Points d'accès virtuels pour une mobilité transparente

Yan Grunenberger, Franck Rousseau

Points d'accès virtuels pour une mobilité transparente

Yan Grunenberger* — **Franck Rousseau****

** Mootwin*
Grenoble, France
yan.grunenberger@mootwin.com

*** Université de Grenoble*
LIG — Laboratoire d'Informatique de Grenoble
681 rue de la passerelle, BP72
38402 Saint Martin d'Hères Cedex, France
Franck.Rousseau@imag.fr

RÉSUMÉ. *La gestion efficace de la mobilité dans les réseaux WiFi est toujours un problème ouvert aujourd'hui : aucune méthode n'a été standardisée, et le déplacement d'un mobile entre les points d'accès d'un réseau local sans fil est soit traité par des protocoles propriétaires, soit par ré-association. Hors, la gestion de cette mobilité dans une infrastructure est cruciale pour plusieurs raisons : maîtrise du délai et de sa variance, contrôle du réseau sur les clients, optimisation de performances. Nous présentons le concept de* point d'accès virtuel *pour gérer la mobilité des terminaux dans un réseau d'infrastructure. De ce fait, les terminaux n'ont plus conscience de leur mobilité, et toute la complexité est reportée dans le réseau. Il est ainsi possible de contrôler précisément la mobilité, d'optimiser les ressources lors des déplacements, et donc fournir une meilleure qualité de connexion globale, tout en conservant une compatibilité avec les clients existants sans aucune modification matérielle ou logicielle de ceux-ci.*

ABSTRACT. *Mobility management in WiFi networks is still an open issue today: there is no standard method defined, and terminal mobility is handled either via proprietary protocols, or simply by re-association. However, managing mobility in an infrastructure network is utterly important for several reasons: controlling delay and jitter in communications, managing clients from the network, optimizing performance. We propose the concept of* virtual access points *to manage terminal mobility in infrastructure networks. In this scheme, terminals are not aware that they move, and all the complexity is pushed back in the network. It is then possible to control mobility from a global point of vue, to optimize network resources for mobile terminals, hence providing a better quality of service. Finally, this scheme is compatible with existing clients without any hardware nor software modification.*

MOTS-CLÉS : *Réseaux sans fil, mobilité, point d'accès, virtualisation, infrastructure.*

KEY WORDS: *Wireless networks, mobility, access point, virtualization, infrastructure.*

1. Introduction

La mobilité des terminaux est un problème largement étudié dans la littérature. En effet, débarrassés du point d'attache physique de leur terminal, les utilisateurs aspirent à une liberté totale de mouvement, comme avec un téléphone mobile classique, à savoir le maintien de la connexion au cours du déplacement. Dans le contexte des réseaux WiFi, il s'agit principalement de maintenir la connectivité de l'interface IEEE 802.11 d'un terminal mobile *associé* en mode infrastructure à son point d'accès.

Dans une approche de type réseau d'opérateur, l'association est décidée par le réseau lui-même ; dans les réseaux WiFi, les décisions de mobilité sont laissées au terminal. De ce fait, le terminal doit *scanner* les canaux potentiels afin de découvrir de nouveaux points d'accès et solliciter l'association. De plus, le réseau d'interconnexion doit réagir à ces associations successives en mettant à jour ses tables de commutation, ou en allouant une nouvelle adresse. Ces opérations font donc varier énormément les temps de réaction, ce qui est très pénalisant pour la qualité du trafic contraint, comme la voix sur IP par exemple ; de plus, les décisions étant prises par le mobile, il est impossible de gérer les ressources d'un réseau de point d'accès de manière optimale, pour l'équilibrage de charge ou la réduction d'interférences par exemple.

Dans ce cadre, notre approche est donc d'éliminer la gestion de la mobilité par les clients pour la replacer intégralement au sein du réseau constitué par les points d'accès interconnectés. Pour ce faire, nous décidons d'appliquer ce que l'on peut appeler un changement de référentiel par analogie avec la mécanique classique. Nous proposons de considérer les clients mobiles comme des entités fixes et par conséquent de rendre les points d'accès auxquels ils sont connectés mobiles. Évidemment, dans la réalité ce n'est pas le cas, nous avons donc pour cela recours au concept de *point d'accès virtuel*, qui est un élément mobile au sein du réseau d'infrastructure. Chaque mobile se voit alors associer son propre point d'accès virtuel lorsqu'il s'associe au réseau, et celui-ci le suivra lors de ses déplacements.

De cette manière nous nous affranchissons totalement des problèmes énoncés plus haut, tout en conservant une compatibilité totale avec les clients existants sans aucune modification matérielle ou logicielle de ceux-ci. Nous allons voir par la suite comment nous avons pu implémenter très facilement ce concept grâce à un *framework* de manipulation de paquets appelé PACMAP. Une première implémentation en Python a été réalisée afin de tester le concept, pour ensuite être transposée nativement en C. Les expérimentations menées avec ces deux prototypes ont permis d'évaluer les performances ainsi que les limitations de la solution proposée. Enfin nous replacerons ces travaux dans le contexte de la gestion de mobilité pour les réseaux WiFi et présenterons les perspectives.

2. Gestion de la mobilité dans les WLAN

Ordinairement la gestion de la mobilité est divisée en deux grandes classes : la macro-mobilité qui traite des mouvements à grande échelle, lors desquels l'utilisateur va changer de réseau IP ; et la micro-mobilité, qui s'attache au problème de la mobilité locale au sein d'un réseau composé de points d'accès contigus. Dans le premier cas, cela implique d'effectuer des opérations au niveau de 802.11 ainsi que du réseau, notamment pour l'obtention d'une nouvelle adresse. Cette problématique a été largement étudiée dans le cadre de Mobile IP notamment.

Nous nous plaçons ici dans le second cas, celui de la micro-mobilité, appliquée au protocole 802.11, que les auteurs de [MON 03] ont appelé le *handoff* de niveau 2. Le fait de transférer une connexion entre deux points d'accès d'un même réseau 802.11 va imposer des contraintes temporelles afin de maintenir la continuité des opérations dans les couches supérieures, typiquement IP, TCP, RTP. Des techniques de *buffering* permettent d'éviter les pertes de données, mais certains types de trafics interactifs comme la voix sur IP, ne peuvent tolérer un délai supplémentaire trop important lors d'un déplacement sous peine de perturber le service.

En mode infrastructure, chaque AP 802.11 forme un BSS, *basic service set*. Leur interconnexion via un DS, *distribution system*, en vue d'offrir un réseau sans fil étendu forme un ESS, *extended service set*. Dans ce contexte, la norme 802.11 ne définit pas de manière générique le système de distribution, et la commutation ou *handoff* d'un point d'accès à un autre est laissée à l'entière responsabilité du mobile. Dans les implémentations actuelles des stations, le *handoff* découle d'une suite d'opérations déclenchées par le terminal mobile telle que décrite dans [MIS 03] :

– Évaluation de l'évolution du rapport signal bruit du lien radio utilisé par l'écoute des balises, et notification de seuils.

– Lancement de la recherche d'autres points d'accès par détection de balises en scrutant les canaux, le *scan*. Cette opération peut être soit active soit passive : si elle est active, des paquets de sondes sont envoyés par la station pour interroger les différentes canaux ; dans ce cas, l'opération peut entraîner une perte de paquet, car le changement de canal n'est pas instantané [BAH 04]. Certaines cartes disposent d'un mode passif qui assure un *scan* durant des phases d'inactivité, lors du blocage par le *Network Allocation Vector* (NAV) par exemple.

– Ré-authentification : la station s'authentifie à nouveau en fonction d'une liste de priorités des AP. La ré-authentification peut être accomplie grâce au transfert des informations d'accréditation par un protocole dédié afin de diminuer le surcoût lié aux échanges de sécurité et aux fonctions cryptographiques.

– Ré-association avec le nouveau point d'accès.

Ce processus est la cause de délais importants et très variables lors du déplacement des utilisateurs au sein d'un réseau WiFi. Mishra *et al.* ont étudié de manière empirique le *handoff* dans les réseaux 802.11 [MIS 03] et ont évalué les durées de ces opérations. Les auteurs ont relevé une grande disparité dans les délais de transition — entre 200 et 1 000 ms, sachant qu'il est recommandé un délai maximum de bout en bout de 150 ms pour le transport de la voix.

Les délais identifiés par Mishra *et al.* sont principalement le délai de sonde (échange de 3 à 7 trames), le délai d'authentification (3 à 4 trames), et le délai de ré-association (3 à 4 trames 802.11). Les auteurs mentionnent aussi le délai dit de *bridging*, correspondant au rafraîchissement des tables ARP des points d'accès utilisés dans la procédure de *handoff*. D'après les auteurs, le délai de sonde constitue 90% de la perte de temps liée au *handoff*. D'autres expériences [VEL 04] confirment ces résultats : les phases de détection et de recherche prennent trop de temps.

Le choix de positionner la décision de mobilité au sein du terminal peut paraître pertinent dans le sens où le terminal est le plus à même d'identifier les réseaux disponibles à proximité. Cependant, le but ultime d'un réseau supportant la mobilité est d'assurer le transport des données vers et depuis le terminal, et cette tâche doit être privilégiée devant toute autre.

3. Principes des points d'accès virtuels

Ayant constaté que la mobilité des terminaux pose de sérieux problèmes, nous proposons comme solution qu'ils ne se déplacent plus ! Bien évidemment, ils continueront de bouger physiquement, mais par un simple renversement de point de vue et un changement de référentiel adéquat, nous pouvons rendre les terminaux fixes du point de vue du réseau : il suffit pour cela que ce soit le réseau qui bouge de concert avec les mobiles. Toutefois, les mobiles ayant des comportements potentiellement tous différents, il n'est pas possible de gérer le problème uniformément. Nous devons offrir à chaque terminal sa propre vue du réseau, son propre réseau virtuel.

Dans le cas des réseaux locaux sans fil 802.11, en mode infrastructure donc, cela se traduit finalement très simplement. La vue du réseau à laquelle accède un client lui est fournie par le point d'accès auquel il est associé. Mettre en place la solution proposée ci-dessus revient donc à associer à chaque mobile un point d'accès virtuel qui le suivra dans ses déplacements, lui rendant ainsi la mobilité totalement transparente. La Figure 1 présente ce principe.

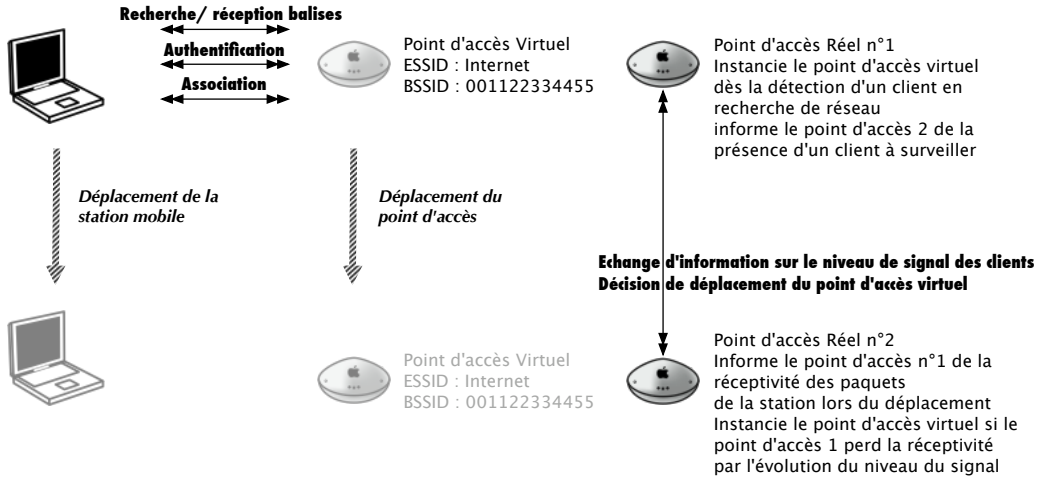

Figure 1 – Mobilité avec utilisation de point d'accès virtuels.

La gestion de mobilité des terminaux 802.11 est maintenant transformée en gestion de mobilité de points d'accès virtuels au sein même du réseau d'infrastructure, qui lui est fixe. Cela soulève deux problèmes :

– posséder le moyen de détecter le déplacement des terminaux, afin de s'assurer que son AP virtuel le suive dans le réseau d'infrastructure ; plusieurs solutions sont possibles ici : contrôle du niveau de signal, géo-localisation, etc.

– faire croire au terminal que la connectivité est assurée en permanence où qu'il se trouve.

Pour le premier problème lié à l'évaluation du déplacement du terminal, il s'agit avant tout de maintenir un niveau de signal suffisant pour assurer l'échange des paquets. Les points d'accès sur-

veilleront le niveau de signal des mobiles, générant des événements lors de fortes variations, afin de déclencher les actions adéquates.

Le second problème est plus épineux. Les clients 802.11 standards utilisent deux éléments pour évaluer leur connectivité : d'une part, les acquittements reçus indiquent une connexion toujours active ; d'autre part, en l'absence de trafic, les terminaux utilisent les balises du point d'accès pour évaluer la disponibilité du réseau. Donc, si l'on arrive à assurer la présence continuelle de ces deux éléments au niveau d'une station mobile, de son point de vue la connectivité sera assurée.

4. Implémentation des AP virtuels

PACMAP [GRU 09] est un *framework* que nous avons développé comme support au développement d'architectures *cross-layer*. Son rôle est la manipulation de packets bruts, venant du réseau pour être traités dans le système ou inversement. Couplé à *Scapy*[1], un outil initialement conçu pour faciliter l'écriture de *parsers* et générateurs de paquets dans le contexte de la sécurité sans fil, il est rapide de développer des gestionnaires de protocoles quelconques. Grâce aux possibilités de manipulation du protocole 802.11 incluses, nous pouvons simuler la présence d'un point d'accès dès lors que la station est à portée radio. Ainsi, du point de vue de la station, il n'y a plus de déplacement, nous avons créé un point d'accès virtuel.

Une technique proche de celle-ci est déjà utilisée par les points d'accès actuels. Ils simulent des réseaux multiples en émettant plusieurs types de balises sur un même canal. Cependant, ces techniques sont limitées et chaque point d'accès virtuel constitue une entité indépendante. Ici, en utilisant PACMAP, nous pouvons récupérer les informations d'un point d'accès virtuel et les transférer d'un point d'accès réel à l'autre. Les AP virtuels sont donc mobiles.

L'utilisation d'AP virtuels permet d'éviter toute perte de connectivité au noeud mobile, facilitant le support de la mobilité pour les applications exigentes comme la VoIP. De plus, le contrôle de la connectivité est confiné au coeur de réseau, ce qui facilite la gestion d'un réseau purement sans fil. Enfin, l'utilisation d'AP virtuels permet d'associer au point d'attache du mobile l'intégralité de ses paramètres lors de ses déplacements : informations sur le routage, éventuels caches, ensemble de modulations autorisées, etc. Nous obtenons une optimisation *cross-layer* et une personnalisation de la connection de manière très simple dans cet exemple précis.

Pour cette première implémentation nous nous plaçons dans le cas d'une topologie dense de points d'accès, fonctionnant sur un canal commun. Si cette topologie causera une augmentation des collisions pour une densité de clients élevée, elle offre des propriétés simplificatrices intéressantes, notamment pour la détection de la mobilité et pour la signalisation entre point d'accès, qui ne sont pas l'objet premier de cette étude.

Nous évaluons d'abord la faisabilité du concept d'AP virtuels avec PACMAP en utilisant le langage Python. Selon le principe de fonctionnement des AP virtuels, un client qui cherche à se connecter doit se voir offrir un point d'accès dédié. La première étape consiste à intercepter les requêtes de sondage des clients 802.11 pour envoyer une réponse spécifique. Nous présentons ci-dessous un extrait de code dans le simple but de montrer la facilité d'implémentation à l'aide de l'outil PACMAP.

1. `http://www.secdev.org/projects/scapy/`

```
def proto80211_probereq(packet, length):
    # Reception d'une trame de decouverte des points d'acces
    dot11_frame = Packet(packet)
    dot11_frame.decode_payload_as(Dot11)
    # Recuperation de l'adresse du client
    client = dot11_frame.getlayer(Dot11).addr2
    # Generation d'un nom de reseau de la forme "Client-XX:XX:XX:XX:XX:XX"
    # ou XX:XX:XX:XX:XX:XX est l'adresse materielle unique du client
    ssid = "Client-%s" % client
    current_timestamp = time.mktime(datetime.datetime.now().timetuple())*1e6
        +datetime.datetime.now().microsecond
    # Preparation d'un paquet de reponse
    dot11_answer = Dot11(
    type = "Management",
    addr1 = dot11_frame.getlayer(Dot11).addr2,
    addr2 = bssid,
    addr3 = bssid)/Dot11ProbeResp(timestamp=current_timestamp,cap = 0x0104)/
        Dot11Elt(ID=0,info=ssid)/Dot11Elt(ID=1,info="\x82")/Dot11Elt(ID=3,
        info="\x06")
    # Envoi de la reponse
    pacmap.sendpacket(str(dot11_answer),len(str(dot11_answer)),1)
    return 1
```

Le client perçoit donc la présence d'un point d'accès personnalisé, dont le nom est de la forme `Client-00:11:22:33:44:55` où `00:11:22:33:44:55` est l'adresse matérielle du client. Il cherche ensuite à se connecter suivant la procédure standard.

Dès qu'un client est associé, on ajoute ses références dans la listes des clients gérés. À partir de ce moment, une fonction périodique envoie une balise à intervalles réguliers, indiquant que le point d'accès est toujours présent, ce qui permet au client de se savoir toujours associé au réseau. Nous profitons de cette balise pour y insérer le niveau de signal du dernier paquet reçu, que nous stockons à chaque arrivée d'un paquet. Désormais, nous disposons d'un point d'accès qui pour chaque client diffuse dans la balise associée le niveau du signal reçu, et qui par un procédé de *Beacon Stuffing*[CHA 07], permet d'avertir son voisinage de points d'accès de sa prise en charge du client.

Il ne reste plus qu'à traiter le point de vue d'un point d'accès secondaire, situé sur le même canal radio : celui-ci reçoit les balises et doit les traiter. Nous maintenons deux listes par point d'accès : une liste des clients, et une liste des clients à surveiller. Il suffit alors de surveiller le dernier niveau de signal reçu avec le niveau de signal rapporté au niveau du point d'accès initial. La migration est un processus sans signalisation particulière : à partir du moment où le nouveau point d'accès enregistre un nouveau client, il émule à son tour le point d'accès par émission de balises. Le point d'accès initial en est donc averti par les balises, et peut donc détruire l'association.

À ce stade, nous disposons d'une architecture de mobilité fonctionnelle en quelques lignes de code Python. À cela nous incorporons une gestion des trames DHCP, ainsi qu'une gestion des trames ARP. Ainsi, toute requête ARP sera interceptée et fera l'objet d'une réponse en fonction de la situation de la station concernée.

5. Tests de mobilité

La mise en oeuvre de notre prototype nous a conduit à considérer un certain nombre de paramètres ajustables pour la gestion de mobilité. Ces paramètres sont principalement liés à la réactivité de notre solution, évaluée dans notre laboratoire pour deux points d'accès équipés de PACMAP et du script d'AP virtuel, dans une configuration identique à la Figure 1.

Le premier paramètre est le seuil à partir duquel il est plus intéressant de faire transiter le trafic sur un point d'accès plutôt qu'un autre. Dans notre approche, le seuil est empiriquement déterminé à partir des seuils de réception obtenus par le placement des points d'accès vis à vis du client. Mais ce seuil pourrait être complété par d'autres paramètres : la charge du point d'accès, le niveau de trafic ambiant par exemple. À l'aide d'une fonction d'évaluation satisfaisante, on obtiendrait ainsi également un équilibrage de charge dans le réseau.

Dans notre cas, nous avons déterminé empiriquement pour la situation que le seuil de signal assurant une bonne couverture permettant une absence de perte de paquet était une différence de 15 dB dans le niveau de signal reçu : dès que le niveau de signal des paquets reçus par un AP dépasse celui d'un autre de ce seuil, nous amorçons l'enregistrement du terminal sur le nouvel AP et le désenregistrement sur l'ancien.

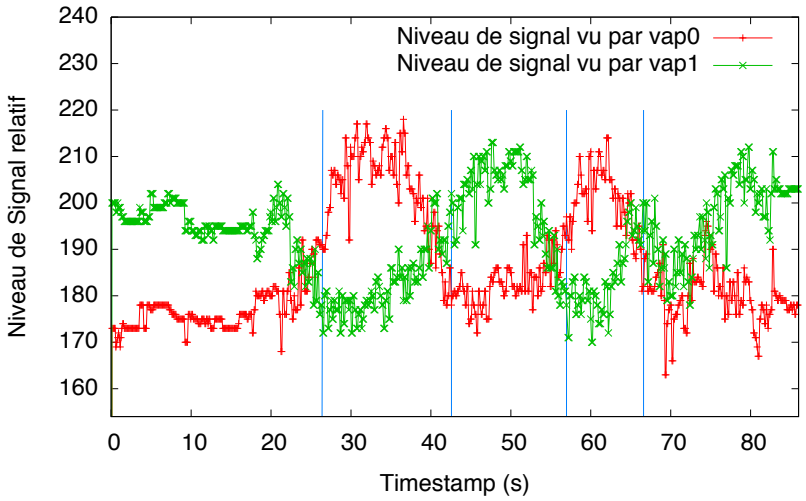

Figure 2 – Evolution du niveau de signal du client vu par les deux points d'accès et décisions de mobilité.

Un exemple de l'évolution du signal reçu par les deux points d'accès est présenté en Figure 2. Dans une première phase, le mobile est statique, et son trafic est géré par le point d'accès vap1. Puis, il y a déplacement, le niveau de signal est beaucoup plus fluctuant, et ceci, au niveau des deux points d'accès. Une fois la valeur de seuil atteinte, le trafic du client est écoulé par vap0. Le client se déplaçant entre les deux points d'accès, il y a 3 autres décisions de mobilité qui sont prises, de telle sorte que le terminal client est toujours associé au point d'accès ayant la meilleure réception.

La mise en corrélation des deux mesures, sur le point d'accès actuel et sur le point d'accès distant permet d'éliminer les fluctuations et d'obtenir un bon compromis entre stabilité de la décision et maintien de la connectivité.

Le désenregistrement est également un paramètre de réactivité de notre solution. En effet, le désenregistrement, qui correspond à l'abandon par un point d'accès de la gestion des paquets d'un client, est fonction de la réception des balises émises par le point d'accès qui prend désormais en charge la gestion des paquets de ce client.

Dans notre cas, ces balises sont envoyées au rythme d'une balise toutes les 100 ms, ce qui correspond à notre temps de réaction pour mesurer le niveau du signal. Cependant dans la pratique, il est possible qu'une balise soit transmise par l'ancien point d'accès alors que la migration vient d'avoir lieu. Cela est imputable au temps de traitement des balises par PACMAP. Afin de s'assurer que la migration a bien eu lieu, nous introduisons un paramètre Δ qui correspond au nombre de balises issues du nouveau point d'accès. Dans la pratique, 2 balises consécutives suffisent pour éviter tout désenregistrement intempestif. Le problème et la solution retenue sont présentés sur la Figure 3 : l'arrêt des balises correspond au désenregistrement effectif du client grâce à l'utilisation de l'intervalle Δ.

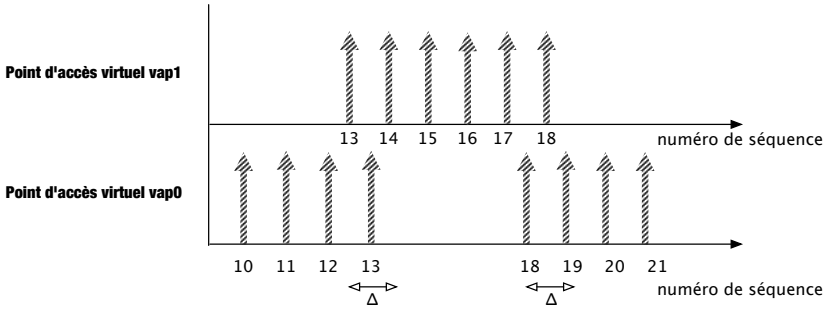

Figure 3 – Émission des balises lors d'une détection de mobilité.

En terme d'usage, nous avons effectué des tests de trafic bidirectionnel de taille faible et de fréquence régulière, simulant ainsi un trafic VoIP. La plate-forme se compose de deux ordinateurs équipés d'une carte sans fil et exécutant PACMAP et le script Python. Les interfaces Ethernet créées par PACMAP sont ensuite reliées par pont Ethernet l'une à l'autre. Ainsi nous reproduisons le schéma classique d'un réseau doté de plusieurs points d'accès.

Nous utilisons un $ping$ de 64 octets toutes les 200 ms sur un client se déplaçant entre les deux points d'accès hébergeant les AP virtuels et nous étudions l'évolution de la latence en fonction de la migration du terminal. Le $ping$ est lancé depuis le point d'accès initial.

La Figure 4 présente l'évolution de la latence. Les instants où le terminal migre d'un point d'accès à un autre sont indiqués par les traits verticaux, entre les numéros de séquences $seq = 144$ et $seq = 344$ où la station est connectée sur le point d'accès AP 2.

Mis à part les effets du pont réseau, nous constatons qu'il n'y a pas de réelle augmentation de la latence lors des phases de transition : nous atteignons ainsi l'objectif fixé, à savoir une mobilité trans-

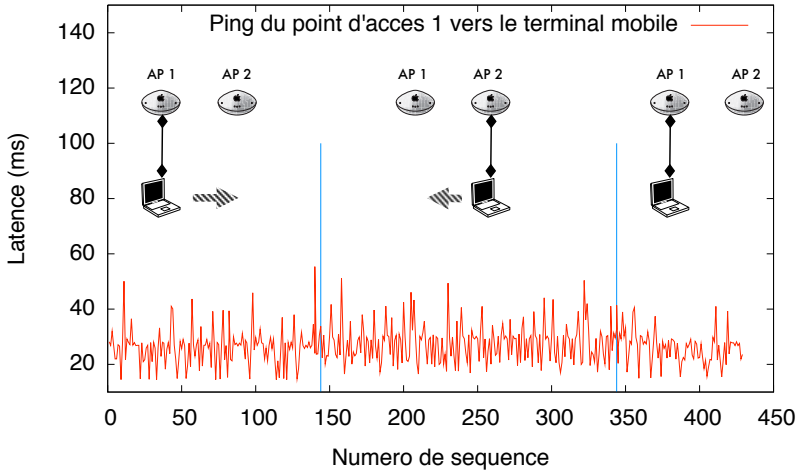

Figure 4 – Évolution de la latence en fonction de l'état de mobilité du terminal (version Python).

parente pour les terminaux mobiles. Cependant, les niveaux de latence relevés et leurs fluctuations en régime continu sont imputables à l'utilisation du code *Scapy* dans le script Python.

Néanmoins, les résultats obtenus avec PACMAP lors de l'examen comparé d'une implémentation d'une machine à état 802.11 en langage natif vis à vis de son équivalent en Python semblent indiquer qu'une implémentation native du concept d'AP virtuel, bien que plus complexe à réaliser, bénéficierait d'un gain notable sur la latence moyenne observée. Nous décidons donc de réimplémenter ce prototype en C et de conduire les mêmes mesures que nous reportons sur la Figure 5.

Nous observons que la latence a très fortement diminué grâce à l'utilisation du code natif. Les perturbations observées sont alors uniquement dues à l'accès au médium, et nous observons les mêmes propriétés de conservation de la connectivité et d'absence d'augmentation de la latence durant les phases de mobilité. Le coût du pont réseau filaire entre les deux points d'accès est dorénavant identifiable : ajout de 0,4 ms sur la latence moyenne observée de 4 ms.

6. Discussion

Comme annoncé, la solution implémentée s'inscrit dans un cadre très particulier d'un canal radio unique et de points d'accès à portée radio les uns des autres. Cependant, il est envisageable d'étendre cette solution à des topologies plus diversifiées.

Tout d'abord, le principe même du point d'accès virtuel implique une multiplication directe du nombre de balises en fonction du nombres de clients. Il est possible de limiter ce phénomène en réduisant la fréquence d'émission des balises de manière inversement proportionnelle au nombre de clients sur la même fréquence. Cependant, la réactivité de la détection de la mobilité s'en trouve

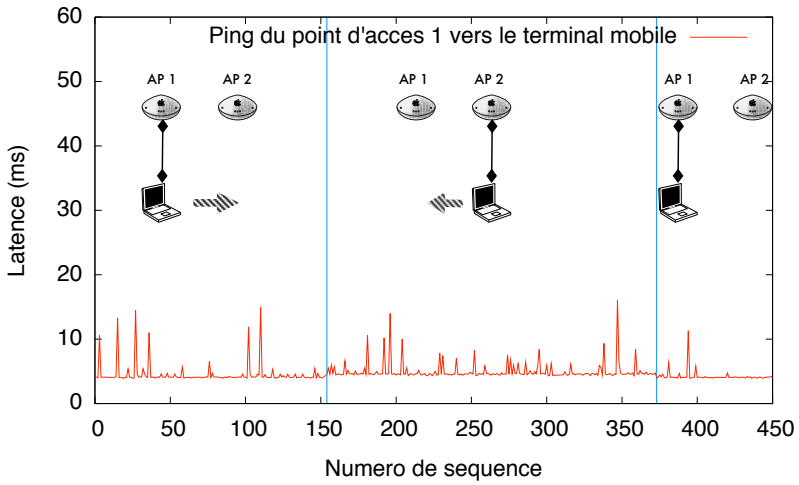

Figure 5 – Évolution de la latence en fonction de l'état de mobilité du terminal (version native).

réduite car les points d'accès connexes ne pourront informer de la prise en charge des clients qu'après le délai d'émission des balises concernées.

Cet écueil est à relativiser en fonction du type de réseau d'interconnection des points d'accès — le système de distribution. Dans notre exemple, les points d'accès utilisaient le canal radio comme méthode de signalisation. Toutefois, si l'interconnexion est indépendante du réseau d'accès, soit par l'usage d'une autre technologie comme Ethernet, soit par l'utilisation d'un canal radio distinct, il est envisageable que cette signalisation passe par un protocole d'interopérabilité (de type 802.11r ou LWAPP) afin d'assurer la synchronisation des points d'accès. Dès lors, ceux-ci pourraient s'échanger périodiquement, sans surcoût pour le réseau d'accès, les informations sur le niveau de signal reçu et ainsi assurer la continuité de la connectivité pour les clients.

Enfin, l'utilisation d'un canal radio unique a pour conséquence directe l'augmentation de la probabilité de collision. Il faut profiter de l'utilisation de canaux radio multiples afin de réduire les interférences. Une piste à fort potentiel peut être la manipulation directe de la balise envoyée au client. En effet, nous avons pu constater sur des clients usuels de type iPhone et iPod Touch que ceux-ci initiaient un changement de canal lorsque les balises émises indiquaient l'utilisation d'un canal différent du canal courant. Là encore, le prérequis immédiat est l'existence d'un protocole d'interopérabilité entre les points d'accès assurant la couverture radio de la zone.

7. Travaux connexes

IAPP [IEE 03] a été la première proposition de protocole de gestion de la mobilité dans IEEE 802.11 concernant la communication entre points d'accès. Il est intéressant de noter que ce standard

a été retiré et les solutions laissées au libre choix des constructeurs, qui ont privilégié une gestion de la mobilité au niveau des terminaux clients, sans réelle prise en compte dans les points d'accès. Les recherches se sont de fait concentrées sur le comportement des clients.

Mishra *et al.* [MIS 03] dont nous avons évoqué les travaux précédemment ont développé des heuristiques visant à utiliser un minimum de phases de détection active pour augmenter le temps de réponse. Les auteurs proposent ensuite d'utiliser des graphes de voisinage dans [MIS 04] et ont proposé une modification d'IAPP en conséquence. Cette modification inclut un système de cache proactif : il utilise l'information sur le voisinage pour envoyer de manière proactive le contexte au voisin concerné.

Un mécanisme de cache a été également proposé par Shin *et al.* dans [SHI 04] : il consiste à réutiliser des informations obtenues lors d'un *scan* actif précédent.Les auteurs proposent également de profiter du caractère adjacent des canaux et d'effectuer un *scan* total des canaux pour construire un masque qui sera utilisé lors des *handoffs* suivants. Ces propositions ne sont efficaces que lorsque la densité du réseau est suffisante, et réduisent la réactivité des clients à l'apparition d'un nouveau point d'accès.

Velayos *et al.* [VEL 04] ont une approche différente : ils proposent une modification du comportement des cartes 802.11 en déclenchant le phase de sondage dès que la perte de paquets en l'absence de collision est identifiée. Les auteurs démontrent ainsi que la phase de *scan* peut être déclenchée dès que 3 paquets consécutifs sont perdus en l'absence de collision, ce qui réduit pour les auteurs le délai de *handoff* de 900 ms à 3 ms en l'absence d'authentification et en présence de trafic pour la station.

Mhatre *et al.* [MHA 06] approfondissent la thématique des *triggers* permettant d'identifier le besoin d'effectuer un *handoff*. Le *scan* actif par sondage ne doit être réalisé que lorsqu'aucune information n'a pu être récupérée de manière passive. Les auteurs proposent ensuite et évaluent une série de *triggers* sur les valeurs de signal reçu pour déclencher un changement d'AP. Ainsi, ils évaluent un algorithme à base de détection de balise, un algorithme à seuil, puis à base d'hystérésis, et enfin un algorithme analysant les tendances. Au final, les délais de *handoff* obtenus sur leur plate-forme expérimentale indiquent un fort délai (entre 530 et 860 ms) pour les algorithmes à base de seuil et de détection de beacon. Pour les autres algorithmes, les délais sont nettement plus courts (140 à 450 ms), car il s'agit en fait d'algorithmes proactifs, initiant un *handoff* même lorsque la connexion est quand même existante.

Cependant, même si des modèles de mobilité sont proposés permettant d'anticiper les déplacements de l'utilisateur, il n'existe pas à notre connaissance de proposition d'amélioration du handoff 802.11 bénéficiant d'une décision prise par le réseau lui-même, comme dans les réseaux cellulaires par exemple. Les réseaux 802.11 représentent donc une opportunité intéressante pour l'étude des mécanismes de micro-mobilité : en effet, la prise en compte des caractéristiques physiques, comme le niveau du signal, ou encore la présence de balises permettent des améliorations substantielles de la micro-mobilité.

8. Conclusion

Le problème de la gestion de la mobilité des clients mobiles est essentiel dans les réseaux 802.11. La norme, n'ayant pas proposé de mécanisme générique, a laissé un espace vacant pour une fonctionnalité naturellement présente dans les usages de 802.11. Les approches actuelles reposent donc essentiellement sur la qualité de l'implémentation du client, où celui-ci est rendu responsable de la gestion de sa connectivité. Lors des phases de mobilité, les caractéristiques des réseaux 802.11 induisent des délais incompatibles avec les applications sensibles comme la voix sur IP en usage sur ces réseaux. En replaçant la gestion de la mobilité au coeur du réseau des points d'accès, nous proposons une solution élégante permettant la mise en oeuvre d'une mobilité efficace avec les clients 802.11 existants, tout en offrant des possibilités de gestion inédites depuis le coeur de réseau. La mise en œuvre de cette approche a requis le développement d'une solution de points d'accès virtuels, qui offre des performances très satisfaisantes.

9. Bibliographie

[BAH 04] BAHL P., CHANDRA R., DUNAGAN J., « SSCH : slotted seeded channel hopping for capacity improvement in IEEE 802.11 ad-hoc wireless networks », *Proceedings of MobiCom'04*, septembre 2004, p. 216–230.

[CHA 07] CHANDRA R., PADHYE J., RAVINDRANATH L., WOLMAN A., « Beacon-Stuffing : Wi-Fi Without Associations », *Proceedings of the 8th IEEE Workshop on Mobile Computing Systems and Applications (HotMobile 2007)*, février 2007.

[GRU 09] GRUNENBERGER Y., ROUSSEAU F., « PACMAP : A Packet Manipulation Framework for Cross-Layer Implementation », 2009, Soumis à publication.

[IEE 03] IEEE STD 802.11F^{TM}–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^{TM} Operation », IEEE Standard, 2003.

[MHA 06] MHATRE V., PAPAGIANNAKI K., « Using smart triggers for improved user performance in 802.11 wireless networks », *Proceedings of the 4th International Conference on Mobile Systems, Applications and Services*, janvier 2006, p. 246–259.

[MIS 03] MISHRA A., SHIN M., ARBAUGH W., « An empirical analysis of the IEEE 802.11 MAC layer handoff process », *ACM SIGCOMM Computer Communication Review*, vol. 33, n° 2, 2003, p. 93–102.

[MIS 04] MISHRA A., SHIN M., ARBAUGH W., « Context caching using neighbor graphs for fast handoffs in a wireless network », *Proceedings of INFOCOM 2004*, mars 7–11 2004.

[MON 03] MONTAVONT N., NOËL T., « Analysis and evaluation of mobile IPv6 handovers over wireless LAN », *Mobile Networks and Applications*, vol. 8, n° 6, 2003, p. 643–653.

[SHI 04] SHIN S., FORTE G., RAWAT A., SCHULZRINNE H., « Reducing MAC layer handoff latency in IEEE 802.11 wireless LANs », *Proceedings of the Second International Workshop on Mobility Management & Wireless Access Protocols*, janvier 2004, p. 19–26.

[VEL 04] VELAYOS H., KARLSSON G., « Techniques to Reduce IEEE 802.11 b MAC Layer Handover Time », *Proceedings of IEEE International Conference on Communications*, 2004.