Les Réseaux Mobiles dans IPv6

Thierry Ernst, MOTOROLA LABS Paris et INRIA Rhône-Alpes
Claude Castelluccia, INRIA Rhône-Alpes
Hong-Yon Lach, MOTOROLA LABS Paris

DNAC'99 (De Nouvelles Architectures pour les Communications)
Paris 1-3 décembre 1999
thierry.ernst@inrialpes.fr
http://www.inrialpes.fr/planete/people/ernst/Welcome.html

Résumé

Ce papier traite du routage de paquets de données vers les noeuds localisés dans un réseau IP mobile. Un réseau mobile est un réseau qui change dynamiquement son point d'attachement dans la topologie Internet. Les applications sont les réseaux embarqués dans un avion, un train ou une voiture. Les protocoles définis par l'IETF pour le support de noeuds mobiles ne permettent pas de supporter les réseaux mobiles efficacement. Nous montrons en particulier que Mobile-IPv6 n'est pas dimensionné pour le support de réseaux mobiles de grande taille et qu'il introduit des problèmes d'authentification.

1 Introduction

La mobilité des noeuds dans IPv4 et IPv6 [2] est gérée par Mobile-IP (protocoles Mobile-IPv4 [8], Mobile-IPv4 avec optimisation de routage [6] et Mobile-IPv6 [3]). L'objectif de ces protocoles est de permettre aux noeuds mobiles de conserver une connectivité permanente à l'Internet sans rupture des connections en cours lors de leurs déplacements tout en routant les paquets de données de manière la plus optimale possible. Par contre, ces protocoles ne permettent pas la mobilité d'un réseau comme nous allons le démontrer dans ce papier.

Nous appelons *réseau* un ensemble de noeuds (machines ou routeurs) qui partagent le même préfixe IP et qui est attachée à l'Internet via un seul routeur externe (Border Router). Nous appelons *réseau mobile* un réseau dont le routeur externe change dynamiquement son point d'attachement à l'Internet et donc le chemin par lequel il est joignable dans la topologie Internet. Ceci est à ne pas confondre avec les réseaux *ad-hoc* qui sont des réseaux dont l'ensemble des noeuds sont des routeurs mobiles.

Les applications possibles des *réseaux mobiles* incluent entre autres les réseaux de capteurs déployés dans les avions, les trains, les bateaux ou les voitures, ou encore les réseaux personnels (Personal Area Networks) constitués par un ensemble d'interfaces de petite taille (téléphones cellulaires, agendas électroniques, ...). Un exemple plus démonstratif est celui d'un avion dans lequel la compagnie aérienne offre à ses passagers une connectivité permanente à l'Internet. Ceci permet aux passagers d'utiliser leurs ordinateurs portables, de se connecter sur un site distant, télécharger de la musique et de la vidéo depuis n'importe quel fournisseur de service, et de surfer sur la toile sans interruption de service au cours des déplacements de l'avion. Outre l'utilisation de l'Internet par les passagers, l'Internet peut aussi être utilisé pour échanger les données destinées à la navigation entre l'avion et les tours de contrôle aérien. Ce scénario a d'ailleurs fait l'objet de recherches de la part d'Eurocontrol (une organisation européenne pour la sécurité de la navigation aérienne) [9]. Durant son vol, l'avion change son point d'attachement à l'Internet et est joignable via des adresses IP distinctes qui peuvent appartenir à différents fournisseurs de service. Un tel scénario justifie qu'un *réseau mobile* puisse être de taille relativement grande (de l'ordre de plusieurs centaines de machines inter-connectées par plusieurs routeurs) et qu'il puisse s'attacher à l'Internet via des points très éloignés dans la topologie. De plus, un tel exemple montre que

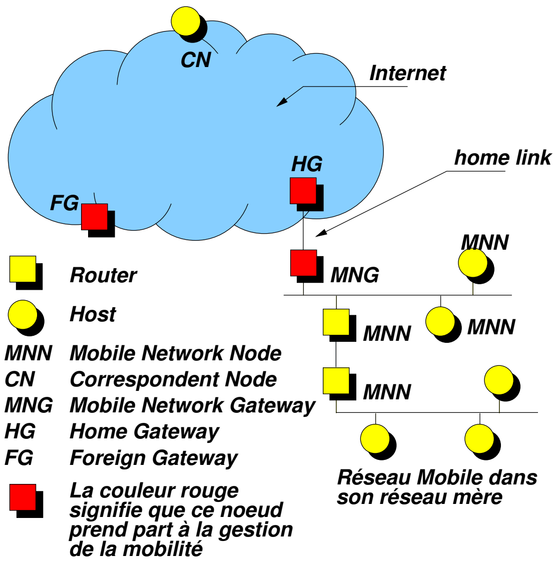

Figure 1: Terminologie pour les Réseaux Mobiles

nous devons faire face à deux niveaux de mobilité, celle du réseau lui-même, et celle des machines à l'intérieur du réseau, puisque les ordinateurs portables sont des mobiles visitant le *réseau mobile*.

Bien que les concepteurs de Mobile-IP prétendent que Mobile-IP peut gérer la mobilité des réseaux de la même manière que la mobilité des noeuds, il n'est pas possible de router les paquets de données de manière optimale depuis les noeuds externes au *réseau mobile* vers ceux *réseau mobile*, à moins que des changements importants ne soient apportés aux spécifications, en particulier dans Mobile-IPv6.

Ce papier est structuré de la manière suivante: dans la section 2, nous précisons la terminologie relative aux *réseaux mobiles* et nous donnons leurs caractéristiques essentielles ainsi que les contraintes à respecter pour fournir une gestion optimale de leur mobilité. La section 3 présente les protocoles gérant la mobilité des *noeuds* dans IPv4 et IPv6 respectivement. La section 4 montre comment les *réseaux mobiles* pourraient être supportés à l'aide de Mobile-IP. La section suivante explique ensuite pourquoi les spécifications actuelles de Mobile-IP ne permettent pas de gérer les *réseaux mobiles* de manière optimale sans de nombreuses modifications.

2 Terminologie et caractéristiques des réseaux mobiles

Dans le cadre de cette étude, nous avons défini la terminologie suivante: le routeur interne au *réseau mobile* par lequel celui-ci s'attache à l'Internet est appelé le *MNG* (Mobile Network Gateway). Le point d'attachement initial dans le réseau mère est appelé le *HG* (Home Gateway) et les points d'attachement suivants successifs sont appelés les *FGs* (Foreign Gateways). Nous appelons *MNN* (Mobile Network Node) toute machine ou routeur faisant partie du *réseau mobile*, et *CN* (Correspondant Node) tout noeud externe au *réseau mobile* communiquant avec un ou plusieurs *MNNs*. Ceci est illustré sur la figure 1. Un *réseau mobile* est donc un réseau dont le *MNG* s'attache à plusieurs *FGs* successifs au cours de ses déplacements.

Afin de débattre du cas le plus simple possible, nous faisons la supposition que le *réseau mobile* ne s'attache qu'à un seul *FG* à la fois, et qu'il n'a qu'un seul *MNG*. D'autre part, seul le trafic destiné à un *noeud du réseau mobile* transite par le *MNG*. Nous ne traitons donc pas le cas des réseaux de transit. Nous ne traitons pas non plus le cas où le *HG* ou le *FG* sont eux-mêmes mobiles.

La terminologie et le contexte de travail étant établis, nous remarquons que les réseaux mobiles ont certaines caractéristiques particulières:

- La structure interne d'un *réseau mobile* est préservée lors de ses déplacements. Ceci signifie que les noeuds composant le *réseau mobile* ne bougent pas l'un par rapport à l'autre bien qu'ils bougent par rapport aux noeuds externes au *réseau mobile*. Les *noeuds du réseau mobile* sont donc fixes par rapport au *MNG* mais apparaissent mobiles par rapport aux *CNs*.
- Tous les paquets transmis entre *MNNs* et *CNs* transitent nécessairement par le *MNG*. Ils transitent également soit par le *FG* courant ou soit par le *HG*.
- Les *réseaux mobiles* étant susceptibles d'embarquer un nombre important de *noeuds du réseau mobile* (de l'ordre de plusieurs centaines), chacun communiquant avec un certain nombre de *noeuds correspondants*, le nombre de *noeuds correspon-*

dants croît linéairement avec la taille du *réseau mobile* et devient un paramètre significativement important. Ceci nous permet de faire une comparaison avec la gestion de la mobilité pour les *noeuds mobiles* où le paramètre important était le nombre de *noeuds mobiles* et non pas celui des *noeuds correspondants*.

- Au vu du nombre de *noeuds correspondants* de l'ordre de plusieurs fois celui des *noeuds du réseau mobile*, un grand nombre de communications peuvent avoir lieu simultanément, toutes transitant via le *MNG*. Ainsi, la quantité de trafic induit par ou vers un *réseau mobile* est significativement importante d'autant plus que le réseau est grand. Dans un tel contexte, la question de l'optimisation du routage devient cruciale.
- Du point de vue des protocoles de routage, la distinction entre les *noeuds du réseau mobile* n'est nécessaire que pour le routage à l'intérieur du *réseau mobile*. Un *réseau mobile* peut donc être virtuellement perçu par les noeuds externes au *réseau mobile* comme un seul noeud, le *MNG*, avec une seule adresse IP et n interfaces qui lui seraient attachées. Autrement dit, l'emplacement d'un *noeud du réseau mobile* dans la topologie Internet étant dépendante de celui de l'emplacement du *MNG*, la connaissance de l'emplacement du *MNG* permet de router les paquets vers le *noeud du réseau mobile*.

Au vu de ces caractéristiques, nous pouvons établir que la gestion de la mobilité des *réseaux mobiles* doit faire face à un certain nombre de contraintes. Tout d'abord, il convient de supporter les *réseaux mobiles* en nombre et en taille importantes. Le nombre important de correspondants nous impose de minimiser la quantité de messages de contrôle relatifs à la gestion de la mobilité tout en optimisant le routage. Ces messages doivent être échangés en toute sécurité et authentifiés par leurs destinataires pour s'assurer qu'ils ne sont pas envoyés par un usurpateur. D'autre part, il est souhaitable que la gestion de la mobilité du *réseau mobile* se fasse de manière transparente du point de vue des *noeuds du réseau mobile* puisque ceux-ci ne bougent pas réellement. De la même manière, il est préférable que des noeuds mobiles puissent visiter le réseau mobile de manière tout aussi transparente en leur permettant d'utiliser les mécanismes actuels de gestion de la mobilité.

3 Mobile-IP

Mobile-IP est un protocole standardisé par l'IETF (Internet Engineering Task Force) au sein du groupe de travail du même nom. Il permet la mobilité des noeuds dans Internet sans interruption de la connectivité. La mobilité des noeuds est gérée en allouant deux adresses IP distinctes à chaque noeud mobile.

L'une d'entre elle est une adresse permanente (*home address*) $MN_{haddress}$ utilisée pour identifier le noeud en question. Elle est obtenue dans le réseau mère du mobile et a le même préfixe que tous les noeuds attachés sur le même lien (*home link*). Elle permet donc de router les paquets jusqu'au point d'attachement initial du mobile dans son réseau mère.

Lorsque le mobile se déplace, il obtient une adresse temporaire (*careof address*) MN_{coa} à chacun de ses points d'attachement. Elle reflète sa position dans la topologie Internet et est utilisée pour router les paquets de données jusqu'à la position courante du mobile. Le mobile enregistre cette adresse temporaire auprès du Home Agent (*HA*), un routeur positionné sur le lien *home link* dans le réseau mère, c'est-à-dire le réseau originel du mobile. Cet enregistrement se fait par l'intermédiaire d'un message appelé *Binding Update*, un paquet spécial contenant à la fois l'adresse permanente et l'adresse temporaire. Le *Binding Update* instruit le *HA* d'intercepter les paquets de données destinés au mobile identifié par l'adresse permanente et de les rediriger vers son adresse temporaire au moyen d'un tunnel.

Le protocole se comporte différemment selon que l'on utilise Mobile-IPv4 [8], Mobile-IPv4 avec l'optimisation de routage [6], ou Mobile-IPv6 [3]. Le principe général décrit ci-dessus est le même à la différence près du processus d'envoi des *Binding Updates*, ce qui influence la qualité du routage.

3.1 Mobile-IPv4 (RFC2002)

Dans Mobile-IPv4, le mobile visitant un réseau s'enregistre auprès d'un routeur appelé le *foreign agent* (*FA*) et qui se trouve sur le même lien que le point d'attachement du mobile. Le *FA* procure au mobile une adresse tempo-

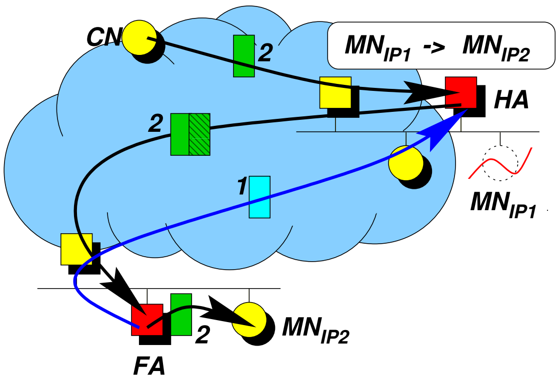

Figure 2: Mobile-IPv4 pour les noeuds mobiles

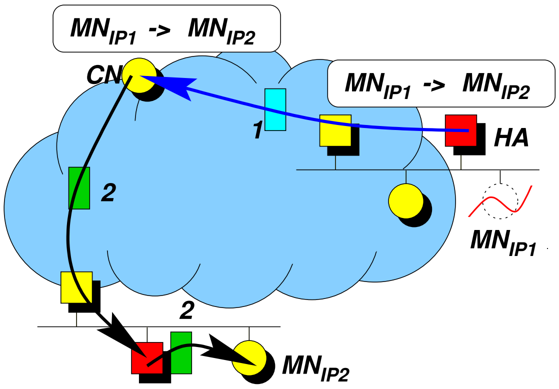

Figure 3: Mobile-IPv4 avec Optimisation de routage pour les noeuds mobiles

raire MN_{coa} qui correspond en fait à la propre adresse IP du *FA* et l'enregistre lui-même auprès du *HA* du mobile.

Les noeuds correspondant avec le mobile (*CNs*) n'étant pas informés de la l'adresse MN_{coa} du mobile, ils n'ont pas connaissance de sa position courante dans la topologie. Ils envoient donc les paquets vers la $MN_{haddress}$, comme le montre la figure 2. Sur le *home link*, le *HA* les intercepte et comprend qu'ils doivent être encapsulés vers MN_{coa}. Dans le réseau visité, le *FA* décapsule le paquet et le fait suivre au mobile.

3.2 Mobile-IPv4 avec optimisation de routage

Cette extension de Mobile-IPv4 permet un routage optimal sans passer par le *HA* entre les correspondants et le mobile en procurant à ces derniers l'adresse temporaire MN_{coa} du mobile.

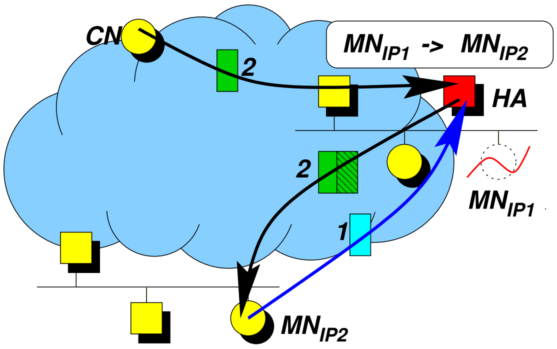

Figure 4: Premiers paquets de données vers un noeud mobile avec Mobile-IPv6

Lorsque des paquets destinés au mobile parviennent au *HA* , celui-ci comprend que le correspondant n'a pas connaissance de l'adresse MN_{coa} et la lui envoie au moyen d'un *Binding Update*. A réception d'un *Binding Update*, le correspondant enregistre dans un cache (Binding Cache) la correspondance entre $MN_{haddress}$ et MN_{coa}. Tous les paquets destinés au mobile seront par la suite encapsulés vers son adresse MN_{coa}, et décapsulés ultérieurement par le *FA* (figure 3).

3.3 Mobile-IPv6

Les nouvelles fonctionnalités d'IPv6 comparées à IPv4 permettent une meilleure gestion de la mobilité. Il existe donc un certain nombre de différences entre Mobile-IPv4 et Mobile-IPv6, bien que le principe général demeure le même. En particulier, l'optimisation du routage entre les correspondants et le mobile est intégrée dans la spécification de Mobile-IPv6. En effet, les nouvelles fonctionnalités d'IPv6 permettent au mobile de se passer d'un *FA* et d'envoyer lui-même ses *Binding Updates*.

A chacun de ses déplacements, le *MN* s'enregistre auprès d'un routeur sur le lien auquel il se rattache et obtient dynamiquement par le biais de DHCPv6 (Stateful [11] ou Stateless Autoconfigutation [1]) une adresse MN_{coa} qui lui est propre. Il peut posséder simultanément plusieurs adresses MN_{coa} sur des liens différents, mais il n'en enregistre qu'une seule, appelée l'adresse temporaire primaire.

Le mobile fait ensuite parvenir l'adresse temporaire primaire MN_{coa} au moyen d'un *Binding Update*, non seulement à son *HA*, mais aussi à chacun de ses correspondants ainsi qu'à un

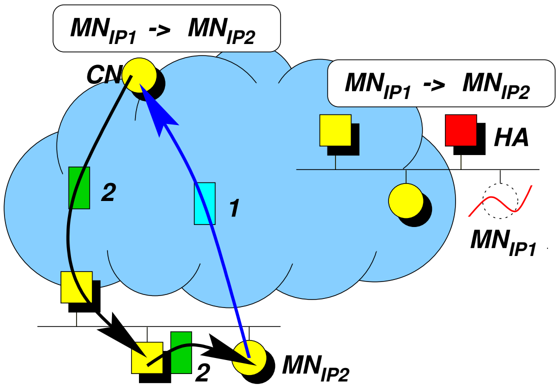

Figure 5: Routage optimal vers les noeuds mobiles avec Mobile-IPv6

routeur sur le lien précédemment visité afin de faire suivre les paquets précédemment envoyés à son adresse temporaire précédente. Les *Binding Updates* IPv6 sont des paquets spéciaux contenant deux *options* dans une extension d'entête IPv6 supplémentaire (*Destination Option extension header*): l'option *Home Address Option* qui contient l'adresse permanente du mobile pour l'identifier, et l'option *Binding Update Option* qui instruit le destinataire d'ajouter ou de mettre à jour l'entrée correspondante dans son Binding Cache. En sus de ces deux options, les *Binding Updates* doivent également contenir une extension d'entête *ESP* [5] ou *AH* [4] afin de permettre l'authentification du paquet par son destinataire et la confidentialité de l'information qu'il contient.

Le *HA* est instruit d'intercepter les paquets destinés au mobile et de les encapsuler vers son adresse MN_{coa}. Au début d'une communication entre un correspondant et un mobile, le correspondant n'a pas connaissance de la MN_{coa}. Il envoie donc les paquets normalement vers l'adresse $MN_{haddress}$ du mobile où le *HA* les encapsule vers la MN_{coa} comme cela est montré sur la figure 4. A la réception d'un paquet encapsulé, le mobile le décapsule, ajoute le correspondant dans sa liste de correspondants et envoie un *Binding Update* à celui-ci. Le correspondant comprend qu'il communique avec un mobile; il enregistre la correspondance entre $MN_{haddress}$ et MN_{coa} dans son cache. Les paquets suivants seront envoyés à l'adresse MN_{coa} en utilisant une extension d'entête IPv6 (*Routing extension header*) contenant l'adresse $MN_{haddress}$ pour l'identification du mobile. En recevant un paquet contenant cette entête, la couche IP du mobile permute l'adresse destination MN_{coa} et l'adresse $MN_{haddress}$ contenue dans l'option et passe le paquet à la couche supérieure (figure 5).

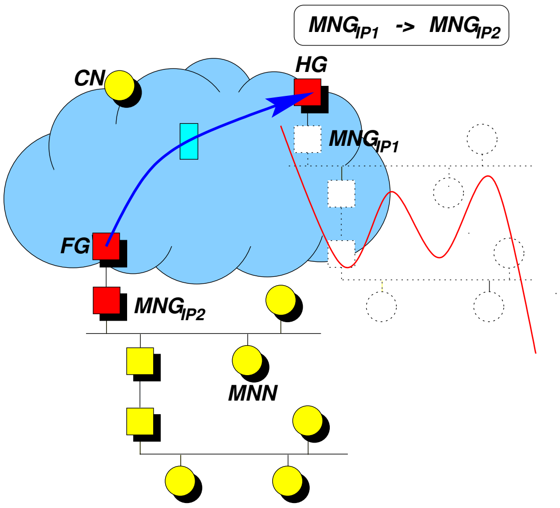

Figure 6: Réseaux mobiles avec Mobile-IPv4

4 Mobile-IP et les Réseaux Mobiles

Jusqu'à ce jour, les *réseaux mobiles* ont reçu très peu de considération au sein de l'IETF. Leur support est considéré explicitement dans Mobile-IPv4, mais il n'en est plus fait mention dans Mobile-IPv4 avec l'optimisation de routage ni dans Mobile-IPv6. Dans les sections suivantes, nous discutons du support des *réseaux mobiles* dans les trois cas en suivant les mécanismes intrinsèques de Mobile-IP pour les *noeuds mobiles*.

4.1 Mobile-IPv4

Les concepteurs de Mobile-IPv4 proposent de gérer la mobilité des réseaux de manière similaire à celle des noeuds en partant de l'observation qu'un *réseau mobile* n'est autre qu'un réseau rattaché à un routeur mobile, c'est à dire un noeud comme n'importe quel autre noeud (voir [8] section 4.5, [7] section 5.12, [10] section 11.2), et que nous appelons le *MNG*. Pour se faire, le *HG* fait office de *home agent* tandis que le *FG* courant fait office de *foreign agent*. A chacun de ses déplacements, le *MNG* obtient l'adresse

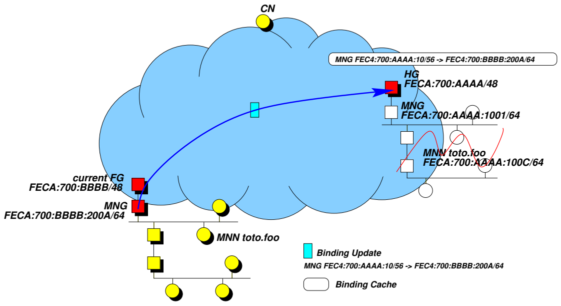

Figure 7: Réseaux mobiles avec Mobile-IPv6: Enregistrement auprès du HG

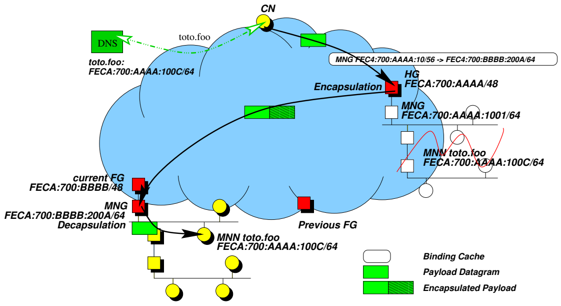

Figure 8: Réseaux mobiles avec Mobile-IPv6: premiers paquets via le HG

IP du *FG* courant qu'il utilise comme adresse temporaire MNG_{coa}. Le *FG* enregistre ensuite cette adresse temporaire auprès du *HG* dans son réseau mère, comme ceci est montré sur la figure 6.

Bien que Mobile-IPv4 permette le support de *réseaux mobiles* sans modification dans la spécification, son grand inconvénient est que tous les paquets de données passent nécessairement par le *HG*. Au regard des contraintes que nous nous sommes fixées dans la section 2, cette solution n'est pas acceptable car la quantité de trafic adressé à un *réseau mobile* peut être importante.

4.2 Mobile-IPv4 avec optimisation de routage

Cette extension de Mobile-IPv4 ne fait pas mention explicite des *réseaux mobiles*. En suivant le même mécanisme que dans Mobile-IPv4 avec optimisation de routage pour le support des noeuds mobiles, le *MNG* obtient l'adresse $FG_{ip\_address}$ du *FG* qu'il utilise comme adresse temporaire. Le *FG* enregistre ensuite cette adresse temporaire auprès du *HG*. Toujours suivant le même principe, le *HG* a également la charge d'envoyer un *Binding Update* aux *CNs* communiquant avec les *MNNs* du *réseau mobile* afin que ceux-ci puissent envoyer les paquets directement sans passer par le *HG*.

4.3 Mobile-IPv6

Mobile-IPv6 ne mentionne pas explicitement les *réseaux mobiles*. En suivant le même mécanisme que dans Mobile-IPv6 pour les *noeuds mobiles*, le *MNG* doit obtenir une adresse IP temporaire MNG_{coa} auprès du *FG* auquel il s'attache. Il faut noter ici que contrairement à Mobile-IPv4, l'adresse temporaire qu'il reçoit n'est pas l'adresse IP du *FG*, mais une adresse ayant le même préfixe que celle du *FG*. Le *MNG* doit ensuite enregistrer cette adresse temporaire auprès du *HG* dans le réseau mère du réseau mobile comme le montre la figure 7. La figure 8 montre comment les premiers paquets sont routés entre le *CN* et un *MNN* du *réseau mobile*. Ceux-ci atteignent le réseau mère du *réseau mobile* et parviennent jusqu'au point d'attachement initial du *réseau mobile*, c'est-à-dire le *HG*, qui les redirige en les encapsulant vers la MNG_{coa}. Les paquets sont ensuite décapsulés par le *MNG* et routés normalement vers l'adresse $MNN_{ip\_address}$ du *MNN*.

Afin de permettre un routage optimal, le *MNG* a la charge d'envoyer périodiquement des *Binding Updates* contenant l'adresse MNG_{coa} à chacun des *CNs* qui communiquent avec un *MNN* du *réseau mobile*. En effet, si on suit le même mécanisme que dans Mobile-IPv6, l'envoi des *Binding Updates* vers les *CNs* incombe au noeud obtenant l'adresse temporaire, donc au *MNG*. Les *CNs* doivent alors pouvoir envoyer directement leurs paquets de données à l'adresse $MNN_{ip\_address}$ via l'adresse MNG_{coa} en utilisant une extension d'entête IPv6 *Routing extension header*, comme illustré par la figure 9. Lorsqu'ils atteignent MNG_{coa}, les adresses sont permutées et les paquets sont routés jusqu'au *MNN* en utilisant le protocole de routage interne au *réseau mobile*. Suivant la spécification relative aux noeuds mobiles, l'envoi des *Binding Updates* incombe au *MNG*.

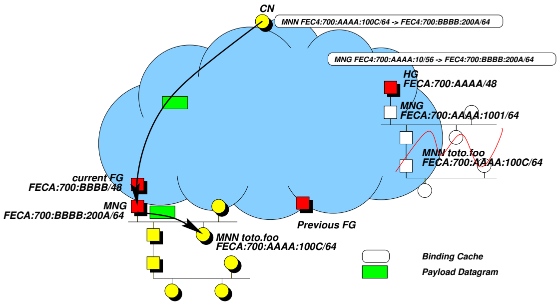

Figure 9: Réseaux mobiles avec Mobile-IPv6: routage optimal

5 Analyse de Mobile-IP pour le support des Réseaux Mobiles

L'étude de Mobile-IP révèle que ces protocoles ne sont pas adaptés pour le support des *réseaux mobiles*. Tout d'abord, nous avons vu que Mobile-IPv4 ne permet pas un routage optimal, ce qui est pourtant nécessaire pour les *réseaux mobiles* tel que cela a été montré dans la section 2. En ce qui concerne Mobile-IPv4 avec l'optimisation de routage et Mobile-IPv6, on peut théoriquement obtenir un routage optimal. Ceci est fait au moyen des *Binding Updates* émis périodiquement par respectivement le *HG* et le *MNG*. Ces *Binding Updates* doivent être envoyés à chacun des *CNs* communiquant avec les noeuds du *réseau mobile*, ce qui ne peut pas se faire sans modifications dans les spécifications pour les raisons que nous allons développer ci-dessous. Nous ne traiterons pas du cas spécifique de Mobile-IPv4 avec l'optimisation de routage car les problèmes rencontrés sont similaires à ceux de Mobile-IPv6.

Dans le cas du support des réseaux mobiles par Mobile-IPv6, l'envoi des *Binding Updates* doit se faire par le *MNG* pour le compte de ses *MNNs*. Or, ceci n'est pas permis par la spécification, pour des raisons d'authentification de la provenance des *Binding Updates* effectuée par les *CNs*. L'authentification est basée sur une clé que seul l'émetteur peut détenir. Le *Binding Update* étant émis par le *MNG*, le *CN* comprend que les paquets destinés à l'adresse $MNG_{home\_address}$ doivent être envoyés via l'adresse MNG_{coa}, mais rien ne lui permet pas de déduire qu'il doit en faire autant pour tous les noeuds qui ont le même préfixe que l'adresse $MNG_{home\_address}$. Il est donc

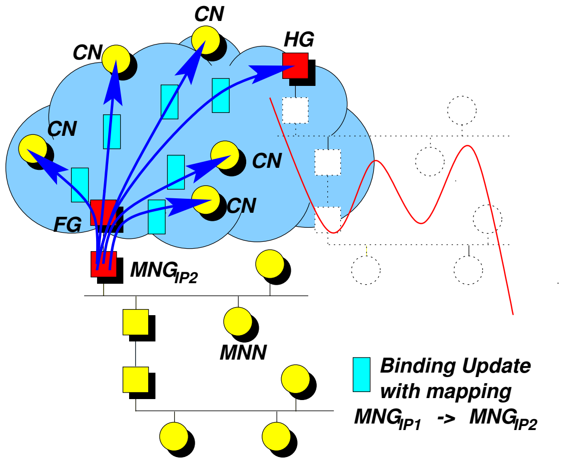

Figure 10: Explosion des messages de contrôle (Binding Updates)

souhaitable que Mobile-IPv6 intègre cette notion de préfixe afin que les *CNs* utilisent la même adresse temporaire pour chaque adresse $MNN_{ip\_address}$ ayant un préfixe identique à celui de l'adresse $MNG_{home\_address}$ enregistrée dans leur cache.

On pourrait aussi envisager que le *MNG* envoie les *Binding Updates* aux *CNs* en se faisant passer pour chacun de ses *MNNs*, en envoyant l'adresse $MNN_{ip\_address}$ du noeud concerné. Le *CN* doit alors vérifier que l'émetteur du *Binding Update* est bien le *MNN*. Cela nécessiterait un nouveau mécanisme permettant aux *MNNs* de faire parvenir leur clé au *MNG*. Cette dernière solution est réalisable, mais pas souhaitable car elle viole le principe d'authentification de bout en bout. D'autre part, on constate une possible duplication des *Binding Updates* dans le cas où un *CN* correspond avec plus d'un *MNN* du même *réseau mobile*. En effet, le *MNG* enverrait alors plusieurs *Binding Updates* à ce *CN*, ce qui consommerait inutilement de la bande passante, et le *CN* enregistrerait alors dans son cache une adresse temporaire MNG_{coa} identique pour tous les mobiles du *réseau mobile* avec lesquels il communique. Pour pallier à ces problèmes, on peut envisager que les *MNNs* envoient directement les *Binding Updates* à leurs propres *CNs*, mais cela nécessite également des modifications dans la spécification, entre autres un mécanisme pour que les *MNNs* détectent la mobilité du réseau et obtiennent l'adresse temporaire du *MNG*. De plus, on constate que la mobilité du réseau ne se fait plus de manière transparente pour les *MNNs*.

Bien que ces modifications soient possibles, nous avons vu que les *réseaux mobiles* peuvent être de taille significativement grande. Dans ce cas, l'envoi de *Binding Updates* à chaque *CN* provoque une explosion de *Binding Updates*, comme cela est montré sur la figure 10. L'explosion de *Binding Updates* se traduit à la fois par un coût très élevé en ressource mémoire pour garder l'historique des *Binding Updates* envoyés aux différents *CNs*, en CPU pour l'envoi des *Binding Updates*, et en bande passante en particulier à proximité du *HA* où les liens pourraient être congestionnés par un nombre excessif de *Binding Updates*.

Nous constatons donc que les spécifications actuelles de Mobile-IP ne permettent pas de supporter les réseaux mobiles sans d'abord y apporter de nombreuses modifications. De plus, les mécanismes intrinsèques de Mobile-IP doivent être revisités pour permettre un routage optimal vers les réseaux mobiles tout en évitant le problème de l'explosion des *Binding Updates*.

6 Conclusion

Dans ce papier, nous avons étudié la question de la mobilité des réseaux au sein de la topologie Internet et la possibilité de leur support par les protocoles actuels gérant la mobilité des noeuds, respectivement Mobile-IPv4, Mobile-IPv4 avec l'optimisation de routage et Mobile-IPv6.

Nous avons mis en avant l'importance de l'optimisation du routage dans le contexte des *réseaux mobiles* à cause de la quantité de trafic qui peut leur être destiné. Or, comme nous l'avons vu, non seulement les spécifications actuelles ne permettent pas de gérer la mobilité des réseaux sans procéder auparavant à d'importantes modifications, mais de plus les mécanismes intrinsèques de ces spécifications induisent de trop nombreux messages de contrôle pour éviter un routage triangulaire. En effet, l'envoi périodique de l'adresse temporaire à tous les noeuds correspondant avec un ou plusieurs noeuds du *réseau mobile* conduit à une explosion de ces messages au niveau de leur émetteur et à une quantité excessive de message de contrôle sur le réseau. Il convient donc soit d'étendre Mobile-IP pour supporter les *réseaux mobiles* efficacement ou de définir de nouvelles solutions mieux adaptées.

Nous travaillons actuellement sur les possibles extensions à apporter à Mobile-IP pour permettre un routage optimal en évitant cette explosion de *Binding Updates* ainsi que les problèmes d'authentification, et ce dans le contexte d'IPv6 qui offre de meilleurs outils qu'IPv4. Bien que cela puisse nécessiter de petites modifications dans chaque noeud IPv6, cela ne pose pas de problème dans la mesure où IPv6 n'a pour l'instant pas commencé à être déployé. Ces travaux feront l'objet d'une prochaine soumission de nos résultats obtenus par simulation avec NS-2.

References

[1] J. Bound and C. Perkins. Dynamic Host Configuration Protocol for IPv6 (DHCPv6). Internet-Draft draft-ietf-dhc-dhcpv6-14.txt, Internet Engineering Task Force (IETF), February 1999.

[2] S. Deering and R. Hinden. Internet Protocol Version 6 (IPv6) Specification. Request For Comments 2460, Internet Engineering Task Force (IETF), December 1998.

[3] David B. Johnson and C. Perkins. Mobility Support in IPv6. Internet Draft draft-ietf-mobileip-ipv6-08.txt, Internet Engineering Task Force (IETF), June 1999. Work in progress.

[4] S. Kent and R. Atkinson. IP Authentication Header. Request For Comments 2402, Internet Engineering Task Force (IETF), November 1998.

[5] S. Kent and R. Atkinson. IP Encapsulating Security Payload (ESP). Request For Comments 2406, Internet Engineering Task Force (IETF), November 1998.

[6] Charles Perkins and David B. Johnson. Route Optimization in Mobile IP. IETF Internet Draft draft-ietf-mobileip-optim-08.txt, Sun Microsystems and Carnegie Mellon University, February 1999. Work in progress.

[7] Charles E. Perkins. *Mobile IP, Design Principles and Practices.* Wireless Communications Series. Addison-Wesley, 1998. ISBN 0-201-63469-4.

[8] Charles Perkins (Editor). IP Mobility Support. Request For Comments 2002, Internet Engineering Task Force (IETF), October 1996.

[9] Thomas Quinot. An IPv6 architecture for Aeronautical Telecommunication Network. Master's thesis, Ecole Nationale Supérieure des Télécommunications Paris, EUROCONTROL - European Organization for the Safety of Air Navigation - ISA project (IPv6, Satellite communication and ATMode for ATN), 1998. http://www.eurocontrol.fr/.

[10] James D. Solomon. *Mobile IP, The Internet Unplugged.* Prentice Hall Series in Computer Networking and Distributed Systems. Prentice Hall PTR, 1998. ISBN 0-13-856246-6.

[11] S. Thomson and T. Narten. IPv6 Stateless Address Autoconfiguration. Request For Comments 2462, Internet Engineering Task Force (IETF), December 1998.