif de détecter le changement de réseau afin que le MN puisse réagir à ce changement et lancer les procédures correspondants, telles que Découverte de routeur, Auto-configuration d'adresses IPv6 sur le nouveau réseau, Mise à jour d'association avec HA et CN.

Selon le protocole IPv6 Mobile, trois méthodes sont proposés pour que le MN puisse recueillir les événements suivants comme les signes du déclenchement du handover de niveau 3. Ces événements sont Routeur non-accessible, Absence de réception du message

"Annonce de routeur", ou Signe du déclenchement du handover de niveau 2. Une fois que ces événements sont engendrés, le MN lance la procédure de Découverte de routeur. Si le MN découvre le nouveau routeur avec un préfixe différent du sien, il conclut que le handover de niveau 3 est entamé et qu'il s'est connecté à un nouveau réseau. Cependant ces événements qui se sont manifestés n'indiquent assurément pas le déclenchement du handover de niveau 3, par exemple, le routeur peut être non-accessible à cause d'une panne.

Routeur non-accessible

Le MN utilise le mécanisme de Détection de voisin non-accessible (en anglais *Neighbor Unreachability Detection*) pour détecter si le routeur est toujours accessible dans les deux sens [RFC 4861]. Cependant, ce processus est exécuté seulement au moment où le MN a des paquets à envoyer. La vérification de l'accessibilité du routeur se fait en deux étapes :

- La première étape : lorsque le MN envoie les paquets TCP, si tous les paquets sont correctement envoyés et que les accusés de réception ont été bien reçus ou qu'un nouveau paquet du CN est reçu, le MN considère que le routeur est toujours accessible. Dans le cas contraire, il doit passer à la deuxième étape pour revérifier l'accessibilité du routeur. Lorsque le MN envoie les paquets UDP, il est impossible de savoir si les paquets sont correctement envoyés, par conséquent, le MN ne peut pas attester de l'accessibilité du routeur, il doit ainsi passer à l'étape suivante.

- La deuxième étape : Lorsque le MN ne peut pas confirmer l'accessibilité du routeur dans la première étape, il doit envoyer le message "Sollicitation de voisin" au routeur pour solliciter la réponse "Annonce de voisin" du routeur. Si le MN ne peut pas recevoir la réponse pendant RetransTimer millisecondes (1000 millisecondes par défaut), il déduit que le routeur n'est plus accessible et devrait lancer la procédure de Découverte de routeur.

Mais le problème est que lorsque le MN n'a pas de paquets à envoyer, il ne peut pas savoir si le routeur est accessible ou non. Par conséquent, le MN ne s'aperçoit probablement pas du déclenchement du handover de niveau 3. De plus, la procédure de Détection de voisin non-accessible dure au moins 1 seconde. Ce délai est inacceptable pour les applications en temps réel.

Absence de réception du message "Annonce de routeur"

Quand le MN se trouve dans un réseau IPv6, il peut continuer de recevoir le message "Annonce de routeur non-sollicitée" envoyé par le routeur qui se situe dans ce même réseau [RFC 4861]. Le message "Annonce de routeur" contient un champ, appelé Intervalle de l'annonce, la valeur de ce champ représente l'intervalle maximum entre deux messages "Annonces de routeur" successives. Cette valeur est égale à la valeur de la variable *MaxRtrAdvInterval* qui est définie par l'administrateur du réseau. Le MN utilise cette valeur comme un indice de la fréquence à laquelle il compte recevoir le prochain message "Annonce de routeur non-sollicitée". Si le MN ne reçoit aucun message "Annonce de routeur" de son routeur pendant un intervalle, il peut déduire qu'au moins un message "Annonce de routeur" est perdu. Si le MN n'a reçu aucun message "Annonce de routeur

non-sollicitée" pendant 3 × *MaxRtrAdvInterval* secondes, il considère que ce routeur n'est plus accessible. Le MN devrait lancer la procédure de Découverte de routeur pour trouver un nouveau routeur.

En fait, comme nous l'avons décrit, le MN identifie le changement de réseau selon la détection du routeur non-accessible et la découverte d'un nouveau routeur avec un différent préfixe à l'aide des messages – "Annonce de routeur" et "Sollicitation de routeur".

Cet événement est aussi indépendant de différents types des réseaux, mais le délai pour conclure le changement de réseau est trop long. Selon la norme RFC 4861, la valeur minimum de *MinRtrAdvInterval* et la valeur minimum de *MaxRtrAdvInterval* sont 3 secondes et 4 secondes respectivement, donc, le délai est au minimum de 12 secondes. Par conséquent, pour réduire ce délai, il faut intensifier la fréquence d'envoi du message "Annonce de routeur non-sollicitée". Le protocole IPv6 Mobile assigne une valeur de 0,03 secondes pour *MinRtrAdvInterval* et une valeur de 0,07 secondes pour *MaxRtrAdvInterval*, dans ce cas-là, le MN attend 210ms pour conclure de la non-accessibilité de son routeur.

Signe du déclenchement du handover de niveau 2

Dans certains types de réseaux, le signe du déclenchement du handover de niveau 2 peut être obtenu à partir des protocoles de la couche inférieure ou des pilotes de périphériques du MN. Lorsqu'un MN change d'un AP à un autre, le signe peut être acquis à la suite du handover de niveau 2. Cependant, le handover de niveau 2 n'implique pas de façon certain le handover de niveau 3, parce que, si les deux APs appartiennent à un même réseau, il n'y a pas de handover de niveau 3. Il faut utiliser d'autres méthodes pour reconnaitre le déclenchement du handover de niveau 3.

La norme [RFC 3775] propose d'utiliser le protocole – la Découverte de voisin à la suite du déclenchement du handover de niveau 2 pour confirmer le déclenchement du handover de niveau 3. Le MN envoie le message "Sollicitation de voisin" et attend la réponse – "Annonce de voisin" du routeur afin de vérifier l'accessibilité du routeur dans les deux sens. 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.

En somme, la phase de Detection de mouvement gérée par ces trois méthodes est trop longue. Du fait que le MN ne peut ni recevoir ni envoyer les paquets pendant la phase de Détection de mouvement, c'est évident que ces trois méthodes ci-dessus ne peuvent pas répondre à la demande des applications qui exige un délai maximum de centaines de millisecondes. Par conséquent, plusieurs propositions sont faites pour réduire le délai de la phase de Détection de mouvement.

2. Auto-configuration d'adresses

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 ce nouveau réseau. Le

MN ne peut pas communiquer avec les CN avant l'accomplissement de cette phase. Comme nous l'avons décrit dans la section 2.1, cette phase peut prendre une seconde au minimum ou durer jusqu'à cinq secondes, le délai de la procédure DAD représente une grande partie du délai total.

3. Mise à jour d'association

La phase de Mise à jour d'association a pour objet de mettre à jour la table d'associations du HA et celle du CN afin que le HA puisse faire suivre les paquets à destination d'adresse mère du MN vers l'adresse temporaire de ce dernier et que le CN puisse communiquer directement avec le MN sans passer par le HA.

Comme nous l'avons décrit, la phase de Mise à jour d'association est décomposée également en trois phases : la phase de Mise à jour d'association avec le HA, la phase de Routabilité de retour et la phase de Mise à jour d'association avec le CN.

Mise à jour d'association avec le HA

Dès que le MN finit la phase d'Auto-configuration d'adresses, il envoie le message "Mise à jour d'association" (*en anglais Binding Update*) au HA pour mettre à jour la table d'associations (*en anglais Binding Cache*) du HA qui contient l'association entre l'adresse mère et l'adresse temporaire du MN. Lorsque le HA reçoit ce message, il actualise cette table d'associations et envoie un message "Acquittement de Mise à jour d'association" (*en anglais Binding Acknowledgement*) au MN comme la réponse. Le HA intercepte ainsi les paquets destinés à l'adresse mère du MN, soit en diffusant un message "Annonce de voisin" comme s'il était le MN, soit en répondant aux messages "Sollicitation de voisin" à la place du MN, ensuite, il envoie ces paquets à l'adresse temporaire du MN qui est enregistré dans la table d'associations.

D'ailleurs, le MN et le HA doivent utiliser le protocole IPSec pour protéger les messages de signalisation, mais ils ne sont pas obligés d'utiliser le protocole IPSec pour protéger les données. Comme nous n'avons pas étudié l'aspecte de la sécurité dans la recherche, nous ne détaillons pas ici le mécanisme de sécurité ainsi ses problèmes.

La figure 19 présente la phase de Mise à jour d'association ainsi que le message "Mise à jour d'association" et le message "Acquittement de Mise à jour d'association".

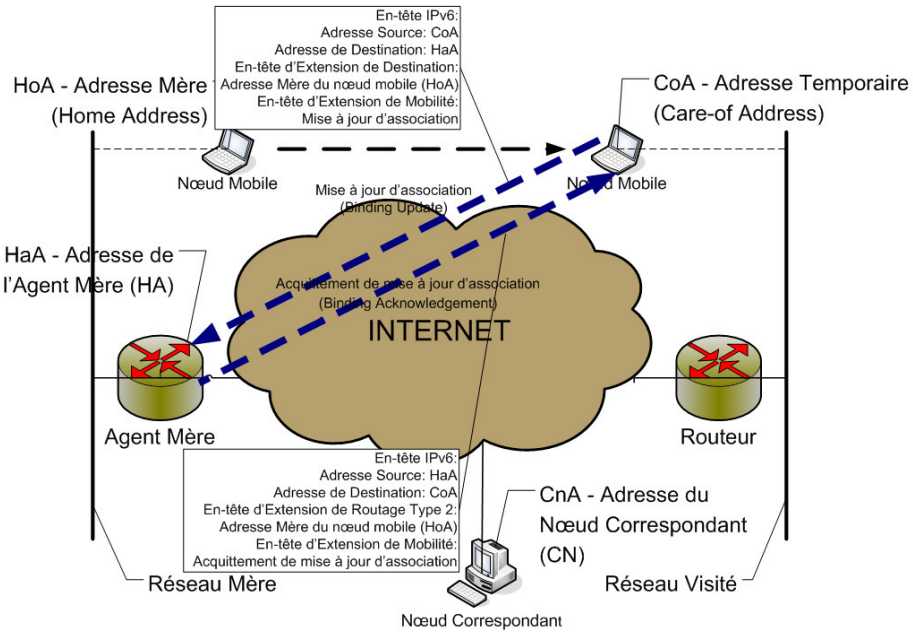


Figure 19 : Mise à jour d'association entre le MN et le HA

Routabilité de retour

A la différence du protocole IPv4 Mobile, pour le protocole IPv6 Mobile, lorsque le MN se trouve sur un réseau visité, il peut communiquer directement avec le CN sans passer par le HA. Ce mécanisme est baptisé "le routage de paquets optimisés ". Cependant, pour pouvoir utiliser ce mécanisme, non seulement le MN et le HA doivent supporter le protocole IPv6 Mobile, mais le CN doit aussi supporter le protocole IPv6 Mobile. C'est-à-dire que le CN supporte le protocole IPv6, il a une table d'associations et maintient la mise à jour de cette table. Si le CN ne supporte pas le protocole IPv6 Mobile, la communication entre le MN et le CN doit passer par le HA, comme pour IPv4 Mobile.

Comme le MN et le CN ne peuvent pas utiliser le protocole IPSec pour sécuriser les messages échangés entre eux, la procédure Routabilité de retour est déployée. Elle a pour but d'établir la preuve au CN que le MN est accessible à son adresse mère et à son adresse temporaire et de déterminer les jetons qui sont utilisés pour dériver une clé de la gestion de Mise à jour d'association. Cette clé est employée pour calculer des valeurs de données d'autorisation pour les messages de Mise à jour d'association. Comme ceux présents dans la figure 20, le CN envoie le message HoTI à l'adresse mère du MN en passant par le HA et envoie le message CoTI à l'adresse temporaire du MN en utilisant le chemin direct. Le MN envoie ainsi le message HoT et CoT comme réponse en utilisant le même chemin respectivement.

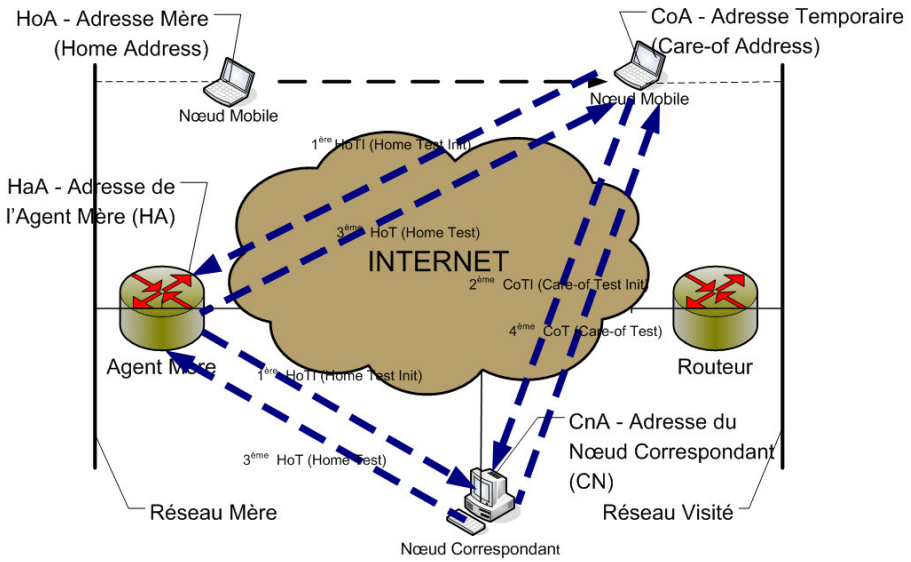


Figure 20 : Routabilité de retour

Mis à jour d'association avec le CN

Le MN et le CN utilisent la clé générée dans la phase Routabilité de retour pour authentifier les messages – Mise à jour d'association et Acquittement de mise à jour d'association. Lorsque le CN reçoit le message "Mise à jour d'association", il met à jour sa table d'associations et envoie le message "Acquittement de mise à jour d'association" au MN.

Une fois que la table d'association du CN est actualisée, le MN et le CN peuvent communiquer en utilisant le mécanisme de routage de paquets optimisé comme dans la figure 21.

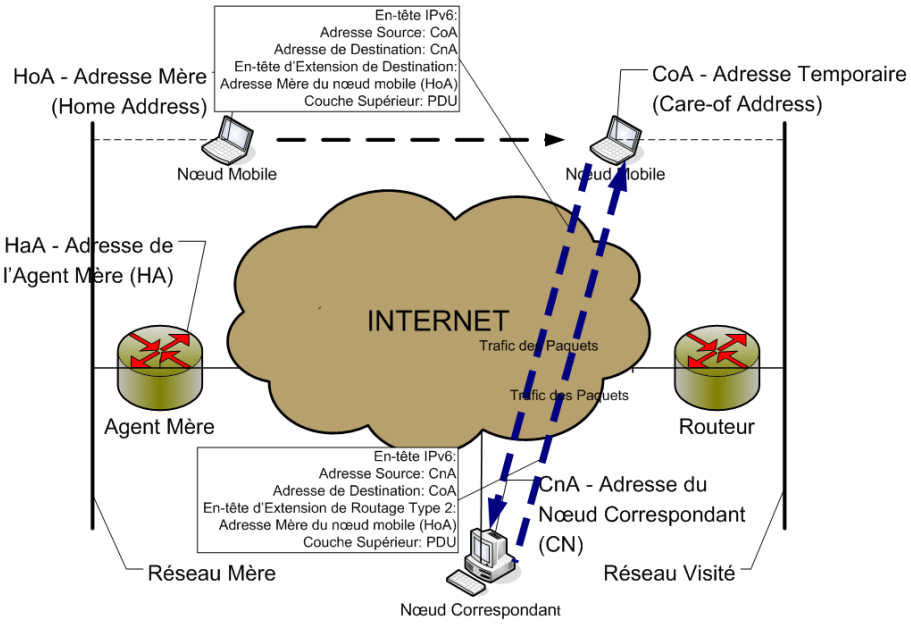


Figure 21 : Mécanisme de routage de paquets optimisé

Bien que le protocole IPv6 Mobile permette de résoudre le problème de routage de paquets triangulaire utilisé dans le protocole IPv4 Mobile, il souffre encore de plusieurs faiblesses. Parmi ces faiblesses, nous citons:

- Le délai du handover est long. Particulièrement, le délai de la phase de Detection de mouvement, celui de la phase d'Auto-configuration d'adresses et celui de la phase de Mise à jour d'association sont très long pour les applications en temps réel.

- La perte de paquets pendant le handover peut etre important. Le protocole IPv6 Mobile n'a pas proposé une solution pour réduire la perte de paquets.

Pour faire face aux limites du protocole IPv6 Mobile, plusieurs solutions ont été proposées. Le processus de handover peut etre amélioré soit en réduisant la perte de paquets, soit en diminuant la charge de la signalisation, soit encore en rendant le processus le plus rapide possible. Parmi les différentes propositions, nous présentons un aperçu sur deux principales solutions : le protocole IPv6 Mobile Hiérarchique et le protocole Fast handover pour IPv6 Mobile.

2.2.3 Protocole IPv6 Mobile Hiérarchique

Le protocole IPv6 Mobile Hiérarchique (*en anglais Hierarchical Mobile IPv6 – HMIPv6*) est une extension du protocole IPv6 Mobile [RFC 4140] [HSI02]. Il est développé par l'INRIA et Ericsson Research, et est standardisé par l'IETF. Il a pour objectif de réduire la quantité des messages de signalisation du protocole IPv6 Mobile induits par le handover de niveau 3. Les messages de signalisation sont les messages de la phase de Mise à jour d'association avec le HA, les messages liés avec la phase de Routabilité de retour et les messages de la phase de Mise à jour d'association 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 les CNs. Par conséquent, il améliore la performance de la procédure du handover de niveau 3 gérée par le protocole IPv6 Mobile.

Pour atteindre son objectif, le protocole HMIPv6 introduit une nouvelle entité, baptisée Point d'Ancrage Mobile (*en anglais Mobility Anchor Point – MAP*). Il peut être implanté à n'import quel endroit de la hiérarchie des routeurs. 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 a une fonctionnalité similaire que celle du HA du protocole IPv4 Mobile. 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 "Annonce de routeur". 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 auto-configure deux adresses temporaires : une adresse temporaire régionale (*en anglais Regional Care-of Address – RCoA*) et une adresse temporaire locale (*en anglais Local Care-of Address – LCoA*). 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. Donc, c'est

une adresse du réseau où le MAP se trouve. 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 le message "Mise à jour d'association locale" au MAP en vue d'y 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 "Acquittement de mise à jour d'association locale" au MN. Cela signifie que la phase de Mise à jour d'association avec le MAP est réussie. Ensuite, le MN effectue la phase de Mise à jour d'association avec le HA et les CNs en utilisant son adresse RCoA comme sa nouvelle adresse temporaire. Le HA et les CNs mettent à jour leurs tables d'associations 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. En conclure, le MAP, le MN et les CNs transfèrent les paquets de données de la même façon que dans le cas du protocole IPv4 Mobile. 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 Mise à jour d'association avec le HA et les CNs quand il n'a pas changé son adresse RCoA. Donc, on peut dire que le MAP masque 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 d'un MAP et la macro-mobilité le mouvement du MN entre des domaines. 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 IPv6 Mobile. Donc, il faut mieux choisir la taille du domaine pour éviter la macro-mobilité fréquente du MN.

Plusieurs approches sont proposées pour améliorer la performance de réseaux HMIPv6, telle que [HOS05] propose une méthode pour choisir la position de MAP dans le réseau. En outre, les comparaisons de diverse propositions et les analyses de la performance des réseaux HMIPv6 sont décrits dans [PACK04] [PACK06] respectivement.

2.2.4 Protocole Fats Handover pour IPv6 Mobile

Le protocole Fast Handover pour IPv6 Mobile (*en anglais Fast Handover for IPv6 Mobile – FMIPv6*) [RFC 4068] [Blondia04] qui est une extension du protocole IPv6 Mobile vise à réduire le délai de la phase de Détection de mouvement, celui de la phase d'Auto-configuration d'adresses et la perte de paquets. Il définit de nouveaux mécanismes qui

permettent au MN de pouvoir envoyer les paquets dès qu'il s'attache au nouveau réseau et de pouvoir recevoir les paquets dès que son attachement est détecté par le nouveau routeur d'accès (*en anglais Next Access Router – NAR*). Nous détaillons ce mécanisme par la suite. Une fois que le MN peut envoyer et recevoir les paquets sur ce nouveau réseau, il procède à la phase de Mise à jour d'association avec le HA et avec les CNs. Pendant cette phase, le MN peut continuer de communiquer avec les CNs via le tunnel bidirectionnel qui est créé par le routeur d'accès précédent (*en anglais Previous Access Router – PAR*) entre lui-même et le NAR. Lorsque la procédure du handover de niveau 3 est achevée, le MN peut communiquer directement avec les CNs et que le tunnel est enlevé. Dans le protocole FMIPv6, le PAR signifie le AR, auquel le MN se connecte en ce moment, et que le NAR signifie le AR, auquel le MN va se connecter. C'est de la même définition pour les adresses que pour les APs.

Le protocole FMIPv6 définit de nouveaux messages pour réaliser son nouveau mécanisme.

- Sollicitation de routeur pour l'annonce par procuration (*en anglais Router Solicitation for Proxy Advertisement – RtSolPr*) : est envoyé par le MN à son PAR pour demander les informations concernant un handover potentiel.

- Annonce de routeur par procuration (*en anglais Proxy Router Advertisement – PrRtAdv*) : est envoyé par le PAR au MN pour fournir les informations concernant les réseaux voisins. Ce message permet aussi la détection rapide de mouvement et fonctionne en tant que déclenchement du handover de niveau 3 pour le MN.

- Mise à jour d'association rapide (*en anglais Fast Binding Update – FBU*) : est envoyé par le MN à son PAR. Il a pour objet de permettre au PAR de lier l'adresse temporaire précédente (*en anglais Previous Care-of Address – PCoA*) à la nouvelle adresse temporaire (*en anglais Next Care-of Address – NCoA*) et de rediriger les paquets destinés à l'adresse temporaire précédente (PCoA) à sa nouvelle adresse temporaire (NCoA).

- Acquittement de la Mise à jour d'association rapide (*en anglais Fast Binding Acknowledgement – FBack*) : est envoyé par le PAR au MN et au NAR pour indiquer la création d'un tunnel.

- Handover déclenché (*en anglais Handover Initiate – HI*) : est envoyé par le PAR au NAR pour le handover du MN.

- Acquittement du handover (*en anglais Handover Acknowledge – HAck*) : est envoyé par le NAR au PAR pour répondre au message HI.

- Annonce de voisin rapide (*en anglais Fast Neighbor Advertisement – FNA*) : 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.

Mécanisme du protocole FMIPv6:

Le protocole FMIPv6 vise réduire le délai de la phase d'Auto-configuration d'adresses en préconfigurant sa nouvelle adresse temporaire. Lorsque le MN doit changer l'AP, il sonde tous les canaux pour chercher les APs disponibles à sa portée. Ensuite, il se reconnecte à son PAP et envoie le BSSID d'un AP ou ceux de plusieurs à son PAR via le message RtSolPr. A la réception du message RtSolPr, le PAR répond au MN en envoyant le message PrRtAdv qui contient les associations entre les APs et les routeurs d'accès (ARs), ainsi que les informations concernant les routeurs d'accès, tels que le préfixe, l'adresse IP et l'adresse MAC des routeurs d'accès. Grâce au message PrRtAdv reçu, le MN peut auto-configurer une nouvelle adresse temporaire – NCoA qui est potentiellement utilisable dans le nouveau réseau. Grâce à la connaissance des associations entre les APs et les routeurs d'accès, le MN peut détecter rapidement le changement de réseau une fois il change l'AP.

Selon le cas où le MN peut recevoir le message FBack sur le réseau du PAR ou non, la procédure suivante est distinguée en mode Prophétique et en mode Réactif.

Mode Prophétique

Dans ce mode, 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, l'AR précédent envoie le message FBack au MN et au NAR pour répondre au message FBU. Si le NAR propose une nouvelle adresse NCoA, l'AR précédent doit l'informer au MN au moyen du message FBack. Donc, le MN doit utiliser cette nouvelle adresse NCoA. Comme le MN a reçu le message FBack avant de changer le réseau, il peut utiliser sa nouvelle adresse NCoA dans le nouveau 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.

La figure 22 présente la procédure du protocole FMIPv6 en mode Prophétique :

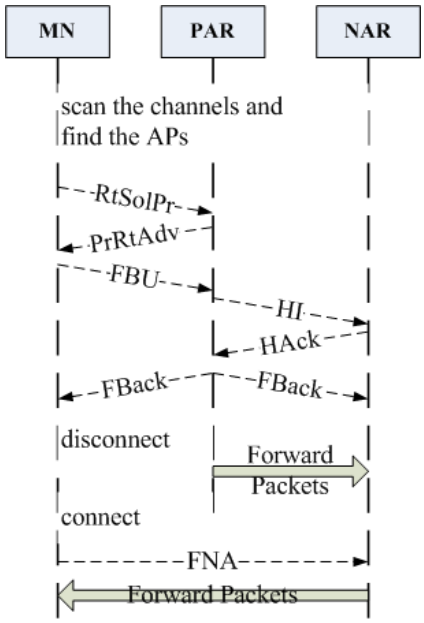


Figure 22 : Procédure du protocole FMIPv6 en Mode Prophétique

Mode Réactif

Dans ce mode, le MN n'a pas pu envoyer le message FBU ou n'a pas pu recevoir le message FBack avant de changer de réseaux. Donc, le MN ne peut pas assurer qu'il peut utiliser la nouvelle adresse NCoA. Le PAR peut créer une association entre l'adresse PCoA et l'adresse NCoA. Une fois que le MN s'attache au nouveau réseau, il utilise son adresse NCoA comme l'adresse source du message FNA. Le message FBU est encapsulé dans le message FNA. Ce message FNA est envoyé au NAR. Si le NAR approuve l'utilisation de la nouvelle adresse NCoA, il envoie le message FBU au PAR. Dans le cas contraire, le NAR soit propose une nouvelle adresse NCoA au MN, soit lui demande de générer une nouvelle tout en envoyant l'Annonce de Routeur au MN. En réponse au message FBU, l'AR précédent crée la association entre l'adresse PCoA et l'adresse NCoA et crée le tunnel entre l'adresse PCoA et l'adresse NCoA. Ce tunnel est toujours actif pendant la phase de Mise à jour d'association.

La figure 23 présente la procédure du protocole FMIPv6 en mode Réactif

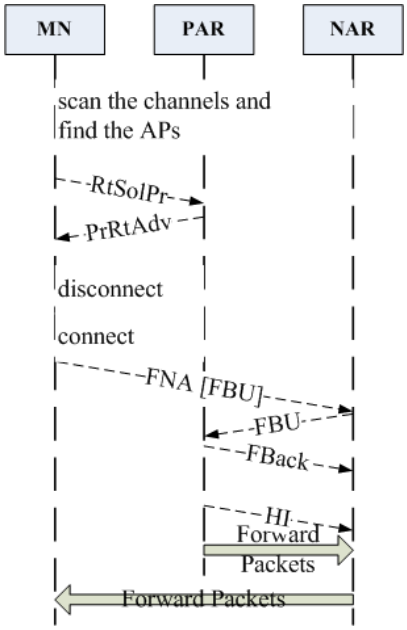


Figure 23: Procédure du protocole FMIPv6 en mode Réactif

Comme nous l'avons décrit, le MN peut auto-configurer une nouvelle adresse NCoA potentiellement utilisable quand il est toujours connecté au réseau du PAR. Le délai de la phase d'Auto-configuration d'adresses peut être éliminé. En utilisant le tunnel bidirectionnel, le MN peut communiquer avec les CNs pendant la phase de Mise à jour d'association pour éviter l'interruption de la communication en cours.

Cependant, le protocole FMIPv6 se concentre seulement sur l'exécution du protocole alors qu'il n'aborde pas d'autres aspects, telles que la découverte et le choix des APs, la découverte de routeurs d'accès potentiels, qui sont importants pour la performance du handover gérée par le protocole FMIPv6. Le protocole FMIPv6 n'a pas proposé une méthode qui permet aux routeurs d'accès d'échanger les informations de réseaux. De plus, dans beaucoup de réseaux sans fil, il est impossible de savoir exactement quand un MN s'est détachée de réseau précédent et s'est attaché au nouveau réseau. Donc, il est impossible pour PAR de déterminer le moment où il commence à transférer des paquets au NAR. Certaines technologies sans fil impliquent le déclenchement du handover de niveau 2, il instruit le MN du handover ou indique que le MN est détaché ou est attaché au réseau. Cependant, même si l'AR pourrait extraire cette information, il n'y aurait pas suffisamment de temps de détecter le détachement du MN et de commencer à rediriger des paquets au NAR avant que le MN s'attache au nouveau réseau. Cela s'explique par le fait que le délai du handover de niveau 2 est parfois court. Par conséquent, le MN risque de ne plus pouvoir recevoir les paquets avant sa déconnexion du réseau précédent, ou les paquets risquent de se perdre avant la connexion du MN au nouveau réseau.

2.3 Conclusion

Dans ce chapitre, nous présentons le protocole IPv4/IPv6 et le protocole IPv4 Mobile, IPv6 Mobile. Nous expliquons particulièrement l'Auto-configuration d'adresses du protocole IPv6, le mécanisme de gestion de mobilité du protocole IPv6 Mobile. Comme il existe des problèmes en termes de délai et de perte de paquets pour la mobilité du MN géré par le protocole IPv6 Mobile, plusieurs propositions sont faites pour résoudre ces problèmes, telles que le protocole HMIPv6, FMIPv6. Cependant, ces propositions sont soit imparfaites, soit non-implantables à cause de leur complexité. Dans le chapitre suivant, nous présenterons notre méthode, baptisé Méthode E-HCF. Avec cette méthode, nous pouvons limiter la perte de paquets et garantir un délai acceptable.

3 Méthode E-HCF

Jusqu'à présent, nous avons présenté la norme IEEE 802.11/Wi-Fi, le protocole IPv6, le protocole IPv6 Mobile dans le chapitre 1 et le chapitre 2. Nous avons aussi présenté la procédure du handover de niveau 2 gérée par la norme IEEE 802.11/Wi-Fi et celle de niveau 3 gérée par le protocole IPv6 Mobile. En outre, les principales propositions qui ont pour objectif d'améliorer soit la performance de la procédure du handover de niveau 2 gérée par la norme IEEE 802.11/Wi-Fi, soit celle du handover de niveau 3 gérée par le protocole IPv6 Mobile sont décrits dans les chapitres précédents. Cependant, nous avons vu qu'il y avait un manque important d'adaptabilité, de flexibilité ou d'une solution globale pour ces approches. C'est la raison pour laquelle qu'il devient intéressant de concevoir une solution de gestion intégrale des procédures du handover de niveau 2 et de niveau 3.

En partant du principe que les réseaux Wi-Fi et les routeurs d'accès sont déjà massivement implantés, telles que dans les campus ou les sites industriels, nous proposons d'ajouter une nouvelle fonctionnalité, dénommé E-HCF (Extended Handover Control Function), dans un routeur sans modifier les autres équipements du réseau. Le routeur pourvu de cette fonctionnalité E-HCF est dénommé le routeur E-HCF. La fonctionnalité E-HCF permet au routeur de générer une topologie des points d'accès en utilisant la théorie des graphes de voisinage et de maintenir un pool d'adresses IP disponibles. Lorsque le MN a besoin de changer son point d'accès, le routeur E-HCF peut proposer au MN une liste des points d'accès potentiellement utilisables qui sont choisis et classés par un algorithme de sélection et de classement que nous avons élaboré dans la thèse. Si le changement d'AP implique un changement de réseau, le MN doit avoir une nouvelle adresse IP. Dans ce cas, le routeur E-HCF peut attribuer une adresse IP unique à ce MN. Le MN peut donc utiliser cette adresse sans exécuter la phase d'Auto-configuration d'adresses ni exécuter la procédure de Détection d'adresse dupliquée. Cette nouvelle fonctionnalité E-HCF nous permet d'améliorer la performance du handover en termes de délai. Par ailleurs, par le moyen que le MN met fin à l'association entre son adresse mère et son adresse temporaire avec le HA et les CNs avant de procéder la procédure du handover, le HA peut intercepter et garder les paquets destinés à l’adresse mère du MN dans son mémoire tampon. Une fois le MN met à jour l'association entre son adresse mère et sa nouvelle adresse temporaire avec le HA, le HA peut envoyer les paquets stockés dans son mémoire de tampon au MN. Par ce moyen, nous pouvons limiter la perte de parquets durant le handover.

Ce chapitre est organisé comme suite : nous présentons d'abord l'architecture du réseau avec la fonctionnalité E-HCF. Ensuite, nous décrivons les messages définies par la méthode E-HCF. Dans la section 3.3, nous donnons la description de l'E-HCF et leurs avantages par rapport au protocole MIPv6. En fin, nous présentons une estimation de performance de l'E-HCF comparée avec autres propositions (MIPv6, HMIPv6 et Fast Handover).

3.1 Architecture de réseaux avec la méthode E-HCF

L'architecture du réseau avec la fonctionnalité E-HCF est présentée à la figure 24. Nous dénommons le routeur doté la fonctionnalité E-HCF le routeur E-HCF. Le routeur E-HCF contrôle plusieurs routeurs d'accès, et les APs qui se connectent aux routeurs d'accès en filaire. Un routeur E-HCF peut communiquer avec les autres routeurs E-HCF via Internet.

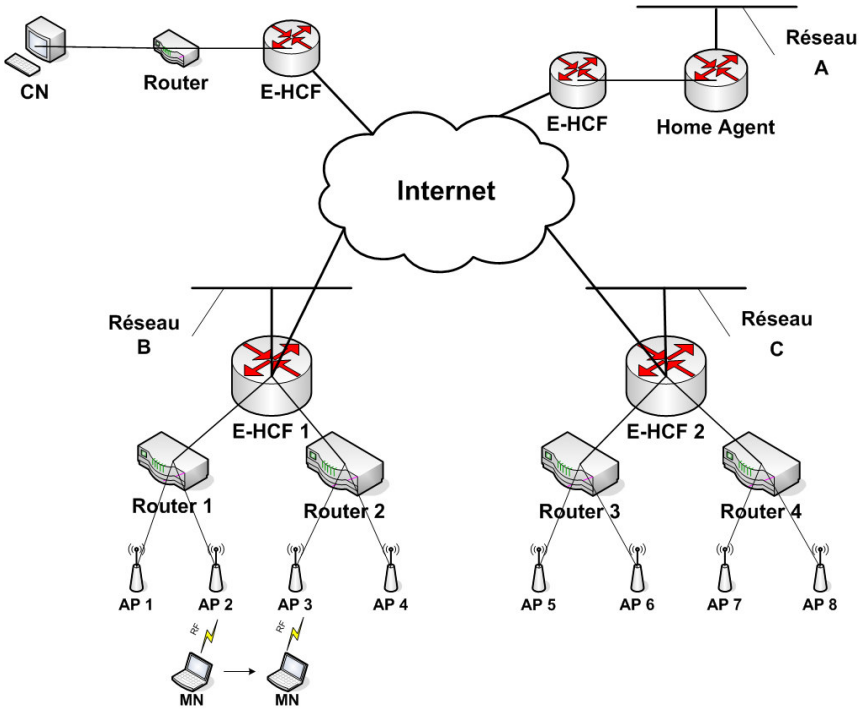


Figure 24: Architecture de réseaux avec E-HCF

Selon la norme IEEE 802.11, quand un MN se déplace dans les réseaux Wi-Fi, s'il constate que la puissance du signal (RSSI) d'AP courant descend en-dessous d'un seuil prédéterminé, il va le déconnecter et s'associer avec un nouveau AP, avec lequel il a une meilleure réception du signal. Dans la figure 24, si le MN passe de l'AP 1 à l'AP 2, le changement d'AP n'implique pas le changement de réseau (c'est un handover de niveau 2), parce que ces deux APs appartiennent au même réseau de l'AR 1. Cependant, si le MN passe de l'AP 2 à l'AP 3, cela implique non seulement le handover de niveau 2, mais aussi celui de niveau 3, parce que ces deux APs n'appartiennent pas à un même réseau.

Nous avons décrit dans les chapitres 1 et 2 que le délai du handover de niveau 2 et de niveau 3 est trop long (2080-5380 ms) pour supporter des applications temps réel. De plus, un handover entraîne encore à la fois des interruptions de communication. Par conséquent, le taux de la perte de paquets durant un handover est important.

La fonctionnalité E-HCF pourrait réduire le délai du handover et minimiser la perte de paquets due au handover.

3.2 Formats des messages

Pour réaliser la méthode E-HCF, nous définissons six nouveaux messages dans le protocole IPv6 Mobile. Ces messages servent à échanger les informations du réseau entre le routeur E-HCF et le MN ou entre les routeurs E-HCF. Nous utilisons également l'en-tête d'extension de mobilité pour définir ces messages :

- MNReq (MN Request – Requête du Nœud Mobile) – est un message envoyé par le MN au routeur E-HCF. Ce message est pour une demande du handover.

- E-HCFRep (E-HCF Reply – Réponse du routeur E-HCF) – est un message envoyé par le routeur E-HCF. Ce message contient la décision du routeur E-HCF concernant la demande du handover du MN.

- Int–E-HCFReq (Inter E-HCF Request) et Int-E-HCFRep (Inter E-HCF Reply) – sont des messages envoyés entre les deux routeurs E-HCF pour échanger les informations du réseau.

- MNHC (MN Handover Complete – Accomplissement du handover du MN) – est un message envoyé par le MN au routeur E-HCF pour libérer la ressource réservée par le routeur E-HCF pour ce MN.

- E-HCFHC (E-HCF Handover Confirmation – Confirmation du handover du routeur E-HCF) – est un message envoyé par le routeur E-HCF en recevant du message MNHC. Ce message est utilisé comme acquittement du message MNHC. L'envoi de ce message est optionnel.

Le message MNReq (MN Request – Requête du Nœud Mobile)

Le MN définit un seuil pour la puissance du signal d'AP. Si la puissance du signal d'AP connecté descend en dessous de ce seuil, le MN envoie le message MNReq au routeur E-HCF pour solliciter les informations de réseaux.

Le format du message MNReq est présenté dans le tableau 5:

Tableau 5 : Format du message MNReq

Ver (4bits)	Traffic Class (8 bits)	Flow Label (20 bits)	
Payload Length (16 bits)		Next Header (8 bits) = 60	Hop Limit (8 bits)
Source IPv6 Address (128 bits)			
Destination IPv6 Address (128 bits)			
Next Header (8 bits) = 135	Header Length (8 bits) = 4	Option Type (8 bits) = 201	Option Length (8 bits) = 16
Reserved (32 bits)			
Home Address of Mobile Node (128 bits)			
Next Header (8 bits) = 59	Header Length (8 bits)	MH Type (8 bits)	Sequence Number (8 bits)
Checksum (16 bits)		E-HCFUID (16 bits)	
Channel Number (8 bits)	Time Connection (8 bits)		
BSSID of Access Point 1 (48 bits)			
Channel Number (8 bits)	Time Connection (8 bits)		
BSSID of Access Point 2 (48 bits)			
Channel Number (8 bits)	Time Connection (8 bits)		
BSSID of Access Point N (48 bits)			
Reserved (64 bits)			

Nous utilisons l'en-tête d'extension de destination et l'en-tête d'extension de mobilité pour contenir les informations du MN, tels que l'adresse mère du MN et le BSSID d'AP courant. Eventuellement, les BSSID des APs avec lesquels le MN est connecté peuvent être ajoutés dans l'en-tête d'extension de mobilité dans un ordre précis : du plus récent au plus ancien. Cela constitue le chemin parcouru par le MN.

Lorsque le message MNReq est reçu par le routeur E-HCF, il lit l'en-tête d'extension de destination et remplace l'adresse source de paquet par l'adresse contenue dans le champ "Home Address of Mobile Node " (l'adresse mère du MN).

Le champ "MH Type" (Type d'en-tête de Mobilité) d'en-tête d'extension de mobilité est utilisé pour distinguer le type des messages du protocole IPv6 Mobile, par exemple, la valeur 5 représente le message — Mise à jour d'association (Binding Update). Nous utilisons la valeur 11 pour représenter le message MNReq.

Le champ "Sequence Number" (Numéro de Sequence) identifie le message MNReq qui est envoyé par le MN. Il est également utilisé par le routeur E-HCF. Le routeur E-HCF va copier cette valeur dans le champ "Sequence Number " du message E-HCFRep. Avec ce numéro, le MN peut associer le message E-HCFRep reçu avec le message MNReq envoyé auparavant. Un message HCFRep périmé est jeté par le MN qui a déjà envoyé un nouveau message MNReq. L'intervalle d'envoi du message MNReq est défini par l'administrateur du réseau.

Le champ "E-HCFUID" (E-HCF Unique Identifier) – E-HCF Identifiant Unique est un numéro d'identifiant unique généré par le MN. Le routeur E-HCF utilise la combinaison de cet identifiant et de l'adresse mère du MN pour identifier ce MN.

Le champ "Channel Number" (Numéro de Canal) est le numéro de canal où cet AP se trouve. Quand cette valeur est égale à 0, cela signifie que le numéro du canal n'est pas indiqué.

Le champ "Time Connection" (Moment de connexion) représente le moment de la connexion avec l'AP. Nous pouvons utiliser cette valeur pour déduire la vitesse de déplacement du MN.

Le champ "BSSID of Access Point 1" (BSSID du Point d'Accès 1) contient le BSSID d'AP avec lequel le MN est connecté en ce moment.

Le champ "BSSID of Access Point 2" contient le BSSID d'AP avec lequel le MN était connecté auparavant. Si sa valeur est égale à 0, cela signifie que le MN n'indique pas les APs, avec lesquels le MN étai connecté auparavant.

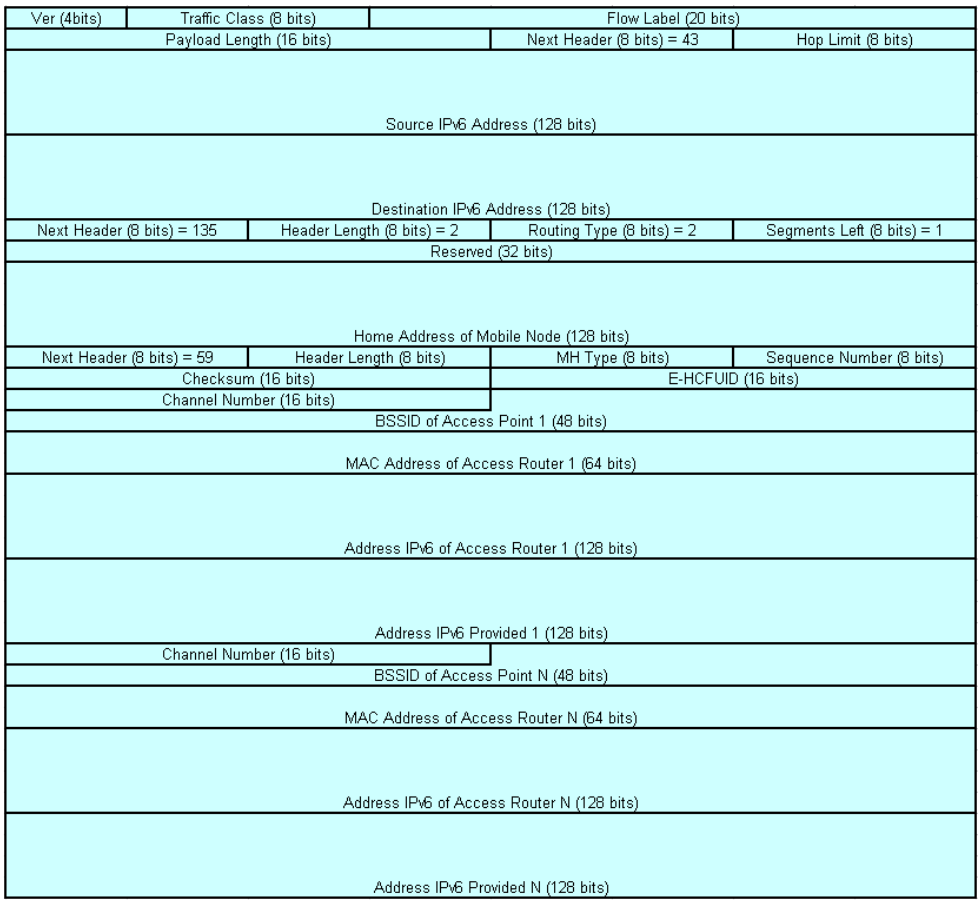
Le champ "BSSID of Access Point N " contient le BSSID d'AP avec lequel le MN était connecté auparavant. N est égale à 3 ou plus.

Le champ "Reserved" (Réservé) n'est pas utilisé pour l'instant.

E-HCFRep (E-HCF Reply – Réponse du routeur E-HCF)

Le message E-HCFRep (E-HCF Reply – Réponse du routeur E-HCF) est utilisé par le routeur E-HCF pour fournir au MN les informations du réseau, telles que la liste des APs potentiellement utilisables, les BSSIDs des APs, l'adresse MAC du AR, l'adresse globale du AR et les adresses globales disponibles. Nous exposons dans les paragraphes suivants comment le routeur E-HCF choisit les informations du réseau et les propose au MN en fonction du comportement du MN. Le format du message E-HCFRep est présenté dans le tableau 6.

Tableau 6 : Format du Message E-HCFRep



Nous utilisons l'en-tête d'extension de Routage (Type 2) et l'en-tête d'extension de mobilité pour contenir les informations du réseau dans ce message.

Lorsque le message E-HCFRep est reçu par le MN, il lit l'en-tête d'extension de routage (Type 2) et remplace l'adresse destination de paquet par l'adresse contenue dans le champ "Home Address of Mobile Node " (l'adresse mère du MN).

Nous utilisons la valeur 12 contenue dans le champ "MH Type" (Type d'en-tête d'extension de Mobilité) pour représenter le message E-HCFRep.

Le champ "Sequence Number" (Numéro de Sequence) identifie le message E-HCFRep qui est envoyé par le routeur E-HCF. Le routeur E-HCF copie la valeur du champ "Sequence Number " du message MNReq reçu dans ce champ. Avec ce numéro, le MN peut associer le message E-HCFRep reçu avec le message MNReq envoyé auparavant. Un message HCFRep périmé est rejeté par le MN qui a déjà envoyé un nouveau message MNReq.

Le champ "E-HCFUID" (E-HCF Unique Identifier) – E-HCF Identifiant Unique est un numéro d'identifiant unique généré par le MN. Le routeur E-HCF copie la valeur du champ "E-HCFUID" du message MNReq reçu dans ce champ. Le MN peut aussi utiliser la combinaison de cet identifiant et l'adresse mère du MN contenue dans le champ "Home Address of Mobile Node" pour identifier le routeur E-HCF.

Le champ "Channel Number" (Numéro de canal) est le numéro du canal où l'AP se trouve. Quand cette valeur est égale à 0, cela signifie que le numéro du canal n'est pas indiqué.

Le champ "BSSID of Access Point 1" (BSSID du Point d'Accès 1) contient le BSSID de premier AP proposé par le routeur E-HCF. Le routeur E-HCF propose une liste des APs qui sont choisis et classés par un algorithme de sélection et de classement que nous avons élaboré. Le MN doit se connecter à ces APs selon leur classement dans la liste.

Le champ "MAC Address of Access Router 1" (Adresse MAC du Routeur d'Accès 1) contient l'adresse MAC de l'AR avec lequel l'AP 1 connecte. Les 16 premiers bits doivent être égaux à 0 pour avoir une taille totale de 64 bits.

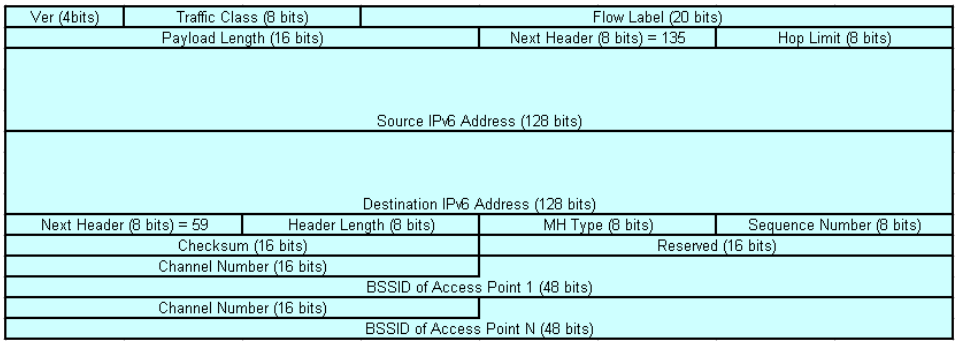
Le champ "Address IPv6 of Access Router 1" (Adresse IPv6 du Routeur d'Accès 1) contient l'adresse IPv6 globale de l'AR 1 avec lequel l'AP 1 est connecté.

Le champ "Address IPv6 Provided" (Adresse IPv6 Fournie) est la nouvelle adresse temporaire du MN s'il se connecte à l'AP 1.

Messages Int-E-HCFReq (Inter E-HCF Request) et Int-E-HCFRep (Inter E-HCF Reply)

Les messages Int-E-HCFReq et Int-E-HCFRep utilisent l'en-tête d'extension de mobilité, mais n'utilisent pas l'autre en-tête d'extension. Le format du message Int–E-HCFReq est présenté dans le tableau 7.

Tableau 7 : Format du Message Int–E-HCFReq



La valeur du champ MH Type (Type d'en-tête de Mobilité) est égale à 13 dans le message Int-E-HCFReq.

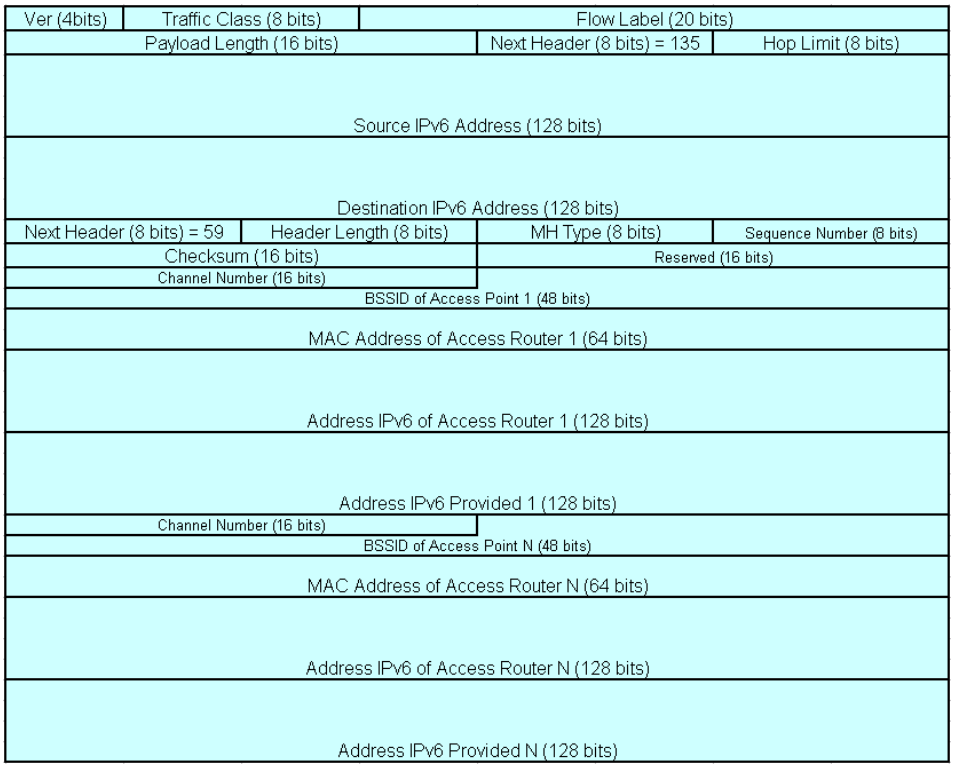
Le champ "Sequence Number " (Numéro de Sequence) identifie le message Int-E-HCFReq qui est envoyé par le routeur E-HCF origine. Le routeur E-HCF distant copie la valeur du champ "Sequence Number " du message Int–E-HCFReq dans le champ "Sequence Number " du message Int–E-HCFRep. Avec ce numéro, le routeur E-HCF peut associer le message Int-E-HCFRep reçu avec le message Int-E-HCFReq envoyé auparavant. Un message Int-E-HCFRep périmé est jeté par le routeur E-HCF qui a déjà envoyé un nouveau message Int-E-HCFReq.

Le champ "Channel Number" (Numéro de canal) est le numéro du canal où cet AP se trouve. Dans ce message, sa valeur est égale à 0.

Le champ "BSSID of Access Point 1" (BSSID du Point d'Accès 1) contient le BSSID d'AP 1. Le routeur E-HCF demande les informations concernant cet AP et l'AR avec lequel cet AP est attaché.

Le format du message Int-E-HCFRep est présenté dans le tableau 8.

Tableau 8 : Format du Message Int–E-HCFRep



La valeur du champ MH Type (Type d'en-tête d'extension de Mobilité) qui est égale à 14 représente le message Int–E-HCFRep.

A la demande du routeur E-HCF voisin, ce routeur E-HCF répond en envoyant des informations, telles que le numéro du canal d'AP, les BSSID des APs, l'adresse MAC d'AR, l'adresse globale d'AR et les adresses globales disponibles correspondantes.

La fonctionnalité du message Int–E-HCFRep est assez similaire à celle du message E-HCFRep. Le message E-HCFRep et le message Int–E-HCFRep sont utilisés pour fournir les informations du réseau au MN et au routeur E-HCF origine respectivement.

MNHC (MN Handover Complete – Accomplissement du handover du MN)

Une fois que le MN reçoit le message E-HCFRep, il commence la procédure du handover. Nous expliquons cette procédure dans la suite de cet exposé.

Quand le MN se connecte au nouveau AP, il vérifie si le changement d'AP implique le changement de réseau. Si le MN change de réseau, il envoie tout de suite le message – la Sollicitation de voisin à l'AR de ce nouveau réseau pour notifier son attachement. L'AR envoie l'Annonce de voisin comme réponse. De plus, le MN envoie le message MNHC au routeur E-HCF pour libérer les ressources réservées.

Le message MNHC utilise l'en-tête d'extension de destination, et l'en-tête d'extension de mobilité, le format du message est présenté dans le tableau 9.

Tableau 9 : Format du message MNHC

Ver (4bits)	Traffic Class (8 bits)	Flow Label (20 bits)	
Payload Length (16 bits)		Next Header (8 bits) = 60	Hop Limit (8 bits)
Source IPv6 Address (128 bits)			
Destination IPv6 Address (128 bits)			
Next Header (8 bits) = 135	Header Length (8 bits) = 4	Option Type (8 bits) = 201	Option Length (8 bits) = 16
Reserved (32 bits)			
Home Address of Mobile Node (128 bits)			
Next Header (8 bits) = 59	Header Length (8 bits)	MH Type (8 bits)	Sequence Number (8 bits)
Checksum (16 bits)		E-HCFUID (16 bits)	
Channel Number (16 bits)			
BSSID of Access Point 1 (48 bits)			
Reserved (64 bits)			

La valeur du champ MH Type (Type d'en-tête de Mobilité) qui est égale 15 représente le message MNHC.

Dans ce message, l'adresse source n'est plus l'adresse précédente du MN, c'est une adresse qui est attribuée par le routeur E-HCF au moyen du message E-HCFRep. Cette adresse est la nouvelle adresse temporaire du MN dans ce nouveau réseau.

Le champ "BSSID of Access Point 1" (BSSID du Point d'Accès 1) contient le BSSID d'AP avec lequel le MN est connecté en ce moment.

Le routeur E-HCF lit l'en-tête d'extension de destination et remplace l'adresse source du message par l'adresse mère dans ce champ. Il identifie le MN par la combinaison d'E-HCFUID et de l'adresse mère du MN. Selon le BSSID d'AP que le MN a marqué dans ce message, le routeur E-HCF libère les autres ressources réservées, tels que les adresses IPv6.

E-HCFHC (E-HCF Handover Confirmation – Confirmation du handover du routeur E-HCF)

Le routeur E-HCF décide librement s'il envoie le message E-HCFHC au MN comme acquittement du message MNHC.

Le format de ce message est présenté dans le tableau 10.

Tableau 10 : Format du message E-HCFHC

Ver (4bits)	Traffic Class (8 bits)	Flow Label (20 bits)	
Payload Length (16 bits)		Next Header (8 bits) = 43	Hop Limit (8 bits)
Source IPv6 Address (128 bits)			
Destination IPv6 Address (128 bits)			
Next Header (8 bits) = 135	Header Length (8 bits) = 2	Routing Type (8 bits) = 2	Segments Left (8 bits) = 1
Reserved (32 bits)			
Home Address of Mobile Node (128 bits)			
Next Header (8 bits) = 59	Header Length (8 bits)	MH Type (8 bits)	Sequence Number (8 bits)
Checksum (16 bits)		E-HCFUID (16 bits)	
Reserved (64 bits)			

La valeur du champ MH Type (Type d'en-tête de Mobilité) est égale à 16 et représente le code du message E-HCFHC.

Dans ce message, l'adresse de destination est la nouvelle adresse temporaire du MN. C'est une adresse attribuée par le routeur E-HCF au moyen du message E-HCFRep.

Lorsque le routeur E-HCF reçoit le message MNHC, il marque l'adresse utilisée par le MN, libère toutes les ressources réservées pour le MN et envoie le message E-HCFHC au MN comme acquittement du message MNHC. Si le routeur E-HCF n'a pas reçu le message MNHC, il libère toutes les ressources réservées dans un délai prédéfini par l'administrateur du réseau.

3.3 Fonctionnement de la méthode E-HCF

Nous avons décrit la procédure du handover de niveau 2 et de niveau 3 dans les chapitres 1 et 2. La phase de découverte, la phase d'authentification et la phase de réassociation constituent la procédure du handover de niveau 2. La phase de détection de mouvement, la phase d'Auto-configuration d'adresses, et la phase de Mise à jour d'association constituent la procédure du handover de niveau 3. Il faut également noter que la phase de Mise à jour d'association est décomposée en trois phases : la phase de Mise à jour d'association avec le HA, la phase de routabilité de retour et la phase de Mise à jour d'association avec le CN.

Dans les paragraphes suivants, nous présentons le fonctionnement de la méthode E-HCF, ainsi que la façon dont cette méthode optimise les procédures du handover de niveau 2 et de niveau 3.

3.3.1 Optimisation de la procédure du handover de niveau 2

Dans un réseau Wi-Fi, quand le MN se déplace loin de l'AP connecté, la puissance du signal (RSSI) se dégrade. Dès que la puissance du signal descend en-dessous d'un seuil

prédéterminé, selon la norme IEEE 802.11, le MN commence à chercher et à s'associer avec un nouveau AP, avec lequel il a une meilleure réception du signal. Par ailleurs, quand la puissance du signal se dégrade, le MN ne peut plus recevoir tous les accusés de réceptions d'AP pour les paquets envoyés. Dans ce cas, le MN doit réduire le débit de la transmission pour maintenir la connectivité [Broad03]. Par conséquent, quand le MN utilise des applications qui ont un débit faible, il peut répondre au besoin en débit de ces applications. Mais quand le MN utilise des applications, telles que la vidéo conférence ou les jeux multimédia, qui demandent un débit plus élevé, le MN risque de perdre des paquets même quand la puissance du signal est assez bonne. Ce phénomène est testé par les fabricants d'équipements de réseaux. Par exemple, pour l'AP sans fil du modèle F5D7230 802.11g de BELKIN [BELKIN], la portée opérationnelle et le débit supporté sont présentés dans le tableau 11 :

Tableau 11 : Portée et Débit du Model F5D7230 802.11g de BELKIN

Norme	Distance maximale	Débit maximal
802.11b	180 m	11 Mbits
	300 m	5.5 Mbits
	450 m	2 Mbits
	570 m	1 Mbits
802.11g	50 m	54 Mbits
	150 m	18 Mbits

Comme nous l'avons décrit dans le premier chapitre, le MN lance la procédure du handover de niveau 2 pour chercher un nouveau AP et s'y connecte. Cette procédure est décomposée en trois phases : la phase de découverte, la phase d'authentification et la phase de réassociation. Le délai total de ces trois phases est entre 250 ms et 400ms, dont le délai de la phase de découverte, $\mathbf{T}_{scan}$, représente 90% de ce délai [Mish03].

Le délai $\mathbf{T}_{scan}$ est calculé de la façon suivante :

$$N \times \mathbf{T}_{min} \leq \mathbf{T}_{scan} \leq N \times \mathbf{T}_{Max,}$$

Pour réduire le délai $\mathbf{T}_{scan}$, nous devons réduire la valeur de $\mathbf{T}_{min}$ (MinChannelTime), celle de $\mathbf{T}_{max}$ (MaxChannelTime), ou celle de N (le nombre des canaux qui doit être sondés). Les valeurs de $\mathbf{T}_{min}$ et de $\mathbf{T}_{max}$ ne peuvent pas être réduites en raison de la restriction physique, N est une valeur fixée dans chaque pays parce que les bandes de fréquences sont désignées par l'autorité de régulation. Cependant, si nous connaissons les APs et leurs canaux utilisés, le MN n'a pas besoin de scanner tous les canaux pour obtenir une liste des APs et se connecter à un de ces APs.

Normalement, il existe plusieurs APs dans une zone où le MN se trouve, comme dans un centre commercial ou dans un campus. D'après la norme IEEE 802.11, le MN doit d'abord scanner tous les canaux pour générer une liste des APs qui sont à sa portée, ensuite, il choisit un AP de cette liste pour s'y connecter. A part un long délai de la phase de découverte dont nous venons de parler, le MN ne peut pas forcement utiliser les APs qu'il a sondés. Cela est dû au fait qu'il existe des APs qui ne permettent pas au MN de s'associer

avec eux pour des raisons de sécurité ou du droit d'utilisation ou parce que ces APs sont trop chargés à cet instant et ne peuvent pas supporter ce MN en sus. Cependant, en utilisant la norme IEEE 802.11, le MN n'a pas de moyen de connaître l'état d'un AP avant d'essayer de s'y connecter. Par ailleurs, il vaut mieux éviter d'impliquer le handover de niveau 3 quand le MN change d'AP. Par conséquent, le MN doit utiliser une autre méthode pour trouver un AP plus utilisable.

Pour conclure, les problématiques de la procédure du handover de niveau 2 se traduisent par les questions suivantes :

- A quel moment le MN doit-il lancer la procédure du handover ?
- Comment le MN peut trouver rapidement les APs disponibles ?
- Comment le MN peut-il mieux choisir un AP utilisable ?

Ci-dessous, nous expliquons comment notre méthode E-HCF peut résoudre ces problématiques.

Pour mieux décider du moment de déclenchement de la procédure du handover de niveau 2, nous proposons non seulement d'utiliser la puissance du signal d'AP, mais aussi le débit supporté d'AP comme indice du déclenchement du handover de niveau 2. Le MN lance la procédure du handover quand le débit supporté de son AP ne peut pas répondre à sa demande ou quand la puissance du signal descend en dessous du seuil du déclenchement. Le seuil du déclenchement est décidé par le MN. Il est ajusté en fonction de la vitesse du déplacement du MN et en fonction d'autres paramètres. Par exemple, si le MN se déplace à une grande vitesse, il doit choisir un seuil de déclenchement plus élevé pour qu'il ait le temps de demander les informations du réseau au routeur E-HCF et de recevoir la réponse du routeur E-HCF.

Pour que le MN puisse connaître les APs potentiellement utilisables, le routeur E-HCF doit fournir les informations des APs à la demande du MN avant que le MN lance la procédure du handover de niveau 2.

Quand le MN doit changer d'AP, il envoie le message – MNReq au routeur E-HCF. Le MN garde les informations du routeur E-HCF qui lui servent en ce moment dans son cache. Donc, le MN peut toujours savoir à qui il va adresser le message MNReq. Dans le message MNReq, le MN notifie au routeur E-HCF le BSSID d'AP connecté actuellement. Si le routeur E-HCF supporte la fonctionnalité du choix des APs selon le chemin parcouru du MN, le MN envoie les BSSIDs des APs connectés auparavant et les moments de la connexion avec ces APs. Le MN peut aussi envoyer des critères, tels que le débit demandé ou le besoin de la qualité de service. Ces critères sont optionnels.

Le routeur E-HCF maintient une table E-HCFMAP qui contient tous les BSSIDs des APs qui sont dans son domaine. Cette table contient aussi les BSSIDs des APs à proximité des APs qui sont dans le domaine du routeur E-HCF. Dans cette table, il y a aussi l'adresse MAC et l'adresse IPv6 de l'AR avec lequel l'AP est connecté, ainsi que le nom du routeur

E-HCF correspondant. Ces informations réseau sont mises à jour par les messages Int-E-HCFReq et Int-E-HCFRep.

La table E-HCFMAP du routeur E-HCF1 de la figure 24 est présentée dans le tableau 12 :

Tableau 12 : Table E-HCFMAP

BSSID du Point d'Accès	Numéro du Canal du Point d'Accès	Routeur d'Accès du Point d'Accès	Adresse MAC du Routeur d'Accès	Adresse IP du Routeur d'Accès	Routeur E-HCF du Routeur d'Accès
BSSID du Point d'Accès 1	1	Routeur d'Accès 1	Adresse MAC du Routeur d'Accès 1	Adresse IP du Routeur d'Accès 1	E-HCF1
BSSID du Point d'Accès 2	6	Routeur d'Accès 1	Adresse MAC du Routeur d'Accès 1	Adresse IP du Routeur d'Accès 1	E-HCF1
BSSID du Point d'Accès 3	11	Routeur d'Accès 2	Adresse MAC du Routeur d'Accès 2	Adresse IP du Routeur d'Accès 2	E-HCF1
BSSID du Point d'Accès 4	2	Routeur d'Accès 2	Adresse MAC du Routeur d'Accès 2	Adresse IP du Routeur d'Accès 2	E-HCF1
BSSID du Point d'Accès 5	7	Routeur d'Accès 3	Adresse MAC du Routeur d'Accès 3	Adresse IP du Routeur d'Accès 3	E-HCF2
BSSID du Point d'Accès 6	3	Routeur d'Accès 3	Adresse MAC du Routeur d'Accès 3	Adresse IP du Routeur d'Accès 3	E-HCF2
BSSID du Point d'Accès 7	8	Routeur d'Accès 4	Adresse MAC du Routeur d'Accès 4	Adresse IP du Routeur d'Accès 4	E-HCF2
BSSID du Point d'Accès 8	4	Routeur d'Accès 4	Adresse MAC du Routeur d'Accès 4	Adresse IP du Routeur d'Accès 4	E-HCF2

Avec cette table, le routeur E-HCF peut trouver l'association entre l'AP, l'AR et le routeur E-HCF. Généralement, l'AP, l'adresse IP de l'AR, l'AR et cette correspondance, qui sont configurées par l'administrateur du réseau, ne sont pas modifiés souvent.

Pour pouvoir proposer au MN des APs potentiellement utilisables, le routeur E-HCF utilise d'abord le Graphe de Voisinage (*en anglais Neighborhood Graph*) pour construire un graphe qui représente la distribution géographique des APs. Ensuite, le routeur E-HCF élimine certains APs selon la trajectoire potentielle du MN. A la fin, le routeur E-HCF propose au MN une liste des APs classés par un algorithme de classement que nous avons élaboré.

Ici, nous présentons les notions sur le graphe de voisinage [Tou92] [Rod98] :

Un graphe *G*, noté *G (V, E)* consiste en un ensemble de sommets (ou nœuds) *V* et d'arcs (ou arêtes) *E*.

Un sommet *V* est un point d'extrémité ou un point d'intersection d'un graphe. Il s'agit d'une abstraction d'un lieu tel une ville, une division administrative, une intersection routière ou

une infrastructure de transfert (stations, terminus, ports et aéroports). Nous appliquons cette définition: les sommets représentent les APs.

Un arc *E* est un lien entre deux sommets. Nous notons l'arc *E (i, j)* qui est un arc reliant le sommet initial *i* et le sommet terminal *j*. Un arc est une représentation abstraite d'infrastructures de support des déplacements entre deux sommets. Selon que la direction est unidirectionnelle ou bidirectionnelle, le graphe est aussi caractérisé en orienté ou non-orienté. Un graphe non-orienté est un graphe *G (V, E)* tel que l'arc *E (i, j)* est confondu avec l'arc *E (j, i)*. On dit qu'un sommet *j* est voisin de *i* si $(i, j) \in E$. Nous appliquons cette définition: s'il existe une zone de recouverture pour les deux APs, cela signifie que le MN peut changer son point d'attachement entre ces deux APs. Nous créons un arc *E (i, j)* représentant la possibilité du changement d'AP *i* à l'AP *j* ou d'AP *j* à l'AP *i*. Si le MN ne peut pas changer son point d'attachement entre ces deux APs, il n'existe pas d'arc pour ces deux APs.

Une longueur d'un chemin Ch_q dans un graphe *G (V, E)* est une longueur ensemble d'un nombre de *q* arcs constituant ce chemin. $Ch_q = ((x, x_1), (x_1, x_2), \ldots, (x_q, y))$ où *x* est l'extrémité initiale et *y* l'extrémité finale du chemin. Le chemin le plus court est le chemin de longueur minimale parmi l'ensemble des chemins de *x* à *y*. Nous appliquons cette définition: une longueur d'un chemin Ch_1 est une longueur d'arc *E (i, j)* reliant l'AP *i* et l'AP *j*. La longueur d'arc *E (i, j)* n'est pas la distance directe spatiale entre ces deux APs, elle est la distance du chemin parcouru par le MN entre ces deux APs. S'il existe plusieurs chemins entre ces deux APs, la longueur d'arc *E (i, j)* est la longueur moyenne de ces différents chemins.

La construction de notre graphe repose sur une connaissance de la position de tous les APs, leurs portées réelles et les différents chemins entre ces APs. Ces connaissances peuvent être obtenues au moyen du système GPS (Global Positioning System) [Eng99]. Par conséquent, avec ce graphe, à partir d'un AP, nous pourrons trouver l'ensemble des APs disponibles qui sont à la portée du MN.

Prenons un exemple, la figure 25 présente la distribution géographique des APs qui appartiennent à l'operateur Télécom Orange dans un quartier de Paris:

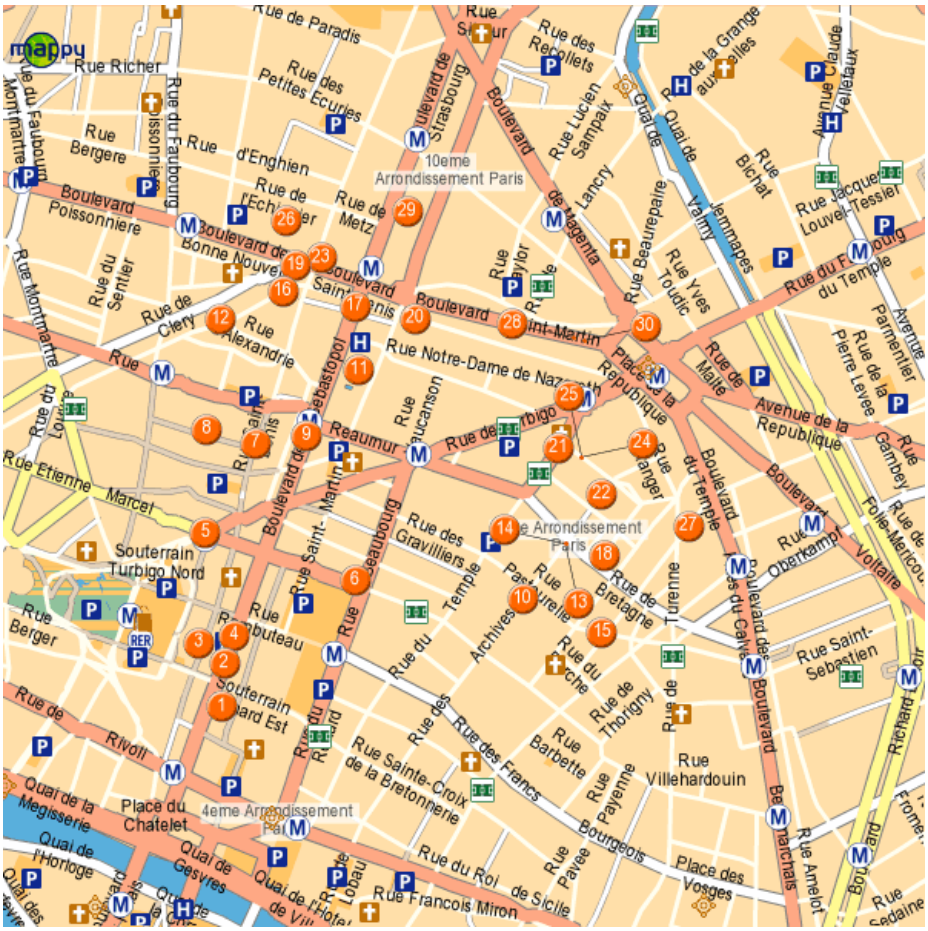


Figure 25: La distribution géographique des APs dans un quartier de Paris

La figure 26 présente le graphe des APs qui correspond à la distribution géographique des APs dans la figure 25:

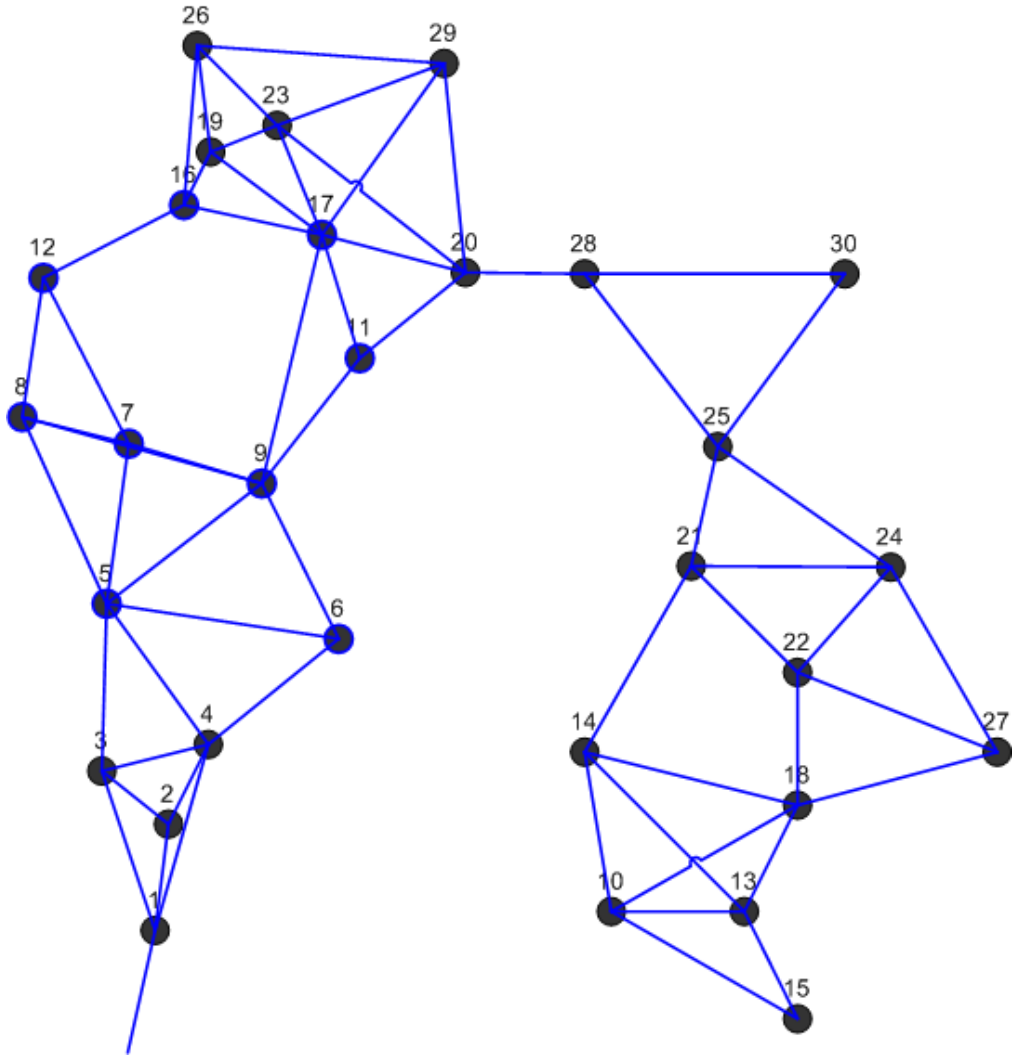


Figure 26 : Graphe des points d'accès dans un quartier de Paris

Ce graphe se définit de façon suivante :

G = G (V, E)
V = (1, 2, 3, 4, 5, 6, 7... 28, 29, 30)
E = (1, 2), (1, 3), (1, 4), (2, 3), (3, 4), (3,5) … (28, 30), (25,30)

Dont, les sommets, *1, 2, 3, 47... 28, 29, 30,* représentent les différents APs. Les arcs, *(1, 2), (1, 3), (1, 4), (2, 3), (3, 4), (3,5) … (28, 30), (25,30),* représentent les possibilités du handover entres ces deux APs. La longueur entre deux APs est la longueur moyenne de différents chemins entre eux.

Quand le routeur E-HCF reçoit le message MNReq, il répertorie tous les APs disponibles à partir de l'AP, avec lequel le MN est connecté. Le routeur E-HCF élimine les APs selon la

trajectoire potentielle du MN. La trajectoire potentielle du MN est décidée selon l'AP connecté actuellement et l'AP connecté précédemment.

Les autres méthodes utilisent le mécanisme de prédiction de la mobilité des utilisateurs pour prédire la trajectoire potentielle du MN. Son principe est fondé sur l'historique du mouvement des utilisateurs et sur les statistiques déduites des probabilités de déplacement des utilisateurs selon le comportement habituel d'autres utilisateurs qui ont parcouru le même chemin [LIU96], [BHA97], [JAN97].

Si le routeur E-HCF supporte le choix des APs selon la vitesse du déplacement du MN, il peut encore éliminer certains APs qui sont trop proche d'AP courant. En fait, si le MN qui se déplace à grande vitesse se connecte à des APs qui sont trop proche d'AP courant, cela provoque le changement d'AP plus fréquent.

Une fois que le routeur E-HCF a éliminé certains APs, il classe les APs restants en une liste des APs selon notre algorithme de classement. Notre algorithme est présenté ici :

- Les APs classés en premier sont ceux qui sont les moins chargés et qui n'impliquent pas de handover de niveau 3 (c'est-à-dire le changement d'AP n'implique pas de changement de réseau).

- Les APs classés en second sont ceux qui sont les moins chargés et qui impliquent le handover de niveau 3.

- Les APs classés en troisième sont ceux qui sont les moins chargés, qui appartiennent à l'autre E-HCF et qui n'impliquent pas le handover de niveau 3.

- Les APs classés en quatrième sont ceux qui sont les moins chargés, qui appartiennent à l'autre E-HCF et qui impliquent le handover de niveau 3.

Nous présentons un exemple d'application de ce procédé dans la figure 28. Nous supposons que :

Le MN est venue d'AP *1* (qui est l'AP précédent) et se connecte à l'AP *2* (qui est l'AP courent) pour l'instant.

- Selon la trajectoire potentielle du MN, le routeur E-HCF élimine d'abord l'AP *1* puisque le MN est venue de cet AP. Parmi les APs *3 et 4,* si le MN va tout droit, il est évident qu'il ne puisse pas utiliser l'AP 3. Donc, le routeur E-HCF propose l'AP 4 au MN comme l'AP potentiellement utilisable.

Le MN réussit à se connecter à l'AP *4*. Il peut choisit l'AP *5 ou 6* comme le prochain AP.

- Supposons que les APs *4* et *6* appartiennent à un même réseau et que les APs *4* et *5* n'appartiennent pas à un même réseau, le routeur E-HCF classe l'AP *6* avant l'AP *5.* Notons que, si l'AP *6* était beaucoup plus chargé que l'AP *5,* le routeur E-HCF

devrait mettre l'AP *5* avant l'AP *6* même si ce changement d'AP implique le handover de niveau 3.

Notre MN est maintenant connectée à l'AP *6*, puis, il continue à aller tout droit. Il se connecte donc à l'AP *9.* Ensuite, il doit choisir l'AP *11 ou 17* comme le prochain AP.

- Ici, nous calculons la vitesse de déplacement du MN en fonction de la distance entre les APs *4* et *9* et de l'intervalle entre le moment de la connexion avec l'AP *4* et le moment de la connexion avec l'AP *9*. Supposons que le MN se déplace à une grande vitesse, il vaut mieux utiliser l'AP *17* pour éviter un changement d'AP supplémentaire (le changement d'AP *11* au AP *17* ou *20*).

Pour résumer, le routeur E-HCF construit la liste des APs potentiellement utilisables et l'envoi au MN au moyen du message E-HCFRep. Quand le MN reçoit ce message, il n'a plus besoin de lancer la phase de Découverte pour trouver les APs disponibles. Il sonde le premier AP de la liste proposé par le routeur E-HCF. Si cet AP répond à sa demande, le MN se connecte à lui. Si non, le MN va sonder et essayer de se connecter à l'AP suivant.

Donc, le délai minimum de la procédure du handover de niveau 2 est le suivant:

$$\mathbf{T}_{\text{Handover de niveau 2}} = \mathbf{T}_{\text{Découverte}} + \mathbf{T}_{\text{Authentification}} + \mathbf{T}_{\text{reassociation}} = 20 + 10 + 40 \text{ ms} = 70 \text{ ms}$$

Le délai maximum de la procédure du handover de niveau 2 est :

$$\mathbf{T}_{\text{Handover de niveau 2}} = \mathbf{T}_{\text{Découverte}} + \mathbf{T}_{\text{Authentification}} + \mathbf{T}_{\text{reassociation}} = 20 \times N + 10 + 40 \text{ ms} = 20 \times N + 50 \text{ ms}$$

Où, N représente le nombre d'APs que le MN doit sonder avant de pouvoir se connecter à un AP de cette liste. La valeur de N est décidée par l'administrateur du réseau, elle est moins de 3 par défaut.

3.3.2 Optimisation de la procédure du handover de niveau 3

Nous présentons ici l'optimisation de la phase de détection de mouvement, celles de la phase d'Auto-configuration d'adresses et de la phase de Mise à jour d'association.

3.3.2.1 Optimisation de la phase de détection de mouvement

Si le MN change l'AP et que ce nouveau AP appartient à un réseau différent, le changement d'AP entraîne un changement de réseau. Dans ce cas, le MN doit effectuer la procédure du handover de niveau 3 pour pouvoir maintenir sa connexion avec ses correspondants. Pour cela, le MN doit d'abord détecter le changement de réseau avant d'auto-configurer sa nouvelle adresse IP. Dans le chapitre 2, nous avons présenté plusieurs propositions pour détecter le mouvement (c'est-à-dire le changement de réseau). Dans ces propositions, la durée de la détection de mouvement est plus longue que celle que les applications temps réel peuvent supporter.

Pour détecter aussitôt que possible ce mouvement, nous utilisons également le handover de niveau 2 comme indice du déclenchement du handover de niveau 3, mais le MN n'a pas besoin d'entamer la procédure de Découverte de Voisin pour vérifier le changement de réseau. En effet, le routeur E-HCF a déjà proposé une liste des APs et de leurs routeurs d'accès correspondants au MN. Il suffit pour le MN de vérifier si le nouvel AP et l'AP précédent appartiennent à un même AR. Si la réponse est positive, le changement d'AP n'implique pas le changement de réseau. Si ce n'est pas le cas, un handover de niveau 3 se produit.

Notre méthode E-HCF n'a pas besoin d'effectuer la phase de Détection de mouvement définie dans protocole IPv6 Mobile. Avec notre méthode, le temps de la détection de mouvement est égal au temps de traitement d'information du MN, qui est ici négligeable, nous avons donc :

$\mathbf{T}_{\text{Détection de mouvement}} \approx 0$ ms

3.3.2.2 Optimisation de la phase d'Auto-configuration d'adresses

Le handover de niveau 3 nécessite que le MN change son adresse IP dans le nouveau réseau. Le temps d'auto-configuration d'une adresse IP atteint parfois plusieurs secondes : une seconde minimum dans le cas d'Auto-configuration d'adresses sans état, car la procédure DAD du standard représente un délai important dans la phase d'Auto-configuration d'adresses. Pour réduire le délai induit par cette procédure du standard, nous proposons que le routeur E-HCF attribue un pool d'adresses IP uniques au MN au moyen du message E-HCFRep. Pour chaque nouveau réseau où le MN va peut-être s'attacher, le routeur E-HCF attribue une adresse IP correspondante. Selon le réseau attaché, le MN peut donc choisir une adresse correspondante comme sa nouvelle adresse temporaire dans ce nouveau réseau. Par conséquent, le MN n'a pas besoin d'auto-configurer son adresse IP, ni de lancer la procédure DAD du standard pour vérifier l'unicité d'une adresse IP dans le nouveau réseau.

Afin que le MN puisse utiliser l'adresse IP attribuée par le routeur E-HCF sans entraîner de conflit d'adresses IP dans le nouveau réseau, nous proposons deux méthodes pour que le routeur E-HCF puisse proposer des adresses IP uniques au MN : la méthode *Interactive* et la méthode *Directe*.

La méthode Interactive :

Le routeur E-HCF réserve d'abord un pool d'adresses IP et génère une liste d'adresses IP, appelée *Liste Mobile*. Ces adresses IP sont uniquement distribuées au MN comme ses nouvelles adresses temporaires dans ces réseaux. Le routeur E-HCF crée et met à jour aussi une autre liste d'adresses IP, appelée *Liste Usage*. Ce sont les adresses IP utilisées en ce moment par les nœuds dans les réseaux.

Grâce à l'utilisation du protocole de Découverte de voisin, l'AR connaît toutes les adresses utilisées par les nœuds à cet instant dans le réseau. Il signale au routeur E-HCF toutes ces

adresses. En comparant les deux listes – *Liste Mobile* et *Liste Usage*, le routeur E-HCF peut trouver les conflits d'adresses potentiels dans les réseaux. Nous donnons deux moyens pour éviter le conflit d'adresses potentiel. Lorsque un nœud voudrait utiliser une adresse IP déjà réservée par le routeur E-HCF: soit le routeur E-HCF retire cette adresse IP de la *Liste Mobile*, c'est le plus simple à réaliser, soit, avant que le nœud fixe finit la procédure DAD du standard, le routeur E-HCF demande au AR d'envoyer le message – Annonce de voisin à ce nœud fixe pour signifier que cette adresse est déjà prise. Dans ce cas, le nœud fixe ne peut pas utiliser cette adresse.

Donc, nous pouvons assurer que le routeur E-HCF propose une adresse IP globale unique au MN.

La méthode Directe :

Cette méthode est plus simple à réaliser que la méthode *Interactive*. Comme la méthode *Interactive*, le routeur E-HCF réserve d'abord un pool d'adresses IP et génère une liste d'adresses IP *Liste Mobile*. Il fournit cette liste aux routeurs d'accès. Les routeurs d'accès gardent cette liste dans leurs caches.

Quand le nœud fixe auto-configure son adresse, il doit lancer la procédure DAD pour vérifier l'unicité de son adresse dans le réseau. Dans cette procédure, le nœud fixe doit diffuser le message *Sollicitation de voisin* à tous les nœuds de ce réseau. Parce que l'adresse dans le champ de l'adresse de source de ce message est indéterminée, quand l'AR reçoit ce message, il peut réaliser qu'il est un message Sollicitation de voisin utilisé par la procédure DAD. Si l'adresse dans le champ de l'adresse de destination de ce message est déjà existée dans la *liste Mobile*, l'AR envoie le message – *Annonce de voisin* à ce nœud pour signifier que cette adresse est prise. Dans ce cas, le nœud fixe ne peut pas utiliser cette adresse. Donc, nous pouvons aussi assurer que le routeur E-HCF propose une adresse IP unique au MN.

La méthode *Directe* est plus facile à réaliser, mais il manque de la souplesse par rapport de la méthode *Interactive*. Nous préférons d'utiliser cette méthode pour des raisons de sa simplicité et de sa modification minimal apportés aux ARs.

En conclusion, le MN peut utiliser l'adresse IP distribuée par le routeur E-HCF dans le nouveau réseau et que la procédure DAD peut être complètement évitée dans la procédure de handover. Le temps pour le MN d'avoir une adresse IP peut être négligeable avec notre méthode, nous avons donc :

$\mathbf{T}_{\text{Configurations d'adresse}} \approx 0$ ms

3.3.2.3 Optimisation de la phase de Mise à jour d'association

Quand le MN s'attache à un nouveau réseau, il utilise tout de suite l'adresse attribuée par le routeur E-HCF comme sa nouvelle adresse temporaire. Ensuite, il envoie le message *Annonce de voisin* à l'AR pour signaler son attachement dans ce réseau. Il envoie aussi le message MNHC au routeur E-HCF pour libérer les ressources réservées pour lui.

Pour accomplir la procédure du handover de niveau 3, le MN doit procéder à la phase de Mise à jour d'association avec le HA, la phase de Routabilité de retour et la phase de Mise à jour d'association avec les CNs (voir la section 2.2.2). Le délai de ces trois phases est égal à la somme total du temps d'aller-retour (en anglais Round Trip Time - RTT) des messages entre le MN, le HA et les CNs.

Le temps d'aller-retour entre les nœuds dans les réseaux qui se trouvent en Amérique du Nord est de 50 ms en moyenne [PingER06]. Si nous supposons que le MN, le HA et les CNs sont tout en Amérique du Nord, le temps de la phase de Mise à jour d'association est le suivant :

$\mathbf{T}_{\text{Mise à jour d'association}} = \mathbf{T}_{\text{Mise à jour d'association avec le HA}} + \mathbf{T}_{\text{Routabilité de retour}} + \mathbf{T}_{\text{Mise à jour d'association avec le correspondant}} = 50 + 75 + 50 \text{ ms} = 175 \text{ ms}$

Le délai total pour le handover de niveau 3 est le suivant:

$\mathbf{T}_{\text{Handover de niveau 3}} = \mathbf{T}_{\text{Détection de mouvement}} + \mathbf{T}_{\text{Configurations d'adresse}} + \mathbf{T}_{\text{Mise à jour d'association total}} = 0 + 0 + 175 \text{ ms} = 175 \text{ ms}$

Nous pouvons constater que le délai de handover diminue grâce à notre méthode de handover.

Par ailleurs, le temps d'aller-retour entre les nœuds dans les réseaux dépend de la distribution géographique des nœuds et de l'état du réseau. Il est impossible de réduire largement cette valeur. Certaines approches sont proposées pour réduire l'effet du délai de la phase de Mise à jour d'association. Parmi les propositions, le protocole HMIPv6 propose d'ajouter une entité MAP dans les réseaux qui fonctionne comme un HA local. Quand le MN se déplace dans le domaine de MAP, il met à jour l'association entre l'adresse LCoA et RCoA avec MAP. Le temps d'aller-retour des messages entre le MN et la MAP est plus court par rapport à celui entre le MN et son HA. Donc, le délai de Mise à jour d'association est réduit. Mais un tunnel bidirectionnel devrait être créé entre le MN et la MAP et rester toujours actif. Les paquets des CNs sont envoyés à l'adresse RCoA du MN, la MAP intercepte ces paquets et les redirige à l'adresse LCoA du MN. De même, les paquets du MN sont envoyés à l'adresse RCoA en traversant le tunnel, la MAP intercepte ces paquets et les redirige aux CNs.

En outre, le protocole FMIPv6 n'a pas essayé de réduire le délai de la phase de Mise à jour d'association, il propose une autre façon de minimiser l'interruption de la communication due à cette phase. Un tunnel bidirectionnel est aussi crée entre le PAR et le NAR. Les paquets envoyés par le MN traversent le tunnel ; arrivent au PAR et sont redirigés par celui-ci aux CNs. Les paquets envoyés par les CNs arrivent au PAR et ensuite sont redirigés par celui-ci au MN via le tunnel.

Pour ces deux protocoles, les ARs doivent créer le tunnel bidirectionnel et rediriger les paquets vers le MN ou vers les CNs. Le temps de la création du tunnel, le délai du traitement des paquets et le charge supplémentaire pour les ARs ne sont pas négligeable

En réalité, l'utilisateur se déplace souvent dans une ville, ainsi la plupart du temps, il se déplace dans un campus ou dans un site industriel. La distance géographique entre l'utilisateur et le HA est souvent assez proche, ainsi le temps RTT entre eux est assez court. Pourtant, le temps d'aller-retour entre le MN et le CN peut être très variante.

Selon le protocole IPv6 Mobile, le MN doit envoyer le message – Mise à jour d'association au HA et aux CNs pour mettre à jour l'association entre son adresse temporaire et son adresse mère. Cette association a une durée de vie limitée qui est indiquée dans le message. Une fois la durée de vie est expirée, les CNs doivent envoyer les paquets à l'adresse mère du MN à la place du MN. Par conséquent, afin de rafraîchir la durée de la validité de cette association, le MN doit envoyer périodiquement le message – Mise à jour d'association au HA et aux CNs. Toutefois, il envoie simplement le message au HA et aux CNs sans entamer la procédure de Routabilité de Retour. Nous proposons d'utiliser cette fonctionnalité pour réduire l'effet du délai de la phase de Mise à jour d'association.

Le MN met fin à l'association entre son adresse mère et son adresse temporaire avec le HA et les CNs avant de procéder la procédure du handover. Dès que les CNs reçoivent le message – Mise à jour d'association, ils commencent à envoyer les paquets à l'adresse mère du MN. Le HA intercepte ces paquets et les garder dans son mémoire tampon. Une fois que le MN s'attache au nouveau réseau, il procède à la procédure de Mise à jour d'association avec le HA et les CNs. Le MN peut recevoir à nouveau les paquets après la phase de Mise à jour d'association avec le HA. Le HA continue d'intercepte et de rediriger les paquets des CNs vers la nouvelle adresse du MN jusqu'à l'accomplissement de la phase de Mise à jour d'association avec les CNs. Le HA aussi intercepte et redirige les paquets du MN vers l'adresse du CN.

Donc, nous pouvons dire que le délai d'interruption des communications n'est que le délai de la phase de Mise à jour d'association avec le HA.

3.3.2.4 Réduction de la perte des paquets

Quand le MN reçoit le message E-HCFRep, il va évaluer la possibilité de changement de réseau. Si le changement d'APs implique certainement le changement de réseau, le MN envoie le message - Mise à jour d'association au HA pour lui demander d'intercepter et de garder les paquets des CNs dans son mémoire tampon. Le MN envoie aussi le message : Mise à jour d'association aux CNs pour leur demander de mettre fin à l'association entre son adresse mère et son adresse temporaire, et d'envoyer les paquets à son adresse mère comme s'il était retourné dans son réseau mère, même si ce n'est pas la réalité. Une fois que le MN s'attache au nouveau réseau, il procède la procédure de Mise à jour d'association avec le HA et les CNs. Le MN peut recevoir à nouveau les paquets après la phase de Mise à jour d'association avec le HA. Le HA intercepte et redirige les paquets des CNs vers la nouvelle adresse du MN jusqu'à l'accomplissement de la phase de Mise à jour d'association avec les CNs. Le HA aussi intercepte et redirige les paquets du MN vers l'adresse du CN.

3.3.3 Procédures du handover gérées par la méthode E-HCF

Avant de comparer notre méthode et les autres, nous expliquons les procédures du handover du MN gérées par la méthode E-HCF quand le MN change d'un AP d'un réseau au celui d'un autre réseau (Figure 28) :

1) MN se déplace dans le réseau. Quand la puissance du signal (RSSI) descend en dessous d'un seuil prédéterminé ou quand l'AP courant ne peut plus garantir son service, le MN envoie le message MNReq au routeur E-HCF pour demander les informations de réseaux. Il fourni au routeur E-HCF le BSSID d'AP courant, éventuellement, les BSSID des APs connectés auparavant et les moments de la connexion avec ces APs au moyen de ce message. Avec les BSSID des APs, nous pouvons prédire son trajectoire probable. Dans notre future recherche, il peut aussi ajouter le temps d'attachement à chaque AP, avec ce temps, nous pouvons calculer la vitesse de son déplacement, et mieux choisir un AP selon sa vitesse et trajectoire probable.

2) Le routeur E-HCF répond à la demande du MN en lui envoyant un message E-HCFRep. Le routeur E-HCF propose une liste des APs disponibles et offre les adresses IP disponibles qui correspondent au réseau où chaque AP se trouve. Si l'AP auquel le MN va s'attacher appartient au réseau d'un routeur E-HCF distant. Le routeur E-HCF origine va envoyer le message Int-E-HCFReq au routeur E-HCF distant pour lui demander de lui fournir les adresses IP disponibles correspondantes et de mettre à jour des informations relatives, telles que l'adresse MAC du AR, l'adresse IP du AR, etc. Le routeur E-HCF distant envoie le message Int-E-HCFRep comme la réponse.

3) En recevant le message MNReq, le routeur E-HCF s'arrêt de transférer les paquets qui sont destinés au MN, les bufférisер dans son mémoire tampon afin d'éviter la perte de ces paquets durant la procédure du handover.

4) Ensuite, le MN se déconnecte avec son AP courant, et essaie de se connecter avec le première AP de la liste. Si le premier AP répond aux critères du MN, le MN se connecte à lui. Si non, le MN va se connecter à l'AP suivant de la liste. Une fois le MN s'est connecté à un nouvel AP, d'après le BSSID de l'AP et les informations fournis par le message E-HCFReq, le MN peut réaliser instantanément s'il a changé de réseaux. Si le handover de niveau 2 implique le handover de niveau 3 pour ce MN, il va utiliser la nouvelle adresse IP correspondante.

5) Une fois le MN s'attache au nouveau réseau, il envoie le message "Sollicitation de voisin" à l'AR courant pour prouver l'accessibilité de l'AR et signaler sa présence dans ce réseau. L'AR lui répond en envoyant le message "Annonce de voisin". Le MN envoie aussi le message MNHC au routeur E-HCF pour l'informer de son attachement dans le réseau. Une fois que le routeur E-HCF reçoit ce message, il libère les ressource réservées et envoie le message E-HCFHC au MN comme confirmation.

6) En même temps, le MN effectue la procédure de Mise à jour d'association avec le HA. Quand le HA reçoit le message "Mise à jour d'association", il envoie le message "Acquittement de mise à jour d'association" au MN comme réponse. Il envoie aussi les paquets stockés dans son mémoire tampon au MN, dans le cas où le MN a effectué la procédure de réduction de paquets.

7) Le MN lance la procédure de Routabilité de retour. Une fois que cette procédure est finie, il va mettre à jour la table des associations de son correspondant en échangeant les messages : Mise à jour d'association et l'acquittement de Mise à jour d'association.

8) Le MN peut donc communiquer directement avec son correspondant en utilisant le routage optimisé.

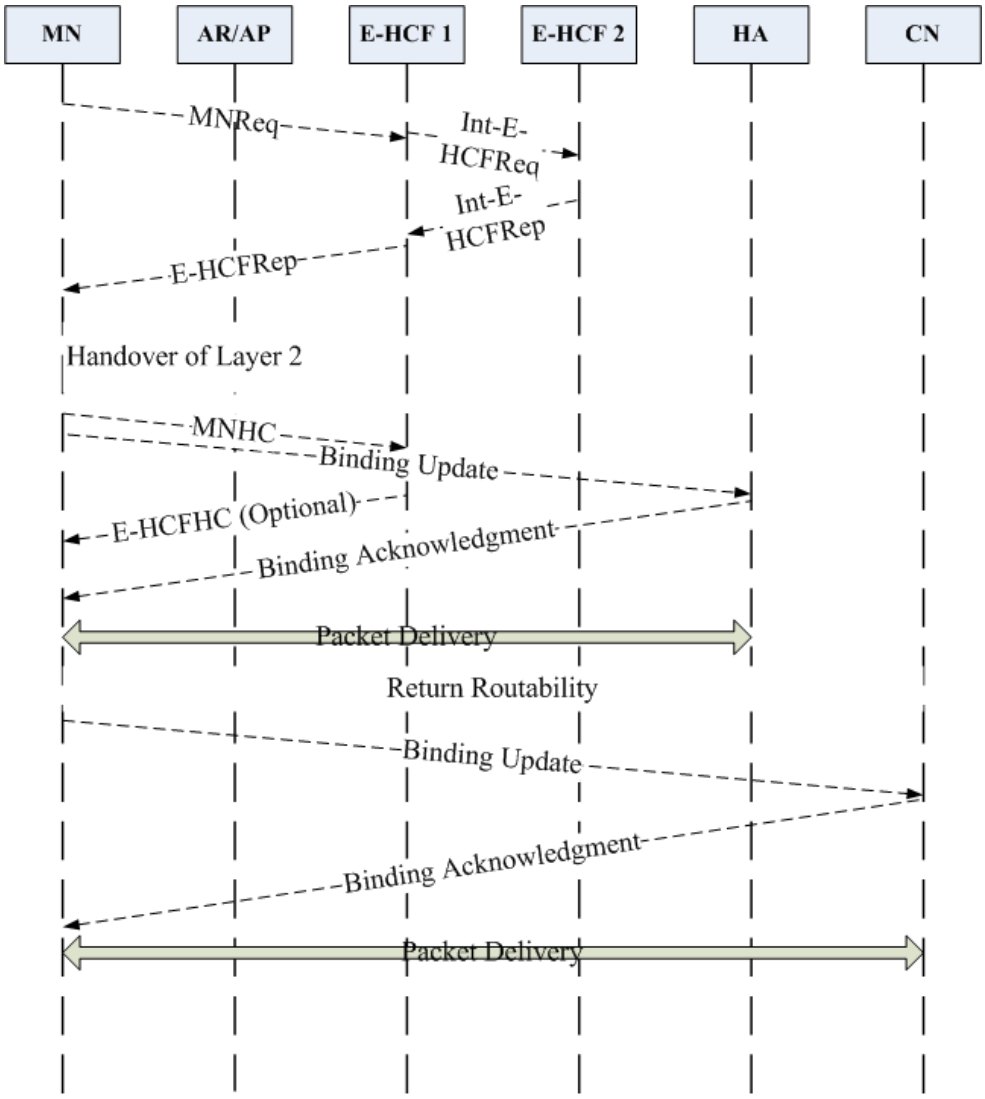


Figure 27 : Procédure d'Handover Avec Méthode E-HCF

3.4 Délai de la procédure du handover gérée par l'E-HCF

Pour vérifier la durée de la procédure du handover gérée par la méthode E-HCF, nous donnons les notations suivantes :

- $\mathbf{T}_{\text{Handover de niveau 2}}$: est le délai total de la procédure du handover de niveau 2 gérée par la méthode E-HCF.
- $\mathbf{T}_{\text{MNReq}}$: est le délai de transmission d'un message MNReq du MN à son routeur E-HCF origine.
- $\mathbf{T}_{\text{décision}}$: est le délai nécessaire pour qu'un routeur E-HCF puisse construire et classer une liste des APs avec lequel le MN va y attacher, y compris les délais pour l'échange des messages Int–E-HCFReq et Int–E-HCFRep.
- $\mathbf{T}_{\text{E-HCFRep}}$: est le délai de transmission d'un message E-HCFRep.
- $\mathbf{T}_{\text{E-HCFHC}}$: est le délai de transmission d'un message E-HCFHC.
- $\mathbf{T}_{\text{Mise à jour d'association}}$: est le délai pour achever la phase Mise à jour d'association avec le HA et le CN.

Donc, le délai total peut être exprimé comme suit :

$$\mathbf{T}_{\text{E-HCF}} = \mathbf{T}_{\text{Handover de niveau 2}} + \mathbf{T}_{\text{MNReq}} + \mathbf{T}_{\text{décision}} + \mathbf{T}_{\text{E-HCFRep}} + \mathbf{T}_{\text{E-HCFHC}} + \mathbf{T}_{\text{Mise à jour d'association}}$$

Puisque le délai de transmission du message dépend de la bande passante du réseau et un délai de traitement dépend de la capacité de calcul, on peut estimer le délai total $\mathbf{T}_{\text{E-HCF}}$ selon la bande passante et la capacité de calcul. Les valeurs de la bande passante et de la capacité choisies pour l'estimation de $\mathbf{T}_{\text{E-HCF}}$ sont notées dans le tableau ci-dessous.

Tableau 13 : Paramètres et valeurs pour estimer E-HCF

Paramètre	Valeur	Comment
Temps pour scanner des sous canaux (en moyenne)	200 ms	MIPv6 standard
Délai moyen de BU/BA	175 ms	MIPv6 standard
Débit du réseau	5.5 Mb/s	IEEE 802.11b
Débit du réseau	2 Mb/s	UMTS
Débit du réseau	150 kb/s	GPRS
Débit du réseau	9 kb/s	GSM
Capacité d'un routeur	20 Mb/s	Capacité de calcul
Capacité d'une station mobile	10 Mb/s	Capacité de calcul
Taille du message MNReq	72 octets	Handover E-HCF
Taille du message E-HCFRep	45 octets	Handover E-HCF
Taille du message Int–E-HCFReq	45 octets	Handover E-HCF
Taille du message Int–E-HCFRep	45 octets	Handover E-HCF
Taille du message MNHC	45 octets	Handover E-HCF
Taille du message E-HCFHC	24 octets	Handover E-HCF

Selon les valeurs citées dans le tableau 14, on estime le délai total en fonction du réseau sans fil, la taille d'un message et la capacité de calcul. La figure 26 illustre une comparaison de délai du handover. Par rapport au délai moyen par MIPv6 standard (1290 ms), le délai du handover géré par la méthode E-HCF est réduit à 200–250 ms avec un réseau de haut débit.

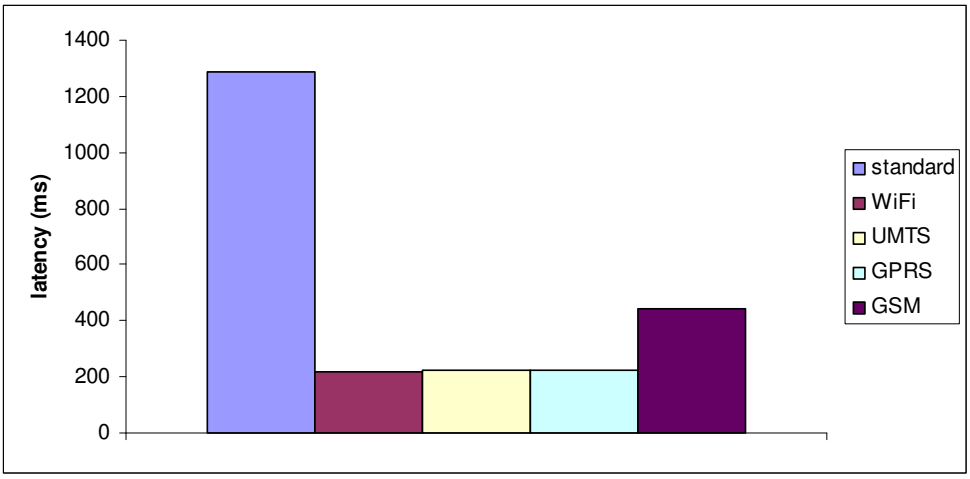


Figure 28 : Comparaison des délais avec E-HCF par rapport à celles avec standard

L'avantage principal de la procédure du handover gérée par la méthode E-HCF est de réduire le délai en supprimant la phase DAD. Bien entendu, une gestion centrale a un coût supplémentaire (délai supplémentaire concernant la maintenance de la fonction E-HCF). Nous avons montré que le délai pourrait réduire de 2080 ms à 100 ms par analyse et par simulation. Ceci signifie que la procédure du handover E-HCF est efficace.

Ensuite, nous utilisons une table de synthèse pour comparer les différentes propositions dans le but d'améliorer le handover du protocole IPv6 Mobile dans le réseau Wi-Fi.

Nous vous rappelons que la mobilité du MN implique le handover de niveau 2 (le changement d'AP) et le handover de niveau 3 (le changement de réseau).

3.5 Conclusion

Les principaux problèmes du handover de niveau 2 et du handover de niveau 3 viennent du fait que le délai des procédures du handover est trop important pour de nombreuses applications, surtout pour les applications temps réel. Le délai entraîne à la fois des interruptions de communication et des pertes de paquets perceptibles pour les utilisateurs. Comme nous l'avons décrit, notre méthode permet de réduire le délai du handover de niveau 2 des 200 ms (ou plus) aux 40 ms. Pour le délai du handover de niveau 3, avec la méthode E-HCF, nous ressuons d'éliminer les délais provoqués par la phase de Detection de mouvement et par la phase d'Auto-configuration d'adresses. Pour réduire la perte des paquets due aux procédures du handover, nous proposons de modifier le protocole IPv6 Mobile. Le Nœud Mobile met fin à la association entre son adresse mère et son adresse temporaire avec l'agent mère et les Nœuds Correspondants avant de procéder la procédure du handover. Par conséquent, nous pouvons utiliser l'agent mère pour intercepter et rediriger les paquets des Nœuds Correspondants ou du Nœud Mobile vers la nouvelle adresse du Nœud Mobile ou vers les adresses des Nœuds Correspondants respectivement pendant la phase de Mise à jour d'association. Avec cette méthode, nous pouvons limiter la perte de paquets et garantir un délai acceptable.

4 Amélioration de performance par E-HCF

Nous avons présenté notre méthode E-HCF qui a pour objectif d'améliorer la performance du handover dans le chapitre 3. Dans ce chapitre, nous utilisons OPNET pour simuler les procédures du handover dans les réseaux Wi-Fi. Dans ce chapitre, nous présentons d'abord le simulateur OPNET. Ensuite, nous présentons les résultats des simulations et analysons les résultats obtenus par les simulations.

4.1 Simulateur OPNET

OPNET est un outil de modélisation et de simulation de réseaux qui est développé et commercialisé par OPNET Technologies Inc. [OPNET]. Il est aujourd'hui un standard de référence dans le domaine de la simulation de réseaux.

Il existe d'autres outils de simulation de réseaux similaires, tels que NS-2 [NS2], OMNET++ [OMNET]. Nous avons choisi OPNET en tant que l'outil de simulation de réseaux, parce qu'OPNET qui est développé en C++ utilise un environnement graphique et est exécutable sous Unix et sous Windows. Ces caractéristiques nous permettent de concevoir, d'étudier, de modifier et de simuler des réseaux et des protocoles de communication avec une grande flexibilité. Par ailleurs, OPNET nous permet également de simuler plusieurs sortes de matériels, comme les routeurs, les switches qui sont fabriqués par Cisco, Nortel ou Lucent…. Grâce à cela, touts les réseaux existants deviennent très faciles à être modélisés et simulés.

L'environnement de simulation de réseaux d'OPNET est organisé d'une façon hiérarchique. Il est composé de trois niveaux : le niveau du modèle de réseau, le niveau du modèle de nœud et le niveau du modèle de processus.

Niveau du modèle de réseau

C'est le niveau supérieur de la hiérarchie de l'environnement de simulation de réseaux d'OPNET. Il représente un réseau qui est un ensemble des nœuds de réseaux et de liens interconnectés entre eux. Les nœuds de réseaux communiquent en utilisant les protocoles, leurs comportements sont définis par les paramètres préconfigurés. Les nœuds de réseaux peuvent aussi être définis au niveau inférieur, c'est-à-dire au niveau du modèle de nœud.

L'utilisateur utilise l'éditeur de projet (*en anglais Project Editor*) pour créer une simulation de réseaux: la topologie du réseau, les caractéristiques des liens physiques, les protocoles utilisés, les communications qui ont lieu... Par exemple, dans notre simulation, nous

concevons un réseau en plaçant les nœuds de réseaux, tels que les MNs, les routeurs principaux et les routeurs d'accès (*en anglais Access Router – AR*), les terminaux dans les endroits appropriés. Ces nœuds peuvent être reliés ensemble en utilisant des câbles filaires ou des antennes radio. Nous pouvons aussi utiliser un outil de définition de trajectoire qui est développé par OPNET pour simuler la trajectoire des MNs. Avec cet outil, nous pouvons définir la vitesse, la durée et l'orientation du déplacement du MN. En utilisant l'éditeur de projet, nous pouvons aussi choisir des statistiques du réseau à collecter, lancer une simulation, et analyser les résultats des simulations.

L'architecture de réseaux de notre projet est présentée dans la figure 29 :

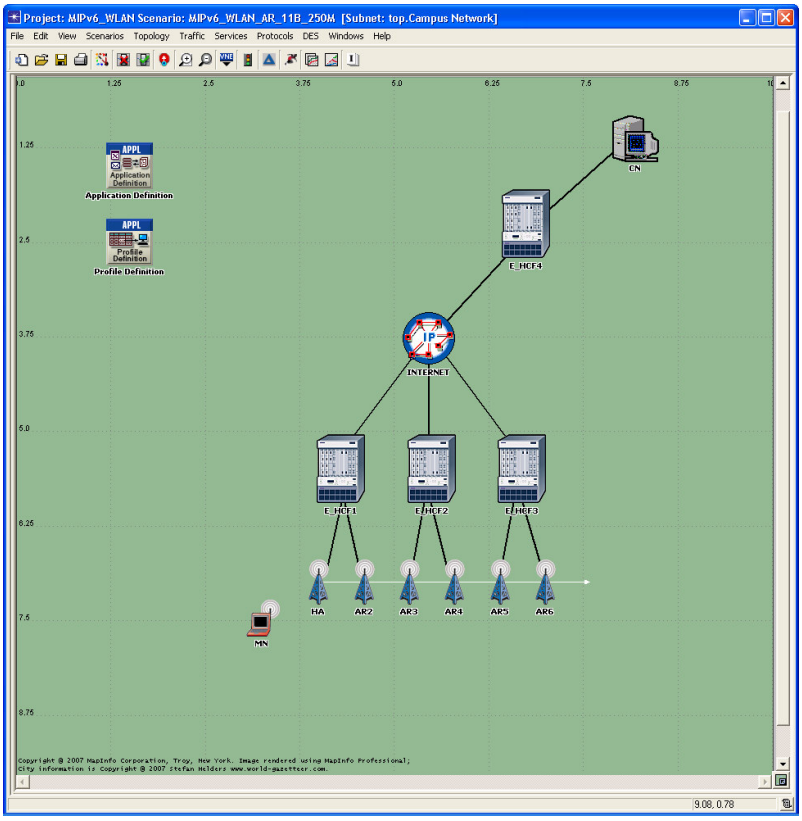


Figure 29 : Architecture de réseaux avec E-HCF implanté dans OPNET

Dans cette figure, les routeurs E-HCF se communiquent via Internet. Les APs de type IEEE 802.11b ou IEEE 802.11g sont intégrés dans les ARs. Donc, il n'y a pas d'AP affiché dans cette figure. Les ARs sont reliés avec le routeur E-HCF par les câbles filaires. La couverture de chaque AR est de 250 mètres. C'est une valeur définie par les paramètres. La distance entre les deux routeurs d'accès est de 500 mètres. Le MN se connecte à l'AR en onde radio et se déplace dans le réseau.

Niveau du modèle de nœud

Il représente typiquement la pile du protocole d'un nœud de réseau. Un nœud dans un réseau se compose typiquement des modules multiples qui définissent son comportement. Un module peut être un processus, une file d'attente, un générateur de données, un

émetteur, un récepteur ou bien une antenne. Les modules sont liés entre eux par des connexions de type flux de paquets (c'est pour le transport des données) ou de type fils de statistique (c'est pour la transmission des signalisations). Grâce à l'éditeur de nœuds (en anglais Node Editor), nous pouvons créer des nœuds de réseau comme un routeur, un ordinateur, etc. (Voir la figure 30).

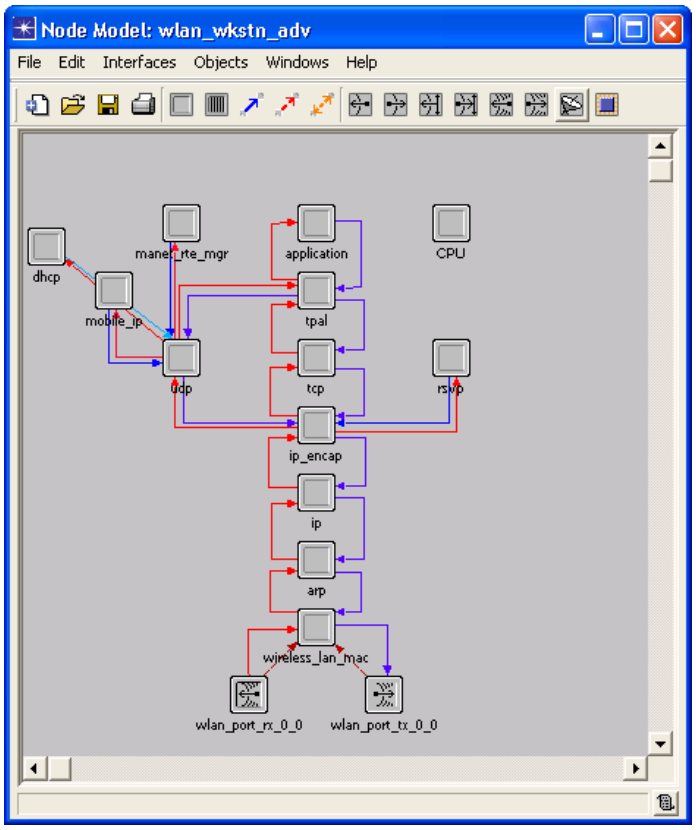


Figure 30 : Exemple de nœud construit avec l'éditeur de nœuds

Niveau du modèle du processus

Il facilite la définition du comportement d'un module appartenant à un nœud par l'utilisation des différents processus. Les processus sont des machines à états finis (*en anglais Finite State Machines – FSMs*) construites en langage C/C++. Le processus se compose des états et des transitions entre ces états. Il y a deux types d'états: les états obligatoires (*en anglais forced states*) et les états non-obligatoires (*en anglais unforced states*). Un processus peut attendre dans un état non-obligatoire tandis qu'un processus doit quitter l'état obligatoire sans délai dès qu'il entre dans cet état.

Chaque état se compose d'un état d'entrée et d'un état de sortie. OPNET permet d'ajouter du code dans l'état d'entrée et dans l'état de sortie. Lorsque le processus entre dans un état d'entrée, il exécute du code de l'état d'entrée (*en anglais enter executives*). Avant que le processus quitte cet état, il doit exécuter du code de l'état de sortie (*en anglais exit executives*).

OPNET a fourni des instructions et des fonctions détaillées pour définir les processus typiques de réseaux. Cependant, des antennes, des émetteurs, des récepteurs et des générateurs sont déjà prédéfinis dans OPNET et ne peuvent pas être édités à ce niveau.

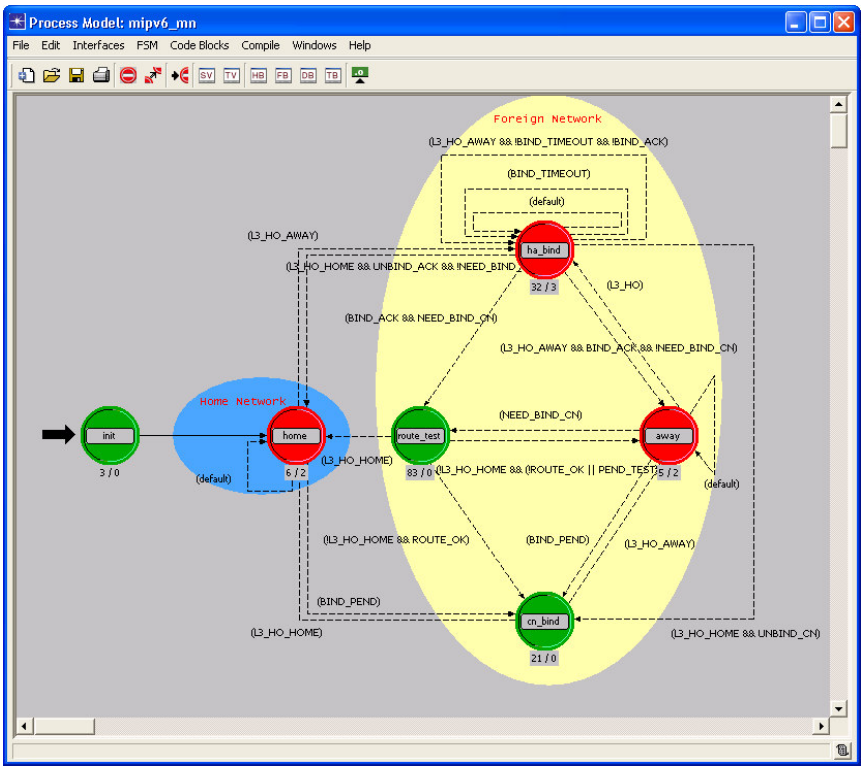


Figure 31 : Exemple de processus du MN du protocole IPv6 Mobile construit avec l'éditeur de processus

Ici, nous résumons le principe de développement d'un projet. Lorsque l'on crée un nouveau projet, il faut dans un premier temps définir l'objectif de la simulation, la topologie du réseau, les nœuds du réseau (ordinateurs, routeur, etc.…). Chacun de ces nœuds, comme vu précédemment, sont composés de différents modules qui sont composés eux-mêmes de différents processus réalisés avec un diagramme d'état.

Nous allons simuler d'abord les procédures du handover dans les réseaux Wi-Fi gérées par la norme IEEE 802.11 et le protocole IPv6 Mobile, ensuite nous allons simuler les procédures du handover gérées par notre méthode E-HCF qui est conçue pour optimiser la performance du handover dans les réseaux Wi-Fi. Dans notre projet, nous allons utiliser différents types d'applications, telles que la VoIP, la Vidéo conférence et le FTP (*en anglais File Transfer Protocol – FTP*), qui génèrent différents flux de données dans les réseaux, pour évaluer et analyser les performances du handover des MNs dans les réseaux Wi-Fi.

Nous présentons d'abord dans le paragraphe suivant les caractéristiques des applications.

4.2 Caractéristiques des applications

Nous utilisons des applications qui génèrent un flux de données d'un débit constant pour bien observer l'interruption de la réception des flux de données au MN et la perte de paquets à cause du handover dans les réseaux Wi-Fi. Les applications que nous avons choisies sont classées selon leur mode de transport : le mode fiable avec le protocole TCP (*en anglais Transmission Control Protocol – TCP*) et le mode non-fiable avec le protocole UDP (*en anglais User Datagram Protocol – UDP*).

Les protocoles TCP et UDP sont les deux protocoles principaux de la couche transport. La couche transport se trouve entre la couche session et la couche réseau du modèle OSI. Le rôle principal de la couche transport est de prendre les messages de la couche session, de les segmenter s'il le faut en unités plus petites et de les passer à la couche réseau, tout en s'assurant que les morceaux arrivent correctement de l'autre côté. Cette couche effectue donc aussi le réassemblage du message à la réception des morceaux [IPZERO].

- Protocole TCP: est un mode fiable et orienté connexion. Il assure le contrôle du flux de données au moyen de fenêtres glissantes et utilise des numéros de séquence et des accusés de réception pour garantir bon acheminement des segments. Il retransmet tous segments non-reçus. Ce protocole présente l'avantage de garantir la transmission des données.

- Protocole UDP : est un mode non fiable et sans connexion. Bien que chargé de la transmission des messages, il n'exécute aucune vérification logicielle sur l'acheminement des segments au niveau de cette couche. L'avantage de ce protocole est sa vitesse. Comme il ne fournit pas d'accusés de réception, le trafic dans le réseau est plus faible, ce qui accélère les transferts.

4.2.1 Applications utilisant le protocole TCP

Les applications qui demandent la fiabilité de transfert des flux de données utilisent en général le protocole TCP, c'est le cas de l'application Email, la messagerie instantanée, le SSH (Secure Shell), l'application Web, le FTP (File Transfer Protocol), etc.

FTP

Le protocole FTP est un protocole de communication dédié à l'échange informatique de fichiers sur un réseau TCP/IP. Il permet, depuis un ordinateur, de copier des fichiers depuis ou vers un autre ordinateur du réseau, d'administrer un site web, ou encore de supprimer ou modifier des fichiers sur cet ordinateur. Il utilise le mode client-serveur, c'est-à-dire qu'un ordinateur qui joue le rôle du client envoie des commandes, et l'autre qui joue le rôle du serveur attend des requêtes pour effectuer des actions. Lors d'une connexion FTP, le protocole TCP est utilisé pour créer deux connexions virtuelles : l'une sert à transférer les commandes, et l'autre sert à transférer de données.

Nous définissons un modèle de FTP. Le MN envoie la commande avec un intervalle d'une seconde pour télécharger le fichier du serveur. La taille de fichier est constante, elle est de 50 000 octets. Avec ce modèle, nous pouvons recevoir un flux d'un débit constant de 50 Koctets/s à la couche transport sous le format du paquet TCP avec une fréquence de 9 paquets TCP/s et un flux d'un débit constant de 435 Kbits/s à la couche MAC du MN. (Voir la figure 32).

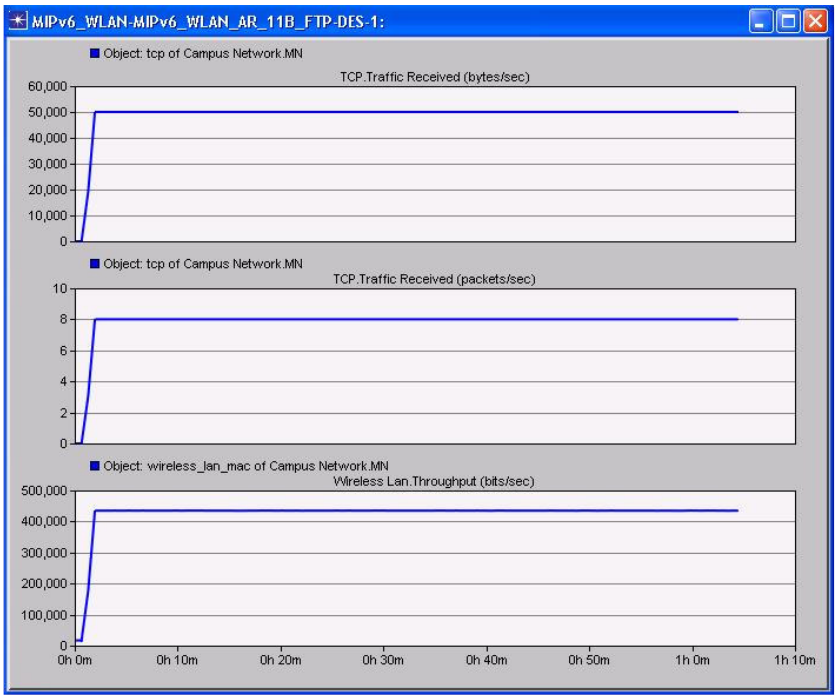


Figure 32 : Réception d'un flux d'un débit constant d'application FTP au MN

4.2.2 Applications utilisant le protocole UDP

Avec le protocole UDP, les applications peuvent simplement encapsuler des datagrammes IP et les envoyer sans établir de connexion. Donc, le protocole UDP est adapté aux applications en temps réel, tel que la VoIP, la Vidéo conférence, etc.

En effet, les applications multimédias se composent de plusieurs flux : son, vidéo, texte et éventuellement d'autres flux. Pour transporter ces flux media sur réseaux IP, il faut utiliser non seulement le protocole UDP, mais aussi le protocole RTP (en anglais *Real-Time Transport Protocol – Protocole de Transmission en Temps Réel*) [RFC 1889]. Le protocole RTP est un protocole de transport implanté dans la couche applications. Comme le protocole UDP, le protocole RTP ne bénéficie d'aucun contrôle de flux, ni de contrôle d'erreurs, ni d'acquittement, ni de mécanisme de demande de retransmission, mais il peut multiplexer plusieurs flux de données en temps réel en un flux de paquets UDP qui est ensuite envoyé par le protocole UDP. Le protocole RTP permet aussi au récepteur de compenser la gigue et les éventuels déséquencements de paquets UDP introduits par les réseaux.

VoIP

La VoIP utilise le réseau IP pour offrir des communications vocales téléphoniques. Les sons sont d'abord numérisés, ensuite, ils sont transmis dans les réseaux IP sous forme de paquets, et sont reconvertis en sons à la destination. Les codecs audio sont utilisés pour convertir les sons sous forme de données digitales. Les différents types de codecs audio sont choisis par l'utilisateur selon la qualité de voix, le débit et le délai. La qualité de voix est très souvent notée par Score MOS (en anglais *Mean Option Score - MOS).*

Le tableau 14 présente les Scores MOS et le tableau 15 présente les caractéristiques des différents types de codecs [HERS].

Tableau 14 : Score MOS

Score MOS	Définition	Exemple
4 à 5	Haute qualité	Téléphone RNIS
3,5 à 4	Qualité commerciale	Téléphones fixe classiques
3 à 3,5	Qualité acceptable avec dégradation perceptible	
2,5 à 3	Qualité militaire	
Moins de 2,5	Qualité synthétique	Voix robotisée

Tableau 15 : Caractéristiques des différents codecs audio

Codec	MOS	Débits	Délai
G.711	4,2	64 Kbits/s	125µs
G.722	5	48, 56 ou 64 Kbits/s	1,5ms
G.722.1	4,8	24 ou 32 Kbits/s	20ms
G.723.1	3 ,7/3,9	5,3/6,4 Kbits/s	30ms
G.729	4,0	8 Kbits/s	10ms

Les operateurs de VoIP voudraient réduire la bande passante utilisée par chaque utilisateur. En effet, Pendant une conversation, nous ne parlons en général que 35% du temps, et par conséquent il est très utile de pouvoir supprimer ces périodes de silence. Dans les conversations de point à point, cela permet d'économiser jusqu'à 50% de la bande passante et beaucoup plus pour des conversations multipoint. Donc, la technique de compression de silence est utilisée pour réduire l'utilisation de la bande passante. Avec cette technique, les codecs peuvent stopper la transmission d'information quand le module Detection d'activité vocale (*en anglais Voice Activity Detection – VAD*) a détecté une période de silence. Donc, le flux de données produit par les codecs n'est plus constant.

Pour avoir un flux d'un débit constant, nous avons fait le choix de ne pas utiliser la technique de compression de silence dans notre simulation. Nous utilisons le codec G.711 pour générer un flux d'un débit constant de 10 Koctets/s à la couche transport sous le format du paquet UDP avec une fréquence de 100 paquets UDP/s et un flux d'un débit constant de 128 Kbits/s en moyenne à la couche MAC au MN (Voir la figure 33).

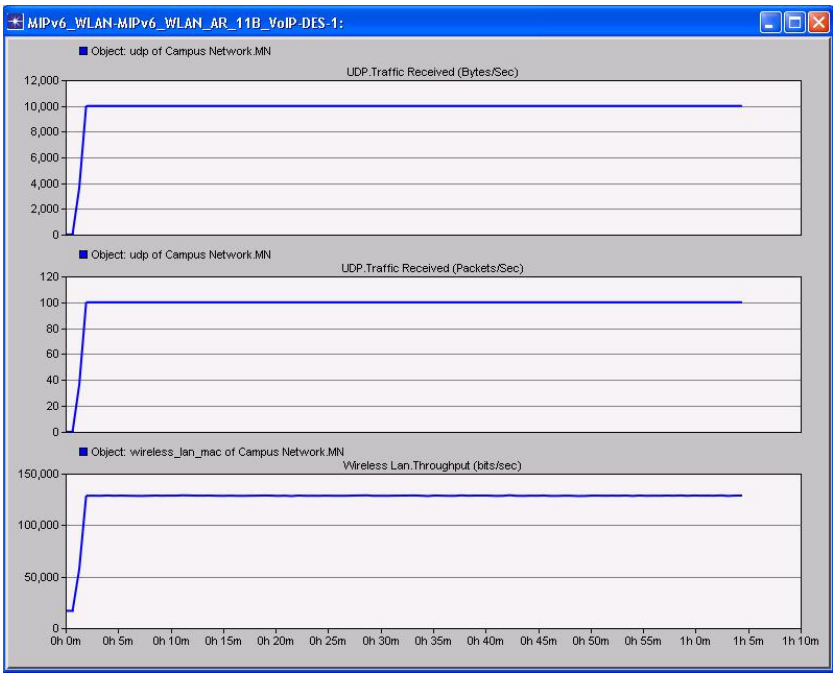


Figure 33 : Réception d'un flux d'un débit constant d'Application VoIP au MN

Vidéo conférence

La Vidéo conférence permet à un utilisateur de voir et de dialoguer avec son interlocuteur. Comme la VoIP, la Vidéo conférence utilise non seulement les codecs audio pour coder les paroles, mais aussi les codecs vidéo pour coder les images. La continuité des images constitue une vidéo. Nous pouvons choisir une vitesse de défilement de 10, 20 ou 30 images par seconde pour la vidéo sortante et entrante. Chaque image possède une résolution de 128 ×120 pixels, 128 × 240 pixels ou 352 × 240 pixels qui correspond à une taille d'image de 17280 octets, 34560 octets ou 253440 octets respectivement dans OPNET. La vitesse de défilement d'images et la qualité d'image décident de la qualité de la vidéo.

Le tableau 16 présente la qualité de la vidéo définie pour l'application - Vidéo conférence dans OPNET :

Tableau 16 : Qualité de la vidéo définie dans l'OPNET

Qualité de la vidéo	Vitesse de défilement d'image	Qualité d'image
Vidéo basse résolution	10 images/s	128 ×120 pixels
Vidéo haute résolution	15 images/s	128 × 240 pixels
Vidéo avec la qualité Magnétoscope	30 images/s	352 × 240 pixels

Nous choisissons la vidéo basse résolution pour notre simulation. Le MN et son correspondant envoient 10 images/s. Nous avons un flux d'un débit constant de 173 Koctets/s à la couche transport sous le format du paquet UDP avec une fréquence de 30 paquets UDP/s et un flux d'un débit constant de 1,45Mbits/s en moyenne à la couche MAC au MN. En fait, le MN envoie 10 images/s, comme la taille du data est de 17280

octets à la couche application, le data est fragmenté sous forme de segments pour les transférer. Donc, le MN reçoit 30 paquets UDP/s, c'est-à-dire qu'il reçoit 3 paquets UDP toutes les 100 ms.

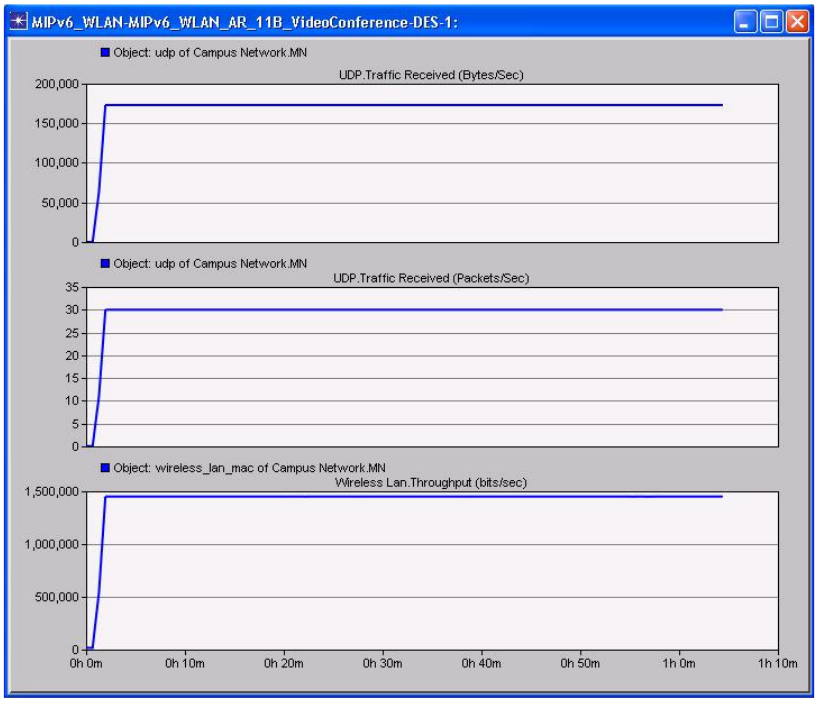


Figure 34 : Réception d'un flux d'un débit constant d'application Vidéo conférence au MN

Si nous utilisons la vidéo haute résolution pour notre simulation. Nous avons un flux d'un débit constant de 520 Koctets/s à la couche transport sous le format du paquet UDP et un flux constant de 4,3Mbits/s en moyenne à la couche MAC au MN. Mais la perte de paquets est produite pour les réseaux 802.11b, parce qu'il ne peut pas supporter ce débit important. En effet, pour transmettre la vidéo haute résolution dans les réseaux, les algorithmes de compression de vidéo, tel que MPEG-1, MPEG-2 et MPEG-4, sont utilisés pour réduire la taille de la vidéo.

4.3 Résultats et analyse de performance de E-HCF par simulations

Notre simulation a pour objectif de simuler la procédure du handover de niveau 2 et celle de niveau 3 dans un réseau Wi-Fi, de montrer la perte de paquets provoqués par le handover, de comparer les performances des procédures du handover gérées par la norme IEEE 802.11 et le protocole IP Mobile ou par notre méthode E-HCF. Afin de simplifier les explications des résultats, nous dénommons les procédures du handover gérées par la norme 802.11 et le protocole IPv6 Mobile, la méthode Standard, nous dénommons les procédures du handover gérées par notre proposition, la méthode E-HCF.

Nous rappelons que les procédures du handover incluent la procédure du handover de niveau 2 et la procédure du handover de niveau 3. La phase de découverte, la phase d'authentification et la phase de réassociation constituent la procédure du handover de niveau 2. La phase de Détection de mouvement, la phase d'Auto-configuration d'adresses et la phase de Mise à jour d'association constituent la procédure du handover de niveau 3. Il faut également noter que la phase de Mise à jour d'association est décomposée en trois phases: la phase de Mise à jour d'association avec le HA, la phase de Routabilité de retour et la phase de Mise à jour d'association avec le CN.

Comme nous l'avons analysé, la durée de la procédure du handover de niveau 2 gérée par la norme IEEE 802.11 est environ 300 ms. La durée de la procédure du handover de niveau 3 gérée par le protocole IPv6 Mobile est la somme totale de toutes les trois phases. La durée de la phase de Détection de mouvement est de 200 ms au minimum dans le cas où le MN utilise l'Absence de réception du message "Annonce de routeur" comme le signe du déclenchement du handover de niveau 3. Celle de la phase d'Auto-configuration d'adresses est de 1000 ms au minimum. Celle de la phase de Mise à jour qui est le temps d'aller-retour (RTT) entre le MN, le HA et le CN, est environ 175 ms. Par conséquent, La durée de la procédure du handover gérée par la méthode Standard est de 1675 ms au minimum. La durée de la procédure du handover de niveau 2 gérée par notre méthode E-HCF est de 70 ms en moyenne. Celle de niveau 3 gérée par notre méthode E-HCF est environ 175 ms, parce que la durée de la phase de Détection de mouvement et celle de la phase d'Auto-configuration d'adresses sont considérée comme négligeable, celle de la phase de Mise à jour d'association est la même que celle de la méthode Standard. Par conséquent, La durée de la procédure du handover gérée par la méthode E-HCF est de 245 ms au minimum.

Nous simulons les procédures du handover en utilisant un scenario avec trois différents types des applications – le FTP, la VoIP, la Vidéo conférence. Le scenario est donné dans la figure 35.

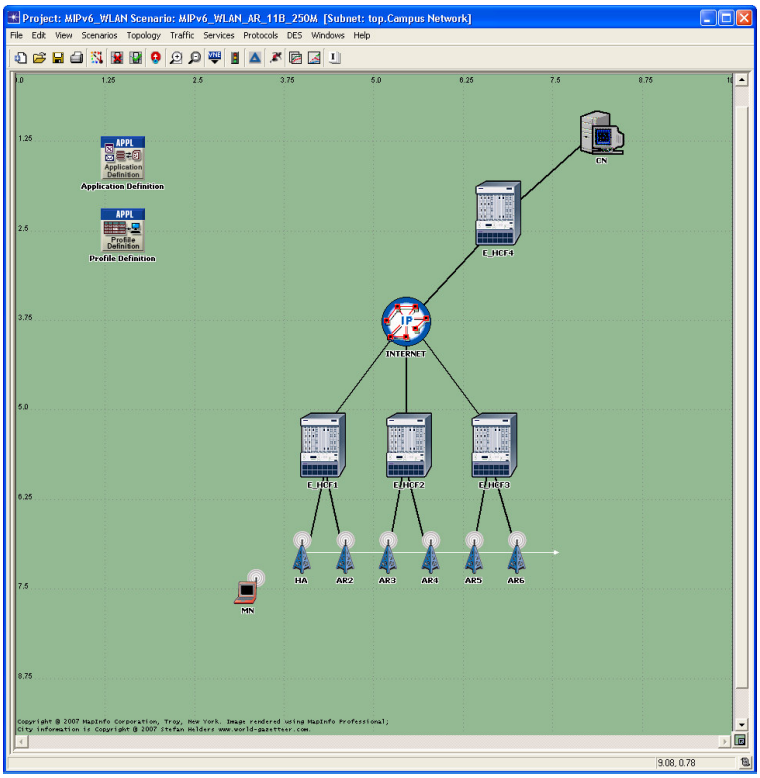


Figure 35 : Architecture de réseaux avec E-HCF implanté dans OPNET

Le MN se déplace en traversant les routeurs d'accès (*en anglais Access Router – AR*). La distance entre les deux routeurs d'accès est de 500 mètres. Quand le MN change de l'AR, cela implique un changement de réseau. Dans notre simulation, la vitesse de déplacement du MN est de 3 km/heure. C'est une vitesse moyenne de marche à pied. Nous pouvons aussi augmenter la vitesse de déplacement, cela ne produit pas un effet sur la durée du handover. Le temps d'aller-retour entre le MN et le HA ou le CN a une valeur entre 10 et 15 ms dans notre simulation. Le MN commence à lancer une application entre (100, 110) secondes, il se connecte d'abord à son HA et reste dans son réseau mère sans bouger pendant 5 minutes. Ensuite, il se déplace à une vitesse de 3 km/heure et traverse 5 ARs, il perd la connexion avec l'AR 6 après une heure de trajet. Nous observons 5 handovers qui se sont produits pendant la simulation, le premier handover est celui du réseau mère au réseau visité, et les autres sont ceux du réseau visité au réseau visité.

Nous pouvons choisir le nombre de valeurs collectées pour chaque statistique pendant la simulation. Du fait qu'OPNET génère une valeur d'une statistique à partir des données collectées pendant une période mesure. Plus le nombre de valeurs est grand, plus la période de mesure pour collecter les données est courte et plus le temps de la simulation augmente.

Les figures suivantes présentent les résultats des simulations. Le graphique du haut représente les résultats des simulations en utilisant la méthode E-HCF et celui du bas représente les résultats des simulations en utilisant la méthode Standard. Nous comparons et expliquons ces résultats de simulations dans les paragraphes suivants.

4.3.1 Résultats et analyse des simulations pour les applications utilisant le protocole UDP

Lorsque le MN et le CN lancent une application qui utilise le protocole UDP. Le MN et le CN envoient les paquets UDP en espérant que l'autre coté soit capable de les recevoir, il n'y a aucune garantie que les paquets UDP soient livrés à la destination. Si la connexion du réseau est coupée, les paquets sont perdus.

Nous présentons les résultats des simulations en utilisant l'application VoIP et ceux en utilisant l'application Vidéo conférence dans les paragraphes suivantes.

VoIP

Comme nous l'avons décrit, nous utilisons le codec G.711 pour générer un flux d'un débit constant de 10 Koctets/s à la couche transport sous le format de paquet UDP avec une fréquence de 100 paquets UDP/s.

La figure 36 présente une comparaison entre le délai du handover géré par la méthode Standard et celui du handover géré par la méthode E-HCF durant une durée de simulation de 3900 secondes. Il y a 5 handovers qui se sont produits pendant cette simulation.

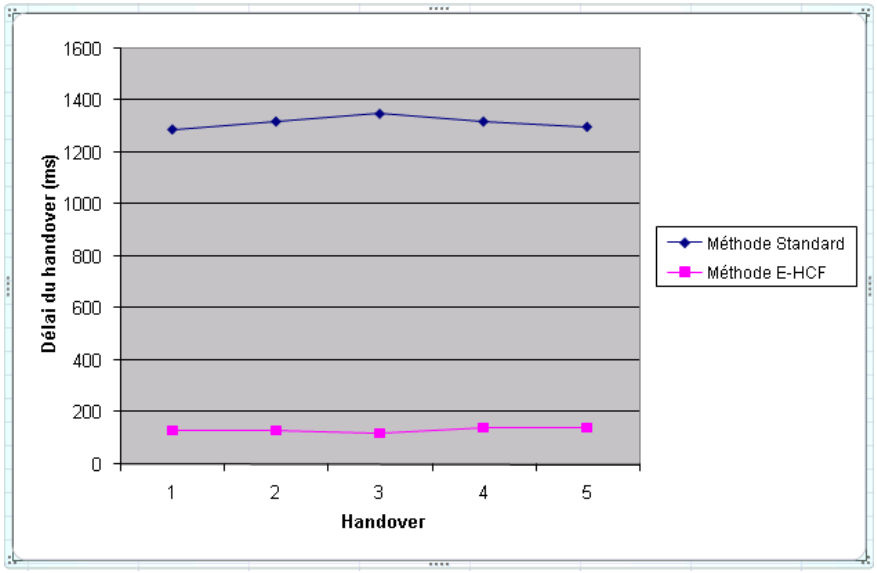


Figure 36: Comparaison entre le délai du handover géré par la méthode Standard et celui du handover géré par la méthode E-HCF

Le délai du handover dans les réseaux Wi-Fi est l'intervalle du temps compris entre le moment où le MN quitte son AP courant, jusqu'au moment où la phase de Mise à jour d'association a été effectuée. Dans la simulation, nous considérons le délai du handover comme étant l'intervalle du temps compris entre le moment où le MN ne reçoit plus les données d'une application VoIP, jusqu'au moment où le MN reçoit à nouveau les données d'une application VoIP.

La figure 37 présente la comparaison entre la méthode Standard et la méthode E-HCF pour la réception des paquets UDP au MN durant une durée de simulation de 3900 secondes. Il y a 5 handovers qui se sont produits pendant cette simulation. OPNET génère une valeur de statistique (paquets UDP/s) toutes les 100 ms. Nous pouvons constater la chute du débit reçu par le MN pendant cinq handovers durant la simulation.

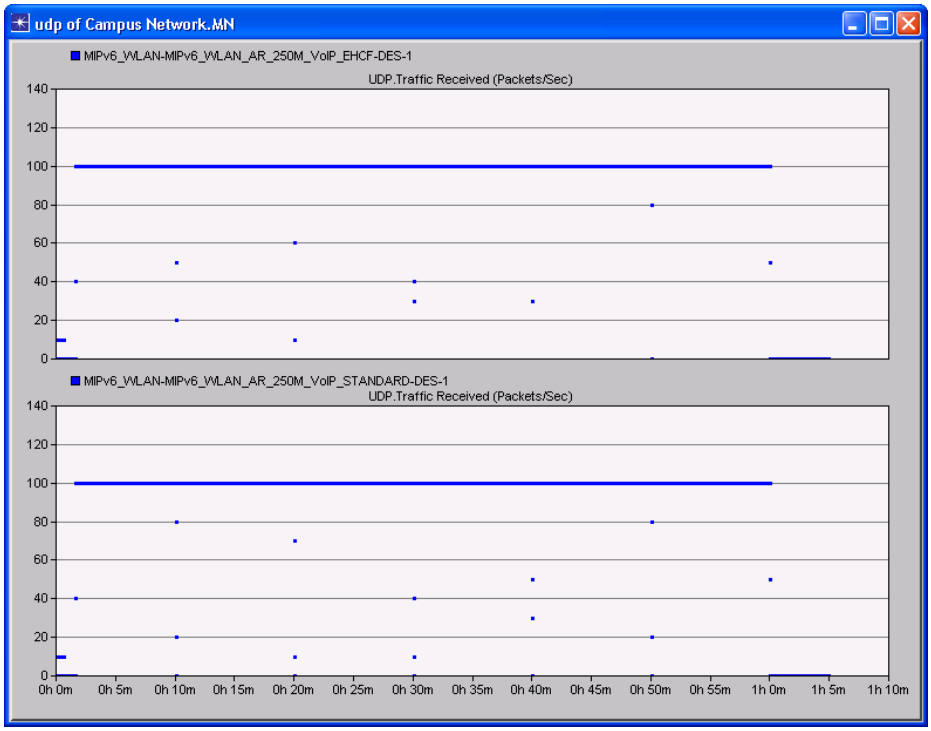


Figure 37: Comparaison entre la méthode Standard et E-HCF pour la réception des paquets UDP (nombre de paquets reçu par seconde) au MN durant la simulation

Pour une analyse plus fine, la figure 38 présente une comparaison entre la méthode Standard et la méthode E-HCF pour les paquets reçus par le MN entre 600 et 610 secondes. La procédure du handover s'est produite à 605,8 secondes. Nous pouvons constater dans cette figure une coupure de la réception du flux de données dans la méthode Standard et une chute du débit reçu par le MN dans la méthode E-HCF. En fait, il existe aussi une coupure de la réception du flux de données très courte dans la méthode E-HCF, mais nous ne percevons pas dans cette figure. En effet, l'application VoIP envoie 10 paquets pendant 100 ms, OPNET mesure pendant une période de 100 ms et génère une valeur de statistique pendant la simulation. Comme la durée des procédures du handover gérées par la méthode E-HCF n'est que de 140 ms environ, c'est-à-dire que le handover se commence et se termine souvent au milieu d'un période de mesure, par conséquent, nous pouvons constater une chute du débit reçu, mais nous ne constatons pas une coupure de la réception du flux de données dans la méthode E-HCF.

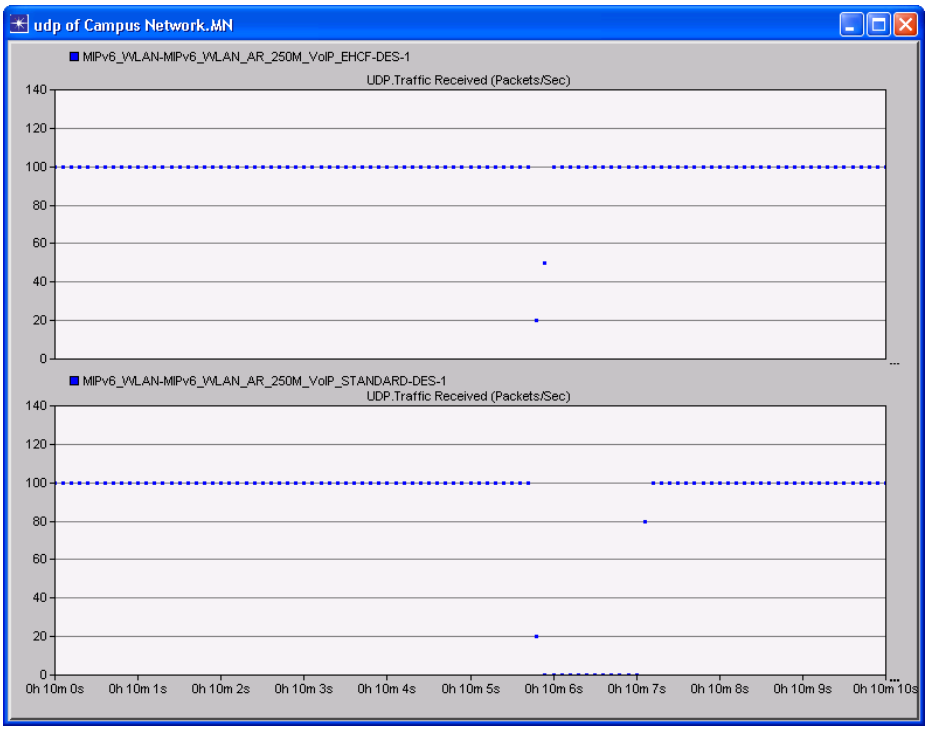


Figure 38 : Comparaison entre la méthode Standard et E-HCF pour la réception des paquets UDP (nombre de paquets reçu par seconde) au MN entre 600 et 610 secondes

Ici, nous donnons une comparaison entre le taux de perte de paquets due au handover géré par la méthode Standard et celui due au handover géré par la méthode E-HCF.

Pour simplifier, nous supposons qu'il y a un handover qui s'est produit pendant une minute d'application VoIP. Nous calculons le taux de perte de paquets sur une minute d'application VoIP. Nous considérons nous pouvons recevoir 100 paquets UDP/s en moyenne en hors de la période des procédures du handover. Nous avons effectuons cinq simulations, et nous rapportons ici le nombre de paquets perdus en moyenne dû au handover est de 13,4 paquets pour la méthode E-HCF et de 131,8 paquets pour la méthode Standard (le nombre de paquets perdus en moyenne sont calculés selon les valeurs de statistique collectées par OPNET).

Donc, le taux de la perte de paquets pour la méthode Standard :

$$P = \frac{131{,}8}{100 \times 60} \% = 2{,}197\ \%$$

Et le taux de la perte de paquets pour la méthode E-HCF :

$$P = \frac{13{,}4}{100 \times 60} \% = 0{,}223\ \%$$

Lorsque le protocole IPv6 Mobile est utilisé, l'en-tête d'extension de mobilité est ajouté dans chaque paquet IP, la taille de chaque paquet est ainsi augmentée. Comme tous les

paquets sont ensuite encapsulés dans les trames MAC et envoyés à la destination, nous pouvons constater une augmentation du débit du flux à la couche MAC dans la figure 40.

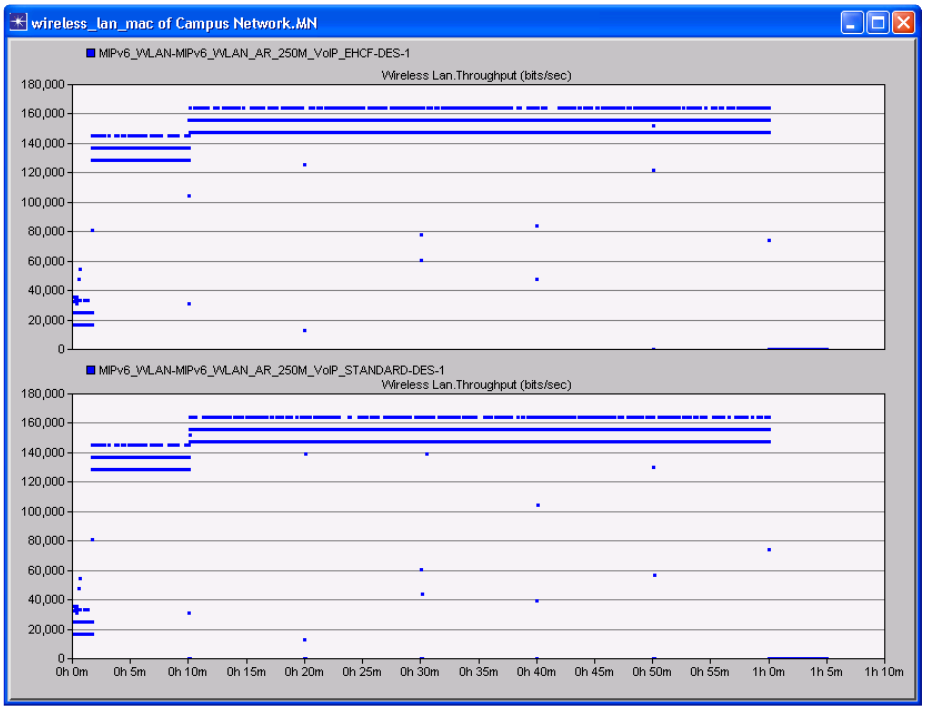


Figure 39: Comparaison entre la méthode Standard et E-HCF pour la réception du flux à la couche MAC du MN

Vidéo conférence

Nous avons choisi la vidéo basse résolution pour notre simulation. Nous avons un flux constant de 173 Koctets/s à la couche transport sous le format du paquet UDP avec une fréquence de 30 paquets UDP/s et un flux d'un débit constant de 1,45Mbits/s en moyenne à la couche MAC au MN.

La figure 41 présente la comparaison entre la méthode Standard et la méthode E-HCF pour la réception des paquets UDP au MN durant une durée de simulation de 3900 secondes. Il y a 5 handovers qui se sont produits pendant cette simulation. Nous collectons une valeur de statistique (paquets UDP/s) tous les 100 ms. Nous pouvons constater la chute du débit reçu par le MN pendant cinq handovers durant la simulation. L'application Vidéo conférence est similaire à l'application VoIP dans le sens où les deux applications tout utilisent le protocole UDP pour transporter leurs paquets. Leurs différences consistent au débit du flux et à la fréquence d'envoie de paquets.

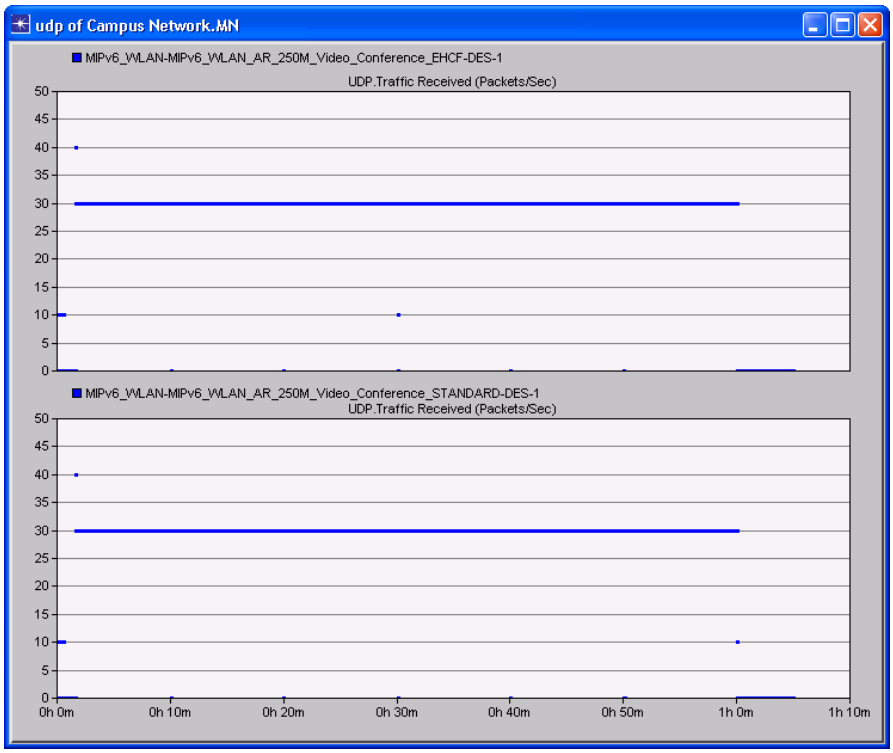


Figure 40 : Comparaison entre la méthode Standard et E-HCF pour la réception des paquets UDP (nombre de paquets reçu par seconde) au MN durant la simulation

Pour une analyse plus fine, la figure 41 présente une comparaison entre la méthode Standard et la méthode E-HCF pour les paquets reçus par le MN entre 600 et 610 secondes. La procédure du handover s'est produite à 605,8 secondes. Nous pouvons constater dans cette figure une coupure de la réception du flux de données dans la méthode Standard et aussi dans la méthode E-HCF. En fait, l'application Vidéo conférence envoie 1 image au début de tous les 100 ms, le data est ensuite fragmenté sous forme de segments pour les transférer, OPNET mesure pendant une période de 100 ms et génère une valeur de statistique pendant la simulation, la durée des procédures du handover gérées par la méthode E-HCF est de 140 ms environ, même que le handover se commence et se termine au milieu d'un période de mesure, nous pouvons constater une coupure de la réception du flux de données dans la méthode E-HCF.

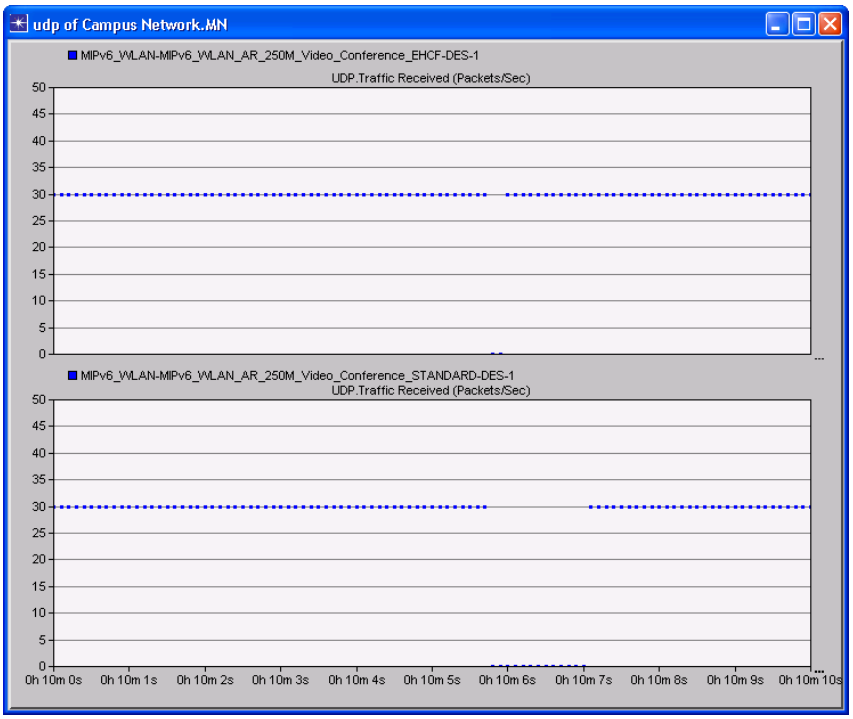


Figure 41 : Comparaison de la réception des paquets UDP (nombre de paquets reçu par seconde) au MN entre 600 et 610 secondes

Ici, nous donnons une comparaison entre le taux de perte de paquets due au handover géré par la méthode Standard et celui due au handover géré par la méthode E-HCF.

Pour simplifier, nous supposons qu'il y a un handover qui s'est produit pendant une minute d'application Vidéo conférence. Nous calculons le taux de perte de paquets sur une minute d'application Vidéo conférence. Nous considérons nous pouvons recevoir 30 paquets UDP/s en moyenne en hors de la période des procédures du handover. Nous avons effectuons cinq simulations, et nous rapportons ici le nombre de paquets perdus en moyenne dû au handover est de 5,2 paquets pour la méthode E-HCF et de 40,8 paquets pour la méthode Standard (le nombre de paquets perdus en moyenne sont calculés selon les valeurs de statistique collectées par OPNET).

Donc, le taux de la perte de paquets pour la méthode Standard :

$$P = \frac{40,8}{30 \times 60} \% = 2,267 \%$$

Et le taux de la perte de paquets pour la méthode E-HCF :

$$P = \frac{5,2}{30 \times 60} \% = 0,289 \%$$

4.3.2 Résultats et Analyse des Simulations pour les applications utilisant le protocole TCP

Le protocole TCP géré un flux par le principe "fenêtre de glissant". Ainsi, après l'envoie de paquet, un MN attend un accuse de réception du CN avant d'envoyer les paquets suivants. Cette gestion de flux amène le nombre de paquets reçus variable par rapport aux applications UDP.

Nous présentons les résultats des simulations pour l'application FTP dans les figures 41. Nous collectons 10 000 fois des statistiques pendant une simulation. Nous pouvons donc obtenir une statistique tous les 400 ms environ. Mais le nombre des paquets par seconde qui est reçu à la couche TCP par le MN varie entre 6,5 et 8,2. Mais il est de 8 paquets/s en moyenne si nous réduisons le nombre de fois des statistiques collecté pendant la simulation (Voir la figure 31 ci–dessus). Cela s'explique par les caractéristiques du protocole TCP. En effet, le CN (serveur FTP) envoie un fichier de 5 000 octets chaque seconde au MN (client). Ensuite, il attend l'accuse de réception du MN pour le prochain envoie des paquets. Par conséquent, si nous collectons une statistique tous les 400 ms pour le MN, il y a un moment où il ne reçoit pas les paquets. C'est le moment où le CN arrêt d'envoyer la transmission des paquets et attend d'accuse de réception du MN. Si nous collectons les statistiques tous les 4 secondes, nous ne pouvons pas obtenir un résultat assez précis et satisfaisant.

La figure 42 présente la comparaison de la réception des paquets TCP au MN.

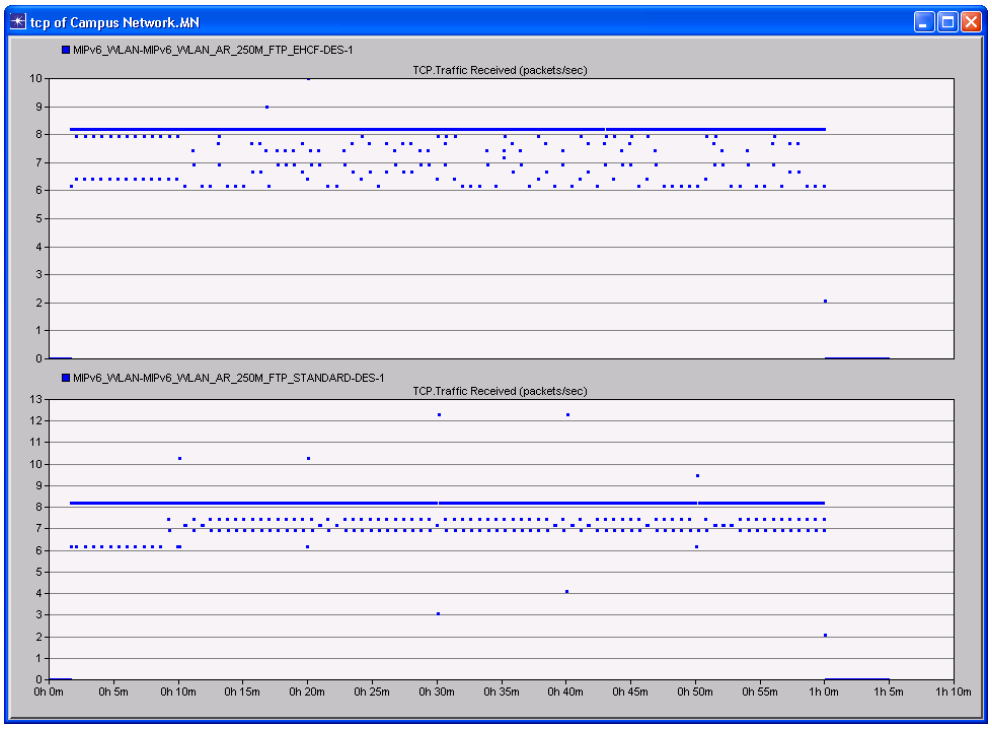


Figure 42: Comparaison entre la méthode Standard et E-HCF pour la réception des paquets TCP (nombre de paquets reçu par seconde) au MN durant la simulation

La figure43 présente le résultat de la simulation pour le flux reçus à la couche MAC.

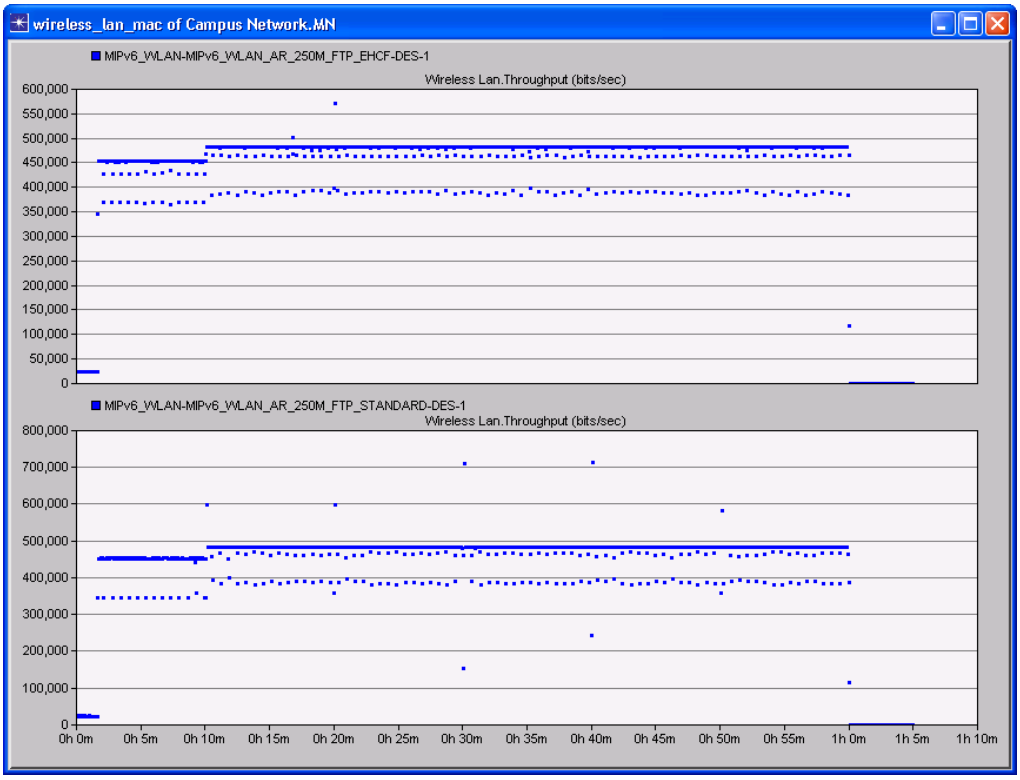


Figure 43: Comparaison entre la méthode Standard et E-HCF pour la réception du flux à la couche MAC du MN

4.4 Conclusion

Nous constatons que l'interruption de la réception du flux est bien plus réduite dans la méthode E-HCF que dans la méthode Standard. Nous obtenons un résultat visible pour les applications qui utilisent le protocole UDP. Mais nous avons aussi constaté que le débit du flux est augmenté à cause d'utilisation du protocole IPv6 Mobile. Pour l'application VoIP, cette augmentation a un effet très négatif, en effet, elle représente 15 % du débit du flux. Pour réduire son effet, il faut utiliser la méthode de compression des en-têtes de paquets IP.

Par contre, ici, nous utilisons un scénario où tous les APs n'ont pas de charge. Ils ne servent donc qu'au MN. Ce n'est pas le cas dans la réalité. Si l'AP auquel le MN va attacher est chargé, l'AP ne peut pas offrir le service que le MN demande. Nous introduisons la qualité de service dans le handover dans les réseaux Wi-Fi pour garantir la performance du handover du MN.

Nous faisons les simulations qui utilisent différents méthodes de la qualité de service dans la procédure du handover dans le chapitre 5. Partant des résultats des simulations, nous donnons des conclusions pour le handover avec la qualité de service supporté dans les réseaux Wi-Fi.

5 Qualité de service appliquée dans le handover

Quand un utilisateur se déplace loin de son AP dans les réseaux Wi-Fi, la puissance de signal reçu se dégrade et que son AP ne peut plus répondre à sa demande en termes du débit supporté et du taux de la perte de paquet. Il doit passer de son AP courant à un nouveau AP, avec lequel il a une meilleure réception du signal. Cependant, même si cet utilisateur a choisi de se connecter à un nouveau AP, le nouveau AP ne peut pas répondre de façon certaine à sa demande s'il y a déjà des charges importantes sur cet AP. Ces charges de l'AP sont constituées par les différents types d'applications des différents utilisateurs. Les différents utilisateurs n'ont pas le même niveau de priorité de service dans les réseaux, de même, les différentes types d'applications n'ont pas la même demande qualitative. Chaque application a une demande qualitative particulière, par exemple, l'application VoIP n'a besoin qu'une bande passante faible, tolère un certain niveau de perte de paquet, mais elle a les contraintes très fortes sur le délai et. L'application FTP demande plus de bande passante, mais il tolère un certain niveau du délai. Par conséquent, la Qualité de service (en anglais Quality of Service – QoS) doit être appliquée dans les réseaux pour mieux servir aux utilisateurs selon leurs priorités, leurs demandes qualitatives et équilibrer les différentes besoins des utilisateurs. La QoS est définie comme l'effet général de la performance du service qui détermine le degré de satisfaction d'un utilisateur du système par l'Union Internationale des Télécommunications [ITU94].

Dans ce chapitre, nous décrivons d'abord le terme de QoS et les différents mécanismes de la gestion de QoS dans les réseaux. Ensuite, nous appliquons les différents mécanismes de QoS dans les réseaux Wi-Fi et analysons les résultats des simulations obtenus.

5.1 Qualité de Service

Le développement d'Internet a suscité un engouement croissant à la fois pour de nouveaux modes de communication, tel que l'e-mail, le messagerie instantanée, et pour de nouvelles applications multimédias, telles que la diffusion vidéo ou audio sur Internet, la VoIP, la Vidéo conférence, les jeux interactives. La nature de ces nouvelles applications impose des exigences qualitatives spécifiques, par exemple, le faible délai, la large bande de passante et la fiabilité. Or, actuellement, Internet se base sur le modèle "Meilleur effort" (*en anglais Best Effort*). Le modèle "Meilleur effort" maximise l'utilisation de ressources de réseaux tout en simplifiant l'opération des équipements intermédiaires de réseaux. Avec ce modèle, tous les paquets sont traité indépendamment les uns des autres et sont servis identique avec la gestion dite "Premier entre premier servi" (*en anglais First In, First Out – FIFO*) dans les équipements intermédiaires de réseaux. Cette politique de gestion est simple à mettre en œuvre, mais lorsque la file d'attente est pleine, il conduit à la perte de tous les nouveaux

paquets entrants, donc il pénalise toutes les sources indifféremment de leur responsabilité dans la congestion. De plus, la régulation du trafic n'intervient que sur débordement, non seulement il n'y a pas anticipation, mais la file d'attente étant pleine, le délai moyen de traitement peut être important [SERVIN].

Pour répondre aux différentes demandes qualitatives des utilisateurs, la réalisation de QoS devient primordiale. Le terme QoS se réfère aux moyennes de régulariser instantanément les acheminements de paquets dans les réseaux. Selon les besoins des utilisateurs, les paquets peuvent transiter plus ou moins vite dans chaque section de réseau en fonction de la charge des liaisons ou des équipements de réseaux. En cas de saturation, certains paquets peuvent être perdus. Par conséquent, le concept de QoS consiste en comment gérer au mieux les paquets et par quel moyen.

Deux mécanismes aux finalités différentes sont mis en œuvre dans les équipements de réseaux pour gérer les paquets qui sont en attente de traitement: le mécanisme de gestion de file d'attente et le mécanisme d'ordonnancement. Le premier détermine comment éliminer certains paquets, en cas de congestion, au sein d'une même file d'attente d'un équipement de réseaux. Le deuxième a pour objectif de distribuer la ressource entre différentes files d'attente correspondant chacune à une classe de service différente. L'IETF a proposé ainsi deux modèles pour identifier les différents flux dans les réseaux: le modèle Intégration de services (*en anglais Integrated Service - IntServ*) [RFC 1633] et le modèle Différentiation de services (*en anglais Differentiated Service - DiffServ*) [RFC 2475].

Nous décrions d'abord les paramètres de QoS qui caractérisent les demandes qualitatives des applications. Ensuite, nous présentons les mécanismes de gestion de paquets, les modèles – IntServ et DiffServ, ainsi la norme IEEE 802.11e fonctionne avec le modèle DiffServ.

5.1.1 Paramètres de QoS

Une séquence de paquets envoyés d'une source vers une destination est appelée un flux. Les besoins qualitatives d'un flux peuvent être caractérisés par quatre paramètres : la bande passante/débits (*en anglais Bandwidth*), le délai d'acheminement (*en anglais Delay*), la variation du délai/Gigue (*en anglais Jitter*) et la perte de paquet (*en anglais Packet loss*).

Bande passante/Débits

Il défini le volume maximal d'information (bits) que le réseau est capable d'accepter ou de délivrer par unité de temps. Le débit maximum dépend de la couche qu'on parle. Par exemple, le débit de la couche liaison de donnés représente la capacité de transport, mesurée en bits/s, dans laquelle les données n'incluent pas les bits nécessaires pour les en-têtes des trames. Lorsqu'on se place à une couche supérieure à la couche réseau, on considère que la capacité du lien (*en anglais throughput*) correspond au volume effectif de données des applications transmis. La capacité utile du lien (*en anglais good put*) est égale au nombre total de bits issus de l'application et correctement transmis par unité de temps. Par exemple, pour un flux TCP, on ne comptabilise que les paquets reçus et on retire des paquets retransmis. C'est ce débit maximum qui est pertinent pour évaluer la capacité de réseau.

Délai d'acheminement

Il caractérise l'intervalle du temps entre l'émission et la réception d'un paquet. Le délai comporte du délai de propagation, du délai de transmission, du délai d'attente dans la file d'attente, et du délai de traitement dans les équipements intermédiaires de réseaux. La contrainte de délai en termes de QoS est variable selon les applications de l'Internet.

Par exemple, l'ITU (International Telecommunication Union) précise les classes de QoS dans G.114 pour la transmission téléphoniques au niveau du délai est montrées dans le tableau 17 [ITU96] :

Tableau 17 : Classement de QoS au niveau de délai d'acheminement

Classe	Délai d'acheminement	Commentaire
1	0 à 150ms	Satisfaisante
2	150 à 300 ms	Faible interactivité
3	300 à 700 ms	Devient half–duplex
4	Au delà de 700 ms	Inutilisable sans half–duplex

Variation du délai/Gigue

Il correspond à une variation du délai d'acheminement. Elle est due au fait que les paquets sont en effet susceptibles de traverser les différents chemins et les différents des équipements intermédiaires de réseaux entre une source et une destination. Par conséquent, le délai d'acheminement pour les paquets n'est surement pas le même. Ce phénomène mené au problème de synchronisation, tel que les paquets de la voix ou la vidéo doivent être arrivé dans son ordre. Pour compenser la variation du délai, le récepteur utilise souvent des mémoires tampons (*en anglais buffers*) pour synchroniser les paquets arrivés. Cependant, ce mécanisme de synchronisation rallonge le délai d'acheminement.

Perte de paquet

Elle correspond soit à la non-réception d'un paquet, soit à la réception d'un paquet erroné pour la destination.

La non-réception d'un paquet est causée par la congestion de réseaux, l'instabilité du routage ou les défaillances de liens [Collet98]. Parmi ces trois arguments, la perte due à la congestion de réseau représente la plupart de cas. Quand la file d'attente d'équipements est plein, les nouveaux paquets sont jetés et ils ne peuvent pas arriver à la destination.

Un paquet erroné est produit plutôt pendant sa transmission sur un lien. Un lien réseau existe un taux d'erreur pour la transmission des bits. Actuellement, dans les liaisons filaires, le taux d'erreur est très faible, par exemple, 10^{-7} pour xDSL sur la paire cuivrée et inferieure à 10^{-9} pour les fibres optiques. Cependant, dans les réseaux sans fil, le taux d'erreur n'est pas négligeable.
En conclusion, les applications ont des exigences diverses en matière de ces quatre paramètres. Le tableau 18 synthétise les demandes de QoS pour les différents types des applications multimédias [Tanenbaum].

Tableau 18 : Applications Multimédias et paramètres de QoS correspondants

Type d'application	Détails	Qualité de service requise
Diffusion vidéo (Télévision Internet, Vidéo à la demande)	MPEG2, MPEG4	Débits : 64 Kbits/s à 2 Mbits/s Délai : 250 ms Gigue : compensables par la mémoire tampon
Diffusion audio (Radio Internet)	MP3, AAC, OggVorbis	Débits : de 32 Kbits/s à 256 Kbits/s Délai : 100 –150 ms Gigue : compensables par la mémoire tampon
VolP	PCM-MIC, G.711	Débit : 6,4 Kbits/s à 64 Kbits/s Délai : 150 ms à 300 ms Gigue : 0 à 50 ms Pertes : < 0,1 %
Vidéo conférence	Architecture : H.323 Résolution vidéo (H.263) : de SUB-QCIF (128 × 96) à 16CIF (1 408 × 1 152)	Débit : 64 Kbits/s à 1 920 Kbits/s Délai : de l'ordre de 150 ms à 300 ms Gigue : 0 ms à 50 ms Pertes : < 0,1 %
Session Interactive	SSH, Telnet, VNC, T120	Débits variables Délai de l'ordre de 600 ms Pertes nulles

5.1.2 Mécanismes de gestion des paquets

Les mécanismes de gestion des paquets consistent à définir le moyenne de gérer les paquets qui sont dans la file d'attente d'un équipement des réseaux. Les mécanismes de gestion des files d'attente détermine comment éliminer certains paquets, en cas de congestion, au sein d'une même file d'attente d'un équipement de réseaux. Les mécanismes d'ordonnancement ont pour objectif de distribuer la ressource entre différentes files d'attente correspondant chacune à une classe de service différente.

Mécanismes de gestion de files d'attente

Le mécanisme de gestion de file d'attente traditionnelle – FIFO jette tous les nouveaux paquets entrants dans la file d'attente lorsque cette file d'attente est pleine. C'est un mécanisme simple à mettre en œuvre, mais il pénalise toutes les sources indifféremment de leur responsabilité dans la congestion. De plus, la régulation du trafic n'intervient que sur débordement, il n'y a pas anticipation. En outre, lorsque la file d'attente étant pleine, le délai moyen de traitement des paquets peut etre important.

En mesurant la taille moyenne de la file d'attente et des qu'un certain seuil est atteint, en éliminant de manière aléatoire les paquets, le RED (*Random Early Discard*) pénalise d'autant plus un flux que la probabilité qu'un paquet appartenant à ce flux soit présent dans la file est importante. Le RED tente ainsi de réguler le trafic en écartant les paquets des flux les plus responsables d'un état naissant de congestion. Cependant, le RED n'agit que sur des paramètres de volumétrie, il ne prend pas en compte la priorité des différents flux. A l'instar du RED dont il dérive, le WRED (*Weighted RED*), intervient à partir d'un certain

seuil de remplissage des files, mais chaque type de flux se voit, en fonction de son niveau de priorité, attribuer un seuil différent.

Mécanismes d'ordonnancement

Les mécanismes d'ordonnancement visent à garantir un partage équitable de la bande passante. Le mécanisme le plus simple est le WFQ (*Weighted Fair Queuing*) qui réalise une insertion ordonnée en fonction d'un niveau de priorité dans la file d'attente (système à file d'attente unique), celle-ci étant ensuite traitée en mode FIFO.

Les autres méthodes s'appliquent aux systèmes à files multiples, dont le principe de base consiste à lire séquentiellement les différentes files, d'y prélever un paquet et, si une file est vide, de passer à la suivante.

Ce mécanisme est inéquitable, il accorde d'autant plus de bande passante à une file que les paquets qui y séjournent sont de taille importante. Notamment ce principe est incompatible avec les flux isochrones qui se caractérisent généralement par de petits paquets et une priorité importante. Le WRR (*Weighted Round Robin*) introduite la notion de priorité et peut offrir en fonction de celle-ci une bande passante différenciée (volume ou temps de lecture d'une file d'attente).

5.1.3 IntServ et DiffServ

5.1.3.1 IntServ

Le modèle IntServ, qui tend au respect de l'intégrité du flux, a pour objectif de garantir la QoS à l'intégrité du flux dans les réseaux. Il simule la commutation de circuits. Tous les paquets d'un même flux suivent un même chemin et bénéficient la même priorité.

Le modèle IntServ utilise le protocole RSVP (*en anglais Resource reServation Protcocol – RSVP*) [RFC 2210] pour réserver la ressource nécessaire, telle que la bande passante et mémoire tampon, avant d'expédier le flux à travers le réseau. En fait, Chaque application formule d'abord une demande de réservation de ressource de bout en bout en utilisant le protocole RSVP au début d'une session de communication. Cette session est identifiée par l'adresse IP de destination, le type de protocole de la couche transport et le numéro de port de destination. Pour réserver la ressource, la source doit émettre vers la destination un message PATH qui contient les caractéristiques du flux qu'il va émettre. Tandis que le message PATH se propage, chaque routeur emprunté enregistre alors dans le message PATH les caractéristiques du routeur, tels que la bande passante disponible, etc. Lorsque la destination reçoit le message PATH, elle émet en retour un message RESV qui emprunte le chemin inverse et qui demande alors les ressources nécessaires. Chaque routeur peut alors accepter ou rejeter cette demande. Si elle est acceptée, la bande passante et la mémoire tampon sont allouées au flux. Les routeurs doivent conserver les ressources allouées de chaque flux qui les traverse. Par ailleurs, cette réservation de ressource n'est pas définitive,

elle doit être régulièrement rafraichie par l'utilisateur. Dans le cas contraire, celle-ci est supprimée des routeurs au bout d'un certain temps.

En conclure, le modèle IntServ permet de faire une réservation de ressources pour chaque flux circulant sur les réseaux en utilisant le protocole RSVP. Pourtant, il est difficile d'implanter ce modèle dans un réseau de grande échelle. Non seulement que le protocole RSVP génère un trafic important dans le réseau, du fait que chaque session devait effectuer ses réservations de ressources et rafraîchir régulièrement son chemin de communication sur chaque routeur, mais aussi le protocole RSVP entraîne une réduction considérable de performance pour chaque routeur, du fait que chaque routeur doit analyser tous les flux séparément et attribuer les ressources à chaque flux [Yang03]. Compte tenu de sa complexité, le modèle IntServ n'est pas adapté aux grands réseaux des operateurs, il n'as connu qu'un développement limité dans les réseaux privés.

Une variation du modèle IntServ est utilisée dans le réseau ATM (*en anglais Asynchronous Transfert Mode – ATM*) [Awa96] ou MPLS (*en anglais Multiprotocol Label Switching – MPLS*) [Réseaux05]. Le réseau ATM ou MPLS utilise les signalisions pour établir des Circuits virtuels (en anglais Virtual Circuits - VCs) et réserver la bande passante, au lieu d'utiliser le protocole RSVP. ATM ou MPLS peuvent allouer les ressources nécessaires pour garantir le débit demandé par les applications avant de transférer les flux.

5.1.3.2 DiffServ

Le modèle DiffServ propose de procéder à chaque paquet d'un flux de façon indépendante, contrairement à IntServ qui procédait à une séparation par flux. La conséquence directe est que les routeurs qui supporte le modèle DiffServ traitent tous les paquets d'une classe donnée de la même manière, sans distinction d'émetteur ni de récepteur. DiffServ implémente un mécanisme de partage de bande passante en introduisant la notion de politique d'acheminement en fonction d'une classe de service. Les flux ne sont plus traités individuellement comme dans IntServ, mais sont affectés à une classe de service identifiée par un champ spécifique Differentiated Service (DS) dans le datagramme IP. Tous les flux d'une même classe sont traités de la même manière dans le réseau dit traitement par saut (*en anglais Per Hip forwarding Behaviour – PHB*). Le champ DiffServ remplace le champ TOS d'IPv4 et le champ Classe de Service d'IPv6.

La classification des flux est réalisée à la périphérie du réseau (classifier). Les propriétés du flux sont ensuite analysées (metering ou dimensionnement) en fonction d'un contrat de service préétabli (*en anglais Service Level Agreement – SLA*). Les datagrammes sont alors marqués par positionnement du champ DS. Le trafic différencié est analysé, certains paquets peuvent etre retardés, voire éliminés pour prévenir un éventuel état de congestion. Les paquets sont ensuite affectés à une file d'attente spécifique avant d'etre transmis dans le réseau (Forwarding).

L'architecture DiffServ est bien adaptée aux grands réseaux. En effet, les classes de services étant attribuées en périphérie du réseau DiffServ, elles ne génèrent ni trafic de gestion, ni surcharge CPU. Cependant, Si DiffServ permet de hiérarchiser les flux, il ne dispose pas de mécanisme d'information d'état du réseau. De ce fait, les routeurs de

bordure ne sont pas en mesure d'anticiper ni de réagir à un état de pré-congestion ou de congestion.

5.1.4 Norme IEEE 802.11e

La norme IEEE 802.11e [IEEE 802.11e] a pour objectif d'améliorer la couche MAC 802.11 pour inclure la QoS dans 802.11 afin d'offrir un support aux applications sensibles au phénomène de latence, telles que les applications voix ou vidéo. Pour offrir la QoS dans les réseaux Wi-Fi, la norme IEEE 802.11e prévoit la définition de huit classes de trafic (*en anglais Trafic Classe – TC*) distinctes et associe chaque paquet à une classe de trafic. De plus, chaque classe de trafic a une priorité particulière pour accéder au medium (*Access Priority – AC*). Le standard 802.11e propose jusqu'à huit niveaux de TC et un AP doit en mettre en œuvre au minimum quatre. Deux nouveaux mécanismes de contrôle d'accès sont définis: le HCCA (*HCF Controlled Channel Access*) et l'EDCA (*Enhanced Distributed Channel Access*). Ainsi, le mode DCF est remplacé par le mode Fonction de Coordination Hybride (*en anglais Hybrid Coordination Function – HCF*) avec accès à compétition qui est plus connue sous la désignation EDCF (*Enhanced DCF*). Le mode PCF est remplacé par le mode HCF avec accès contrôlé. Cependant, le mode EDCF n'utilise que l'EDCA alors que le mode HCF avec accès contrôlé utilise les deux mécanismes de contrôle d'accès.

Ici, nous présentons le mode EDCF, parce qu'il est plus utilisé dans les réseaux 802.11e et comme le mode DCF dans les réseaux 802.11. Les principes du mode EDCF pour supporter la QoS sont les suivants [Lin03]:

- Les délais d'attente pour envoyer les paquets sont différents selon la classes de trafic (TC) : Le mécanisme d'envoi de paquets est le même que DCF. Cependant les paquets à haute priorité ont plus de chances d'être émis rapidement que ceux à basse priorité. Pour cela, EDCF règle les délais AIFS (*Arbitration Inter Frame Space*) et CW selon les classes : plus la classe est prioritaire, plus les délais d'attente sont courts.

- Chaque station gère des files d'attente par la classe de trafic et applique des règles probabilistes pour déterminer de quelle file d'attente le prochain paquet à émettre fera partie. Un paquet à transmettre entre donc dans la file d'attente selon sa classe de trafic, puis lorsque son tour arrive, il doit remplir deux conditions avant d'être transmis :
  1. contre les paquets des autres files d'attente du même adaptateur (condition interne) ;
  2. contre les paquets des autres stations (condition externe).

- Une station peut envoyer plusieurs paquets successifs. La station profite d'une "opportunité de transmission" (TXOP). La durée maximale d'une TXOP peut être précisée dans les trames balises de l'AP. Pendant une TXOP, la station envoie autant de paquets qu'elle le souhaite les uns après les autres en ne les espaçant que de SIFS. Puisque SIFS est le délai le plus court, personne ne peut l'interrompre. Pendant la TXOP, les paquets n'ont que la condition interne à gagner.

En conclusion, l'EDCF est simple à mettre en œuvre, il permet de régler les flux en fonction des classes de trafic. Cependant, il peut arriver que certains paquets prioritaires soient retardés un peu trop longtemps et les paquets peu prioritaire peut être émis avec beaucoup de retard s'il y a un trafic régulier et plus prioritaire sur le réseau, cela peut faire perdre de l'efficacité au réseau.

5.2 Résultats obtenues par simulations

Nous avons présenté différents mécanismes de QoS dans les paragraphes précédents. Ici, nous les utilisons avec différents types d'applications pour simuler leurs impacts sur les procédures du handover dans un réseau Wi-Fi gérées par la méthode E-HCF.

L'architecture de réseaux pour notre simulation est présentée dan la figure 44. Nous ajoutons deux nœuds fixes – MN2 et MN3 qui communiquent avec les CNs – CN2 et CN3 respectivement via l'AR 3 en radio. Le MN – MN1 se déplace de la même façon que celle du scenario utilisé dans le chapitre 4. Tous les trois nœuds utilisent la même application – Vidéo conférence. Les applications envoient la même taille de trame avec un même intervalle des trames. Donc, leurs applications ont le même débit, mais ils n'ont pas les mêmes priorités. L'application du MN 1 a une priorité le plus haute, celle du MN2 a une priorité le plus basse.

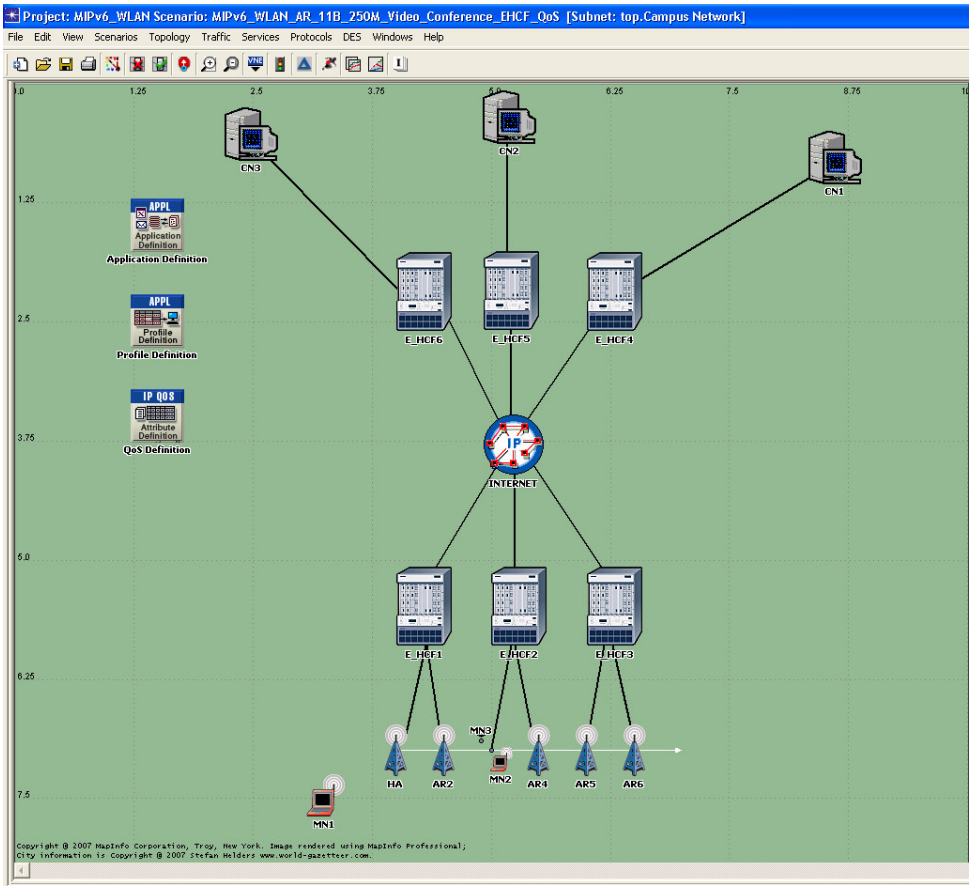


Figure 44 : Architecture de réseaux avec E-HCF Implémenté et QoS supportée

Nous présentons d'abord les résultats des simulations sans le mécanisme de QoS implémenté dans le réseau, ensuite les résultats des simulations en utilisant le mécanisme EDCA, Priorité Queuing et la WFQ.

5.2.1 Les simulations sans les mécanismes de QoS implémentés

La figure 45 présente les paquets reçus par les trois nœuds – MN1, MN2 et MN3 sans les mécanismes de QoS implémentés dans le réseau Wi-Fi. Quand le MN1 n'est pas connecté avec l'AR 3, les nœuds fixes MN2 et MN3 peuvent communiquer avec leurs correspondants, il y a une petite perte de paquets qui s'est produit. Une fois le MN1 attache avec cet AR, tous les trois nœuds ne peuvent plus garantir leurs communications, la perte de paquets est importante pour tous ces trois nœuds. Quand le MN1 se déconnecte avec cet AR, les deux nœuds fixes peuvent maintenir à nouveau leurs communications.

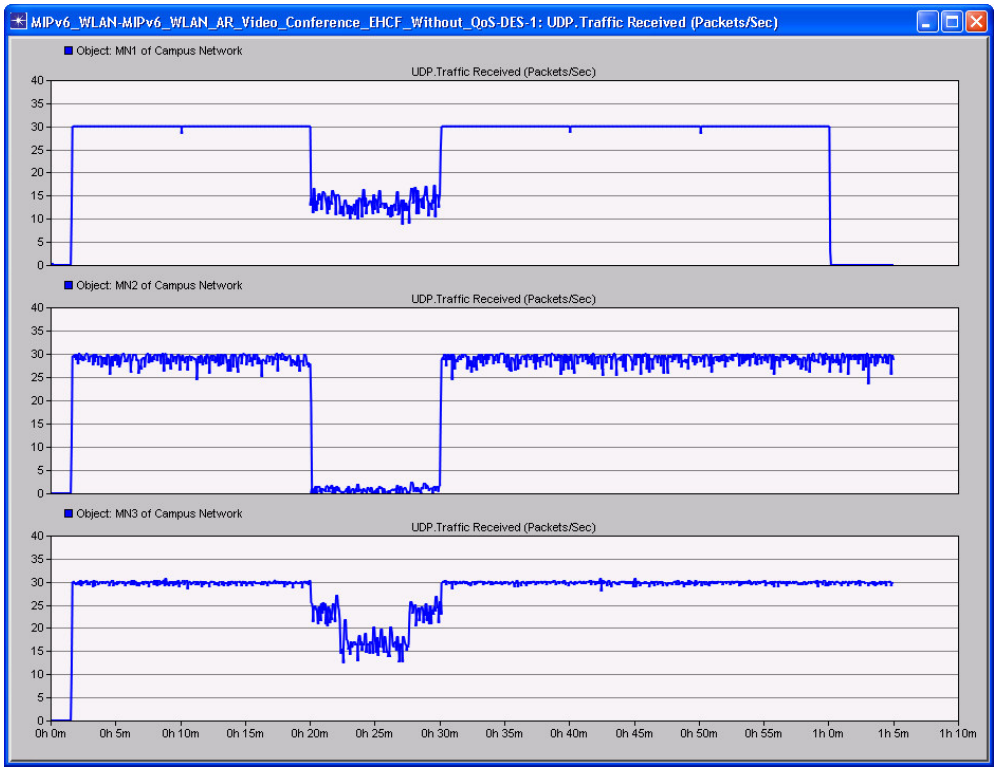


Figure 45 : Réceptions des paquets UDP aux nœuds sans les mécanismes de QoS implémentés

5.2.2 Les simulations avec les mécanismes de QoS implémentés

5.2.2.1 EDCA

Comme nous avons présenté, le mécanisme EDCA utilise le concept de DiffServ pour assurer la QoS à la couche MAC.

La figure 46 présente les paquets reçus par les trois nœuds – MN1, MN2 et MN3 avec le mécanisme EDCA implémenté dans le réseau Wi-Fi. Quand le MN1 n'est pas connecté avec l'AR 3, les nœuds fixes MN2 et MN3 peuvent communiquer avec leurs correspondants, il n'y a pas de perte de paquets qui s'est produit. Cela s'explique par le fait que le mécanisme EDCA offert un contrôle d'accès à compétition avec une meilleur performance que celui de DCF. Avec le DCF, il y a une petite perte des paquets pour les deux nœuds fixes. Une fois le MN1 attache avec cet AR, il peut maintenir sa communication en cours, parce qu'il utilise une application avec une priorité le plus haute. Cependant, tous les trois nœuds ne peuvent plus garantir leurs communications, la perte de paquets est importante pour tous ces deux nœuds. Quand le MN1 se déconnecte avec cet AR, les deux nœuds fixes peuvent maintenir à nouveau leurs communications.

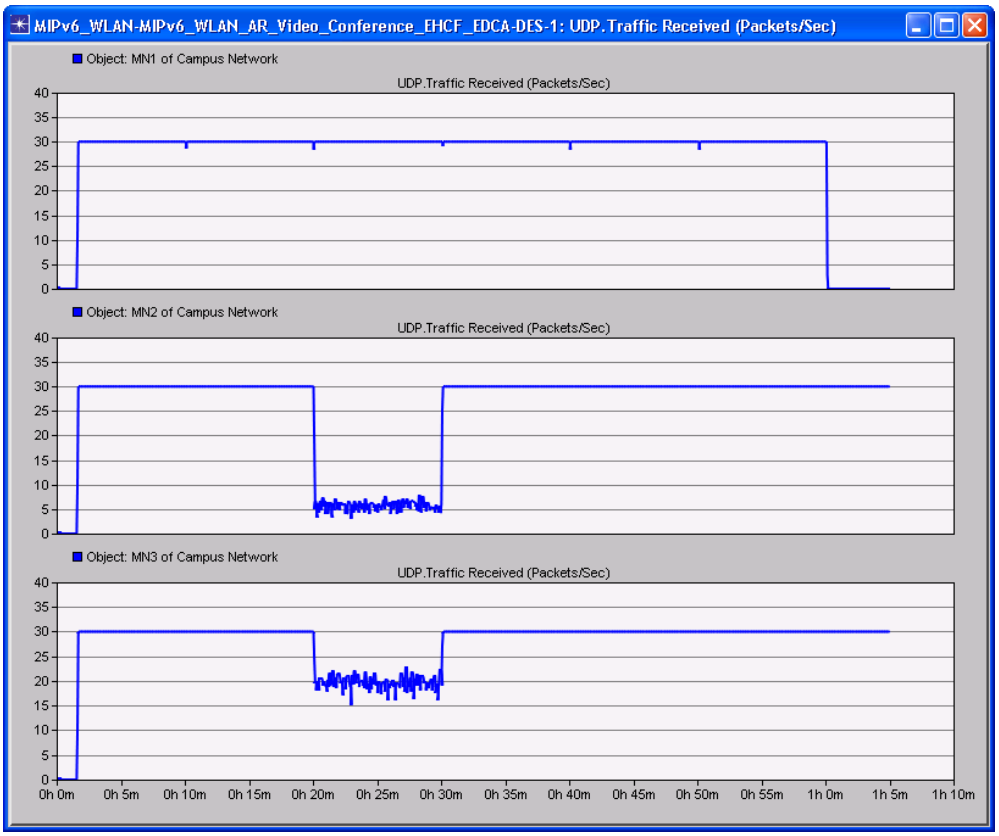


Figure 46 : Réceptions des paquets UDP aux nœuds avec EDCA implémenté

5.2.2.2 Priority Queuing

La figure 47 présente les paquets reçus par les trois nœuds – MN1, MN2 et MN3 avec le mécanisme Priority Queuing implémenté dans le réseau Wi-Fi. Quand le MN1 n'est pas connecté avec l'AR 3, les nœuds fixes MN2 et MN3 peuvent communiquer avec leurs correspondants, il y a de petite perte de paquets qui s'est produit. Cela s'explique par le fait que les deux nœuds fixes utilisent les priorités similaires – Standard et Excellent Effort.

L'AR n'a pas traité les deux flux de la façon différentielle. Une fois le MN1 attache avec cet AR, il ne peut pas maintenir sa communication en cours, même il utilise une application avec une priorité plus haute. Tous les trois nœuds ne peuvent plus garantir leurs communications, la perte de paquets est importante pour tous ces trois nœuds. Quand le MN1 se déconnecte avec cet AR, les deux nœuds fixes peuvent maintenir à nouveau leurs communications.

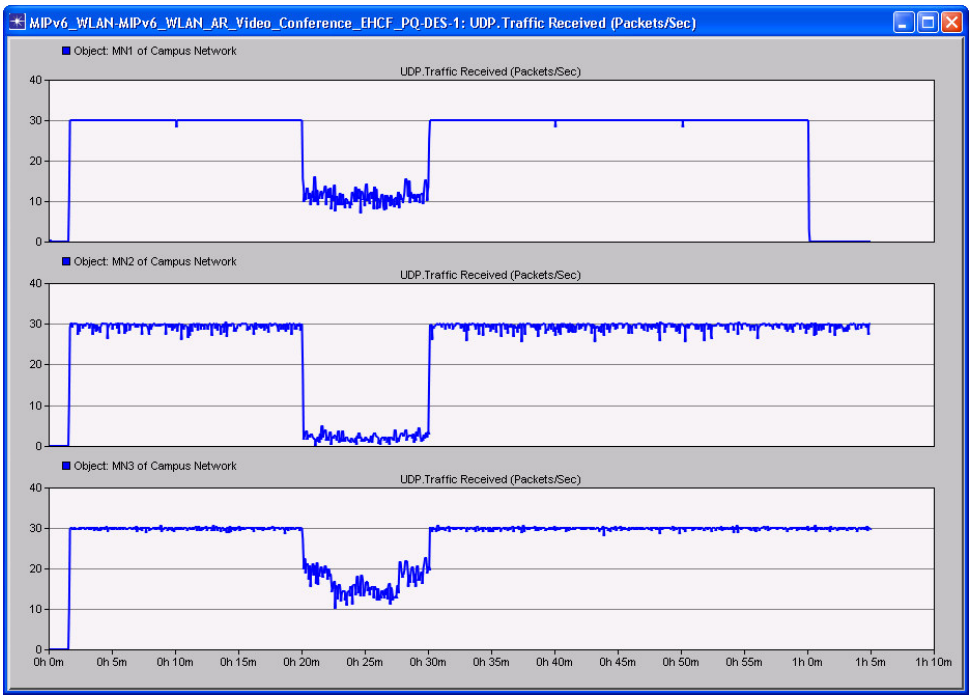


Figure 47: Réceptions des paquets UDP aux nœuds avec PQ implémenté

5.3 Conclusion

Dans ce chapitre, nous avons présenté les notions de QoS, les différentes caractéristiques de QoS, ainsi les différents mécanismes de gestion de paquets dans l'équipement de réseau. Nous décrions le modèle IntServ qui utilise le protocole de signalisation RSVP pour réserver la ressource et le modèle DiffServ. La norme 802.11e est aussi présentée dans ce chapitre pour monter la gestion de QoS à la couche MAC dans les réseaux Wi-Fi. Nous validons notre méthode E-HCF avec la supporte de norme IEEE 802.11e. Les résultats obtenus par simulation illustrent les améliorations des performances significatives lorsqu'une station mobile avec une haute priorité se connecte à un AP chargé.

Conclusions et perspectives

Le protocole IPv6 Mobile est standardisé par l'IETF en 2003 dans le but de masquer la mobilité d'un MN à ses CNs et d'offrir au MN la possibilité de maintenir une connexion au réseau tout en effectuant son déplacement. Le délai du handover est estimé de 1675 ms au 4675 ms par une estimation du standard IPv6 Mobile. Cette solution est satisfaite dans le cas du nomadisme, mais elle est insupportable pour les communications à qualité de service des réseaux sans fil.

Différentes approches ont été proposées consistant à améliorer les procédures du handover. En partant du principe que les réseaux Wi-Fi et les routeurs d'accès sont déjà massivement implantés dans le monde, nous proposons d'ajouter une nouvelle fonctionnalité, appelée E-HCF (Extended Handover Control Function) dans le routeur sans modifier les autres équipements du réseau. Cette méthode permet à un routeur de mieux choisir et proposer les nouveaux APs au MN en équilibrant la charge du réseau local. Pour réduire la perte de paquets due aux procédures du handover, nous proposons de modifier le protocole IPv6 Mobile. Le MN met fin à l'association entre son adresse mère et son adresse temporaire avec l'Agent mère (HA) et le Nœud correspondant (CN) avant de procéder la procédure du handover. Par ce moyen, le HA peut intercepter les paquets destinés à l'adresse mère du MN et les garder dans son mémoire tampon. Une fois le MN met à jour l'association entre son adresse mère et sa nouvelle adresse temporaire avec le HA, le HA peut envoyer les paquets stockés dans son mémoire de tampon au MN. Il intercepte et redirige également les paquets du CN ou du MN vers la nouvelle adresse temporaire du MN ou vers les adresses du CN respectivement pendant la phase de mise à jour d'association. Avec cette méthode, nous pouvons limiter la perte de paquets et garantir un délai acceptable.

Ensuite, nous avons estimé la performance de QoS en termes de délai et de la perte de paquets. Avec notre méthode E-HCF, le délai d'un handover est diminué de 1675 ms à environ 100 ms par rapport au standard IPv6 Mobile. En plus, nous avons également étudié les différents types de trafic tels que les trafics TCP et UDP dans le cadre d'étude. Dans tous les cas, la méthode E-HCF donne une satisfaction à la performance du handover.

J'aurais cependant d'aimer de continuer à travailler sur le délai du handover dans le protocole IPv6 Mobile afin de diminuer le délai. De plus, cette thèse n'a pas encore débordé le problème de la sécurité qui est une problématique à étudier dans les réseaux sans fil, par exemple, l'authentification est un autre sujet important à traiter par la méthode E-HCF.

Glossaire

ACK: Acknowledgment
AIFS: Arbitration Inter Frame Spacing
AP: Access Point
AR: Access Router
ATM: Asynchronous Transfer Mode
BA: Binding Acknowledgement
BSS: Basic Service Set
BSSID: Basic Service Set Identifier
BU: Binding Update
CoA: Care-of Address
CoT: Care-of Test
CoTI: Care-of Test Initiate
CN: Correspondent Node
CTS: Clear To Send
DAD: Duplicate Address Detection
DHCP: Dynamic Host Configuration Protocol
DHCPv6: Dynamic Host Configuration Protocol for IPv6
DCF: Distribution Coordination Function
DiffServ: Differentiated Services
DIFS: Distributed Coordination Function IFS
DS: Distribution System
DSSS: Direct Sequence Spread Spectrum
EDCA: Enhanced Distributed Channel Access
EIFS: Extended IFS
ESS: Extended Service Set
ESSID: Extended Service Set Identifier
FBA: Fast Binding Acknowledgment
FBU: Fast Binding Update
FHSS: Frequency Hopping Spread Spectrum
FIFO: First In First Out
FNA: Fast Neighbour Advertisement
HA: Home Agent
HCCA: HCF Controlled Channel Access
HCCA: HCF Controlled Channel Access
HCF: Hybrid Coordination Function
HI: Handover Initiate
HoT: Home Test
HoTI: Home Test Initiate
IBSS: Independent Basic Service Set
IEEE: Institute of Electrical and Electronics Enginneers
IETF: Internet Engineering Task Force

IFS: Inter Frame Spacing
IP: Internet Protocol
IPv4: Internet Protocol version 4
IPv6: Internet Protocol version 6
INTSERV: Integrated Services
LLC: Logical Link Control
MAC: Medium Access Control
Mobile IP: Mobile Internet Protocol
Mobile IPv4: Mobile Internet Protocol version 4
Mobile IPv6: Mobile Internet Protocol version 6
MN: Mobile Node
NA: Neighbour Advertisement
NAP: Next Access Point
NAR: Next Access Router
NCoA: Next Care-of Address
NAT: Network Address Translation
NS: Neighbour Solicitation
PAP: Previous Access Point
PAR: Previous Access Router
PCoA: Previous Care-of Address
PrRtAdv: Proxy Router Advertisement
OFDM: Orthogonal Frequency Division Multiplexing
OSI: Open Systems Interconnection
PCF: Point Coordination Function
PIFS: Point Coordination Function IFS
PLCP: Physical Layer Convergence Procedure
PMD: Physical Medium Dependant
QoS: Quality of Service
RA: Router Advertisement
RED: Random Early Discard
RS: Router Solicitation
RFC: Request for Comment
RSVP: Resource Reservation Protocol
RTP: Real Time Protocol
RTT: Round Trip Time
SIFS: Short Inter Frame Spacing
Wi-Fi: Wireless Fidelity
WiMax: Worldwide interoperability for
WLAN: Wireless Local Area Network
WFQ: Weighted Fair Queuing
WMAN: Wireless Metropolitan Area Network
WPAN: Wireless Personal Area Network
WRAN: Wireless Regional Area Network
WRED: Weighted Random Early Discard
WRR: Weighted Round Robin

Références

[802.11] IEEE Computer Society, "IEEE 802.11 standard Wireless," 1996

[802.1199] IEEE Standard 802.11, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," IEEE Standard 802.11-1999, 1999

[802.11a99] IEEE Std. 802.11a 1999, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: High–speed Physical Layer in the 5 GHz Band," 1999

[IEEE 802.11b99] IEEE Std. 802.11b 1999, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher–Speed Physical Layer Extension in the 2.4 GHz Band," 1999

[IEEE 802.11e] IEEE Std. 802.11e 2001 WG, "Draft Supplement to STANDARD FOR Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Medium Access Control (MAC) Enhancements for Quality of Service (QoS), " IEEE 802.11e/D2.0, Nov. 2001.

[802.11g 03] IEEE Std. 802.11g 2003, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications – Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band,"2003

[802.15.1] IEEE Computer Society, "IEEE 802.15.1 standard Wireless," 2002

[802.15.3] IEEE Computer Society, "IEEE 802.15.3 standard Wireless," 2003

[802.15.4] IEEE Computer Society, "IEEE 802.15.4 standard Wireless," 2003

[802.16] IEEE Computer Society, "IEEE 802.16 standard Wireless," 2004

[802.20] IEEE Computer Society, "IEEE 802.20 standard Wireless," 2002

[ABR73] N.Abramson, "The Aloha system," In Computer Communication Networks, pp. 501-518, Englewood Cliffs, New Jersey, 1973

[Awa96] G.Awater, J.Kruys, "Wireless ATM – an overview," in Mobile Networks and Applications, Vol.1, Issue 3, pp.235-243, December 1996

[B04] Bluetooth SIG, "Draft Specification of the Bluetooth System, Version 2.0, "November 2004

[BHA 94] V.Bharghavan, A.Demers, S.Shenker, "ACAW: A media access protocol for wireless LANs", ACM Sigcomm, 1994.

[BroadWP] Broadcom, "White Paper IEEE 802.11g," 2003

[BHA97] V.Bharghavan and M. Jayanth, "Profile–based Next–cell Prediction in Indoor Wireless LAN," in Proc. IEEE SICON'97, April 1997

[Blondia04] C. Blondia, O. Casals, L. Cerda, N. Wijngaert and G.Willems, "Performance Evaluation of Layer 3 Low Latency Handoff Mechanisms," in Mobile Networks and Applications, Vol. 9, No.6, pp.633-645, December 2004

[CAPONE01] A.Capone, R.Kapoor, M.Gerla, "Efficient Polling Schemes for Bluetooth Picocells," In Proceedings of IEEE International Conference on Communications, Vol.7, pp.1990-994, Helsinki, Finland, June 2001

[CAR05] T.CARLU, "Comprendre IPv6 - panorama technique," Studio ISI - le MAG, Jan 2005

[Collet98] P.Collet, M.Dudet, O.Hersent "Téléphonie sur Internet : quelles perspectives ?," France Telecom 1998

[Cord05] C.Cordeiro, K.Challapali "IEEE 802.22: The First Worldwide Wireless Standard based on Cognitive Radios," in First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2005, pp.328-337, November 2005

[EUI-64] IEEE, "Guidelines For 64–Bits Global Identifier (EUI-64) Registration Authority," http://standards.ieee.org/regauth/oui/tutorials/EUI64.html

[Eng99] P.Enge and P.Misra, "Special Issue on Global Positioning System," in Proceedings of the IEEE, Special Issue on GPS, Vol.87, pp.3-15, Javier 1999

[HOS05] A.Hossain, K.Kanchanasut, "A handover management scheme for mobile IPv6 networks," in Proceeding 14th International Conference on Computer Communications and Networks, pp.43-48, 2005

[HSI02] R. Hsieh, A. Seneviratne, H. Soliman, "Performance Analysis on Hierarchical Mobile IPv6 with Fast-handoff over End-to-End TCP," in IEEE Global Telecommunications Conference (GLOBECOM), 2002.

[Hua06] P.Huang, Y.Tseng, K.Tsai, "A Fast Handoff Mechanism for IEEE 802.11 and IAPP Networks," in IEEE 63rd Vehicular Technology Conference, 2006

[IPZERO] Concepts Réseaux http://www.iprezo.org

[ITU96] ITU, "General Characteristics of International Telephone Connections and International Telephone Circuits: One–way Transmission Time," Recommendation G.114, 1996

[ITU94] ITU, "Terms and definitions related to quality of service and network performance including dependability," Recommendation, E.800, 1994

[JAN97] J. Jannink, D. Lam, N. Shivakumar, J. Widom and D. Cox, "Efficient and Flexible Location Management Techniques for Wireless Communication System," ACM/Baltzer Wireless Networks, Vol.3, pp.361-374, 1997

[Kim04] Hye–Soo Kim, Sang–Hee Park, "Selective Channel Scanning for Fast Handoff in Wireless LAN Using Neighbor Graph ", in International Technical Conference on Circuits/Systems, Computers and Communications (ITC–CSCC2004), Japan, July, 2004

[LI07] Q.Li, T.Jinmei, K.Shima, "IPv6 Advanced Protocols Implementation," Morgan Kaufmann Publishers 2007

[Lin03] A.Lindgren, A.Almquist, "Quality of Service Schemes for IEEE 802.11 Wireless LANs – An evaluation," in Mobile Networks and Applications, Vol. 8(3), pp.223-235, juin 2003

[LIU96] G. Liu and G. Maguire Jr., “A Class of Mobile Moti on Prediction Algorithms for Wireless Mobile Computing and Communications,” ACM/Baltzer MONET, 1(2), 1996, pp. 113–121.

[Mat00] W.Matthews, L.Cottrell, "The PingER Project: Active Internet Performance Monitoring for the HENP Community," *Communications Magazine May 2000*

[Mish03] A.Mishra, M.Shin and W.Albaugh, "An Empirical Analysis of the IEEE 802.11 MAC Layer Handoff Process," Proceeding ACM SIGCOMM Computer Communication Review, vol. 33, pp. 93–102, April 2003

[MW06] "Mobile WiMAX – Part II: A Comparative Analysis ", WiMAX Forum, 2006

[NOR03] N.Noraswamy, D.Harkins, "IPSec," CampusPress, juillet 2003

[FALL00] K.Fall, K.Varadhan, "The NS Manual," The VINT Project, 2000, http://www.isi.edu/nsnam/ns/doc

[OPNET] OPNET Modeler, http://www.opnet.com/products/modeler/home.html

[OMNET] OMNET++, www.omnetpp.org

[PACK04] S.Pack, T.Kwon and Y.Choi, "A Comparative Study of Mobility Anchor Point Selection Schemes in Hierarchical Mobile IPv6 Network," in Proceeding ACM MobiWac 2004, September 2004

[PACK06] S.Pack, Y.Choi, M.Nam, "Design and Analysis of Optimal Multi-level Hierarchical Mobile IPv6 Networks," in Wireless Personal Communications (2006) 36, pp.95-112, 2006

[PAUL02] P.Muhlethaler, "802.11 et les réseaux sans fil," Éditions Eyrolles, Paris, Août 2002.

[PERK98] C.Perkins, S.Alpert, B.Woolf, "Mobile IP: Design Principles and Practices," Editeur : Prentice Hall PTR, janvier 1998

[PEYR05] F.PEYRARD "La sécurité des réseaux Wi-Fi " Séminaire L2I, Blagnac Jul.2005.

[PH03] Porcino D, Hirt W,"Ultra–wideband radio technology: Potential and challenges ahead," IEEE Commun Mag 2003

[PingER06] Project PingER, "Internet End-to-End Performance Measurement," https://confluence.slac.stanford.edu/display/IEPM/PingER

[Pujolle05] G.Pujjole, "Les Réseaux," Edition 2005, EYROLLES, 2005

[Ram05] I.Ramani, S.Savage, "SyncScan: Practical Fast Handoff for 802.11 Infrastructure Networks," Proceeding of IEEE Infocom 2005

[RFC 791] J.Postel, "Internet Protocol," IETF, RFC 791, Septembre 1981

[RFC 1519] V.Fuller, T.Li, J.Yu, " Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy," September 1993

[RFC 1633] R.Braden, D.Clark and S.Shenker, "Integrated Services in the Internet Architecture: an Overview," IETF, RFC 1663, June 1994

[RFC 2210] J.Wroclawski, "The Use of RSVP with IETF Integrated Services," IETF, RFC 2210, September 1997

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

[RFC 3220] C.Perkins, "Mobility support for IPv4," IETF, RFC 3220, January 2002

[RFC 3513] R.Hinden, S.Deering, "Internet Protocol Version 6 (IPv6) Addressing Architecture," IETF, RFC 3513, April 2003

[RFC 3587] R.Hinden, S.Deering, E.Nordmark, "IPv6 Global Unicast Address Format," IETF, RFC 3587, August 2003

[RFC 3315] R.Droms, J.Bound, B.Volz, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)," IETF, RFC 3315, July 2003

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

[RFC 3810] R.Vida, L.Costa, "Multicast Listener Discovery Version 2 (MLDv2) for IPv6," IETF, RFC 3810, June 2004

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

[RFC 4140] H.Soliman, C.Castelluccia, K.Malki, L.Bellier, "Hierarchical Mobile IPv6 Mobility Management (HMIPv6)," IETF, RFC 4140, August, 2005

[RFC 4260] P.McCann, "Mobile IPv6 Fast Handovers for 802.11 Networks," IETF, RFC 4260, November 2005

[RFC 4429] N.Moore, "Optimistic Duplicate Address Detection (DAD) for IPv6," RFC 4429, IETF, April 2006

[RFC 4861] T.Narten, E.Nordmark, W.Simpson, "Neighbor Discovery for IP version 6 (IPv6)," RFC 4861, IETF, September 2007

[RFC 4862] S.Thomson, T.Narten, T.Jinmei, "IPv6 Stateless Address Autoconfiguration," IETF, RFC 4862, September 2007

[Rice00] J. A. Rice, "Telesonar Signalling and Seaweb Underwater Wireless Networks," Proceeding NATO Symposium on New Information Processing Techniques for Military Systems, Istanbul, Turkey, Oct. 9-11, 2000

[Ram01] K.Ramakrishnan, S.Floyd and D.Black, "The Addition of Explicit Congestion Notification (ECN) to IP," RFC 3168 IETF, September 2001

[Rod98] J.Rodrigue, "Théorie des graphes: définition et propriétés," Site Web Géographie des Transports, Hofstra University: Department of Economics and Geography, 1998

[Stallings] William Stallings, "Réseaux et communication sans fil," 2nd Edition, Pearson Education 2005

[Shin04] S.Shin, A.Forte, "Reducing MAC Layer Handoff Latency in IEEE 802.11 Wireless LANs," in International Conference on Mobile Computing and Networking, P19-26, 2004

[Tanenbaum] A. Tanenbaum, "Computer Networks," 4th Edition, Pearson Education 2003

[TOU92] G.Toussaint, J.Jaromczyk, "Relative Neighborhood Graphs and Their Relatives," In Proceeding IEEE, Vol.80, pp.1502–1517, 1992

[VAN05] Q.Van, "Contribution l'Etude de la Qualité de Service pour les Protocoles Sécurisés de Télécommunications. Application à IPSec," mémoire de thèse, pp. 17-29 Décembre 2005, Université de Paris XII – Val de Marne.

[WANG07] T.Wang, J.Chuang, "Fast Duplicate Address Detection for Seamless Inter-Domain Handoff in All-IPv6 Mobile Networks," Wireless Personal Communications (2007) 42, pp.263-275, 2007

[Wi05] "Haut débits sans-fil de demain ?", Dossier WiMax sur le Journal du Net

[Yang03] S.Yang, H.Chou, "Adaptive QoS Parameters Approach to Modelling Internet Performance," in International Journal of Network Management, Vol.13, Issue 1, January/February 2003, pp.69-82, 2003

[ZHAO05] Q.Zhao, L.Feng, "Movement Detection Delay Analysis in Mobile IP," in Elsevier journal on Computer Communications 28 (2005), pp. 550-556, 2005

Annexe

Liste des publications

1. G.Z.Wei, A.Wei, K.Xu and G.Dupeyrat, “Optimization of Handover Performance Using E-HCF Method,” In International Conference of Computer Science 2007, Beijing, China, 27–30 May, 2007.

2. H.Lin, G.Z.Wei, H.Labiod and A.Wei, “Handover Optimization for Host and Network Mobility, ” In Proceedings of IEEE/International Conference on Wireless Information Networks and Systems, Setubal, Portugal, 7–10 August, 2006.

3. G.Z.Wei, A.Wei, K.Xu and H.Deng, “Handover Control Function Based Handover for Mobile IPv6,” In International Conference of Computer Science 2006, University of Reading, UK, 28–31 May, 2006.

4. A.Wei, B.Geller, G.Z.Wei, S.Boumerdassi and E.Renault, “A Cross–Layer Solution to Improve Security and Privacy in RFID Systems,” IJCSNS International Journal, Vol.6, No. 5, pp 211 –217, May, 2006.

Paramètres dans la norme RFC 4861 et RFC 4862

Les paramètres utilisés pour la procédure DAD et la procédure de Découverte de routeur sont définis dans la norme [RFC 4861] [RFC 4862]. Les paramètres plus importants sont présentés ci-dessus :

1. ***DupAddDetectTransmits*** : détermine le nombre de messages "Sollicitations de voisin" consécutifs qui peut etre envoyé par le nœud pour exécuter la procédure DAD.

Tableau : Signification de la valeur *DupAddDetectTransmits*

DupAddDetectTransmits	0	1 (Par défaut)	2 (ou plus)
Signification	Le message "Sollicitation de voisin" ne peut pas être envoyé. C'est-à-dire que la procédure DAD n'est pas effectuée.	Le message "Sollicitation de voisin" ne peut être envoyé qu'une fois pour effectuer la procédure DAD.	Le message "Sollicitation de voisin" peut être envoyé en plusieurs fois. L'intervalle entre les messages est défini dans [RFC 4861].

2. ***RetransTimer*** : détermine l'intervalle entre les messages "Sollicitation de Voisin" consécutifs envoyés par le nœud. RetransTimer est aussi le temps qu'un nœud doit attendre après l'envoi du dernier message "Sollicitation de voisin" et avant de achever la procédure DAD [RFC 4862]. La valeur par défaut est de 1000 ms.

3. ***MaxRtrAdvInterval*** : détermine l'intervalle maximum autorisé entre les messages "Annonce de routeur non-sollicitée" envoyés par le routeur. Il doit être au moins de 4 secondes et être inferieur à 1800 secondes.

4. ***MinRtrAdvInterval*** : détermine l'intervalle minimum autorisé entre les messages "Annonce de routeur non-sollicitée" envoyés par le routeur. Il doit être au moins de 3 secondes et être inferieur à 0.75 * *MaxRtrAdvInterval* secondes. Par défaut, il vaut : 0.33 * *MaxRtrAdvInterval* secondes si *MaxRtrAdvInterval* ≥ 9 secondes.

5. ***AdvDefaultLifetime*** : Cette valeur est définie dans le champ "la durée de vie du routeur" du message "Annonce de routeur". Elle peut valoir 0 ou une valeur entre *MaxRtrAdvInterval* et 9000 secondes. Si elle vaut zéro, ceci signifie que le routeur ne doit pas être utilisé en tant que routeur par défaut. Par défaut, il vaut: 3 * MaxRtrAdvInterval secondes.

6. ***MAX_INITIAL_RTR_ADVERTISEMENTS*** : détermine le nombre maximum de fois qu'un message "Annonce de routeur non-sollicitée" peut être envoyé par le routeur avec un intervalle maximum de *MAX_INITIAL_RTR_ADVERT_INTERVAL* secondes lorsque le routeur vient d'être (re)initialisé. La valeur par défaut est de 3 fois.

7. ***MAX_INITIAL_RTR_ADVERT_INTERVAL*:** détermine l'intervalle maximum entre les MAX_INITIAL_RTR_ADVERTISEMENTS fois envois des messages "Annonce de routeur non-sollicitée" consécutifs lorsque un routeur vient d'être (re)initialisé. La valeur par défaut est de 16 secondes.

8. ***MAX_RTR_SOLICITATION_DELAY*** : détermine le délai aléatoire tiré entre *(0, MAX_RTR_SOLICITATION_DELAY)* que le nœud doit attendre avant d'envoyer le premier message "Sollicitation de routeur" lorsqu'il vient de se connecter à un nouveau réseau ou vient d'être (re)initialisé. La valeur par défaut est de 1 seconde.

9. ***MAX_RTR_SOLICITATIONS*** : détermine le nombre maximum de fois que le nœud peut envoyer le message "Sollicitation de routeur" avant de conclure qu'il n'y a pas de routeur dans le réseau. La valeur par défaut est de 3 fois.

10. ***RTR_SOLICITATION_INTERVAL*** : détermine l'intervalle minimum entre les envois consécutifs de messages "Sollicitation de routeur". La valeur par défaut est de 4 secondes.

11. ***MAX_RA_DELAY_TIME*** : détermine le temps que le routeur doit attendre avant d'envoyer le message "Annonce de routeur sollicitée". La valeur par défaut est de 0,5 seconde.

12. ***MIN_DELAY_BETWEEN_RAS*** : détermine l'intervalle minimum pour tous les types de messages "Annonce de routeur" successifs. La valeur par défaut est de 3 secondes.

Liste des figures

Liste des tableaux