

---

# Mécanismes de *handover* pour les réseaux IP sans-fil

Farouk Belghoul\* — Yan Moret\*\* — Christian Bonnet\*

\* Département de Communications Mobile  
Institut Eurecom  
2229 Route des Crêtes, BP 193  
F-06904 Sophia Antipolis Cedex  
{prénom.nom}@eurecom.fr

\*\* École des Mines d'Alès  
LGI2P - Institut EERIE  
Parc scientifique Georges Besse  
F-30035 Nîmes cedex  
{prénom.nom}@ema.fr

---

*RÉSUMÉ.* Le *handover* est le processus qui permet, à un terminal mobile, d'effectuer le passage entre deux points d'attachement à un réseau. Ce changement de point d'attachement implique une déconnexion momentanée du terminal mobile, et des perturbations des communications en cours. Ainsi, pour disposer d'une communication de qualité avec un terminal mobile, le *handover* doit introduire des mécanismes efficaces en toutes circonstances. Dans ces termes, plusieurs techniques de *handover* ont été proposées pour le protocole IP. Dans cet article, nous présentons une analyse et une comparaison de ces diverses techniques. Nous évaluons les performances de bout-en-bout des communications utilisant les protocoles UDP et TCP. Les résultats de cette analyse sont exploités pour présenter finalement une proposition de *soft-handover*.

*ABSTRACT.* Handover is the process which allows the roaming of a mobile node between two access points. This roaming implies the momentary disconnection of the mobile node, and disruptions of current communications. Several handover mechanisms have been proposed for IP based protocols. In this document, we show comparisons and analyses of these mechanisms. We evaluate the end-to-end communication performance with UDP and TCP protocols. Finally, we propose a *soft-handover* mechanism.

*MOTS-CLÉS :* IP, mobilité, *handover*, *soft-handover*, *fast-handover*, *smooth-handover*, TCP.

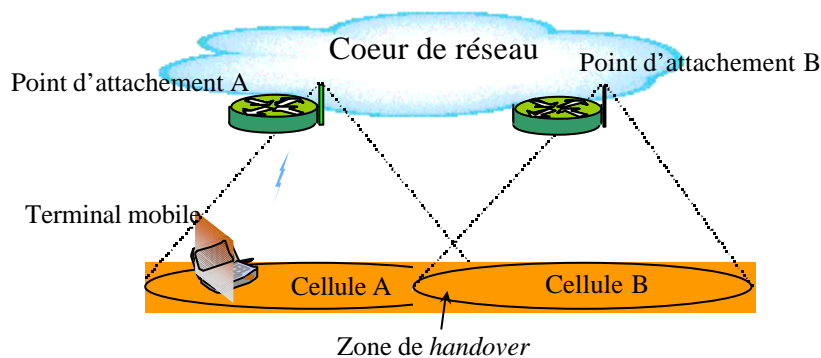
*KEYWORDS:* IP, mobility, *handover*, *soft-handover*, *fast-handover*, *smooth-handover*, TCP.

---

## 1. Introduction

De nos jours, différentes technologies d'accès réseaux sans-fil coexistent. A quelques exceptions près, elles permettent à un terminal de se déplacer tout en gardant une connectivité avec un réseau de cœur (réseau d'interconnexion). Plusieurs points d'attachements sont répartis dans le réseau, et assurent la connectivité des terminaux mobiles. Une caractéristique primordiale d'une technologie d'accès est la distance maximale (la portée) entre un point d'attachement et un terminal mobile, à partir duquel la réception des informations devient précaire. La zone délimitée par cette portée est appelée cellule de bas niveau. La Figure 1 présente un terminal mobile connecté à un point d'attachement A relié à un réseau filaire. La portée du point d'attachement est symbolisée par la cellule A. Tant que le terminal mobile est situé au centre de la cellule A, la qualité de réception de la communication sans-fil est optimale. Plus le terminal mobile se rapprochera du bord de la cellule, plus la qualité de réception se dégradera. En dehors de la cellule A, le terminal mobile ne peut plus communiquer avec le point d'attachement A, et le terminal perd sa connectivité.

Le déplacement du terminal mobile entraîne la déconnexion du terminal mobile avec le point d'attachement A, et la connexion avec le point B. Ce phénomène est le *handover*. Les technologies d'accès sans-fil étant incompatibles, ce type de *handover* de bas niveau ne permet pas au terminal mobile d'effectuer un mouvement entre cellules hétérogènes (technologies d'accès distinctes). Le délai  $D$  de déconnexion au réseau est susceptible de provoquer des pertes de paquets, et d'influencer les délais de transmission des autres paquets. Durant cette période, aucun paquet ne peut être transmis vers ou depuis le terminal mobile.

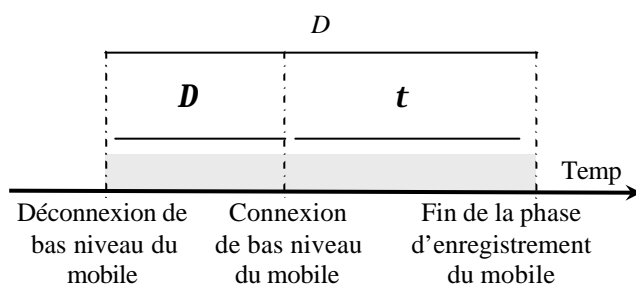


**Figure 1.** Interaction entre un terminal mobile et le cœur de réseau

Le protocole IP (Internet Protocol) est très largement utilisé comme protocole d'interconnexion de réseaux filaires. Il est indépendant des technologies d'accès

sous jacentes. Cette propriété est fondamentale pour pouvoir effectuer un mouvement entre cellules hétérogènes. IP apparaît comme le protocole permettant de fédérer les diverses technologies d'accès filaires et sans-fil.

Un point d'attachement au réseau IP est un routeur d'accès. Il permet d'accéder à une cellule IP constituée d'une ou plusieurs cellules homogènes de bas niveau. Le *handover* IP est le processus qui permet à un terminal mobile de changer de routeur d'accès. Le délai  $D$  de déconnexion IP du terminal mobile désigne le temps d'indisponibilité du mobile au niveau IP provoqué par le *handover* (Figure 2). Durant ce délai, aucun paquet IP ne peut être transmis depuis ou vers le terminal mobile. Cette indisponibilité débute au moment précis où le mobile perd sa connectivité avec son ancien routeur d'accès, jusqu'au moment où il est capable d'envoyer et recevoir les paquets IP à travers son nouveau routeur d'accès. La quantité de paquets IP perdus, provoqués par le *handover* IP, est proportionnelle au délai  $D$ . Ce délai est composé de deux grandes périodes  $t$  et  $D$ . La période  $t$  peut précéder ou succéder à la période  $D$ . Cette période correspond au délai nécessaire de configuration des paramètres IP du mobile. L'enregistrement d'une adresse IP est un exemple typique de cette configuration.



**Figure 2.** Délai  $D$  de déconnexion IP du mobile

Les mécanismes de *handover* IP induits par *Mobile IPv4* (Perkins, 2002) ou *mobile IPv6* (Johnson et al., 2001) (Gustaafsson *et al.*, 2001) sont similaires. Le délai  $D$ , et la quantité de paquets IP perdus, sont relativement importants.

De nouvelles techniques comme le *fast-handover* (Koodli *et al.*, 2002), *bidirectional edge tunnel* (Kempf *et al.*, 2001) et de façon moindre *hierarchical mobile IP* (Castellucia, 2002), réduisent le délai. De fait, le délai  $D$  et la quantité de paquets perdus sont diminués.

Contrairement à ces dernières techniques, le *smooth-handover* (Koodli *et al.*, 2000) (Perkins *et al.*, 1999) a pour objectif de réduire le taux de pertes en sauvegardant, pendant la déconnexion, tous les paquets à destination du mobile. Après le *handover* IP, ces paquets sont renvoyés au terminal mobile par l'intermédiaire du nouveau routeur d'accès.

Enfin, la dernière technique nommée *soft-handover* tente de réduire la période **D**. Si le terminal mobile a la possibilité technique de se connecter simultanément à deux points d'attachement, il lui est possible d'éviter une déconnexion totale du mobile lors d'un *handover*. (Zhang et al., 2001) énonce les bases de cette technique.

Dans cet article, nous allons analyser et comparer les diverses techniques de *handover* IP, en considérant leurs impacts sur un flux UDP (User Datagram Protocol) et TCP (Transport Control Protocol) entre un terminal mobile et un terminal fixe. Le délai de transfert, le nombre de perte, et la gigue (variation du délai de transfert) des paquets seront considérés. De cette première analyse, nous proposerons une nouvelle approche de *soft-handover* basée sur IPv6 (Moret, 2002).

Cet article sera organisé comme suit : le chapitre 2 contiendra une description des protocoles classiques de *handover* IP : *mobile IPv4*, *mobile IPv6*, *hierarchical mobile IP*, *smooth-handover*, *fast-handover* et finalement *bidirectionnel edge tunnel handover*. Dans le chapitre 3, nous analyserons l'effet de ces mécanismes sur un flux TCP. Le chapitre 4 sera consacré à la présentation des principes de bases du *soft-handover*. Finalement, le chapitre 5 sera présentera quelques résultats numériques, afin d'illustrer partiellement les analyses théoriques des chapitres précédents.

## 2. Les diverses techniques de *handover* IP

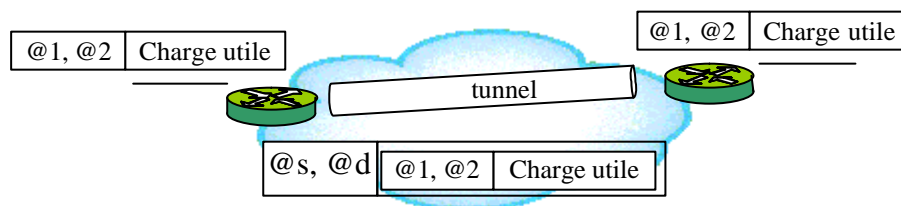
Dans ce chapitre, nous allons décrire les diverses techniques de *handover* basées sur le protocole IP. Une analyse de ces techniques, nous permettra de définir le comportement théorique d'un flux UDP entre un terminal mobile (nommé mobile) et un terminal fixe (nommé correspondant). Le mobile dispose d'au moins une interface radio (802.11, UMTS, etc...) lui permettant de se connecter à un ou plusieurs routeurs d'accès disposant du même type d'interface radio. Le correspondant dispose d'une interface filaire (Ethernet, etc...) lui permettant de se connecter au réseau. La communication (flux UDP) entre le correspondant et le mobile est unidirectionnelle et soutenue (il n'y a pas d'interruption de la transmission de la part du correspondant). Le comportement du flux UDP sera caractérisé par le délai de transfert, le nombre de perte et la gigue induits par le *handover* sur un flux de type UDP. Le délai de transfert représente le délai entre l'émission d'un datagramme UDP par le correspondant, et la réception de ce datagramme par le mobile. Le nombre de perte représente le nombre de datagramme UDP reçu par le mobile moins le nombre de datagramme émis par le correspondant durant le *handover*. La gigue représente la variation du délai de transfert (valeur absolue du délai de transfert d'un paquet en réception moins le délai de transfert du paquet précédemment reçu). Afin de simplifier notre analyse des *handover*, nous supposerons qu'une cellule IP n'est constituée que d'une cellule de bas niveau, que le point d'attachement de bas niveau et le routeur d'accès sont les mêmes entités,

que le taux d'erreur bit est négligeable, et que les routeurs ne sont pas congestionnés.

Dans tout notre exposé, la Figure 1 sera la figure de référence. Le routeur d'accès A initie le processus de *handover* IP, et le routeur B stoppe ce processus. Le mobile identifie le terminal mobile, et le correspondant un terminal fixe ayant une communication avec le mobile. Toutes les techniques de *handover* (sauf *mobile IPv4*) présentées dans ce document fonctionnent avec IPv4 ou IPv6. Nous supposons qu'elles utilisent IPv6.

### 2.1. Mobile IPv4

*Mobile IPv4* (Perkins, 2002) est la technique la plus ancienne de gestion de mobilité dans IP. Elle doit son succès à sa simplicité et sa flexibilité. Elle est à l'origine de plusieurs documents IETF (Johnson *et al.*, 2001). La gestion de la mobilité IP consiste à localiser et acheminer les paquets IP vers le mobile. Le mobile dispose d'un réseau de référence et d'une adresse de référence dans ce réseau. Cette adresse identifie à tout instant le mobile.



**Figure 3.** Représentation d'un tunnel IP

Chaque fois que le mobile se connecte au réseau, il se voit attribuer par un routeur, nommé *foreign agent*, une adresse IP temporaire. Le mobile enregistre cette adresse auprès d'un routeur de référence nommé agent mère, et s'identifie à l'aide de son adresse de référence. Cet agent est situé sur le réseau de référence du mobile. Ceci est la phase d'enregistrement, elle fait partie intégrante de la période  $t$  décrite précédemment. L'agent mère permet d'associer l'adresse de référence du mobile et son adresse temporaire en cours. Cette association est stockée dans une table de liaison, et permet de localiser à tout moment le mobile.

Un correspondant utilise l'adresse de référence du mobile afin de lui envoyer les paquets IP. L'agent mère intercepte tous les paquets destinés au mobile, et sont ensuite envoyés au *foreign agent* du mobile par l'intermédiaire d'un tunnel IPv4.

Un tunnel IPv4 (Figure 3) est une entité logique identifiée par un routeur  $s$  et un routeur  $d$ . Après interception d'un paquet IP, le routeur  $s$  encapsule ce paquet dans un paquet IPv4 dont l'adresse source  $@s$  est l'adresse de  $s$ , et l'adresse de

destination @d est l'adresse de *d*. Ainsi, quelque soit l'adresse source @1 et de destination @2 du paquet intercepté, le paquet transitera de *s* à *d* comme s'il avait été injecté dans un tunnel. L'établissement d'un tunnel est la seule méthode permettant d'imposer un chemin à un paquet IP sans modifier l'intégrité de son contenu. Son usage est obligatoire si le paquet est protégé par une entête d'authentification.

Le tunnel entre l'agent mère et le *foreign agent* est préalablement établi pendant la phase d'enregistrement du mobile. Arrivés au *foreign agent*, ces paquets sont envoyés directement au mobile à l'aide de l'adresse temporaire associée.

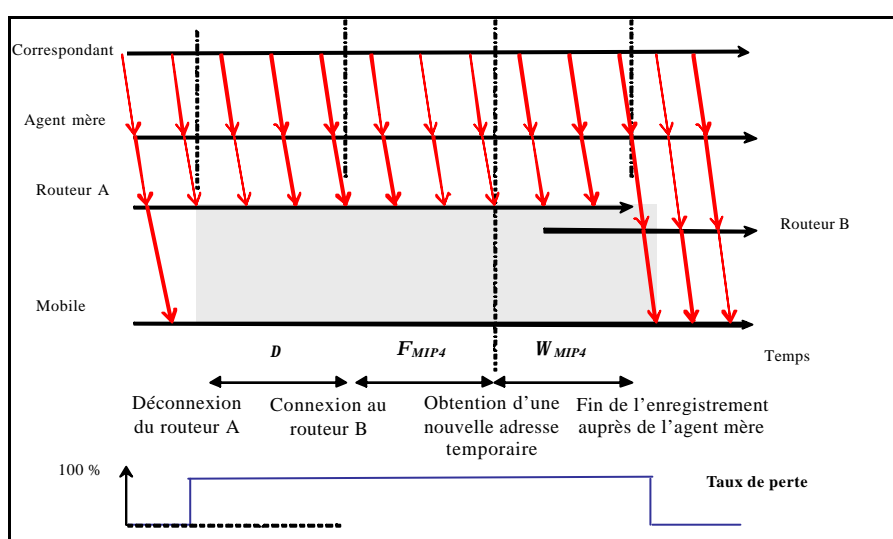


Figure 4. Diagramme temporel pour mobile IPv4

La Figure 4 présente un diagramme temporel des événements intervenant lors d'un *handover* IP pour *mobile IPv4*. Pour faciliter l'analyse, nous considérons que les *foreign agent* sont les routeurs d'accès A et B. Les axes horizontaux représentent l'espace temps dans lequel évolue le mobile, le routeur A, le routeur B, et le correspondant. Les flèches obliques décrivent le routage des paquets IP entre les entités. La partie basse du diagramme présente le taux de perte provoqué par le *handover*. Le délai global de déconnexion du mobile est :

$$D_{MIP4} = D + F_{MIP4} + W_{MIP4} \quad [1]$$

*D* est, comme défini dans l'introduction, le délai du *handover* de bas niveau. *F<sub>MIP4</sub>* est le délai nécessaire au mobile pour obtenir une nouvelle adresse temporaire, et *W<sub>MIP4</sub>* le délai nécessaire pour la phase d'enregistrement de cette adresse auprès de

l'agent mère.  $W_{MIP4}$  est égal au délai aller retour entre le mobile et l'agent mère. La somme de  $F_{MIP4}$  et de  $W_{MIP4}$  est la valeur  $t$  définie dans l'introduction. Durant la période  $D_{MIP4}$ , tous les paquets en transmission sont perdus. Ainsi de l'équation [1], nous déduisons que le nombre de paquets perdu  $N_{MIP4}$  lors du *handover* est :

$$N_{MIP4} = R.(D + F_{MIP4} + W_{MIP4})$$

avec  $R$  le débit moyen de transmission entre le correspondant et le mobile. La réduction de la distance entre l'agent mère et le mobile permet de réduire le nombre de pertes.

Enfin, nous remarquons que les paquets envoyés par le correspondant sont interceptés par l'agent mère, puis sont envoyés au mobile. Ceci induit un délai de transfert non optimal (routage triangulaire), et augmente la charge du trafic au niveau du cœur de réseau. Après le *handover*, ce délai est :

$$T_{MIP4} = T_{CH} + T_{HB} + T_{radio}$$

avec  $T_{CH}$  le délai de transfert entre le correspondant et l'agent mère,  $T_{HB}$  le délai de entre l'agent mère et le routeur B, et  $T_{radio}$  le délai moyen de transmission sur l'interface radio. L'anomalie de routage appelée routage triangulaire, provoque un délai additionnel lors du routage de paquets. Si le protocole d'accès au médium n'autorise pas la retransmission des paquets perdus,  $T_{radio}$  sera constant et la gigue  $J_{radio}$  induite par la transmission sera nulle. Par contre, si les retransmissions sont autorisées, la gigue  $J_{radio}$  ne sera plus nulle. En effet, lors d'un *handover*, le niveau de signal radio devient relativement faible provoquant des pertes isolées et la retransmission aléatoire de paquets. De plus, les retransmissions augmentent le délai de transmission, le délai moyen  $T_{radio}$  sera donc plus important. La gigue induite par le *handover* est :

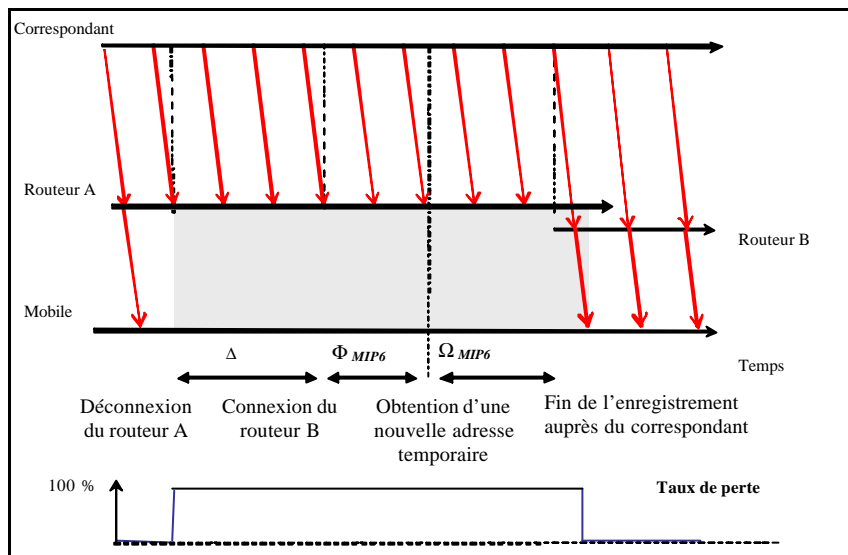
$$J_{MIP4} = |T_{HA} - T_{HB}| + J_{radio}$$

avec  $T_{HA}$  le délai de transfert entre l'agent mère et le routeur d'accès A,  $T_{HB}$  le délai entre l'agent mère et le routeur B.

## 2.2. Mobile IPv6

*Mobile IPv6* est l'évolution logique de *mobile IPv4*. Il exploite les mécanismes avancés d'IPv6 pour introduire quelques améliorations par rapport à *mobile IPv4*. Le mécanisme de configuration automatique des adresses d'IPv6 permet au mobile d'obtenir plus rapidement son adresse temporaire (Johnson, 2000). L'adresse temporaire combine l'adresse MAC de l'interface d'accès du mobile avec le préfixe du sous-réseau transmis par le routeur d'accès. Il n'y a plus de *foreign agent*. Un

espace d'adresses plus étendu est également disponible pour le mobile. La Figure 5 présente le diagramme temporel pour *mobile IPv6*.



**Figure 5.** Diagramme temporel pour *mobile IPv6*

Le mobile enregistre sa nouvelle adresse temporaire auprès de son agent mère, mais aussi directement auprès de l'ensemble de ses correspondants. Ainsi, après réception de la nouvelle adresse, le correspondant envoie directement les paquets vers l'emplacement courant du mobile sans passer par l'agent mère. Ce mécanisme est la solution apportée par *mobile IPv6* au problème du routage triangulaire de *mobile IPv4*. Le délai de transfert de paquets après le *handover* devient :

$$T_{MIP6} = T_{CB} + T_{radio}$$

avec  $T_{CB}$  le délai de transfert entre le correspondant et la routeur B. Or, nous avons  $T_{CB} < T_{CH} + T_{HB}$ . Ceci implique que  $T_{MIP6} < T_{MIP4}$ . La diminution de ce délai a un coût, puisque le mobile doit s'enregistrer auprès de plusieurs entités. Alors que *mobile IPv4* ne nécessite que l'enregistrement auprès de l'agent mère. La quantité de message de signalisation est donc accrue, ce qui diminue d'autant les ressources disponibles. Afin de réduire cette surcharge, le mobile doit sélectionner les correspondants privilégiés qui auront l'usage et l'intérêt de ces enregistrements.

Tout comme *mobile IPv4*, le *handover* dans *mobile IPv6* engendre une période de déconnexion du mobile et une perte de tous les paquets envoyés lors de cette période. Ce délai de déconnexion est :



$$D_{MIP6} = D + F_{MIP6} + W_{MIP6} \quad [2]$$

avec  $F_{MIP6}$  le délai de configuration automatique de l'adresse temporaire, et  $W_{MIP6}$  le délai d'enregistrement de cette adresse. Ce dernier est égal au délai aller-et-retour entre le mobile et le correspondant. Le nombre de paquets perdus lors du *handover* est donc :

$$N_{MIP6} = R.(D + F_{MIP6} + W_{MIP6}) \quad [3]$$

L'absence de routage triangulaire, dans *mobile IPv6*, améliore le délai de transferts par rapport à *mobile IPv4*. Cependant, la gigue de *mobile IPv6* est relativement identique à celle de *mobile IPv4* :

$$J_{MIP6} = |T_{CA} - T_{CB}| + J_{radio}$$

avec  $T_{CA}$  le délai de transfert entre le correspondant et le routeur A.

### 2.3. Hierarchical mobile IP

*Hierarchical mobile IP* (Soliman, 2000) est une extension de *mobile IPv4* et *mobile IPv6*. Il peut être associé à toutes les autres techniques de *handover*. Ce protocole est particulièrement conçu pour les mobiles changeant fréquemment leurs points d'attache au réseau dans un périmètre réduit.

Cette approche est basée sur l'introduction d'une architecture hiérarchique d'agents mobiles dans le réseau. Ces agents sont considérés comme des agents mère locaux, capables d'effectuer des opérations d'enregistrement du mobile. L'architecture hiérarchique du réseau, consiste à le structurer en domaines, chaque domaine ayant son propre agent de mobilité. Ce domaine à son tour est découpé en plusieurs régions ayant chacune son propre agent de mobilité. Ces agents sont hiérarchiquement inférieurs à l'agent mobile du domaine. Une région peut à son tour être découpée en sous-régions. Dès lors, les agents des sous-régions sont hiérarchiquement inférieurs aux agents de la région. Lors de la première connexion du mobile dans un domaine, il enregistre son adresse temporaire une première fois avec son agent mère et à l'ensemble des agents de mobilité hiérarchiquement supérieurs au point d'accès courant. L'agent de mobilité d'une région a une table de liaison permettant d'associer l'adresse temporaire du nœud mobile dans cette région, et l'adresse temporaire de la région de niveau hiérarchique supérieur. Les paquets IP sont véhiculés de région en région par l'intermédiaire de tunnels.

Chaque mouvement du mobile au sein d'une région, entraîne un enregistrement local de l'adresse temporaire. Cet enregistrement est transparent pour les agents hiérarchiquement supérieurs, pour l'agent mère et pour les correspondants. Ceci permet de réduire la charge d'enregistrement des adresses temporaires auprès des

diverses entités.  $W_{HMIP}$  est égal au délai aller et retour entre le mobile et l'agent de mobilité. L'agent de mobilité étant vraisemblablement plus proche que le correspondant, nous obtenons :

$$W_{HMIP} < W_{MIP6}$$

L'intérêt principal d'une telle approche est d'accélérer l'opération d'enregistrement des mobiles en traitant localement les déplacements. Le délai nécessaire pour l'obtention d'une nouvelle adresse temporaire étant identique à *mobile IPv6*, le délai de déconnexion est :

$$D_{HMIP} = D + F_{MIP6} + W_{HMIP},$$

et le nombre de paquets perdus pendant le *handover* devient :

$$N_{HMIP} = R(D + F_{MIP6} + W_{HMIP}) \quad [4]$$

De [3] et [4], nous déduisons que  $N_{HMIP} < N_{MIP6}$ . Cependant, l'introduction des agents de mobilité  $MA_i$  et des tunnels successifs augmente le délai de transfert des paquets IP :

$$T_{HMIP} = T_{MAI} + \sum T_{MA_i, MA_{i+1}} + T_{MA_n, B} + T_{radio}$$

avec  $T_{MA_i, MA_{i+1}}$  le délai de transfert entre les agents de mobilité  $MA_i$  et  $MA_{i+1}$ ,  $T_{CMAI}$  le délai entre le correspondant et l'agent  $MA_1$ , et  $T_{MA_n, B}$  le délai entre l'agent de mobilité  $MA_n$  et le routeur B. or,

$$T_{CN, MAI} + \sum T_{MA_i, MA_{i+1}} + T_{MA_n, B} \geq T_B$$

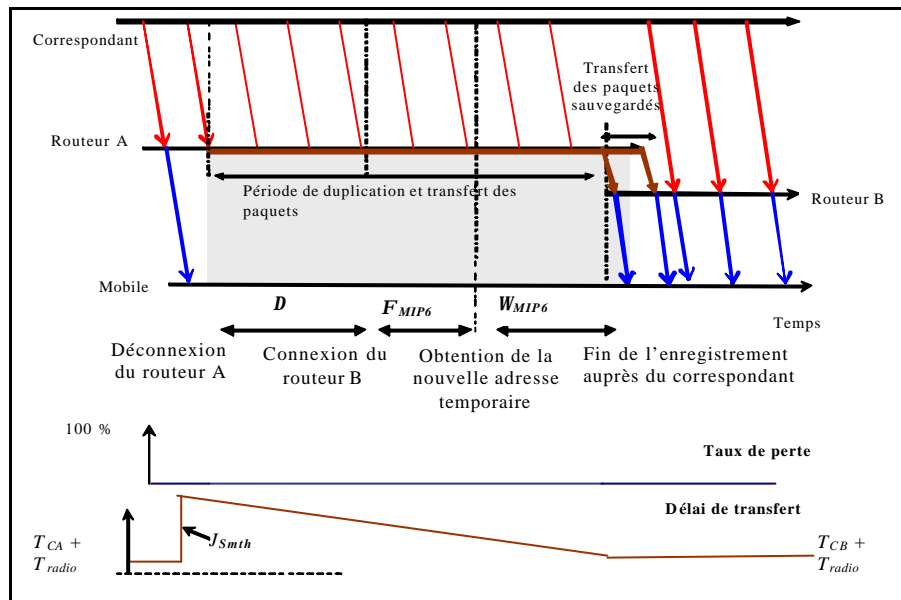
de ce fait  $T_{HMIP} > T_{MIP6}$ . La gigue induite par le *handover* est :

$$J_{HMIP} = |T_{MA_n, A} - T_{MA_n, B}| + J_{radio}$$

avec  $T_{MA_n, A}$  le délai de transfert entre l'agent  $MA_n$  et le routeur d'accès A. Les agents de mobilité étant proche des routeurs d'accès et si A et B appartiennent à un même domaine de gestion, il est fortement probable que la gigue de *hierarchical Mobile IP* soit inférieure à celle de *Mobile IPv6*. Si A et B n'appartiennent pas au même domaine de gestion, il n'y a pas de comparaison possible.

Toutefois, si l'on suppose que la gigue  $J_{radio}$  est prépondérante, la gigue globale de *hierarchical Mobile IP*, de *mobile IPv4* et de *mobile IPv6* serait similaire :

$$J_{HMIP} \approx J_{MIP6} \approx J_{MIP4}$$



**Figure 6.** Diagramme temporel pour le *smooth-handover*

#### 2.4. *Smooth-handover*

Le *smooth-handover* (Koodli, 2000) est une technique censée réduire considérablement le nombre de pertes de paquets IP lors d'un *handover*. Pour réduire ces pertes, elle fait appel à un mécanisme de sauvegarde dans le routeur d'accès A. Le routeur A effectue une copie de tous les paquets qu'il transmet au mobile avant, pendant et après la déconnexion. Bon nombre de paquets perdus en transmission ont été sauvegardés. Dès que le mobile obtient sa nouvelle connexion avec le routeur B et sa nouvelle adresse temporaire, le mobile dévoile au routeur B l'adresse du routeur A. Le routeur B établit un tunnel IP avec le routeur A et lui indique la présence du mobile. A cet instant, le routeur A cesse de sauvegarder et transmette les paquets sur l'interface sans-fil à destination du mobile. Il transmet au mobile, et à travers le tunnel, tous les paquets précédemment sauvegardés. Le routeur B se chargera de relayer ces paquets vers le mobile. Les paquets dupliqués et sauvegardés lors de la déconnexion sont récupérés localement.

Selon la technique de gestion du tampon, le mobile peut recevoir deux fois le même paquet. Il existe plusieurs techniques de sauvegarde afin d'optimiser les

ressources des routeurs d'accès (Perkins, 1999). La Figure 6 présente le diagramme temporel concernant le *smooth-handover*.

Le délai de déconnexion du mobile lors d'un *handover* est exactement le même que celui d'un *handover* pour *mobile IPv6* (équation [2]). Toutefois, le nombre de paquets perdus est :

$$N_{Smth} = \max(0, R.D_{MIP6} - B)$$

avec  $B$  la taille du tampon de sauvegarde. Si  $B$  est supérieur à  $R.D_{MIP6}$ , il n'y a aucune perte due au *handover*. En contre-partie, le mécanisme de sauvegarde et la tunnelisation des paquets du routeur A vers le routeur B augmentent notablement le délai de transfert et la gigue. Si nous négligeons le délai de transmission de A vers B, le délai de transfert des paquets sauvegardés dans le routeur A est :

$$T_{Smth} = T_{CA} + x.D_{MIP6} + T_{AB} + T_{radio}$$

avec  $T_{AB}$  le délai de transfert entre les routeurs d'accès A et B, et  $0 \leq x \leq 1$ . Le délai de transfert des autres paquets est identique à *mobile IPv6*. La gigue induite par le *handover* est :

$$J_{Smth} = D_{MIP6} + T_{AB} + J_{radio}$$

Or,  $T_{AB} \geq 0$  et  $D_{MIP6} > 0$ . De ce fait, nous obtenons :

$$J_{Smth} > J_{MIP6}$$

Nous pouvons conclure que le *smooth-handover*, peut éviter ou diminuer la perte de paquets, mais introduit un délai de transfert additionnel et une gigue importante. Son utilisation pour des transmissions de données ayant des contraintes temporelles paraît impossible.

### 2.5. *Fast-handover*

Le *fast-handover* (Koodli, 2002) réduit le délai de déconnexion du *handover*. Une des lacunes du *handover* dans *mobile IPv6* est la détection tardive du mouvement du mobile, et l'enregistrement tardive de l'adresse temporaire. Dans le cadre de *mobile IPv6*, le mobile détecte son mouvement après l'obtention de la nouvelle connexion physique avec le routeur B. A partir de ce moment, le mobile obtient sa nouvelle adresse temporaire, et l'enregistre. Afin d'anticiper le mouvement du mobile, le *fast-handover* suppose une interaction entre la couche IP et la couche de bas niveau. Cette anticipation du *handover* de bas niveau permet au

mobile, et aux routeurs d'accès de préparer la nouvelle liaison avec le routeur B avant même de perdre la liaison avec le routeur A.

Avant l'exécution du *handover* de bas niveau, le mobile identifie le routeur d'accès B. Il communique cette information au routeur A. Le routeur A établit un tunnel avec le routeur B. Le mobile peut obtenir sa nouvelle adresse temporaire, et entamer le processus d'enregistrement de cette adresse à travers le routeur A. Ainsi, dès que le mobile est lié au routeur B, il est immédiatement en mesure d'envoyer et de recevoir des paquets IP. Juste après la déconnexion, tous les paquets reçus par le routeur A, et destinés au mobile seront transmis au routeur B par l'intermédiaire du tunnel. Le routeur B les transmettra au mobile. Il est à noter que la charge due à la signalisation IP du *fast-handover* est importante. La Figure 7 présente le diagramme temporel pour le *fast-handover*.

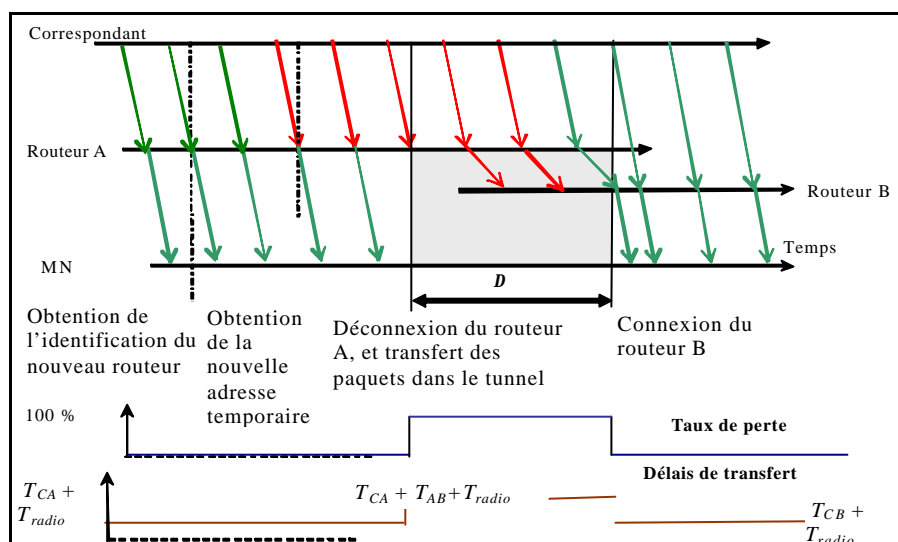


Figure 7. Diagramme temporel pour le *fast-handover*

Ce mécanisme réduit considérablement la durée de déconnexion du mobile lors du *handover* IP. Si le temps de déconnexion de bas niveau est inférieur au délai de traversée du tunnel, tous les paquets redirigés par le routeur A arriveront au mobile après sa liaison avec le routeur B. A cette condition, aucun paquet n'est perdu. Dans le cas contraire, un certain nombre de paquets arriveront au routeur B avant l'établissement de la nouvelle connexion et seront perdus. Dans tous les cas, le nombre de paquet perdu  $N_{fast}$  a la propriété suivante :

$$N_{Fast} < R.D$$

Contrairement au *smooth-handover* les paquets ne sont pas sauvegardés lors du *handover*. Le délai de transfert est donc largement diminué. Pendant le *handover*, ce délai est :

$$T_{Fast} = T_{CA} + T_{AB} + T_{radio}$$

Ensuite, ce délai devient équivalent à celui de *mobile IPv6* :

$$T_{Fast} = T_{CB} + T_{radio}$$

La gigue est :

$$J_{Fast} = T_{AB} + J_{radio}$$

Or, nous avons  $T_{AB} \geq 0$  ce qui implique :

$$J_{Fast} \geq J_{MIPv6} \text{ et } J_{Smth} > J_{Fast}$$

## 2.6. *Bi-directional Edge Tunnel Handover*

BETH (Bi-directional Edge Tunnel Handover) (Kempf, 2001) est une extension du *fast-handover*, pour améliorer ces performances lors d'un *handover* rapide (mouvement extrême du mobile). BETH élimine la phase d'obtention de l'adresse temporaire et de son enregistrement. Quand un mouvement du mobile est détecté, les routeurs d'accès ont deux choix. Soit ils appliquent le mécanisme du *fast-handover* et entament le processus d'anticipation pour constituer la nouvelle adresse du mobile. Soit ils décident de ne pas modifier l'adresse temporaire en cours, et d'utiliser cette adresse dans le nouveau réseau. Dans ce cas, un tunnel bidirectionnel est créé entre les routeurs A et B. Le routeur B est averti que le mobile va établir une liaison, et qu'il est identifié par l'adresse définie par le routeur A. Le routeur A intercepte tous les paquets destinés au mobile, et les dirige dans le tunnel. Le routeur B transmet directement ces paquets au mobile identifié par l'adresse temporaire initiale. Sachant que le mobile ne change pas d'adresse temporaire, tous les paquets qui lui sont destinés transiteront par le routeur A. De même, tous les paquets transmis par le mobile transiteront par le routeur A par l'intermédiaire du tunnel (contrairement au *fast-handover*, où les paquets sont transmis directement au correspondant). Ainsi, le déplacement du mobile est complètement transparent vis-à-vis du correspondant et de l'agent mère.

Le nombre de pertes et la gigue sont sensiblement identiques à ceux du *fast-handover*. Le délai de transfert est supérieur à celui du *fast-handover* puisque le tunnel entre les routeurs d'accès est utilisé en continu. Cependant, cette approche est intéressante, lors d'un déplacement fréquent et rapide du mobile à travers le réseau.

Il ne nécessite aucun enregistrement auprès de l'agent mère et des correspondants. Il réduit la charge du réseau induite par l'échange de messages de signalisation IP. D'autre part, si les délais d'obtention de la nouvelle adresse et d'enregistrement de cette adresse sont supérieurs au délai de stabilité du mobile, le *fast-handover* devient inopérant.

### 2.7. Analyse générale des diverses techniques de *handover*

Dans ce chapitre, nous proposons de résumer notre analyse des diverses techniques de *handover*. La Table 2 présente un récapitulatif des performances brutes de ces techniques, et la Table 1 les diverses notations associées.

$T$	Délai de transfert
$N$	Nombre de paquets perdus lors du <i>handover</i>
$R$	Débit moyen de transmission entre le mobile et le correspondant
$D$	Délai de déconnexion
$D$	Délai du <i>handover</i> de bas niveau
$W$	Délai d'enregistrement du mobile
$F$	Délai de configuration de l'adresse temporaire
$T_{CA}$	Délai de transfert entre le correspondant et le routeur d'accès A
$T_{CB}$	Délai de transfert entre le correspondant et le routeur d'accès B
$T_{CH}$	Délai de transfert entre le correspondant et l'agent mère
$T_{AB}$	Délai de transfert entre les routeurs d'accès A et B
$T_{HB}$	Délai de transfert entre l'agent mère et le routeur d'accès B
$T_{radio}$	Délai de transmission sur une interface radio
$J_{radio}$	Gigue de transmission sur une interface radio
$B$	Taille du tampon de sauvegarde

**Table 1.** Notations générales

*Mobile IPv4* introduit pour la première fois les bases de gestion de mobilité dans le monde IP. Lors d'un *handover*, le temps de déconnexion du mobile est relativement important, ce qui engendre un nombre important de pertes de paquets. De plus, le routage triangulaire oblige tous les paquets destinés au mobile de transiter par l'agent mère. Ainsi, l'agent mère devient un goulot d'étranglement, et les délais de transfert sont allongés.

	Performances brut pendant un <i>handover</i>	Comparaisons
<b>Mobile IPv4</b>	<ul style="list-style-type: none"> <li>- <math>D_{MIP4} = \mathbf{D} + \mathbf{F}_{MIP4} + \mathbf{W}_{MIP4}</math></li> <li>- <math>N_{MIP4} = R.D_{MIP4}</math></li> <li>- <math>T_{MIP4} = T_{CH} + T_{HB} + T_{radio}</math></li> <li>- <math>J_{MIP4} =  T_{HA} - T_{HB}  + J_{radio}</math></li> </ul>	
<b>Mobile IPv6</b>	<ul style="list-style-type: none"> <li>- <math>D_{MIP6} = \mathbf{D} + \mathbf{F}_{MIP6} + \mathbf{W}_{MIP6}</math></li> <li>- <math>N_{MIP6} = R.D_{MIP6}</math></li> <li>- <math>T_{MIP6} = T_{CB} + T_{radio}</math></li> <li>- <math>J_{MIP6} =  T_{CA} - T_{CB}  + J_{radio}</math></li> </ul>	$\mathbf{F}_{MIP4} > \mathbf{F}_{MIP6}$ $T_{MIP6} < T_{MIP4}$
<b>Hierarchical mobile IP</b>	<ul style="list-style-type: none"> <li>- <math>D_{HMIP} = \mathbf{D} + \mathbf{F}_{MIP6} + \mathbf{W}_{HMIP}</math></li> <li>- <math>N_{HMIP} = R.D_{HMIP}</math></li> <li>- <math>T_{HMIP} = T_{MAI} + \sum T_{MAiMAi+1}</math>  <math>+ T_{MA n.B} + T_{radio}</math></li> <li>- <math>J_{HMIP} =  T_{MA n.A} - T_{MA n.B}  + J_{radio}</math></li> </ul>	$N_{HMIP} < N_{MIP6}$ $T_{HMIP} > T_{MIP6}$
<b>Smooth-handover</b>	<ul style="list-style-type: none"> <li>- <math>N_{Smth} = \max(0, R.D_{MIP6} - B)</math></li> <li>- <math>T_{Smth} = T_{CA} + x.D_{MIP6} + T_{AB} + T_{radio}</math></li> <li>- <math>J_{Smth} = D_{MIP6} + T_{AB} + J_{radio}</math></li> </ul>	$N_{Smth} < N_{HMIP}$ $T_{Smth} > T_{MIP6}$ $J_{Smth} > J_{MIP6}$
<b>Fast-handover</b>	<ul style="list-style-type: none"> <li>- <math>N_{Fast} &lt; R.D</math></li> <li>- <math>T_{Fast} = T_{CA} + T_{AB} + T_{radio}</math></li> <li>- <math>J_{Fast} = T_{AB} + J_{radio}</math></li> </ul>	$N_{Fast} < N_{MIP6}$ $T_{Fast} > T_{MIP6}$ $J_{Fast} \geq J_{MIP6}$
<b>BETH</b>	Similaire au <i>fast-handover</i>	

**Table 2.** Tableau récapitulatif des performances de *handover* basés sur IP

*Mobile IPv6* est une amélioration de *mobile IPv4* pour IPv6. Il profite des avantages d'IPv6 comme la configuration automatique des adresses. Dés lors, le temps de déconnexion du mobile est plus faible, et le nombre de paquets perdus est réduit proportionnellement. Il évite le routage triangulaire, ce qui diminue le délai de transfert des paquets. La gigue est identique à *mobile IPv4*.



La restructuration du réseau, proposé par *hierarchical mobile IP*, a le mérite d'améliorer les performances du *handover* lors d'un déplacement local du mobile. La charge des messages de signalisation nécessaire aux enregistrements des mobiles est réduite. Dans le cas général, le délai de la déconnexion est plus faible que pour *mobile IPv6*, et donc le nombre de perte est lui aussi réduit. De plus, la gigue est plus faible que pour *mobile IPv6*. Toutefois, l'utilisation successive des tunnels entre chaque agent de mobilité augmente sensiblement les délais de transfert des paquets.

Les mécanismes de stockage introduits dans le *smooth-handover* réduisent considérablement le risque de perte de paquets au détriment du délai de transfert et de la gigue. Il n'est donc pas adapté à la transmission de données ayant de fortes contraintes temps réel.

Le *fast-handover* réduit le délai de déconnexion au minimum. Les pertes sont donc plus faibles, voir inexistantes si le délai de reconnexion physique est prompt. Les délais de transfert sont plus longs que pour *mobile IPv6*, mais plus courts que pour le *smooth-handover*. BETH a les mêmes performances que le *fast-handover*. Cependant, il est capable de gérer très rapidement la mobilité des terminaux. Le *fast-handover*, comme toutes les autres techniques décrites précédemment, sont incapables de contrôler des mobiles se déplaçant trop rapidement.

Toutes les techniques de *handover* IP ont une influence sur le flux UDP. Il n'y a aucune isolation parfaite du flux.

### 3. Les effets du *handover* sur la couche TCP

TCP (Transmission Control Protocole) (Postel, 1981) (Stevens, 1994) et UDP (User Datagram Protocol) sont les protocoles de transport les plus utilisés sur IP. TCP fournit aux applications un service de transmission fiable des données. TCP est un protocole complexe qui dispose d'un contrôle de flux et de congestion, afin d'utiliser au mieux les ressources du réseau et des terminaux. Les nombreuses évolutions de TCP ont été conçues et optimisées pour un réseau filaire. La présence d'accès sans-fil peut perturber les performances de TCP. L'objectif de ce chapitre est de montrer l'influence du *handover* sur ces performances.

#### 3.1. Mécanismes généraux de TCP

Ce chapitre expose uniquement les mécanismes de base de TCP intégrés dans les systèmes d'exploitation actuels. Les autres mécanismes seront évoqués, et non détaillés.

TCP est un protocole de transport orienté connexion. Une connexion est une entité logique constituée de deux points d'accès applicatifs. Elle permet de transférer les paquets, de contrôler, et d'évaluer continuellement l'état du réseau entre ces

deux points. En fonction de ces évaluations, TCP ajuste le débit d'émission sur la connexion. Ce mécanisme complexe est le contrôle de congestion. Tant que TCP estime que le réseau n'est pas congestionné, le débit d'émission est augmenté. Dans le cas contraire, le débit est diminué. Plus TCP détectera des congestions, plus le débit moyen d'émission sera faible.

Dans un réseau filaire, le taux d'erreur bit est relativement faible. Ainsi, la perte d'un paquet révèle généralement la présence d'une congestion dans le réseau. TCP utilise ce principe pour détecter les congestions du réseau. S'il détecte la perte d'un ou de plusieurs paquets, il supposera que le réseau est en état de congestion.

Une boucle de contrôle permet de détecter les pertes de paquets. D'une part, tous les paquets TCP transmis sont numérotés séquentiellement. D'autre part, tous les paquets réceptionnés, et non erronés, doivent être acquittés. Le numéro de séquence est utilisé pour identifier les paquets et leur acquittement. TCP utilise deux méthodes pour détecter les pertes de paquet, et par extension les congestions.

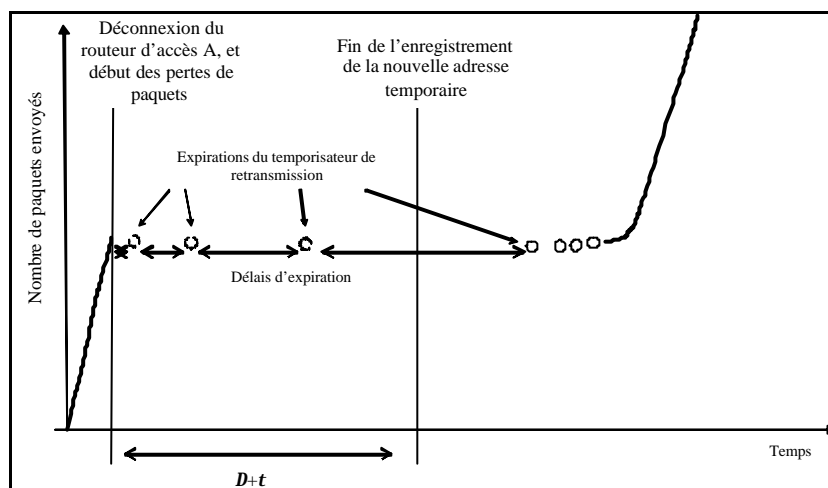
La première méthode consiste à utiliser un temporisateur de retransmission. Ce temporisateur est enclenché lors de l'émission d'un paquet TCP. S'il expire avant la réception de l'acquittement de ce paquet, TCP considèrera cet évènement comme une détection de perte. A ce moment précis, le débit de l'émetteur est réduit au minimum, et plusieurs paquets seront retransmis. Le délai d'expiration de ce temporisateur est fonction de l'estimation du délai aller-et-retour entre les deux points de la connexion. Une mauvaise estimation de ce délai, provoquera des retransmissions superflues, réduira inutilement le débit d'émission ou la réactivité de TCP (vitesse de convergence de l'estimation de l'état du réseau). Ce délai est doublé après chaque expiration du temporisateur.

La deuxième méthode de détection de perte, utilise le numéro de séquence des acquittements. Quand le destinataire reçoit un paquet TCP dont le numéro de séquence n'est pas correct (présence d'un trou de numérotation), il renvoie un acquittement du dernier paquet reçu. L'émetteur recevra donc plusieurs acquittements avec le même numéro de séquence. C'est ce que nous appelons des acquittements dupliqués. Dans ce cas, la vitesse d'augmentation du débit est diminuée. En d'autres termes, la prochaine augmentation du débit sera plus faible.

### **3.2. Influences de mobile IPv4 et mobile IPv6 sur TCP**

Comme nous l'avons précisé dans les chapitres précédents, le délai de la déconnexion du mobile pour *mobile IPv4* ou *mobile IPv6* est important. Pendant cette période, tous les paquets TCP et les acquittements envoyés ou provenant du mobile sont perdus. Ceci a deux conséquences directes sur les performances de TCP :

- Si le temporisateur de retransmission expire ou si l'émetteur reçoit plusieurs acquittements dupliqués, TCP conclut que le réseau est en état de congestion. Le débit d'émission sera réduit à tort.
- Une longue période de déconnexion implique plusieurs réductions successives du débit la connexion, et la diminution de la réactivité de TCP. Après la reconnexion du mobile, le débit d'émission autorisé sera très faible, et il augmentera très lentement alors que le réseau n'est absolument pas congestionné.
- Si tous les paquets transmis sont perdus (cette probabilité est d'autant plus forte que le débit d'émission est faible), l'émetteur ne pourra émettre de nouveau qu'au moment de l'expiration du temporisateur de retransmission. Si le délai de déconnexion entraîne plusieurs expirations, le délai du temporisateur sera très important (le délai est doublé après chaque expiration). Dès lors, le temporisateur risque d'expirer bien après la fin effective du *handover* IP (Figure 8) (Fladenmuller, 1999), et l'émetteur sera incapable de transmettre le moindre paquet pendant cette période.



**Figure 8.** Expirations du temporisateur de retransmission pendant le *handover*

### 3.3. Influence du *smooth-handover* sur TCP

L'objectif du *smooth-handover* est la réduction des pertes de paquets lors du *handover*. Si le débit d'émission de la connexion est bien dimensionné, il ne devrait pas y avoir de pertes, et les phénomènes décrits précédemment ne devraient pas apparaître.

Toutefois, le mécanisme de sauvegarde du *smooth-handover* peut abuser TCP. En effet, le mobile peut recevoir un paquet une première fois avant le *handover*, et

une deuxième fois après le *handover* quand le routeur A retransmet les paquets sauvegardés. Ainsi, le mobile recevra deux acquittements identiques. Pour TCP ce sont des acquittements dupliqués. TCP estimera à tort qu'il est en présence d'une congestion. L'algorithme du *fast recovery and fast retransmit* de TCP devrait résoudre ce problème (Stevens, 1994).

Enfin, le stockage des paquets augmente considérablement la gigue. Si cette gigue est supérieure au délai d'expiration du temporisateur de retransmission, le temporisateur expirera. Cet événement entraînera la retransmission inutile de plusieurs paquets, et réduira la disponibilité des ressources. Ceci correspond à une phase de dégradation des performances, et à la diminution du débit d'émission.

### 3.4. Influence du *fast-handover* et *BETH* sur TCP

Le *fast-handover* et *BETH* sont des techniques de *handover* qui peuvent subir des pertes. Toutefois, contrairement à *mobile IPv4* et *mobile IPv6*, le délai de déconnexion est très faible. Les phénomènes décrits pour *mobile IPv4* et *mobile IPv6* ne sont pas applicables. Certes, quelques pertes de paquets sont à considérer, mais il n'y aura pas d'expiration successive du temporisateur de retransmission. La détection de perte par la réception d'acquiescement dupliqué s'effectuera avant l'expiration du temporisateur.

La dégradation du *handover* sera limitée. D'après (Hartenstein, 2001), la dégradation (augmentation du débit nécessaire à la transmission des paquets de données) de TCP est de 8% pour le *fast-handover*, alors qu'il est de l'ordre de 17% pour *mobile IPv6*.

### 3.5. Analyse générale de l'influence des *handover* sur TCP

Le *handover* pour *mobile IPv4* ou *mobile IPv6* est susceptible d'engendrer des expirations successives du temporisateur de retransmission. Ceci augmente de manière excessive le délai d'expiration du temporisateur et peut empêcher la transmission des paquets sur la connexion. Le *fast-handover* dégrade les performances de TCP d'environ 8%. Enfin, l'introduction de mécanismes de stockage permet d'éviter les pertes pour le *smooth-handover*, mais engendre une gigue importante. Cette gigue entraîne la détection erronée de perte de paquets, et la réduction des performances de TCP.

En conclusion, toutes les techniques de *handover* décrites précédemment dégradent les performances de TCP. Si nous ajoutons les problèmes liés au manque de fiabilité des liaisons sans-fil, l'efficacité du protocole TCP doit être remise en cause. Une mutation profonde de TCP ou la définition d'une autre technique de *handover* est nécessaire, afin de disposer d'un service plus fiable sur Internet.

#### 4. *Soft-handover*

Dans les chapitres précédents, nous avons confirmé l'impossibilité d'isoler un flux UDP ou TCP lors d'un *handover* classique. Ceci nous incite à définir une nouvelle technique permettant de résoudre le problème de dégradation des performances pour un flux TCP ou UDP.

Le *soft-handover* est une technique qui permet au mobile de se déplacer d'un routeur d'accès à un autre routeur d'accès sans déconnexion. Ainsi, le mobile a toujours une connectivité de bonne qualité avec le réseau de cœur : les pertes de paquets induites par le *handover* sont inexistantes, et la gigue induite par la dégradation du signal radio est minime. Le *soft-handover* est réalisable, si le mobile est capable de communiquer simultanément avec plusieurs routeurs d'accès : soit le mobile dispose de plusieurs interfaces sans-fil (homogène ou hétérogène), soit la technologie d'accès permet la connexion du mobile vers plusieurs routeurs d'accès (802.11 en mode ad-hoc (ieee, 1999), ou WCDMA (Sanchez, 2001)).

Dans les chapitres suivants, nous allons brièvement présenter la technique de *soft-handover* défini dans (Zhang, 2001), puis nous détaillerons une autre proposition de *soft-handover* initiée à Eurécom.

##### 4.2. Les propositions de Zhang et al

Tao Zhang et al. ont identifié plusieurs éléments clés pour la conception d'un système efficace de *soft-handover* basé sur le protocole IP (Zhang et al., 2001). Premièrement, un flux IP entre un correspondant et un mobile doit être dupliqué. Ces flux dupliqués doivent traverser des routeurs d'accès distincts. Deuxièmement, les flux dupliqués doivent être synchronisés pour pouvoir recombinaison le flux d'origine.

Pour établir ces mécanismes, un mobile possède une adresse MAC unique appelée *shadow address*. Le mobile utilise une unique adresse IP pour l'ensemble des flux dupliqués. Lors de l'établissement de la connexion avec un nouveau routeur d'accès, le mobile doit insérer sa *shadow address* dans une table de correspondance du routeur d'accès. Cette table contient la liste de tous les mobiles connectés au routeur. Si un correspondant décide d'envoyer un paquet à un mobile, il doit d'abord déterminer le *shadow address* du mobile, ainsi que l'ensemble des routeurs qui ont cette adresse dans leur table de correspondance. Finalement, plusieurs copies des paquets sont envoyées à ces routeurs. La duplication des flux est effectuée par une entité du réseau de cœur.

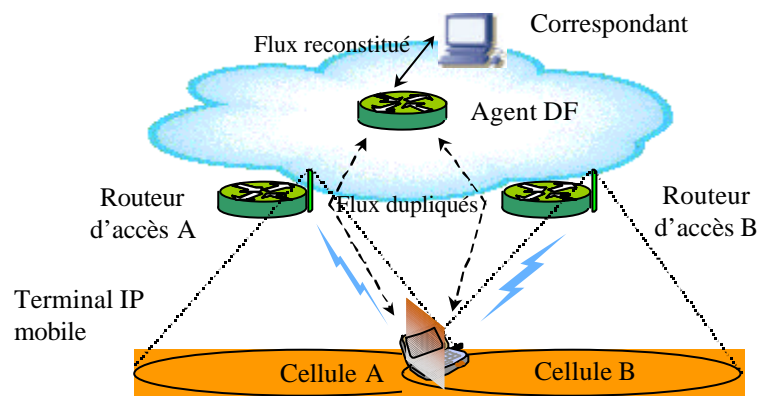
Pour fusionner ces copies, il est primordial que ces derniers arrivent aux mobiles en même temps. Il est donc nécessaire de définir un mécanisme de synchronisation au niveau physique entre tous les routeurs d'accès. Les auteurs de cette méthode n'ont pas défini précisément les différents mécanismes de duplication et de

synchronisation nécessaire. La réalisation de mécanismes de synchronisation physique est très complexe. De plus, elle limite le potentiel du *soft-handover*. Cette technique de *soft-handover* est totalement dépendante de la couche physique.

#### 4.3. *Soft-handover* d'Eurécom

Dans ce chapitre, nous allons décrire le *soft-handover* (Moret, 2002) initiée à Eurécom et basée sur le protocole IPv6. Le principe de base consiste à dupliquer et reconstituer un flux en utilisant les fonctionnalités du protocole IPv6.

Le *soft-handover* nécessite l'intégration d'un agent capable de dupliquer, et de reconstituer un flux IP. Nous le nommerons agent DF (Duplication et Fusion). La description des processus de bases suivant permettra d'exposer les principes du *soft-handover* : processus d'enregistrement, de duplication, de fusion et d'*handover*.



**Figure 9.** Duplication et reconstitution d'un flux par le *soft-handover*

##### 4.3.1. Processus d'enregistrement

La Figure 9 présente le schéma de base pour le *soft-handover*. Le mobile est connecté au routeurs d'accès A et B. Il possède une adresse temporaire locale pour chacune des cellules. Ces adresses sont obtenues par le système classique de configuration automatique des adresses IPv6. Ces adresses sont identifiées par un numéro local du mobile (par exemple un numéro d'interface).

Afin de disposer des services de *soft-handover* de l'agent DF, le mobile s'enregistre auprès de cet agent. L'adresse de l'agent peut être définie explicitement par les routeurs d'accès durant la configuration automatique des adresses, ou implicitement par l'intermédiaire d'une adresse *anycast*. Le mobile transmet à

l'agent un message de sollicitation contenant les deux adresses temporaires locales, les numéros des interfaces associées, et son adresse de référence. Si l'agent accepte de servir le mobile, il lui affecte une adresse temporaire principale. Il lui transmet un message de confirmation contenant l'adresse principale. Le mobile et l'agent DF insèrent l'adresse principale ainsi que les adresses locales correspondantes dans une table de liaison spécifique au *soft-handover* (table DF).

Si une adresse locale du mobile est modifiée, le mobile sollicite l'agent en lui transmettant la nouvelle adresse temporaire locale, son numéro d'interface, ainsi que l'adresse principale qui lui a été précédemment affectée. L'agent remplacera l'ancienne adresse temporaire par la nouvelle.

Si le mobile dispose d'une nouvelle liaison, le mobile sollicite l'agent en lui transmettant la nouvelle adresse temporaire locale, son numéro d'interface (par exemple 3, puisque c'est la troisième interface) et l'adresse principale. L'agent ajoutera cette nouvelle interface et adresse dans la table.

Si le mobile veut disposer du service de *soft-handover* avec un correspondant spécifique, il enregistre son adresse principal auprès de ce correspondant. S'il veut bénéficier du service de base de *mobile IPv6*, il enregistrera une adresse locale. Les deux techniques peuvent parfaitement coexister.

#### 4.3.2. *Le processus de duplication*

L'agent DF intercepte les paquets destinés au mobile (l'adresse de destination du paquet est l'adresse principale répertoriée dans la table DF). Les paquets sont ensuite dupliqués. Le premier paquet est encapsulé dans un paquet IPv6 dont l'adresse de destination est la première adresse locale associée à l'adresse principale. Le paquet est en fait transmis dans un tunnel IPv6 dont les extrémités sont l'agent DF et le mobile. Le tunnel traverse le routeur A. Le deuxième paquet est encapsulé dans un paquet IPv6 dont l'adresse de destination est la deuxième adresse locale associée à l'adresse principale (le tunnel traverse le routeur B), etc... Par cette méthode, les paquets dupliqués arriveront au mobile en utilisant les différents routeurs d'accès auxquels est lié le mobile.

Les paquets dupliqués contiennent une extension IPv6 de destination. Cette extension n'est traitée que par le destinataire du paquet (en l'occurrence l'extrémité du tunnel). Elle contient un numéro d'identification. Tous les paquets provenant d'une même copie sont encapsulés dans des paquets ayant le même numéro d'identification. Le numéro d'identification est incrémenté à chaque transmission.

Inversement, le mobile est capable de dupliquer les paquets et de les transmettre à l'agent DF par l'intermédiaires des différents routeurs d'accès (les tunnels sont inversés).

#### 4.3.3. *Le processus de fusion*

L'agent DF intercepte tous les paquets provenant des tunnels de duplication. Si le paquet reçu est associé à une extension de destination identifiant le paquet d'origine, le paquet est analysé. L'adresse source du paquet permet de retrouver l'entrée dans la table DF. Cette entrée contient la liste des numéros des paquets manquants. Si le numéro identifie un paquet déjà transmis, il est détruit par l'agent. Dans le cas contraire le paquet est transmis à son destinataire. La liste est mise à jour si nécessaire (voir (moret, 2002) pour une description plus détaillée).

Inversement, le mobile est capable de traiter les flux dupliqués provenant de l'agent DF.

Ce processus de fusion permet de rétablir le flux d'origine. La réception de paquets dupliqués est impossible.

#### 4.3.4. *Le processus de handover*

Pour la description du processus de *handover*, nous supposons que le mobile est connecté uniquement au routeur A, qu'il dispose de son adresse temporaire locale associée, et qu'il est enregistré auprès d'un agent DF.

Quand le mobile se connecte au routeur d'accès B, il obtient sa nouvelle adresse temporaire locale par le mécanisme de configuration automatique d'IPv6. Il l'enregistre auprès de son agent DF. Les processus de duplication et de fusion, qui sont décrits dans les sections précédentes, rentrent alors en fonction.

Le mobile peut décider à tout moment de libérer la connexion avec le routeur d'accès A. Cette décision ne doit pas être trop rapide : si le mobile oscille entre les deux routeurs d'accès, le mobile devra à plusieurs reprises contacter l'agent (effet ping-pong). La duplication des flux permet de réguler l'effet ping-pong. Cet effet n'est pas traité par les autres techniques d'*handover* IP.

La libération de la connexion est notifiée à l'agent DF. Dès lors, le mobile ne disposera plus que d'une liaison avec le réseau. Le mobile aura effectué un *handover* sans déconnexion au réseau filaire. L'ensemble des correspondants et l'agent mère n'ont pas été sollicités.

#### 4.3.5. *Analyse Théorique du handover*

La Figure 10 présente le diagramme temporel du *handover* décrit au chapitre 4.3.4. Le délai de transfert après le *handover* est le suivant

$$T_{soft} = T_{DFC} + T_{DFB} + T_{radio}$$

avec  $T_{DFB}$  le délai de transfert entre l'agent DF et le routeur d'accès B, et  $T_{DFC}$  le délai entre le correspondant et l'agent DF. Ce délai est supérieur à celui de *mobile IPv6*.

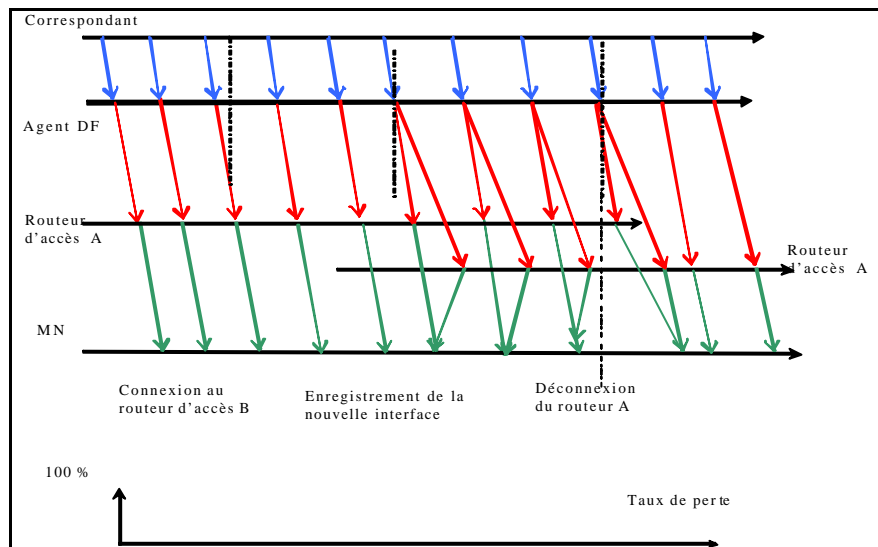


La gigue induite par le *handover* est :

$$J_{soft} = |T_{DFB} - T_{DFA}| + J_{radiosoft} \text{ avec } J_{radiosoft} \approx \min(J_{radioA}, J_{radioB}),$$

et  $T_{DFA}$  le délai de transfert entre l'agent DF et le routeur d'accès A.  $J_{radioA}$  est la gigue de transmission depuis le routeurs d'accès A et  $J_{radioB}$  depuis le routeur B. La gigue  $J_{radiosoft}$  est inférieure à  $J_{radio}$ , car il y a toujours une des liaisons avec une qualité de réception correcte et donc avec un nombre de retransmissions réduit. La proximité de l'agent DF et des routeurs d'accès influe sur la gigue et le délai de transfert. La position de l'agent DF est donc importante. Durant le déplacement du mobile, il sera nécessaire de changer d'agent. (Moret, 2002) décrit une méthode de changement d'agent qui ne perturbe pas les communications préalablement établies. L'agent DF agit comme un agent de mobilité du système *hierarchical mobile IP*. Le mobile n'ayant subi aucune déconnexion, il n'y a aucune perte et nous obtenons :

$$N_{soft} = 0$$



**Figure 10.** Diagramme temporel pour le *soft-handover*

Si nous considérons les taux d'erreur des paquets entre le mobile et les routeurs d'accès, le taux d'erreur bit durant la le *handover* est :

$$P_{soft} = AP.BP$$

avec  $AP$  le taux d'erreur bit de la connexion avec le routeur A, et  $BP$  le taux d'erreur bit de la connexion avec le routeur B. Durant le *handover*, le taux d'erreur bit obtenu est optimal. De même, durant le *handover*, le délai de transfert est :

$$T_{soft} = T_{DFC} + \min(T_{DFB}, T_{DFA}) + T_{radiosoft}$$

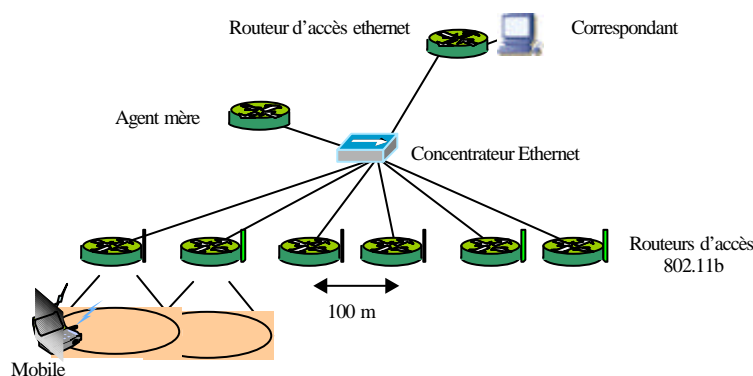
avec  $T_{radiosoft}$  le délai de transmission sur l'interface radio. Pour les mêmes raisons évoquées pour la gigue, ce délai est inférieur à  $T_{radio}$ . La redondance des liaisons réduit fortement le taux d'erreur bit, et diminue les délais de transfert. Ces deux points sont très importants. En effet, c'est une justification supplémentaire pour l'usage de la duplication des flux.

Cette technique de *handover* évite les pertes de paquet dues aux déconnexions, réduit le taux de pertes, bénéficie d'une gigue faible, et élimine tous risques de duplication de paquets. De plus, si l'agent DF est proche des routeurs d'accès le délai de transfert est minimisé. Ainsi, les dégradations apportées aux performances de TCP sont relativement faibles.

La contrepartie de cette technique est l'augmentation des ressources nécessaires au support des flux. La duplication des liaisons nécessite l'établissement de tunnels et nécessite un débit deux fois plus important par rapport aux autres techniques. Le *soft-handover* est donc plutôt réservée aux flux qui nécessitent une bonne qualité de service de transmission. Les autres flux peuvent utilisés conjointement *mobile IPv6*.

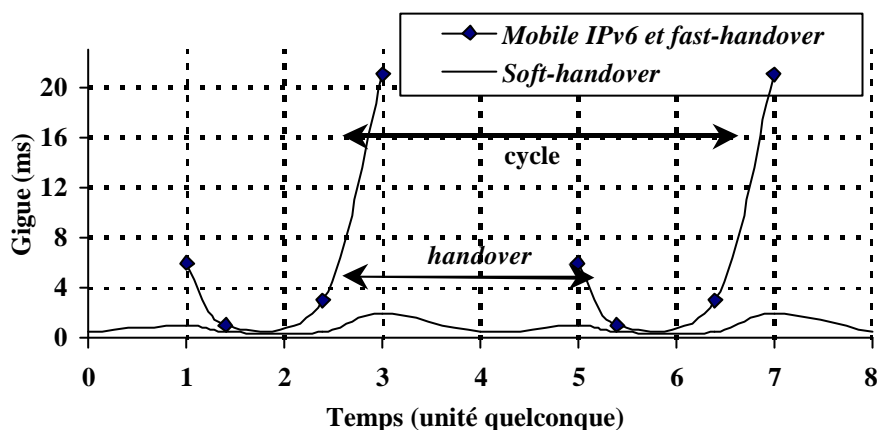
## 5. Résultats de simulations

Dans ce chapitre, nous allons présenter quelques résultats numériques concernant les protocoles *mobile IPv6*, *fast-handover* et *soft-handover*. Ces résultats ont été obtenus à l'aide d'un nouveau simulateur de réseau à événement discret nommé Gémini.



**Figure 11.** Topologie du réseau utilisée pour les simulations

Les résultats proviennent du réseau dont la topologie est exposée en Figure 11. Ce réseau est constitué d'un terminal mobile utilisant une interface 802.11b (11 Mb/s) pour accéder au cœur du réseau, et de routeurs d'accès munis d'une interface 802.11b. Il est rappelé que la technologie d'accès radio 802.11 permet la retransmission de paquets perdus. La probabilité d'erreur de transmission sur l'interface radio est fonction de la distance entre le mobile et le routeur d'accès 802.11b : 0% d'erreur entre 0 et 50 mètres, augmentation linéaire des erreurs de 50 à 400 mètres, et 100% d'erreur au delà de 400 mètres. Les routeurs d'accès 802.11 sont alignés et espacés de 100 mètres. Le mobile suit une trajectoire parallèle à l'alignement des routeurs d'accès 802.11b avec une vitesse constante. Un flux UDP de débit  $R=500\text{kb/s}$  est établi entre le terminal mobile et un correspondant. Les délais de transfert entre les routeurs d'accès 802.11b et le correspondant sont d'environ 50ms ( $T_{CA}=T_{CB}=50\text{ms}$ ). Le délai de transfert  $T_{AB}$  entre A et B est proche de 0ms. Nous avons effectué des simulations avec des vitesses de mobile variant de 1 à 10m/s (vitesse d'un homme entre la marche et le pas de course). Les différents tests que nous avons effectués indiquent que la vitesse du mobile a peu d'influence sur les résultats.



**Figure 12.** Variation de la gigue pendant un cycle

La **Figure 12** présente la variation de la gigue  $J$  pendant un cycle (un cycle est délimité par deux *handover*). Concernant *mobile IPv6* et le *fast-handover*, les variations de gigue sont similaires. Au début du *handover*, la gigue augmente considérablement jusqu'à atteindre 21ms. Après le *handover*, la gigue débute à environ 6ms et décroît rapidement. Ces variations importantes sont liées aux retransmissions provoquées par une mauvaise qualité de réception au début et à la fin du *handover*. Au milieu du *handover* tous les paquets sont perdus. La gigue induite par la topologie du réseau est négligeable ( $T_{CA}=T_{CB}$  et  $T_{AB}=0$ ). La figure présente donc la variation de la gigue  $J_{radio}$ . Pour le *soft-handover*, cette variation est plus faible et est proche de 2ms. En fait, sur les deux liaisons radio, il y en a toujours

une avec une qualité de réception correcte. Les retransmissions sont donc des événements plus rares.

La Figure 13 présente la variation du délai de transfert  $T$  durant un cycle. Comme pour la gigue, les variations du délai pour *mobile IPv6* et le *fast-handover* sont très similaires. Au début du *handover*, le délai augmente considérablement jusqu'à atteindre 180ms. Après le *handover*, le délai est stable et égal à 120ms. Pour le *soft-handover*, cette variation est plus faible et est proche de 120ms. Les phénomènes de retransmissions énoncés précédemment pour la gigue justifient le comportement de ce délai de transfert.

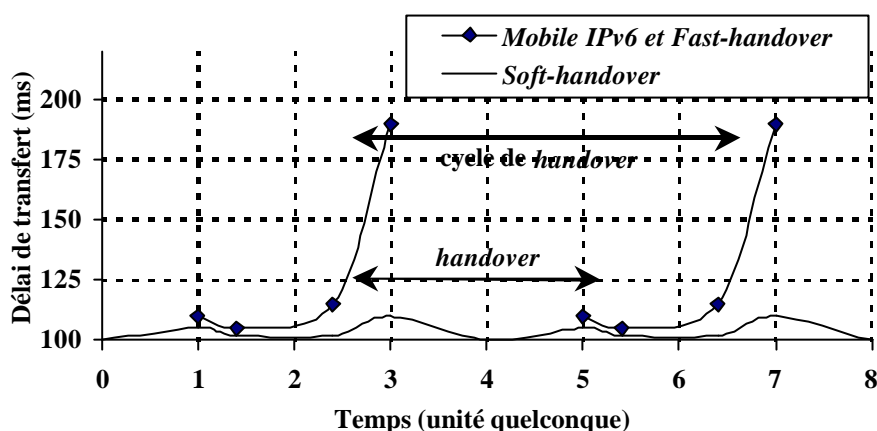


Figure 13. Variation du délai de transfert pendant un cycle

Les mesures de pertes  $N$  de paquet montrent que *mobile IPv6* a la plus mauvaise performance avec 59kb par *handover*. *fast-handover* a des performances moyennes avec une perte de 19kb par *handover*. Enfin, le *soft-handover* a une performance optimale avec une perte proche de 0. Il suffit de diviser ces chiffres par  $R$  pour estimer les délais  $D$  de déconnexion.

Tous les résultats numériques correspondent aux analyses théoriques.

## 6. Conclusion

*Mobile IPv4* a été la première solution de gestion de mobilité dans le monde IP. Les performances du *handover* sont faibles sur le plan de taux de pertes de paquets. Ces contre-performances sur le plan IP se répercutent sur la couche TCP. Elles engendrent un déclenchement inutile de mécanismes de contrôle de congestion et causent une dégradation sensible du débit des connexions TCP. L'introduction d'IPv6 et de *mobile IPv6* a apporté une amélioration à ces mécanismes. IPv6 propose un plus large espace d'adresses pour les mobiles, et introduit un mécanisme

de configuration automatique des adresses plus rapide. *Mobile IPv6* offre une solution pour éviter le routage triangulaire et réduit d'autant le délai de transfert.

*Hierarchical mobile IP* propose de hiérarchiser la gestion de la mobilité. Ceci permet de diminuer les échanges de message de signalisation circulant dans le réseau, et de réduire les pertes. Le *smooth handover* introduit un mécanisme de sauvegarde, afin de minimiser les pertes de paquets. Cependant, ceci ne suffit pas pour garantir l'absence de dégradation de TCP. De plus, la gigue importante ne permet pas le support de flux temps-réels.

Des solutions plus adaptées aux applications sensibles aux délais de transfert comme le *fast-handover* et BETH ont été introduites. Le premier anticipe l'enregistrement du mobile dans son nouveau réseau et le deuxième réduit l'échange de messages de signalisation IP lors du *handover*. Ceci a pour conséquence de réduire la durée globale de l'indisponibilité du mobile et les pertes de paquets. Ces approches diminuent les dégradations des performances de TCP.

Nous avons présenté une technique de *soft-handover* basée sur IPv6 et l'utilisation de flux redondants. Cette solution ne nécessite pas de modification de *mobile IPv6*. Les pertes induites par le *handover* sont très faibles ou inexistantes. Si le protocole d'accès autorise les retransmissions tel que 802.11, la gigue et le délai de transfert sont fortement diminués en comparaison des autres techniques. Les dégradations des performances sur TCP sont minimales. De plus, elle réduit le taux d'erreurs des liaisons sans-fil et l'effet ping-pong est contrôlé. Toutefois, cette technique est gourmande en ressource radio puisqu'elle nécessite un débit de transmission au moins deux fois supérieurs à celui des techniques précédentes. Le *soft-handover* est réservé à des applications sensibles aux moindres perturbations.

Dans un premier temps, afin d'établir les limites d'utilisation du *soft-handover*, nous allons utiliser le simulateur Gemini pour tester le *soft-handover* dans des conditions extrêmes d'utilisation d'un réseau (engorgement des routeurs d'accès radio, des agents DF, forte mobilité, etc...). Nous devons aussi étudier des algorithmes de répartition des charge des agents DF.

Dans un deuxième temps, nous allons intégrer le *soft-handover* dans la pile de protocole IPv6 de Linux. Ceci nous permettra de tester les capacités du *soft-handover* dans des conditions réelles. Nous disposons de routeurs d'accès composés d'interfaces radio 802.11b, 802.11g et UMTS-TDD (l'interface UMTS-TDD est développée au sein d'Eurécom). L'UMTS donne une dimension supplémentaire au *soft-handover*: cette technologie permet de contrôler l'accès en fonction des priorités des flux, ce que 802.11 ne permet pas. A terme, nous voulons démontrer que le *soft-handover* permet à un mobile de se connecter à un réseau ethernet, puis à un réseau 802.11 et enfin à un réseau UMTS sans dégradation notable des communications du mobile.

## 7. Bibliographie

- Belghoul F., Moret Y. et Bonnet C., Performance comparison and analysis on MIPv6, Fast MIPv6 Bi-casting and Eurecom IPv6 soft-handover over IEEE802.11b WLANs, VTC 2004, 59<sup>th</sup> IEEE vehicular Technology Conference, Milan, Italie, mai 2004.
- Campbell AT., Gomez J., IP Micro-Mobility Protocols, *ACM SIGMOBILE* vol.4,no.4, pp 45-54, octobre 2001.
- Castellucia C., A hierarchical Mobile Ipv6 Proposal, *4th CTS Mobile Communication Summit*, juin 1999.
- Eom DS., Sugano M., Murata M., Miyahara H. Performance Improvement by Packet Buffering in Mobile IP Based Networks, *IEICE Transactions on Communications*, vol. E83-B, pp. 2501-2512, novembre 2000.
- Fladenmuller A., De Silva R., The effect of Mobile IP handoffs on the performance of TCP, *ACM Mobile Networks and Applications*, 1999.
- Gustafsson E., Jonsson A., Perkins C., Mobile IP Regional Registration, IETF, draft-ietf-mobileip-reg-tunnel-04.txt, mars 2001
- Hartenstein H., Jonas K., Liebsch M., Schmitz R., Stiemerling M., Westhoff D., Performance of TCP in the Presence of Mobile IP Handoffs, *ICT 2001, IEEE International Conference on Telecom*, Bucharest, Roumanie, juin 2001.
- Johnson D., Perkins C., IETF Internet Draft "Mobility Support in IPv6", draft-ietf-mobileip-ipv6-12.txt. April 2000
- Johnson D., Perkins C. Optimization in Mobile IP, IETF, Draft-ietf-mobileip-optim-11.txt, September 2001.
- Kempf J., Bi-directional Edge Tunnel Handover for IPv6, IETF, draft-kempf-beth-ipv6-02.txt, mars 2001.
- Koodli R., Perkins C., A Framework for Smooth Handovers with Mobile IPv6, IETF, draft-koodli-mobileip-smoothv6-00.txt, juillet 2000.
- Koodli R., Perkins c., Fast Handovers in Mobile IPv6, IETF, draft-koodli-mobileip-fastv6-06.txt, 2002.
- Mathis M., Mahdavi J., Floyd S., Rmanow Q., TCP Selective Acknowledgement Option, IETF, RFC 2018, octobre 1996.
- Moret Y., Bonnet C., Gauthier L., Knopp R., Process and Apparatus for Improved Communication between a Mobile Node and a Communication Network, Office Européen des Brevets, n° 02368057.2, août 2002.
- Perkins C., IP encapsulation within IP, IETF, RFC 2003, 1996.
- Perkins C., Wang KY., Optimized Smooth Handoffs in Mobile IP, *Proceedings of the fourth IEEE Symposium on Computers & Communications*, juillet 1999.
- Perkins C., IP mobility support for IPv4, IETF, RFC 3220, janvier 2002.
- Postel J., Transmission Control Protocol, IETF, RFC 793, 1981.

- Soliman H., Castellucia C., El Malki K., Bellier L., Hierarchical Mobile IPv6 and Fast Handoffs, IETF, draft-ietf-mobileip-hmipv6-00.txt, septembre 2000.
- Stevens WR., *TCP/IP Illustrated Volume 1: The Protocols*, Addison-Wesley, Longman, Reading,Massachusetts, 1994.
- Zhang T., Chen JC., Agrawal P., Distributed soft handoff in all-IP wireless networks, *Proceedings of IEEE International Conference on Third Generation Wireless and Beyond (3Gwireless'01)*, San Francisco, CA, pp. 460-465, mai 2001.
- IEEE standard, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 1999.
- Sanchez J., Mamadou T. *UMTS, services, architecture et WCDMA*, ed. Hermes, 2001.
- Belghoul F., Moret Y.,Bonnet C., Eurecom Soft Handover, *ICWN 2003, International Conference on Wireless Networks*, LasVegas 2003.