THÈSE

présentée à
l'Université Louis Pasteur de Strasbourg
Département Informatique
Laboratoire LSIIT, UMR CNRS-ULP N°7005

Pour obtenir le grade de
Docteur de l'Université Louis Pasteur
Mention SCIENCES
Spécialité INFORMATIQUE

par

Julien MONTAVONT

Gestion des déplacements de terminaux IPv6 mobiles assistée par géolocalisation

Soutenue publiquement le 8 Décembre 2006 devant le jury composé de :

M. **Andrzej DUDA**, Rapporteur externe
Professeur à l'ENSIMAG de Grenoble
M. **Thomas NOEL**, Directeur de thèse
Professeur à l'Université Louis Pasteur de Strasbourg
M. **Jean-Jacques PANSIOT**, Rapporteur interne
Professeur à l'Université Louis Pasteur de Strasbourg
M. **Samuel PIERRE**, Rapporteur externe
Professeur à l'Ecole Polytechnique de Montréal
M. **David SIMPLOT-RYL**, Examinateur
Professeur à l'Université des Sciences et Technologies de Lille

Remerciements

Les travaux réalisés au cours de cette thèse ont bénéficié du soutien d'un grand nombre de personnes. Je profite de l'occasion qui m'est donnée ici pour leur exprimer toute ma gratitude.

Je tenais en premier lieu à remercier vivement Thomas Noël, mon directeur de thèse, pour son encadrement et sa disponibilité. Je le remercie pour la confiance qu'il m'a accordée et pour m'avoir fait bénéficier de ses conseils et de son expérience.

Je remercie Messieurs Andrzej Duda, Jean-Jacques Pansiot, Samuel Pierre et David Simplot-Ryl pour l'intérêt qu'ils ont porté à mes travaux en acceptant de faire partie de mon jury de thèse.

Je souhaite remercier chaleureusement mon frère Nicolas, qui m'a aidé à initier mes premiers travaux de recherches et qui m'a fait bénéficier de ses conseils. Merci d'avoir toujours été là dans les moments critiques.

Je tiens également à remercier toute l'équipe Réseaux et Protocoles du LSIIT, et plus particulièrement les doctorants présents et passés, avec qui j'ai apprécié travailler. Merci à Alexander, Christophe, Emil, Jean, Pascal et Vincent pour votre disponibilité et votre gentillesse.

Enfin, je remercie également Caroline, mes parents, ma soeur Alexandra, et mes amis, pour leur soutien indéfectible tout au long de cette thèse, mais également durant mes années d'études.

A ma famille

Table des matières

Table des figures

Liste des tableaux

Introduction Générale

Les travaux présentés dans cette thèse ont pour objectif d'optimiser la gestion de la mobilité des terminaux dans l'Internet Nouvelle Génération. Plus particulièrement, nous nous sommes intéressés aux bénéfices apportés par l'introduction d'informations de géolocalisation dans les différents mécanismes permettant la mobilité des utilisateurs. Cette thèse a notamment donné lieu à la définition et à l'implémentation de deux nouveaux protocoles, ainsi qu'à l'amélioration d'un outil de simulation de réseau sans fil IPv6.

Contexte

Le fort engouement des technologies sans fil a permis de diversifier les mécanismes d'interconnexion du réseau Internet, ce dernier étant désormais composé de différents réseaux filaires et sans fil. Cette offre de connexions a fait émerger de nouveaux usages tels que la possibilité de communiquer tout en se déplaçant. Parmi ces technologies sans fil, les réseaux de type IEEE 802.11, plus communément appelés Wi-Fi (Wireless Fidelity), sont très populaires. En raison du faible coût des équipements Wi-Fi, cette technologie est abordable pour le grand public et commence à s'imposer en tant que principal réseau d'accès sans fil à l'Internet. Cependant, le déploiement de telles technologies contribue fortement à l'augmentation des terminaux réseaux (téléphones, appareils photos, consoles de jeux, ...) accentuant encore le besoin d'adresses IP. Le déploiement imminent de la nouvelle version du protocole IP (IPv6) est donc plus que jamais nécessaire d'autant plus qu'elle permet l'ajout de services optionnels tels que la mobilité au niveau IP.

Dans les réseaux Wi-Fi IPv6, on distingue généralement la mobilité au niveau des couches liaison et réseau du modèle OSI. Lorsqu'un terminal mobile se déplace entre deux points d'accès, il effectue ce qu'on appelle un *handover de niveau 2*, car il ne met en jeu que les deux premières couches du modèle OSI. Lorsque les deux points

d'accès se situent dans des sous-réseaux IPv6 différents, le terminal doit également effectuer un *handover de niveau 3*, faisant intervenir en plus la couche réseau et de ce fait de nouveaux acteurs. Ces procédures sont respectivement gérées par la norme IEEE 802.11 et par le protocole Mobile IPv6. Cependant, nous avons pu observer que ces procédures provoquent des coupures dans les communications courantes, particulièrement perceptibles lors de communications temps réel du type voix sur IP ou vidéo à la demande. Dans le même temps, la géolocalisation suscite actuellement un vif intérêt dans de nombreux domaines. Cet enthousiasme a permis aux systèmes de positionnement de s'améliorer et d'être disponibles dans un nombre croissant d'environnements. Le travail réalisé au cours de cette thèse fut donc d'étudier les gains obtenus par l'ajout d'informations de géolocalisation dans la gestion du handover. Cette étude nous a amené à la définition de deux nouveaux protocoles de communications, appelés SHAPE (*Seamless Handovers Assisted by Position Estimation*) et FLH (*Fast Location-based Handover*). Ces protocoles reposent notamment sur l'identification des futurs points d'accès des terminaux mobiles afin de positionner toutes les informations nécessaires pour optimiser les deux niveaux des handovers.

Gestion de la mobilité

Lorsqu'un terminal Wi-Fi se déplace, il peut sortir de la couverture de son point d'accès courant, auquel cas il se trouvera dans l'incapacité de continuer à communiquer. Afin de retrouver une connectivité, le terminal doit rechercher un nouveau point d'accès Wi-Fi auquel se rattacher. Cette procédure est décrite dans la norme IEEE 802.11 et peut se décomposer en trois phases : découverte, authentification et association. Il a été clairement établi que c'est la phase de découverte qui est principalement responsable du temps de latence engendré par les handovers de niveau 2. Dès lors, nous avons commencé par définir et évaluer diverses techniques d'amélioration de cette phase [61, 62]. Nos travaux nous ont montré qu'il était possible d'optimiser la phase de découverte et par conséquent le handover de niveau 2 de manière générale lorsque les terminaux mobiles ont une connaissance au préalable de leur environnement. La différence entre les diverses propositions vient donc principalement des mécanismes permettant d'acquérir cette connaissance.

A la fin d'un handover de niveau 2, il est possible que le nouveau point d'accès d'un terminal mobile se situe dans un sous-réseau IPv6 différent du précédent. Sans support spécifique, le terminal mobile va mettre à jour son adresse IPv6 ayant pour conséquence de rompre toutes ses communications courantes. Parmi les solutions proposées pour supporter la mobilité dans les réseaux IPv6, le protocole Mobile IPv6 est en train de s'imposer comme standard. Dans ce dernier, les terminaux mobiles se voient

attribuer deux adresses IPv6. L'adresse mère constitue l'adresse principale d'un terminal et l'identifie dans son réseau mère. Elle lui permet de communiquer de la même manière qu'un noeud fixe. Lorsque le terminal se déplace dans un réseau visité, il obtient en plus une adresse temporaire qui l'identifie à sa localisation actuelle. Dès lors, une nouvelle entité du réseau mère, appelé l'agent mère, va jouer le rôle d'agent relais entre l'adresse mère et l'adresse temporaire du terminal. Bien que relativement transparente pour des applications à faible débit, cette technique peut contribuer au temps de latence total engendré par un handover. Trois facteurs sont principalement mis en cause : la détection du nouveau lien IPv6, la vérification de l'unicité de la nouvelle adresse temporaire et l'enregistrement de cette adresse auprès de l'agent mère. Parmi les nombreuses propositions suggérées afin d'améliorer le protocole Mobile IPv6, nous avons notamment étudié le protocole *Fast Handovers for Mobile IPv6* (FMIPv6). Les résultats expérimentaux obtenus nous ont montré que ce protocole n'engendre aucune perte de paquets lors de handovers de niveau 3 indépendamment des problèmes liés aux trois mécanismes cités précédemment [59]. Cependant, il est nécessaire que les terminaux mobiles connaissent a priori leurs prochains points d'accès et aucune précision sur l'obtention d'une telle information n'est réellement mentionnée dans les spécifications du protocole FMIPv6. De plus, le protocole souffre d'un manque d'optimisation du handover de niveau 2, pouvant déjà fortement perturber les communications.

Utilisation de la géolocalisation dans la gestion du handover

Les analyses citées ci-dessus mettent en évidence la nécessité de connaître au préalable la destination (i.e. le prochain point d'attachement) des terminaux mobiles pour effectuer des handovers rapides (aussi bien au niveau 2 qu'au niveau 3). Dès lors, il paraît évident que l'utilisation d'informations de géolocalisation dans la gestion du handover pourrait simplifier et fiabiliser la détermination des futurs points d'accès des terminaux mobiles. Dans le cadre de cette thèse, nous avons défini et étudié une première approche allant dans ce sens [65]. Baptisé SHAPE (*Seamless Handovers Assisted by Position Estimation*), ce protocole permet à chaque terminal mobile d'envoyer périodiquement sa position à un contrôleur. Disposant des paramètres de niveaux 2 et 3 des points d'accès dont il a la charge, ce contrôleur initie la procédure de handover en fonction de la distance géographique entre les équipements. Dès que la distance entre un terminal et son point d'accès courant dépasse un certain seuil prédéfini, le contrôleur déclenche un handover vers le point d'accès se trouvant actuellement le plus proche du terminal. A cette occasion, les terminaux mobiles reçoivent une notification du contrôleur incluant toutes les informations de niveaux 2 et 3 nécessaires pour réduire la phase de

découverte et permettre la détection a priori des nouveaux liens IPv6. L'évaluation du protocole SHAPE a donné lieu à une implémentation basée sur le nouveau démon Mobile IPv6 pour GNU/Linux. Les résultats obtenus ont révélé que ce protocole permet de réaliser des handovers n'excédant pas 50 millisecondes. Cette valeur est communément admise comme la limite supérieure du temps de latence pour laquelle les handovers n'ont pas de répercussions visibles sur les communications en cours. Cependant, nous avons constaté lors de notre étude approfondie réalisée par simulation, que le point d'accès le plus proche n'est souvent pas le plus indiqué pour couvrir un terminal mobile. De plus, les handovers étant initiés par rapport à la position des équipements, les erreurs de géolocalisation peuvent fortement perturber l'algorithme. En effet, nous avons identifié trois types d'erreurs possibles : soit le handover est initié alors que le terminal mobile n'est pas encore dans la portée du point d'accès cible, soit le terminal sort de la couverture de son point d'accès courant sans avoir reçu de notifications du contrôleur, soit le contrôleur déclenche un handover alors que cela n'est pas nécessaire. Toutes ces réflexions nous ont amenés à développer un nouveau protocole plus robuste face à ces problèmes.

Le protocole Fast Location-Based Handover

L'élaboration et l'évaluation du protocole Fast Location-based Handover [62, 63, 64, 66] constituent le coeur de ma thèse. Ce travail a notamment été effectué en collaboration avec les centres recherche et développement de France Télécom. Par rapport à nos précédents travaux, c'est principalement la pré-sélection des futurs points d'accès et l'envoi des paramètres associés qui sont ici améliorés. Dans ce protocole, le contrôleur est désormais capable de déterminer la trajectoire des terminaux mobiles. En se basant sur ces trajectoires et sur la position des points d'accès, il devient possible de sélectionner le point d'accès offrant la plus vaste zone de couverture pour un terminal donné. Les paramètres relatifs aux points d'accès sélectionnés sont ensuite envoyés aux terminaux mobiles qui les enregistrent dans un cache. Ce contexte est également sauvegardé au niveau du contrôleur afin de limiter les messages et la charge. De plus, les handovers sont ici initiés par les terminaux mobiles. Dès que la qualité du lien entre un terminal et son point d'accès courant passe sous un seuil prédéfini, le terminal essaie de s'associer au point d'accès identifié par les paramètres précédemment envoyés par le contrôleur. En connaissant par avance les informations habituellement obtenues lors de la phase de découverte, il est possible de supprimer cette phase afin d'accélérer le handover. Lorsque les terminaux mobiles doivent en plus effectuer un handover de niveau 3, ils peuvent immédiatement mettre à jour leur agent mère dès la fin du handover de niveau 2 grâce aux paramètres fournis par le contrôleur.

L'évaluation de ce protocole a été réalisée par simulation [64, 66]. Nous avons utilisé le simulateur de réseau sans fil SimulX, développé au sein de notre équipe, auquel j'ai activement contribué. SimulX propose une implémentation complète de la norme IEEE 802.11 et du protocole Mobile IPv6. Les résultats de simulation obtenus montrent que notre protocole permet de réaliser des handovers rapides (inférieurs à 50 millisecondes), mais également de limiter le nombre de handovers réalisés. Les problèmes soulevés dans notre précédente étude sont ici restreints étant donné que le handover est initié en se basant notamment sur la qualité du lien radio et que les contextes sont positionnés suffisamment à l'avance sur les terminaux mobiles.

Cependant, même lors de handovers rapides, nous avons encore pu observer des perturbations dans les communications en raison de pertes de paquets. Aux vues des performances et des limitations du protocole FMIPv6, il nous est apparu intéressant de le coupler au protocole Fast Location-based Handover. Ce dernier va permettre d'identifier le prochain point d'accès des terminaux mobiles et apporte une optimisation du handover de niveau 2. Le niveau 3 va lui être géré par le protocole FMIPv6 en vue d'éviter la perte de paquets lors du handover. De plus, l'utilisation du protocole FMIPv6 lève une hypothèse faite dans le protocole Fast Location-based Handover sur le délai nécessaire pour atteindre l'agent mère. Cette solution a donné lieu à une implémentation dont l'évaluation préliminaire a permis de mettre en évidence le gain apporté par chaque protocole, avec des handovers de niveau 2 et 3 imperceptibles aux utilisateurs même lors de communications temps réel.

Plan de la thèse

Ce document se décompose en trois parties. La première partie est consacrée à la présentation du contexte de travail, à savoir la gestion de la mobilité dans l'Internet Nouvelle Génération. Nous présenterons notamment la technologie de communication IEEE 802.11 ainsi que la nouvelle version du protocole pour l'Internet (IPv6). Nous détaillerons également les différentes procédures permettant les déplacements des terminaux mobiles tout en mettant en évidence les limitations des standards actuels en termes de temps de déconnexion engendrés par les handovers. Enfin, nous ferons état des différentes propositions d'optimisation de la gestion de la mobilité disponibles dans la littérature.

Dans une seconde partie, nous présenterons nos premiers travaux nous permettant d'acquérir une certaine expérience dans le domaine étudié. Ces derniers consistent en la proposition et en l'évaluation de différentes optimisations de la procédure de handover

de niveau 2 dans les réseaux Wi-Fi. Nous y présenterons également l'outil de simulation SimulX, auquel j'ai activement contribué.

La troisième et dernière partie sera consacrée à la gestion des handovers assistée par géolocalisation. Elle fera dans un premier temps état des différentes techniques et méthodes communément utilisées pour déterminer la position d'un équipement. Puis, nous décrirons brièvement les usages actuels de la géolocalisation dans les réseaux de télécommunication et notamment dans la gestion de la mobilité des utilisateurs. Enfin, nous exposerons nos contributions sur l'optimisation des handovers à l'aide d'informations de géolocalisation. Cette dernière partie constitue le coeur de cette thèse.

Contexte de recherche

Chapitre 1

La technologie de communication IEEE 802.11

1.1 Introduction

C'est en 1997 que l'organisme de standardisation IEEE (*Institute of Electrical and Electronics Enginneers*) [42] ratifie la norme 802.11 [1] régissant les réseaux locaux sans fil aussi appelés WLAN (*Wireless Local Area Network*). Résultat de 7 années de travaux, cette norme définit les règles fondamentales de la signalisation et des services sans fil (radio et infrarouge). Cette première version proposait des débits maximums de l'ordre de 2Mbits/s dans la bande de fréquence libre des 2,4 GHz. Cependant, le développement de réseaux basés sur cette technologie est limité par les faibles débits proposés (en comparaison avec la technologie filaire Ethernet [9]) et par le coût élevé des équipements qui la rend principalement accessible aux professionnels. Conscient des problèmes sus-cités, l'IEEE fait évoluer la norme. En 1999, un amendement haut débit est ajouté au standard [3]. Les principales modifications portent sur la couche physique et proposent des débits supérieurs et une connectivité plus robuste. Deux nouveaux débits sont proposés : 5,5 Mbits/s et 11Mbits/s. Dès lors, la technologie IEEE 802.11 commence à connaître un fort engouement. La sortie en 2003 de la version 802.11g [6] la popularise définitivement. En portant le débit maximal théorique à 54 Mbits/s, les performances des réseaux locaux sans fil commencent à rattraper celles des réseaux filaires Ethernet.

Actuellement, trois versions de la norme cohabitent : 802.11a [2], 802.11b [3] et 802.11g [6]. Les versions 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.

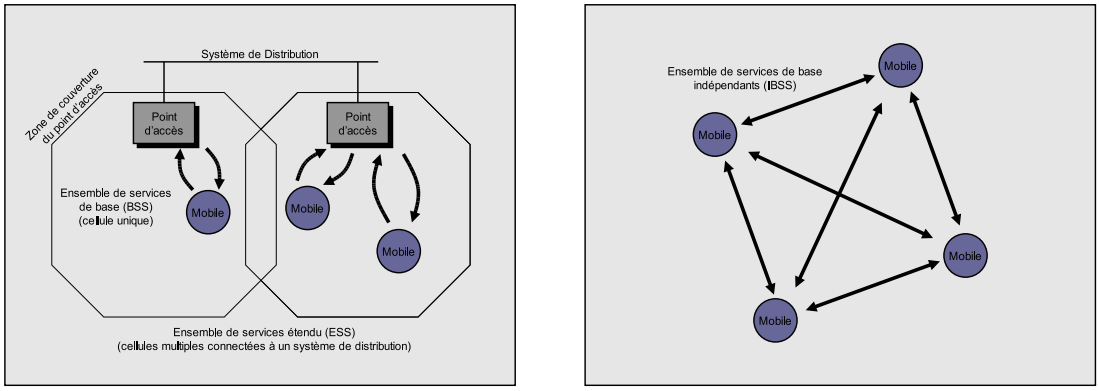
La version 802.11a propose également un débit maximal de 54Mbits/s mais utilise la bande de fréquence des 5GHz. Les versions 802.11b et 802.11g étant interopérables, un équipement 802.11b peut communiquer avec un équipement 802.11g et inversement. Par contre, un équipement 802.11a ne pourra établir une liaison radio qu'avec un autre équipement 802.11a en raison des bandes de fréquences différentes. La version 802.11a étant moins répandue, nous allons plus particulièrement nous intéresser par la suite aux versions 802.11b et 802.11g.

1.2 Principe de fonctionnement

La norme 802.11 met principalement en jeu deux types d'équipements. Les terminaux mobiles sont généralement des terminaux utilisateurs disposant d'une interface sans fil pour communiquer. On distingue également les points d'accès qui jouent le rôle de points relais entre les terminaux sans fil et permettent de faire le pont entre des réseaux filaires et sans fil. Le standard 802.11 propose deux modes d'interaction entre ces deux types d'équipements : le mode infrastructure et le mode Ad Hoc.

Dans le mode infrastructure, chaque terminal mobile est connecté à un point d'accès via une liaison sans fil. Dès lors, toutes les communications entre un terminal mobile et son correspondant vont transiter par un point d'accès. Ce dernier est généralement connecté à une infrastructure filaire, offrant ainsi la possibilité aux terminaux mobiles d'accéder aux services disponibles sur le réseau auquel est relié le point d'accès. L'ensemble formé par un point d'accès et par les terminaux mobiles associés est appelé ensemble de services de base (BSS). Chaque BSS est différencié par un identifiant de 6 octets appelé BSSID (*Basic Service Set Identifier*). L'ensemble de services étendu (ESS) est un ensemble d'un ou de plusieurs BSS connecté à un système de distribution (e.g. un réseau Ethernet) formant au final un seul et même réseau. Chaque ESS est différencié par un identifiant de 32 octets appelé ESSID ou plus généralement SSID (*Service Set Identifier*). Le SSID est notamment nécessaire lors de la connexion d'un terminal à un point d'accès. La figure 1.1(a) illustre les différents acteurs du mode infrastructure.

Inversement, le mode Ad Hoc permet à un terminal mobile de communiquer directement avec d'autres équipements sans fil sans point d'accès ni connexion filaire. Ce mode offre la possibilité de créer simplement et rapidement un réseau sans fil dans un environnement dépourvu d'infrastructure ou lorsqu'une telle infrastructure n'est pas nécessaire au regard des services attendus. L'ensemble formé par des terminaux mobiles utilisant le mode Ad Hoc est appelé ensemble de services de base indépendants (IBSS). Chaque IBSS est également identifié par un SSID. La figure 1.1(b) donne un aperçu d'un réseau IBSS.



(a) Mode infrastructure

(b) Mode Ad Hoc

FIG. 1.1 – Mode de fonctionnement d'un réseau Wi-Fi

1.3 Intégration dans le modèle TCP/IP

Appartenant à la famille de protocoles IEEE 802, la norme 802.11 a été pensée pour s'intégrer directement dans le modèle en couche actuellement utilisé dans l'Internet : le modèle TCP/IP. Ce dernier n'est en réalité qu'une simplification du modèle OSI [77] et tire son nom des deux principaux protocoles qui le composent. Le modèle TCP/IP correspond à une approche plus pragmatique du découpage d'une pile de protocoles réseaux que le modèle OSI. La norme IEEE 802.11 intervient particulièrement dans la couche physique et dans la couche liaison du modèle TCP/IP (voir figure 1.2). La couche liaison se décompose généralement en deux sous-couches appelées *Contrôle de liaison logique* (LLC) et *Contrôle d'accès au médium* (MAC). Comme tous les protocoles de la famille 802, le standard 802.11 utilise un adressage sur 48 bits. Cela permet notamment de simplifier les interactions entre les réseaux filaires et sans fil. Par contre, la sous-couche MAC est spécifique à la norme 802.11.

La couche physique 802.11 supporte deux médiums de communication différents : les ondes infrarouges et les ondes radio. Ces dernières ont notamment pris le pas sur les ondes infrarouges, devenant ainsi le support physique standard des communications 802.11. Dans la version de base de la norme 802.11, deux techniques d'étalement de spectre étaient proposées pour les ondes radio. La première, appelée FHSS (*Frequency-Hopping Spread Spectrum*), découpe la bande des 2,4 GHz en 75 sous-canaux de 1 MHz. Les communications s'effectuent donc sur une série de sous-canaux, l'émetteur et le récepteur sautant régulièrement d'un sous-canal à l'autre. Cette technique limite

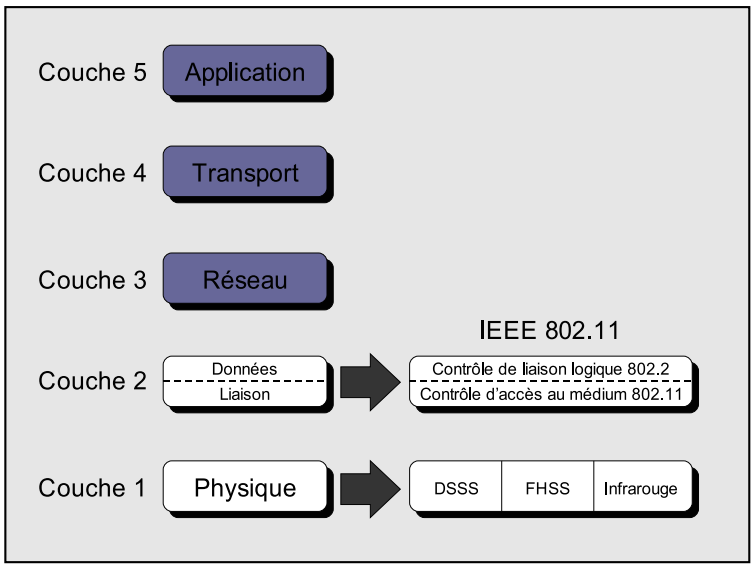


FIG. 1.2 – Niveau d'application du protocole 802.11 dans le modèle TCP/IP

cependant le débit maximal à 2 Mbits/s en raison des réglementations de la FCC (*Federal Communications Commission*) qui restreint la bande passante des sous-canaux à 1 MHz. C'est actuellement la technique DSSS (*Direct Sequence Spread Spectrum*) qui est utilisée par les équipements sans fil. Cette dernière découpe la plage des 2,4 GHz en 14 sous-canaux de 22 Mhz chacun. Les données sont ici transmises sur un seul sous-canal sans saut de fréquence. Cette technique supporte des débits plus importants, allant notamment jusqu'à 54 Mbits/s (802.11g). Cependant, les canaux adjacents se recouvrent partiellement ce qui peut provoquer des interférences dans les communications. Par rapport aux réglementations des différents pays, c'est généralement les canaux numéro 1, 6 et 11 qui sont utilisés car ils n'interfèrent pas entre eux. La figure 1.3 représente la répartition des différents canaux 802.11 avec la technique DSSS.

1.4 Accès au médium

Le partage d'un support physique entre plusieurs utilisateurs nécessite une politique d'accès équitable et performante. En effet, une collision se produit lorsque différents utilisateurs transmettent simultanément des données sur le même médium. Lors d'une collision, les données impliquées ne sont généralement pas reçues correctement par leurs destinataires. Dans les réseaux 802.11, le protocole gérant l'accès au médium est très proche du protocole CSMA/CD (*Carrier Sense Multiple Access with Collision Detection* [9]) utilisé dans les réseaux Ethernet. Le protocole CSMA/CD permet notamment

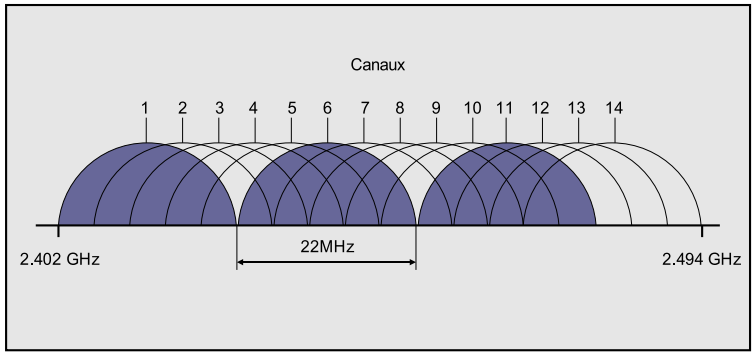


FIG. 1.3 – Répartition des canaux radio par la méthode DSSS

la détection de collisions produites par l'envoi simultané de données provenant de différents émetteurs. Cette détection est possible grâce à la capacité des équipements filaires à transmettre des données tout en écoutant le médium. Lors d'une collision, les émetteurs incriminés interrompent leurs transmissions et attendent un délai aléatoire avant de réémettre les données. Cependant, les équipements 802.11 ne peuvent pas appliquer la même procédure. En effet, ils sont incapables d'écouter le lien radio pendant qu'ils effectuent une transmission. La norme 802.11 définit deux nouvelles méthodes d'accès au médium plus adaptées aux caractéristiques des réseaux sans fil. La méthode PCF (*Point Coordination Function*) étant rarement utilisée, nous allons exclusivement détailler la méthode DCF *Distributed Coordination Function*.

1.4.1 La méthode DCF

Dans les réseaux 802.11, l'accès au médium est généralement contrôlé par la méthode DCF qui utilise le protocole CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*). C'est une méthode d'accès distribuée et asynchrone qui ne tient pas compte des éventuelles priorités des applications. Les collisions sont ici gérées par l'introduction d'accusés de réception. Pour chaque trame de données reçues correctement par un récepteur, un acquittement positif est envoyé à l'émetteur. Lorsqu'une donnée n'est pas acquittée, l'émetteur considère qu'il y a eu collision et retransmet la donnée concernée. Il est intéressant de noter que certaines trames de contrôle nécessitent également un acquittement.

Dans DCF, tout accès au médium est précédé d'une écoute du lien radio de façon à s'assurer qu'il n'est pas en cours d'utilisation. Pour une trame de donnée, un émetteur doit attendre que le support devienne libre et le reste pendant une durée appelée DIFS (*DCF Inter Frame Space*). Ensuite, l'émetteur doit encore patienter pendant une durée

déterminée par l'algorithme de backoff. Cette procédure est basée sur un algorithme exponentiel et gère les retransmissions à la manière d'Ethernet. Elle permet également d'éviter les collisions en temporisant les émissions lorsque différents émetteurs désirent accéder au médium simultanément. Pour déterminer la durée d'attente supplémentaire, l'émetteur tire un nombre aléatoire X dans l'intervalle $[0; CW]$ où CW (*Contention Window*) est une variable entière. La valeur numérique du paramètre CW dépend des caractéristiques du médium aCWmin et aCWmax et est restreinte par la relation $aCWmin \leq CW \leq aCWmax$. A la première tentative d'émission d'une donnée, le paramètre CW est positionné à aCWmin. A chaque retransmission de cette donnée (en raison de collision), le paramètre CW est séquentiellement positionné à la puissance de 2 supérieure moins 1 jusqu'à atteindre aCWmax (voir figure 1.4).

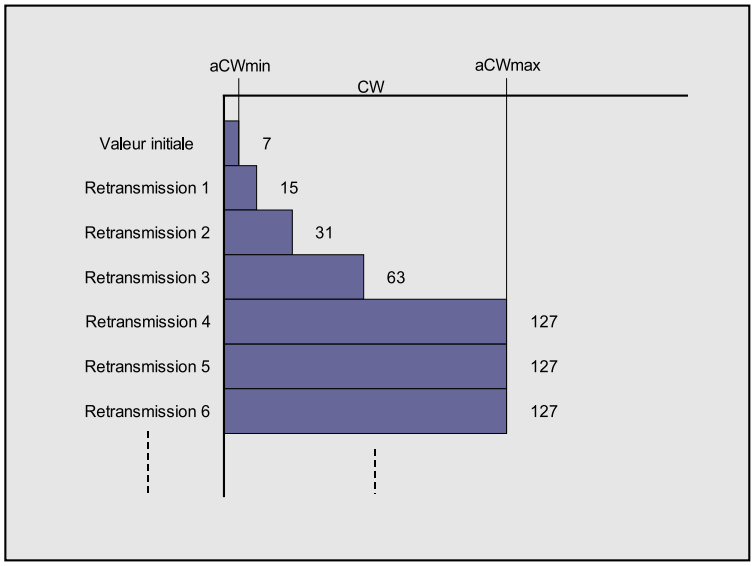


FIG. 1.4 – Exemple de l'incrémentation du paramètre CW

Dès la sélection de X, l'émetteur continue d'écouter le support et décrémente la valeur de X lorsqu'il a été libre pendant tout un *slottime*. La durée d'un *slottime* est définie de telle sorte qu'un terminal sera toujours en mesure de déterminer si un autre terminal a accédé au support au début du slot précédent. Lorsque le médium est à nouveau occupé, l'émetteur 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. La durée de la procédure de backoff est communément appelée fenêtre de contention. Lorsque la transmission d'une donnée s'est effectuée sans collision, le récepteur doit envoyer un acquittement dès que le support a été libre pendant SIFS (*Short Inter Frame Space*). Cette période est volontairement inférieure à la période DIFS utilisée par les trames de données afin de favoriser

l'émission d'acquittements suite à la réception d'une donnée. De plus, l'émission d'accusés de réception ne fait pas intervenir la procédure de backoff. La figure 1.5 présente un exemple d'accès au médium suivant la méthode DCF dans lequel deux émetteurs veulent transmettre une trame.

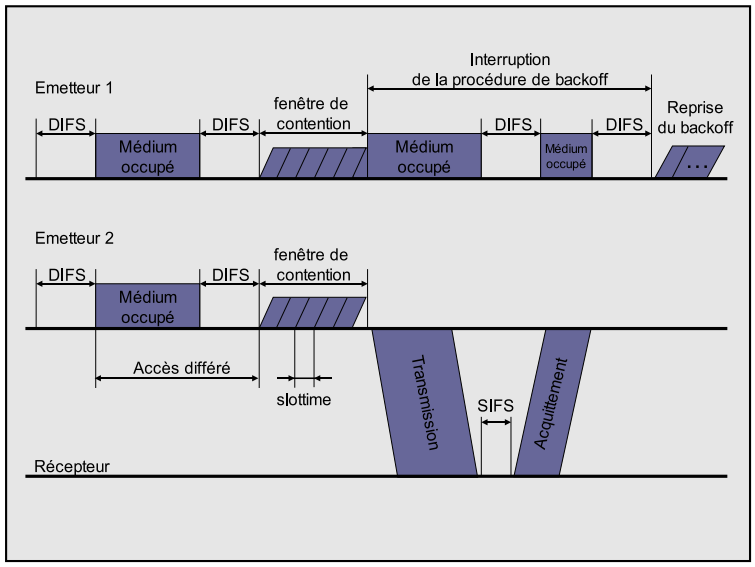


FIG. 1.5 – Méthode DCF d'accès au médium

Suivant la nature du médium (ondes radio ou infrarouges) et suivant la technique d'étalement de spectre utilisée (FHSS ou DSSS pour les ondes radio), les valeurs des paramètres aCWmin, aCWmax, *slottime*, SIFS et DIFS diffèrent. Les valeurs définies par la norme pour les ondes radio et la technique DSSS sont présentées dans la table 1.1.

Paramètre	Valeur
aCWmin	31
aCWmax	1023
slottime	20 microsecondes
SIFS	10 microsecondes
DIFS	50 microsecondes

TAB. 1.1 – Définition des paramètres pour les ondes radio et la technique DSSS

1.4.2 Mécanisme RTS/CTS

Bien que la méthode DCF permette de partager le support 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 aux *terminaux cachés*. Lorsqu'un terminal s'accapare le médium et transmet une trame, les autres terminaux se trouvant dans la portée radio de l'émetteur détectent cette émission. Comme nous venons de le présenter, la fonction DCF va empêcher l'utilisation simultanée du médium par ces terminaux. Mais il est possible que d'autres terminaux (associés au même point d'accès ou utilisant le même canal radio) n'entendent pas cette communication en raison de leurs portées radio. Imaginant le médium libre, rien ne les empêche alors de transmettre une donnée au même moment. En fonction des zones de recouvrement radio, ces émissions simultanées peuvent provoquer des collisions au niveau du récepteur. Afin de palier ces problèmes, la norme propose un mécanisme de réservation du médium. Avant une transmission, l'émetteur envoie au récepteur une trame RTS (*Request To Send*) indiquant qu'il va lui transmettre une trame de données. En retour, le récepteur envoie une trame CTS (*Clear To Send*). Cette trame notifie les terminaux se trouvant dans la portée radio du récepteur de ne pas utiliser le médium car une émission est imminente. Lorsque l'émetteur reçoit la trame CTS, le canal est réservé et il peut transmettre sa trame de données. La figure 1.6 illustre ce mécanisme.

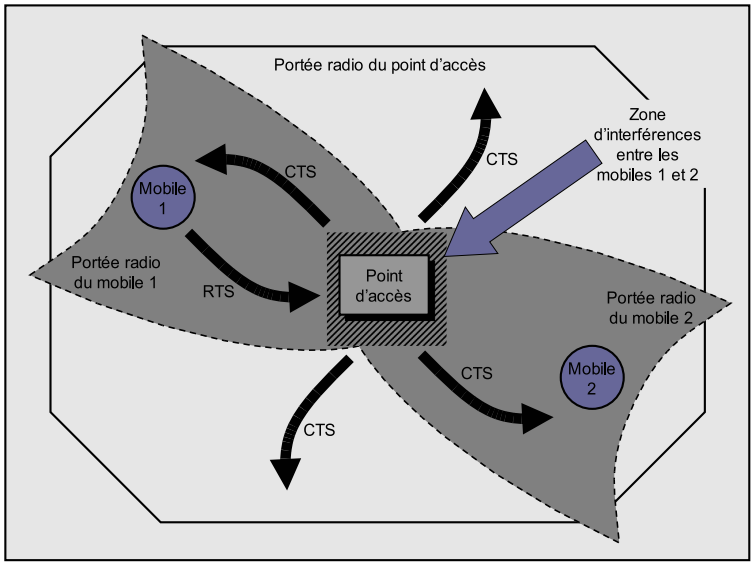


FIG. 1.6 – Procédure RTS/CTS pour éviter le problème du terminal caché

La procédure RTS/CTS est cependant un mécanisme optionnel, dont l'utilisation est déterminée par le paramètre *dot11RTSThreshold*. 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.

1.5 Sécurité

Les communications sans fil, en raison de la nature du support de transmission, sont particulièrement sensibles aux problèmes de sécurité. Deux principaux problèmes surviennent : l'accès au réseau et la confidentialité des communications. En effet, aucune restriction physique n'empêche un terminal mobile d'utiliser un point d'accès dès lors qu'ils sont à portée radio l'un de l'autre. De la même manière, un utilisateur malintentionné peut espionner les communications des différents équipements sans fil qui sont dans sa portée radio. Pour résoudre ces problèmes, la norme permet de restreindre l'accès au réseau par deux méthodes d'authentification et propose de chiffrer les données.

1.5.1 Le protocole WEP

La confidentialité des données est assurée par un algorithme de chiffrement baptisé WEP (*Wired Equivalent Privacy*). Le protocole WEP utilise l'algorithme de chiffrement par flot RC4 (*Rivest Cipher 4*). Cet algorithme de cryptage n'a jamais été officiellement publié et reste propriétaire. L'organisme de standardisation IETF (*Internet Engineering Task Force* [43]) a donc défini un algorithme compatible avec l'algorithme RC4, appelé *Alleged-RC4* ou *ARCFOUR* [49].

Le chiffrement par flot est un chiffrement symétrique (une seule clé permet de chiffrer et de déchiffrer les données) dans lequel une même clé ne doit pas être utilisée à plusieurs reprises. Le principe consiste à utiliser une clé primaire connue des différentes entités à laquelle on combine un vecteur d'initialisation (suite de nombres aléatoires) dans le but de créer une clé temporaire. Cette clé temporaire est donc formée d'une

suite de nombres pseudo-aléatoires dont la longueur finale est égale à la taille maximale du champ réservé aux données dans les trames sans fil. Pour chaque trame de données, un nouveau vecteur d'initialisation et par conséquent une nouvelle clé temporaire sont calculés de façon à ne jamais utiliser deux fois une même clé de chiffrement. La clé temporaire est ensuite combinée aux données du message original par l'opération logique XOR (*ou exclusif*). Enfin, on ajoute encore au message ainsi formé le vecteur d'initialisation utilisé. Les vecteurs d'initialisation apparaissent de manière transparente dans les messages pour permettre aux récepteurs de déchiffrer les messages. Dans les réseaux 802.11, la longueur de la clé primaire est de 40 ou 104 bits et celle des vecteurs d'initialisation est de 24 bits. La figure 1.7 illustre le chiffrement d'une trame de données par l'algorithme WEP.

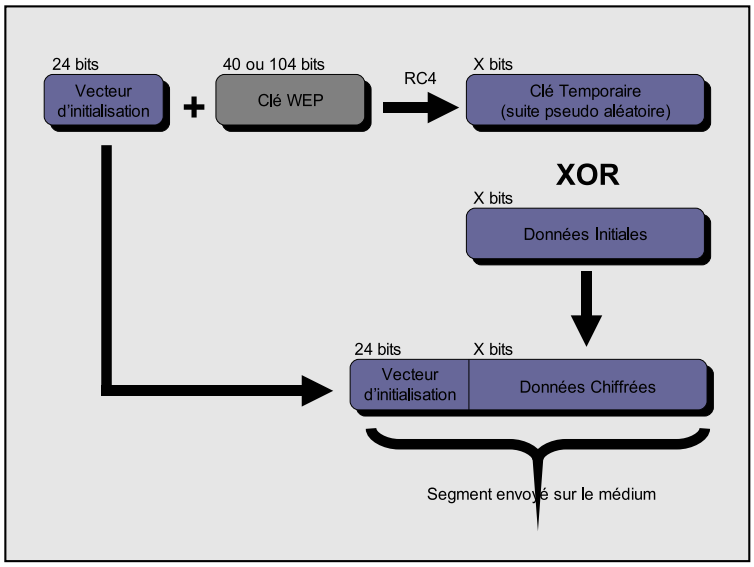


FIG. 1.7 – Chiffrement des données par le protocole WEP

1.5.2 Méthodes d'authentification

La norme 802.11 propose deux méthodes d'authentification : la méthode ouverte *Open System Authentication* et la méthode à clé partagée *Shared Key Authentication*. La méthode ouverte n'est pas, à proprement parler, une méthode d'authentification puisqu'elle autorise l'accès au réseau à tout terminal. Cette méthode d'authentification offre donc la possibilité de créer des réseaux sans fil accessibles à tous. Par contre, la méthode à clé partagée permet de restreindre l'accès au réseau. Cette méthode introduit le concept du secret partagé : le point d'accès et les terminaux autorisés à accéder au réseau établissent au préalable un secret. Lors de l'authentification d'un terminal, le

point d'accès s'assure que ce terminal est en possession du secret avant de l'autoriser à accéder au réseau.

Dans la pratique, la méthode d'authentification à clé partagée requiert l'utilisation du protocole WEP. En effet, le secret partagé va correspondre à la clé WEP (de 40 ou 104 bits) actuellement positionnée sur le point d'accès. Pour authentifier un terminal, le point d'accès crée une clé temporaire (cf. section 1.5.1) et l'envoie au terminal. Dès réception, le terminal copie la clé dans un nouveau message qu'il chiffre en utilisant le protocole WEP avant de le renvoyer au point d'accès. Puis, le point d'accès déchiffre le message à l'aide de la clé WEP et du vecteur d'initialisation qu'il contient et vérifie que les données déchiffrées correspondent à la clé temporaire initiale qu'il avait envoyée. Si les deux clés correspondent, le terminal est authentifié et autorisé à accéder au réseau. La figure 1.8 illustre la méthode d'authentification à clé partagée.

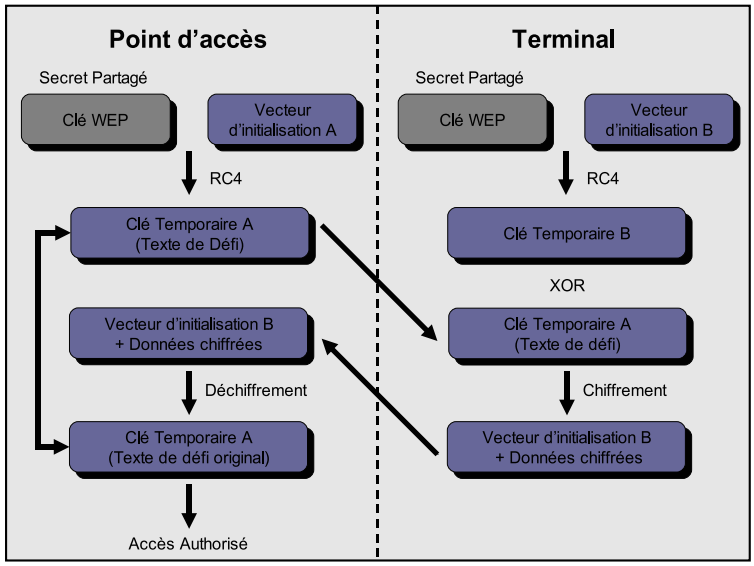


FIG. 1.8 – Méthode d'authentification à clé partagée

1.6 Extensions de la norme

Le standard 802.11 évolue constamment et de nombreux groupes de travail de l'IEEE tentent d'améliorer chaque aspect de cette technologie. On peut notamment relever la norme 802.11e [4] qui se propose d'apporter une gestion de la qualité de service au niveau de la couche liaison des données, ainsi que la norme 802.11f [5] qui définit un protocole d'échange d'informations entre différents points d'accès. Cependant, l'un

des principaux reproches émis à l'encontre de la technologie 802.11 porte sur les mécanismes de sécurité proposés par défaut. En effet, il a été rapidement prouvé que le protocole WEP n'est pas assez robuste pour établir une sécurité efficace [15, 18]. Il est notamment assez facile de deviner une clé WEP en raison de la faible longueur des vecteurs d'initialisation qui introduisent des répétitions de clefs lors de réseaux très actifs. Afin de palier les faiblesses du WEP, une extension à la norme 802.11 a été ratifiée par l'IEEE en 2004 : la norme 802.11i [7].

1.6.1 La norme 802.11i

La norme IEEE 802.11i est destinée à établir les mécanismes qui seront communément utilisés pour assurer une sécurité maximale des réseaux Wi-Fi. Sa mise en place au sein des équipements 802.11 s'effectue en deux étapes à travers les protocoles WPA et WPA2 (*Wi-Fi Protected Access*) définis par la Wi-Fi Alliance [107]. Cette dernière est une association à but non lucratif d'entreprises qui certifie le matériel utilisant le sigle Wi-Fi.

Le protocole WPA

Le protocole WPA est une solution intermédiaire qui vise à remplacer rapidement le protocole WEP le temps que la norme 802.11i soit finalisée. Ce protocole cherche également à rester compatible avec les anciens équipements Wi-Fi.

Dans WPA, les données sont toujours codées avec un algorithme de chiffrement par flot RC4 mais les vecteurs d'initialisation comportent désormais 48 bits et la clé primaire 128 bits. Le protocole WPA ajoute également un mécanisme de changement dynamique des clés de chiffrement appelé TKIP (*Temporal Key Integrity Protocol*). A l'aide de ce mécanisme, les clés de chiffrement sont donc périodiquement renouvelées lors des communications. De plus, un nouvel algorithme d'identification des messages (MIC) appelé *Michael* a été mis en oeuvre. Bien qu'il ne garantisse pas l'absence de contrefaçons des messages, il constitue le mécanisme le plus robuste possible qui reste compatible avec les anciens équipements réseaux. Au niveau de l'authentification des utilisateurs, le protocole WPA utilise désormais un serveur d'authentification 802.1X [8] et s'appuie sur la famille des protocoles EAP (*Extensible Authentification Protocol* [10]) qui supporte de nombreux mécanismes d'authentification.

A l'aide de ces différents mécanismes, le protocole WPA rend l'intrusion dans un réseau sans fil 802.11 beaucoup plus difficile mais pas impossible. C'est pourquoi le protocole WPA2, considéré comme complètement sécurisé, est amené à le remplacer.

Le protocole WPA2

Le protocole WPA2 est la version certifiée par la Wi-Fi Alliance de la norme 802.11i. Il supporte les différents mécanismes obligatoires de la norme, ce qui ne le rend pas forcément compatible avec certains anciens équipements sans fil. Il reprend les différents éléments du protocole WPA mais propose l'utilisation d'un nouvel algorithme de chiffrement appelé CCMP (Counter-Mode / CBC-Mac Protocol) qui est basé sur un chiffrement par bloc AES (*Advanced Encryption System*). Dans un chiffrement par bloc, les données sont découpées en blocs de taille généralement fixe, qui sont ensuite chiffrés les uns après les autres. L'algorithme CCMP utilise des clés et des blocs de 128 bits pour chiffrer les données. A ce jour, aucune faille n'a été répertoriée sur ce système.

1.7 Conclusion

La technologie IEEE 802.11, bien que relativement récente, a rapidement su s'imposer comme l'une des principales technologies d'accès sans fil au réseau Internet. Ce succès est notamment dû à des performances en perpétuelle évolution (débits proposés, ...) ainsi qu'au maintien d'une compatibilité avec les premières générations des équipements. Le coût du matériel ainsi que la création simple et rapide des réseaux Wi-Fi ont également contribué à la popularisation de cette technologie auprès des particuliers. Néanmoins, le monde de l'entreprise a été moins enthousiaste dans l'adoption de cette technologie en raison des problèmes de sécurité que nous avons abordés. Les nouveaux mécanismes introduits par la norme IEEE 802.11i à travers les protocoles WPA et WPA2 devraient lever les dernières craintes afin de pérenniser le déploiement des réseaux Wi-Fi.

L'introduction des réseaux Wi-Fi dans le réseau Internet a notamment permis d'intensifier la mobilité des utilisateurs lors de communications. De tels déplacements demandent une gestion particulière intervenant à différents niveaux du modèle TCP/IP. Dans le chapitre suivant, nous allons présenter les différents mécanismes communément utilisés pour permettre la mobilité des utilisateurs.

Chapitre 2

Gestion de la mobilité dans les réseaux de nouvelle génération

2.1 Introduction

Le réseau Internet constitue à ce jour le plus grand réseau de communication. L'acheminement des données sur l'Internet est assuré par le protocole IP (*Internet Protocol*) qui intervient au niveau de la couche réseau (i.e. couche numéro 3) du modèle TCP/IP. Actuellement, c'est la version 4 de ce protocole (IPv4 [81]) qui est notamment utilisée sur l'Internet. Cependant, cette version commence à montrer ses limites en raison du nombre d'adresses IP disponibles. Ces adresses sont utilisées pour identifier de manière unique un équipement sur le réseau à un instant donné. Suite à la popularisation du réseau Internet, le nombre d'équipements connectés simultanément et donc disposant d'une adresse IP a littéralement explosé, laissant envisager à court terme une pénurie d'adresses IP. En effet, les adresses IPv4 sont codées sur 32 bits, ce qui permet d'identifier théoriquement 2^{32} équipements simultanément, soit environ 4 milliards de machines. Ce nombre est en pratique limité par l'attribution de plages d'adresses à diverses organisations ou pays qui n'utilisent pas forcément tout l'espace d'adressage qui se trouve à leur disposition.

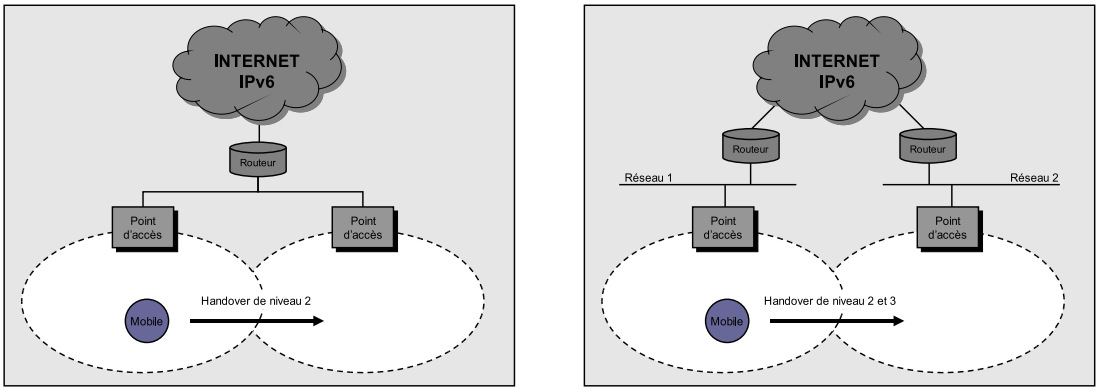
Pour faire face à ce problème, une nouvelle version du protocole IP a été développée par l'organisme de standardisation IETF [43]. Baptisée IPv6 [23], cette nouvelle version propose désormais des adresses codées sur 128 bits ce qui devrait permettre l'adressage de plusieurs centaines de milliards de machines. Les 64 premiers bits sont utilisés pour indiquer le préfixe du sous-réseau dans lequel se trouve un équipement, et les 64 derniers bits identifient l'équipement au sein de ce sous-réseau. En outre, le

protocole IPv6 supporte dans ses spécifications de base l'ajout d'options dans l'en-tête IP facilitant ainsi le développement d'extensions. Une autre nouveauté intéressante repose sur l'introduction d'une méthode d'autoconfiguration d'adresses sans état [101], ce qui signifie que les terminaux sont capables d'obtenir automatiquement une adresse IPv6 valide sans l'intervention d'un serveur centralisé. Grâce à toutes ces nouveautés et possibilités, la version 6 du protocole IP est destinée à être le protocole de l'Internet Nouvelle Génération.

Dans ce chapitre, nous allons présenter les différents mécanismes et procédures qui permettent aux terminaux mobiles de se déplacer à travers de multiples réseaux Wi-Fi IPv6. Nous détaillerons notamment les procédures standard et leurs facteurs limitants, ainsi que les optimisations proposées dans la littérature qui nous paraissent particulièrement efficaces.

2.2 Concepts de mobilité

Dans les réseaux IPv6, on distingue généralement deux types de déplacements. Un changement du point d'attachement physique au réseau est référencé par les termes *handover de niveau 2* car il ne fait intervenir que les deux premières couches du modèle TCP/IP (i.e. physique et liaison). Dans les réseaux Wi-Fi, les handovers de niveau 2 peuvent par exemple se produire lorsqu'un terminal mobile change de point d'accès (voir la figure 2.1(a)).



(a) Handover de niveau 2

(b) Handover de niveau 2 et 3

FIG. 2.1 – Illustration des handovers de niveau 2 et 3

A la suite d'un handover de niveau 2, les terminaux mobiles disposent d'une connectivité de niveau 2, c'est-à-dire qu'ils sont capables de communiquer avec les différents équipements situés sur le même lien. Tant que les terminaux ne changent pas de sous-réseau IP, ils disposent également d'une connectivité de niveau 3. Le deuxième type de déplacement est référencé par les termes *handover de niveau 3* et correspond au changement de sous-réseau IP. Lorsque, par exemple, le nouveau point d'attachement d'un terminal se situe dans un sous-réseau différent du précédent, le terminal devra effectuer en plus un handover de niveau 3 afin de rétablir sa connectivité de niveau 3 (voir la figure 2.1(b)).

2.3 Itinérance de niveau 2 dans les réseaux Wi-Fi

Suite à une mise en veille ou lors d'un déplacement dans une nouvelle cellule radio, un terminal mobile doit s'associer au point d'accès en charge de cette cellule avant de pouvoir communiquer. Cette procédure est définie par la norme 802.11 qui la décompose en trois phases : découverte, authentification et association.

2.3.1 Phase de découverte

La première étape d'une procédure d'association consiste à découvrir un point d'accès dont les caractéristiques s'accordent à celles du terminal mobile. Une telle recherche est rendue possible par la phase de découverte qui établit la procédure à suivre pour détecter les points d'accès environnants. Deux méthodes de recherche sont proposées, l'une active et l'autre passive.

Scan actif

Dans la recherche active, les terminaux mobiles sondent les différents canaux radio en émettant des messages *Probe Request*. Lorsqu'un point d'accès entend un tel message, il répond au terminal émetteur par une *Probe Response* contenant les différents paramètres qu'il supporte. Suivant le nombre de points d'accès à proximité et suivant les canaux radio utilisés, l'envoi d'une *Probe Request* peut donc engendrer la transmission de multiples messages *Probe Response*. Lorsque le terminal reçoit une *Probe Response*, il enregistre les différents paramètres du point d'accès contenus dans ce message. Puis, il continue sa phase de recherche. Après avoir sondé tous les canaux radio

(ou une liste de canaux radio), le terminal sélectionne un point d'accès parmi ceux qu'il a découverts et passe à la phase d'authentification.

On peut noter que les *Probe Request* sont les seuls messages de la procédure d'association qui ne nécessitent pas d'être acquittés. En effet, l'absence de *Probe Response* suite à l'envoi d'une *Probe Request* sur un canal particulier peut être interprété de deux manières. Soit une collision s'est produite sur la *Probe Request*, soit il n'y a pas de point d'accès à proximité qui opère sur ce canal. Etant donné que les messages *Probe Response* nécessitent un accusé de réception, si un point d'accès envoie une *Probe Response* au terminal, ce dernier est pratiquement certain de la recevoir en un temps fini (grâce au mécanisme de retransmission). Pour éviter que les terminaux mobiles ne s'attardent sur des canaux qui ne sont pas utilisés, la norme définit deux temps d'attente lors du scan d'un canal : *MinChannelTime* et *MaxChannelTime*. Suite à l'émission de la première *Probe Request* sur un canal, le terminal initie un compteur de temps. Lorsque le compteur atteint *MinChannelTime* et que pendant ce laps de temps le terminal n'a pas reçu de *Probe Response*, il en déduit qu'aucun point d'accès n'opère sur ce canal et passe au canal suivant. Dans le cas contraire, il attend que le compteur atteigne *MaxChannelTime* avant de classer les messages *Probe Response* reçus et de passer au canal suivant. La norme ne définit que la relation $MinChannelTime \leq MaxChannelTime$ 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.

Scan passif

La norme 802.11 spécifie également une méthode de recherche passive, dans laquelle les terminaux se contentent d'intercepter des trames de signalisation provenant des points d'accès. Ces trames sont appelées *Beacon* et sont généralement envoyées toutes les 100 millisecondes. Le temps d'attente passé sur chaque canal est identique à celui décrit pour la méthode active.

2.3.2 Phase d'authentification

Lorsqu'un terminal mobile a sélectionné un nouveau point d'accès suite à une phase de découverte, il doit en premier lieu s'y authentifier. Comme nous l'avons présenté dans le chapitre 1, deux méthodes d'authentification sont possibles. La méthode ouverte ne nécessite qu'une séquence de deux messages (requête / réponse) car chaque terminal est systématiquement autorisé à accéder au réseau. Par contre, la méthode à clé partagée est

décomposée en une séquence de quatre messages. Le terminal commence par envoyer son identité au point d'accès. Celui-ci demande alors au terminal de répondre à un texte de défi permettant de vérifier si le terminal possède le secret partagé. Après vérification de la réponse au texte de défi, le point d'accès communique au terminal le résultat de l'authentification (réussie ou non).

2.3.3 Phase d'association

La phase d'association constitue la dernière étape d'un handover de niveau 2 et se décompose en deux messages. Suite à une authentification réussie, la phase d'association permet au terminal et au point d'accès de s'accorder sur les différents paramètres qu'ils vont utiliser pour leurs futurs communications. Un terminal mobile est capable de transmettre et de recevoir des données dès la fin de la phase d'association.

La figure 2.2 illustre les différentes phases introduites par un handover de niveau 2. Pour des raisons de lisibilité, nous n'avons pas représenté les différentes émissions d'accusés de réception.

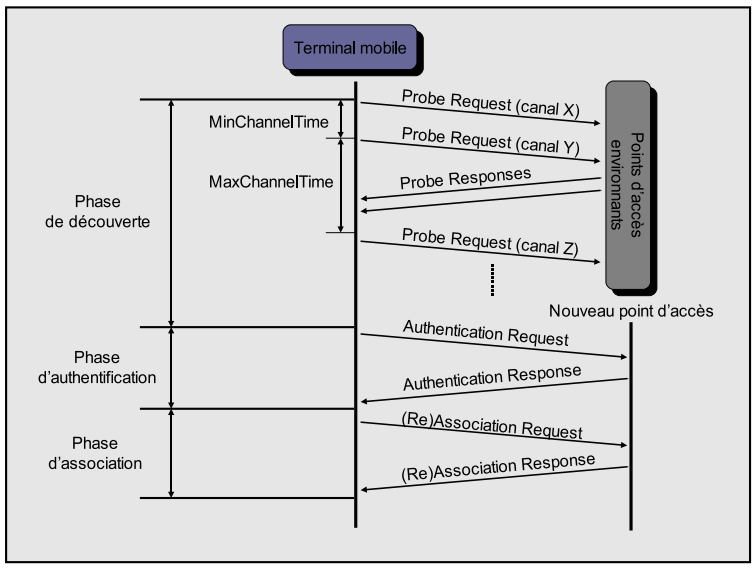


FIG. 2.2 – Handover de niveau 2 dans un réseau 802.11 utilisant un scan actif

2.4 Itinérance de niveau 3 dans les réseaux IPv6

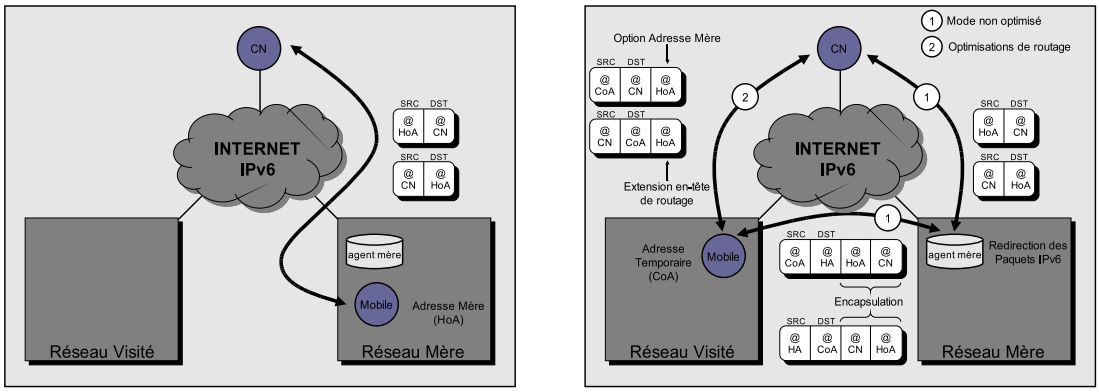
Nous avons vu que la norme 802.11 définit la procédure permettant aux terminaux mobiles de se déplacer entre divers points d'accès. Ainsi, ils sont capables de maintenir une connectivité de niveau 2 (couche liaison du modèle TCP/IP). Cependant, la norme 802.11 ne définit pas la manière dont les points d'accès suivent les déplacements des utilisateurs au niveau 3 (couche réseau du modèle TCP/IP). Alors qu'un déplacement entre deux points d'accès d'un même sous-réseau n'introduit pas de problématique de routage, le fait de changer de sous-réseau nécessite une mise à jour de l'adresse IP du terminal. Sans support spécifique, les éventuels correspondants ne sont pas informés de ce changement et continuent à envoyer leurs données à l'ancienne adresse du terminal qui est devenue obsolète. Dès lors, le terminal est obligé de réinitialiser toutes ses communications.

Pour palier ces problèmes, deux protocoles de gestion de la mobilité dans les réseaux IPv6 sont en cours de standardisation au sein de l'organisme IETF. Le protocole *Mobile IP* permet le déplacement de terminaux mobiles en chargeant chaque terminal de la gestion de sa propre mobilité. De son côté, le protocole *NEMO (Network Mobility) Basic Support* [25] place la gestion de la mobilité au niveau des routeurs, ce qui permet le mouvement de réseaux entiers tout en conservant la complexité de la gestion des déplacements dans l'Internet sur ces dits routeurs. Alors que le protocole NEMO Basic Support a été spécialement défini pour les réseaux IPv6, deux versions du protocole Mobile IP coexistent. L'une est spécialement définie pour les réseaux IPv4 (MIPv4 [28]) alors que l'autre est adaptée aux réseaux IPv6 (MIPv6 [46]). Etant donné que nous nous sommes focalisés sur l'Internet Nouvelle Génération, nous allons nous intéresser plus particulièrement à la version MIPv6.

2.4.1 Le protocole Mobile IPv6

Le principe du protocole MIPv6 est d'utiliser un point relais en vue de rediriger les communications des terminaux mobiles vers leurs localisations courantes. Pour un terminal donné, le réseau Internet IPv6 est décomposé en deux catégories : le réseau mère et les réseaux visités. Le réseau mère d'un terminal constitue son réseau principal dans lequel il communique de la même façon qu'un terminal fixe à l'aide de son adresse mère (HoA). Ce cas est illustré sur la figure 2.3(a). Le point relais du terminal, appelé agent mère (HA), est également situé dans le réseau mère. Lorsque le terminal sort de son réseau mère et arrive dans un réseau visité, il obtient une seconde adresse IPv6. Cette nouvelle adresse est une adresse temporaire (CoA) qui identifie le terminal dans son nouveau réseau. Afin de maintenir ses communications, le terminal doit avertir son

agent mère au sujet de son déplacement en lui indiquant sa nouvelle adresse temporaire. Dès lors, l'agent mère intercepte tous les paquets destinés au terminal (paquets étant toujours envoyés vers l'adresse mère du terminal) et les redirige vers la position courante du terminal. Pour toutes ses émissions, le terminal passe également par l'agent mère de manière à rendre le déplacement transparent pour les correspondants. Dès lors, un tunnel bidirectionnel est établi entre le terminal et son agent mère (voir la figure 2.3(b)).



(a) Terminal dans son réseau mère

(b) Terminal dans un réseau visité

FIG. 2.3 – Le protocole Mobile IPv6

Pour réaliser ces opérations, l'agent mère maintient à jour un cache d'association entre l'adresse mère et l'adresse temporaire du terminal. Ce cache est mis à jour par les messages BU (*Binding Update*) / BACK (*Binding Acknowledgement*) échangés entre le terminal mobile et l'agent mère. Il est possible de sécuriser ces messages en utilisant le protocole IPsec [11]. La redirection des paquets IPv6 (aussi bien au niveau du terminal qu'au niveau de l'agent mère) utilise l'encapsulation d'en-tête permise par le protocole IPv6 dans laquelle les équipements n'ajoutent qu'un en-tête de routage supplémentaire au paquet IPv6 original (voir la figure 2.3(b)).

Les spécifications de base du protocole MIPv6 définissent également deux optimisations de routage (voir la figure 2.3(b)). La première alternative au tunnel bidirectionnel est le routage triangulaire. Dans ce mode, le terminal mobile peut envoyer directement ses paquets IPv6 aux correspondants (CN) sans passer par l'agent mère. Pour ce faire, le terminal utilise son adresse temporaire mais ajoute une option contenant son adresse mère. L'ajout de l'adresse mère permet aux correspondants d'identifier le terminal émetteur. Par contre, les paquets provenant des correspondants transitent toujours par l'agent mère (d'où le nom de routage triangulaire). Néanmoins, la deuxième optimisation lève cette dernière contrainte. Appelée *Routing Optimization*, elle permet aux correspon-

dants d'utiliser l'adresse temporaire du terminal mobile pour communiquer avec lui. De la même manière que l'agent mère, les correspondants qui supportent ce mode possèdent un cache d'association qui fait la correspondance entre adresse mère et adresse temporaire. Dès lors, le terminal mobile doit également leur notifier tout déplacement en utilisant les messages BU et BACK. Chaque mise à jour d'un correspondant est précédée d'une procédure de *Return Routability*. Cette procédure vise à empêcher que des utilisateurs malintentionnés n'envoient des mises à jour fictives aux correspondants en se faisant passer pour le terminal mobile. Dans cette procédure, le correspondant s'assure que c'est bien le même terminal qui est joignable à l'adresse mère et à l'adresse temporaire. Lorsque le cache d'un correspondant est à jour, il ajoute aux paquets destinés au terminal mobile un en-tête de routage particulier. Cet en-tête de routage contient l'adresse mère du terminal mobile de façon à indiquer la destination finale du paquet. Bien que cette technique de routage évite les redirections de paquets, elle nécessite une gestion particulière au niveau des correspondants et ne peut donc pas être utilisée sur des terminaux qui ne sont pas compatibles. Par la suite, nous allons nous baser uniquement sur la méthode du tunnel bidirectionnel.

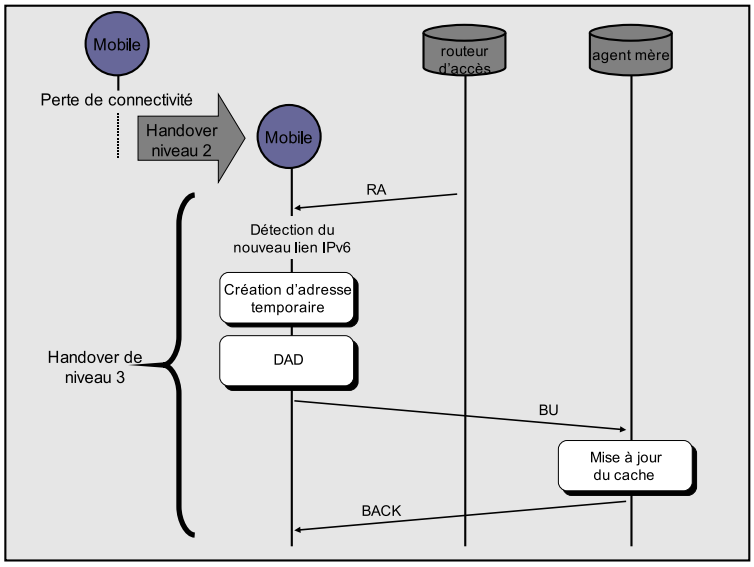


FIG. 2.4 – Gestion des handovers de niveau 3 par le protocole MIPv6

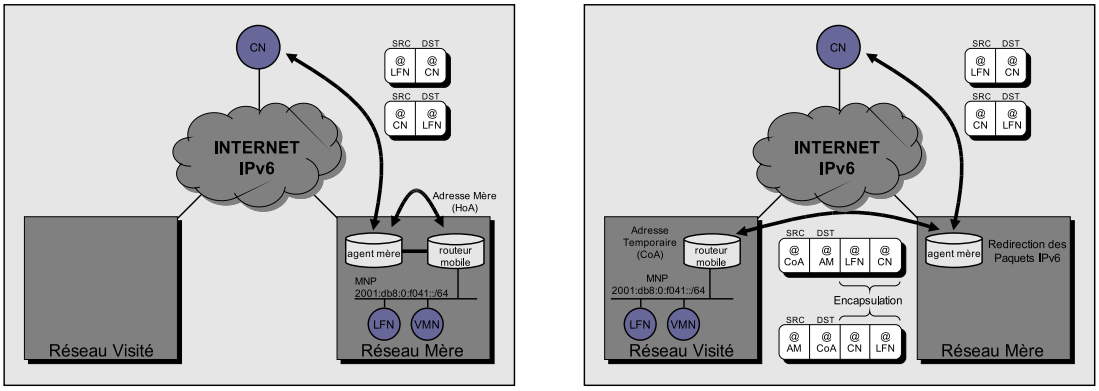
Les mécanismes mis en place par le protocole MIPv6 entre l'arrivée d'un terminal dans un réseau visité et l'établissement du tunnel bidirectionnel sont référencés par les termes *handover de niveau 3*. Dès la fin d'un handover de niveau 2, le terminal doit déterminer si son nouveau point d'attachement se situe dans un nouveau sous-réseau. Cette détection est généralement basée sur la réception d'un message RA (*Router Advertisement*). Ces messages sont envoyés périodiquement par les routeurs d'accès du

lien et sont utilisés lors de l'autoconfiguration d'adresse sans état [101] et dans le protocole de découverte des voisins [72]. A la réception d'un tel message, le terminal détecte qu'il s'est déplacé et peut configurer sa nouvelle adresse temporaire. Après avoir vérifié que cette adresse est unique, le terminal peut envoyer un BU pour mettre à jour le cache de son agent mère. Lorsque la mise à jour est effectuée, l'agent mère envoie un BACK au terminal signifiant la fin du handover de niveau 3. La figure 2.4 illustre ces différentes procédures.

2.4.2 Le protocole NEMO Basic Support

Les mécanismes introduits par le protocole NEMO Basic Support reprennent principalement ceux mis en place par le protocole MIPv6. La différence majeure provient de la migration de la gestion de la mobilité au sein des routeurs, désormais appelés routeurs mobiles. Cela permet la mobilité de réseaux entiers, tout en rendant ces déplacements transparents aux équipements situés derrière le routeur mobile. Dès lors, de tels équipements doivent uniquement supporter le protocole IPv6. On peut cependant distinguer derrière un routeur mobile trois types d'équipements différents. Les LFN (*Local Fixed Node*) sont des terminaux ou des routeurs qui appartiennent au réseau mobile mais qui ne sont pas capables de changer de point d'attachement sans interrompre leurs communications (pas de support du protocole MIPv6 ou du protocole NEMO Basic Support). Par contre, les VMN (*Visited Mobile Node*) sont des équipements mobiles (terminal ou routeur) qui sont capables de se déplacer tout en maintenant leurs communications. De tels équipements supportent donc soit le protocole MIPv6 (dans le cas d'un terminal), soit le protocole NEMO Basic Support (dans le cas d'un routeur). Pour eux, le réseau mobile ne constitue qu'un réseau visité qu'ils utilisent de manière temporaire. Enfin, les LMN (*Local Mobile Node*) sont similaires aux VMN à la seule différence que leur réseau mère appartient au réseau mobile alors que ce n'est pas le cas pour les VMN.

Le protocole NEMO Basic Support reprend entièrement l'architecture du protocole MIPv6 en y ajoutant le concept des préfixes MNP (*Mobile Network Prefix*). A l'instar du protocole MIPv6, un routeur mobile va posséder deux adresses et établir un tunnel bidirectionnel entre sa localisation courante et son agent mère. En raison de sa fonction de routeur, il annonce un préfixe IPv6 aux équipements localisés derrière lui à l'aide des messages RA. Ce préfixe est appelé préfixe MNP et reste identique tant que le routeur mobile maintient son association avec l'agent mère. Les paquets IPv6 envoyés vers un préfixe MNP sont automatiquement acheminés jusqu'à l'agent mère par les mécanismes de routage traditionnels des réseaux IPv6. L'agent mère joue alors également le rôle de routeur et transmet de tels paquets soit directement au routeur mobile lorsque ce dernier se situe dans le réseau mère, soit à travers le tunnel bidirectionnel (voir la figure 2.5).



(a) Routeur mobile dans son réseau mère

(b) Routeur mobile dans un réseau visité

FIG. 2.5 – Le protocole NEMO Basic Support

Dans le cadre de cette thèse, nous avons initié l'évaluation de ce protocole en tirant parti du déploiement d'un réseau Wi-Fi IPv6 au sein de l'université Louis Pasteur de Strasbourg [60].

2.5 Limitations des standards

Nous venons de détailler les protocoles standard qui permettent aux terminaux mobiles de se déplacer tout en communiquant à travers des réseaux Wi-Fi IPv6. Cependant, lorsqu'un terminal est en procédure de handover, il est dans l'incapacité de recevoir ou d'émettre des données. En fonction des applications utilisées, ces coupures peuvent être plus ou moins perceptibles par les utilisateurs. En raison de la démocratisation de la technologie 802.11 et de l'augmentation des débits de cette technologie, les communications dites *temps réel* sont de plus en plus véhiculées par des réseaux sans fil IPv6. Ce type de communication regroupe les applications qui sont soumises à des contraintes de temps dans la réception ou l'émission des données. Les plus répandues sont les applications de type voix sur IP ou vidéo à la demande. Pour que de telles communications ne soient pas perturbées, il est généralement admis que le temps de latence engendré par un handover (de niveau 2 ou de niveau 2 et 3) ne dépasse pas 50 millisecondes.

2.5.1 Temps de latence au niveau 2

Les études réalisées ces dernières années sur les réseaux 802.11 montrent que les handovers de niveau 2, tels qu'ils sont décrits dans la norme, ne permettent pas de satisfaire les contraintes des communications temps réel [58, 103, 104]. En effet, le temps de latence généré dépasse généralement le seuil de 50 millisecondes cité ci-dessus. En occupant 90% du temps d'un handover, c'est la phase de découverte qui constitue la cause principale du temps de latence introduit dans les communications [58]. En fonction de la répartition des canaux radio sur les points d'accès, un terminal peut être amené à sonder de nombreux canaux avant de découvrir un nouveau point d'accès. Dès lors, les canaux non utilisés vont être sondés en vain pendant *MinChannelTime* chacun et le terminal va attendre *MaxChannelTime* sur ceux utilisés. Suivant les valeurs numériques des paramètres *MinChannelTime* et *MaxChannelTime*, le terminal peut largement passer plus d'une seconde pour sonder les 14 canaux disponibles.

Dans la pratique, nous avons toutefois pu constater qu'en plus des valeurs numériques des paramètres *MinChannelTime* et *MaxChannelTime*, les algorithmes de recherche peuvent également varier en fonction des équipements utilisés. En effet, la norme ne définit pas l'ordre dans lequel les canaux doivent être sondés ni le nombre de canaux à sonder. Dès lors, certains équipements sondent systématiquement tous les canaux radio alors que d'autres débutent directement à la phase d'authentification après avoir passé *MaxChannelTime* sur un canal (signifiant qu'ils ont détecté des points d'accès sur ce canal). Même dans ce dernier cas, les handovers de niveau 2 peuvent rester perceptibles par l'utilisateur. Le temps de latence engendré par un handover de niveau 2 est approximativement compris entre 50 et 400 millisecondes lors de l'utilisation de cartes sans fil relativement récentes [58, 103, 104].

2.5.2 Temps de latence au niveau 3

Comme nous l'avons vu, les terminaux mobiles peuvent également réaliser un handover de niveau 3 à la suite d'un handover de niveau 2. Le temps de déconnexion total peut donc encore être aggravé par les mécanismes du protocole MIPv6 [67, 68]. Trois facteurs sont principalement mis en cause : la détection du nouveau lien IPv6, la vérification de l'unicité de la nouvelle adresse temporaire et la mise à jour de cette adresse auprès de l'agent mère. La détection du déplacement de niveau 3 est réalisée lors de la réception d'un message RA (i.e. *Router Advertisement*). Le temps nécessaire à la détection dépend donc de la fréquence à laquelle ces messages sont envoyés par les routeurs d'accès. La fréquence d'envoi par défaut de ces messages est comprise entre 200 et 600 secondes [72], ce qui n'est pas adapté à une gestion rapide de la mobilité. Le protocole

MIPv6 suggère d'augmenter cette fréquence entre 30 et 70 millisecondes mais précise que ces valeurs ne doivent pas être utilisées par défaut. Avec une telle fréquence, il faut donc en moyenne 50 millisecondes pour détecter le nouveau lien IPv6 et par conséquent obtenir sa nouvelle adresse temporaire.

Lorsqu'un terminal acquiert une nouvelle adresse IPv6 (de manière automatique ou manuelle), il doit vérifier au préalable que cette adresse est unique sur le lien avant de pouvoir l'utiliser. Pour ce faire, le terminal mobile réalise une procédure appelée DAD (*Duplicate Address Detection* [101]) qui tire parti du protocole de découverte des voisins disponible dans IPv6 [72]. Dans la pratique, cette procédure ajoute un délai supplémentaire au temps total de déconnexion de niveau 3 étant donné qu'elle retarde l'émission du BU vers l'agent mère. Dès la configuration d'une nouvelle adresse IPv6, le terminal mobile doit attendre entre 0 et 1 seconde avant d'envoyer sa première requête de vérification qui consiste en un message NS (*Neighbor Solicitation*) [72, 101]. Par défaut lors du DAD, un terminal émet un unique NS. Si au bout d'une seconde il n'a pas reçu de NA (*Neighbor Advertisement*) lui indiquant que sa nouvelle adresse est déjà attribuée, il conclut qu'elle est unique sur le lien et peut désormais l'utiliser pour communiquer. Dans le meilleur des cas, le DAD introduit donc un délai supplémentaire d'une seconde.

Néanmoins, une nouvelle solution appelée ODAD (*Optimistic Duplicate Address Detection* [70]) vise à supprimer les délais engendrés par le DAD. Cette proposition se base sur le fait que les adresses IPv6 ont de très faibles chances (approximativement $1/10^6$ [70]) d'être dupliquées lorsqu'elles ont été obtenues par des mécanismes automatiques tels que l'autoconfiguration d'adresses sans état du protocole IPv6 [101]. Le principe de ODAD est donc d'autoriser les terminaux à utiliser directement leurs nouvelles adresses IPv6 tout en réalisant le DAD en parallèle. Appliqué au protocole MIPv6, cela permet aux terminaux mobiles d'envoyer une demande d'enregistrement à l'agent mère dès la création des nouvelles adresses temporaires.

Enfin, le délai d'acheminement des paquets entre l'agent mère et la localisation courante du terminal peut également contribuer à l'augmentation du temps total de déconnexion. Suite au déplacement d'un terminal mobile dans un nouveau sous-réseau, l'agent mère continue d'envoyer les paquets de données vers l'ancienne localisation du terminal tant qu'il n'a pas reçu de nouvelles notifications. Le terminal s'étant déplacé, ces paquets sont donc définitivement perdus. Dès la fin de la configuration de la nouvelle adresse (si l'on considère l'utilisation de ODAD), le délai de réception des paquets de données sur le nouveau lien IPv6 dépend donc directement du délai d'acheminement des paquets entre l'agent mère et le terminal (et vice versa). Plus ils sont éloignés en termes de distance réseau, plus la mise à jour de l'adresse temporaire va être longue.

A la vue des performances de la norme 802.11 et du protocole MIPv6, de nombreuses solutions ont été proposées afin de réduire le temps de déconnexion engendré par les handovers. Dans la prochaine section, nous allons détailler les solutions les plus populaires ou qui nous ont paru les plus pertinentes.

2.6 Optimisation des handovers

Parmi les différentes optimisations proposées dans la littérature, on distingue principalement celles qui se focalisent sur les handovers de niveau 2 dans les réseaux 802.11 et celles qui s'intéressent plus particulièrement au niveau 3 et donc au protocole MIPv6. On peut cependant relever que certaines propositions fournissent des solutions complètes, traitant à la fois le niveau 2 et le niveau 3.

2.6.1 Solutions à vocation de standardisation

Parmi les solutions proposées dans la littérature, certaines sont en cours de standardisation à l'IETF. Ces propositions se focalisent essentiellement sur l'optimisation des handovers de niveau 3.

Mobile IPv6 hiérarchique

La mise en place d'une architecture hiérarchique vise à réduire considérablement le temps d'enregistrement des adresses temporaires. Le réseau global est ici découpé en différents domaines qui sont indépendants des sous-réseaux IP et dont la taille est définie par l'opérateur ou l'entité administrative en charge du réseau. Différents modèles hiérarchiques sont disponibles dans la littérature, mais c'est le protocole Mobile IPv6 hiérarchique (HMIPv6 [95]), soutenu par l'IETF, qui semble être sur la voie de la standardisation. Ce dernier constitue une extension au protocole MIPv6 classique.

Dans le protocole HMIPv6, une nouvelle entité appelée MAP (*Mobility Anchor Point*) apparaît dans chaque domaine. Le MAP va essentiellement jouer le rôle d'agent mère local, permettant ainsi de masquer certains mouvements des terminaux au niveau de l'agent mère de façon à minimiser le trafic entre les agents mères et les terminaux mobiles. Lors de déplacements internes à un domaine, le protocole HMIPv6 permet également d'offrir des délais d'enregistrement d'adresses plus courts. La figure 2.6 illustre les procédures introduites par le protocole HMIPv6.

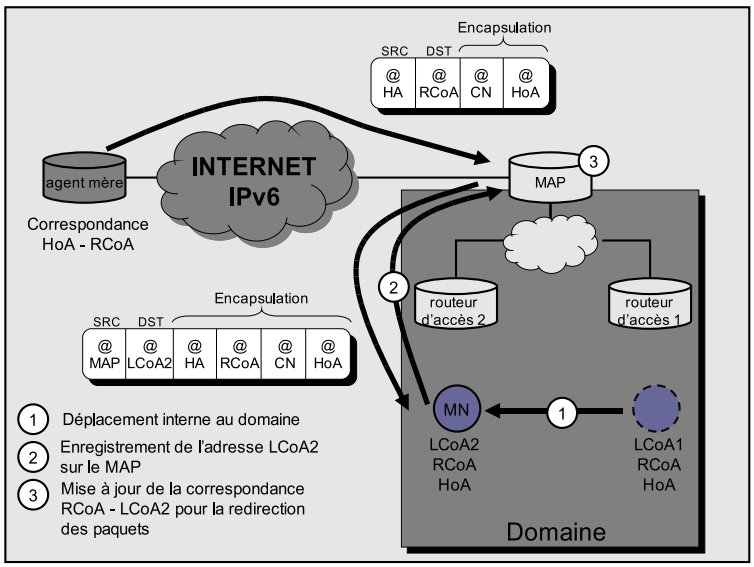


FIG. 2.6 – Le protocole HMIPv6

Lorsqu'un terminal mobile arrive dans un nouveau domaine, il obtient l'adresse du MAP (ou des MAPs) de ce domaine à l'aide d'une nouvelle option présente dans les messages RA. Cette nouvelle option permet également au terminal mobile de se configurer une adresse temporaire valide dans le même sous-réseau que celui du MAP. Une telle adresse est appelée RCoA (*Regional Care-of Address*) et va être conservée par le terminal tant qu'il ne sort pas du domaine. Par ailleurs, nous avons vu précédemment qu'à la réception d'un RA, le terminal mobile est capable de configurer une adresse temporaire qui l'identifie dans son sous-réseau actuel. Dans HMIPv6, une telle adresse est appelée LCoA (*on-Link Care-of Address*). Dès l'obtention de ces deux adresses, le terminal envoie un premier BU au MAP en vue d'y créer une nouvelle correspondance entre son adresse RCoA et son adresse LCoA. Un tunnel bidirectionnel similaire à celui du protocole MIPv6 est donc établi entre le MAP et la localisation courante du terminal. Dans le même temps, le terminal communique son adresse RCoA à son agent mère à l'aide d'un deuxième BU. Lorsque l'agent mère reçoit ce BU, il met à jour sa table de correspondance et envoie vers l'adresse RCoA les nouveaux paquets de données destinés au terminal. Ces derniers sont interceptés par le MAP qui les retransmet à la localisation actuelle du terminal dans le domaine grâce au tunnel bidirectionnel établi au préalable (voir la figure 2.6).

Lors d'un changement de sous-réseau à l'intérieur du domaine, le terminal obtient une nouvelle LCoA qu'il enregistre auprès du MAP. Etant donné que sa RCoA reste inchangée, de tels déplacements sont donc complètement transparents au niveau de l'agent mère (voir la figure 2.6). Par conséquent, le temps de mise à jour des adresses tempo-

raires est considérablement réduit car le MAP et le terminal se situent dans le même domaine. En revanche, lors d'un changement de domaine, le terminal obtient une nouvelle adresse RCoA et doit donc effectuer un nouvel enregistrement auprès de son agent mère. Le changement de domaine est détecté grâce à la nouvelle option incluse dans les RA que nous avons présentée précédemment.

Le protocole FMIPv6

Le protocole Fast Handovers for Mobile IPv6 (FMIPv6 [29]) est une amélioration du protocole MIPv6 et figure parmi les solutions les plus prometteuses. Sa vocation est de réduire au maximum le temps de déconnexion de niveau 3 tout en limitant la perte de paquets de données. L'idée principale de ce protocole repose sur la détermination a priori du futur lien IPv6 des terminaux mobiles.

Le protocole FMIPv6 définit de nouveaux mécanismes grâce auxquels les terminaux mobiles sont en mesure de demander à leurs routeurs d'accès courants les paramètres de niveau 3 des liens IPv6 sur lesquels se situent les points d'accès environnants. De telles requêtes sont réalisées à l'aide des messages RtSolPr (*Router Solicitation for Proxy*) et PrRtAdv (*Proxy Router Advertisement*). Les messages RtSolPr sont envoyés aux routeurs d'accès courants par les terminaux mobiles. Ils peuvent contenir l'identifiant d'un ou de plusieurs points d'accès (obtenus par exemple à l'aide d'une procédure de scan) pour lesquels un terminal désire obtenir les paramètres de niveau 3 qui leur sont relatifs. Un terminal peut également demander la liste de tous les couples point d'accès / routeur d'accès de la zone environnante. A la réception d'un message RtSolPr, le routeur d'accès courant répond par un message PrRtAdv contenant les informations demandées. Ces dernières sont représentées sous la forme de couples points d'accès / routeur d'accès et comportent, pour chaque couple, l'adresse MAC du point d'accès, l'adresse MAC du routeur d'accès, le préfixe IPv6 annoncé par le routeur d'accès et la longueur de ce préfixe. Par la suite, la procédure effective de handover peut se dérouler selon deux cas de figure.

Dans le mode prédictif, les terminaux mobiles sont capables d'anticiper la nécessité d'effectuer un handover (en utilisant par exemple des informations de niveau 2 telles que la qualité du signal radio). Lorsqu'un terminal réalise une telle anticipation, il envoie un message FBU (*Fast Binding Update*) à son routeur d'accès courant (référencé dans la suite par le terme PAR pour *Previous Access Router*). Ce message contient l'adresse temporaire courante du terminal mobile (PCoA) ainsi que l'identifiant du routeur d'accès vers qui le terminal désire se déplacer (référencé dans la suite par le terme NAR pour *Next Access Router*). Dès la réception de ce message, le PAR envoie au NAR un message HI (*Handover Initiate*) contenant diverses informations sur le terminal : adresse

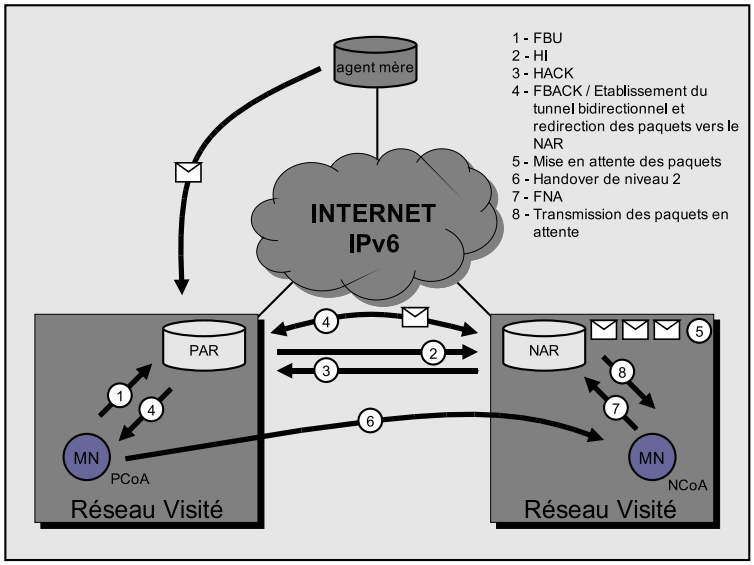


FIG. 2.7 – Mode prédictif du protocole FMIPv6

MAC, PCoA et éventuellement la future adresse du terminal au sein du sous-réseau du NAR (NCoA). Ce message est utilisé pour prévenir le NAR des intentions du terminal mobile en vue de s'assurer au préalable que le handover est réalisable. Le NAR peut donc accepter ou refuser le handover à l'aide d'un message HACK (*Handover Acknowledge*). Dès la réception du HACK, le PAR envoie au terminal un message FBACK (*Fast Binding Acknowledgement*). A la fin de ces différents échanges de messages, le terminal est fin prêt à effectuer un handover. Dans le même temps, le PAR et le NAR établissent un tunnel bidirectionnel. Tous les paquets de données destinés au terminal mobile sont interceptés par le PAR et transmis au NAR à travers le tunnel. A la réception de ces paquets, le NAR les stocke dans un tampon afin de les retransmettre au terminal à la fin du handover. Dès son arrivée sur le nouveau lien correspondant au NAR, le terminal envoie un message FNA (*Fast Neighbor Advertisement*) qui est censé mettre à jour la table de correspondance du NAR de façon à initier la transmission des éventuels paquets de données qui ont été mis en attente. Ce dernier message termine ainsi la signalisation du protocole FMIPv6. La redirection des paquets entre le PAR et le NAR est généralement maintenue suffisamment longtemps pour que le terminal puisse enregistrer sa nouvelle adresse temporaire (NCoA) auprès de son agent mère sans perte de paquets. Tant que ce tunnel est actif, le terminal est également capable d'envoyer des paquets de données à l'aide de son ancienne adresse temporaire (PCoA). Le mode prédictif est illustré sur la figure 2.7.

Le protocole FMIPv6 définit également un mode réactif, qui représente les cas où les terminaux mobiles sont incapables d'anticiper leurs déplacements. De ce fait, la

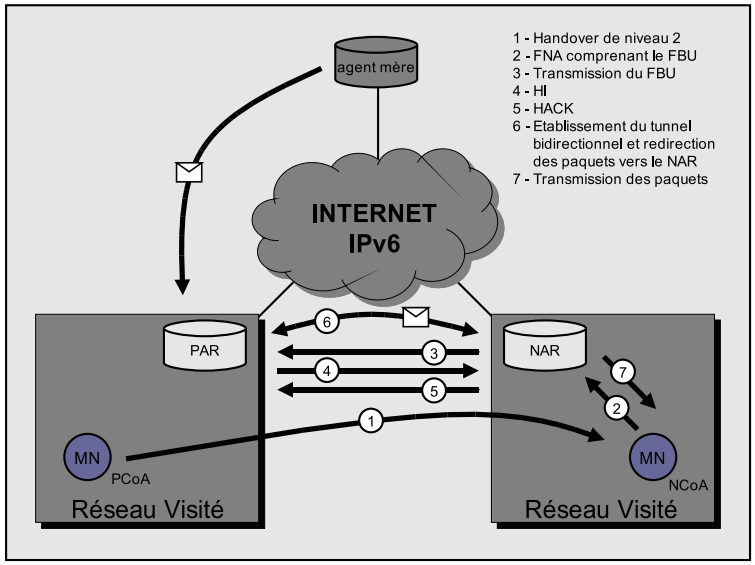


FIG. 2.8 – Mode réactif du protocole FMIPv6

signalisation FMIPv6 prend place uniquement après le handover de niveau 2. Dans ces cas particuliers, le FBU est envoyé depuis le sous-réseau du NAR et encapsulé dans le FNA. A sa réception, le NAR transmet le FBU au PAR. Puis, l'échange des messages HI / HACK se déroule de la même manière que dans le mode prédictif, ce qui permet au PAR de transmettre les paquets de données vers le NAR à travers le tunnel. Le mode réactif est illustré sur la figure 2.8.

Bi-casting

Le protocole FMIPv6 peut être étendu grâce à l'utilisation de la méthode de bi-casting ou n-casting [56]. Le principe est de dupliquer le trafic destiné à un terminal mobile pendant une courte période dans le but de transmettre les paquets de données vers sa localisation courante, mais également vers une ou plusieurs autres localisations pour lesquelles le terminal est susceptible de se déplacer. Par conséquent, le nombre de paquets perdus lors d'un handover est réduit et l'ambiguïté sur le temps optimal pour initier la transmission des paquets entre le PAR et le NAR dans le protocole FMIPv6 est levée. De plus, le bi-casting est une bonne solution contre l'effet *ping pong* (allers et venues entre deux sous-réseaux). La méthode du bi-casting peut également être utilisée dans le cas du protocole MIPv6 classique ou du protocole HMIPv6. Les procédures étant quasiment identiques dans ces différents cas (seul l'agent de redirection diffère entre

routeur d'accès, agent mère et MAP), nous allons nous intéresser plus particulièrement au cas du protocole MIPv6 classique pour plus de clarté.

Pour utiliser le bi-casting, un terminal doit être capable de gérer plusieurs adresses temporaires simultanément. D'un autre côté, l'agent mère doit être en mesure d'associer plusieurs adresses à un même terminal. Cela se traduit par des associations multiples dans le cache d'association de l'agent mère. La méthode du bi-casting ne nécessite aucun nouveau message, toutes les requêtes et réponses liées à cette méthode sont ajoutées dans les messages existants du protocole MIPv6.

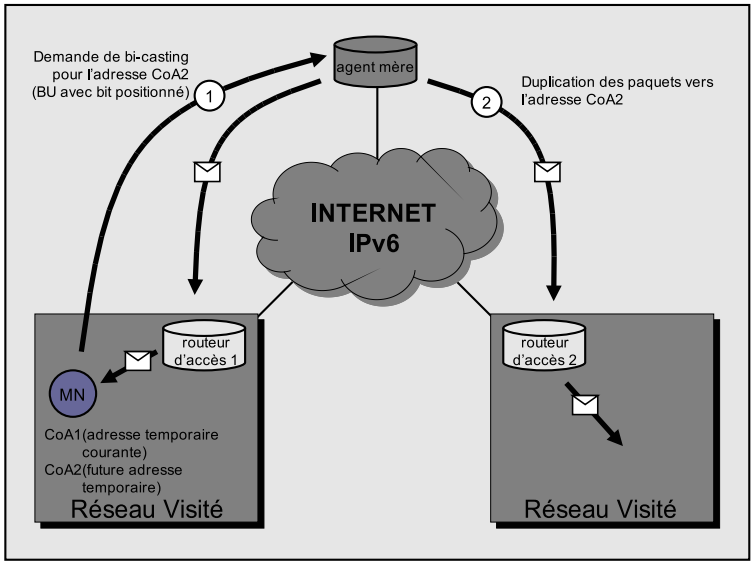


FIG. 2.9 – Bi-casting

Lorsque le terminal désire réaliser une procédure de bi-casting (e.g. lorsqu'un handover est imminent) il lui suffit d'envoyer un BU à son agent mère contenant la nouvelle adresse CoA qu'il désire utiliser en plus de sa précédente. Pour indiquer à l'agent mère qu'il s'agit d'une adresse temporaire supplémentaire et qu'il ne doit pas écraser son association courante, le terminal positionne un bit particulier dans le BU. A la réception d'un tel message, l'agent mère ajoute une nouvelle entrée dans le cache d'association et initie la transmissions des paquets de données vers toutes les adresses temporaires présentes dans le cache d'association pour ce terminal. Lors de la présence de correspondants supportant le protocole MIPv6, le terminal peut également leur envoyer de tels BU. Si ces derniers ne supportent pas les associations multiples, ils ignoreront tout simplement l'option. Les associations multiples sont actives au niveau de l'agent mère (et des éventuels correspondants) pendant une durée indiquée dans le BU qui réalise la demande de bi-casting. Lorsque la durée de validité du bi-casting expire, l'agent mère retire de son cache d'association les champs correspondants et remplace l'ancienne as-

sociation de l'ancienne CoA du terminal par la nouvelle. La figure 2.9 illustre la méthode du bi-casting.

Le bi-casting au niveau de l'agent mère du terminal n'est cependant pas réellement envisageable à grande échelle. En effet, l'ensemble du trafic pour le terminal mobile est dupliqué sur tout le chemin allant de l'agent mère au terminal alors que les paquets de données prennent généralement le même chemin mis à part dans les quelques derniers sauts, ce qui génère un surplus de trafic dans le réseau. Le bi-casting est donc plus sérieusement envisagé dans le cas des protocoles FMIPv6 et HMIPv6 dans lesquels le trafic ne serait dupliqué qu'au niveau du PAR ou du MAP.

2.6.2 Utilisation de multiples interfaces

Certaines solutions visant à réduire le temps de latence des handovers reposent sur l'utilisation de plusieurs interfaces Wi-Fi. Dans [80], les auteurs proposent d'équiper les terminaux mobiles d'une seconde interface afin de réaliser des handovers rapides. A un instant donné, l'une des deux interfaces est associée à un point d'accès et utilisée pour communiquer normalement. Tant que la qualité du signal entre cette interface et le point d'accès est suffisante, la seconde interface est en mode veille. Lorsque le terminal s'éloigne du point d'accès, la qualité du signal décroît. De ce fait, le terminal active sa seconde interface et l'utilise pour rechercher un nouveau point d'accès en vue de s'y associer. Dès l'obtention d'une nouvelle adresse sur la seconde interface, le terminal peut envoyer un BU à son agent mère lui indiquant d'envoyer simultanément les paquets de données vers ses deux interfaces. C'est la méthode du bi-casting que nous avons présentée précédemment. Lorsque le terminal n'a plus l'utilité de sa première interface, il la passe en mode veille et interrompt la procédure de bi-casting. Cette technique permet de réaliser des handovers complètement transparents pour l'utilisateur, étant donné que le terminal est continuellement associé à un point d'accès. Grâce à cette interface supplémentaire, le terminal peut donc réaliser toutes les procédures définies dans la norme 802.11 et dans le protocole MIPv6 sans perturber ses communications.

Etant donné que les terminaux mobiles sont généralement des équipements ayant de fortes contraintes énergétiques, l'ajout d'une seconde interface peut avoir un impact sur la consommation globale de tels équipements. Une alternative envisageable consiste à ajouter cette seconde interface sur les points d'accès [78]. A l'aide de cette deuxième interface, les points d'accès peuvent détecter les terminaux qui sont proches en interceptant les trames échangées dans les cellules voisines. Il est notamment possible d'identifier un terminal mobile et son point d'accès courant grâce aux adresses MAC visibles dans les en-têtes des trames 802.11. Lorsqu'un point d'accès *entend* un terminal mobile, il lui transmet diverses informations de niveau 2 le concernant. Il com-

munique également l'intensité du signal avec laquelle il a *entendu* le terminal. Toutes ces notifications sont compilées par le point d'accès courant du terminal afin de fournir une liste unique de cibles potentielles pour un prochain handover. Dès la réception de cette liste, le terminal peut sélectionner son prochain point d'accès avant d'initier une procédure de handover. Par conséquent, il peut éviter la phase de découverte et directement s'associer au point d'accès choisi. Le temps total de déconnexion engendré par un handover de niveau 2 est donc fortement réduit. Cependant, la solution présentée ici ne propose aucune optimisation de niveau 3.

2.6.3 Gestion d'historique et masque de canaux radio

D'autres approches proposent de tirer parti d'un historique des déplacements dans le but d'optimiser les handovers de niveau 2. L'une des plus aboutie est appelée *Selective Scanning and Caching* [90]. Cette solution se décompose en deux étapes. Dans un premier temps, les terminaux mobiles construisent un masque de canaux radio qui indique les canaux à sonder en priorité lors d'un handover. Au fur et à mesure de leurs déplacements, les terminaux construisent également un historique des points d'accès avec lesquels ils se sont associés. Lors d'un handover, ils pourront éventuellement utiliser les informations enregistrées dans l'historique pour éviter la réalisation d'une phase de découverte. Comme nous l'avons vu précédemment, cette étape constitue la cause principale du temps de latence engendré par les handovers de niveau 2. Même si l'historique ne contient aucune information pertinente pour un handover particulier, l'utilisation du masque de canaux permet tout de même de limiter la durée de la phase de découverte.

Lorsqu'un terminal allume son interface 802.11, il effectue une procédure de scan actif sur les 14 canaux 802.11 afin de créer son masque de canaux radio. Pour chaque *Probe Response* reçue sur un canal, il enregistre ce canal dans le masque (voir la figure 2.10). Par défaut, les canaux 1, 6 et 11 sont également ajoutés dans le masque étant donné qu'ils sont généralement préférés aux autres canaux radio car ils n'interfèrent pas et sont utilisables dans la majorité des pays malgré différentes restrictions de bande passante. Dès la fin de la construction du masque, le terminal s'associe à un point d'accès et supprime le canal radio correspondant du masque en raison de la faible probabilité que deux points d'accès adjacents d'un même opérateur utilisent le même canal radio. Lors d'un handover, le terminal ne sonde que les canaux positionnés dans le masque. Si le terminal n'a reçu aucune réponse, il inverse son masque et recommence une nouvelle procédure de scan. Si le terminal n'a toujours pas de réponse, il réalise un scan complet de tous les canaux de manière à créer un nouveau masque. Cette procédure est appelée *Selective Scanning* et limite la durée des handovers de niveau 2 à 130 millisecondes environ [90].

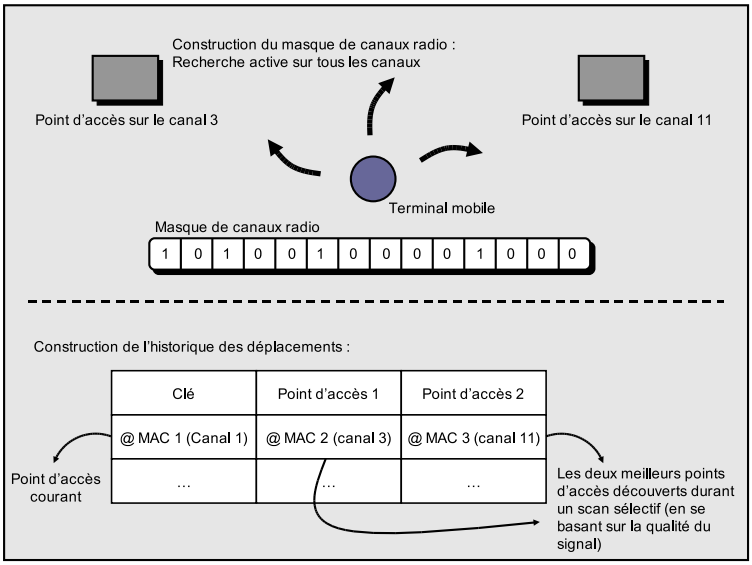


FIG. 2.10 – Construction du masque de canaux et de l'historique

D'autre part, les terminaux sont également amenés à construire un historique de leurs déplacements. Lorsqu'un terminal s'associe à un point d'accès, il crée une nouvelle entrée dans son historique et enregistre l'adresse MAC et le canal radio qui correspondent à ce point d'accès. Pour chaque entrée de l'historique, le terminal ajoute également les paramètres (adresse MAC et canal radio) de deux points d'accès adjacents (voir la figure 2.10). Ces informations sont obtenues lors d'un *Selective Scanning* ou complétées lors des handovers. Lorsque le terminal désire effectuer un handover, il cherche dans son historique les paramètres des points d'accès adjacents à son point d'accès courant. Si ces champs ne sont pas encore renseignés, il réalise une procédure de *Selective Scanning*. Dans le cas contraire, il essaie de s'authentifier au premier point d'accès de l'historique. Si l'authentification réussit, le terminal passe à la phase d'association. En revanche, si l'authentification échoue (le terminal n'est pas autorisé à utiliser ce point d'accès ou le point d'accès n'est pas à portée radio), il essaie de s'authentifier auprès du second point d'accès de l'historique. Lorsque cette authentification échoue également, le terminal effectue une procédure de *Selective Scanning*.

L'utilisation conjointe de l'historique et du *Selective Scanning* permet de réduire le temps de latence engendré par un handover de niveau 2 à 3 millisecondes dans les meilleurs cas [90].

2.6.4 Synchronisation de Beacons

Une nouvelle approche appelée *SyncScan* propose de réaliser des handovers rapides en se basant sur un système de synchronisation des trames de contrôle [88]. Cette méthode offre aux terminaux mobiles la possibilité d'écouter périodiquement les différentes trames *Beacon* émises par les points d'accès environnants afin d'obtenir a priori la liste des points d'accès voisins. Elle abolit notamment la réalisation de scan actif et par conséquent réduit la procédure de handover de niveau 2 aux seules phases d'authentification et d'association. De plus, une telle approche permet une gestion plus fine du déclenchement des handovers car les terminaux mobiles surveillent constamment la qualité du signal provenant de multiples points d'accès. Un terminal est donc en mesure d'anticiper ou de différer la réalisation d'un handover en fonction des différentes intensités des signaux qui proviennent des points d'accès voisins.

Les horloges des poins d'accès sont ici synchronisées à l'aide du protocole de synchronisation d'horloge NTP (*Network Time Protocol* [57]). A l'instant t, tous les points d'accès opérant sur le canal 1 vont émettre un *Beacon*. A l'instant $t + d$ millisecondes, c'est au tour des points d'accès positionnés sur le canal 2 d'émettre un *Beacon* et ainsi de suite. De cette manière, un terminal mobile associé à un point d'accès qui opère sur le canal c est en mesure de détecter les points d'accès voisins qui utilisent le canal $(c+1)$ en se positionnant sur ce canal d millisecondes après la réception d'un *Beacon* provenant de son point d'accès courant. Pour limiter les collisions sur les trames *Beacon* entre des points d'accès qui utilisent un même canal radio, le temps exact d'émission des trames *Beacon* pour un canal donné varie légèrement (e.g. $t + x, x \in [0; 3]$ millisecondes).

Périodiquement (e.g. toutes les 500 millisecondes), un terminal effectue une phase de recherche passive dans l'intention d'intercepter les trames *Beacon* émises par les points d'accès voisins. Chacune de ces phases est réalisée sur un canal différent. Pour ce faire, le terminal indique en premier lieu à son point d'accès courant qu'il désire passer en mode d'économie d'énergie. Ce mode active la mise en attente des paquets de données au niveau du point d'accès de sorte que le terminal peut éteindre son interface radio pendant de courtes durées (généralement un multiple de la fréquence d'émission des trames *Beacon*) en vue de limiter la dépense d'énergie. Dans le cas présent, cela permet au terminal de ne pas perdre de paquets alors qu'il s'apprête à changer de canal radio. Puis, il passe sur le prochain canal radio qu'il doit sonder. Ce changement de canal est réalisé de manière synchronisée avec l'émission des trames *Beacon* sur ce canal. Après 5 millisecondes, le terminal enregistre les paramètres des différents points d'accès découverts grâce à l'éventuelle réception de trames *Beacon*. Ensuite, il revient sur son canal initial et indique à son point d'accès courant qu'il est sorti du mode d'économie d'énergie. Grâce à de multiples recherches passives de la sorte, le terminal obtient a priori la liste des points d'accès environnants. Lors d'un handover de niveau 2, le ter-

minal peut donc directement débuter la procédure par la phase d'authentification, ce qui rend les handovers de niveau 2 transparents aux utilisateurs [88].

Dans la pratique, il n'est pas aisé de synchroniser de manière précise des équipements réseau et plus particulièrement des équipements sans fil en raison du support physique instable. D'autant plus que le changement de canal radio introduit un délai non négligeable au niveau du périphérique sans fil. Ce délai peut varier de 5 à 40 millisecondes suivant l'équipement [88]. Cela laisse relativement peu de marges d'erreurs à cette méthode qui demande alors une gestion appropriée à l'équipement sans fil utilisé.

2.6.5 Solution propriétaire

Le constructeur d'équipements réseau Cisco Systems propose une solution complète de gestion rapide et sécurisée des handovers de niveau 2 et 3 [96, 97, 98]. Bien que cette solution ait été prévue pour s'intégrer dans les réseaux IPv4, elle devrait être transposable aux réseaux IPv6 sans demander trop de modifications. Appelée système WDS (*Wireless Domain Service*), elle repose sur l'utilisation de protocoles propriétaires et demande des équipements réseau bien particuliers (voir la figure 2.11).

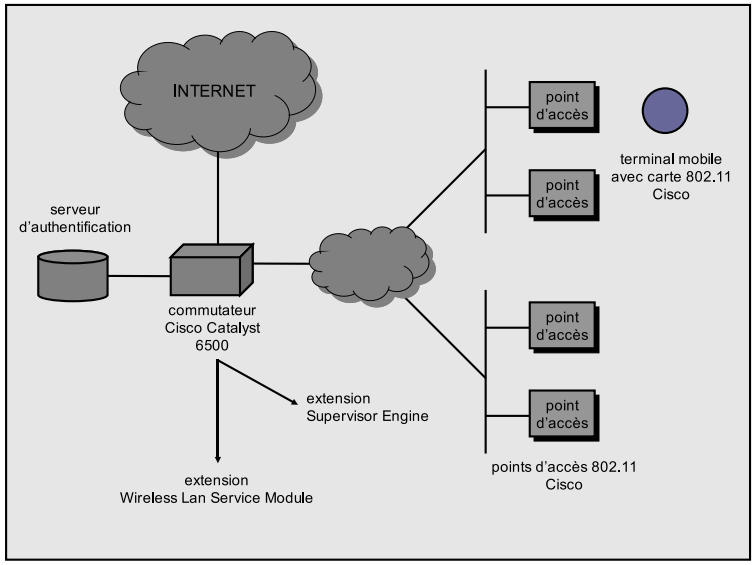


FIG. 2.11 – Acteurs du système WDS

Cette solution introduit un nouvel équipement réseau appelé le WDS. Ce dernier va permettre d'authentifier les points d'accès ainsi que les terminaux mobiles participants au système. Il est également en charge de la gestion des déplacements des terminaux

mobiles. Dans les sections suivantes, nous allons détailler les mécanismes mis en place par ce système pour permettre des handovers rapides. Nous présenterons également les mécanismes mis en place pour assurer la sécurité du réseau.

Gestion des handovers de niveau 2

La principale amélioration des handovers de niveau 2 du système WDS consiste à fournir aux terminaux mobiles la liste des points d'accès environnants de façon à optimiser la phase de recherche définie dans la norme IEEE 802.11. Chaque point d'accès du réseau construit de manière dynamique sa propre liste d'adjacence grâce à de nouvelles informations fournies par les terminaux mobiles lors des différentes associations. Ces informations correspondent essentiellement aux paramètres utilisés par leurs précédents points d'accès tels que le SSID et le canal radio. Afin de créer une liste d'adjacence pertinente, les terminaux mobiles indiquent également la durée depuis laquelle ils ont été déconnectés de leurs précédents points d'accès. Lorsque ce temps dépasse 10 secondes, les points d'accès en question ne sont pas considérés comme des voisins et par conséquent ne sont pas ajoutés à la liste d'adjacence. Le temps nécessaire à la construction d'une liste d'adjacence complète dépend donc directement du nombre de points d'accès environnants, du nombre de terminaux mobiles et de la fréquence à laquelle ces derniers passent d'un point d'accès à l'autre.

Lorsqu'un terminal mobile s'associe à un point d'accès, ce dernier lui transmet la liste d'adjacence actuellement en sa possession. Lors d'un handover de niveau 2, le terminal utilise cette liste de manière à ne sonder que les canaux utilisés par les points d'accès adjacents. Dès l'obtention d'une réponse d'un point d'accès de la liste, le terminal passe directement à la phase d'authentification. Cette procédure permet donc de réduire fortement le temps de latence engendré par un handover de niveau 2. Dans la pratique, l'utilisation de la liste d'adjacence dépend du trafic présent au niveau du terminal juste avant le déclenchement du handover. Lorsque ce dernier a reçu ou envoyé un paquet de données dans les 500 millisecondes précédant le handover, il utilise la liste comme nous venons de le décrire. Dans le cas contraire, le terminal n'a aucune communication critique en cours (e.g. temps réel), c'est pourquoi la réalisation d'un handover rapide est inutile. Dans ce cas, le terminal n'utilise pas la liste d'adjacence et effectue un handover classique.

Si on ne considère que les handovers de niveau 2, le système WDS nécessite l'utilisation de points d'accès et de carte cliente 802.11 de marque Cisco Systems. Dans une telle configuration, c'est l'un des points d'accès qui va jouer le rôle du WDS pour l'authentification des points d'accès et des terminaux.

Gestion des handovers de niveau 3

Dans le système WDS, le support de la mobilité de niveau 3 ne s'appuie pas sur le protocole Mobile IP mais utilise une approche relativement similaire. Un réseau logique de niveau 3 est mis en place au-dessus du réseau IP. Ce réseau logique va permettre aux terminaux mobiles de garder la même adresse IP indépendamment des réseaux IP sous-jacents traversés. Par conséquent, ce système fait abstraction des principes fondamentaux du protocole IP pour lesquels l'adresse IP d'un terminal correspond à sa localisation courante. Pour activer la gestion de la mobilité de niveau 3, il faut impérativement posséder le commutateur Cisco Catalyst 6500 muni des extensions WLSM (*Wireless Services Module*) et SE (*Supervisor Engine 720*). Dans ce cas, c'est obligatoirement le commutateur Cisco Catalyst qui tient le rôle de WDS (grâce au module WLSM).

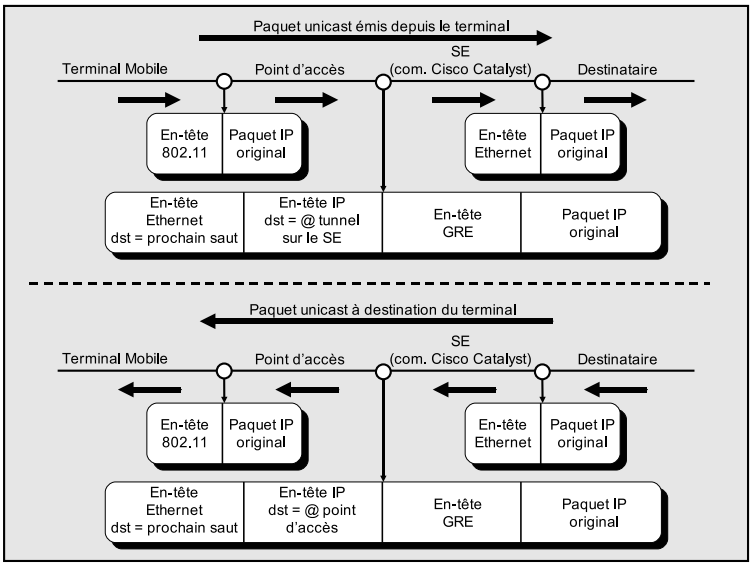


FIG. 2.12 – Utilisation du réseau logique pour la transmission des paquets de données unicast

La création du réseau logique fait essentiellement intervenir le SE et les points d'accès. Le SE tire parti d'une variante du mécanisme d'encapsulation générique (GRE [36]) appelée mGRE (*multipoint Generic Routing Encapsulation*). Ce mécanisme permet de créer de simples tunnels de communication entre une source unique et de multiples destinataires. La mise en place de divers tunnels utilisant l'encapsulation mGRE entre le SE et les points d'accès constitue le réseau logique de niveau 3. Tous les paquets de données IP envoyés en unicast utilisent le réseau logique ainsi formé pour atteindre leurs destinations. Le SE devient par conséquent le point central du réseau (voir la figure

2.12). En revanche, le trafic de contrôle (entre les points d'accès et le WDS) n'utilise pas le réseau logique mais un nouveau protocole appelé WLCCP (*Wireless LAN Context Protocol*). Ce dernier est en quelque sorte une version propriétaire du protocole LWAPP (*Light-Weight Access Point Protocol* [17]) qui est standardisé par l'IETF. Ces protocoles permettent principalement de centraliser la gestion et la configuration des points d'accès d'un réseau sans fil. Le SE maintient également à jour un cache de mobilité local dans lequel il enregistre l'adresse IP, l'adresse MAC et le point d'accès courant de chaque terminal mobile.

Pour chaque sous-réseau IP contrôlé par le WDS, un tunnel est créé sur le SE et associé à un groupe de mobilité. Lorsqu'un terminal arrive sur le réseau, il doit s'identifier auprès du WDS pour avoir accès au réseau. Lors de la requête du terminal, le WDS transmet au SE un message comprenant l'adresse IP et l'adresse MAC du terminal ainsi que l'identifiant de son point d'accès courant. A la réception de ce message, le SE met à jour son cache de mobilité et ajoute le terminal à un groupe de mobilité en fonction de son adresse IP. Il ajoute également le point d'accès courant du terminal en tant que nouvelle extrémité du tunnel qui correspond à ce groupe de mobilité. Puis, il envoie un message au WDS lui notifiant que la mise à jour a été effectuée. Le WDS transmet ce message au point d'accès courant du terminal afin qu'il mette à jour sa table de correspondance. Cette table permet de transmettre les paquets IP qui arrivent par le tunnel vers les terminaux mobiles et inversement.

Lors d'un changement de point d'accès entre deux sous-réseaux différents, la procédure réalisée est quasiment identique à celle que nous venons de décrire. Le terminal mobile reste associé au même groupe de mobilité étant donné qu'il ne change pas d'adresse IP et ce, indépendamment du sous-réseau correspondant à sa nouvelle localisation. Par contre, c'est le tunnel associé à ce groupe de mobilité qui est mis à jour : le nouveau point d'accès est ajouté en tant que nouvelle extrémité du tunnel et l'ancien point d'accès est éventuellement supprimé dès lors qu'il n'est plus utilisé par les terminaux du groupe de mobilité. Il est donc intéressant de relever que dans le système WDS, les terminaux mobiles n'interviennent d'aucune manière dans la réalisation du handover de niveau 3, toute la procédure étant entièrement gérée par le réseau (voir la figure 2.13).

Gestion de la sécurité

Le système WDS utilise le protocole 802.1X [8] pour assurer la sécurité du réseau. Lors de l'utilisation basique de ce protocole, les terminaux mobiles sont obligés de s'authentifier auprès du serveur d'authentification après chaque handover de niveau 2. Or, de telles authentifications sont généralement assez longues étant donné qu'elles font in-

tervenir de nombreux échanges de messages. Par conséquent, ces procédures peuvent introduire des délais supplémentaires dans le temps de déconnexion de niveau 2. Le système WDS optimise cette étape grâce à l'utilisation conjointe de la gestion centralisée de clés de cryptage CCKM (*Cisco Centralized Key Management*) et du protocole Cisco LEAP (*Cisco Lightweight Extensible Authentication Protocol*) qui permettent au WDS de tenir le rôle du serveur d'authentification. La phase d'authentification avec le WDS se déroule lors de la phase d'association du handover de niveau 2 et n'introduit que deux messages WLCCP entre le point d'accès et le WDS (requête / réponse de pré-enregistrement). Au final, le système WDS réduit le temps de latence engendré par les handovers de niveau 2 et 3 à moins de 50 millisecondes [96, 97, 98]. La figure 2.13 présente un exemple de handover de niveau 2 et 3 dans le système WDS.

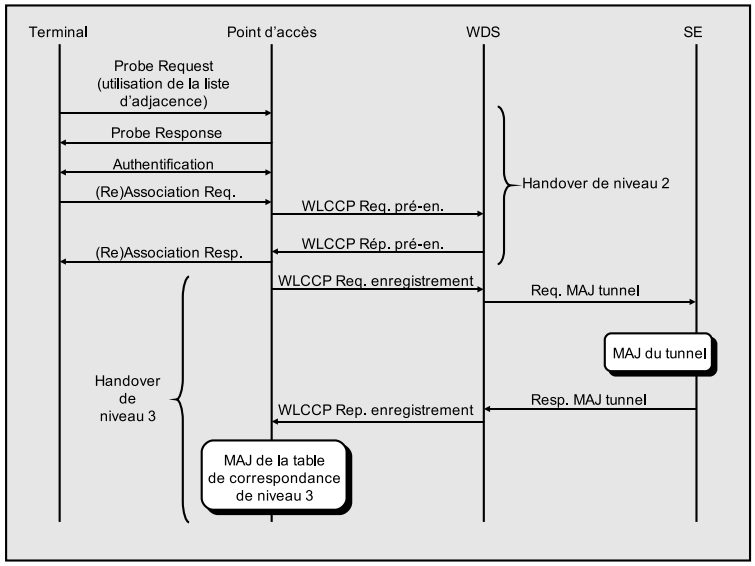


FIG. 2.13 – Handover de niveau 2 et 3 dans le système WDS

2.7 Conclusion

La popularisation des réseaux sans fil et notamment celle des réseaux Wi-Fi a fait apparaître de nouveaux comportements auprès des utilisateurs. L'un des plus significatif étant le désir de communiquer tout en se déplaçant. Nous avons vu que la norme IEEE 802.11 définit les mécanismes de base permettant aux terminaux mobiles de maintenir une connectivité de niveau 2 tout en se déplaçant. Cependant, les études récentes ont montré que ces procédures introduisent un temps de latence dans les communications qui peut s'avérer particulièrement handicapant lors de l'utilisation d'applications

réseaux à forte contrainte de temps (e.g. vidéoconférence). Occupant 90% de la durée d'un handover de niveau 2, c'est principalement la phase de recherche, telle qu'elle est définie dans la norme, qui en est la cause. De plus, le support des déplacements de niveau 3 au sein des réseaux IPv6 a nécessité la création d'un nouveau protocole. Parmi les différentes propositions suggérées dans la littérature, c'est finalement le protocole MIPv6 qui s'est imposé comme standard. Toutefois, les mécanismes qui le composent accentuent encore les temps de déconnexion lors des handovers.

Comme nous l'avons présenté, de nombreuses solutions ont été proposées dans le but d'améliorer les performances des handovers dans les réseaux Wi-Fi et IPv6. Il apparaît que la majorité de ces solutions s'accordent sur la nécessité de connaître a priori les paramètres de niveaux 2 et 3 des prochains points d'attachement des terminaux mobiles. Lors d'un handover de niveau 2, la connaissance préalable du canal radio, de l'adresse MAC et du nom du réseau (SSID) du futur point d'accès accélère considérablement la phase de découverte. L'obtention des paramètres de niveau 3 (notamment le préfixe réseau et l'adresse du routeur par défaut) qui correspondent à ce point d'accès permet également au terminal d'anticiper la réalisation d'un handover de niveau 3. Si les différentes optimisations de la littérature s'entendent sur ces points, elles diffèrent cependant sur les méthodes mises en place pour obtenir de tels paramètres.

Afin d'approfondir notre étude préliminaire, nos premiers travaux ont porté sur l'évaluation d'optimisations se focalisant sur les handovers de niveau 2. Dans le chapitre suivant, nous allons dans un premier temps présenter une étude expérimentale du système WDS que nous avons décrit dans la section 2.6.5 du présent chapitre. Par la suite, nous exposerons une analyse dans laquelle nous avons comparé plusieurs algorithmes tirés de la littérature ou provenant de nos propres recherches.

Propositions et évaluations d'optimisations de niveau 2

Chapitre 3

Evaluation du système Cisco WDS

3.1 Introduction

Lors de la phase préliminaire de nos travaux, nous avons souhaité nous familiariser davantage avec les différents mécanismes disponibles dans la littérature pour gérer la mobilité des utilisateurs. Pour ce faire, nous avons réalisé une analyse du système WDS proposé par le constructeur Cisco System [62]. Le système WDS [96, 97, 98] est une solution disponible dans le commerce qui permet de réaliser des handovers rapides et sécurisés. Le support complet de la mobilité (de niveau 2 et 3) proposé dans ce système requiert un nombre important d'équipements (cf. section 2.6.5). N'ayant pas à disposition les équipements nécessaires à la gestion du niveau 3, l'étude présentée dans ce chapitre se limite à l'évaluation des mécanismes de niveau 2. La prochaine section décrit la plate-forme mise en place pour effectuer les différentes expérimentations ainsi que nos deux scénarii de tests. Notre analyse se focalise sur les temps de chaque phase du handover de niveau 2. Nous étudierons également l'impact du temps de latence engendré par les handovers de niveau 2 sur la réception d'un flux applicatif.

3.2 Plate-forme de tests

La plate-forme de tests que nous avons utilisée comprend un terminal mobile, un correspondant et deux points d'accès. Le terminal mobile est équipé d'une carte 802.11b Cisco Aironet 350 et les points d'accès sont des Cisco Aironet 1200 supportant la norme 802.11b. Les points d'accès ont été positionnés sur les canaux radio 11 et 6 (voir figure

3.1). Le point d'accès 2 joue simultanément le rôle du WDS et celui du serveur d'authentification.

Dans le premier scénario, le terminal mobile se déplace entre les points d'accès 1 et 2 en réalisant des handovers de niveau 2. En vue d'activer l'optimisation, le correspondant (CN) envoie au terminal mobile un flux applicatif continu. Ce flux correspond à un flux audio compressé avec le codec G.711 [44]. Rappelons qu'un codec constitue un pilote de compression et de décompression de données. Dans le codec G.711, les paquets de données ont une taille finale de 1280 bits chacun et sont envoyés toutes les 20 millisecondes. Pour créer un tel flux applicatif, nous avons utilisé le générateur de trafic MGEN [86]. Le scénario 2 est similaire au scénario 1 à l'exception de la transmission du flux applicatif. A titre de référence, nous avons souhaité évaluer les performances du système WDS lorsque l'optimisation n'est pas active, c'est pourquoi nous avons délibérément désactivé toutes transmissions de flux applicatif dans ce deuxième scénario.

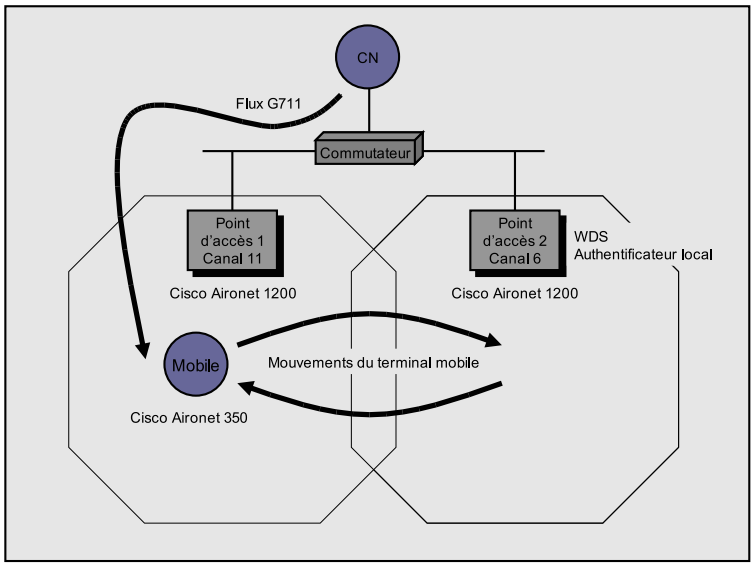
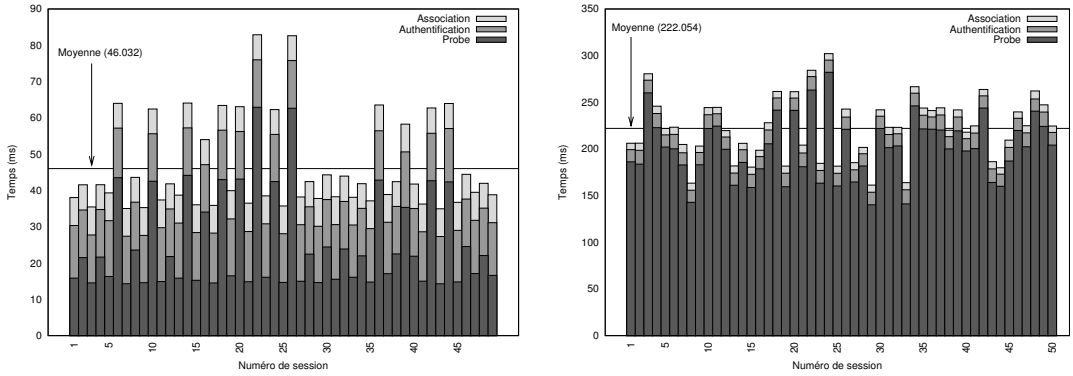


FIG. 3.1 – Plateforme d'évaluation de la solution Cisco WDS

3.3 Résultats

Les résultats présentés dans cette section ont été obtenus à l'aide de deux analyseurs réseau (i.e. sniffeurs) utilisant le logiciel Ethereal [22]. Un sniffeur est un équipement qui intercepte toutes les trames circulant sur un support de communication. Pour chaque scénario, nous avons effectué 50 mesures. La figure 3.2 représente les temps de latence

des handovers de niveau 2 pour les scénarii 1 et 2. Il apparaît que le système WDS réduit le temps de latence à 46,032 millisecondes en moyenne dans le scénario 1 (voir la figure 3.2(a)). Grâce à la liste des points d'accès voisins, le temps pris par la phase de découverte est minimisé. Toutefois, nous pouvons constater que cette phase requiert encore 24,96 millisecondes en moyenne. Néanmoins, les temps de latence globaux respectent bien les performances avancées dans la documentation relative au système WDS qui annoncait des handovers de niveau 2 et 3 inférieurs à 50 millisecondes lorsque l'optimisation est active [96, 97, 98].



(a) Scénario 1

(b) Scénario 2

FIG. 3.2 – Temps de latence des handovers de niveau 2 avec le système WDS

Nous pouvons également noter que la méthode d'authentification utilisée n'a qu'une influence très limitée sur le temps total de déconnexion. En effet, cette étape ne met en jeu qu'une requête / réponse entre le point d'accès et l'équipement WDS. En outre, il faut noter que l'équipement WDS se situe sur l'un des deux points d'accès et que les deux points d'accès se trouvent dans le même sous-réseau. En délocalisant l'équipement WDS dans un autre niveau du domaine, les délais pour l'atteindre peuvent augmenter et par conséquent accroître le temps de déconnexion.

Comme nous l'avons montré dans le chapitre précédent (voir la section 2.6.5), le système WDS de Cisco est censé offrir de moins bonnes performances lorsque le terminal mobile n'émet ou ne reçoit pas de flux applicatif dans les 500 millisecondes précédant le handover. En l'absence de flux (scénario 2), les temps de latence augmentent jusqu'à 222,054 millisecondes en moyenne. Cependant, ces temps restent inférieurs à ceux obtenus dans [58]. En effet, nous avons constaté lors de l'utilisation d'un pilote de périphérique récent que les terminaux équipés de carte Cisco sauvegardent la liste des canaux utilisés et s'associent directement aux points d'accès détectés. Cette procé-

dure est assez proche de la solution du *Selective Scanning and Caching* que nous avons détaillée dans la section 2.6.3.

Enfin, la figure 3.3 illustre l'impact d'un handover de niveau 2 sur la réception d'un flux applicatif au niveau du terminal mobile. Chaque point représente la réception d'un paquet de données au temps indiqué sur l'axe des ordonnées. Nous pouvons constater que lors de la réception d'un flux audio utilisant le codec G.711, le terminal perd en moyenne 3 paquets de données pendant le handover de niveau 2. Suivant l'application utilisée, ce taux de pertes pourrait déjà être perceptible par l'utilisateur. Malheureusement, le flux utilisé dans ces tests était un flux émulé. Par conséquent, nous n'avons pas pu mesurer l'influence réelle du handover sur la perception de l'utilisateur. Néanmoins, cet aspect reste très dépendant du comportement de l'application utilisée.

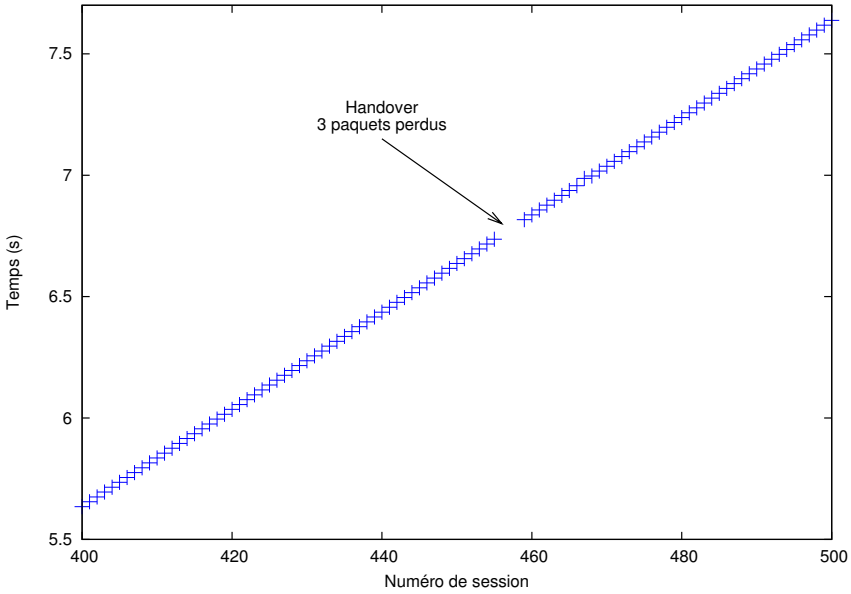


FIG. 3.3 – Impact des handovers de niveau 2 du système Cisco WDS sur les flux applicatifs

3.4 Conclusion

Cette première étude expérimentale du système Cisco WDS a permis de nous familiariser avec les environnements IEEE 802.11. Nous avons notamment pu vérifier que la connaissance au préalable des paramètres de niveau 2 des points d'accès environnants permet de considérablement réduire la durée de la phase de découverte et par conséquent le temps de latence total engendré par un handover de niveau 2.

Il reste cependant difficile d'établir des scénarii de tests plus complexes lors de l'évaluation expérimentale d'un protocole. En effet, les deux scénarii utilisés ici sont assez simplistes et bien adaptés au mécanisme d'optimisation du système WDS. Avec un unique point d'accès voisin, il est relativement aisé de sélectionner son futur point d'accès parmi la liste des points d'accès adjacents.

A la vue des résultats obtenus, nous avons décidé de poursuivre notre étude préliminaire à l'aide d'un outil de simulation. Dans le chapitre suivant, nous présenterons un comparatif entre divers mécanismes d'optimisations des handovers de niveau 2. Les solutions retenues pour cette analyse sont aussi bien tirées de la littérature que de notre propre recherche.

Chapitre 4

Comparaison de solutions de niveau 2

4.1 Introduction

Dans la continuité de notre étude préliminaire, nous avons réalisé une analyse comparative de diverses optimisations des handovers de niveau 2 dans les réseaux Wi-Fi [61]. De nombreuses solutions ont été proposées dans la littérature (cf. 2.6) mais nous nous sommes aperçus d'un manque de comparatifs entre ces diverses propositions. Les optimisations retenues ici se focalisent essentiellement sur la réduction du temps pris par la phase de découverte. Nous avons notamment défini un nouveau protocole appelé *Periodic Scanning* ainsi qu'une approche relativement similaire au système WDS étudié dans le chapitre précédent, afin d'évaluer ses performances dans des configurations plus complexes. Notre étude intègre également la solution *Selective Scanning and Caching* qui a été détaillée dans la section 2.6.3. Les performances de ces trois solutions ont été comparées à celles obtenues avec la procédure standard telle qu'elle est décrite dans la norme IEEE 802.11.

L'étude présentée dans ce chapitre a été effectuée par simulation à travers six scénarii allant de cas académiques à des environnements plus réalistes. Les simulations ont été réalisées à l'aide de notre simulateur de réseaux sans fil SimulX [93]. Nous consacrerons donc une section à la présentation de ses fonctionnalités.

4.2 Le simulateur SimulX

4.2.1 Contexte

Dans le domaine des réseaux, la simulation est un outil puissant qui permet d'observer rapidement le comportement d'un protocole en cours de spécification. Bien que l'implémentation réelle d'un protocole constitue le meilleur moyen de démonstration de son bon fonctionnement, elle reste habituellement fastidieuse et limite souvent le nombre d'équipements présents dans la plate-forme de tests. La simulation permet de créer des environnements à très grande échelle afin de détecter et de corriger rapidement les éventuels problèmes qui n'ont pas été pris en compte lors des spécifications. Cette première phase de validation est nécessaire et permet d'avoir une description claire du protocole qui sera par la suite moins soumise aux modifications. Dès lors, l'implémentation du protocole à titre de validation finale sera en partie simplifiée.

Au sein de ses activités de recherche, l'équipe Réseaux et Protocoles du LSIIT avait initié le développement de son propre simulateur de réseaux sans fil IPv6 nommé *SimulX* [93]. Débuté en 2003, ce projet fut motivé par le manque d'un réel simulateur de réseaux de nouvelle génération respectant les spécifications des protocoles simulés. En constante évolution, SimulX est devenu un puissant outil de recherche, mais également un outil pédagogique intéressant pouvant être mis à profit dans l'enseignement. Le simulateur SimulX est désormais disponible sous licence GPL [93].

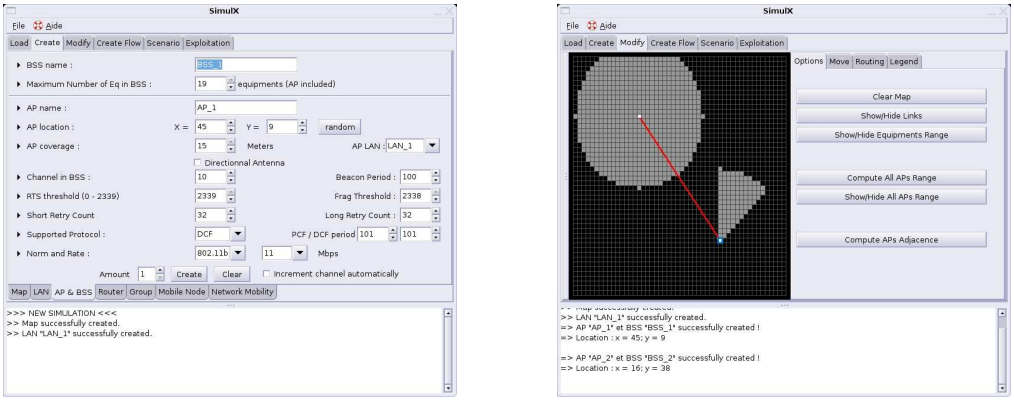
4.2.2 Contributions

Lors de mes travaux de thèse, je me suis beaucoup investi dans le développement de SimulX. En plus de l'implémentation de différentes solutions d'optimisations des handovers dans les réseaux WiFi IPv6, j'ai contribué à l'évolution de ses fonctionnalités et de ses performances. J'ai notamment été très impliqué dans l'écriture de différents correctifs de stabilité et d'optimisation.

4.2.3 Principe de fonctionnement

Le simulateur SimulX vise à simuler des réseaux sans fil 802.11. Il offre également la possibilité de créer des environnements de niveau 3 avec le support des protocoles IPv6 et MIPv6. Le simulateur est développé dans le langage de programmation C++. Il dispose d'une interface graphique utilisant la librairie GTK+-2 (*Gimp Tool Kit version*

2 [39]). Une carte réalisée à l'aide de la librairie OpenGL (*Open Graphics Library* [76]) permet de visualiser et de manipuler les différents équipements d'une simulation. La figure 4.1 donne un aperçu de l'interface du simulateur.



(a) Configuration d'un point d'accès (b) Visualisation d'un scénario

FIG. 4.1 – Interface du simulateur SimulX

L'interface du simulateur permet de configurer l'ensemble des paramètres de chaque équipement qu'on souhaite inclure dans une simulation. La configuration ainsi obtenue peut ensuite être enregistrée dans des fichiers de sauvegarde, de façon à pouvoir réutiliser une configuration donnée. Les résultats d'une simulation sont fournis sous forme de fichiers texte qu'il est possible de sélectionner avant chaque simulation. Parmi les fichiers disponibles, un fichier est consacré aux handovers de niveau 2 et retrace tous les messages de signalisation échangés au niveau liaison. Un autre fichier récapitule les temps des handovers de niveau 3 pour chaque terminal mobile. Enfin, un fichier plus général retrace les statistiques de la simulation : nombre de retransmissions, de pertes, de paquets échangés, etc.

Le déroulement d'une simulation repose sur une boucle principale appelée à chaque événement. Il est également possible de lancer une simulation en avançant intervalle de temps par intervalle de temps (correspondant à 2 microsecondes dans SimulX). Un événement peut correspondre à l'émission / réception d'une trame, au déplacement d'un équipement sur la carte, etc. A chaque événement, le simulateur commence par déplacer les différents équipements mobiles (lorsque cela est nécessaire) et propage les trames présentes sur les multiples liens (radio et filaires). Puis, il traite l'émission et la réception des trames, efface les objets devenus inutiles et vérifie si la simulation est terminée. Lorsqu'il ne reste plus d'événements, le simulateur génère les différents fichiers de résultats demandés ce qui complète la simulation. Sinon, il saute au prochain événement

(ou intervalle de temps selon la configuration) et commence une nouvelle itération de la boucle. La figure 4.2 illustre le déroulement d'une simulation.

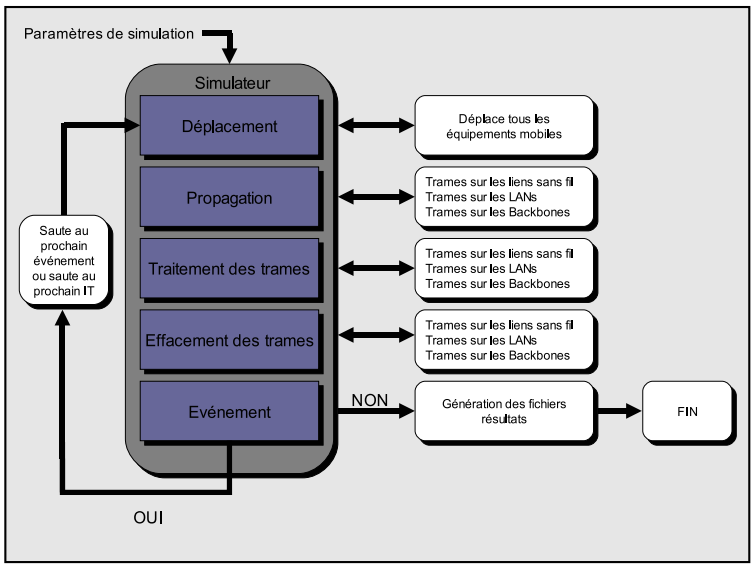


FIG. 4.2 – Boucle principale du simulateur SimulX

4.3 Description des protocoles

Parmi les nombreuses solutions disponibles dans la littérature ou issues de notre propre recherche, nous nous sommes focalisés sur les optimisations de niveau 2 qui nous semblaient les plus performantes et intéressantes. Parmi les propositions existantes, nous avons retenu le protocole 802.11 standard (à titre de référence) et le *Selective Scanning and Caching* [90]. Ces deux protocoles ont déjà été détaillées dans les sections 2.3 et 2.6.3. De plus, la présente étude intègre deux de nos propositions : les protocoles *Adjacent AP* et *Periodic Scanning*. Dans cette section, nous allons brièvement décrire les différents mécanismes qui les composent.

4.3.1 Adjacent AP

Cette méthode est relativement proche des mécanismes d'optimisation de niveau 2 proposés dans le système WDS (sans la partie portant sur l'authentification rapide, cf. section 3). Grâce à la simulation, nous avons pu approfondir l'idée du positionnement d'une liste de point d'accès voisins sur les terminaux mobiles. Dans notre méthode, les

points d'accès possèdent a priori la liste d'adjacence des cellules voisines. Cette liste contient l'adresse MAC, le canal radio et le SSID de chaque point d'accès adjacent à un point d'accès donné. Ces informations pourraient être complétées par les paramètres de sécurité utilisés sur chaque point d'accès, mais nous nous sommes attachés à une étude dans un système ouvert.

La liste des voisins d'un point d'accès est envoyée aux terminaux mobiles lors du handover de niveau 2, à l'aide de nouveaux paramètres introduits dans les trames *(Re)Association Response*. Lorsqu'un terminal doit réaliser un handover, il essaie de s'associer aux points d'accès contenus dans la liste. Ayant une connaissance préalable des différents paramètres obtenus normalement lors de sondage des différents canaux radio, le terminal mobile peut supprimer la phase de découverte et directement envoyer une requête d'authentification vers le premier point d'accès de la liste. Lorsque ce point d'accès est à portée radio et accepte l'authentification, le terminal débute la phase d'association et finalise le handover.

Lorsqu'une requête d'authentification n'est pas acquittée, cela peut signifier qu'il y a eu une collision ou que le point d'accès cible n'est pas dans la portée radio du terminal. La probabilité de cette dernière possibilité étant relativement importante, le nombre de retransmissions des requêtes d'authentification a été modifié, car cela peut significativement augmenter le temps de latence des handovers de niveau 2. Nous avons positionné le nombre maximum de retransmissions à 3 comme suggéré dans [104]. Après trois retransmissions successives d'une requête d'authentification, le terminal considère que le point d'accès n'est pas joignable et tente de s'associer au prochain point d'accès de la liste. Dans le cas où tous les points d'accès de la liste ne seraient pas joignables, le terminal effectue un handover standard.

4.3.2 Periodic Scanning

Le *Periodic Scanning* constitue une approche originale issue de notre recherche. L'idée principale de cette solution repose sur la réalisation de courtes phases de découverte alors que les terminaux mobiles sont encore associés à leurs points d'accès courants. Lors de ces recherches anticipées, les terminaux mobiles ont l'occasion de découvrir leurs futurs points d'accès avant le déclenchement de la procédure de handover. Par conséquent, la phase de découverte définie par la norme IEEE 802.11 peut être supprimée. Comme nous l'avons vu précédemment, la réduction / suppression de cette étape lors d'un handover effectif permet de réduire significativement le temps de latence engendré par les déplacements de niveau 2 (i.e. réduction de l'ordre de 90% du temps de handover). La figure 4.3 illustre les différentes étapes du *Periodic Scanning*.

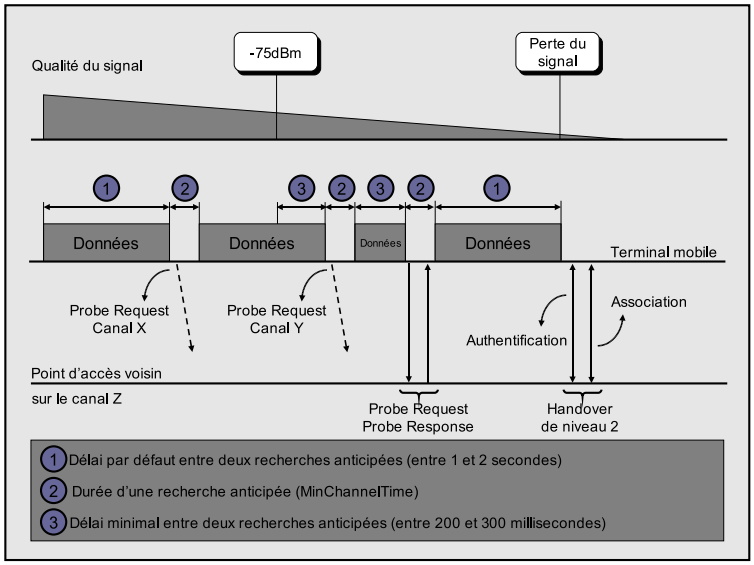


FIG. 4.3 – La méthode Periodic Scanning

Les terminaux débutent une phase de découverte anticipée suivant deux périodes de temps. En fonction du nombre de points d'accès déjà identifiés et de la qualité du signal radio, le terminal mobile augmente ou réduit la fréquence de ces phases. Lorsque la qualité du signal est relativement correcte (entre $-50dBm$ et $-75dBm$ en fonction des mesures trouvées dans [69]), le terminal tire aléatoirement un nombre réel entre 1 et 2 secondes et l'utilise pour armer un compteur de temps. Lorsque le compteur arrive à échéance, le terminal change de canal radio et effectue un scan actif de ce canal pendant *MinChannelTime*. Dès que la qualité du signal devient faible (i.e. inférieur à $-75dBm$) et si le terminal n'a pas encore trouvé de point d'accès cible, il positionne la fréquence des recherches anticipées entre 200 et 300 millisecondes. Cette fréquence relativement rapide est nécessaire pour accélérer la découverte d'un nouveau point d'accès alors qu'un handover peut survenir très prochainement. Dès la découverte d'un point d'accès, le terminal règle à nouveau la fréquence des recherches à sa valeur par défaut (i.e. entre 1 et 2 secondes) afin de limiter les perturbations que peuvent générer ces phases dans les communications de la cellule. En effet, lorsque le terminal mobile reçoit un flux applicatif pendant qu'il réalise une phase de recherche anticipée, il n'est pas en mesure de recevoir les trames de données émises par son point d'accès courant. Ce dernier ne recevant pas d'acquittement pour ces données, les réémet jusqu'à l'obtention d'accusés de réception ou jusqu'à atteindre la limite maximale de retransmissions. De ce fait, le lien radio est monopolisé par ces différentes retransmissions, ce qui peut générer de légers temps de latence au sein des communications des autres équipements de la cellule (la durée maximale de retransmission d'une trame 802.11 est d'environ 4 millisecondes [88]).

Durant les phases de recherches anticipées, le terminal mobile construit une liste de points d'accès qui constituent des cibles potentielles pour le futur handover. Pour chaque point d'accès découvert, le terminal enregistre son adresse MAC, son SSID et le canal radio utilisé. Lorsque le terminal perd la connectivité avec son point d'accès courant, il consulte sa liste de points d'accès cibles. Dans le cas où la liste est vide, le terminal réalise un handover standard tel qu'il est décrit dans la norme IEEE 802.11. Sinon, le terminal débute une phase d'authentification avec le premier point d'accès de la liste (i.e. le dernier point d'accès découvert). Comme pour la méthode *Adjacent AP*, nous avons limité le nombre de retransmissions des requêtes d'authentification car il est probable que certains points d'accès de la liste ne soient plus à portée radio. Lorsque le terminal ne reçoit pas de réponses à ses requêtes, il essaie de s'associer au point d'accès suivant de la liste. Lorsqu'il a entièrement parcouru la liste en vain, le terminal effectue une procédure de handover standard.

4.4 Evaluation des performances

Les différents protocoles retenus pour ce comparatif ont été évalués par simulation. Pour ce faire, nous les avons intégrés dans le simulateur SimulX. Nous avons également défini six scénarii variant entre des cas théoriques et des environnements plus réalistes. Lors des simulations, les paramètres *MinChannelTime* et *MaxChannelTime* ont été respectivement positionnés à 30 et 200 millisecondes. Rappelons que ces paramètres sont notamment utilisés lors d'une procédure standard de handover (voir la section 2.3.1). Lors des handovers standard, les terminaux mobiles ont également été configurés pour qu'ils initient la phase d'authentification après avoir passé *MaxChannelTime* sur un canal, c'est-à-dire dès la découverte de points d'accès sur un canal.

4.4.1 Scénarii de simulation

Le modèle de mobilité visé par nos six scénarii présente le cas d'utilisateurs se déplaçant à pied à l'intérieur de bâtiments. Pour modéliser un tel environnement, le rayon de portée radio des différents équipements (terminaux mobiles et points d'accès) a été positionné à 20 mètres et chaque terminal mobile se déplace à la vitesse d'1m/s.

Les deux premiers scenarii sont des cas académiques et font intervenir 11 points d'accès et 10 terminaux mobiles. Les points d'accès sont alignés de manière à ce que 30 mètres séparent chacun d'entre eux. Par conséquent, la taille de la zone de chevauchement des différentes cellules BSS est de 10 mètres. Les points d'accès utilisent

uniquement les canaux radio 1, 6 et 11. Rappelons que ces trois canaux radio ne s'interfèrent pas et qu'ils sont utilisables dans la majorité des pays. Les terminaux mobiles débutent leurs déplacements dans la même seconde. Au début de la simulation, les terminaux mobiles sont associés au point d'accès 1 et se déplacent suivant une trajectoire rectiligne. La seule différence entre les scénarii 1 et 2 provient de la distribution des canaux radio (voir figure 4.4).

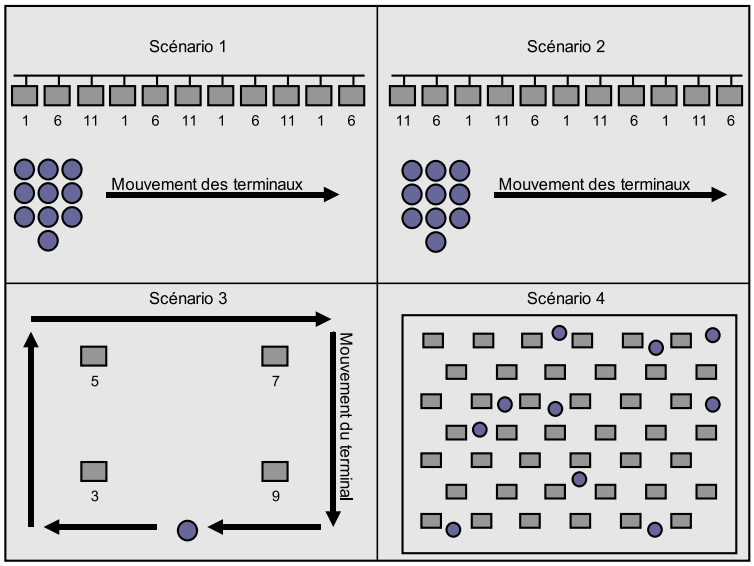


FIG. 4.4 – Scénarii de simulations pour l'évaluation des optimisations de niveau 2

Le troisième scénario a été spécialement conçu pour le protocole *Selective Scanning and Caching* en vue d'apporter un environnement propice aux mécanismes d'optimisation qui le compose. Quatre points d'accès sont disséminés sur la carte et un terminal mobile effectue un mouvement cyclique autour d'eux. Les canaux radio utilisés par les points d'accès sont illustrés sur la figure 4.4.

Le scénario 4 vise à simuler un environnement réaliste comprenant 42 points d'accès et 10 terminaux mobiles. Les points d'accès sont placés de manière à couvrir une zone de 200 mètres sur 188 mètres. La position initiale des terminaux mobiles et le canal radio des points d'accès sont choisis aléatoirement. Chaque terminal effectue 10 déplacements rectilignes dont chaque point d'arrivée est déterminé de façon aléatoire dans la zone couverte.

Les deux derniers scénarii (5 et 6) reprennent la topologie des scénarii 1 et 2. Afin d'évaluer l'impact de chaque protocole sur la réception de données, nous avons ajouté un correspondant pour chaque terminal (i.e. 10 correspondants au total). Les correspon-

dants envoient chacun un flux audio à l'un des terminaux en utilisant le codec G.711 [44]. Dans ce codec, un paquet de 1280 bits est envoyé toutes les 20 millisecondes.

4.4.2 Résultats de simulation

Les résultats présentés dans cette section ont été obtenus en simulant chaque couple scénario / protocole à 100 reprises. La figure 4.5 représente les valeurs moyennes (axe de gauche) et les écart-types (axe de droite) des temps de latence obtenus pour chaque protocole dans les quatre premiers scénarii. On peut remarquer que la méthode standard offre toujours de moins bonnes performances avec un temps de latence moyen compris entre 312 millisecondes (scénario 3) et 481 millisecondes (scénario 2). Le scénario 2 fait apparaître un temps de latence plus important en raison du nombre moyen de canaux radio à sonder avant de découvrir un nouveau point d'accès. En observant l'allocation des canaux radio et les déplacements dans le scénario 2, on constate qu'un terminal mobile sonde en moyenne 10,3 canaux (lors de la procédure standard) avant de découvrir son prochain point d'accès (contre 5,7 par exemple dans le scénario 1).

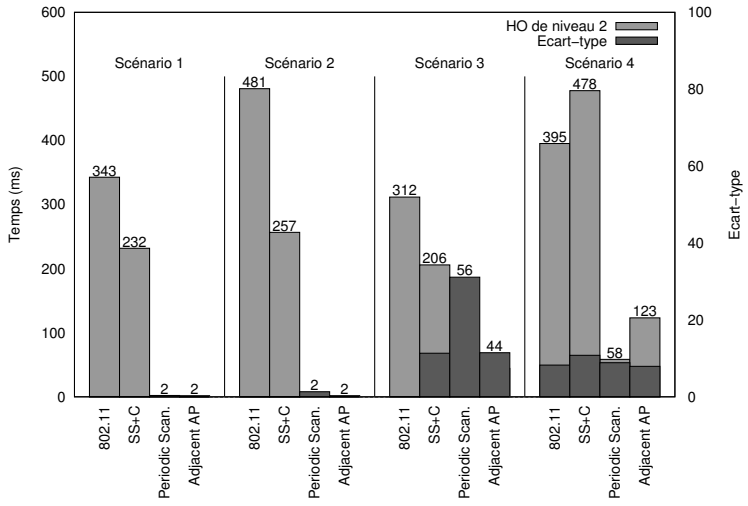


FIG. 4.5 – Moyennes et écart-types du temps de latence des handovers de niveau 2

La méthode *Selective Scanning and Caching* (référencée par *SS+C* dans les figures) permet de réduire le temps de latence des handovers dans les scénarii 1 et 2. Cependant, le handover de niveau 2 y requiert encore 240 millisecondes en moyenne. Cette réduction est possible grâce à l'utilisation du masque de canaux radio qui limite le nombre des canaux radio à sonder ; mais le mécanisme de cache n'est pas utile car les terminaux mobiles ne repassent jamais par les mêmes points d'accès. Dans le scénario 3, nous espérions de meilleurs résultats car le terminal mobile s'associe à plusieurs reprises aux

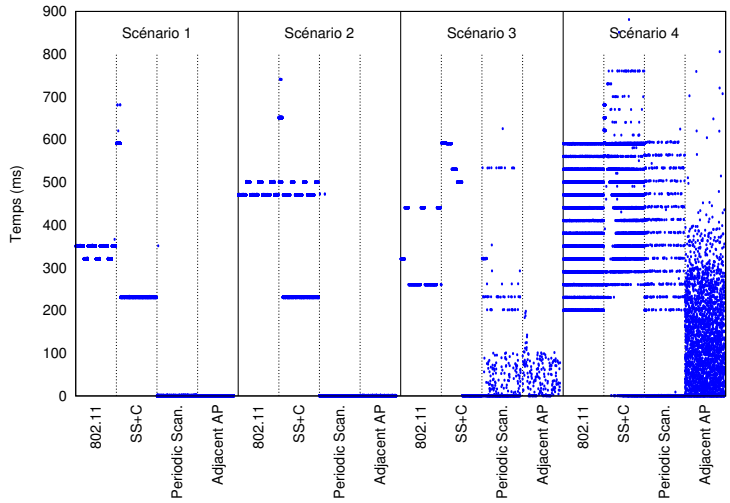


FIG. 4.6 – Détail du temps de latence des handovers de niveau 2

mêmes points d'accès et peut donc tirer parti des informations du cache. Si on observe la figure 4.6 dans laquelle chaque point représente la durée d'un handover de niveau 2, on peut remarquer que les temps de latence sont concentrés autour de 4 valeurs. Les premiers handovers sont relativement longs, mais lorsque les terminaux ont construit leurs caches, les handovers deviennent alors très rapides (environ 3 millisecondes sont nécessaires pour finaliser la procédure). On peut relever ici que le nombre de handovers réalisés en 3 millisecondes est beaucoup plus important que le nombre de ceux qui sont supérieurs à 200 millisecondes. Le regroupement des résultats autour de quatre valeurs explique l'écart-type important observé dans la figure 4.5, ce qui rend la valeur moyenne non pertinente. Lorsqu'on considère chacune des quatre valeurs indépendamment, l'écart-type devrait être proche de 0. Les temps de latence considérables observés dans le scénario 4 pour cette méthode sont principalement dû à de nombreuses procédures d'inversion et de reconstruction du masque de canaux radio en raison de la nature très aléatoire de ce scénario.

D'après les résultats présentés dans les figures 4.5 et 4.6, il apparaît que nos deux nouvelles méthodes semblent réduire significativement le temps de latence engendré par un handover de niveau 2 indépendamment du scénario utilisé. Dans les scénarii 1 et 2, le temps d'un handover est de 2 millisecondes, ce qui correspond au temps minimal nécessaire pour échanger les trames d'authentification et d'association. En raison de la disposition des points d'accès et du mouvement des terminaux, il n'y a qu'un point d'accès candidat pour chaque handover.

Dans le scénario 3, le temps de latence moyen augmente à 56 millisecondes pour le *Periodic Scanning* et à 44 millisecondes pour la méthode *Adjacent AP*. Nous pouvons aussi remarquer que l'écart-type de ces deux solutions augmente également. Lors d'un handover, le terminal mobile a le choix entre plusieurs points d'accès candidats alors que seul l'un d'entre eux est réellement joignable. Pour le *Periodic Scanning*, cela signifie que le terminal a pu découvrir un point d'accès qui ne sera pas joignable lors du handover effectif. Dès lors, il est possible qu'il ne trouve pas d'autres points d'accès candidats car la fréquence des recherches anticipées reste à sa valeur par défaut (entre 1 et 2 secondes). Dans le cas de la méthode *Adjacent AP*, les terminaux peuvent essayer de s'associer à plusieurs points d'accès de la liste des voisins avant de tomber sur celui qui est réellement à portée.

Cette observation est plus claire dans le cas du scénario 4. Dans ce scénario, nous pouvons noter que le *Periodic Scanning* donne de meilleurs résultats que la méthode *Adjacent AP* avec des temps de latence respectifs de 58 et 123 millisecondes. On constate que 71% des handovers sont réalisés en moins de 5 millisecondes avec le *Periodic Scanning* alors que seulement 26% des handovers sont inférieurs à 50 millisecondes dans la méthode *Adjacent AP* (voir la figure 4.6). La disposition des points d'accès permet d'expliquer ce phénomène. En effet, chaque point d'accès à un important nombre de voisins et dans le cas de la méthode *Adjacent AP*, les terminaux essaient de s'associer aux points d'accès dans l'ordre défini par la liste des voisins. Un terminal peut donc effectuer 5 à 6 tentatives d'association avant d'atteindre un point d'accès à portée radio. C'est pourquoi de nombreux handovers engendrent des temps de latence supérieurs à 200 millisecondes avec cette méthode. Avec le *Periodic Scanning*, les résultats sont meilleurs car les terminaux mobiles essaient de s'associer aux derniers points d'accès découverts. Cependant, il peut arriver qu'un terminal n'ait pas le temps de sonder le bon canal avant une procédure de handover en raison de la fréquence relativement lente des recherches anticipées lorsque le terminal a déjà découvert un point d'accès. Pour palier ces problèmes, nous pourrions augmenter la fréquence des recherches anticipées même si le terminal a déjà découvert des points d'accès. Par contre, cela générerait plus de trafic sans garantie sur le fait que le terminal réaliserait effectivement un handover.

La figure 4.7 représente les valeurs moyennes et les écart-types du nombre de messages nécessaires à la réalisation d'un handover. On constate que la méthode *Adjacent AP* génère le moins de messages (6 et 9 en moyenne suivant le scénario) car les listes d'adjacence sont envoyées à l'aide de messages existants et que les phases de découvertes y sont absentes. D'un autre côté, le *Periodic Scanning* génère un trafic plus important que les autres protocoles : entre 25 et 58 messages sont nécessaires à la réalisation d'un handover en raison des recherches anticipées. Le nombre de messages introduits par le *Selective Scanning and Caching* est approximativement le même que celui de la méthode standard. Cela provient principalement de la construction du masque de canaux

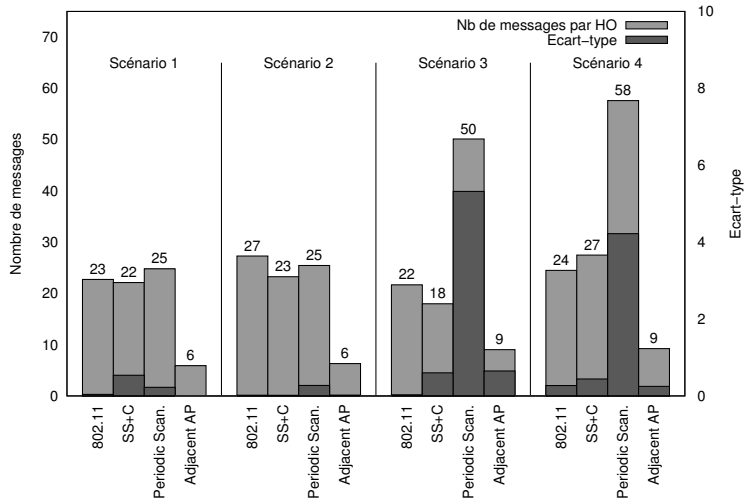


FIG. 4.7 – Moyennes et écart-types du nombre de messages par handover

pendant laquelle les terminaux sondent tous les canaux radio. De plus, le mécanisme de cache est rarement utile dans nos scénarii (scénario 3 mis à part). C'est pourquoi nous n'observons pas de réduction significative du nombre de messages dans ce protocole en comparaison avec la méthode classique.

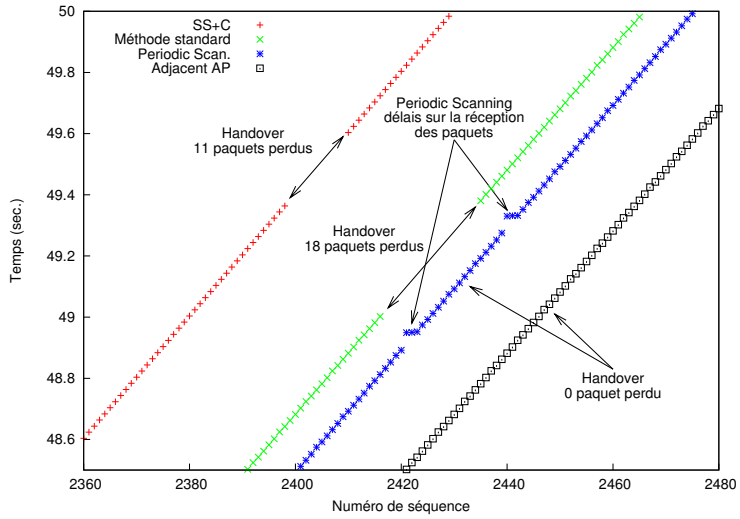


FIG. 4.8 – Impact des handovers de niveau 2 sur les flux applicatifs

Enfin, la figure 4.8 illustre l'impact d'un handover sur la réception d'un flux applicatif dans nos deux derniers scénarii (i.e. les scénarii 1 et 2 auquel on a ajouté des flux applicatifs). Chaque point représente la réception d'un paquet de données au temps

indiqué sur l'axe des ordonnées. On constate que la méthode standard et le *Selective Scanning and Caching* perdent respectivement 18 et 11 paquets de données en moyenne. Dans le *Periodic Scanning*, le handover est imperceptible étant donné qu'il n'y a aucun paquet perdu. En revanche, nous pouvons observer de courts délais dans la réception de deux paquets lors d'une procédure de recherche anticipée. Quant à la méthode *Adjacent AP*, elle permet de ne perdre aucun paquet de données et ce, sans introduire de délais dans les communications.

4.5 Conclusion

Dans ce chapitre, nous avons étudié différentes optimisations se focalisant sur les handovers de niveau 2. Six scénarii de simulation représentant divers environnements ont été définis de façon à fournir une analyse aussi complète que possible. Il ressort de cette analyse que toutes les solutions présentées donnent de meilleurs résultats que la méthode standard. Toutefois, nous avons pu remarquer que les performances de ces protocoles étaient très dépendantes de l'environnement dans lequel se trouvent les terminaux mobiles. Par exemple, la méthode *Selective Scanning and Caching* est vraiment efficace dans les petits environnements pour lesquels les terminaux utilisent souvent les mêmes points d'accès. La méthode *Adjacent AP* est performante mais n'est réalisable qu'entre points d'accès appartenant au même opérateur. En outre, l'ordre des points d'accès au sein de la liste d'adjacence peut considérablement influer sur les performances de cette méthode. Enfin, le *Periodic Scanning* semble efficace dans tous les environnements, mais génère du trafic supplémentaire qui augmente la consommation énergétique de l'équipement. De plus, lorsqu'un terminal change de canal radio pour effectuer une phase de découverte anticipée, le trafic de la cellule peut éventuellement être perturbé (cf. section 4.3.2). Pour éviter ce problème, le terminal pourrait indiquer à son point d'accès de mettre en attente les trames qui lui sont destinées avant chaque procédure de recherche anticipée, comme cela est suggéré dans [88].

A la vue des nos différentes études préliminaires sur les handovers de niveau 2, il ne subsiste plus aucun doute sur la faisabilité de handovers rapides dans les réseaux Wi-Fi dès lors que les terminaux possèdent a priori les paramètres des points d'accès environnants. Néanmoins, les performances des optimisations évaluées sont très dépendantes de l'environnement dans lesquels les terminaux mobiles sont placés. Bien que la procédure utilisée lors d'un handover effectif soit très similaire (réduction / suppression de la phase de découverte), ce sont réellement les mécanismes d'acquisition des paramètres des points d'accès voisins qui influent sur les performances. La détention d'une liste de points d'accès adjacents (à la manière du système WDS) n'est pas forcément suffisante à la réalisation d'un handover rapide. Lorsque cette liste n'est pas spécifiquement adap-

tée à chaque terminal mobile par rapport à sa position, le temps perdu à la recherche du futur point d'accès parmi la liste des candidats peut, dans certain cas réduire à néant la suppression de la phase de découverte, nous ramenant pratiquement aux mêmes performances que la procédure standard. Ainsi, il paraît évident que des informations de géolocalisation pourraient fournir une indication supplémentaire au choix des futurs points d'accès. A l'aide de mécanismes efficaces, il serait possible de trier la liste des points d'accès candidats en tirant parti des positions des différents équipements. Nous pourrions également étendre l'acquisition des informations de niveau 2 à celles de niveau 3 en vue d'offrir un support complet de la mobilité au sein des réseaux Wi-Fi IPv6. Dans les prochains chapitres, nous étudierons la mise en place de telles fonctionnalités.

Dans un premier temps, nous allons présenter les systèmes de géolocalisation actuels ainsi que les méthodes qu'ils utilisent pour déterminer la position d'un équipement. Puis, nous présenterons les diverses propositions d'utilisation d'informations de géolocalisation dans les réseaux et plus particulièrement dans la gestion des handovers au sein de réseaux sans fil. Enfin, nous détaillerons nos différents travaux dans ce domaine, travaux qui comprennent notamment la spécification, l'évaluation et l'implémentation de deux nouveaux protocoles utilisant des informations de géolocalisation pour optimiser les handovers de niveau 2 et 3 dans les réseaux Wi-Fi IPv6.

Gestion des handovers assistée par géolocalisation

Chapitre 5

Techniques et méthodes de géolocalisation

5.1 Introduction

La géolocalisation est la capacité d'un système à déterminer la position géographique d'un équipement, qu'il soit mobile ou non. Les positions obtenues sont généralement exprimées sous forme de coordonnées géodésiques (latitude, longitude, altitude) ou sous forme de coordonnées relatives (x,y,z) à un point donné. Principalement utilisée pour la navigation, la géolocalisation a su profiter des évolutions technologiques en s'intégrant dans les systèmes de communication sans fil. Lorsqu'on a localisé un terminal, il est possible d'envoyer à son utilisateur des informations contextuelles, relatives par exemple aux commerces, aux services et aux lieux remarquables qui existent près de l'endroit où il se trouve. Les services de secours commencent également à tirer profit de la géolocalisation, notamment lors de la recherche de personnes en détresse.

La position géographique d'un équipement peut être déterminée de deux manières différentes. Soit on utilise une infrastructure complètement dédiée à cette fonction, soit on incorpore une telle fonctionnalité dans une infrastructure existante. Dans ce chapitre, nous allons présenter les différents types de signaux ainsi que les multiples méthodes utilisées dans les systèmes de géolocalisation actuels. Nous illustrerons ensuite ces techniques en présentant divers systèmes de positionnement tirés de la littérature ou disponibles dans le commerce.

5.2 Types de signaux

La mise en place d'un système de géolocalisation nécessite la connaissance de la position de certains points de l'environnement, appelés *points références*. La détermination de la position géographique d'un équipement repose principalement sur l'analyse de signaux émis, soit par ces points références, soit par l'équipement lui-même.

Différents types de signaux ont été utilisés dans les systèmes de positionnement [99]. Les principales caractéristiques d'un signal sont sa vitesse de propagation, sa portée et sa bande passante. D'un autre côté, un signal subit des effets de réflexion, de réfraction, de diffraction et d'absorption. Nous présentons ici les signaux les plus utilisés dans les systèmes de positionnement actuels.

5.2.1 Les signaux infrarouge

Découverts en 1800, les signaux infrarouges sont des rayonnements électromagnétiques dont la longueur d'onde est supérieure à celle de la lumière visible. En raison de leur déploiement omniprésent, les transmetteurs infrarouge sont bon marché, petits, et ne consomment pas beaucoup d'énergie. La vitesse de propagation des infrarouges est rapide mais la bande passante effective disponible est réduite en raison des interférences provoquées par la lumière ambiante et par les autres équipements utilisant les infrarouges. Un autre problème provient du fait que ce type de signaux se reflète sur pratiquement toutes les surfaces et ne se diffuse donc pratiquement pas. La portée typique est de 5 mètres.

5.2.2 Les Ultrasons

Les signaux ultrasons deviennent de plus en plus fréquents dans les systèmes de positionnement [99]. La fréquence du signal est ici limitée par l'oreille humaine sur les basses et hautes fréquences. Un être humain peut entendre des sons dont la fréquence est approximativement comprise entre 20 Hz et 20 kHz, c'est pourquoi les systèmes à ultrason utilisent généralement une fréquence de 40 kHz. Les ultrasons sont sensibles à l'environnement (température, humidité, ...), qui agit particulièrement sur la vitesse de propagation du son. Par exemple, une température variant de 0 à $30\,^{\circ}$ altère la vitesse de propagation du son de 3 %. De plus, il est important de noter que les ultrasons se reflètent sur la plupart des surfaces. Dans un système de positionnement, ce type de signal est généralement utilisé conjointement avec des ondes radio [75, 84, 85].

5.2.3 Les ondes radio

Les ondes radio proposent de nombreux avantages : elles traversent divers matériaux, ont une bonne vitesse de propagation, proposent des débits élevés, et les équipements ne sont pas chers. La diffusion des ondes radio est régulée, c'est pourquoi les systèmes de géolocalisation autonomes (i.e. utilisant une architecture propre) opèrent généralement dans des plages de fréquences libres de façon à n'être soumis à aucune licence d'exploitation. La portée de telles ondes en intérieur varie approximativement de 10 à 50 mètres.

5.2.4 Les champs électromagnétiques

Les champs électromagnétiques sont utilisés dans de nombreux systèmes de positionnement à haute précision. Leur vitesse de propagation est très élevée mais leur zone d'émission est limitée à 3 mètres environ. Cela est dû au fait que ce type de signal est très sensible aux interférences de l'environnement comme le champ magnétique de la terre ou la présence de métaux à proximité d'un émetteur / récepteur. De plus, les systèmes utilisant ce type de technologie demandent une calibration très précise et le prix du matériel nécessaire est relativement élevé. Ce type de technologie n'est donc pas adapté à un déploiement sur une grande étendue.

D'autres technologies ont été expérimentées, comme l'utilisation d'équipements optiques (caméra ou laser) mais coûtent trop cher pour être déployées même à échelle moyenne. Nous n'en parlerons donc pas dans ce chapitre.

5.3 Détermination d'une position

Le calcul d'une position par analyse de signaux repose principalement sur trois métriques différentes. La première technique consiste à mesurer la puissance du signal reçu (RSS pour *Received Signal Strength*). En effet, dans un environnement dégagé, la puissance d'un signal est directement proportionnelle à la distance qu'il a parcourue. Si l'on dispose de plusieurs antennes, une autre possibilité est d'analyser l'angle d'arrivée du signal. Enfin, on peut mesurer le temps d'arrivée du signal lorsqu'on connaît sa vitesse de propagation et qu'on est capable de déterminer de manière précise à quel instant il a été émis.

En se basant sur ces métriques, les systèmes de positionnement utilisent principalement quatre méthodes pour déterminer la position d'un équipement : l'angle d'arrivée

du signal (AOA), le temps d'arrivée du signal (TOA), la différence de temps d'arrivée (TDOA) et le *fingerprinting*. Ces différentes techniques sont présentées dans les prochaines sections. Une dernière méthode simpliste appelée Cell-ID peut encore être utilisée (cf. section 5.3.1). Afin d'illustrer ces différentes techniques, nous considèrerons à chaque fois le cas d'un réseau Wi-Fi dans lequel les points d'accès jouent le rôle de points références.

5.3.1 La méthode Cell-ID

Cette technique dite *à la cellule près* est la plus simple et la moins coûteuse. Les réseaux sans fil se composent d'un ensemble de stations de base (points d'accès) qui échangent des signaux avec les terminaux mobiles situés dans leurs zones de couverture encore appelées cellules. Il est donc aisé de déterminer de quelle station de base dépend un terminal. A l'aide de cette information recoupée avec les caractéristiques géographiques de la cellule, il est possible de déterminer approximativement la position d'un terminal mobile (quelques centaines de mètres en milieu urbain et jusqu'à plusieurs kilomètres en milieu rural lors de son application au sein d'un réseau cellulaire). Une représentation de cette méthode est donnée dans la figure 5.1.

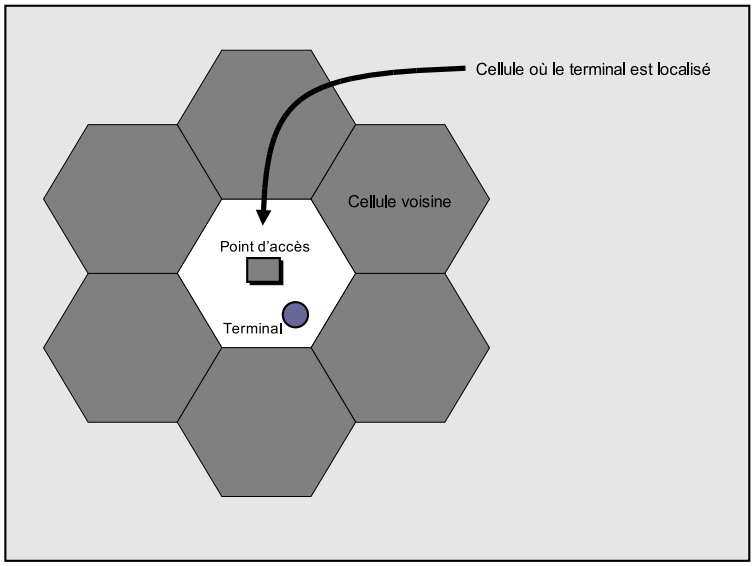


FIG. 5.1 – Méthode de géolocalisation Cell-ID

L'avantage de la méthode Cell-ID est qu'elle est compatible avec tous les terminaux mobiles existants et que pour fonctionner, elle nécessite seulement un aller-retour de signalisation avec le terminal. Par contre, la localisation de l'équipement n'est vraiment

pas précise, c'est pourquoi cette méthode est plus généralement utilisée comme méthode de dépannage (lorsque la méthode utilisée pour localiser les équipements n'est plus disponible).

5.3.2 L'angle d'arrivée

La technique AOA (*Angle Of Arrival*) se base sur un principe de triangulation (voir la figure 5.2). Dans cette méthode, les signaux émis par un terminal sont interceptés par deux points d'accès qui sont séparés par une distance R connue à l'avance. Chaque point d'accès mesure l'angle d'arrivée du signal émis par le terminal. En se basant sur les identités trigonométriques, il est alors possible de déterminer la longueur de la hauteur issue du terminal et par conséquent la position géographique de ce terminal (cf. figure 5.2). En pratique, on peut utiliser plus de 2 points d'accès de manière à augmenter la précision. Cette méthode nécessite l'utilisation d'antennes directionnelles ou de rangées d'antennes sur les points d'accès afin de mesurer les angles des signaux.

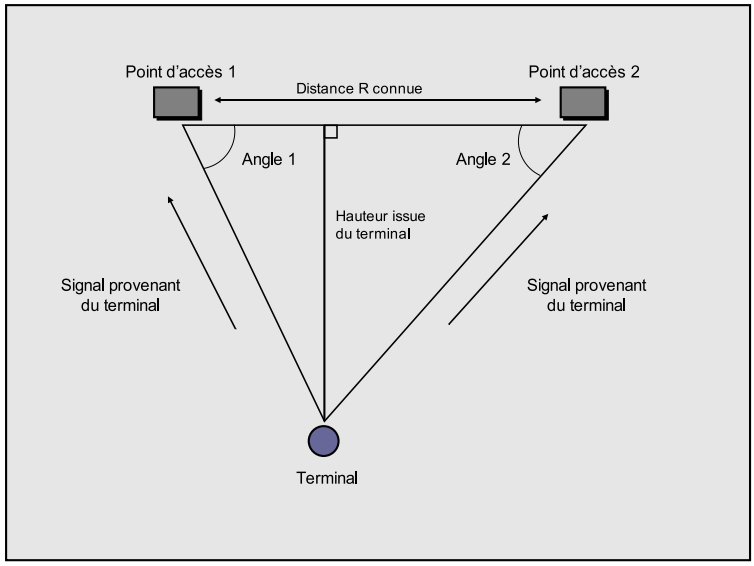


FIG. 5.2 – Méthode de géolocalisation basée sur l'angle d'arrivée

5.3.3 Le temps d'arrivée

La méthode TOA (*Time Of Arrival*) repose sur une technique de trilatération qui utilise l'intersection de cercles de distance pour déterminer la position d'un terminal. Le

temps de propagation d'un signal étant directement proportionnel à la distance traversée, il est possible d'obtenir un cercle centré sur l'émetteur dont le rayon constitue la distance qui sépare le terminal de cet émetteur. Lorsqu'on utilise au moins 3 points de référence, l'intersection des 3 cercles ainsi obtenus permet de déterminer la position exacte du terminal. Cette méthode est illustrée sur la figure 5.3.

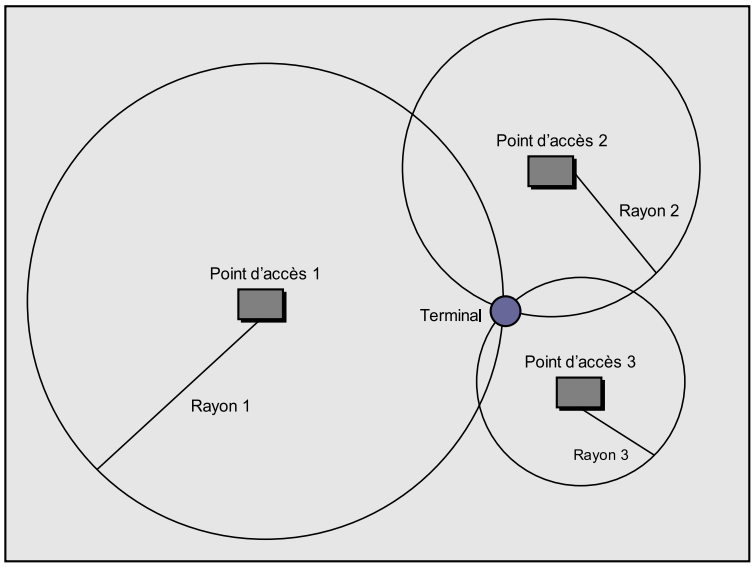


FIG. 5.3 – Méthode de géolocalisation basée sur le temps d'arrivée

La méthode TOA nécessite que les équipements possèdent des horloges précises et qu'elles soient toutes synchronisées entre elles. On peut relever ici que la méthode TOA est notamment utilisée dans le système GPS (*Global Positioning System* [31]).

5.3.4 La différence de temps d'arrivée

La méthode TDOA (*Time Difference of Arrival*), aussi connue sous le nom de positionnement hyperbolique, détermine la position d'un terminal en se basant sur une multilatération (voir la figure 5.4). Cette technique utilise la différence de temps mesurée plutôt que le temps absolu utilisé dans la méthode TOA. On calcule la différence de temps d'arrivée entre deux signaux provenant de deux points d'accès différents. Cette différence est ensuite convertie en une distance constante afin d'obtenir une hyperbole qui correspond à la position possible du terminal. L'équation de l'hyperbole caractérise cette distance constante. Pour déterminer une position, il faut donc deux paires d'émetteurs (i.e. au moins trois points références) en vue d'obtenir deux hyperboles dont l'in-

tersection donne la position du terminal. La précision d'un tel système dépend de la localisation des émetteurs et d'une synchronisation précise des horloges.

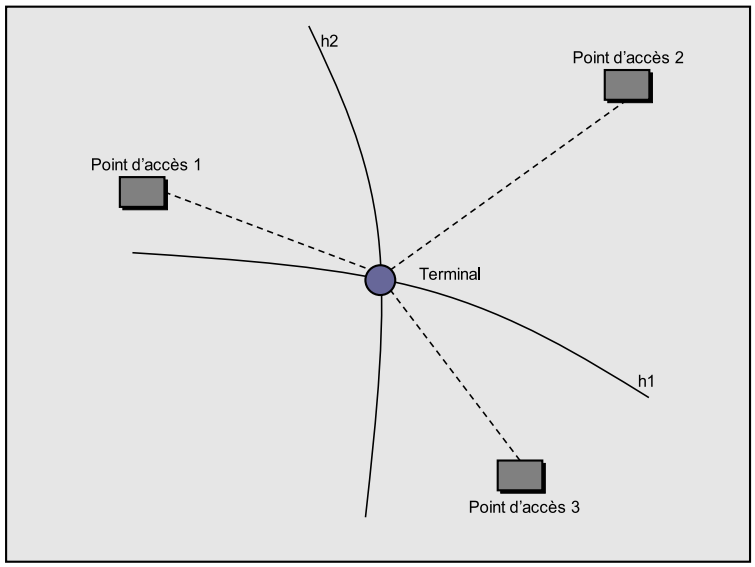


FIG. 5.4 – Méthode de géolocalisation basée sur la différence du temps d'arrivée

5.3.5 Le fingerprinting

La technique *fingerprinting* repose sur la similarité d'empreintes caractéristiques de signaux. Cette technique nécessite au préalable une phase de calibration pendant laquelle on enregistre, pour divers points références dont les positions sont connues, les caractéristiques des différents signaux reçus (généralement la puissance de réception). Ces différentes empreintes sont ensuite stockées dans une base de données. Lorsqu'un terminal mobile désire connaître sa position, on compare son empreinte actuelle avec celles qui sont stockées dans la base de données. La position calculée correspond à la position du point référence dont l'empreinte est la plus ressemblante. Il est également possible d'attribuer au terminal la position moyenne parmi plusieurs points références dont les empreintes sont proches de celle du terminal. Le principe de cette technique est représenté dans la figure 5.5.

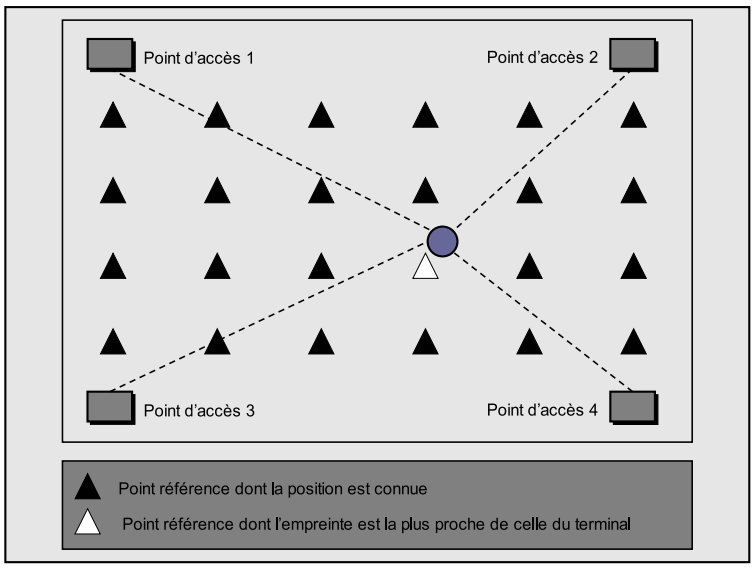


FIG. 5.5 – Méthode de gélocalisation basée sur des empreintes de signaux

5.4 Les systèmes de positionnement

Depuis quelques années, plusieurs systèmes de positionnement ont vu le jour. Dans cette section, nous allons détailler certains des systèmes les plus connus ou les plus efficaces. L'idée n'est pas de donner ici une liste exhaustive des systèmes existants mais plutôt d'illustrer l'application des techniques que nous venons de présenter.

5.4.1 Le système GPS

Dans les années 1960, les techniques spatiales ont progressé et l'utilisation de l'informatique a ouvert de nouvelles perspectives dans le domaine de la navigation terrestre, aérienne et maritime. Deux systèmes expérimentaux donnent naissance en 1973 au système satellitaire de positionnement américain NAVSTAR/GPS (*NAVigation System with Time And Ranging / Global Positioning System*) qui permet de donner à n'importe quel endroit du globe, une position et une vitesse.

Le système GPS [31] est constitué depuis 1994 de 24 satellites actifs regroupés sur 6 plans orbitaux situés à environ 20200 Km d'altitude et inclinés de 55 ° par rapport au plan équatorial. Il est ainsi possible de voir de 4 à 10 satellites de n'importe quel point du globe. Les satellites du réseau GPS embarquent chacun une horloge atomique de grande précision (environ 3 nanosecondes ce qui correspond à une dérive horaire dans

le temps de 1 seconde tous les 70000 ans). Une telle précision est nécessaire car les distances récepteur-satellite sont calculées à partir de la différence entre le temps auquel le satellite émet et celui auquel le récepteur reçoit (ce qui correspond à la méthode TOA vue précédemment).

Le GPS est un système entièrement passif, c'est-à-dire que les récepteurs GPS n'effectuent aucune transmission. Ils se contentent de recevoir les signaux émis par les satellites. Sans dégradation volontaire des Etats-Unis, il n'y a donc aucune restriction sur l'utilisation et la disponibilité des signaux pour les utilisateurs. Pour déterminer une position (exprimée sous forme de coordonnées géodésiques) en 2 dimensions, il est nécessaire de recevoir le signal provenant d'au moins 3 satellites différents et de 4 si on désire déterminer une position en 3 dimensions. La précision du système GPS est de 10 mètres, ce qui dans certaines applications n'est pas forcément suffisant. D'autre part, la fréquence de rafraîchissement des coordonnées est relativement faible (1 seconde), ce qui peut aussi être un inconvénient lors de déplacements à grande vitesse. Des techniques ont donc été présentées afin d'améliorer le système.

Le système D-GPS

Le DGPS (*Differential-GPS* [71]) est une technique d'optimisation du système GPS qui vise à réduire l'erreur due aux conditions atmosphériques. Le principe est d'utiliser deux récepteurs GPS ou plus, dont la position de l'un au moins est exacte.

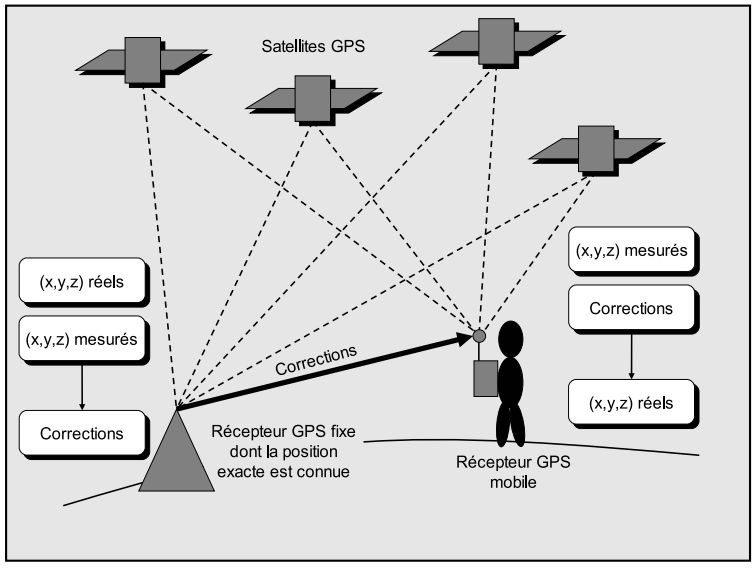


FIG. 5.6 – Une amélioration du système GPS, le D-GPS

Pour fonctionner correctement, il faut également que les récepteurs ne soient pas trop éloignés géographiquement et qu'ils puissent communiquer entre eux. Dès lors, celui dont la position est connue sera en mesure de calculer les erreurs d'orbites ainsi que les erreurs issues des conditions atmosphériques et des horloges des satellites. Les corrections sont ensuite envoyées aux autres récepteurs GPS de manière à augmenter la précision de ces derniers (voir figure 5.6). Le système D-GPS est précis à 1 mètre près.

Le système A-GPS

L'idée de base du système A-GPS (*Assisted-GPS* [26]) est d'établir un réseau de référence constitué de récepteurs GPS qui fonctionnent continuellement et qui ont une vue dégagée du ciel. Un serveur d'assistance récupère toutes les informations pertinentes provenant du réseau de référence. Ce serveur est aussi relié au réseau utilisé par le terminal mobile et fournit des données telles que la position approximative du terminal, la visibilité des satellites, les corrections d'horloge, etc. Le système A-GPS est notamment utilisé dans les environnements urbains, où la visibilité du ciel est souvent réduite en raison des habitations.

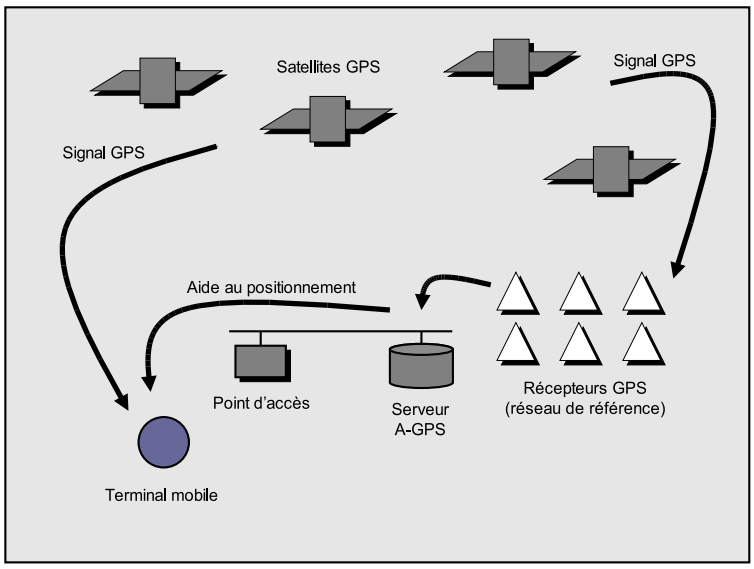


FIG. 5.7 – Une amélioration du système GPS, le A-GPS

Lorsque le terminal envoie une requête, les données d'assistance du réseau de référence sont envoyées au récepteur GPS du terminal mobile pour augmenter la précision ainsi que le démarrage du système. En effet, avec un récepteur GPS, il faut un certain temps au système (appelé *Time To Fix*) avant de pouvoir donner la position de l'équipe-

ment. Le GPS conventionnel met quelques minutes avant d'obtenir la première position alors qu'avec le système A-GPS, il est possible de réduire ce temps à 30 secondes. La précision du système est du même ordre qu'avec le système D-GPS (i.e. 1 mètre).

L'inconvénient majeur d'un système basé sur le GPS est le fait qu'il ne fonctionne pas à l'intérieur de bâtiments. Cela est dû au nombre de satellites visibles dans un bâtiment qui n'est pas suffisant pour proposer une localisation précise et fiable. En effet, dans un immeuble, un récepteur GPS ne peut pas recevoir les signaux issus des satellites ou alors très faiblement. C'est pourquoi bien que ce système soit très fiable et peu cher, d'autres systèmes ont été développés, notamment pour permettre une localisation à l'intérieur de bâtiments.

On peut également noter que d'autres systèmes de positionnement satellitaires existent ou sont en court de déploiement tels que le système GLONASS (*Global Navigation Satellite System*) qui constitue l'équivalent russe du système GPS et le projet européen Galileo qui devrait être utilisable en 2008.

5.4.2 Systèmes de localisation en intérieur

En vue d'offrir un service de localisation à l'intérieur de bâtiments, de nombreux systèmes ont vu le jour. Mais la géolocalisation en intérieur pose de nouveaux problèmes. Alors qu'avec les méthodes citées précédemment, deux ou trois points d'accès sont nécessaires pour déterminer une position avec précision dans de bonnes conditions, cela devient plus compliqué lorsqu'on essaie de les appliquer dans un bâtiment. Les principales contraintes de la géolocalisation en intérieur sont :

- les effets de réfraction et de réflexion des signaux.
- le coût des points d'accès.
- les interférences provoquées par la structure des murs et par les personnes. Elles peuvent dégrader les signaux et il est difficile de prévoir à quel point la dégradation peut être importante.

L'effet de *multipath* (le signal d'un même point d'accès peut venir de plusieurs directions lorsqu'il rebondit contre les murs) complique la géolocalisation basée sur le signal reçu. Beaucoup d'articles proposent des algorithmes pour calculer le nombre de murs traversés par le signal mais il est difficile d'obtenir un modèle efficace. Par la suite, nous allons présenter les systèmes de géolocalisation les plus utilisés à l'intérieur des bâtiments.

Active Badge

Le système *Active Badge* [106] a été l'un des premiers système de géolocalisation en intérieur. Basé sur une architecture propre, il utilise les signaux infrarouges. Dans ce système, un transmetteur infrarouge est placé sur chaque terminal et émet toutes les 15 secondes un signal en diffusion (i.e. broadcast) contenant un identifiant unique. Grâce au déploiement d'un réseau de capteurs dans le bâtiment, il est possible d'intercepter les signaux provenant des terminaux. Lorsqu'on identifie les capteurs qui perçoivent un signal particulier, on est en mesure de déterminer la position du terminal qui émet ce signal. Ce système n'est cependant pas très précis et est principalement conçu pour identifier les pièces occupées par les équipements.

Cricket

Le système de positionnement *Cricket* [84] dispose également d'une infrastructure dédiée et repose sur l'utilisation conjointe de signaux radio et d'ultrasons. Il est intéressant de constater que dans ce système, c'est le terminal qui détermine lui-même sa position, ce qui assure la confidentialité de cette information. Le calcul d'une position repose sur la méthode TDOA décrite précédemment. Dans ce système, chaque pièce dispose de couples d'émetteurs radio et ultrason. Pour une pièce donnée, les couples d'émetteurs sont placés de telle manière à ce qu'ils se situent à équidistance des murs. Périodiquement, un couple d'émetteurs envoie simultanément deux trames de contrôle (l'une par onde radio et l'autre par ultrason). Lorsqu'un terminal reçoit ces signaux, il mesure la différence de temps entre la réception des deux ondes (radio et ultrason). Grâce aux vitesses de propagation différentes, le terminal peut calculer la distance qui le sépare du couple émetteur. En utilisant plusieurs couples, il peut alors déterminer la pièce dans laquelle il se trouve.

Pour fonctionner, ce système demande que les trames de signalisation provenant de deux couples d'émetteurs différents ne s'interfèrent pas. L'envoi de ces trames est donc régulé par une méthode reposant sur l'aléatoire. Chaque couple choisit aléatoirement le délai avant l'envoi de ses prochaines trames de signalisation dans l'intervalle $[150; 350]$ millisecondes. Un autre problème de ce système est dû aux caractéristiques des signaux radio et ultrasons. En effet, les ondes radio se propagent plus loin que les ultrasons et peuvent passer à travers des obstacles tels que les murs alors que les ultrasons s'y reflètent. Un terminal peut donc prendre le signal radio de la pièce voisine comme étant celui de la pièce où il se trouve. Ce problème est contré par l'émission de longues trames de signalisation de façon à recevoir le signal ultrason tant qu'on reçoit le signal radio.

Cricket permet de localiser la pièce dans laquelle se trouve un terminal dans 95% des cas, même lorsque le terminal se déplace à 10 m/s. Nous sommes donc en présence d'un système de géolocalisation relativement peu cher, utilisant une architecture dédiée, et ne nécessitant pas de configuration minutieuse. Par contre, les terminaux mobiles doivent être équipés à la fois de récepteurs radio et de récepteurs ultrasons.

Cricket Compass

Le système *Cricket Compass* [85] est une amélioration du système précédent. Tout en gardant certains des avantages de *Cricket* (confidentialité, indépendance), il engendre des coûts plus importants mais augmente grandement la précision. En effet, la position du terminal mobile sera exprimée à l'aide de coordonnées relatives et non plus en indiquant uniquement la pièce où il se trouve. De plus, le système est capable de donner l'orientation des terminaux. Le calcul d'une position est toujours réalisé à l'aide de la méthode TDOA.

Dans ce système, les terminaux mobiles sont désormais équipés de cinq récepteurs ultrasons placés de manière à former un *V*. Pour déterminer sa position et son orientation, un terminal utilise les trames de signalisation provenant d'au moins quatre émetteurs différents qui sont directement dans sa ligne de mire. Le système *Cricket Compass* permet d'atteindre ainsi une précision de 6 centimètres dans de bonnes conditions (terminal mobile placé au centre de la pièce) mais il est moins robuste que le précédent système face aux réflexions des ultrasons sur les murs.

Active Bats

Le système *Active Bats* [75] est basé sur le système de localisation *Active Badges*. Comme dans les systèmes *Cricket* et *Cricket Compass*, il utilise la méthode TDOA sur la réception de signaux radio et d'ultrasons.

Dans ce système, les terminaux sont équipés d'émetteurs ultrasons. Afin d'éviter les problèmes d'interférences entre terminaux (émissions simultanées), on utilise un système de *polling*. Lorsqu'un terminal arrive dans la zone couverte par ce système, il doit s'enregistrer à l'aide d'un canal radio. Puis, les points d'accès envoient un signal radio en diffusion (ie. broadcast) avec un GID unique correspondant à un terminal spécifique. Lorsqu'un terminal reçoit ce signal et que le GID lui correspond, il envoie en diffusion un signal d'ultrasons. Le TDOA mesuré entre l'émission du signal radio et la réception du signal d'ultrasons permet de déterminer la position du terminal. *Active Bats* propose une précision inférieure à 9 centimètres.

Ce système nécessite le déploiement d'émetteurs radio et de récepteurs d'ultrasons dans le bâtiment. De leur côté, les terminaux doivent être équipés de récepteurs radio et d'émetteurs d'ultrasons, ce qui implique des coûts matériels assez élevés. En outre, le calcul de la position n'est pas effectué par le terminal lui-même mais par une machine spécifique du réseau, ce qui centralise le trafic vers cette dernière. Pour préserver la confidentialité de la position d'un terminal, il faut s'assurer que les communications avec cette machine sont sécurisées.

RADAR

Le système *RADAR* [13] utilise les réseaux sans fil de type 802.11. Comme une majorité d'autres systèmes de géolocalisation en intérieur [16, 47, 54, 82], *RADAR* se base sur une localisation de type *fingerprinting*. Une première phase, dite *offline* ou de calibrage permet de créer une base d'empreintes de puissance de signaux radio envoyés par les terminaux mobiles lorsqu'ils sont placés aux points références dont les positions sont connues, et interceptés par les points d'accès 802.11. Lors de la phase dite *online*, la puissance des signaux radio émis par les terminaux mobiles est mesurée par les points d'accès puis envoyée à la base de données qui détermine l'empreinte la plus ressemblante. On assimile ainsi la position du terminal à celle du point de référence dont l'empreinte est la plus proche.

La précision du système *RADAR*, et de tous les systèmes utilisant la méthode *fingerprinting*, dépend directement de la distance séparant chaque point référence. Plus on a de points références, plus le système est précis. En contrepartie, lors de la détermination d'une position, le temps nécessaire pour identifier l'empreinte la plus proche sera plus long. Il faut donc trouver un compromis entre la précision du système et le temps nécessaire pour connaître sa position. Dans le cas de *RADAR*, la précision est d'environ 2 mètres.

D'autres systèmes tels que *Place Lab* [54] ou *Ekahau* [30] proposent une légère variante dans laquelle les mesures des signaux radio sont effectuées par les terminaux mobiles. Néanmoins, quel que soit le niveau auquel les mesures sont effectuées, il faut toujours modifier un type d'équipement (soit les points d'accès, soit les terminaux mobiles). La méthode choisie dépend donc de l'objectif recherché. On peut également noter que ce ne sont pas les terminaux mobiles qui déterminent directement leur position mais une machine spécifique du réseau (sur laquelle est stockée la base d'empreintes). Par conséquent, le trafic est centralisé sur cette dernière et il faut donc s'assurer de la confidentialité des informations avec lesquelles elle travaille.

On pourra également remarquer que lorsque ce sont les terminaux mobiles qui effectuent les mesures, et que le système de positionnement s'intègre dans la même infrastructure 802.11 que celle utilisée pour véhiculer les données (e.g. *Ekahau* [30]), il est probable que de légères coupures se produisent dans les communications. En effet, les points d'accès des cellules voisines utilisent rarement les mêmes canaux radio. Cela oblige les terminaux à changer plusieurs fois de canal lors d'une mesure. D'après notre expertise, de tels changements peuvent générer des temps de latence non négligeables dans les communications courantes des terminaux. Ce problème peut cependant être facilement évité lorsque les mesures sont effectuées par les points d'accès. Ces derniers n'ont pas de contraintes énergétiques, c'est pourquoi on peut facilement leur ajouter une interface 802.11 dédiée aux mesures utiles pour le système de géolocalisation.

Le tableau 5.1 propose un récapitulatif des spécificités des différents systèmes de géolocalisation que nous avons présentés dans les sections précédentes.

Système	Type	Méthode utilisée	Signaux utilisés	Précision
GPS	extérieur (global)	TOA	ondes radio	10m
D-GPS	extérieur (grande échelle)	TOA + corrections	ondes radio	1m
A-GPS	extérieur (grande échelle)	TOA + corrections	ondes radio	1m
Active Badge	intérieur (local)	Equivalent Cell-ID	infrarouges	pièce
Cricket	intérieur (local)	TDOA	ondes radio + ultrasons	pièce
Cricket Compass	intérieur (local)	TDOA	ondes radio + ultrasons	6cm
Active Bats	intérieur (local)	TDOA	ondes radio + ultrasons	9cm
RADAR	int. / ext. (local)	fingerprinting	ondes radio	2m
Ekahau	int. / ext. (local)	fingerprinting	ondes radio	1m
Place Lab	int. / ext.[1]	fingerprinting	ondes radio	15-20m[2]

[1]Place Lab fonctionne aussi bien en local qu'à plus grande échelle
[2]lors d'expérimentations extérieures à grande échelle (voir [54])

TAB. 5.1 – Récapitulatif des spécificités des systèmes de géolocalisation présentés

5.5 Conclusion

Dans ce chapitre, nous avons présenté les différentes techniques qui permettent de déterminer la position d'un équipement en se basant sur la réception de signaux. Nous avons également détaillé divers systèmes de géolocalisation qui ont été proposés dans la littérature ou qui sont disponibles dans le commerce. On peut notamment relever le système GPS qui est un système global relativement peu cher. Ce système est entièrement passif (seul un récepteur est nécessaire) et ne demande aucune calibration particulière. Toutefois, il ne fonctionne pas à l'intérieur des bâtiments. Parmi les systèmes de géolocalisation en intérieur, il apparaît que les systèmes les plus performants déterminent la position d'un équipement au centimètre près. Cependant, ces systèmes nécessitent une architecture dédiée, ce qui génère des coûts matériels importants. D'autre part, la popularité des réseaux locaux sans fil de type Wi-Fi a fait émerger une nouvelle technique de géolocalisation particulièrement efficace dans les bâtiments : le *fingerprinting*. En raison de sa relative simplicité, cette technique semble s'imposer dans la plupart des systèmes actuels de géolocalisation en intérieur.

Nous avons pu constater que dans la majorité des cas, les informations de géolocalisation sont obtenues, ou du moins véhiculées à partir d'un réseau de communication. Dès lors, il est possible d'utiliser ces informations pour améliorer certains aspects de ces réseaux. Dans le chapitre suivant, nous allons exposer les différentes propositions disponibles dans la littérature sur l'adjonction d'informations de géolocalisation dans les réseaux de communication.

Chapitre 6

Usage de la géolocalisation dans les réseaux de communication

6.1 Introduction

Le développement des systèmes de géolocalisation a donné naissance à une nouvelle tendance dans le monde des réseaux de communication, qui consiste à tirer parti de la connaissance des positions des différents équipements de façon à améliorer certains aspects du réseau. On peut notamment relever que la famille des protocoles de routage multipoints s'est enrichie d'une nouvelle technique, le *geocasting* [51, 73, 92], qui s'appuie sur des informations de géolocalisation. Cette méthode est en quelque sorte une variante des protocoles de routage multicast traditionnels et permet de transmettre simultanément des paquets de données à plusieurs équipements situés dans une même zone géographique. Dans les réseaux *Ad Hoc*, les positions des équipements peuvent aussi être employées pour faciliter le routage des paquets de données entre les terminaux mobiles [32, 37, 48, 50]. D'autres propositions suggèrent d'utiliser les informations de géolocalisation afin d'améliorer les performances des handovers au sein d'une même technologie sans fil mais également entre différentes technologies sans fil. Dans le présent chapitre, nous allons essentiellement nous intéresser aux handovers assistés par des informations de géolocalisation, en présentant les différentes solutions disponibles dans la littérature.

6.2 La géolocalisation dans la gestion des handovers

Parmi les diverses propositions d'optimisation des handovers basées sur la position des équipements, ce sont majoritairement les réseaux cellulaires ainsi que le protocole Mobile IP qui ont bénéficié de la plus grande attention de la part de la communauté scientifique. En outre, d'autres techniques s'intéressent à la gestion des handovers inter-technologies. Ces derniers mettent en jeu des terminaux qui peuvent utiliser différentes technologies de communication. Au final, on ne recense que peu de solutions s'intéressant plus particulièrement à la mobilité de terminaux Wi-Fi IPv6.

6.2.1 Améliorations des réseaux cellulaires

Les premières solutions qui tirent parti d'informations de géolocalisation dans la gestion de la mobilité ont été proposées pour les réseaux cellulaires correspondant aux réseaux GSM, GPRS et UMTS. On peut notamment citer le projet CELLO (*Cellular Network Optimization based on Mobile Location*) [20, 38, 52, 53] qui occupe une place prépondérante dans ce domaine.

Dans l'architecture CELLO, deux nouveaux équipements font leur apparition sur le réseau : le MGIS (*Mobile network Geographic Information System*) et le LS (*Location Server*). Le LS permet de surveiller les déplacements des terminaux mobiles en enregistrant leurs positions actuelles. Le MGIS dispose de la carte des cellules, du nombre de terminaux mobiles attachés à chaque cellule, de la charge courante de chaque cellule, etc. Grâce aux informations fournies par ces deux équipements, les terminaux mobiles peuvent s'associer aux stations de bases (l'équivalent des points d'accès 802.11 pour les réseaux cellulaires) les mieux disposées à les accueillir. De plus, lors de l'utilisation de services à débit élevé, il est important que le réseau puisse prédire la station de base cible d'un handover en vue d'y réserver les ressources nécessaires. Cela peut également être réalisé à l'aide des informations dont disposent le MGIS et le LS. Les données provenant du MGIS peuvent être utilisées pour identifier les cellules voisines de celle où se trouve actuellement le terminal mobile. En analysant les données du MGIS pour ces cellules, il est possible de détecter les stations de base avec lesquelles les chances de succès du handover sont faibles (e.g. charge trop importante sur la station de base). En combinant ces informations avec celles qui sont contenues par le LS au sujet de la direction et de la vitesse d'un terminal, il est donc possible d'estimer la future station de base de ce terminal. En outre, l'utilisation du LS permet une gestion plus fine du déclenchement des handovers. Les auteurs proposent par exemple de retarder la procédure de handover lorsqu'un terminal mobile se déplace entre deux cellules adjacentes de façon à éviter des basculements incessants entre les deux stations de bases (effet *ping-pong*).

Néanmoins, ces propositions ne constituent au final qu'une présentation des éventuels bénéfices que peuvent apporter les informations de géolocalisation dans la gestion des handovers. Les méthodes suggérées ne sont que brièvement décrites, ce qui rend leur appréciation et leur évaluation difficiles. En revanche, d'autres solutions plus détaillées ont été proposées. Le seuil d'intensité du signal à partir duquel les handovers sont déclenchés peut être constamment adapté en fonction de la position des terminaux [105]. Cela permet notamment de réduire considérablement le nombre de handovers inutiles. Dans [41], le nombre et la durée des réservations de ressources nécessaires au maintien de la qualité de services lors de déplacements sont limités par l'utilisation de la direction et de la vitesse des terminaux.

6.2.2 Améliorations du protocole Mobile IP

Le protocole Mobile IP a lui aussi bénéficié de nombreuses propositions d'optimisation basées sur des informations de géolocalisation. Ces solutions se concentrent essentiellement sur des améliorations du modèle hiérarchique [95] et sur l'identification des futurs routeurs d'accès des terminaux mobiles. Dans cette section, nous allons considérer, comme cela est généralement le cas lorsqu'on aborde des optimisations de niveau 3, que les routeurs d'accès IP et les points d'accès sans fil (802.11 ou autres) ne forment qu'une seule et même entité.

Perfectionnement du modèle hiérarchique

Une première possibilité d'utilisation des localisations des équipements de niveau 3 propose de réduire le nombre de paquets perdus lors de déplacements intra-domaine [33, 34, 35]. L'idée principale consiste à réutiliser une architecture hiérarchique dont les positions géographiques des routeurs d'accès du domaine sont connues. Chaque routeur d'accès dispose d'une table de correspondance entre les positions des autres routeurs et leurs adresses IP. Ces tables sont maintenues à jour à l'aide de messages spécifiques qui permettent aux différents routeurs d'accès de communiquer leurs positions.

Lorsqu'un paquet de données arrive au niveau du routeur racine de l'arbre hiérarchique, il vérifie dans sa table de correspondance sur quelles branches de l'arbre il doit envoyer une copie de ce paquet afin d'atteindre à la fois le routeur d'accès courant du terminal mais également ses voisins géographiques. De même, chaque routeur se situant sur le trajet d'un de ces paquets va vérifier dans sa table sur quelles interfaces il doit transmettre une nouvelle copie du paquet. On se retrouve donc en quelque sorte avec un routage de type *geocasting* depuis le routeur racine (voir la figure 6.1). Lorsque des

paquets dupliqués arrivent sur les routeurs d'accès voisins, ces derniers les enregistrent pendant une certaine durée en vue de les transmettre au terminal après un éventuel handover. Un terminal mobile sera donc en mesure de recevoir son trafic dès son arrivée sur un nouveau lien sans avoir prévenu son agent mère (ou l'agent mère local dans le cas hiérarchique). Bien que cette technique limite effectivement le nombre de paquets perdus, la procédure de détection des nouveaux liens reste identique à celle décrite dans le protocole Mobile IP. En outre, cette solution peut augmenter significativement le trafic global du domaine, même lorsque les terminaux mobiles n'effectuent pas de procédures de handovers.

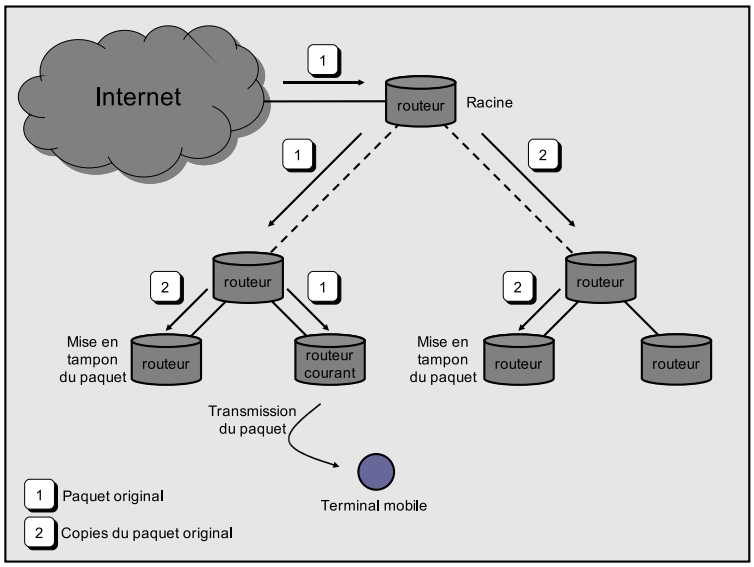


FIG. 6.1 – Duplication des paquets en fonction des positions géographiques des routeurs d'accès

Les auteurs de [33, 34, 35] proposent également d'optimiser les handovers inter-domaine du modèle hiérarchique à l'aide d'informations de géolocalisation. Lorsqu'un terminal arrive dans un nouveau domaine, il s'enregistre auprès de son nouvel agent mère local (i.e. le MAP dans le cas du protocole HMIPv6 [95]). Ce dernier doit théoriquement transmettre cet enregistrement à l'agent mère global (situé dans le réseau mère), afin de l'informer du déplacement du terminal dans un nouveau domaine. Or, cette étape peut s'avérer relativement longue lorsque l'agent mère local se trouve loin de l'agent mère global, ayant pour conséquence l'augmentation du temps de déconnexion de niveau 3. Pour palier ce problème, il est possible d'utiliser des informations de géolocalisation de façon à ce que l'agent mère local puisse calculer la distance géographique qui le sépare de l'agent mère global ainsi que celle qui le sépare du précédent agent mère local du terminal. Suivant la distance la plus courte, il enverra l'enregistrement soit à l'agent mère global, soit à l'ancien agent mère local. Cette deuxième possibilité

introduit une nouvelle redirection dans l'acheminement des paquets de données : les paquets provenant de l'agent mère global seront interceptés par l'ancien agent mère local qui les retransmettra à son tour au nouvel agent mère local (voir la figure 6.2).

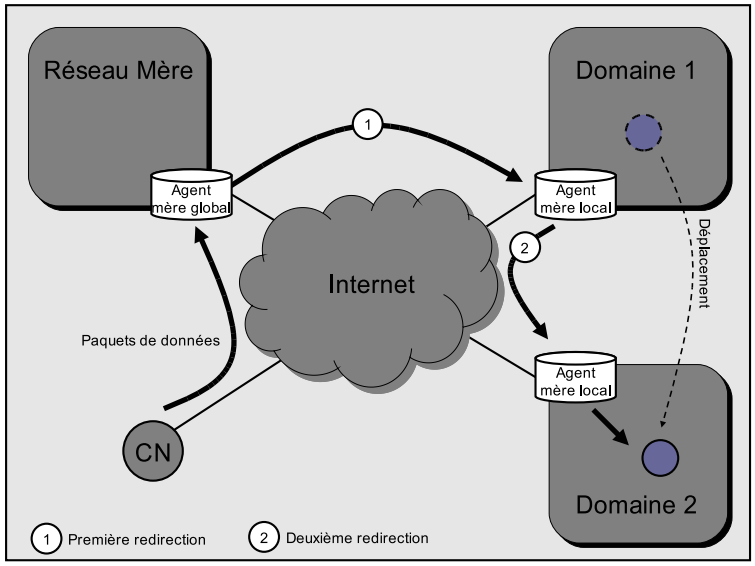


FIG. 6.2 – Enregistrement auprès du précédent agent mère local

On peut cependant relever que la distance géographique entre deux équipements n'est pas forcément équivalente à la distance réseau (nombre de sauts ou délai d'acheminement des paquets) entre ces deux entités. Considérons par exemple que l'actuel agent mère local soit géographiquement proche de l'ancien agent mère local mais que le délai entre ces deux entités soit relativement important. Considérons également que l'actuel agent mère local et que l'agent mère global sont géographiquement éloignés alors que le délai entre ces deux entité est court. Dans le cas présent, il vaut mieux envoyer l'enregistrement (BU) à l'agent mère global et non à l'ancien agent mère local. Cette optimisation concernant les handovers inter-domaine n'est donc pas satisfaisante.

Identification du prochain routeur d'accès

De nombreuses techniques relativement similaires ont également été proposées dans le but de déterminer, grâce aux informations de géolocalisation, les futurs routeurs d'accès des terminaux mobiles. Cette anticipation permet notamment la transmission d'une copie des paquets auprès des prochains routeurs d'accès afin de limiter le nombre de paquets perdus. Dans certaines solutions, elle permet également aux terminaux mobiles de réaliser le handover de niveau 3 avant celui de niveau 2.

Une première proposition allant dans ce sens repose sur la position géographique des routeurs d'accès et des terminaux mobiles [14]. Chaque routeur d'accès possède également une table de correspondance locale entre les adresses IP et les positions géographiques des routeurs voisins. Périodiquement, chaque terminal mobile envoie sa position courante à son routeur d'accès. A la réception d'une nouvelle position d'un terminal, le routeur d'accès mesure la distance qui le sépare de ce terminal. Lorsque cette distance dépasse un certain seuil prédéfini, il conclut qu'un handover est imminent et recherche dans sa table de correspondance le routeur d'accès le plus proche géographiquement du terminal. Le routeur d'accès sélectionné sera identifié comme étant le futur routeur d'accès du terminal (NAR). Dès lors, le routeur d'accès courant initie la transmission vers le NAR d'une copie des paquets destinés au terminal. Il lui indique également d'augmenter la fréquence d'émission des messages RA pendant la procédure de handover afin de permettre au terminal de détecter plus rapidement son changement de sous-réseau. Dès la transmission de la mise à jour de la nouvelle adresse temporaire vers l'agent mère (BU), le NAR répond immédiatement avec un acquittement de manière à autoriser l'utilisation temporaire de la nouvelle adresse. Cela permet notamment de transmettre au terminal les éventuels paquets mis en attente sur le NAR. Cette technique améliore le temps de latence engendré par un handover de niveau 3 sans augmentation notoire de la charge du réseau.

La précédente méthode reste toutefois fortement dépendante du mécanisme de détection des nouveaux liens défini par le protocole Mobile IP. Même avec une fréquence d'émission des RA élevée, cette procédure peut toujours augmenter le temps total de déconnexion engendré par un handover. Certaines propositions suggèrent alors de réaliser le handover de niveau 3 avant celui de niveau 2. Cela revient à pré-enregistrer la future adresse temporaire auprès de l'agent mère alors que le terminal est toujours associé à son routeur d'accès courant (voir la figure 6.3). Ces enregistrements anticipés déclenchent la transmission simultanée des paquets de données vers la localisation actuelle et future du terminal à la manière de [56]. Toutes les méthodes présentées ci-dessous diffèrent donc essentiellement au niveau de la méthode d'anticipation du prochain routeur d'accès des terminaux.

Dans [12], les auteurs utilisent des capteurs sans fil permettant de détecter les mouvements des terminaux mobiles. Ces capteurs sont systématiquement placés au bord des zones de couverture des routeurs d'accès de manière à détecter les mouvements entre deux sous-réseaux spécifiques. Lorsqu'un capteur détecte qu'un terminal s'apprête à se déplacer vers un autre sous-réseau, le routeur d'accès courant du terminal lui transmet les paramètres de son futur lien IPv6. Par conséquent, le terminal peut pré-configurer sa future adresse temporaire et la pré-enregistrer auprès de son agent mère. A la réception d'une requête d'enregistrement préliminaire, l'agent mère transmet le trafic destiné au terminal vers ses deux adresses simultanément.

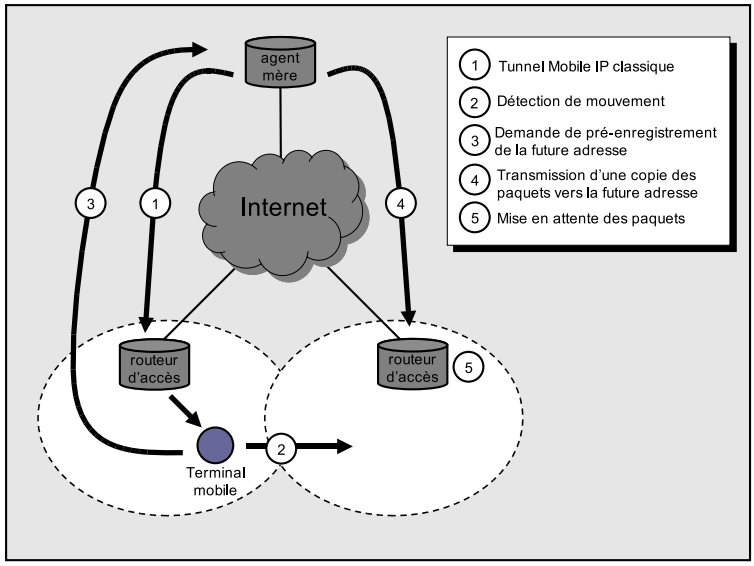


FIG. 6.3 – Schéma général d'enregistrement préliminaire d'adresse

En se basant sur la trajectoire des terminaux mobiles il est possible d'approfondir la solution précédente en réalisant plusieurs pré-enregistrements simultanément [24]. Les trajectoires sont ici obtenues à partir de positions GPS ou déduites de l'environnement dans lequel le terminal évolue (e.g. déplacement sur une autoroute). Cette solution réutilise également une architecture hiérarchique et permet d'éviter la transmission de copies de paquets de données. Dès son arrivée dans un nouveau domaine, un terminal envoie à l'agent mère local une demande anticipée de pré-enregistrement pour différentes adresses qui correspondent aux sous-réseaux du domaine qu'il estime traverser. A la réception d'une telle requête, l'agent mère local sauvegarde les futures configurations du terminal. Lorsque le terminal est plus proche géographiquement du prochain routeur d'accès que du courant, il prévient l'agent mère local qu'il va changer de sous-réseau et lui demande de transmettre les paquets de données vers l'une des adresses préalablement enregistrées. Suivant le délai estimé pour joindre l'agent mère local, le terminal retarde le déclenchement du handover de niveau 2 pour être certain de recevoir les derniers paquets envoyés vers sa précédente adresse. Dès la fin du handover de niveau 2, le terminal peut donc directement communiquer et se voit retransmettre les éventuels paquets mis en attente sur son nouveau routeur d'accès alors qu'il était en procédure de handover.

Une autre solution appelée SMIP [40] propose une approche légèrement différente et s'appuie à la fois sur les protocoles FMIPv6 et HMIPv6 que nous avons déjà présentés dans la section 2.6. Dans cette solution, une entité réseau appelée le DE (*Decision Engine*) est dédiée à la supervision des déplacements des terminaux mobiles. Ces der-

niers surveillent constamment la qualité du lien radio comme cela est suggéré dans le protocole FMIPv6. Lorsque la qualité du signal descend sous un seuil prédéfini, le terminal en déduit qu'il s'approche du bord de la zone de couverture de son point d'accès courant. A cette occasion, il envoie périodiquement au DE les intensités de signaux qu'il reçoit depuis les routeurs d'accès voisins. Grâce à ces informations, le DE peut calculer la position géographique du terminal (méthode de trilatération utilisant les positions des routeurs d'accès comme points références). Dès l'obtention de 3 positions, le DE peut identifier le prochain routeur d'accès du terminal et estimer son modèle de déplacement parmi 3 modèles prédéfinis : aléatoire, stationnaire et linéaire (voir la figure 6.4). Suivant le modèle de déplacement retenu, le DE indique au terminal et aux routeurs d'accès concernés les différentes stratégies et informations à utiliser pour améliorer le handover imminent.

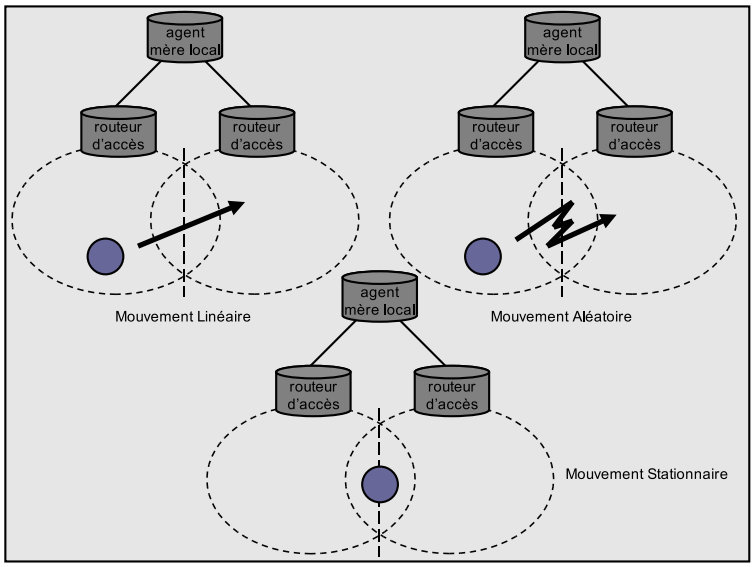


FIG. 6.4 – Modèle de déplacements pris en compte dans SMIP

Le cas linéaire correspond au cas classique, dans lequel il n'y a pas d'ambiguïté. Le DE indique au terminal son prochain routeur et demande à l'agent mère local de dupliquer le trafic destiné au terminal vers le routeur d'accès courant et vers le futur routeur d'accès. Dans le cas stationnaire, le DE demande au terminal d'effectuer plusieurs associations de manière à utiliser plusieurs adresses temporaires simultanément. Chaque adresse correspond à un sous-réseau vers lequel le terminal est susceptible de se déplacer. Dans le cas aléatoire, le routeur d'accès courant et le futur routeur d'accès sont positionnés en mode anticipation, c'est-à-dire qu'ils doivent maintenir leurs associations avec le terminal de telle sorte que ce dernier puisse se déplacer librement entre les deux sous-réseaux sans aucune reconfiguration. Au final, nous pouvons relever que dans le

protocole SMIP, toute l'intelligence réside dans le réseau et plus particulièrement dans le DE qui prend toutes les décisions relatives au handover.

6.2.3 Handovers inter-technologie

Les informations de géolocalisation peuvent également être utilisées pour assister les handovers inter-technologie. Ces derniers correspondent à des changements de technologie d'accès alors que le terminal mobile est en cours de communication. Ils sont généralement référencés par les termes *handovers verticaux* par opposition aux *handovers horizontaux* qui correspondent aux déplacements à travers des points d'accès utilisant la même technologie sans fil.

Le cas majoritairement abordé dans la littérature introduit la cohabitation d'un réseau cellulaire (GSM, GPRS ou UMTS) avec des réseaux Wi-Fi. Dans [55], les auteurs définissent trois scénarii possibles : déplacement du réseau cellulaire vers un réseau Wi-Fi (e.g. utilisateur arrivant à son bureau), déplacement d'un réseau Wi-Fi vers le réseau cellulaire (e.g. utilisateur quittant son bureau) et déplacement passant à travers un réseau Wi-Fi (i.e. combinaison des deux premiers scénarii). En vue d'éviter les recherches inutiles de réseaux Wi-Fi (scénarii 1 et 3) coûteuses en consommation d'énergie, et pour maximiser le temps de connexion aux réseaux Wi-Fi (scénario 2), les auteurs proposent un algorithme à base de logique floue tirant parti de divers paramètres, dont la position et la vitesse des terminaux mobiles. Néanmoins, leurs premiers résultats semblent indiquer que dans les cas simples (trajectoire rectiligne), les informations de géolocalisation n'apportent aucune valeur ajoutée par rapport aux autres métriques (e.g. intensité du signal) utilisées dans l'algorithme de logique floue.

Une autre approche de la gestion des handovers inter-technologie s'appuie sur les trajectoires des terminaux mobiles [79]. Une entité réseau enregistre les déplacements des terminaux mobiles afin de déterminer s'ils sont proches d'une zone couverte par un réseau Wi-Fi. En se basant sur la trajectoire, le type de trafic et la cartographie des points d'accès, cette entité détermine si un handover du réseau cellulaire vers le réseau Wi-Fi est judicieux. Par contre, aucun mécanisme n'est mis en place pour optimiser l'association au réseau Wi-Fi. Cependant, les auteurs suggèrent tout de même de transmettre les paquets de données en utilisant les deux technologies, le temps de terminer la procédure de handover.

6.3 Conclusion

Dans ce chapitre, nous avons présenté les différentes utilisations d'informations de géolocalisation dans les réseaux de communication disponibles dans la littérature. Nous nous sommes principalement intéressés à la gestion des handovers dans les réseaux sans fil. Il ressort de cette étude que les solutions envisagées sont rarement détaillées et que c'est majoritairement le protocole Mobile IP qui a bénéficié des algorithmes les plus intéressants. Il est notamment possible de déterminer à l'avance le prochain routeur d'accès d'un terminal en fonction de sa position et/ou trajectoire, afin de réaliser diverses opérations qui permettent d'optimiser le handover de niveau 3.

Toutefois, on constate que peu de propositions tiennent compte des handovers de niveau 2 dans les réseaux Wi-Fi. On relèvera tout de même la solution présentée dans [102] qui, en plus des informations de topologie classiques (adjacence entre les points d'accès), mentionne également l'intérêt d'utiliser des informations de géolocalisation. Dans cette approche, un serveur dédié possède tous les paramètres des entités réseaux dont il a la charge et envoie ces informations aux terminaux mobiles qui déterminent seuls leurs prochains points d'accès, en fonction de leurs positions et directions. Néanmoins, ni la sélection des prochains points d'accès, ni la procédure du handover de niveau 2 ne sont détaillées, ce qui rend difficile l'appréciation de cette solution. De plus, il est peu probable que les différents opérateurs réseaux transmettent de la sorte les positions physiques de leurs équipements.

A la vue de ces différentes propositions, il nous est apparu évident qu'on pouvait encore pousser plus loin l'utilisation d'informations de géolocalisation dans la gestion des handovers au sein des réseaux de nouvelle génération. En fonction des positions des terminaux mobiles et des points d'accès environnants, le réseau devrait être capable de sélectionner à l'avance le prochain point d'accès des terminaux afin de leur transmettre les informations nécessaires à la réalisation d'un handover rapide (aussi bien de niveau 2 que de niveau 3). Comme le mentionne [83], l'utilisation d'informations de géolocalisation devrait également permettre de limiter le nombre de procédures de handover en choisissant en priorité les points d'accès offrant une vaste zone de couverture. Dans les chapitres suivants, nous allons exposer nos différentes contributions allant dans ce sens.

Contributions à l'optimisation des handovers assistée par géolocalisation dans les réseaux Wi-Fi IPv6

Chapitre 7

Le protocole SHAPE

7.1 Introduction

A la suite de notre étude préliminaire portant sur les optimisations des handovers de niveau 2 dans les réseaux Wi-Fi, nous avons débuté la spécification et l'implémentation d'un nouveau protocole appelé SHAPE (*Seamless Handovers Assisted by Position Estimation* [65]). Ce protocole constitue notre première contribution au sein des propositions utilisant des informations de géolocalisation afin d'améliorer les handovers. Contrairement à la majorité des solutions présentées dans le chapitre précédent, le protocole SHAPE vise à réduire le temps de latence des handovers, aussi bien de niveau 2 dans les réseaux Wi-Fi que de niveau 3 dans les réseaux IPv6. Comme son nom le laisse supposer, ce protocole s'appuie sur un système de géolocalisation pour déterminer les futurs points d'accès des terminaux en fonction de leurs positions. Lors de la phase de validation du protocole SHAPE, nous nous sommes basés sur le système de géolocalisation GPS, en raison de sa facilité d'utilisation, mais tout autre système de géolocalisation disposant de caractéristiques similaires (cf. chapitre 5) pourrait être amené à le remplacer sans générer de modifications notoires dans le protocole.

Les prochaines sections présenteront dans un premier temps les différents mécanismes d'optimisation apportés par le protocole SHAPE. Nous détaillerons ensuite son implémentation qui se base sur le nouveau démon Mobile IPv6 pour GNU/Linux [74]. A la suite de cette implémentation, nous avons réalisé une première évaluation de performances à travers deux scénarii de tests. Cette analyse préliminaire a donné lieu à une évaluation plus complète [59] dans laquelle nous avons effectué un comparatif entre le protocole SHAPE et le protocole FMIPv6 qui bénéficie d'une implémentation libre

[45]. A titre de référence, ce comparatif intègre la procédure de handover standard telle qu'elle est décrite dans la norme IEEE 802.11 et dans le protocole MIPv6.

7.2 Description du protocole

L'idée principale du protocole SHAPE repose sur l'utilisation de la position des terminaux mobiles comme métrique pour améliorer les handovers de niveau 2 et de niveau 3 se produisant dans les réseaux Wi-Fi et IPv6. Ce protocole se focalise essentiellement sur la réduction du temps nécessaire à la phase de découverte du niveau 2 et au temps de détection du nouveau lien IPv6 du niveau 3. Comme nous l'avons vu dans la section 2.5, ce sont principalement les mécanismes mis en place lors de ces phases qui sont responsables des délais engendrés par une procédure de handover.

Notre solution se base sur le protocole MIPv6 et réutilise une architecture hiérarchique afin de minimiser le temps d'enregistrement des adresses temporaires auprès de l'agent mère. Nous pouvons également relever que les handovers sont ici entièrement contrôlés par le réseau.

7.2.1 Le contrôleur de mobilité

Le protocole SHAPE introduit une nouvelle entité réseau appelée le *contrôleur de mobilité*. Situé à l'intérieur d'un domaine réseau, il est destiné à gérer les déplacements des terminaux mobiles au sein de son domaine. Plus précisément, c'est le contrôleur de mobilité qui va sélectionner les futurs points d'accès des terminaux mobiles en fonction des distances géographiques entre les équipements.

Le contrôleur de mobilité maintient une base de données contenant les différents paramètres des équipements fixes du domaine. Les informations enregistrées concernent principalement les points d'accès Wi-Fi et les routeurs d'accès IPv6. Plus précisément, la base de données contient l'adresse MAC, le SSID, le canal radio et la position géographique (en termes de latitude et longitude) de chaque point d'accès du domaine. En outre, le contrôleur dispose de la liste d'adjacence entre tous les points d'accès. Notons qu'un identifiant unique est attribué à chaque point d'accès. Le tableau 7.1 donne un exemple des paramètres de niveau 2 contenus dans la base de données.

ID	Adresse MAC	SSID	Canal radio	Position	Portée radio	Adjacence
1	A:B:C:D:E:F	TEST1	1	(x1,y1)	50	$\{2\}$
2	A:B:C:F:E:D	TEST2	6	(x2,y2)	40	$\{1;3\}$
3	A:B:C:D:F:E	TEST3	11	(x3,y3)	60	$\{2\}$
...	...	...	...	...	...	...

TAB. 7.1 – Paramètres de niveau 2 enregistrés par le contrôleur de mobilité

En plus des informations de niveau 2, la base de données contient également le préfixe IPv6 et l'adresse lien local du routeur par défaut de tous les sous-réseaux IPv6 dans lesquels les points d'accès sont situés. Le tableau 7.2 propose un exemple des informations de niveau 3 contenues dans la base de données. Dans la version actuelle du protocole, toutes ces informations sont configurées statiquement sur le contrôleur et sont gérées par l'entité administrative en charge du réseau.

ID	Adresse lien local	Préfixe IPv6	Points d'accès sur le lien
1	f080::X	2001:db8:0:f02f::/64	$\{2\}$
2	f080::Y	2001:db8:0:f000::/64	$\{1;3\}$
3	f080::Z	2001:db8:0:f010::/64	$\{6;8;10\}$
...	...	...	...

TAB. 7.2 – Paramètres de niveau 3 enregistrés par le contrôleur de mobilité

7.2.2 Mise à jour du contrôleur

Lorsqu'un terminal se déplace, il envoie au contrôleur de mobilité diverses informations en vue d'obtenir éventuellement les paramètres de son prochain point d'accès. Dès l'obtention de ses nouvelles coordonnées (e.g. toutes les secondes avec le système GPS), le terminal s'assure dans un premier temps qu'il s'est déplacé, en mesurant la distance qui le sépare de son ancienne position. Cette vérification permet notamment de réduire le nombre de messages envoyés au contrôleur de mobilité. Pour calculer la distance entre deux points géographiques (exprimés sous formes de coordonnées géodésiques), nous utilisons la formule d'Haversine [94]. Cette formule fait l'hypothèse d'une terre sphérique mais reste particulièrement bien adaptée pour des calculs numériques même à de courtes distances.

Notons respectivement $(lat_1, long_1)$ et $(lat_2, long_2)$ les coordonnées de l'ancienne et de la nouvelle position d'un terminal mobile. Notons également Δ_{lat} la différence entre les latitudes et Δ_{long} la différence entre les longitudes. Tous les angles sont exprimés en

radian et G correspond au rayon de la terre avec $G = 6371km$. La distance d entre deux points peut donc être calculée par la formule :

$$haversin\left(\frac{d}{G}\right) = haversin(\Delta_{lat}) + \cos(lat_1) \times \cos(lat_2) \times haversin(\Delta_{long})$$

où la fonction d'Haversine est donnée par :

$$haversin(\delta) = \sin^2\left(\frac{\delta}{2}\right)$$

Soit $h = haversin(d/G)$. Nous pouvons alors déterminer la distance d en appliquant simplement l'inverse de la fonction d'Haversine ou en utilisant la fonction arcsin (inverse de la fonction sinus) :

$$d = G \times haversin^{-1}(h) = 2G \times \arcsin(\sqrt{h})$$

Lorsque d est supérieure à 1 mètre, on considère que le terminal mobile s'est déplacé. Dans ce cas, il doit envoyer au contrôleur de mobilité un message LU (*Location Update*). Ce message contient la position courante du terminal et l'identité de son point d'accès courant. A la réception d'un message LU, le contrôleur de mobilité initie l'algorithme de sélection du prochain point d'accès.

7.2.3 Sélection des prochains points d'accès

Dès réception d'un message LU par le contrôleur de mobilité, la première étape consiste à calculer la distance séparant le terminal émetteur de son point d'accès courant. Nous avons défini R comme étant la distance maximale entre un terminal et son point d'accès courant pendant laquelle le terminal mobile est encore bien couvert. En se basant sur les mesures effectuées dans [69], nous avons positionné R à 50% de la portée maximale du point d'accès courant du terminal. Le paramètre R va donc varier en fonction des capacités des points d'accès.

Lorsque la distance entre un terminal et son point d'accès est strictement supérieure à R, cela signifie que le terminal s'approche du bord de la zone de couverture de son

point d'accès. Dès lors, le contrôleur de mobilité conclut qu'un handover est imminent et détermine le prochain point d'accès du terminal. Parmi les points d'accès des cellules voisines (identifiés grâce à la liste d'adjacence contenue dans la base de données), le contrôleur de mobilité va sélectionner celui dont la position géographique est la plus proche de celle du terminal. Lorsque le point d'accès sélectionné et le point d'accès courant du terminal sont différents, le contrôleur de mobilité envoie un message HI (*Handover Initiate*) au terminal. Ce message contient l'adresse MAC, le SSID et le canal radio du point d'accès sélectionné par le contrôleur. Quand le futur point d'accès est situé dans un nouveau sous-réseau IPv6, le message HI inclut également le préfixe IPv6 et l'adresse lien local du routeur par défaut qui correspondent à ce nouveau lien. La sélection des prochains points d'accès est illustrée sur la figure 7.1.

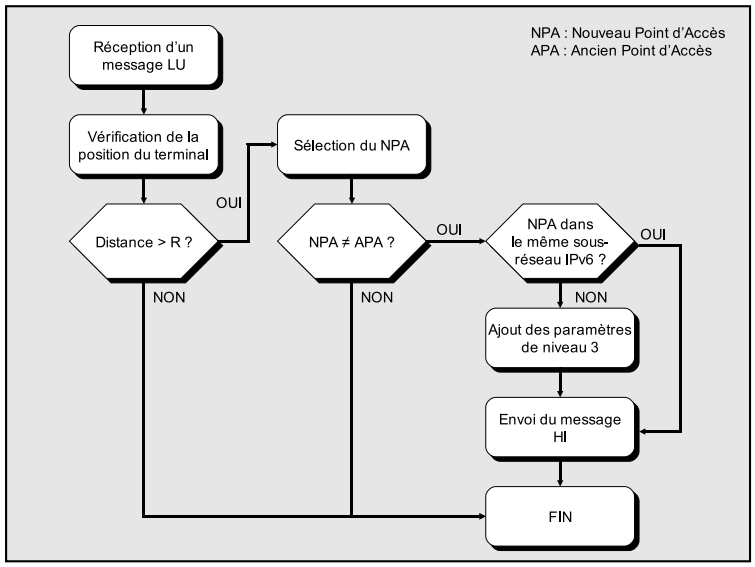


FIG. 7.1 – Sélection des futurs points d'accès par le contrôleur de mobilité

7.2.4 Gestion des Handovers

Lorsqu'un terminal mobile reçoit un message HI, il déclenche une procédure de handover et essaie de s'associer au point d'accès indiqué par le contrôleur de mobilité. Pour ce faire, il utilise les informations contenues dans le message HI de façon à envoyer une *Probe Request* directement sur le bon canal radio et vers le bon SSID. Dès la réception d'une *Probe Response* provenant du point d'accès visé (identifié grâce à son adresse MAC), le terminal passe immédiatement à la phase d'authentification. La phase de découverte est donc uniquement constituée d'un échange *Probe Request* / *Probe Response* avec le point d'accès sélectionné par le contrôleur de mobilité, ce qui réduit fortement

le temps de latence engendré par cette étape. Les paramètres *MinChannelTime* et *MaxChannelTime* ne sont désormais utilisés que dans les cas d'erreurs.

A la fin du handover de niveau 2, le terminal vérifie si le message HI contient également des paramètres de niveau 3 indiquant qu'il s'est déplacé dans un nouveau sous-réseau IPv6. La détection des nouveaux liens IPv6 n'est donc plus basée sur la réception des messages RA. Dès la fin de l'association de niveau 2, le terminal peut utiliser le préfixe IPv6 et l'adresse du routeur par défaut inclus dans le message HI pour réaliser son autoconfiguration d'adresse sans état. Couplé au mécanisme ODAD que nous avons présenté dans la section 2.5.2, cette optimisation permet d'envoyer directement un BU à l'agent mère local et réduit par conséquent le temps de latence du handover de niveau 3. La figure 7.2 illustre la procédure de handover lors de l'utilisation du protocole SHAPE.

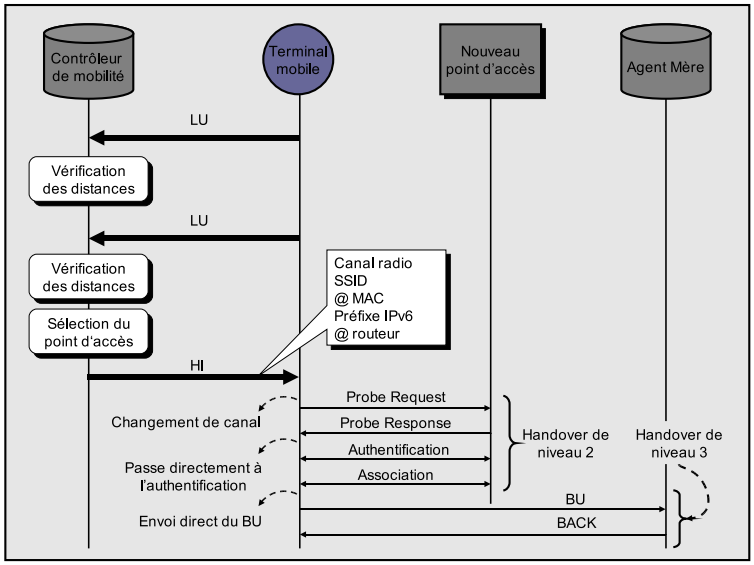


FIG. 7.2 – Procédure de handover dans le protocole SHAPE

7.2.5 Cas d'erreurs

Plusieurs cas d'erreurs peuvent survenir lors de l'utilisation du protocole SHAPE. Dans un premier temps, les positions calculées par le système de géolocalisation contiennent une certaine marge d'erreur (e.g. 10 mètres dans le système GPS) qui peut avoir une influence lors de la sélection d'un nouveau point d'accès. En effet, le contrôleur de mobilité peut sélectionner un point d'accès qui n'est pas à portée radio du terminal ou peut déclencher une procédure de handover alors que le terminal mobile n'a pas réellement franchi le seuil R. Lorsque le terminal n'a pas reçu de *Probe Response* du point

d'accès ciblé après *MinChannelTime*, il considère qu'il n'est pas à portée radio de ce point d'accès. S'il a reçu d'autres réponses pendant cette attente, il tente de s'associer aux points d'accès correspondants. Dans le cas où il n'aurait reçu aucune réponse sur ce canal particulier, il passe au canal suivant et débute une procédure standard de handover. A la fin d'une telle association, les éventuels paramètres de niveau 3 disponibles dans le message HI sont devenus inutiles étant donné que le terminal ne s'est pas associé au point d'accès prévu. Dès lors, le handover de niveau 3 qui peut suivre sera réalisé à l'aide des mécanismes de base du protocole MIPv6.

D'autre part, il est possible qu'un terminal ne soit plus en mesure de connaître sa position (e.g. le système de géolocalisation ne fonctionne plus) ou que le contrôleur de mobilité ne soit plus joignable (e.g. le contrôleur est tombé en panne). Dans les deux cas, le terminal mobile ne recevra jamais de messages HI. Il restera associé donc à son point d'accès courant jusqu'à ce qu'il sorte de la cellule radio. A ce moment, il effectuera une procédure de handover standard.

7.3 Implémentation

Dans l'optique d'évaluer cette première proposition, nous l'avons implémentée dans un système GNU/Linux. Pour ce faire, nous nous sommes basés sur la nouvelle implémentation du protocole MIPv6 pour les système d'exploitation GNU/Linux (MIPL-2 [74]) et sur le pilote libre de cartes sans fil MADWiFi [21]. Concernant le calcul des positions géographiques des terminaux, nous avons utilisé dans cette évaluation le système de géolocalisation GPS, en raison de sa relative facilité d'utilisation et du faible coût des récepteurs GPS dans le commerce. Nous rappelons que le système GPS dispose d'une précision de 10 mètres et que la fréquence de mise à jour des coordonnées est de 1 seconde (cf. chapitre 5).

Afin d'intégrer nos optimisations de niveau 2, nous avons dû légèrement modifier le pilote de périphérique MADWiFi. Ce pilote est principalement utilisé pour les périphériques basés sur des puces Atheros qui fonctionnent sans firmware. MADWiFi est un pilote entièrement logiciel (absence de firmware), ce qui permet de remanier son comportement. Seule une partie du pilote est fournie sous forme binaire de façon à respecter les règles de normalisation des fréquences radio. Par défaut, le pilote MADWiFi réinitialise le périphérique sans fil à chaque modification d'un paramètre de configuration (SSID, canal radio, etc). Etant donné que chaque réinitialisation engendre un certain délai, nous avons dans un premier temps modifié cette procédure pour que seul le changement de canal radio réinitialise le périphérique. A la réception d'un message HI, le terminal configure d'abord le nouveau SSID, puis le nouveau canal radio ce qui réinitia-

lise le périphérique sans fil. Notre deuxième modification du pilote porte sur la phase de découverte. Durant cette étape, le terminal mobile envoie des trames *Probe Request* sur un certain canal et vers un SSID particulier. Dès réception d'une réponse provenant du point d'accès visé, nous avons indiqué au pilote de passer à la phase d'authentification. Les paramètres *MinChannelTime* et *MaxChannelTime* ne seront dès lors utilisés que dans les cas d'erreurs. On peut d'ailleurs noter que par défaut dans le pilote MADWiFi, $MinChannelTime = MaxChannelTime = 200$ millisecondes.

Le protocole SHAPE nécessite un comportement particulier des terminaux mobiles au niveau 3. Nous avons donc également dû apporter quelques modifications à l'implémentation MIPL-2. Cette dernière s'intègre au niveau noyau du système GNU/Linux mais comporte un démon dans l'espace utilisateur. Cette séparation permet de modifier rapidement des parties spécifiques du code. Dans un premier temps, nous avons ajouté une socket de communication de manière à traiter les échanges entre le terminal et le contrôleur de mobilité (échanges effectués en UDP). Par la suite, nous avons modifié le démon pour qu'il réagisse de la façon suivante. A la réception d'un message HI, le démon MIPL-2 envoie les nouveaux paramètres de niveau 2 au pilote MADWiFi à l'aide d'une socket RTNetlink. Ce type de socket permet l'échange de paramètres entre l'espace utilisateur et l'espace noyau d'un système GNU/Linux. Puis, les nouveaux paramètres de niveau 2 sont configurés sur le périphérique sans fil à l'aide de routines IOCTL (fonctions permettant de contrôler des périphériques) ce qui déclenche le handover. Grâce à l'utilisation d'un déclencheur de niveau 2 (*Link Up* [100]), le démon MIPL-2 peut initier la procédure de handover de niveau 3 dès la fin du handover de niveau 2.

Les paramètres de niveau 3 du nouveau lien se présentent sous la forme d'un RA inclus dans le message HI. Ce RA est identique à ceux qui sont envoyés par les routeurs d'accès du nouveau lien IPv6. Dès la fin du handover de niveau 2, le démon MIPL-2 analyse ce RA et agit comme s'il l'avait reçu de manière standard. Le démon MIPL-2 va donc configurer une nouvelle adresse IPv6 temporaire et envoyer un BU à l'agent mère local. Pour émuler la procédure ODAD, nous avons désactivé la réalisation du DAD sur les nouvelles adresses temporaires.

Enfin, nous avons développé un petit logiciel qui permet de gérer les coordonnées du terminal mobile. Ce logiciel récupère périodiquement (i.e. toutes les secondes dans le cas présent) les coordonnées fournies par le récepteur GPS et les enregistre. Dès l'obtention de nouvelles coordonnées, il calcule la distance que le terminal a effectué depuis sa dernière position et envoie, le cas échéant, un message LU au contrôleur de mobilité. La figure 7.3 représente les diverses interactions entre les différentes parties mises en jeu par le protocole SHAPE.

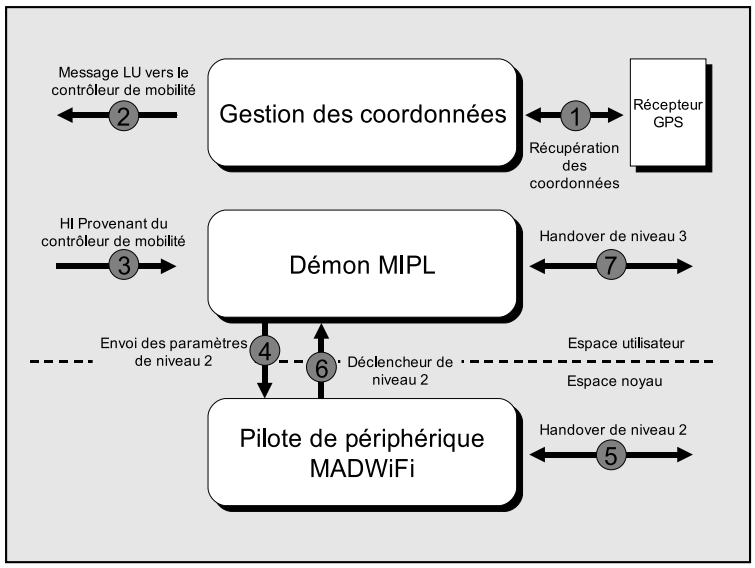


FIG. 7.3 – Schéma général d'un handover réalisé à l'aide du protocole SHAPE au sein du système d'exploitation

7.4 Evaluation des performances

L'évaluation de notre protocole s'est effectuée en deux parties. Dans un premier temps, nous avons mesuré les performances du protocole SHAPE en termes de temps de latence au niveau 2 et au niveau 3 lorsque le terminal effectue un handover. L'impact des handovers sur des flux temps réel émulés a également été analysé lors de cette étude. Notre évaluation s'est poursuivie par un comparatif entre les performances des protocoles SHAPE, MIPv6 et FMIPv6. Dans cette seconde analyse, nous avons notamment mesuré la perception des handovers au niveau des utilisateurs lorsqu'ils utilisent des applications temps réel classiques.

7.4.1 Evaluation préliminaire

La plate-forme de tests mise en place pour l'évaluation préliminaire est illustrée sur la figure 7.4. Elle est composée de trois points d'accès 802.11b provenant du commerce, de deux routeurs d'accès, d'un agent mère, d'un contrôleur de mobilité, d'un correspondant (CN) et d'un terminal mobile. Les délais pour atteindre l'agent mère ou le contrôleur de mobilité sont négligeables (inférieurs à 5 millisecondes), émulant ainsi une architecture hiérarchique.

Etant donné que le système GPS ne fonctionne pas à l'intérieur des bâtiments, nous avons effectué au préalable diverses traces GPS en extérieur. Cette phase consiste à enregistrer les trames envoyées par le récepteur GPS dans des fichiers afin de pouvoir émuler les déplacements du terminal à l'intérieur d'un bâtiment. Cette étape nous a permis de simplifier grandement le déroulement des tests et la prise de mesures. Nous avons ensuite créé la base de données du contrôleur de mobilité, en rentrant statiquement les différents paramètres des équipements de la plate-forme de tests. Par rapport à nos traces GPS, nous avons notamment positionné les coordonnées (latitude et longitude) des points d'accès de sorte qu'ils soient espacés de 50 mètres chacun.

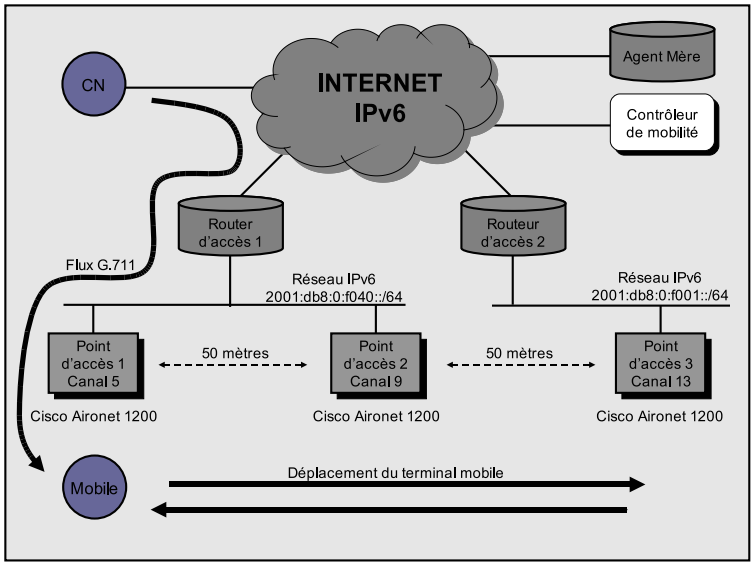


FIG. 7.4 – Plate-forme de tests pour l'évaluation préliminaire du protocole SHAPE

Scénarii de tests

Pour cette première évaluation, deux scénarii de tests ont été établis. Dans le scénario 1, le terminal mobile se déplace de manière rectiligne du point d'accès 1 vers le point d'accès 3 puis revient à son point de départ. Par rapport à la topologie de notre plate-forme de tests, le terminal va donc effectuer quatre handovers de niveau 2 et deux handovers de niveau 3. Afin d'évaluer l'impact de notre protocole sur les flux applicatifs lors des handovers, nous avons ajouté dans le deuxième scénario un flux audio utilisant le codec G.711 [44]. Ce flux, créé par le générateur de trafic MGEN [86], est envoyé au terminal mobile depuis le correspondant. Le scénario 2 reste sinon identique au scénario 1.

Premiers résultats

Les résultats présentés dans le tableau 7.3 et les figures 7.5, 7.6 et 7.7 ont été obtenus en utilisant deux analyseurs réseau (i.e. sniffeurs) et le logiciel Ethereal [22]. La figure 7.5 présente les temps de latence des handovers de niveau 2. Nous avons rejoué 20 fois le premier scénario, ce qui nous a permis d'obtenir un total de 80 mesures concernant les handovers de niveau 2. Il apparaît que notre protocole permet de réaliser des handovers de niveau 2 en 8,926 millisecondes en moyenne. Ce temps est fortement réduit par rapport à la méthode standard dans laquelle un handover de niveau 2 peut prendre entre 58,74 et 396,76 millisecondes d'après [58]. Ce gain de temps s'explique principalement par l'optimisation de la phase de découverte. En effet, dans notre solution, le terminal mobile ne sonde que le canal précisé dans le message HI, et passe à la phase d'authentification dès réception d'une réponse du point d'accès sélectionné par le contrôleur de mobilité. Par conséquent, les paramètres *MinChannelTime* et *MaxChannelTime* ne sont plus utilisés. En outre, la distance entre les canaux radio utilisés par les points d'accès n'a plus d'influence sur les temps de latence lorsque la sélection du prochain point d'accès est satisfaisante. Les fluctuations observées dans les mesures sont principalement dues au trafic des cellules voisines. D'ailleurs, l'écart-type important figurant dans la table 7.3 s'explique par la mesure 48 dans laquelle le handover s'est réalisé en 48,153 millisecondes, en raison des interférences provoquées par les cellules voisines lors de cette mesure. Si on ne considère pas cette mesure, l'écart-type est proche de 1 milliseconde. Concernant l'intervalle de confiance calculé, il y a 95% de chance que la moyenne soit située dans l'intervalle $[7,905; 9,947]$.

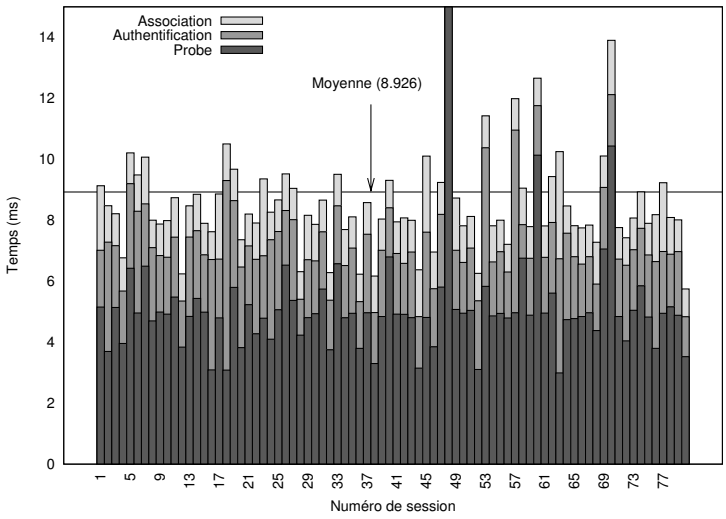


FIG. 7.5 – Temps de latence engendrés par les handovers de niveau 2

Niveau	Nombre de Handovers	Temps moyen de déconnexion (ms)	Ecart-type (ms)	Intervalle de Confiance (ms)
2	80	8,926	4,660	$\Delta = 1{,}021$
3	40	27,334	4,734	$\Delta = 1{,}467$

TAB. 7.3 – Résultats obtenus pour le scenario 1

Lorsque le terminal mobile se déplace entre les points d'accès 2 et 3, le handover de niveau 2 est suivi d'un handover de niveau 3. Lors de l'évaluation des performances au niveau 3, nous nous sommes concentrés sur 3 événements : la fin du handover de niveau 2, l'émission du BU, et la réception du BACK qui conclut le handover de niveau 3. La figure 7.6 représente les différents temps pour lesquels ces événement se produisent. Les résultats présentés sur la ligne 2 du tableau 7.3 font également référence aux handovers de niveau 3. Comme nous pouvons le voir, le protocole SHAPE permet de réaliser des handovers de niveau 3 rapides avec un temps de latence moyen de 27,334 millisecondes. Bien que la détection du nouveau lien soit automatique (grâce aux informations contenues dans les messages HI) et que nous émulions la procédure ODAD, le démon MIPL-2 met encore 14,035 millisecondes en moyenne pour réaliser les différentes opérations nécessaires à l'envoi d'un BU (analyse des informations de niveau 3 du message HI, création de la nouvelle adresse temporaire, mise à jour du tunnel, etc). Le message BACK arrive approximativement 4,724 millisecondes après la transmission du BU, ce qui reflète bien une architecture hiérarchique.

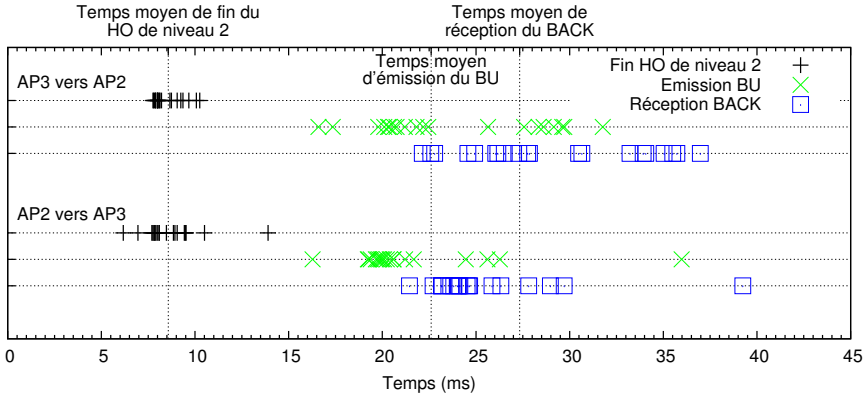


FIG. 7.6 – Temps de latence engendrés par les handovers de niveau 3

Enfin, la figure 7.7 représente l'impact des handovers de niveau 2 et 3 sur la réception d'un flux applicatif dans le scénario 2. Chaque point représente la réception d'un paquet de données au temps indiqué sur l'axe des ordonnées. Nous avons également joué le deuxième scénario à 20 reprises. En nous basant sur les mesures que nous avions effectuées pour le scénario 1 et sur les spécifications du codec G.711, nous espérions

dans les cas les moins favorables (i.e. lors d'un handover de niveau 3) perdre un unique paquet de données. Il apparaît cependant que le terminal mobile perd en moyenne un paquet de données lors d'un handover de niveau 2 et deux paquets de données lors d'un handover de niveau 2 et 3. Il semblerait que la réinitialisation du périphérique sans fil et plus précisément le changement de fréquence radio soit responsable de ces pertes, en introduisant un délai supplémentaire dans les handovers de niveau 2. Ce délai n'a pas été mesuré car nous avons considéré l'émission de la première *Probe Request* comme étant la première étape du handover de niveau 2.

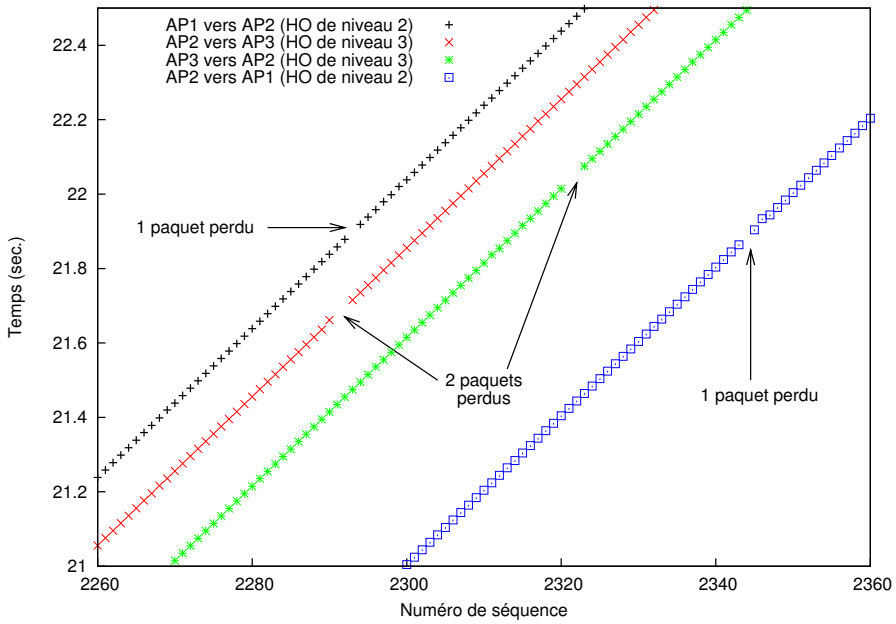


FIG. 7.7 – Impact des handovers sur les flux applicatifs

Pour réellement apprécier les performances du protocole SHAPE, il est nécessaire de le comparer à d'autres protocoles offrant une gestion efficace de la mobilité des utilisateurs. Dans la section suivante, nous allons présenter une nouvelle étude allant dans ce sens.

7.4.2 Comparaison avec les protocoles MIPv6 et FMIPv6

A la vue de nos premiers résultats encourageants, nous avons souhaité approfondir l'évaluation de notre protocole [59]. Cette nouvelle étude présente un comparatif entre les protocoles MIPv6, FMIPv6 et SHAPE. Elle propose notamment une analyse de la perception des utilisateurs lorsqu'ils utilisent diverses applications temps réel pendant une procédure de handover.

Nouvelle plate-forme de tests

Pour effectuer cette nouvelle batterie de mesures, nous avons utilisé la plate-forme de tests mise en place par l'équipe Réseaux et Protocoles du LSIIT lors de l'implémentation du protocole FMIPv6 (fmipv6.org [45]). Cette plate-forme reste cependant assez similaire à la précédente.

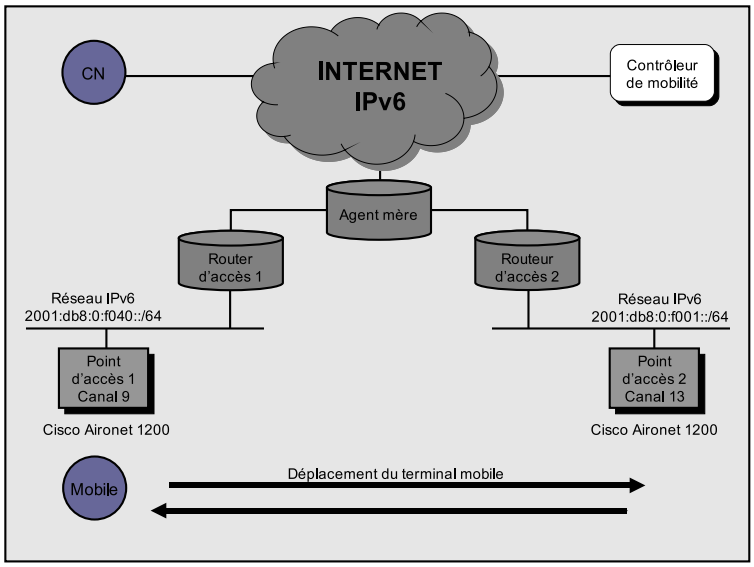


FIG. 7.8 – Nouvelle plate-forme de tests

Cette nouvelle plate-forme se compose de trois routeurs d'accès, de deux points d'accès, d'un terminal mobile et d'un correspondant. En outre, nous y avons ajouté le contrôleur de mobilité. L'agent mère constitue le routeur d'accès principal et permet de relier le reste de la plate-forme à l'Internet IPv6. Chaque point d'accès est situé dans un sous-réseau IPv6 différent et est connecté à un routeur d'accès spécifique. La figure 7.8 illustre cette nouvelle plate-forme d'évaluation.

Excepté les points d'accès qui sont des équipements 802.11b commerciaux, chaque entité réseau de notre plate-forme fonctionne avec le système d'exploitation GNU/Linux. Pour assurer le routage des données, les routeurs d'accès utilisent le démon de routage logiciel Quagga [87]. L'agent mère et le terminal mobile disposent du nouveau démon MIPv6 pour GNU/Linux (MIPL-2 [74]). Lors de l'évaluation du protocole FMIPv6, le terminal mobile ainsi que les routeurs d'accès intègrent en plus l'implémentation libre du protocole FMIPv6 (fmipv6.org [45]). Enfin, nous avons réutilisé les modifications présentées dans la partie 7.3 sur le terminal mobile pour les tests relatifs au protocole SHAPE.

Lors de nos tests correspondant au protocole MIPv6, nous avons pris la liberté de supprimer la procédure du DAD afin d'émuler la procédure ODAD (voir la section 2.5.2). On peut rappeler ici qu'une telle émulation est déjà présente dans l'implémentation du protocole SHAPE. De plus, la fréquence d'émission des messages RA a été positionné entre 0,03 et 0,07 secondes (i.e. à la fréquence maximale autorisée) de manière à limiter autant que possible le temps de détection des nouveaux liens IPv6. Etant donné que la fréquence d'émission de ces messages n'influe pas sur les performances des protocoles FMIPv6 et SHAPE, nous avons décidé de la positionner à sa valeur par défaut (i.e. entre 200 et 600 secondes [72]) lors de l'évaluation de ces protocoles.

Choix des périphériques sans fil

Il a déjà été mentionné que les temps de latence engendrés par les handovers de niveau 2 varient fortement en fonction des périphériques sans fil utilisés. Les protocoles SHAPE et FMIPv6 requièrent tout deux une gestion spécifique du comportement du périphérique sans fil, gestion qui est rendue possible grâce au pilote de périphérique MADWiFi, facilement configurable. Pour ces deux protocoles, nous avons donc utilisé une carte 802.11 a/b/g de marque 3Com qui est compatible avec MADWiFi.

De son côté, le protocole MIPv6 a été conçu comme un protocole réactif qui ne propose aucune interaction avec les couches inférieures. De ce fait, la gestion du handover de niveau 2 est entièrement laissée à la bonne grâce du firmware / pilote de périphérique de la carte, contrairement aux protocoles SHAPE et FMIPv6 dans lesquels le protocole lui-même est capable de déclencher une procédure d'association de niveau 2. Malheureusement, lorsque les handovers de niveau 2 sont entièrement gérés par le pilote MADWiFi de base, ils sont particulièrement longs, à tel point que les résultats que nous aurions pu obtenir pour le protocole MIPv6 n'auraient pas été réalistes ou du moins n'auraient pas reflété un cas ordinaire.

Nous avons donc complété notre étude par une évaluation des périphériques sans fil à notre disposition : la carte 3Com mentionnée précédemment et deux cartes PCMCIA Cisco Aironet 802.11b. Les deux cartes Cisco ne se différencient que par la version du firmware présent dans la carte. La première dispose du firmware 4.25.30 (daté d'avril 2002) alors que l'autre utilise la version 5.60.17 (daté d'août 2005). La figure 7.9 présente le temps de latence engendré par un handover de niveau 2 suivant la carte sans fil utilisée. Les mesures ont été effectuées alors que le terminal recevait un flux applicatif, dans lequel chaque nouveau paquet de données était espacé du précédent de 30 millisecondes. On peut constater que c'est la carte Cisco utilisant le firmware 4.25.30 et la carte 3Com qui engendrent les plus importants temps de latence. En effet, à chaque handover, ces deux cartes sondent systématiquement tous les canaux radio disponibles avant de

choisir un nouveau point d'accès. La carte 3Com introduit des délais plus longs car elle sonde en plus les canaux de la bande de fréquence des 5 GHz (i.e. 802.11a). Par contre, la deuxième carte Cisco (firmware 5.60.17) réalise un handover de niveau 2 en seulement 33 millisecondes. Même sans la mise en place du système Cisco WDS que nous avons évalué dans la partie 3, la carte reste très performante (dans un système ouvert) lorsque le terminal reçoit ou émet un flux. En effet, elle enregistre les canaux sur lesquels elle s'est déjà associée et sonde ces canaux particuliers en priorité. Par ailleurs, elle utilise des paramètres *MinChannelTime* et *MaxChannelTime* très courts ce qui la rend très réactive. En l'absence de flux applicatifs, la carte augmente uniquement les valeurs des paramètres *MinChannelTime* et *MaxChannelTime* mais sonde toujours sa propre liste de canaux. Notons qu'avec seulement deux points d'accès, notre plate-forme d'évaluation est particulièrement bien adaptée au comportement par défaut de cette carte. Nous avons donc décidé de l'utiliser lors de l'évaluation du protocole MIPv6 de façon à limiter l'influence des temps de latence des handovers de niveau 2 sur les résultats globaux.

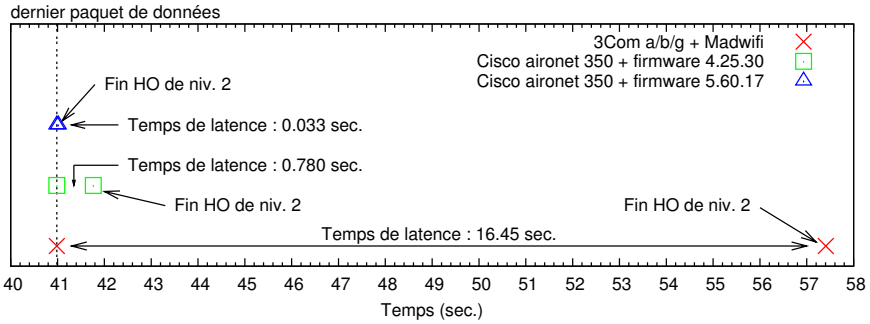


FIG. 7.9 – Temps de latence engendré par un handover de niveau 2 suivant le périphérique sans fil utilisé

Scénarii d'évaluation

Dans cette nouvelle évaluation, nous avons défini deux scénarii dans lesquels le terminal mobile se déplace entre les deux points d'accès (voir figure 7.8). Dans le premier scénario, le correspondant envoie au terminal un flux vidéo en direct grâce au logiciel VideoLAN [19]. Les données sont envoyées dans des paquets RTP (*Real-time Transport Protocol* [91]) dont la taille fait approximativement 1336 octets. Un paquet est envoyé toutes les 30 millisecondes.

Le second scénario met en jeu une vidéoconférence entre le correspondant et le terminal mobile. Ils sont tout deux équipés d'une webcam et utilisent le logiciel Gnomemeeting [89] pour assurer la vidéoconférence. Cette application utilise également des paquets RTP pour véhiculer les données mais sépare les données audio et vidéo en deux

flux distincts. Les paquets audio ont une taille moyenne de 70 octets et sont envoyés toutes les 30 millisecondes. En revanche, les paquets vidéo ont une taille approximative de 950 octets et sont envoyés toutes les 160 millisecondes.

Résultats

Les résultats présentés dans cette section ont été obtenus grâce à des analyseurs réseau (i.e. sniffeurs) et au logiciel Ethereal [22]. Pour chaque scénario et chaque protocole, nous avons évalué les délais engendrés par les handovers de niveau 2 et 3, ainsi que le nombre de paquets perdus et la perception des utilisateurs lors d'un handover. Concernant les handovers de niveau 3, nous avons mesuré le temps écoulé entre le début du handover de niveau 2 et la réception du premier paquet de données sur le nouveau lien IPv6 (envoyé par l'agent mère suite à la réception du BU dans les protocoles MIPv6 et SHAPE, et envoyé par le nouveau routeur d'accès suite à la réception du FNA dans le protocole FMIPv6). Les scénarii 1 et 2 ont respectivement été joués à 10 reprises pour chaque protocole.

Les résultats obtenus pour le scénario 1 sont représentés dans le tableau 7.4 et sur les figures 7.10(a), 7.11(a) et 7.12(a). Nous pouvons observer que la durée moyenne des handovers de niveau 2 est pratiquement identique quel que soit le protocole utilisé. Lors de l'utilisation des protocoles FMIPv6 et SHAPE, le terminal mobile effectue la même procédure de handover de niveau 2 car il possède dans les deux cas les paramètres de son prochain point d'accès avant d'initier le handover. Il peut donc s'associer très rapidement à ce point d'accès sans avoir à sonder de nombreux canaux radio. Nous avons également tenu compte du temps de réinitialisation de la carte sans fil, ce qui explique l'écart entre les mesures présentées ici et celles présentées dans notre évaluation préliminaire du protocole SHAPE. Par ailleurs, lorsque le terminal utilise le protocole MIPv6, les handovers de niveau 2 sont entièrement gérés par le firmware de la carte sans fil. Les performances restent cependant équivalentes à celles observées pour les protocoles FMIPv6 et SHAPE en raison de l'optimisation présente dans la carte que nous avons choisie (voir section 7.4.2).

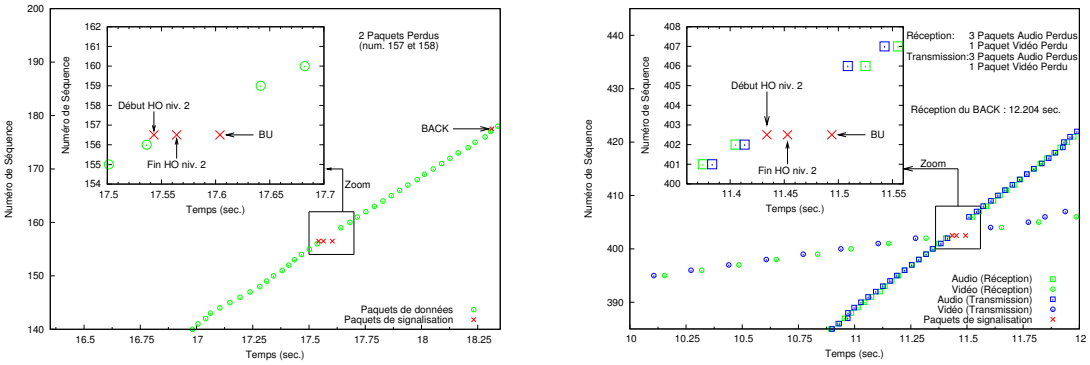
Au niveau 3, on constate que les temps de latence moyens engendrés par les handovers sont relativement proches pour les protocoles FMIPv6 (39,7 millisecondes) et SHAPE (52 millisecondes). Dans le protocole FMIPv6, le terminal envoie un message FNA dès la fin du handover de niveau 2, ce qui déclenche la transmission des paquets mis en attente sur le nouveau routeur d'accès. Tant que le tunnel FMIP est actif, le terminal mobile est donc en mesure de recevoir les paquets envoyés à son ancienne localisation. En outre, la procédure de mise à jour de la nouvelle adresse temporaire auprès de l'agent mère n'a pas d'influence sur les performances du protocole FMIPv6.

Protocole	Temps des HO		Nombre de paquets perdus	Perception des utilisateurs
	de niv. 2	de niv. 3		
MIPv6	22,4ms	116,7ms	3,67	Légère coupure dans la vidéo et le son
FMIPv6	19,4ms	39,7ms	0	Pas d'interruption
SHAPE	19,4ms	52ms	1	Légère coupure dans le son

TAB. 7.4 – Résultats concernant le scénario 1 (moyennes)

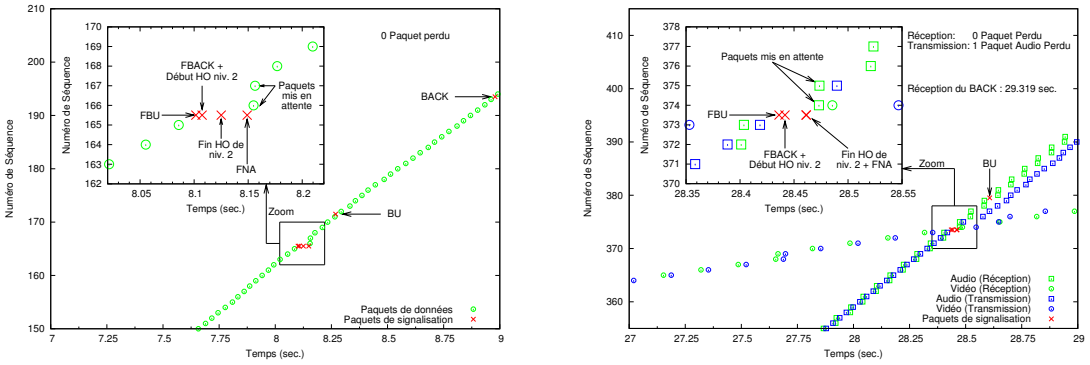
De son côté, le protocole SHAPE permet au terminal d'envoyer le BU dès la fin du handover de niveau 2, grâce aux informations de niveau 3 envoyées par le contrôleur de mobilité et à l'utilisation de la procédure ODAD. Etant donné que le délai d'acheminement des paquets entre le terminal et l'agent mère est négligeable dans notre plate-forme de tests, les paquets de données vont être rédirigés (au niveau de l'agent mère) vers la nouvelle localisation du terminal, quasiment juste après la fin du handover de niveau 2. Les délais engendrés par les procédures qui permettent de recevoir à nouveau des paquets de données au niveau 3 sont donc très similaires entre les protocoles FMIPv6 et SHAPE. Concernant le protocole MIPv6, on constate un temps de latence de niveau 3 plus important (de l'ordre de 116,7 millisecondes) en raison du mécanisme de détection des nouveaux liens IPv6 basé sur la réception des messages RA. Bien que ces derniers soient envoyés à la fréquence maximale autorisée par les spécifications du protocole MIPv6 (i.e. entre 0,03 et 0,07 secondes), le terminal met en moyenne 50 millisecondes pour détecter qu'il se situe sur un nouveau lien IPv6. Dès la détection du nouveau lien, le terminal peut créer une nouvelle adresse temporaire valide et informe son agent mère de sa nouvelle localisation. Etant donné que nous émulons la procédure ODAD, la vérification de la nouvelle adresse temporaire n'engendre pas de délais supplémentaires dans le handover de niveau 3.

En ce qui concerne les flux applicatifs, nous pouvons noter que le protocole FMIPv6 permet de ne perdre aucun paquet de données lors d'un handover. Cela est rendu possible grâce au nouveau routeur d'accès qui enregistre dans un tampon les paquets de données destinés au terminal jusqu'à ce que ce dernier termine son handover de niveau 2. Dès la réception du message FNA, le nouveau routeur d'accès retransmet au terminal les différents paquets en attente. La figure 7.11(a) illustre parfaitement ce phénomène. Chaque point représente la réception (au niveau du terminal) d'un paquet de données au temps indiqué sur l'axe des abscisses. Les numéros de séquence indiqués sur l'axe des ordonnées correspondent aux numéros de séquence des paquets RTP. On peut notamment observer sur cette figure un léger délai sur la réception des paquets mis en attente sur le nouveau routeur d'accès. Ces délais n'ont cependant pas d'influence sur l'application car elle utilise également un tampon de réception. Dès lors, les handovers sont complètement transparents pour les utilisateurs.



(a) Scénario 1 (b) Scénario 2

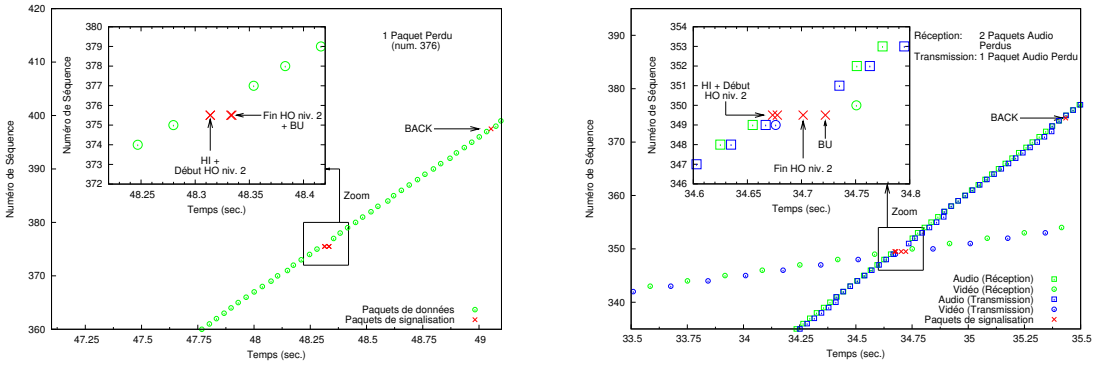
FIG. 7.10 – Résultats obtenus pour le protocole MIPv6



(a) Scénario 1 (b) Scénario 2

FIG. 7.11 – Résultats obtenus pour le protocole FMIPv6

Bien que les handovers sont pratiquement aussi rapides que dans FMIPv6, le terminal perd quand même en moyenne un paquet de données lorsqu'il utilise le protocole SHAPE. Tant que l'agent mère n'a pas reçu de BU, il continue à transmettre les paquets de données vers la précédente localisation du terminal. Ces paquets n'étant pas mis en attente ni retransmis, ils sont définitivement perdus (voir la figure 7.12(a)). Cette perte de paquets introduit de légères coupures au niveau de la bande son de la vidéo. De ce fait, le handover n'est pas transparent pour les utilisateurs. Ce phénomène est encore plus prononcé dans le cas du protocole MIPv6, en raison du temps de latence plus important engendré par les handovers (116,7 millisecondes en moyenne pour le scénario



(a) Scénario 1

(b) Scénario 2

FIG. 7.12 – Résultats obtenus pour le protocole SHAPE

1). Le nombre de paquets perdus est également plus important, avec un taux de perte moyen de 3,67 par handover. Dès lors, l'utilisateur perçoit non seulement des coupures dans le son, mais aussi dans la vidéo lors d'un handover.

Les résultats du scénario 2 sont représentés dans le tableau 7.5 et sur les figures 7.10(b), 7.11(b) et 7.12(b). Rappelons que dans ce scénario, le terminal mobile et le correspondant effectuent une vidéoconférence à l'aide du logiciel Gnomemeeting. Par conséquent, le terminal reçoit et transmet des paquets de données. Il apparaît que les résultats portant sur la réception sont très similaires à ceux du scénario 1. Naturellement, le terminal mobile perd plus de paquets audio que vidéo en raison de la différence entre les fréquences d'émission de ces paquets (toutes les 30 millisecondes pour les paquets audio contre 160 millisecondes pour les paquets vidéo). Au niveau de l'émission, les résultats sont proches de ceux observés pour la réception. Concernant les protocoles MIPv6 et SHAPE, cela est principalement dû au délai pour atteindre l'agent mère. Dans nos mesures, nous constatons que le terminal mobile peut à nouveau émettre des paquets de données dès la transmission du BU. Or, le délai entre le terminal mobile et l'agent mère est négligeable dans notre plate-forme d'évaluation. Les paquets de données vont donc arriver à la nouvelle localisation du terminal juste après que ce dernier ne commence à utiliser sa nouvelle adresse temporaire. Il est évident qu'un délai plus important entre l'agent mère et le terminal engendrerait plus de paquets perdus au niveau de la réception qu'au niveau de l'émission. Dans le cas du protocole FMIPv6, le handover de niveau 3 est très particulier car le terminal mobile peut toujours utiliser son ancienne adresse temporaire sur le nouveau lien IPv6. En effet, tant que le tunnel entre l'ancien routeur d'accès et le nouveau routeur d'accès est actif, tous les paquets de données passent par ce tunnel (aussi bien en émission qu'en réception). Dès lors, ni le

Protocole	Temps des HO		Nbr de paquets perdus		Perception des utilisateurs
	niv. 2	niv. 3	Récep.	Trans.	
MIPv6	20,2ms	87,6ms	2,3 (audio) 0,4 (video)	2,3 (audio) 0,4 (video)	Légère coupure dans le son et la vidéo
FMIPv6	22,5ms	52ms	0,3 (audio) 0 (video)	0,3 (audio) 0 (video)	Pas d'interruption
SHAPE	20,98ms	49,7ms	1,13 (audio) 0,13 (video)	0,88 (audio) 0 (video)	Légère coupure dans le son

TAB. 7.5 – Résultats concernant le scénario 2 (moyennes)

délai pour atteindre l'agent mère, ni le temps de détection du nouveau lien IPv6 n'a d'influence sur les performances du protocole tant que le tunnel FMIP est actif suffisamment longtemps.

Enfin, suites aux mesures effectuées ici, nous pouvons noter que l'agent mère met un certain temps à envoyer le message BACK en réponse au BU. Ce délai est certainement dû à la version du démon MIPL-2 utilisée sur l'agent mère qui n'était pas encore finalisée (i.e. version Release Candidate 2). Néanmoins, ce délai n'a aucune influence sur les performances des protocoles, puisque l'agent mère envoie bien les paquets de données à la nouvelle localisation du terminal dès la réception du BU.

7.5 Conclusion

Dans ce chapitre, nous avons présenté le protocole SHAPE qui constitue notre première proposition sur l'introduction de la géolocalisation dans la gestion des handovers. Suite à sa spécification, nous avons réalisé son implémentation au sein d'un système GNU/Linux en vue d'analyser ses performances sur une réelle plate-forme de tests. Nous avons également pu le comparer aux protocoles MIPv6 et FMIPv6 qui possèdent tout deux des implémentations libres pour les systèmes GNU/Linux.

Lors de l'évaluation de notre solution, nous avons notamment pu constater que même avec un algorithme de sélection du prochain point d'accès assez simpliste (c'est le point d'accès le plus proche géographiquement du terminal mobile qui est sélectionné), le protocole SHAPE est très performant aussi bien lors des handovers de niveau 2 que lors des handovers de niveau 3. Notre comparatif avec le protocole MIPv6 a aussi permis de confirmer que ce dernier n'est réellement pas adapté à une gestion rapide de la mobilité. Même avec un handover de niveau 2 rapide, une fréquence d'émission des messages RA maximale, un agent mère local et l'émulation de la procédure ODAD, le

terminal perd encore trop de paquets de données lorsqu'il utilise une application temps réel. Toutefois, même les performances affichées par notre protocole ne semblent pas suffisantes pour rendre les déplacements complètement transparents aux utilisateurs. En effet, suivant l'application utilisée, un simple paquet perdu peut déjà être perçu par l'utilisateur. A la vue du comparatif effectué, il apparaît que c'est le protocole FMIPv6 qui est le plus à même d'accomplir des handovers transparents pour les utilisateurs. Cependant, la manière d'obtenir les paramètres de niveau 2 des points d'accès environnants pose problème. Il est suggéré, dans les spécifications de FMIPv6, de réaliser une procédure de scan afin d'obtenir ces informations. Or nous avons vu qu'une telle phase de découverte peut s'étendre sur une longue période de temps. Bien que le handover effectif soit rapide, la découverte du prochain point d'accès peut donc engendrer d'importants délais dans les communications. Dès lors, la réalisation de handovers rapides devient complètement inutile.

Par ailleurs, nous n'avons pas encore évalué le comportement du protocole SHAPE lors des cas d'erreurs. Mais à la vue des ses performances actuelles, nous avons dans un premier temps souhaité modifier certains aspects du protocole. Nous restons convaincus que nous pouvons étendre la manière d'utiliser des informations de géolocalisation, notamment lors de la sélection du prochain point d'accès. Toutes ces réflexions nous ont amené à spécifier un nouveau protocole : le *Fast Location-based Handover* (FLH). Dans le chapitre suivant, nous allons présenter les nouvelles fonctionnalités apportées par ce protocole.

Chapitre 8

Le protocole FLH

8.1 Introduction

En nous basant sur nos précédents travaux, nous avons défini une nouvelle approche qui étend les fonctionnalités du protocole SHAPE. Baptisé *Fast Location-based Handover* (FLH [62, 63, 64]), ce nouveau protocole réutilise en grande partie l'architecture mise en place dans notre dernière solution. Le temps de mise à jour des adresses temporaires des terminaux mobiles auprès de l'agent mère est ici toujours minimisé par la mise en place d'une architecture hiérarchique. Le contrôleur de mobilité dispose également des mêmes fonctionnalités que précédemment (base d'informations sur les équipements, etc) mais utilise un nouvel algorithme de sélection des prochains points d'accès. En outre, le protocole FLH se base toujours sur un système de géolocalisation générique qui peut correspondre aux différents systèmes que nous avons présentés dans le chapitre 5. La spécification et l'évaluation de ce protocole ont été réalisées en collaboration avec les centres recherche et développement de France Télécom.

L'idée principale du protocole FLH est de déterminer, par rapport à un échantillon de positions, la trajectoire des terminaux mobiles. Ainsi, le contrôleur de mobilité sélectionnera non plus le point d'accès le plus proche, mais celui qui offre la plus grande zone de couverture radio au terminal en fonction de sa trajectoire. En plus de la réduction du temps de déconnexion, ce protocole devrait donc également limiter le nombre de procédures de handover. Bien que l'optimisation proprement dite du handover reste identique à celle qui est décrite dans le protocole SHAPE, nous avons également ajouté un mécanisme de gestion de contexte. Ce mécanisme permet aux terminaux mobiles d'initier les procédures de handover et de réduire le nombre de messages échangés avec le contrôleur de mobilité.

La version du protocole FLH présentée dans ce chapitre s'inscrit dans un environnement ouvert dans lequel les points d'accès n'utilisent pas de paramètres de sécurité particuliers. Elle constitue la version de base de notre approche qui servira lors des différents tests de performances. Notons qu'il est cependant possible d'étendre cette version de base afin de l'adapter à des systèmes fermés dans lesquels un compte valide est nécessaire pour accéder au réseau. Dans le cas d'un réseau IEEE 802.11i, on peut notamment tirer parti du mécanisme de pré-authentification [7] pour effectuer toutes les procédures de gestion de la sécurité (autorisation d'accès, échange de clés de chiffrement, etc) avant le déclenchement d'un handover. Cette version étendue est toutefois encore à l'étude et ne sera donc pas présentée dans ce chapitre.

Après une description des différentes fonctionnalités du protocole FLH, nous présenterons une première évaluation de ses performances réalisée par simulation à l'aide du simulateur SimulX. Nous ferons ensuite état d'une comparaison entre le protocole FLH et le protocole SHAPE sur l'influence des erreurs de géolocalisation.

8.2 Description du protocole

Dans cette section, nous allons principalement exposer les nouveaux mécanismes introduits par le protocole FLH par rapport à notre précédente solution. Nous détaillerons notamment les nouvelles fonctionnalités du contrôleur de mobilité ainsi que le nouveau mécanisme de gestion de contexte.

8.2.1 Nouvelles fonctionnalités du contrôleur de mobilité

Le protocole FLH maintient le contrôleur de mobilité utilisé dans le protocole SHAPE (cf. chapitre 7) mais étend ses différentes fonctionnalités. En plus de la base d'informations des différents équipements du domaine, il dispose d'un cache de mobilité. Ce cache contient les paramètres actuels des terminaux mobiles qui supportent le protocole FLH et qui sont actuellement pris en charge par le contrôleur de mobilité. Chaque entrée du cache de mobilité contient quatre champs : l'adresse MAC du terminal, l'identifiant de son point d'accès courant, l'identifiant de son prochain point d'accès et une liste variable de ses précédentes coordonnées. Le cache de mobilité est illustré dans le tableau 8.1. La découverte de l'adresse du contrôleur de mobilité se fait toujours par l'intermédiaire d'une nouvelle option présente dans les messages RA. Outre l'adresse du contrôleur, d'autres informations peuvent être incluses dans cette option telles que le système de géolocalisation utilisé dans le domaine.

ID	Adresse MAC	ID Point d'accès courant	ID Prochain point d'accès	Coordonnées précédentes
1	A:B:C:D:E:F	1	2	(x_1, y_1, z_1) (x_2, y_2, z_2) (x_3, y_3, z_3)
2	A:B:C:F:E:D	1	néant	(x_4, y_4, z_4)
3	A:B:C:D:F:E	4	6	(x_5, y_5, z_5) (x_6, y_6, z_6)
...	...	...	...	...

TAB. 8.1 – Cache de mobilité intégré au sein du contrôleur de mobilité

8.2.2 Mise à jour du cache de mobilité

Le cache de mobilité est maintenu à jour dynamiquement par les terminaux mobiles grâce aux messages *Mobility Update* (MUP). L'envoi des messages MUP est régulé par la qualité du signal d'un terminal. Nous avons défini deux seuils d'intensité du signal S_1 et S_2 qui correspondent respectivement à un signal moyen et à un signal faible. Le seuil $S1_1$ est positionné entre $[-75dBm; -78dBm]$ et le seuil S_2 est positionné entre $[-78dBm; -80dBm]$ comme suggéré dans [69]. De plus, nous avons maintenu le paramètre R qui était déjà présent dans le protocole SHAPE. Pour mémoire, R correspond à la distance maximale entre un terminal et son point d'accès courant pendant laquelle le terminal est encore bien couvert. En se basant toujours sur [69], nous avons fixé R à 50% de la portée maximale des points d'accès. Tant que la qualité du signal est inférieure au seuil S_1, le terminal envoie, à chaque actualisation de sa position, un message MUP au contrôleur de mobilité. La fréquence d'émission des messages MUP dépend donc directement de la fréquence de mise à jour des positions du système de géolocalisation utilisé.

A la réception d'un message MUP, le contrôleur de mobilité met à jour le cache de mobilité en fonction des informations contenues dans le message (voir la figure 8.1). Lorsqu'un terminal n'est pas encore référencé, le contrôleur crée automatiquement une nouvelle entrée dans le cache. En premier lieu, le contrôleur met à jour les coordonnées et l'adresse MAC du point d'accès courant du terminal. Puis, il vérifie la distance d séparant le terminal et son point d'accès courant. Si la distance d est supérieure au seuil R défini précédemment, le contrôleur déduit que le terminal est proche du bord de la zone de couverture de son point d'accès courant. L'utilisation conjointe de la qualité du signal (lors de l'émission des messages MUP) et de la distance géographique devrait permettre de palier les problèmes de perturbation temporaire du canal radio ou d'erreurs de géolocalisation. Lorsqu'on a la relation $d > R$, le contrôleur de mobilité doit s'as-

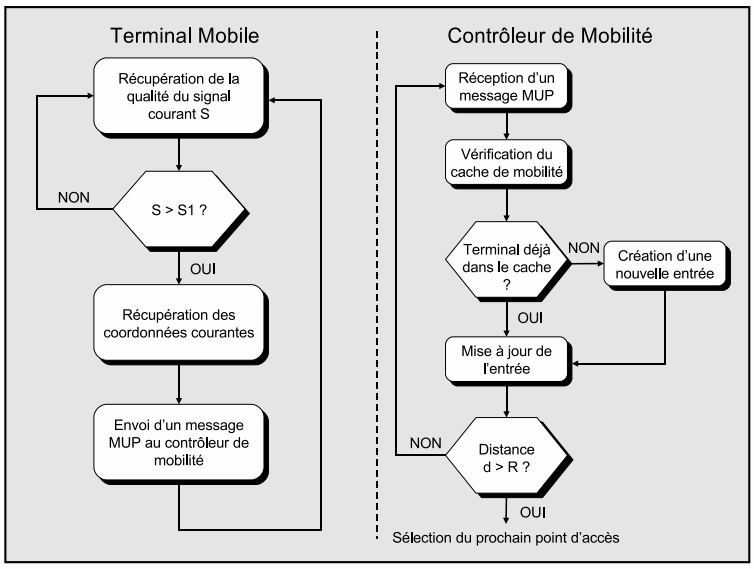


FIG. 8.1 – Mise à jour du cache de mobilité en fonction des seuils S_1 et R

surer qu'un contexte valide est actuellement positionné sur le terminal correspondant. Un contexte est une compilation des différents paramètres nécessaires pour améliorer le temps requis par un handover. Il se compose des mêmes informations que celles utilisées dans le protocole SHAPE à savoir le SSID, le canal radio et l'adresse MAC du prochain point d'accès. Il contient également des informations de niveau 3 (préfixe IPv6 et adresse lien local du routeur par défaut) lorsque le prochain point d'accès est situé dans un nouveau sous-réseau IPv6. Si un tel contexte est déjà positionné (champ *ID du prochain point d'accès* du cache de mobilité renseigné), le contrôleur doit alors s'assurer qu'il est toujours valide, c'est-à-dire que le point d'accès spécifié dans le contexte est toujours une cible potentielle pour le prochain handover. Dans le cas où il est toujours valide, le cache de mobilité est à jour. En revanche, si le contexte n'est plus valide ou lorsque aucun contexte n'est présent, le contrôleur doit en créer un nouveau en tenant compte des nouvelles informations du cache. Pour ce faire, la première étape consiste à déterminer le prochain point d'accès.

8.2.3 Détermination du prochain point d'accès

Le choix du prochain point d'accès d'un terminal mobile est basé sur l'anticipation de ses mouvements. A partir des coordonnées contenues dans les messages provenant des terminaux, le contrôleur de mobilité calcule leurs trajectoires afin d'anticiper leurs

futures positions. A ce stade de nos travaux, nous avons défini deux méthodes d'interpolation. Par la suite, nous considérerons un espace à deux dimensions.

Trajectoire rectiligne

Cette méthode assimile les mouvements des terminaux mobiles à des trajectoires rectilignes. Une interpolation linéaire est alors utilisée pour déterminer leurs futures positions. Notons les deux dernières positions d'un terminal par (x_0, y_0) et (x_1, y_1). L'équation de la trajectoire peut alors s'écrire sous forme paramétrique de la manière suivante :

$$\begin{cases} x(t) &= x_1 + t \times (x_1 - x_0) \\ y(t) &= y_1 + t \times (y_1 - y_0) \end{cases}$$

Interpolation de Lagrange

Cette deuxième méthode utilise les polynômes de Lagrange pour interpoler la trajectoire d'un terminal mobile. Cette méthode correspond à la base d'interpolation la plus simple : $P_i = x^i$ c'est-à-dire celle des monômes. Le polynôme de Lagrange est sans erreur pour le support d'interpolation c'est-à-dire que les $n + 1$ contraintes (ici les positions précédentes d'un terminal mobile) sont de la forme :

$$\forall_i \quad \lambda_n(x_i) = y_i$$

Après résolution du système d'équations découlant de ces contraintes on obtient :

$$\lambda_n(x) = \sum_{i=0}^{n} b_i(x).y_i \qquad \text{avec} \qquad b_i = \frac{\prod_{j=0, i\neq j}^{n}(x - x_j)}{\prod_{j=0, i\neq j}^{n}(x_i - x_j)}$$

Compte tenu des contraintes choisies, le polynôme obtenu est le seul satisfaisant ces contraintes. Cette formulation, si elle est explicite, n'en est pas moins un peu complexe à mettre en oeuvre. D'une part, on ne retrouve pas la forme classique d'un polynôme (les coefficients des puissances de x ne sont pas explicites). D'autre part, seuls les dénominateurs des polynômes b_i sont précalculables ce qui induit un coût non négligeable lors de l'interpolation. En effet, la complexité de l'évaluation de $\lambda_n(x)$ est en $O(n^2)$.

Si on considère trois positions d'un terminal mobile pour interpoler sa trajectoire, on obtient un polynôme de degré 2. Soit $(x0, y0)$, $(x1, y1)$ et $(x2, y2)$ les trois dernières positions d'un terminal. Le polynôme d'interpolation de Lagrange $\lambda_2(x)$ est une parabole de la forme :

$$\lambda_2(x) = y_0.b_0(x) + y_1.b_1(x) + y_2.b_2(x)$$

avec

$$b_0(x) = \frac{(x-x_1)(x-x_2)}{(x_0-x_1)(x_0-x_2)}, \quad b_1(x) = \frac{(x-x_0)(x-x_2)}{(x_1-x_0)(x_1-x_2)}, \quad b_2(x) = \frac{(x-x_0)(x-x_1)}{(x_2-x_0)(x_2-x_1)}$$

Afin de limiter le temps de calcul et les ressources utilisées au niveau du contrôleur de mobilité lors de la détermination d'une trajectoire, on ne considérera que les trois dernières positions des terminaux mobiles dans l'interpolation de Lagrange.

Sélection du futur point d'accès

Lorsque le contrôleur de mobilité a déterminé la trajectoire d'un terminal mobile, il peut prédire ses prochaines positions. Parmi les points d'accès des cellules adjacentes, le contrôleur de mobilité sélectionne ceux qui couvrent ou vont couvrir (en fonction de la trajectoire calculée) le terminal. Cette première liste constitue les points d'accès candidats. Lorsque la liste ne contient aucun élément, le contrôleur de mobilité déduit que le terminal se dirige vers une zone hors de portée des points d'accès dont il a la charge. Dans le cas où la liste comporte un unique élément, c'est le point d'accès en question qui est sélectionné comme prochain point d'accès. En revanche, si la liste contient plus d'un élément, le contrôleur de mobilité sélectionne le point d'accès candidat qui est le plus à même de couvrir le terminal mobile par rapport à sa trajectoire (voir la figure 8.2).

Notons le rayon de la zone de couverture d'un point d'accès par G et ses coordonnées par (a, b). Pour tous les points d'accès candidats, le contrôleur de mobilité va résoudre le système d'équations suivant :

$$\begin{cases} G^2 = (x-a)^2 + (y-b)^2 \\ T(X) \end{cases}$$

La résolution de ce système produit les coordonnées des points d'intersection entre la trajectoire d'un terminal (donnée par l'équation $T(X)$ qui correspond à l'équation

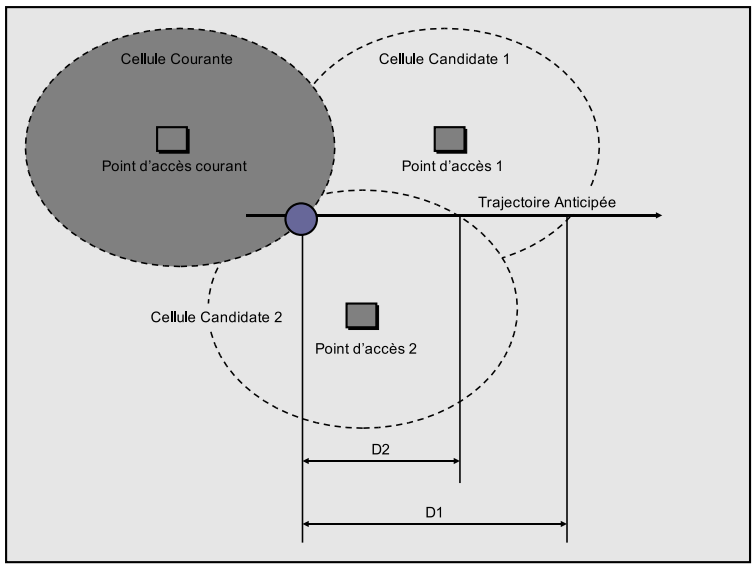


FIG. 8.2 – Sélection du prochain point d'accès en fonction des trajectoires

d'une droite ou d'un polynôme) et la portée maximale du point d'accès (qui correspond à l'équation du cercle de rayon G et de centre (a, b)). Le point d'accès sélectionné est celui qui offre la plus grande distance entre les deux points d'intersection calculés par le système précédent (i.e. la plus grande zone de couverture radio en fonction de la trajectoire anticipée). Suivant les scénarii, cette méthode devrait permettre de réduire le nombre de handovers nécessaires pour un déplacement donné. D'autres paramètres pourraient également être pris en compte pour finaliser la décision, par exemple le nombre de terminaux associés sur chaque point d'accès.

8.2.4 Déroulement du Handover

Lorsque le contrôleur de mobilité a déterminé le prochain point d'accès d'un terminal, il crée un contexte lié à ce point d'accès et l'envoie au terminal à l'aide d'un message CT (*Context Transfer*). A sa réception, le terminal enregistre le contexte présent dans le message jusqu'à ce que le contrôleur envoie un nouveau contexte ou jusqu'à la nécessité d'effectuer un handover.

Lorsque la qualité du signal reçu par un terminal franchit le seuil S_2 indiquant un signal faible (voir la section 8.2.2), il débute la procédure de handover. Grâce au contexte précédemment enregistré, il connaît par avance son futur point d'accès, rendant la phase de découverte inutile. Dès lors, il peut directement passer à la phase d'authentification

en envoyant une requête d'authentification sur le canal et vers le SSID indiqués par le contexte. A la réception d'une réponse positive de la part du point d'accès cible, le terminal effectue la phase d'association et termine le handover de niveau 2. En raison de la suppression de la phase de découverte, le temps de latence engendré par le handover de niveau 2 devrait être ici encore plus réduit que lors de l'utilisation protocole SHAPE.

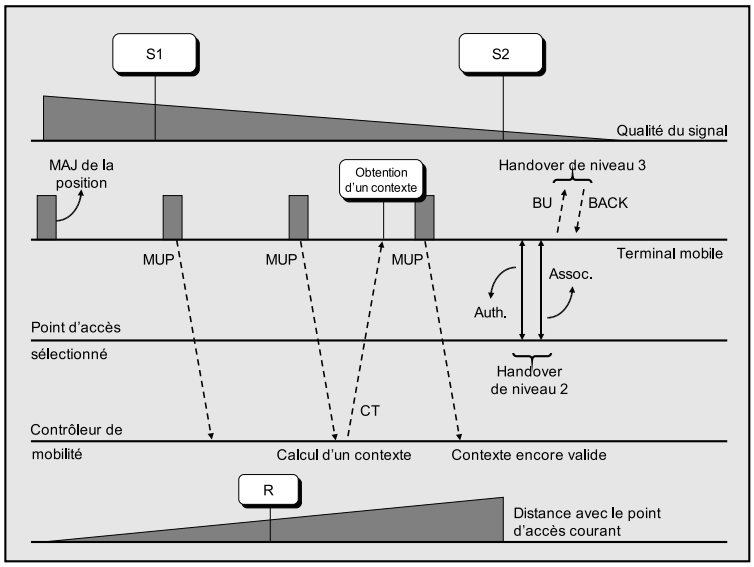


FIG. 8.3 – Déroulement du protocole FLH

Quand le point d'accès sélectionné par le contrôleur se trouve dans un nouveau sous-réseau IPv6, le contexte contient en plus des informations de niveau 3 telles que le préfixe IPv6 du nouveau lien et l'adresse du routeur par défaut. La présence de ces informations au sein d'un contexte signifie au terminal de manière implicite qu'il doit, à la suite du handover de niveau 2, réaliser un handover de niveau 3. Dans le protocole FLH, la procédure de handover de niveau 3 reste identique à celle proposée dans le protocole SHAPE. Grâce aux informations du contexte et à la procédure ODAD, le handover de niveau 3 consiste uniquement en la mise à jour de l'adresse temporaire auprès de l'agent mère. A l'instar du protocole SHAPE, le protocole FLH utilise une architecture hiérarchique qui optimise cette dernière étape. En fin de compte, le temps total de déconnexion dû à un handover de niveau 2 et 3 devrait donc être globalement inférieur (en raison de la suppression complète de la phase de découverte du niveau 2) à celui observé dans le protocole SHAPE. La figure 8.3 illustre les différents échanges de message du protocole FLH.

8.3 Evaluation des performances

Les différentes évaluations du protocole FLH ont toutes été réalisées par simulation. Pour cela, nous avons intégré notre solution dans le simulateur de réseaux sans fil SimulX [93]. Dans une première étude, nous avons comparé le protocole FLH avec la norme IEEE 802.11 et avec le protocole MIPv6 dont les mécanismes constituent la procédure standard d'un handover.

Dans cette première évaluation, nous avons défini quatre scénarii de simulation. Ces différents scénarii ont été élaborés conjointement avec les centres recherche et développement de France Télécom afin d'illustrer des environnements réalistes.

8.3.1 Scénarii de simulation

Scénario 1

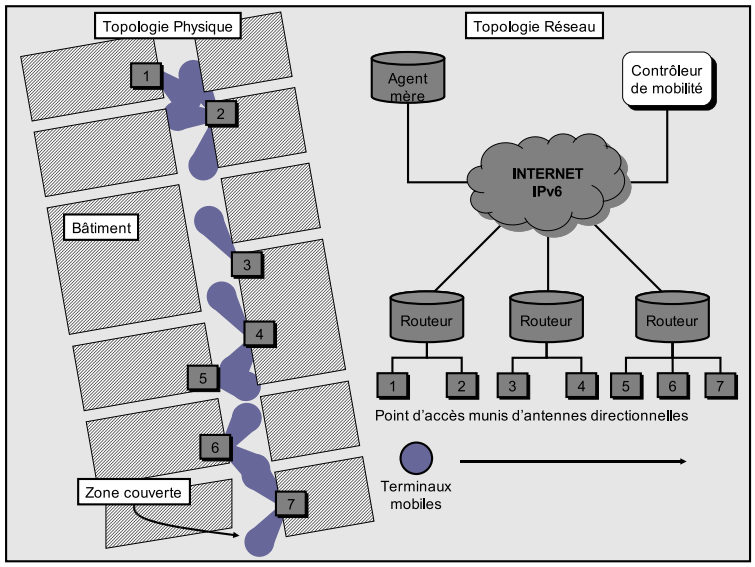


FIG. 8.4 – Scénario 1

Le premier scénario correspond à des points d'accès déployés le long d'une ligne de bus au sein d'une ville. Il se compose de dix terminaux mobiles et de sept points d'accès situés dans trois sous-réseaux IPv6 différents. La portée de chaque équipement sans fil est de 30 mètres. Les points d'accès utilisent uniquement les canaux radio 1, 6 et 11 et sont munis d'antennes directionnelles leur permettant de couvrir partiellement

la rue. Les terminaux mobiles circulent dans la rue en suivant une trajectoire rectiligne à la vitesse constante de 50 Km/h. Lors de leur parcours, ils effectueront donc des handovers de niveau 2 et de niveau 3. Le RTT (*Round Trip Time*) entre l'agent mère et les différents réseaux visités est de 40 millisecondes et celui entre les terminaux mobiles et le contrôleur de mobilité est de 60 millisecondes. La figure 8.4 illustre la topologie réseau utilisée dans ce scénario.

Scénario 2

Le deuxième scénario fait référence à des points d'accès déployés le long d'une autoroute. Il se compose de six points d'accès et de dix terminaux mobiles. Les canaux radio alloués aux différents points d'accès sont illustrés sur la figure 8.5. La portée de chaque équipement sans fil est de 100 mètres. Chaque point d'accès est espacé de 180 mètres avec ses voisins. En outre, ils sont raccordés à deux sous-réseaux IPv6 différents, ce qui implique que les terminaux mobiles effectueront des handovers de niveau 2 et 3. Les terminaux mobiles parcourent une distance de 900 mètres de manière rectiligne à 130 Km/h. Le RTT est de 20 millisecondes entre les terminaux mobiles et l'agent mère, et de 30 millisecondes entre les terminaux mobiles et le contrôleur de mobilité.

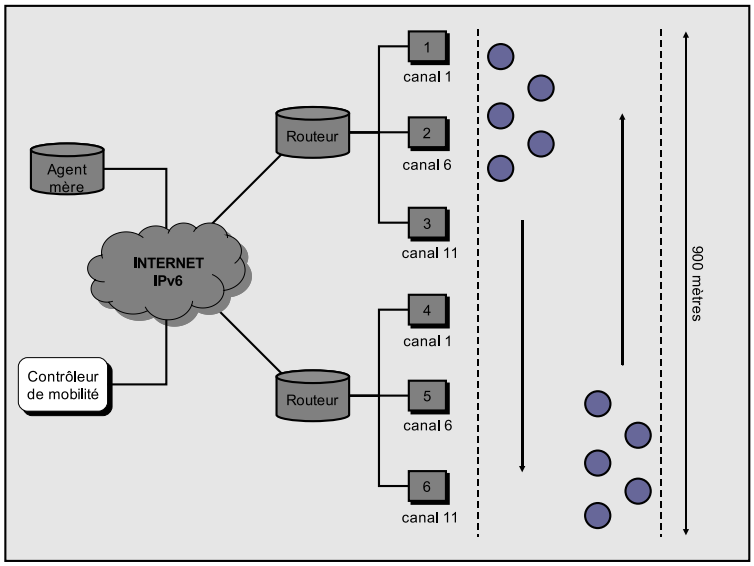


FIG. 8.5 – Scénario 2

Scénario 3

Le troisième scénario met en jeu un terminal mobile et huit points d'accès déployés le long d'une ligne de chemin de fer. La portée des équipements sans fil est ici de 2600 mètres et comme précédemment, seuls les canaux 1, 6 et 11 sont utilisés. Chaque point d'accès est ici espacé de 5 Km avec ses voisins. Le terminal mobile débute la simulation dans une gare et se déplace jusqu'à une seconde gare. Chaque gare disposant de son propre sous-réseau, le terminal effectuera des handovers de niveau 2 (dans le voisinage d'une gare) et des handovers de niveau 3 (lorsque le terminal s'approche de la prochaine gare). Le terminal mobile se déplace à 300 Km/h en suivant une trajectoire rectiligne. Le RTT est de 20 millisecondes entre les terminaux mobiles et l'agent mère, et de 20 millisecondes entre les terminaux mobiles et le contrôleur de mobilité. La figure 8.6 illustre la topologie réseau utilisée dans le scénario 3.

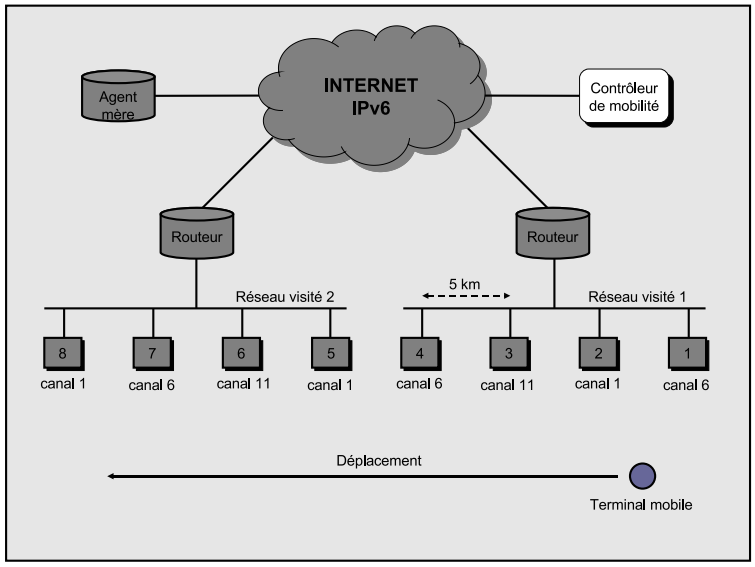


FIG. 8.6 – Scénario 3

Scénario 4

Enfin, le scénario 4 simule un environnement intérieur dans lequel la portée des équipements sans fil est plus limitée (voir la figure 8.7). Ce dernier scénario introduit douze points d'accès et dix terminaux mobiles. La portée des équipements sans fil est de 40 mètres. Les points d'accès sont placés de manière à couvrir une zone de 186 mètres sur 200 mètres et se voient attribuer chacun un canal radio unique. chaque terminal mobile effectue dix déplacements aléatoires. Avant chaque nouveau déplacement, le

terminal choisit aléatoirement une nouvelle destination dans la zone couverte par tous les points d'accès et s'y rend en suivant une trajectoire rectiligne à la vitesse de 1 m/s. Tous les points d'accès étant situés dans le même sous-réseau, les terminaux mobiles effectueront uniquement des handovers de niveau 2. Le RTT est de 40 millisecondes entre les terminaux mobiles et le contrôleur de mobilité.

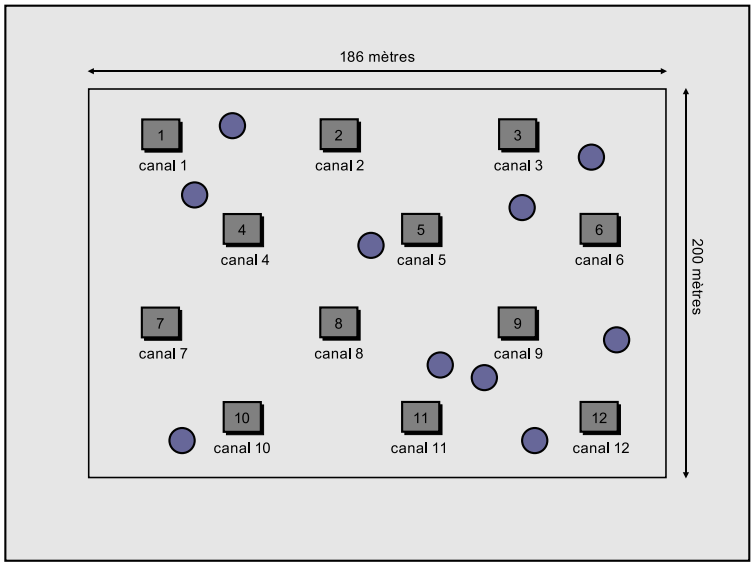


FIG. 8.7 – Scénario 4

8.3.2 Paramètres de simulation

En plus des temps de latence engendrés par les handovers, nous avons évalué la pertinence de nos différents choix concernant les seuils utilisés par le protocole FLH. Grâce à l'outil de simulation, il a été relativement facile d'influer sur divers paramètres.

Gestion des seuils S1 et R

Concernant les seuils S_1 et R, nous avons été contraint de les adapter en raison de l'absence de couche physique dans notre simulateur. En effet, la couverture offerte par les points d'accès est de type *tout ou rien* dans SimulX : soit le terminal est couvert (lorsqu'il est dans la cellule radio du point d'accès), soit il ne l'est pas (lorsqu'il est sorti de la cellule). Il n'y a donc aucun modèle de dégradation de signaux radio implémenté. Pour les simulations, nous avons donc choisi de coupler les seuils S_1 et R en un

unique seuil R'. Ce dernier correspond à la distance maximale entre un terminal mobile et son point d'accès courant pour laquelle la qualité du signal est encore suffisante. Lorsque le terminal franchit le seuil R', il commence à envoyer les messages MUP au contrôleur de mobilité. Dès réception, le contrôleur ne tient plus compte du seuil R et vérifie systématiquement le contexte contenu dans le cache de mobilité.

Dans notre spécification du protocole FLH, nous avions positionné le seuil R à 50% de la portée maximale des points d'accès. Dès lors, nous avons choisi la même valeur par défaut pour notre seuil de simulation R'. Trois valeurs supplémentaires ont également été définies (R' = 0%, R' = 80% et R' = 95% de la portée maximale des points d'accès) afin d'analyser l'influence du seuil R' et par extension l'influence des seuils S_1 et R sur les performances du protocole FLH.

Erreur de géolocalisation

Dans un premier temps, nous avons souhaité évaluer l'influence de la précision du système de géolocalisation sur les performances du protocole FLH. Pour ce faire, nous avons introduit des erreurs dans les coordonnées des terminaux mobiles envoyées au contrôleur de mobilité. Quatre seuils d'erreurs ont été définis : 0, 3, 7 et 10 mètres. Ces seuils correspondent approximativement aux précisions offertes par les systèmes de géolocalisation actuels (e.g. précision de 1 à 3 mètres pour les systèmes de géolocalisation basés sur la technologie Wi-Fi, 10 mètres pour le système GPS).

Notons T le seuil d'erreurs de géolocalisation et (x, y) les coordonnées du terminal mobile. Soit E un nombre réel tiré aléatoirement dans l'intervalle $[0; T]$. Pour chaque position envoyée au contrôleur de mobilité, nous ajoutons ou soustrayons aléatoirement une valeur aux coordonnées de la manière suivante :

$$
\begin{aligned}
&\text{signe} = \text{random}(0, 1)\\
&\text{Si signe} < 0,5\\
&\text{Alors}\\
&\qquad x = x - E/2\\
&\qquad y = y + E\%2\\
&\text{Sinon}\\
&\qquad x = x + E\%2\\
&\qquad y = y - E/2
\end{aligned}
$$

où la fonction $random(0, 1)$ retourne un nombre réel compris dans l'intervalle $[0; 1]$, $E/2$ renvoie le quotient de la division entière de E par 2 et $E\%2$ renvoie le reste de cette même division.

RTT entre le contrôleur de mobilité et les terminaux

Nous avons également mesuré l'incidence du RTT (*Round Trip Time*) entre les terminaux mobiles et le contrôleur de mobilité sur les performances du protocole FLH. Pour mener à bien cette étude, trois valeurs de RTT ont été définies : 30 (valeur par défaut), 100 et 300 millisecondes. Nous nous sommes cependant restreints dans cette étude au scénario 2 car il semblait être le scénario le plus sensible aux paramètres de simulations en raison de la vitesse relativement élevée des terminaux mobiles et de la portée des équipements sans fil.

Paramètres pour la procédure standard

Lors de la simulation de la procédure standard (802.11 + MIPv6), la fréquence d'émission des messages RA a été positionnée entre 0,03 et 0,07 secondes comme cela est suggéré dans [46]. On notera que lors de l'évaluation du protocole FLH, ce paramètre est resté à sa valeur par défaut (i.e. entre 200 et 600 secondes [72]). Concernant les handovers de niveau 2, nous avons respectivement fixé les paramètres *MinChannelTime* et *MaxChannelTime* à 30 et 200 millisecondes. Ces valeurs correspondent aux paramètres utilisés sur les anciens firmware des cartes Cisco. Dans le simulateur SimulX, le comportement par défaut des cartes sans fil consiste à s'associer au premier point d'accès découvert après avoir attendu *MaxChannelTime* sur le canal correspondant.

Le tableau 8.2 récapitule les différents paramètres utilisés pendant les simulations.

Paramètre	Type	Valeur	Description
$Freq_{pos}$	seconde	1	Fréquence d'obtention des coordonnées
ε_{geo}	mètre	$\{0; 3; 7; 10\}$ (0 par défaut)	Erreur maximale introduites dans les coordonnées des terminaux
R'	pourcentage	$\{0; 50; 80; 95\}$ (50 par défaut)	Pourcentage de la portée maximale du point d'accès à partir duquel le terminal envoi des messages MUP au contrôleur
MinChannelTime	milliseconde	30	Durée minimale de sondage d'un canal
MaxChannelTime	milliseconde	200	Durée maximale de sondage d'un canal
RTT_{cm}	milliseconde	$\{30; 100; 300\}$ (30 par défaut)	Délai entre le contrôleur de mobilité et les terminaux mobiles
$Freq_{ra}$ (MIPv6)	milliseconde	$[30, 70]$	Fréquence d'émission des messages RA lors de l'utilisation du protocole MIPv6
$Freq_{ra}$ (FLH)	seconde	$[200, 600]$	Fréquence d'émission des messages RA lors de l'utilisation du protocole FLH

TAB. 8.2 – Paramètres de simulation

8.3.3 Résultats de simulation

Temps de latence

Le premier objectif du protocole FLH est de réduire significativement les temps de latence engendrés par les handovers de niveau 2 et de niveau 3 dans les réseaux Wi-Fi IPv6. Les résultats présentés ici ont été obtenus avec tous les paramètres de simulation positionnés à leurs valeurs par défaut (voir la table 8.2). Pour chaque protocole (802.11 + MIPv6, FLH avec interpolation linéaire et FLH avec interpolation de Lagrange) nous avons rejoué chaque scénario 100 fois.

La figure 8.8 présente les temps de latence moyens engendrés par les handovers de niveau 2 (axe de gauche) ainsi que les écart-types correspondants (axe de droite) pour chaque protocole. On constate que notre solution permet de réaliser des handovers de niveau 2 en 1,7 millisecondes (scénarii 2 et 3) et en 6 millisecondes (scénario 4) en moyenne. Ces temps sont largement inférieurs à ceux obtenus avec la méthode standard

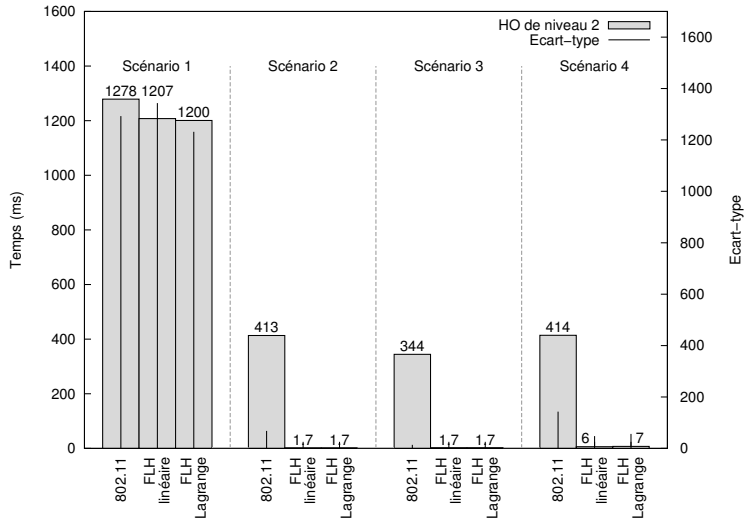


FIG. 8.8 – Temps de latence moyens et écart-types des handovers de niveau 2

(802.11) pour laquelle un handover de niveau 2 engendre un temps de déconnexion d'environ 400 millisecondes. Cette réduction est essentiellement rendue possible par la pré-sélection du futur point d'accès des terminaux mobiles, ce qui permet de se passer entièrement de la phase de découverte de niveau 2. Dès lors, le handover de niveau 2 n'est plus composé que des phases d'authentification et d'association. Nous avons cependant pu observer lors de notre évaluation du protocole SHAPE (voir le chapitre 7), que la réinitialisation du périphérique sans fil et plus précisément le changement de canal radio ajoutait un délai non négligeable (environ 10 millisecondes avec un périphérique sans fil muni d'une puce Atheros) au temps de latence global. Il faut donc également tenir compte de ces délais supplémentaires dans les résultats présentés ici. Les écart-types importants observés pour la méthode standard sont principalement dus à la phase de découverte de niveau 2. En effet, comme nous l'avons déjà vu, la durée de cette étape dépend directement du nombre de canaux radio à sonder avant de découvrir un nouveau point d'accès.

Dans le scénario 1, les temps de latence sont par contre largement plus importants quel que soit le protocole utilisé. En raison de la couverture partielle offerte dans ce scénario, les terminaux mobiles sont souvent dans l'incapacité d'obtenir une connectivité réseau et ce, pendant une période de temps considérable (environ 1,3 secondes). Cela explique notamment les écart-types très importants observés dans le scénario 1. Lors de l'utilisation du protocole FLH, le contrôleur de mobilité est incapable de sélectionner un nouveau point d'accès pour un terminal se dirigeant vers une zone non couverte. Même si le terminal détient un contexte avant de se déplacer dans une telle zone, le point d'accès indiqué dans ce contexte ne sera pas à portée radio. Les terminaux mobiles sont

donc contraints d'effectuer de nombreuses procédures standard de handover (de l'ordre de 90% des handovers réalisés), ramenant les performance du protocole FLH proches de celles obtenues avec le protocole 802.11 classique.

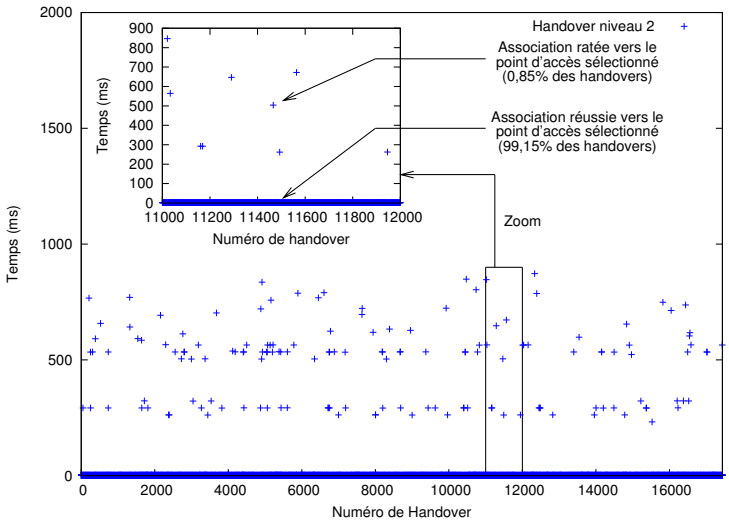


FIG. 8.9 – Détails des handovers de niveau 2 pour le protocole FLH dans le scénario 4

On peut également relever que les temps de latence moyens observés dans le scénario 4 lors de l'utilisation du protocole FLH sont légèrement supérieurs à ceux obtenus pour les scénarii 2 et 3. La figure 8.9 qui illustre les temps de handovers du scénario 4 lors de l'utilisation du protocole FLH avec une interpolation linéaire permet d'expliquer ce phénomène. A première vue, les temps de handovers se concentrent autour de 3 valeurs, mais en regardant dans la partie mise en évidence, on s'aperçoit que 99,15% des handovers sont inférieurs à 2 millisecondes. Les 0,85% restants correspondent aux cas où les terminaux mobiles ont changé de trajectoire juste avant de passer sous le seuil R'. De ce fait, le point d'accès sélectionné par le contrôleur de mobilité n'est plus à portée radio lors du handover effectif, ce qui oblige le terminal mobile à effectuer une procédure standard. Cela explique les temps de handovers supérieurs à 200 millisecondes observés sur la figure 8.9. Lors de l'utilisation d'une interpolation de Lagrange, nous obtenons un comportement similaire.

Dans les trois premiers scénarii, un handover de niveau 2 peut être suivi d'un handover de niveau 3. La figure 8.10 illustre les temps de latence moyens (axe de gauche) et les écart-types (axe de droite) correspondants aux handovers de niveau 3. Nous pouvons noter que nous obtenons également de meilleurs résultats avec notre solution qu'avec le protocole MIPv6. En effet, il faut approximativement 23 millisecondes avec FLH pour réaliser un handover de niveau 3 (scénarii 2 et 3) contre 461 (scénario 2) et 396 (scénario 3) millisecondes lors de l'utilisation du protocole MIPv6. Dans le cas de FLH, ces

résultats satisfaisants s'expliquent par le fait que nous utilisons les mêmes optimisations que dans le protocole SHAPE : les terminaux mobiles peuvent envoyer un BU à l'agent mère dès la fin du handover de niveau 2 sans tenir compte des messages RA. Même lorsque ces messages sont envoyés à la fréquence maximale autorisée, le mécanisme de détection des nouveaux liens utilisé dans MIPv6 introduit toujours un délai supplémentaire dans le temps de latence global. Les résultats présentés ici pour le protocole MIPv6 ne font donc que confirmer ceux que nous avions obtenus dans le chapitre précédent.

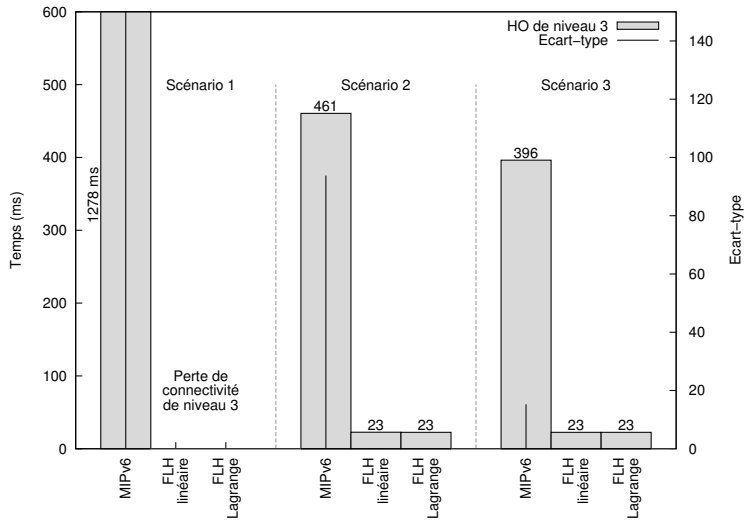


FIG. 8.10 – Temps de latence moyens et écart-types des handovers de niveau 3

Concernant le scénario 1, nous avons vu que les terminaux mobiles traversaient de nombreuses zones non couvertes par les points d'accès. Dans le cas du protocole FLH, le contrôleur de mobilité est incapable de fournir un contexte valide aux terminaux mobiles lorsqu'ils se dirigent vers de telles zones. Nous avons donc constaté qu'ils étaient contraints de réaliser une procédure standard de handover de niveau 2 dès qu'ils se situaient à nouveau dans la portée radio d'un point d'accès. Suite à une telle association, il est possible qu'ils doivent également effectuer un handover de niveau 3. Ne disposant pas d'un contexte valide, les terminaux mobiles sont alors forcés d'utiliser les mécanismes de base du protocole MIPv6 et notamment la procédure de détection des nouveaux liens basée sur la réception des messages RA. Or, nous avons configuré la fréquence d'émission des RA entre 200 et 600 secondes lors de l'utilisation du protocole FLH, ce qui n'est évidemment pas adapté pour une gestion de la mobilité. Les terminaux mobiles n'ont donc jamais l'occasion dans toute la simulation de recevoir un RA, ce qui rend impossible la détection des nouveaux liens IPv6. Par conséquent, les terminaux mobiles n'ont pas conscience des éventuels changements de sous-réseaux, ce qui engendre une perte de connectivité de niveau 3. Il est donc nécessaire d'intégrer au protocole FLH des mécanismes permettant d'éviter ces problèmes tout en conservant

une fréquence d'émission des messages RA acceptable en termes de consommation de bande passante.

Coût de la signalisation

Etant donné que le protocole FLH introduit une nouvelle entité réseau qui communique directement avec les terminaux mobiles, nous avons tenté d'évaluer le coût de cette signalisation supplémentaire. Pour la compréhension des résultats présentés dans cette section, il est important de mentionner que dans tous les scénarii, les points d'accès envoient un message *Beacon* toutes les 100 millisecondes. En outre, les résultats ont été obtenus en positionnant tous les paramètres de simulation à leurs valeurs par défaut et correspondent uniquement au trafic de signalisation. La figure 8.11 représente le nombre moyen de messages de signalisation envoyés sur les liens radio (axe de gauche) et les écart-types correspondants (axe de droite) pour chaque scénario et chaque protocole. Le trafic de signalisation de niveau 2 comprend les messages *Beacon*, les accusés de réception, les requêtes / réponses de *Probe*, d'authentification et d'association. Ce trafic englobe également les messages de contrôle du niveau 3 qui correspondent aux RA, BU et BACK. Lors de l'utilisation du protocole FLH, les résultats tiennent également compte des messages MUP et CT, introduits par notre solution.

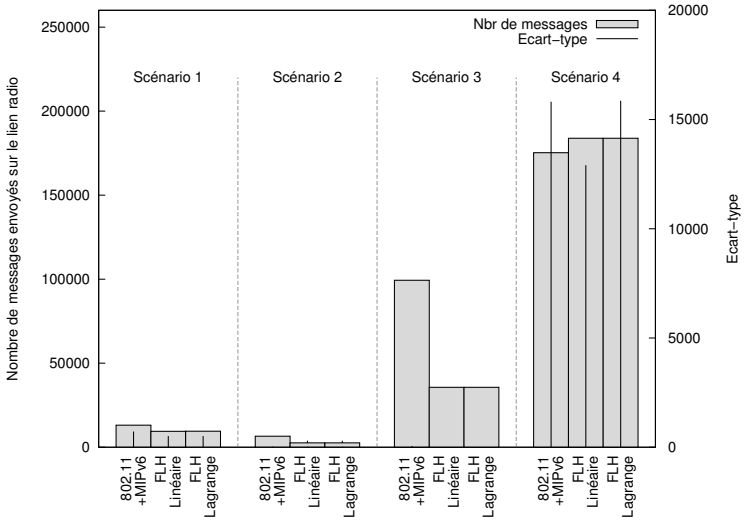
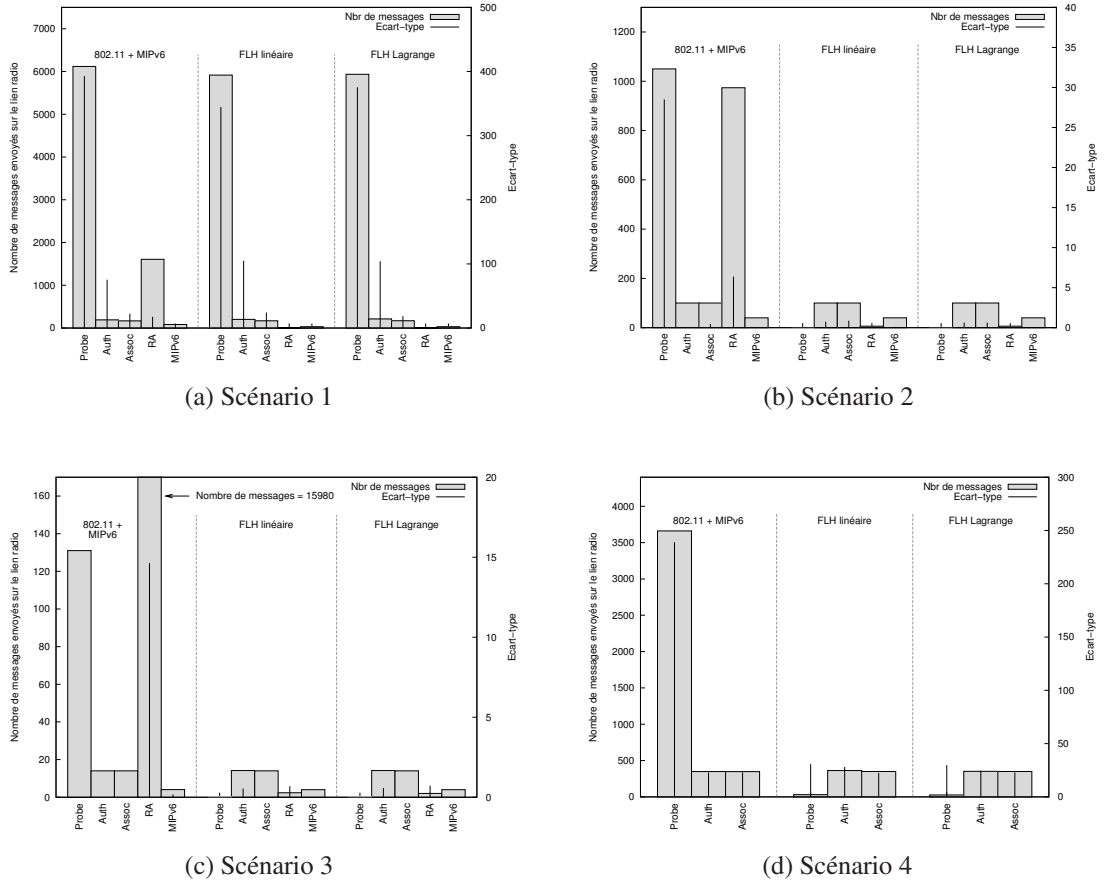


FIG. 8.11 – Nombre moyen et écart-types des messages de signalisation échangés sur les liens radio

Dans les trois premiers scénarii, il apparaît que notre approche utilise moins de messages de contrôle que la procédure standard alors que c'est l'inverse dans le scénario

4. Cette observation est plus claire dans la figure 8.12 qui représente le détail des messages de contrôle échangés dans chaque scénario. Chaque message y a été classé selon son type : *Probe*, authentification, association, RA et MIPv6. Les autres types de messages (i.e. *Beacon*, accusé de réception, MUP et CT) n'ont pas été représentés sur ces figures pour des raisons de lisibilité ou en raison des limitations du simulateur. Néanmoins, la correspondance entre les figures détaillées et la figure 8.11 permet de se faire une idée de la proportion des messages MUP et CT échangés lors de l'utilisation du protocole FLH.



(a) Scénario 1

(b) Scénario 2

(c) Scénario 3

(d) Scénario 4

FIG. 8.12 – Détails du nombre moyen et des écart-types des messages de signalisation échangés sur les liens radio

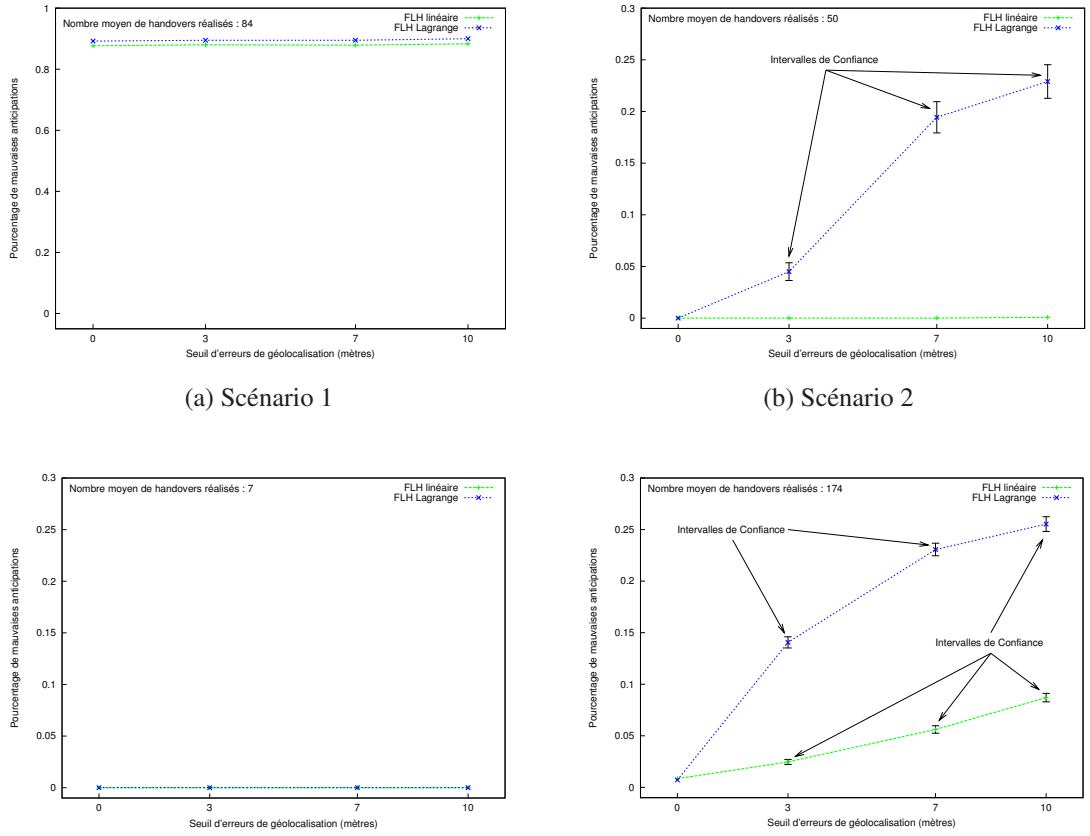
Nous constatons que le trafic de contrôle généré lors de l'utilisation de la méthode standard est essentiellement composé de requêtes / réponses de probe et de messages RA. Rappelons que les requêtes et réponses de *Probe* sont envoyées lors de la phase de

découverte d'un handover de niveau 2. De plus, le protocole MIPv6 nécessite une fréquence d'émission des RA élevée pour être relativement performant. Nous avions donc configuré cette fréquence entre 0,03 et 0,07 secondes ce qui explique le nombre important de RA lors de l'utilisation de la méthode standard. Dans le protocole FLH, c'est uniquement lors de mauvaises anticipations que les terminaux mobiles réalisent des phases de découverte et qu'ils peuvent être conduits à utiliser les RA. Dès lors, la réduction du nombre de messages *Probe* et la faible fréquence des RA (positionnée entre 200 et 600 secondes pour le protocole FLH) permet de contrebalancer les messages MUP et CT introduits par le protocole FLH (scénarii 2 et 3). Même en l'absence de messages RA (désactivés dans le scénario 4 car les points d'accès se situent tous dans le même sous-réseau), la réduction du nombre de messages *Probe* permet toujours de compenser le nombre des nouveaux messages. Cependant, comme nous avons pu l'observer dans le scénario 1, le trafic de contrôle est pratiquement similaire entre la méthode standard et le protocole FLH malgré la différence entre les fréquences d'émissions des RA. En raison de la couverture partielle des points d'accès, les terminaux mobiles effectuent quasiment autant de phases de découvertes avec FLH que dans la méthode standard. Couplé avec les messages MUP et CT, le trafic de contrôle global du protocole FLH finit donc pratiquement par atteindre celui de la méthode standard. Enfin, on peut relever qu'il n'y a pratiquement pas de différence entre les méthodes d'interpolation linéaire et de Lagrange en raison du caractère rectiligne des déplacements des terminaux dans les différents scénarii.

Erreurs de géolocalisation

Nous avons également étudié l'influence des erreurs de géolocalisation sur notre protocole. Pour ce faire, nous avons utilisé différents seuils d'erreurs, répertoriés dans la table 8.2. La figure 8.13 représente la proportion moyenne (en pourcentage) des mauvaises anticipations du prochain point d'accès qui ont engendré une procédure standard de handover. Pour chaque seuil d'erreurs, nous avons fait le ratio entre le nombre de handovers pour lesquels l'anticipation n'a pas fonctionné et le nombre total de handovers réalisés. Les intervalles de confiance représentés sur cette figure ont été obtenus au risque 0,05. On peut les interpréter de la manière suivante : avec une probabilité de 0,95, la valeur moyenne du pourcentage de mauvaises anticipations se trouve entre les bornes de l'intervalle. Pour des raisons de lisibilité, nous n'avons pas représenté les intervalles de confiance lorsqu'ils étaient négligeables (i.e. largeur de l'intervalle inférieure à 0,005). Lors de cette évaluation, nous avons notamment observé deux types d'erreurs : soit le point d'accès sélectionné par le contrôleur de mobilité n'est pas à portée radio du terminal lors du handover effectif, soit le terminal n'a pas reçu de messages CT. Ce dernier cas peut éventuellement survenir lorsque le contrôleur de mobilité n'a

pas été en mesure de sélectionner un nouveau point d'accès pour un terminal mobile disposant d'une trajectoire spécifique.



(a) Scénario 1

(b) Scénario 2

(c) Scénario 3

(d) Scénario 4

FIG. 8.13 – Influence des erreurs de géolocalisation sur le protocole FLH

Nous avons déjà évoqué la particularité du scénario 1 dans lequel les terminaux mobiles effectuent majoritairement des procédures standard de handovers, alors qu'il n'y a pas d'erreurs de géolocalisation. La figure 8.13(a) permet de confirmer cette observation. En effet, on peut y relever qu'environ 90% des handovers réalisés par les terminaux mobiles suivent la procédure standard en raison des nombreuses zones ne disposant pas d'une couverture radio. En effet, de telles zones ne permettent pas au contrôleur d'anticiper le futur point d'accès d'un terminal. On peut également noter que l'introduction d'erreurs de géolocalisation ne modifie en rien ce comportement, aussi bien lors d'interpolations linéaires que lors d'interpolations de Lagrange.

Dans les scénarii 2 et 3, on peut observer que les erreurs de géolocalisation n'ont que peu d'influence sur le protocole FLH lors de l'utilisation d'une interpolation linéaire. En raison de la disposition des points d'accès, le contrôleur de mobilité sélectionne toujours un point d'accès valide (parmi les deux voisins de chaque point d'accès) même lorsque le seuil d'erreurs est positionné à 10 mètres. Par contre, pour l'interpolation de Lagrange, le nombre de mauvaises anticipations augmente de manière significative (scénario 2). Lors d'erreurs de géolocalisation, les trajectoires anticipées à l'aide de cette interpolation peuvent indiquer que les terminaux mobiles se dirigent vers des zones non couvertes par des points d'accès, ou qu'ils reviennent sur leurs pas (voir la figure 8.14). Or cela ne reflète pas leurs réels mouvements. Dans le scénario 2, le contrôleur n'a pas l'occasion de rectifier de telles prédictions en raison de la vitesse de déplacement des terminaux et de la faible portée radio des équipements. C'est pourquoi le nombre de mauvaises anticipations obtenues avec l'interpolation de Lagrange est important. Ces erreurs ne touchent cependant pas le scénario 3, en raison d'une portée radio plus conséquente des équipements sans fil. Dès lors, les terminaux mobiles restent associés plus longtemps aux points d'accès ce qui laisse plus de temps au contrôleur de mobilité pour rectifier une éventuelle mauvaise anticipation.

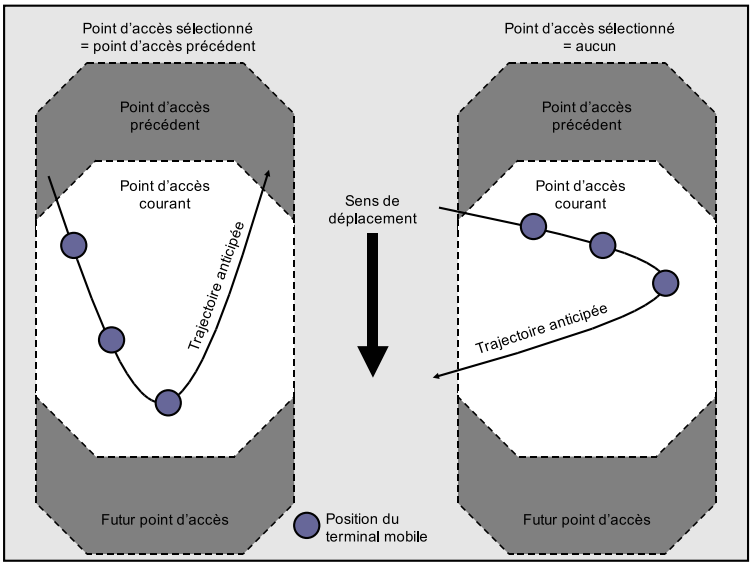


FIG. 8.14 – Cas d'erreurs avec l'interpolation de Lagrange

Enfin, nous avons déjà observé dans le scénario 4 que les terminaux mobiles effectuent des procédures standard de handovers. Lorsqu'on introduit des erreurs de géolocalisation, le nombre de mauvaises anticipations augmente quelle que soit la méthode d'interpolation utilisée. Le pourcentage de mauvaises anticipations reste cependant relativement limité dans le cas de l'interpolation linéaire (9% d'erreurs dans le pire des

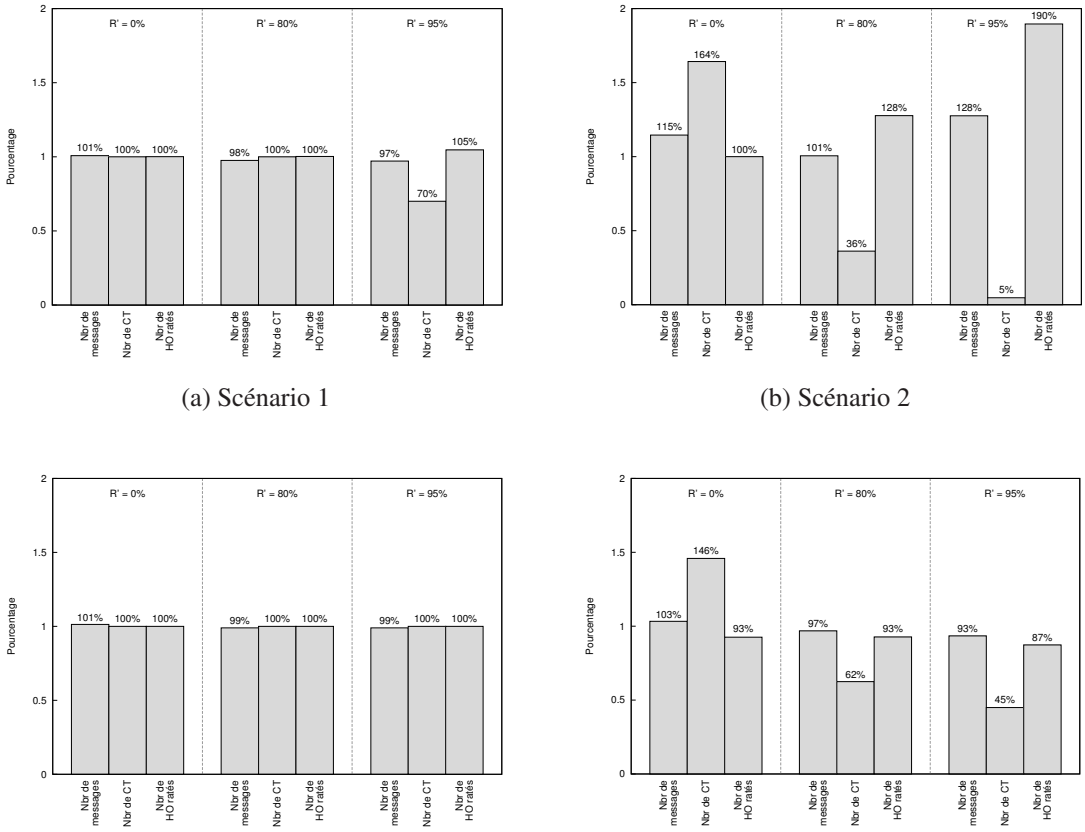
cas). Par contre, le nombre de mauvaises anticipations restent assez important dans le cas de l'interpolation de Lagrange, étant donné qu'elle souffre des mêmes problèmes que ceux qui sont survenus dans le scénario 2.

Influence du seuil R'

L'une des raisons justifiant la mise en place des seuils S_1 et R repose sur la volonté de limiter l'émission de messages MUP afin de réduire la charge sur le contrôleur de mobilité, sans affecter les performances du protocole FLH. Le simulateur SimulX ne disposant pas d'un modèle de dégradation des signaux radio, nous avons simulé les seuils S_1 et R par le seuil R' (cf. section 8.3.2). Dans nos simulations, nous avons souhaité analyser l'influence du seuil R' et par extension des seuils S_1 et R sur le comportement du protocole. Pour ce faire, nous avons rejoué 100 fois chaque scénario pour chaque valeur prédéfinie du seuil R' (voir le tableau 8.2). Les résultats présentés dans cette section concernent le protocole FLH avec interpolation linéaire.

La figure 8.15 présente les valeurs moyennes du nombre total de messages de contrôle générés, du nombres de messages CT envoyés, et du nombre de mauvaises anticipations réalisées pour chaque scénario et chaque valeur du seuil R'. Les résultats sont ici représentés sous forme de pourcentages proportionnels aux résultats obtenus pour la valeur par défaut de R' (i.e. les valeurs obtenues pour $R' = 50\%$ correspondent à 100% sur le graphique). Comme on pouvait le penser, plus le seuil R' est grand, plus le nombre de messages MUP et CT est limité. En revanche, on peut observer que le nombre total de messages de contrôle peut soit augmenter (scénario 2), soit rester stable (scénario 3), soit légèrement diminuer (scénarii 1 et 4). En raison de l'environnement particulier du scénario 1, le seuil R' n'a pas d'influence sur le nombre de mauvaises anticipations. Par conséquent, le nombre total de messages de contrôle n'est que légèrement réduit lorsque le seuil R' est positionné à 80% ou 95%. Dans le scénario 2, les terminaux mobiles se déplacent rapidement et peuvent ne pas disposer du temps nécessaire pour recevoir un message CT. De ce fait, le nombre de mauvaises anticipations augmente significativement, ce qui a pour conséquence de générer plus de trafic de contrôle en raison du retour des phases de découvertes. Concernant le scénario 3, les messages introduits par le protocole FLH ne constituent qu'une infime partie du nombre total de messages de contrôle (composés majoritairement de messages *Beacon*). C'est pourquoi l'augmentation ou la réduction du nombre de messages MUP et CT n'a que peu d'influence sur le trafic total. De plus, nous pouvons relever que le seuil R' n'a pas d'influence sur le nombre de mauvaises anticipations, en raison de la portée importante des équipements sans fil dans ce scénario. Enfin, dans le scénario 4, le nombre de messages de contrôle et de mauvaises anticipations diminue lors de l'augmentation du seuil R'. Toutefois, il est difficile d'en

tirer une quelconque signification en raison du caractère aléatoire des trajectoires des terminaux mobiles.



(a) Scénario 1

(b) Scénario 2

(c) Scénario 3

(d) Scénario 4

FIG. 8.15 – Influence du seuil R' sur les performances du protocole FLH

Délais pour atteindre le contrôleur de mobilité

Nos dernières simulations portent sur l'influence du RTT entre les terminaux mobiles et le contrôleur de mobilité. Les résultats présentés ici concernent le protocole FLH avec interpolation linéaire. Ils ont été obtenus en simulant à 100 reprises le scénario 2 pour chaque valeur prédéfinie du RTT entre les terminaux mobiles et le contrôleur de mobilité (voir le tableau 8.2). Tous les autres paramètres ont été positionnés à leurs valeurs par défaut. Nous avons choisi spécifiquement le scénario 2, en raison de

sa sensibilité particulière aux différents paramètres de simulation. Cette sensibilité est principalement due au rapport portée radio des équipements / vitesse des terminaux.

La figure 8.16 présente les valeurs moyennes des temps de latence engendrés par les handovers de niveau 2 et 3 (axe de gauche) ainsi que le nombre moyen de messages de contrôle (axe de droite). Comme nous pouvons le constater, la valeur du RTT n'affecte aucunement les performances du protocole FLH : les temps de latence ainsi que le nombre de messages de contrôle restent pratiquement identiques quel que soit le RTT entre les terminaux et le contrôleur. En effet, l'utilisation conjointe du mécanisme de sauvegarde de contexte et des seuils S_1 et R permet d'éviter les problèmes liés à un délai significatif pour atteindre le contrôleur de mobilité. Etant donné que notre seuil simulé R' est positionné à sa valeur par défaut (i.e. R' = 50 %), les terminaux mobiles reçoivent toujours un message CT avant d'effectuer un handover. Il est évident qu'en augmentant la valeur du seuil R', le RTT pourrait avoir une influence sur le protocole. Mais nous avons remarqué que la valeur par défaut choisie pour le seuil R' semble être assez proche de la valeur optimale : elle permet de limiter relativement le nombre de messages de contrôle, sans affecter les performances du protocole FLH, même avec un important RTT entre le contrôleur et les terminaux mobiles.

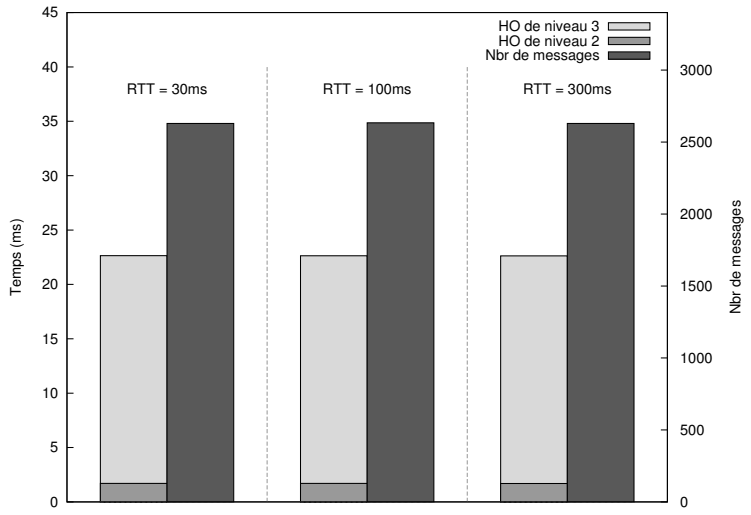


FIG. 8.16 – Influence du RTT entre le contrôleur de mobilité et les terminaux mobiles

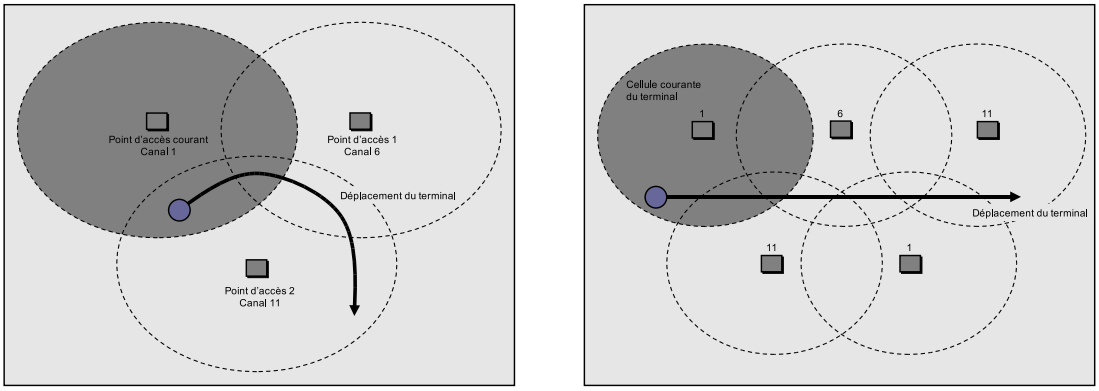
8.4 Comparaison avec le protocole SHAPE

Dans la section précédente, nous avons pu observer que le protocole FLH était particulièrement performant lors de l'utilisation d'une interpolation linéaire. Afin de réaliser une évaluation complète de FLH, nous avons voulu analyser les gains éventuels apportés par ce protocole par rapport au protocole SHAPE qui constitue notre précédente proposition. Les principales différences entre ces deux solutions reposent sur l'algorithme de sélection des prochains points d'accès et sur la manière de déclencher une procédure de handover. Le déroulement propre d'un handover reste cependant quasiment identique. Par conséquent, nous nous sommes focalisés dans cette étude sur le nombre de procédures de handover réalisées pour un scénario donné. Ces protocoles étant tout deux dépendants d'un système de positionnement, nous avons également mesuré l'influence des erreurs de géolocalisation sur le nombre de handovers effectués.

Cette nouvelle étude a été réalisée à l'aide de SimulX auquel nous avons intégré le protocole SHAPE. Les scénarii de simulation définis pour cette nouvelle étude sont présentés dans la section suivante.

8.4.1 Scénarii de simulation

Pour ce nouveau comparatif, deux nouveaux scénarii de simulation ont été définis. Ils représentent chacun le cas d'un utilisateur se déplaçant à l'intérieur d'un bâtiment. Ces scénarii restent assez simples de façon à déduire facilement le nombre minimal de procédures de handovers à réaliser pour maintenir une connectivité suivant la trajectoire du terminal mobile. Dans ces scénarii, tous les points d'accès se trouvent dans le même sous-réseau IPv6, ce qui implique que le terminal mobile n'effectuera que des handovers de niveau 2. En raison de l'environnement ciblé, nous avons réduit la portée des équipements sans fil à 50 mètres. La vitesse de déplacement du terminal est de 1 m/s. Le scénario 1 est spécialement conçu pour évaluer le comportement des protocoles lors de déplacements non rectilignes. Il se compose de trois points d'accès qui opèrent sur les canaux radio 1, 6 et 11. Quant au scénario 2, il a été défini de manière à proposer divers points d'accès au terminal lors de chaque handover. Il devrait mettre en évidence la différence de fréquence des handovers suivant le protocole utilisé. Il se compose de 5 points d'accès utilisant les canaux radio 1, 6 et 11. La figure 8.17 illustre ces deux nouveaux scénarii de simulation.



(a) Scénario 1 (b) Scénario 2

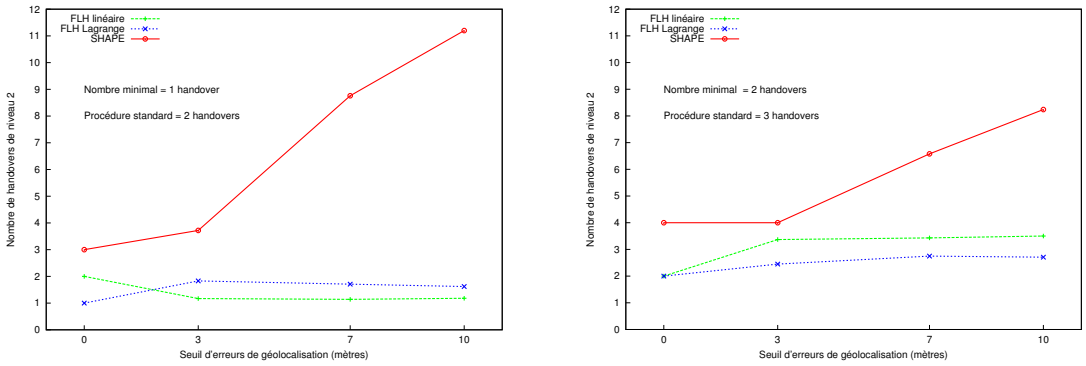
FIG. 8.17 – Scénarii de simulation utilisés lors du comparatif

8.4.2 Résultats

Les résultats présentés dans cette section ont été obtenus en jouant à 100 reprises chaque scénario de simulation pour chaque protocole. En vue d'observer l'influence des erreurs de géolocalisation sur les handovers, nous avons également maintenu nos trois seuils d'erreurs tels que nous les avions utilisés dans la section 8.3.2,

La figure 8.18 présente le nombre moyen de handovers réalisés lors des scénarii 1 et 2 en fonction des erreurs de géolocalisation. A titre de référence, nous avons représenté le nombre de handovers réalisés lors de la procédure standard. Ce nombre dépend directement de l'allocation des canaux radio sur les points d'accès. En effet, dans la procédure standard, le terminal s'accroche généralement au premier point d'accès qu'il détecte sans tenir compte de leur topologie. En outre, nous avons représenté le nombre de handovers minimal permettant de maintenir une connectivité dans chaque scénario. Il apparaît que le protocole SHAPE génère le plus de handovers. En l'absence d'erreurs de géolocalisation, le terminal effectue en moyenne deux fois plus de handovers que lors de l'utilisation du protocole FLH. Ce phénomène est d'autant plus aggravé lors de l'introduction d'erreurs de géolocalisation. Le déclenchement de la procédure de handover, telle qu'elle est définie dans le protocole SHAPE, permet d'expliquer ce phénomène : dès que la distance (distance approximative lors de l'introduction d'erreurs de géolocalisation) entre le terminal mobile et son point d'accès courant dépasse le seuil R, le contrôleur cherche dans sa base d'informations le point d'accès le plus proche géographiquement du terminal. Lorsque le point d'accès sélectionné est différent du point

d'accès courant, le contrôleur initie au niveau du terminal une procédure de handover vers ce point d'accès. En raison de la disposition des points d'accès et de la trajectoire du terminal mobile dans les scénarii de simulation, le contrôleur est amené à déclencher de nombreux handovers, obligeant même le terminal à faire des allers-retours successifs dans certains cas.



(a) Scénario 1

(b) Scénario 2

FIG. 8.18 – Nombre moyen de handovers réalisés

En l'absence d'erreurs de géolocalisation, nous pouvons observer que l'utilisation du protocole FLH permet d'atteindre le nombre minimal de handovers à réaliser quel que soit le scénario. En raison de la trajectoire parabolique du terminal dans le scénario 1, l'interpolation de Lagrange est plus adaptée que l'interpolation linéaire pour ce scénario. Lors de l'introduction d'erreurs de géolocalisation, le nombre de handovers réalisés reste très proche de la valeur minimale, même avec un seuil d'erreurs positionné à 10 mètres. Lors des simulations du protocole FLH avec interpolation de Lagrange, nous avons à nouveau vu survenir de mauvaises anticipations de la part du contrôleur pour les seuils d'erreurs de géolocalisation les plus élevés (i.e. 3, 7 et 10). De leur côté, les protocoles FLH avec interpolation linéaire et SHAPE n'ont jamais souffert de ce type d'erreurs dans les simulations présentées ici. Cette constatation nous amène une nouvelle fois à penser que dans le cadre du protocole FLH, une interpolation linéaire est préférable. On peut noter enfin que la procédure standard semble offrir un nombre acceptable de handovers dans le scénario 2. L'allocation des canaux radio sur les points d'accès permet d'expliquer cette observation. En effet, dans la procédure standard, le terminal s'associe directement au premier point d'accès découvert. Dans le scénario 2, cette procédure permet de s'associer dans la majorité des cas au point d'accès idéal en termes de zones de couverture par rapport à la trajectoire du terminal. En modifiant les canaux radio utilisés par les points d'accès, on pourrait donc augmenter le nombre

de handovers réalisés par le terminal mobile. Dans les protocoles SHAPE et FLH, les canaux radio des points d'accès environnants n'ont pas d'influence sur le protocole, excepté lors de mauvaises anticipations.

8.5 Conclusion

Dans ce chapitre, nous avons présenté le protocole *Fast Location-based Handover* (FLH) qui repose sur l'utilisation d'informations de géolocalisation afin de déterminer les trajectoires des terminaux mobiles. Ces anticipations ont pour but d'identifier a priori les futurs points d'attachement des terminaux mobiles en vue d'optimiser les handovers dans les réseaux Wi-Fi IPv6. Suite à la description des mécanismes qui compose FLH, nous avons évalué ses performances par simulation à l'aide de SimulX. Les résultats présentés dans la section 8.3.3 ont mis en évidence la réduction drastique du temps requis par les handovers de niveau 2 et 3 lors de l'utilisation de notre protocole, par rapport à la procédure standard (respectivement 1,7 et 23 millisecondes contre 344 et 396 millisecondes dans les meilleurs cas). En sélectionnant le futur point d'accès d'un terminal mobile avant le handover effectif, le contrôleur de mobilité est en mesure de fournir au terminal les paramètres de niveau 2 et 3 de son futur point d'attachement. Lors d'un handover, le terminal mobile utilise ces informations pour effectuer directement une tentative d'authentification sur le point d'accès pré-sélectionné. Dès la fin du handover de niveau 2, les paramètres de niveau 3 envoyés par le contrôleur et l'utilisation de la procédure ODAD permettent l'émission instantanée du BU à l'agent mère. Dans la méthode classique, le terminal doit en premier lieu découvrir son futur point d'accès en réalisant une phase de découverte, ce qui engendre des délais non négligeables dans ses communications courantes. Lorsque l'association de niveau 2 est finalisée, le terminal doit encore attendre de recevoir un message RA pour détecter le changement de sous-réseau IPv6 et initier le handover de niveau 3.

Nous avons également mesuré le coût du protocole FLH en termes de messages de signalisation. Bien qu'il introduise de nouveaux messages de contrôle entre les terminaux mobile et le contrôleur de mobilité, FLH génère moins de trafic de signalisation que la méthode standard. En effet, le nombre de messages spécifiques au protocole FLH est non seulement limité par les seuils S_1 (seuil d'intensité du signal correspondant à un signal moyen) et R (distance maximale entre un terminal et son point d'accès courant pendant laquelle le terminal est encore bien couvert), mais est également modéré par le mécanisme de sauvegarde de contexte. De plus, le protocole FLH permet de réduire la fréquence d'émission des messages RA et n'utilise des recherches actives que lors des cas d'erreurs, ce qui explique la réduction globale du nombre de messages de contrôle.

Par ailleurs, l'analyse du seuil R' simulant nos seuils S_1 et R nous a permis de confirmer que la valeur par défaut que nous avions choisie (i.e. R' = 50%) s'avère adéquate quel que soit le scénario simulé. Pour cette valeur, le nombre de messages introduits par le protocole FLH est raisonnablement réduit, sans affecter ses performances. De plus, la combinaison du seuil S_1 et du mécanisme de sauvegarde de contexte permet de se soustraire aux problèmes introduits par de larges RTT entre les terminaux mobiles et le contrôleur de mobilité. Même avec un RTT positionné à 300 millisecondes (ce qui correspond approximativement au RTT entre la France et le Japon) et lorsque les terminaux mobiles se déplacent rapidement, les anticipations sont toujours réussies. De plus, nous avons pu observer, lors de notre étude comparative avec le protocole SHAPE, que FLH permet dans la majorité des cas de réduire le nombre de handovers réalisés. Dans le protocole FLH, le contrôleur de mobilité sélectionne le point d'accès qui semble offrir la plus vaste zone de couverture en fonction de la trajectoire du terminal mobile. Même en présence d'erreurs de géolocalisation, le nombre de handovers réalisés reste très proche de la valeur minimale qui permet, pour un scénario donné, de maintenir une connectivité. Par contre, le nombre de handovers réalisés explose littéralement lors de l'utilisation du protocole SHAPE.

Cependant, le protocole FLH n'est pas exempt de défauts. Nous avons observé que le point d'accès pré-sélectionné peut être hors de portée radio du terminal lors du handover effectif. Cela peut notamment se produire lorsque les terminaux mobiles changent de direction juste avant la réalisation d'un handover, ce qui rend dans certains cas le contexte sauvegardé inutilisable. Ce type d'erreur est encore plus fréquent lors de l'introduction d'erreurs de géolocalisation dans les coordonnées des terminaux mobiles. Néanmoins, nous avons constaté que la méthode d'interpolation linéaire des trajectoires est moins sensible à ce phénomène. Lors d'une mauvaise anticipation, le terminal effectue une procédure de handover standard. A cette occasion, nous avons pu constater que les terminaux mobiles sont généralement incapables de détecter les changements de sous-réseau IPv6, en raison de la fréquence d'émission des messages RA qui était positionnée entre 200 et 600 secondes. On peut palier ces problèmes en envoyant non plus les paramètres d'un unique point d'accès, mais les paramètres d'une liste de points d'accès environnants, triés en fonction de la trajectoire du terminal (afin de limiter les perturbations observées dans notre méthode similaire présentée dans le chapitre 4). De cette manière, le terminal connaît à l'avance tous les paramètres des points d'accès adjacents, ce qui lui permet de constamment réaliser des handovers rapides indépendamment des erreurs de géolocalisation. Si l'authentification vers le premier point d'accès de la liste échoue (e.g. le point d'accès en question n'est pas joignable), le terminal essaie de s'associer au second et ainsi de suite. La réduction du nombre de retransmissions des requêtes d'authentification limitera le délai pour atteindre un point d'accès à portée radio. Enfin, cette optimisation du protocole FLH permet de maintenir la réduction de la

fréquence d'émission des messages RA, étant donné que le terminal mobile connaît tous les paramètres de niveau 3 des points d'accès sur lesquels il est susceptible de s'associer.

De plus, nous avons vu survenir un second problème. Lors de la perte d'un message CT, et bien que le terminal mobile continue à envoyer des messages MUP, le contrôleur de mobilité ne renvoie pas de messages CT tant que le contexte présent dans le cache de mobilité est valide. Lorsqu'un handover devient nécessaire, le terminal n'ayant pas reçu de contexte du contrôleur, sera donc dans l'obligation de réaliser un handover standard. Pour résoudre ce problème, il est possible d'associer à chaque contexte un identifiant unique de manière à tenir informer le contrôleur de mobilité du contexte actuellement positionné sur chaque terminal mobile. Pour ce faire, on intègre cet identifiant dans les messages MUP. Dès la réception d'un message MUP pour lequel l'identifiant du contexte ne correspond pas à celui renseigné dans le cache de mobilité, le contrôleur réémet un CT.

Du reste, les performances présentées dans ce chapitre ne tiennent pas compte du temps nécessaire au changement de canal radio au niveau des terminaux mobiles. Comme nous l'avons remarqué dans le chapitre 7, ce temps n'est pas négligeable (environ 10 millisecondes avec un périphérique sans fil muni d'une puce Atheros). Lors de notre étude comparative entre les protocoles SHAPE, MIPv6 et FMIPv6, nous avons également constaté que même avec des handovers rapides, il est possible de perdre suffisamment de paquets de données pour rendre les déplacements perceptibles à l'utilisateur. Suite à l'évaluation du protocole FLH illustrée dans le présent chapitre, il nous est apparu intéressant de coupler notre solution avec le protocole FMIPv6. En effet, ce dernier ne dispose pas d'un algorithme satisfaisant de découverte et de sélection des futurs points d'attachement de niveau 2, ce dont le protocole FLH s'acquitte de manière efficace. Dans le chapitre suivant, nous allons exposer les modifications apportées au sein des protocoles FLH et FMIPv6 afin de les combiner.

Chapitre 9

Intégration du protocole FLH dans le protocole FMIPv6

9.1 Introduction

Dans le chapitre précédent, nous avons pu constater par simulation que le protocole FLH est un protocole performant. Il permet non seulement de réduire le temps de latence engendré par les handovers, mais limite également la fréquence de changement de point d'accès dans certaines configurations. Notre étude comparative avec le protocole SHAPE a confirmé nos premières conclusions et a mis en évidence les bénéfices apportés par le protocole FLH par rapport à notre précédente contribution. En outre, il a été établi qu'une interpolation linéaire s'avère plus efficace qu'une interpolation de Lagrange dans la détermination des trajectoires des terminaux mobiles. Toutefois, nous avons pu relever qu'il n'est pas exempt de défauts et qu'il est nécessaire de modifier quelque peu ses spécifications pour tenir compte des erreurs d'anticipation.

Avant de nous lancer dans une implémentation réelle du protocole FLH, il reste un point important qu'il est nécessaire de prendre en compte. Fort de notre expérience acquise dans l'étude du protocole SHAPE (voir le chapitre 7), nous sommes désormais intimement persuadés qu'un protocole, aussi efficace soit-il, n'est pas en mesure de rendre transparent les déplacements aux utilisateurs lorsque aucun mécanisme de gestion de paquets n'est mis en place pendant une procédure de handover. A la vue de nos différents résultats, il nous est alors apparu évident que l'intégration de FLH au sein du protocole FMIPv6 nous permettrait certainement d'obtenir un protocole quasiment idéal. En effet, le protocole FMIPv6 propose une gestion des paquets au niveau des routeurs d'accès et permet aux terminaux mobiles de communiquer dès la fin du handover

de niveau 2 grâce au tunnel FMIP. Cependant, ses spécifications se focalisent essentiellement sur le niveau 3 de manière à n'être liées à aucune technologie sous-jacente. Dans le cas des réseaux 802.11, il est donc nécessaire de définir des mécanismes additionnels pour découvrir les informations de niveau 2 des points d'accès voisins. C'est sur ce point particulier que le protocole FLH peut apporter un gain non négligeable. Ce dernier permettrait entre autres de sélectionner les futurs points d'accès des terminaux mobiles en fonction de leurs trajectoires afin de positionner les différentes informations de niveau 2 et 3 nécessaires à la réalisation d'un handover rapide.

Dans ce chapitre, nous allons dans un premier temps décrire les différentes modifications apportées aux protocoles FMIPv6 et FLH en vue de les faire cohabiter au sein des entités concernées. Nous présenterons ensuite une évaluation préliminaire du protocole ainsi obtenu et analyserons nos premiers résultats expérimentaux. Enfin, nous exposerons nos conclusions et nos projets au sujet de cette nouvelle contribution.

9.2 Modifications des protocoles FMIPv6 et FLH

9.2.1 Déroulement du handover

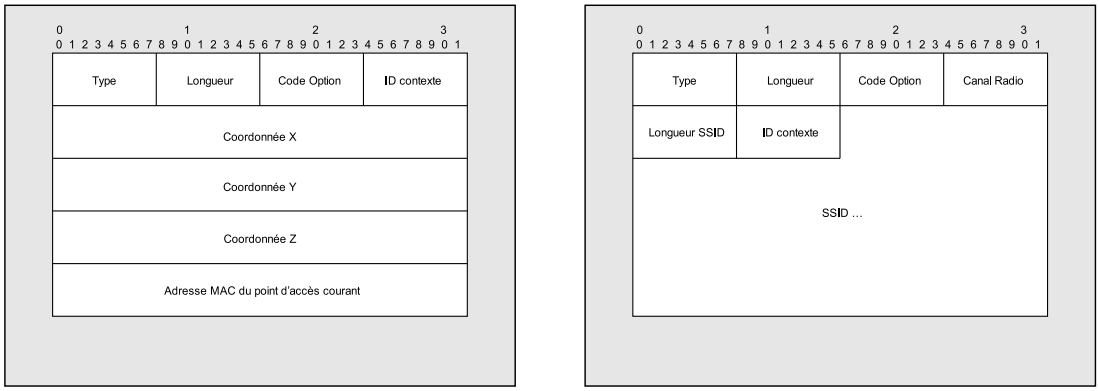
L'intégration de FLH dans le protocole FMIPv6 n'a demandé qu'une légère adaptation de la procédure de handover telle qu'elle est décrite dans FMIPv6. En effet, ce dernier propose un mode prédictif dans lequel les terminaux mobiles sont capables d'anticiper le besoin d'effectuer un handover (voir la section 2.6.1). Transposée aux réseaux 802.11, une telle anticipation peut être réalisée par l'intermédiaire de déclencheurs de niveau 2. Dès lors, nous avons utilisé notre seuil S_2, défini dans le cadre du protocole FLH, pour déclencher l'envoi du FBU et donc initier la procédure de handover. A la réception du FBACK, le terminal mobile réalise la même procédure de handover de niveau 2 que celle présentée dans le protocole SHAPE. A ce stade de nos travaux, nous n'avons donc pas encore supprimé complètement la phase de découverte comme cela est spécifié dans le protocole FLH. Dès que l'association avec le nouveau point d'accès est terminée, c'est le protocole FMIPv6 qui reprend la main : le terminal envoie le FNA, ce qui déclenche la transmission des paquets en attente sur le routeur d'accès. Lors d'un changement de sous-réseau IPv6, le terminal pourra toujours, grâce au protocole FMIPv6, utiliser sa précédente adresse temporaire pendant qu'il finalise le handover de niveau 3. Cette procédure permet notamment de s'affranchir de la mise en place d'une architecture hiérarchique, architecture qui était nécessaire dans FLH de façon à réduire le délai de mise à jour des adresses temporaires auprès de l'agent mère.

9.2.2 Sélection des prochains points d'accès

En ce qui concerne la découverte des points d'accès et l'obtention des paramètres de niveau 2 correspondants, nous avons modifié la procédure d'échange des messages RtSolPr et PrRtAdv. Dans le protocole FMIPv6, ces messages permettent aux terminaux mobiles d'interroger leurs routeurs d'accès courants, afin d'obtenir les paramètres de niveau 3 des liens IPv6 sur lesquels se situent les points d'accès environnants.

Pour commencer, les fonctionnalités du contrôleur de mobilité ont été déportées dans les routeurs d'accès supportant le protocole FMIPv6. En plus des informations de niveau 3 qu'ils contiennent déjà, chaque routeur d'accès possède désormais les paramètres de niveau 2 (SSID, canal radio, etc.) des points d'accès qui lui sont raccordés. De plus, les paramètres d'autres points d'accès sont ajoutés de manière à détenir les informations de tous les voisins géographiques des points d'accès du sous-réseau géré par le routeur. La base globale d'informations est donc décomposée en plusieurs sous-bases dont le contenu est adapté en fonction de la topologie du réseau entourant chaque routeur d'accès.

Les informations véhiculées par les messages MUP et CT du protocole FLH sont ici intégrées dans les messages RtSolPr et PrRtAdv. Pour ce faire, deux nouvelles options ont été définies en respectant le format décrit dans les spécifications du protocole FMIPv6. La figure 9.1 représente le format utilisé pour ces deux nouvelles options.



(a) FLH_OPT_POSITION_INFO (b) FLH_OPT_SSID_CHANNEL_INFO

FIG. 9.1 – Formats des nouvelles options des messages RtSolPr / PrRtAdv

L'option *FLH_OPT_POSITION_INFO* est ajoutée aux messages RtSolPr et contient les coordonnées courantes du terminal mobile émetteur (exprimées en coordonnées géo-

désiques ou relatives) relatives) ainsi que l'adresse MAC de son point d'accès courant. Pour palier les problèmes survenus lors de notre évaluation du protocole FLH, nous avons également ajouté l'identifiant unique du contexte actuellement positionné sur le terminal.

La deuxième option, appelée *FLH_OPT_SSID_CHANNEL_INFO*, est ajoutée dans les messages PrRtAdv par les routeurs d'accès. Elle contient le canal radio et le SSID d'un point d'accès particulier. En fonction de la taille de la liste des futurs points d'accès composant un contexte, cette option peut être incluse à plusieurs reprises dans un même message PrRtAdv. En outre, un champ spécifique permet d'attribuer un identifiant unique à un contexte donné. Cet identifiant est enregistré par le terminal mobile de manière à le réutiliser dans ses futurs messages RtSolPr. Le reste des paramètres constituant un contexte, à savoir l'adresse MAC des prochains points d'accès, les préfixes IPv6 des futurs liens et les adresses MAC et IPv6 des futurs routeurs d'accès [29], peuvent être transmis à l'aide des options de base du protocole FMIPv6 [29].

Etant donné que les messages RtSolPr / PrRtAdv jouent ici le même rôle que les messages MUP et CT, leur émission va se conformer à celle définie dans FLH pour ces mêmes messages. Tant que la qualité du signal d'un terminal est sous le seuil S_1 (cf. chapitre précédent), il émet périodiquement (à chaque mise à jour de sa position par le système de géolocalisation) des messages RtSolPr vers son routeur d'accès. Dès réception, le routeur d'accès réalise les mêmes procédures que celles effectuées par le contrôleur de mobilité lorsqu'il reçoit un message MUP. Quand le routeur d'accès a créé un nouveau contexte pour le terminal, il lui envoie un message PrRtAdv contenant les différentes informations de ce contexte. A la réception d'un PrRtAdv, le terminal sauvegarde le contexte présent dans le message jusqu'à la réception d'un nouveau PrRtAdv, où jusqu'à ce que la qualité de signal passe sous le seuil S_2, ce qui déclenche la procédure de handover.

Un terminal mobile qui ne supporte que le protocole FMIPv6 de base ignore tout simplement l'option FLH_OPT_SSID_CHANNEL_INFO, comme cela est prévu dans FMIPv6. De la même manière, les options FLH_OPT_POSITION_INFO sont ignorées des routeurs d'accès FMIPv6 qui ne supportent pas les fonctionnalités liées au protocole FLH. La figure 9.2 illustre toutes les étapes de notre nouveau protocole.

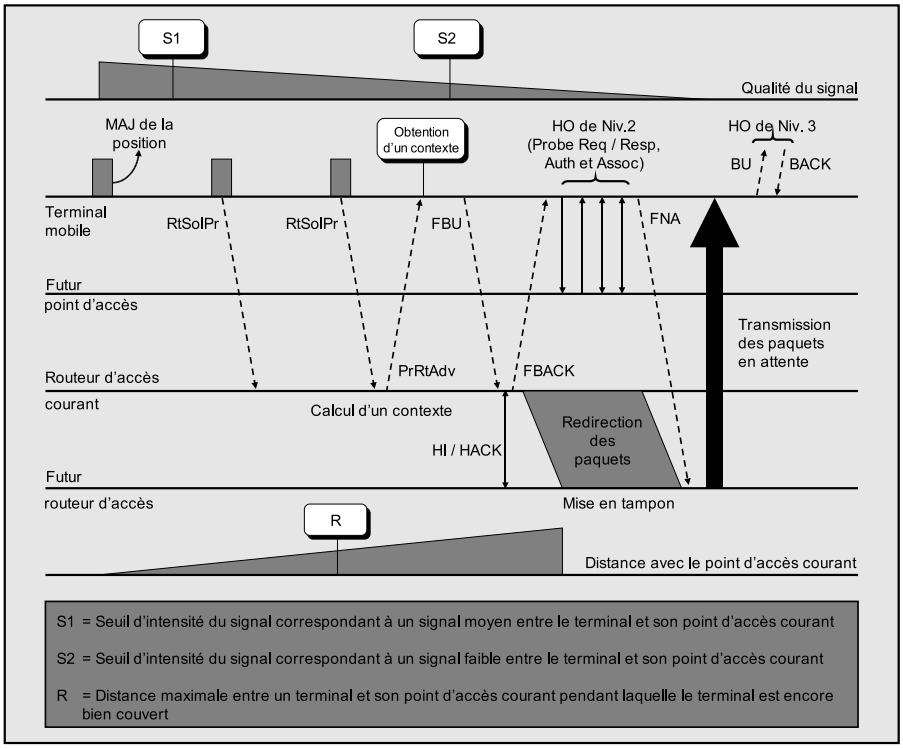


FIG. 9.2 – Intégration du protocole FLH dans le protocole FMIPv6

9.3 Preuve de concept

Dans la continuité de ces travaux, nous souhaitions réaliser au préalable une étude de la faisabilité de cette solution. Pour ce faire, elle a été implémentée dans un système GNU/Linux en respectant nos différentes spécifications. Cette implémentation a ensuite donné lieu à une première évaluation qui sera étendue dans le cadre de futurs travaux.

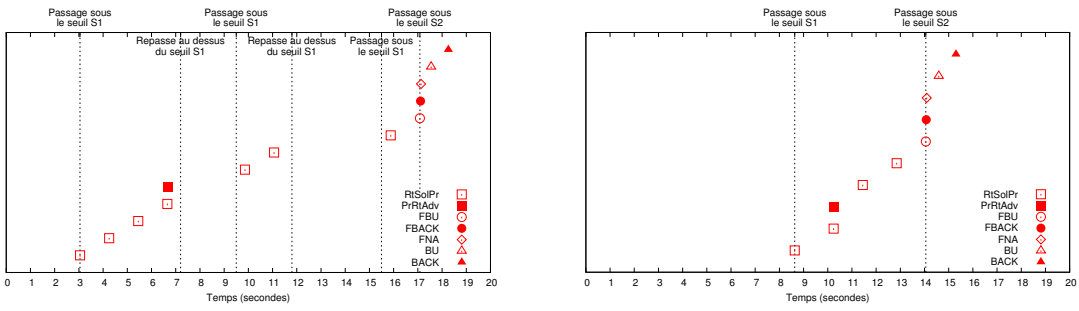
9.3.1 Implémentation

Dès la fin des spécifications de notre nouveau protocole, nous avons procédé à son implémentation dans un système GNU/Linux. Pour ce faire, nous nous sommes basé sur l'implémentation fmipv6.org [45] qui a déjà été mentionnée dans ce rapport. Dans un premier temps, nous avons ajouté la gestion de nos deux nouvelles options aussi bien du côté terminal que du côté routeur. Pour la mise en place des bases d'informations, des caches de mobilité, et des contextes de mobilité, nous nous sommes inspirés des listes

déjà présentes dans fmipv6.org. Du côté des terminaux, nous avons défini de nouvelles fonctions de gestion des coordonnées géographiques et étendu quelque peu l'interaction entre le niveau 2 et 3, de façon à émettre les messages RtSolPr en fonction du seuil S_1. La gestion du seuil S_2 était par contre déjà présente. A ce sujet, nous avons diminué les valeurs de ces seuils afin de simplifier les expérimentations. Pour notre évaluation préliminaire, S_1 et S_2 ont été respectivement positionnés à $-53dBm$ et à $-57dBm$, tout en gardant la possibilité de modifier à loisir ces valeurs. Au niveau des routeurs d'accès, nous avons ajouté les fonctions nécessaires à la détermination des trajectoires et à la sélection des prochains points d'accès. Enfin, nous avons réutilisé nos modifications apportées au pilote de périphérique MADWiFi lors de l'implémentation du protocole SHAPE.

9.3.2 Résultats préliminaires

L'évaluation préliminaire présentée dans cette section reprend la plate-forme et les scénarii de tests utilisés dans notre comparatif entre les protocoles SHAPE, MIPv6 et FMIPv6 (voir chapitre 7). Pour rappel, nous avions défini deux scénarii (diffusion vidéo et vidéoconférence) dans lesquels le terminal mobile se déplaçait entre deux points d'accès situés dans deux sous-réseaux IPv6 différents. Concernant le système de géolocalisation, nous avons également réutilisé le système GPS. Chaque scénario à été joué à 10 reprises en vue de collecter diverses mesures.



(a) Scénario 1 (Réception vidéo)

(b) Scénario 2 (Vidéoconférence)

FIG. 9.3 – Traces d'un déplacement engendrant une procédure de handover

La figure 9.3 présente les traces d'un déplacement du terminal mobile entre les deux points d'accès. Pour des raisons de lisibilité, nous n'avons représenté que le trafic de contrôle de niveau 3. Chaque point représente l'émission ou la réception d'un message,

au niveau du terminal, au temps indiqué sur l'axe des abscisses. On constate que la nouvelle procédure d'échange des messages RtSolPr et PrRtAdv fonctionne correctement. Dès que la qualité du signal passe sous le seuil S_1, le terminal mobile envoie périodiquement des messages RtSolPr. Dès réception du premier RtSolPr, le routeur d'accès met à jour son cache de mobilité local, mais ne crée pas de contexte en raison de la distance entre le terminal et son point d'accès courant. Dès que cette distance est supérieure à R, le routeur d'accès calcule un nouveau contexte et l'envoie au terminal à l'aide d'un message PrRtAdv. Etant donné que la base d'information locale de chaque routeur d'accès ne comporte qu'un unique point d'accès, le contexte créé ne sera pas modifié, ce qui explique l'émission d'un unique message PrRtAdv visible sur les figures 9.3(a) et 9.3(b). Lorsque la qualité du signal passe sous le seuil S_2, le terminal initie la procédure de handover. Cette procédure est d'ailleurs plus détaillée dans les figures 9.4 et 9.5.

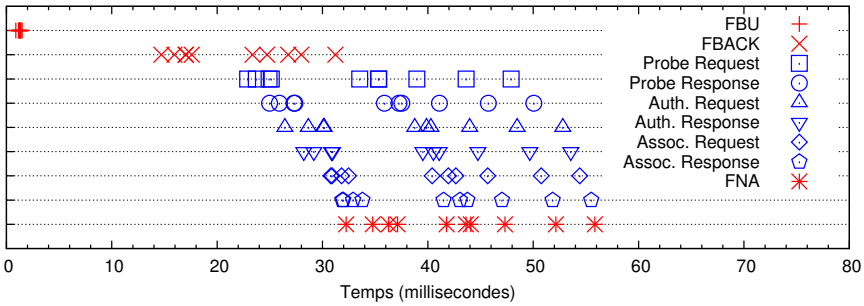


FIG. 9.4 – Résultats préliminaires pour le scénario 1

Les figures 9.4 et 9.5 présentent les résultats correspondant respectivement à nos 10 tests du premier scénario et à nos 10 tests du second scénario. Pour des raisons de lisibilité, nous avons recentré nos différentes mesures sur les temps d'émissions des messages FBU. L'importance des messages BU et BACK étant relativement limitée lors de l'utilisation du protocole FMIPv6, nous avons décidé de ne pas les représenter de façon à conserver une échelle de temps relativement lisible. Comme on pouvait s'y attendre, nous obtenons des performances similaires à celles observées pour le protocole FMIPv6 de base lors de notre comparatif présenté dans le chapitre 7. N'ayant pas modifié la procédure de handover de l'implémentation fmipv6.org, il était envisageable d'obtenir des résultats identiques.

Lorsque la qualité du signal passe sous le seuil S_2, le terminal envoie le message FBU à son routeur d'accès courant. Dès la réception du FBACK, le terminal initie la procédure de handover. Les délais entre la réception du FBACK et l'émission du premier *Probe Request* observés sur les figures 9.4 et 9.5 (respectivement 11,5 et 12,84 millisecondes en moyenne) proviennent de la réinitalisation du périphérique sans fil et notamment du changement de canal radio. Cette réinitialisation fait suite à la configuration des paramètres de niveau 2 correspondant au futur point d'accès. Ces valeurs

confirment les résultats obtenus lors de nos précédentes expérimentations. Dès la réception de la *Probe Response* envoyées par le point d'accès cible, le terminal passe directement à la phase d'authentification puis à la phase d'association, ce qui finalise le handover de niveau 2. Le temps moyen des handovers de niveau 2 (mesuré en effectuant la différence entre les temps de réception de l'*Association Response* et les temps de réception du FBACK) est respectivement de 22,6 millisecondes dans le scénario 1 et de 24,98 millisecondes dans le scénario 2, ce qui rejoint également nos précédents résultats.

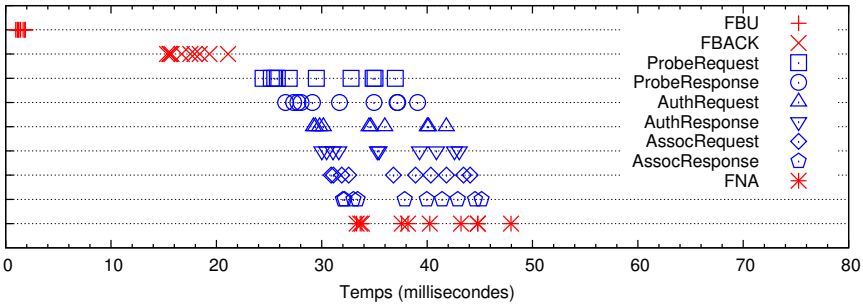


FIG. 9.5 – Résultats préliminaires pour le scénario 2

A la réception de l'*Association Response* au niveau du terminal, le démon FMIPv6 reçoit une notification indiquant la fin du handover de niveau 2 (*Link Up*), ce qui lui permet d'envoyer le FNA. On constate sur les figures 9.4 et 9.5 que le FNA est en moyenne émis 1,2 millisecondes (scénario 1) et 1,6 millisecondes (scénario 2) après la fin du handover de niveau 2. A la réception du FNA, le nouveau routeur d'accès transmets les éventuels paquets de données mis en attente. Dès cet instant, le terminal dispose à nouveau d'une connectivité de niveau 3 et ce, tant que le tunnel FMIP entre l'ancien et le nouveau routeur d'accès est actif. Par conséquent, le délai engendré par la mise à jour de sa nouvelle adresse temporaire auprès de l'agent mère n'a pas d'incidence sur ses communications courantes.

Par rapport aux flux applicatifs échangés dans nos scénarii, on a constaté qu'aucun paquet de données n'a été perdu et ce, durant toute la procédure mise en place dans ce nouveau protocole. Dans FMIPv6 de base, les paramètres des points d'accès environnants sont généralement obtenus lors de sondages successifs des canaux radio, ce qui engendre des temps de latence non négligeables dans les communications courantes du terminal. A l'inverse, ces paramètres sont ici obtenus en même temps que ceux de niveau 3, grâce aux nouvelles options des messages RtSolPr et PrRtAdv. Aucun paquet ne peut donc être perdu lors de cette étape. Par la suite, le handover de niveau 2 est assez rapide pour que la transmission des messages stockés au niveau du nouveau routeur d'accès ne soit pas trop retardée. De ce fait, le handover est complètement transparent au niveau de l'utilisateur, que ce soit lors de la réception du flux vidéo (scénario 1) ou lors de la

vidéoconférence (scénario 2). Il reste toutefois à analyser l'impact des erreurs d'anticipation et notamment l'algorithme de sélection de multiples futurs points d'attachement proposé dans la version révisée de FLH.

9.4 Conclusion

Dans ce chapitre, nous avons présenté une étude de l'intégration du protocole FLH dans le protocole FMIPv6. Après avoir fait état des différentes modifications apportées à chaque protocole, nous avons détaillé son implémentation et analysé les performances obtenues lors d'une première expérimentation. Les résultats préliminaires laisse à penser que ce nouveau protocole serait très performant dans des environnements réels.

Il reste néanmoins à étendre notre plate-forme de tests en vue de créer un environnement plus favorable à une évaluation réelle de notre nouveau protocole. Nous pensons notamment tirer parti du déploiement d'un réseau 802.11 au sein de l'université Louis Pasteur de Strasbourg (composé actuellement de 350 points d'accès différents et utilisé par plus de 5000 utilisateurs distincts) afin d'analyser plus précisément la procédure de sélection des prochains points d'accès. En outre, nous songeons à nous appuyer sur le système de géolocalisation Place Lab [54] que nous avons présenté dans le chapitre 5, car il ne requiert pas d'architecture spécifique et fonctionne aussi bien en extérieur qu'en intérieur. Cette dernière évaluation est à nos yeux une étape nécessaire avant la validation finale de notre nouvelle solution. Elle devrait également permettre de comparer de manière efficace les performances de nos trois contributions au sein des optimisations des handovers assistées par géolocalisation dans les réseaux Wi-Fi IPv6.

Conclusion générale et perspectives

La popularité des réseaux sans fil et plus particulièrement de la technologie IEEE 802.11 (Wi-Fi) est en train de modifier le comportement des utilisateurs, leur permettant de communiquer tout en se déplaçant. Le déploiement de telles technologies couplé à la miniaturisation des terminaux utilisateurs renforcent le désir d'être connecté partout et tout le temps. La convergence des différentes technologies de communication vers le tout IP a nécessité le développement d'un nouveau protocole de gestion de la mobilité au sein des réseaux IP. C'est le protocole Mobile IP (MIP), standardisé par l'IETF, qui est destiné à fédérer l'accès à ces différents réseaux. Deux versions du protocole MIP cohabitent actuellement, l'une pour les réseaux IPv4 (MIPv4) et l'autre pour les réseaux IPv6 (MIPv6). Cependant, la gestion actuelle de la mobilité dans les réseaux Wi-Fi, telle qu'elle est définie par la norme IEEE 802.11, ne permet pas des déplacements transparents entre différentes bornes d'accès (i.e. lors de handovers de niveau 2), notamment lors de communications temps réel. Ce phénomène peut encore être aggravé lors des changements de sous-réseaux IPv6 gérés par le protocole MIPv6 (i.e. lors de handovers de niveau 3). Dans le cadre de ma thèse, nous avons principalement étudié les bénéfices apportés par l'introduction d'informations de géolocalisation dans la gestion de la mobilité.

De nombreuses solutions ont été proposées dans la littérature pour optimiser les handovers de niveau 2 et 3 dans les réseaux Wi-Fi IPv6. Il est aujourd'hui clairement établi que la phase de découverte de niveau 2 est responsable de la majorité du temps de latence engendré par les handovers de niveau 2 dans les réseaux Wi-Fi. De plus, le protocole MIPv6 a été conçu comme un protocole réactif et les mécanismes qui le composent (notamment les méthodes de détection des nouveaux liens IPv6, de vérification des nouvelles adresses et de mise à jour de ces nouvelles adresses auprès de l'agent mère) ne sont pas adaptés à une gestion rapide de la mobilité. Lors de notre étude introductive, nous avons analysé les mécanismes d'optimisation proposés dans la littérature afin d'identifier les modifications nécessaires à la réalisation de handovers rapides. Notre étude bibliographique nous a fait prendre conscience que la majorité des optimisations s'accordent sur la nécessité pour les terminaux mobiles de connaître a priori leur

environnement. C'est donc principalement la manière d'obtenir de telles informations qui les différencie. Nous avons poussé plus loin cette réflexion lors de notre évaluation de solutions de niveau 2, tirées aussi bien de la littérature que de notre propre recherche (voir les chapitres 3 et 4). Ces premiers travaux ont permis de confirmer notre sentiment premier : dès qu'un terminal mobile possède les informations de son prochain point d'accès et par extension de son futur lien IPv6, il est possible de réaliser des handovers inférieurs à 50 millisecondes. Cette valeur est communément admise comme la limite supérieure du temps de latence pour laquelle les handovers sont transparents aux utilisateurs. A la suite de cette étude introductive, il nous a semblé évident que l'utilisation d'informations de géolocalisation dans la gestion des handovers pouvait simplifier la découverte des paramètres relatifs aux points d'accès environnants. En se basant sur les positions géographiques des équipements, il devait être possible d'identifier les futurs points d'accès des terminaux mobiles de façon à leur fournir au préalable les paramètres nécessaires à la réalisation d'un handover rapide.

Dans le chapitre 5, nous avons fait état des méthodes actuelles pour déterminer la position géographique d'un équipement. Cette dernière est généralement calculée à l'aide d'un système de géolocalisation. Les systèmes globaux tels que le système GPS sont devenus très accessibles grâce à la réduction du coût des équipements nécessaires à leur utilisation. La popularisation des réseaux sans fil a aussi permis l'émergence de systèmes locaux qui reposent sur de nouvelles techniques de localisation. Il en ressort que certains de ces nouveaux systèmes s'intègrent parfaitement dans les réseaux Wi-Fi sans nécessiter d'équipements supplémentaires particuliers. De tels systèmes sont donc relativement simples à mettre en place et reviennent au final assez bon marché. Ces observations laissent à penser que la localisation sera de plus en plus présente dans les réseaux de nouvelle génération.

Dans la dernière partie de ce rapport, nous avons présenté nos principaux travaux portant sur l'utilisation d'information de géolocalisation dans la gestion des handovers au sein des réseaux Wi-Fi IPv6. Nos travaux dans ce domaine nous ont amené à spécifier au final trois protocoles différents. Notre première proposition, le protocole SHAPE (*Seamless Handovers Assisted by Position Estimation*), a donné lieu à une implémentation dans un système GNU/Linux. Les premières expérimentations réalisées nous ont montré que malgré un algorithme de sélection des prochains points d'accès assez basique, l'utilisation de la position des équipements apportait une réelle valeur ajoutée dans la gestion des handovers et plus particulièrement dans l'obtention des paramètres des futurs points d'attachement. Dans notre objectif de rendre les déplacements transparents aux utilisateurs quel que soit le trafic en cours, nous avons également analysé l'impact du protocole SHAPE sur des communications temps réel générées à l'aide d'applications usuelles. Cette étude à donné lieu à un comparatif entre les protocoles MIPv6, FMIPv6 et SHAPE. Les résultats obtenus soulignent qu'il ne suffit pas de réa-

liser des handovers rapides mais qu'il est nécessaire de mettre en place des mécanismes de gestion des paquets de données lorsque les terminaux sont en procédure de handover. Le protocole FMIPv6 s'est particulièrement illustré en ce sens lors de ce comparatif, mais manque néanmoins d'une procédure rapide et fiable de sélection et d'obtention des paramètres de niveau 2 des prochains points d'attachement.

La poursuite de nos travaux nous a conduit à la spécification d'un nouveau protocole, le *Fast Location-based Handover* (FLH). Ce dernier se base désormais sur les trajectoires des terminaux mobiles pour sélectionner leurs futurs points d'attachement. Parmi les nombreux résultats de simulations présentés, nous avons entre autres pu montrer qu'en plus de la réduction drastique du temps de latence engendré par les handovers, le protocole FLH permet de limiter le nombre de handovers réalisés suivant l'environnement dans lequel les équipements sans fil prennent place. Par opposition, le protocole SHAPE fait littéralement exploser le nombre d'associations effectuées en raison du mécanisme de déclenchement des handovers qu'il comporte. Nos simulations ont également permis de mettre en évidence les quelques faiblesses du protocole FLH, notamment lors de l'introduction d'erreurs de géolocalisation. En outre, la version de base ne comporte pas de mécanismes pour la mise en attente ou la redirection des paquets de données lors d'un handover. Nos derniers travaux sur l'intégration d'une version révisée de FLH au sein du protocole FMIPv6 ont finalement permis d'obtenir une solution qui, à la vue de nos résultats préliminaires, semble réellement performante.

Perspectives

Parmi les travaux réalisés lors de cette thèse, c'est principalement le protocole FLH qui constitue notre contribution majeure. Néanmoins, ce protocole est encore destiné à évoluer. Dans un premier temps, nous envisageons de réaliser une évaluation plus complète de son intégration au sein du protocole FMIPv6. Pour ce faire, nous allons tirer parti du déploiement du réseaux sans fil au sein du l'université Louis Pasteur afin de créer un environnement de tests réaliste. De plus, la substitution du système de géolocalisation GPS par le système Place Lab devrait offrir une gestion plus fine des déplacements des terminaux mobiles, étant donné qu'il fonctionne aussi bien en extérieur qu'à l'intérieur des bâtiments. Par ailleurs, concernant le calcul des trajectoires, il serait intéressant d'étudier d'autres méthodes d'interpolation moins dépendantes des positions réelles des terminaux (e.g. splines). De même, il est envisageable d'utiliser des mécanismes d'auto-apprentissage du comportement général d'utilisateurs placés dans un environnement donné, de façon à limiter au maximum les mauvaises anticipations de la part du contrôleur de mobilité. Cette dernière suggestion fait notamment intervenir le besoin de modèle de mobilité réaliste au sein de la communauté des réseaux sans fil.

Enfin, il est indispensable de prendre en considération les aspects liés à la sécurité avant un éventuel déploiement de FLH à plus grande échelle. En effet, le protocole doit empêcher des utilisateurs malintentionnés de se faire passer pour le contrôleur de mobilité auprès des autres terminaux, ou de prendre l'identité d'un autre utilisateur lorsqu'ils correspondent avec le contrôleur. De plus, tous les types d'attaques de déni de services au niveau du contrôleur de mobilité doivent être pris en compte. L'adaptation du protocole FLH au sein de réseaux IEEE 802.11i constitue un bon point de départ pour ces travaux. En effet, cette norme propose divers mécanismes renforçant la sécurité dans les réseaux Wi-Fi et permet notamment la pré-authentification des terminaux mobiles auprès de leurs futurs points d'accès. Dès lors, il semble relativement aisé d'y adapter le protocole FLH en tirant parti de ces procédures de pré-authentification.

A plus long terme, nous comptons axer nos recherches sur la prochaine génération des réseaux Wi-Fi, à savoir les réseaux MiMo (Multiple Input / Multiple Output) [27]. En cours de spécification, cette technologie est en quelque sorte une compilation des différentes propositions faites pour les réseaux Wi-Fi permettant d'augmenter le débit ou la portée des équipements. Au niveau de la mobilité, cette norme proposera en standard des optimisations par rapport à la norme actuelle. Il serait notamment intéressant d'y adapter le protocole FLH pour évaluer les avantages qu'il pourrait y apporter.

Bibliographie

[1] IEEE Std. 802.11. 1999 Edition (R2003) (ISO/IEC 8802-11), IEEE Standard for Information Technology - Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks - Specific Requirements - Part 11 : Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 1999.

[2] IEEE Std. 802.11a 1999. Supplement to IEEE Standard for Information Technology - Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks - Specific Requirements - Part 11 : Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications : High-speed Physical Layer in the 5 GHz Band, 1999.

[3] IEEE Std. 802.11b 1999. Supplement to IEEE Standard for Information Technology - Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks - Specific Requirements - Part 11 : Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications : Higher-Speed Physical Layer Extension in the 2.4 GHz Band, 1999.

[4] IEEE Std. 802.11e 2005. IEEE Standard for Information Technology - Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks - Specific Requirements - Part 11 : Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications - Amendment 8 : Medium Access Control (MAC) Quality of Service Enhancements, 2005.

[5] IEEE Std. 802.11f 2003. IEEE Trial-Use Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation, 2003.

[6] IEEE Std. 802.11g 2003. IEEE Standard for Information Technology - Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks - Specific Requirements - Part 11 : Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications - Amendment 4 : Further Higher Data Rate Extension in the 2.4 GHz Band, 2003.

[7] IEEE Std. 802.11i 2004. IEEE Standard for Information Technology - Telecommunications and Information Exchange between Systems - Local and Metropo-

litan Area Networks - Specific Requirements - Part 11 : Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications - Amendment 6 : Medium Access Control (MAC) Security Enhancements, 2004.

[8] IEEE Std. 802.1X-2004. IEEE Standard for Local and Metropolitan Area Networks - Port-Based Network Access Control, 2004.

[9] IEEE Std. 802.3-2005. IEEE Standard for Information Technology - Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks - Specific Requirements - Part 3 : Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications, 2005.

[10] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz. Extensible Authentication Protocol (EAP), Internet Engineering Task Force Request for Comments (RFC) 3748, Juin 2004.

[11] J. Arkko, V. Devarapalli, and F. Dupont. Using IPsec to Protect Mobile IPv6 Signaling Beteween Mobile Nodes and Home Agents, Internet Engineering Task Force Request for Comments (RFC) 3776, Juin 2004.

[12] V. Bahety and R. Pendse. Scalable QoS Provisioning for Mobile Networks using Wireless Sensors. In *Proceedings of IEEE International Conference on Wireless Communications and Networking (WCNC'04)*, Atlanta, USA, Mars 2004.

[13] P. Bahl and V. N. Padmanabhan. RADAR : An In-Building RF-based User Location and Tracking System. In *Proceedings of the 19th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'00)*, pages 775–784, Tel-Aviv, Israel, Mars 2000.

[14] M. Bandai and I. Sasase. A Low Latency Handoff Scheme Using Positional Information for Mobile IP Based Network. In *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM'03)*, San Francisco, USA, Décembre 2003.

[15] N. Borisov, I. Goldberg, and D. Wagner. Intercepting Mobile Communications : the Insecurity of 802.11. In *Proceedings of the 7th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom'01)*, pages 180–189, Rome, Italy, Juillet 2001.

[16] M. Brunato and Csaba K. Kallo. Transparent Location Fingerprinting for Wireless Services. In *Proceedings of the 1st Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net'02)*, Sardegna, Italy, Septembre 2002.

[17] P. Calhoun, B. O'Hara, R. Suri, N. Cam Winget, S. Kelly, M. Williams, and S. Hares. Light Weight Access Point Protocol, Work in Progress, Internet Engineering Task Force draft-ohara-capwap-lwapp-03.txt, Juin 2005.

[18] N. Cam-Winget, R. Housley, D. Wagner, and J. Walker. Security Flaws in 802.11 data link protocols. *Communications of the ACM, special issue on Wireless Networking Security*, 46 :35–39, Mai 2003.

[19] A. Cellerier and Al. VideoLAN - VLC media player, `http://www.videolan.org`.

[20] The CELLO Project. `http://www.telecom.ece.ntua.gr/cello/`.

[21] G. Chesson, M. Renzmann, and Sam Leffler. Multiband Atheros Driver for Wi-Fi (MADWIFI), `http://madwifi.org`.

[22] Gerald Combs and al. The Network Protocol Analyser Ethereal, `http://www.ethereal.com`.

[23] S. Deering and R. Hinden. Internet Protocol, Version 6 (IPv6) Specification, Internet Engineering Task Force Request for Comments (RFC) 2460, Décembre 1998.

[24] N. Van den Wijngaert and C. Blondia. A Location Augmented Low Latency Handoff Scheme for Mobile IP. In *Proceedings of the First International Conference on Mobile Computing and Ubiquitous Networking (ICMU'04)*, Yokosuka, Japan, Janvier 2004.

[25] V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert. Network Mobility (NEMO) Basic Support Protocol, Internet Engineering Task Force Request for Comments (RFC) 3963, Janvier 2005.

[26] G. M. Djuknic and R. E. Richton. Geolocation and Assisted GPS. *IEEE Computer*, 34 :123–125, Février 2001.

[27] IEEE Std. P802.11n draft 1.0. IEEE Standard for Information Technology - Draft Amendment to Standard for Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks - Specific Requirements - Part 11 : Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications - Enhancements for Higher Throughput, 2006.

[28] C. Perkins (éditeur). IP Mobility Support for IPv4, Internet Engineering Task Force Request for Comments (RFC) 3344, Août 2002.

[29] R. Koodli (éditeur). Fast Handovers for Mobile IPv6, Internet Engineering Task Force Request for Comments (RFC) 4068, Juin 2005.

[30] Ekahau. Ekahau Positioning Engine for WLAN based navigation, `http://www.ekahau.com`.

[31] P. Enge and P. Misra. Scanning the Special Issue/Technology on the Global Positioning System. *Proceedings of the IEEE, Special Issue on GPS*, 87 :3–15, Janvier 1999.

[32] F. Erbas, K. Kyamakya, and K. Jobmann. Modelling and Performance Analysis of a Novel Position-Based Reliable Unicast and Multicast Routing Method Using Coloured Petri Nets. In *Proceedings of the 58th IEEE Vehicular Technology Conference (VTC'03)*, Orlando, USA, Octobre 2003.

[33] M. Ergen, S. Coleri, B. Dundar, R. Jain, and A. Puri. Application of GPS to Mobile IP and Routing in Wireless Network. In *Proceedings of the 56th IEEE Vehicular Technology Conference (VTC'02)*, pages 1115 – 1119, Vancouver, Canada, Septembre 2002.

[34] M. Ergen, S. Coleri, B. Dundar, A. Puri, J. Walrand, and P. Varaiya. Fast Handoff with Position Information for Mobile IP. In *Proceedings of the International Conference on IP based Cellular Networks (IPCN Upperside 02)*, Paris, France, Avril 2002.

[35] M. Ergen, S. Coleri, B. Dundar, A. Puri, J. Walrand, and P. Varaiya. Position Leverage Smooth Handover Algorithm for Mobile IP. In *Proceedings of the IEEE International Conference on Networking (ICN'02)*, Atlanta, USA, Août 2002.

[36] D. Farinacci, T. Li, S. Hanks, D. Meyer, and P. Traina. Generic Routing Encapsulation (GRE), Internet Engineering Task Force Request for Comments (RFC) 2784, Mars 2000.

[37] K.T. Feng and T.E. Lu. Velocity and Location Aided Routing for Mobile Ad Hoc Networks. In *Proceedings of the 60th IEEE Vehicular Technology Conference (VTC'04)*, Los Angeles, USA, Septembre 2004.

[38] P. Fournogerakis, S. Kyriazakos, and G. Karetsos. Enhanced Handover Performance in Cellular Systems based on Position Location of Mobile Terminals. In *Proceedings of the 2002 International Conference on Computational Science (ICCS'02)*, Amsterdam, The Netherlands, Avril 2002.

[39] The Gimp Toolkit version 2, `http://www.gtk.org`.

[40] R. Hsieh, Z.G. Zhou, and A. Seneviratne. S-MIP : A Seamless Handoff Architecture for Mobile IP. In *Proceedings of the the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (Infocomm'03)*, San Francisco, USA, Avril 2003.

[41] L. Hsu, R. Purnadi, and S.S. Wang. Maintaining Quality of Service (QoS) during Handoff in Cellular System with Movement Predictions Schemes. In *Proceedings of the 50th IEEE Vehicular Technology Conference (VTC'99)*, pages 2153–2157, Amsterdam, Netherlands, Septembre 1999.

[42] Institute of Electrical and Electronics Enginneers, `http://www.ieee.org`.

[43] The internet engineering task force. `http://www.ietf.org`.

[44] International Communications Union (ITU). Transmission Systems and Media, Digital Systems and Networks, Recommendation G.711 : Pulse Code Modulation (PCM) of Voice Frequencies, 1988.

[45] Emil Ivov and Martin Andre. The FMIPv6 Open Source Implementation Suite. `http://fmipv6.org`.

[46] D. Johnson, C. Perkins, and J. Arkko. Mobility Support in IPv6, Internet Engineering Task Force Request for Comments (RFC) 3775, Juin 2004.

[47] J. R. Beal Jr. Contextual Geolocation : A Specialized Application for Improving Indoor Location Awareness in Wireless Local Area Networks. In *Proceedings of the 36th Annual Midwest Instruction and Computing Symposium (MICS'03)*, Avril 2003.

[48] H. A. Karimi and P. Krishnamurthy. Real-Time Routing in Mobile Networks Using GPS and GIS Techniques. In *Proceedings of the 34th Hawaii International Conference on System Sciences (HICSS'01)*, Maui, Hawaii, Janvier 2001.

[49] K. Kaukonen and R. Thayer. A Stream Cipher Encryption Algorithm "Arcfour", Work in Progress, Internet Engineering Task Force draft-kaukonen-cipher-arcfour-03.txt, Juillet 1999.

[50] Y.B. Ko and N.H. Vaidya. Location-aided Routing (LAR) in Mobile Ad Hoc Networks. In *Proceedings of the 4th annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom'98)*, pages 66–75, Dallas, USA, Octobre 1998.

[51] Y.B. Ko and N.H. Vaidya. Geocasting in Mobile Ad Hoc Networks : Location-based Multicast Algorithms. In *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'99)*, pages 101–110, New Orleans, USA, Février 1999.

[52] S. Kyriazakos, D. Drakoulis, and G. Karetsos. Optimization of the Handover Algorithm based on the Position of the Mobile Terminals. In *Proceedings of the IEEE Symposium on Communication and Vehicular Technology (SCVT'00)*, Leuven, Belgium, Octobre 2000.

[53] S. Kyriazakos, P. Fournogerakis, and G. Karetsos. Location-Aided Handover in Cellular Networks. In *Proceedings of the 4th International Symposium on Wireless Personal Multimedia Communications (WPMC'01)*, Aalborg, Denmark, Septembre 2001.

[54] A. LaMarca, Y. Chawathe, S. Consolvo, J. Hightower, I. Smith, J. Scott, T. Sohn, J. Howard, J. Hughes, F. Potter, J. Tabert, P. Powledge, G. Borriello, and B. Schilit. Place Lab : Device Positioning Using Radio Beacons in the Wild. In *Proceedings of the 3rd International Conference on Pervasive Computing (PERVASIVE'05)*, pages 116–133, Munich, Germany, Mai 2005.

[55] M. Ylianttila and J. Mäkelä and K. Pahlavan. Geolocation Information and Intertechnology Handoff. In *Proceedings of the IEEE International Conference on Communications (ICC'00)*, pages 1573–1577, New Orleans, USA, Juin 2000.

[56] K. El Malki and H. Soliman. Simultaneous Bindings for Mobile IPv6 Fast Handovers, Work in Progress, Internet Engineering Task Force draft-elmalki-mobileip-bicasting-v6-06.txt, Juillet 2005.

[57] D. L. Mills. Network Time Protocol (Version 3), Specification, Implementation and Analysis, Internet Engineering Task Force Request for Comments (RFC) 1305, Mars 1992.

[58] Arunesh Mishra, Minho Shin, and William Arbaugh. An Empirical Analysis of the IEEE 802.11 MAC Layer Handoff Process. *SIGCOMM Comput. Commun. Rev.*, 33(2) :93–102, 2003.

[59] J. Montavont, E. Ivov, and T. Noel. Analysis of Mobile IPv6 Handover Optimizations and their Impact on Real-Time Communication. In *Proceedings of the IEEE Conference on Wireless Communications and Networking (WCNC'07)*, Honk Kong, Chine, Mars 2007.

[60] J. Montavont, J. Lorchat, and T. Noel. Deploying NEMO : A Practical Approach. In *Proceedings of the 6th International Conference on ITS Telecommunications (ITST'06)*, Chengdu, Chine, Juin 2006.

[61] J. Montavont, N. Montavont, and T. Noel. Enhanced Schemes for L2 Handover in IEEE 802.11 Networks and their Evaluations. In *Proceedings of the 16th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'05)*, volume 3, pages 1429–1434, Berlin, Allemagne, Septembre 2005.

[62] J. Montavont and T. Noel. Fast Location-based protocol and Cisco WDS System Comparison. Livrable LSIIT pour le CRE France Télécom R&D, Août 2005.

[63] J. Montavont and T. Noel. Fast Location-based protocol specifications. Livrable LSIIT pour le CRE France Télécom R&D, Janvier 2005.

[64] J. Montavont and T. Noel. Fast Location-based protocol - Performance Evaluation. Livrable LSIIT pour le CRE France Télécom R&D, Août 2006.

[65] J. Montavont and T. Noel. IEEE 802.11 Handovers Assisted by GPS Information. In *Proceedings of the 2nd IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob'06)*, pages 166–172, Montréal, Canada, Juin 2006.

[66] J. Montavont, T. Noel, and K. Guillouard. Anticipation des Handovers des noeuds IPv6 à l'aide d'informations de géolocalisation. In *Colloque Francophone sur l'ingénierie des Protocoles (CFIP'06)*, Tozeur, Tunisie, Novembre 2006.

[67] N. Montavont and T. Noel. Handover Management for Mobile Nodes in IPv6 Networks. *IEEE Communication Magazine*, 40(8) :38–43, Août 2002.

[68] N. Montavont and T. Noel. Analysis and Evaluation of Mobile IPv6 Handovers over Wireless LAN. *Mobile Networking and Applications (MONET), special*

issue on Mobile Networking through IPv6 or IPv4, 8(6) :643–653, Novembre 2003.

[69] N. Montavont and T. Noel. Anticipated Handover over IEEE 802.11 Networks. In *Proceedings of the IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob'2005)*, Montréal, Canada, Août 2005.

[70] N. Moore. Optimistic Duplicate Address Detection (DAD) for IPv6, Internet Engineering Task Force Request for Comments (RFC) 4429, Avril 2006.

[71] G. J. Morgan-Owen and G. T. Johnston. Differential GPS Positioning. *IEEE Electronic and Communication Engineering Journal*, 7 :11–21, Février 1995.

[72] T. Narten, E. Nordmark, and W. Simpson. Neighbor Discovery for IP Version 6 (IPv6), Internet Engineering Task Force Request for Comments (RFC) 2461, Décembre 1998.

[73] J.C. Navas and T. Imielinski. GeoCast - Geographic Addressing and Routing. In *Proceedings of the 3rd annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom'97)*, pages 66–76, Budapest, Hungary, Septembre 1997.

[74] V. Nuorvala, H. Petander, and A. Tuominen. Mobile IP for Linux (MIPL), `http://mobile-ipv6.org`.

[75] University of Cambridge Computer Laboratory Digital Technology Group. The Active Bats Geolocation System. `http://www.cl.cam.ac.uk/research/dtg/research/wiki/BatSystem`.

[76] The Open Graphics Library (OpenGL), `http://www.opengl.org`.

[77] Data Processing Open System Interconnexion, Basic Reference Model, ISO IS 7498, 1984.

[78] Chun-Su Park, Hye-Soo Kim, Sang-Hee Park, Kyunghun Jang, and Sung-Jea Ko. Fast Handoff Algorithm Using Access Points with Dual RF Modules. In *Proceedings of the Universal Multiservice Networks : Third European Conference (ECUMN'04)*, pages 20–28, Porto, Portugal, Octobre 2004.

[79] J. Pesola and S. Pokanen. Location-aided Handover in Heterogeneous Wireless Networks. In *Proceedings of Mobile Location Workshop*, Aalborg, Danemark, Mai 2003.

[80] E. Ivov Petrov and T. Noel. Soft Handovers over 802.11b with Multiple Interfaces. In *Proceedings of the 2nd International Symposium on Wireless Communication Systems (ISWCS'05)*, pages 549–554, Siena, Italy, Septembre 2005.

[81] J. Postel. Internet Protocol, Internet Engineering Task Force Request for Comments (RFC) 791, Septembre 1981.

[82] P. Prasithsangaree, P. Krishnamurthy, and P. K. Chrysanthis. On Indoor Position Location with Wireless Lans. In *Proceedings of the 13th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'02)*, pages 720–724, Lisboa, Portugal, Septembre 2002.

[83] C. Prehofer, N. Nafisi, and Q. Wei. A framework for context-aware handover decisions. In *Proceedings of the 14th Annual IEEE International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC'03)*, Beijing, Chine, Septembre 2003.

[84] N. B. Priyantha, A. Chakaborty, and H. Balakrishnan. The Cricket Location-support System. In *Proceedings of the 6th Annual ACM/IEEE International Conference on Mobile Computing an Networking (MobiCom'00)*, Boston, USA, Août 2000.

[85] N. B. Priyantha, A. K. L. Mui, H. Balakrishnan, and S. J. Teller. The Cricket Compass for Context-Aware Mobile Applications. In *Proceedings of the 7th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom'01)*, Rome, Italy, Juillet 2001.

[86] PROTEAN research group. The Multi-Generator Toolset (MGEN), `http://pf.itd.nrl.navy.mil/mgen/`.

[87] QUAGGA. Quagga routing software suite, `http://www.quagga.net`.

[88] I. Ramani and S. Savage. SyncScan : Practical Fast Handoff for 802.11 Infrastructure Networks. In *Proceedings of the 24th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'05)*, pages 675–684, Miami, USA, Mars 2005.

[89] D. Sandras and Al. Gnomemeeting : an open source VoIP and video conferencing application for GNOME, `http://www.gnomemeeting.org`.

[90] Sangho Shin and Andrea G. Forte and Anshuman Singh Rawat and Henning Schulzrinne. Reducing MAC layer handoff latency in IEEE 802.11 wireless LANs. In *Proceedings of the 2nd International Workshop on Mobility Management & Wireless Access Protocols (MobiWac'04)*, pages 19–26, Philadelphia, USA, 2004. ACM Press.

[91] H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson. RTP : A Transport Protocol for Real-Time Applications, Internet Engineering Task Force Request for Comments (RFC) 3550, Juillet 2003.

[92] K. Seada and A. Helmy. Efficient Geocasting with Perfect Delivery in Wireless Networks. In *Proceedings of IEEE International Conference on Wireless Communications and Networking (WCNC'04)*, Atlanta, USA, Mars 2004.

[93] The Network Simulator SimulX, `http://simulx.u-strasbg.fr`.

[94] R. W. Sinnott. Virtues of the Haversine. *Sky and Telescope*, 68 :158, Décembre 1984.

[95] H. Soliman, C. Catelluccia, K. El Malki, and L. Bellier. Hierarchical Mobile IPv6 Mobility Management (HMIPv6), Internet Engineering Task Force Request for Comments (RFC) 4140, Août 2005.

[96] Cisco Systems. Cisco Catalyst 6500 Series Wireless LAN Services Module : White Paper, `http://cisco.com`.

[97] Cisco Systems. Cisco Fast Secure Roaming Application Note, `http://cisco.com`.

[98] Cisco Systems. Configuring WDS, Fast Secure Roaming and Radio Management, `http://cisco.com`.

[99] Joshua A. Tauber. Indoor Location Systems for Pervasive Computing. *Area Exam Report*, Août 2002.

[100] F. Teraoka, K. Gogo, K. Mitsuya, R. Shibui, and K. Mitani. Unified L2 Abstractions for L3-Driven Fast Handover, Work in Progress, Internet Engineering Task Force, draft-koki-mobopts-l2-abstractions-05.txt, Juin 2006.

[101] S. Thomson and T. Narten. IPv6 Stateless Address Autoconfiguration, Internet Engineering Task Force Request for Comments (RFC) 2462, Décembre 1998.

[102] C. Tseng, L. Yen, H. Chand, and K. Hsu. Topology-Aided Cross-Layer Fast Handoff Designs for IEEE 802.11/Mobile IP Environments. *IEEE Communications Magazine*, 43, Décembre 2005.

[103] J. Vatn. An Experimental study of IEEE 802.11b Handover performance and its Effect on Voice Traffic. In *Technical Report TRITA-IMIT-TSLAB R 03 :01, Telecommunication Systems Laboratory, Department of Microelectronics and Information Technology, KTH, Royal Institute of Technology*, Stockholm, Sweden, Juillet 2003.

[104] H. Velayos and G. Karlsson. Techniques to Reduce the IEEE 802.11b Handoff Time. In *Proceedings of the IEEE International Conference on Communications (ICC'04)*, volume 7, pages 3844–3848, Paris, France, Juin 2004.

[105] S.S. Wang, A. Rajendran, and M. Wylie-Green. Adaptive Handoff Method using Location Information. In *Proceedings of the 12th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'01)*, pages 43–47, San Diego, USA, Septembre 2001.

[106] R. Want, A. Hopper, V. Falcao, and J. Gibbons. The Active Badge Location System. *ACM Transactions on Office Information Systems (TOIS)*, 10 :91–102, Janvier 1992.

[107] The Wi-Fi Alliance. `http://www.wi-fi.org`.

Liste des publications

Conférences internationales

- **Analysis of Mobile IPv6 Handover Optimizations and their Impact on Real-Time Communication**, J. Montavont, E. Ivov and T. Noel, IEEE Conference on Wireless Communications and Networking (WCNC'07), Honk Kong, Chine, 11-15 Mars 2007.

- **Deploying NEMO : A Practical Approach**, J. Montavont, J. Lorchat and T. Noel, 6th International Conference on ITS Telecommunications, Chengdu, Chine, 21-23 Juin 2006.

- **IEEE 802.11 Handovers Assisted by GPS Information**, J. Montavont and T. Noel, 2nd IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob'06), Montréal, Canada, 19-21 Juin 2006.

- **Enhanced Schemes for L2 Handover in IEEE 802.11 Networks and their Evaluations**, J. Montavont, N. Montavont and T. Noel, 16th Annual IEEE International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC'05), Berlin, Allemagne, 11-14 Septembre 2005.

Conférences nationales

- **Anticipation des Handovers des noeuds IPv6 à l'aide d'informations de Géolocalisation**, J. Montavont, T. Noel and K. Guillouard, Colloque Francophone sur l'ingénierie des Protocoles (CFIP'06), Tozeur, Tunisie, 30 Octobre - 3 Novembre 2006.

Brevets

– **FR-06/01251 : Procédé d'allocation d'au moins un point d'accès à un terminal mobile, dans un réseau cellulaire, serveur de mobilité et programmes correspondants**, J. Montavont, T. Noel, K. Guillouard, P. Bertin and S. Bonjour, Février 2006 (date de dépot).

Rapports de contrats

– **Fast Location-Based Handover, Perfomance Evaluation**, J. Montavont and T. Noel, livrable France Télécom, Août 2006.

– **Nautilus6 Project Activity Report in 2005**, Wide Report, Février 2006.

– **Fast Location-Based Handover protocol and Cisco WDS System Comparison**, J. Montavont and T. Noel, livrable France Télécom, Août 2005.

– **Fast Location-Based Handover protocol specification**, J. Montavont and T. Noel, livrable France Télécom, Janvier 2005.

– **Etude de la mobilité IP et des systèmes de géolocalisation dans les réseaux sans fil**, J. Montavont et T. Noel, livrable France Télécom, Juillet 2004.