La sécurité dans Mobile IPv6

SSTIC 2006.

Arnaud EBALARD[1] <arnaud.ebalard@eads.net>
and Guillaume VALADON[2] <guedou@hongo.wide.ad.jp>

[1] EADS Corporate Research Center France
[2] The University of Tokyo - Esaki Lab / LIP6, Paris

Résumé Mobile IPv6 fournit à l'utilisateur nomade un moyen de conserver son adresse IP, quel que soit son réseau d'accueil. Il reste ainsi joignable de manière transparente, indépendamment de ses emplacements.

Pour fournir cette fonctionnalité tout en offrant la sécurité aux différentes entités impliquées, le protocole intègre des mécanismes de sécurité initrinsèques tout en se reposant également sur IPsec pour la protection de certains flux.

1 Introduction

Internet est désormais omniprésent dans notre vie de tous les jours et nous permet de communiquer de façon plus efficace que par le passé. Différentes technologies d'accès telles qu'Ethernet, 802.11, et CDMA permettent aujourd'hui d'offrir une connectivité à tout moment et en tout lieu.

De ce fait, le mode d'utilisation d'Internet est en train d'évoluer considérablement, les utilisateurs et leurs équipements devenant de plus en plus mobiles ; il est en effet devenu courant d'utiliser son ordinateur portable au bureau, dans le train et à la maison au cours d'une même journée.

Généralement, le passage d'une méthode d'accès à une autre ou d'un site d'accès à un autre induit un changement des adresses IP utilisées et une perte quasi certaine des éventuelles connections en cours, notamment TCP.

Le rôle du protocole Mobile IPv6 [RFC3775], MIPv6, est de rendre ce changement de site ou de medium transparent aux applications. En pratique, il permet à une machine de rester joignable et de communiquer avec la même adresse, quelle que soit son medium et sa position courante.

Normalisé par l'IETF [RFC3775,RFC3776] et déjà implémenté pour les systèmes d'exploitation majeurs (Windows XP, Linux, *BSD), différents opérateurs étudient d'ores et déjà la manière de déployer cette technologie dans le cadre de leurs activités commerciales. La généralisation rapide d'IPv6 et l'extension naturelle au protocole que MIPv6 constitue pour le nomadisme vont en faire une technologie incontournable dans les années à venir.

Utilisant des extensions spécifiques à IPv6 et tirant partie d'un environnement plus favorable que sous IPv4 (notamment pour IPsec), la sécurité du protocole a été prise en compte dès sa conception.

Après quelques rappels à l'attention des lecteurs non familiers avec IPv6 dans la section 2, la section 3 décrit le protocole Mobile IPv6 en détails. Les sections 4 et 5 sont respectivement consacrées aux problématiques de sécurité dans Mobile IPv6 et aux contraintes soulevées par l'utilisation d'IPsec pour sécuriser ce protocole. Finalement, la section 6 fournit un état de l'art des implémentations existantes sur les aspects sécurité.

2 Rappels sur IPv6

Pour comprendre le fonctionnement de Mobile IPv6, il est tout d'abord nécessaire de bien appréhender le protocole IPv6. Cette section fournit un résumé des éléments clés du protocole, ceux-ci étant principalement comparés à ceux d'IPv4.

Le lecteur déjà familier avec IPv6 peut se reporter directement à la sous-section 2.2, qui détaille les mécanismes propres à IPv6 et nécessaires à Mobile IPv6.

2.1 Différences fondamentales avec IPv4

Les limitations d'IPv4 ont poussé le développement d'une nouvelle version du protocole IP. IPv6 est le résultat de dix années passées à prendre en compte et à résoudre les problèmes liés à IPv4. Les deux principaux problèmes d'IPv4 (source de nombreux autres) sont :

1. son succès ;
2. ses difficultés de passage à l'échelle.

En 1992, les recherches concernant la future version du protocole ont commencé, donnant lieu en 1995 à IPv6 [RFC1883] (puis [RFC2460] en 1998). Outre le passage à un adressage sur 128 bits, le protocole apporte également un grand nombre d'améliorations obtenues de l'expérience acquise grâce à IPv4.

Généralités D'une part, l'un des buts de l'évolution du protocole a consisté à diminuer le travail des noeuds intermédiaires dans le réseau. Ainsi, la fragmentation est maintenant interdite au niveau des routeurs ; elle est réalisée de manière optionnelle entre la source et la destination[3].

D'autre part, dans une volonté de remettre en place des connexions de bout-en-bout [SALTZER,RFC1958,RFC3439], de nombreux mécanismes ont été

[3] Un mécanisme de découverte de la MTU de chemin (PMTU Discovery) utilisant ICMPv6, et une MTU minimale des liens IPv6 étendue à 1280 octets permettent notamment cette avancée

déplacés pour finir par n'être traités que par les hôtes source et destination. Par exemple, le checksum sur le header IP a disparu.

Dans cette optique, l'élément majeur à prendre en compte est la disparition de la NAT ; ce mécanisme n'ayant plus de sens du fait de l'adressage global permis par la taille des adresses. Désormais, chaque noeud possède une adresse publique, appelée adresse unicast globale dans la terminologie IPv6. Le recours à un élément externe servant de relai dans les connexions de deux clients n'est plus requis. Ainsi, un transfert de fichier entre deux clients peut s'opérer de manière directe sans passer par un tiers, comme une gateway MSN.

IPsec est sans doute le premier bénéficiaire de cet aplanissement du réseau, les clients jusqu'alors inaccessibles du fait de la présence de gateway NAT redevenant à nouveau joignables. Son implémentation est requise dans les piles IPv6 ; ce qui en fait un mécanisme de choix pour la sécurisation de certaines communications.

Au niveau du lien, IPv6 apporte également de nombreuses nouveautés, notamment la disparition d'ARP et son remplacement par un mécanisme d'autoconfiguration basé sur ICMPv6 (Neighbor Discovery, [RFC2461]). Plus généralement, les utilisations d'ICMP ont été étendues, comparativement à celles sous IPv4. Même si certains points sont encore en phase d'étude, l'utilisation de types ICMPv6 séparés laisse un champ propice à une simplification du filtrage et à une sécurisation via IPsec.

Format des paquets La figure 1 présente le format d'un paquet IPv6. Les informations inutiles aux paquets les plus courants ont été supprimées. Un mécanisme de chaînage, utilisant le champ *Next Header* pour indiquer le header suivant, permet d'étendre les informations présentes dans un paquet, par exemple celles concernant la fragmentation, ESP, ou AH[4].

Concrètement, les différences dans le format des headers sont les suivantes :

- les champs *Identification*, *Flags* et *Frag Offset* trouvent des équivalents dans un header optionnel, le *Fragmentation Header*.
- le champ de checksum IP disparait, les vérifications d'intégrité du header IP étant déportées au niveau de TCP, UDP et ICMPv6 via le concept de pseudo-header.
- la diminution du nombre de champs (passage de 14 à 8) permet de réduire le traitement au niveau des routeurs.
- l'alignement sur 64 bits permet d'autres optimisations matérielles.

2.2 Pré-requis pour Mobile IPv6

Routing Header Type 2 Parmi les extensions définies dans [RFC2460], le mécanisme de Routing Header est utilisé par un noeud source pour lister un ou plusieurs noeuds intermédiaires par lesquels le paquet doit transiter pour atteindre sa destination. Lorsqu'il est utilisé, le champ *Next Header* du header précédent prend la valeur 43.

[4] Encapsulation Security Payload et Authentication Header

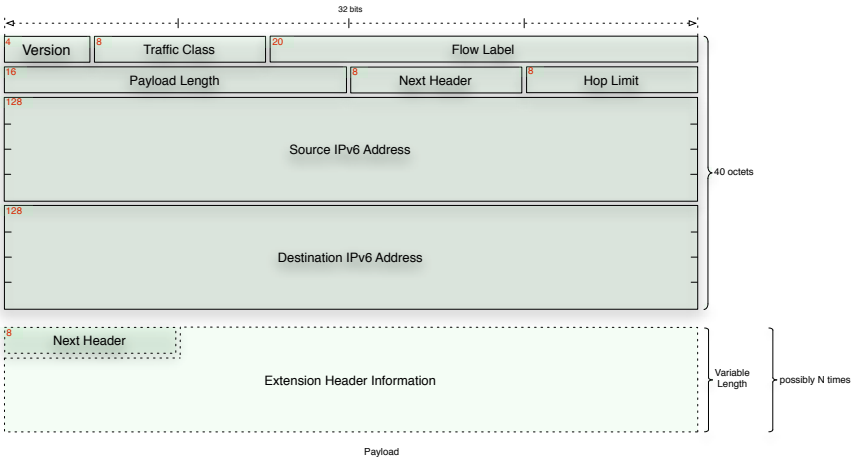

Fig. 1. Header IPv6

Comme présenté sur la figure 2, un champ type permet de modifier la sémantique de l'extension. Dans son utilisation standard (Routing Header Type 0), il fournit l'équivalent du mécanisme de Source Routing bien connu sous IPv4.

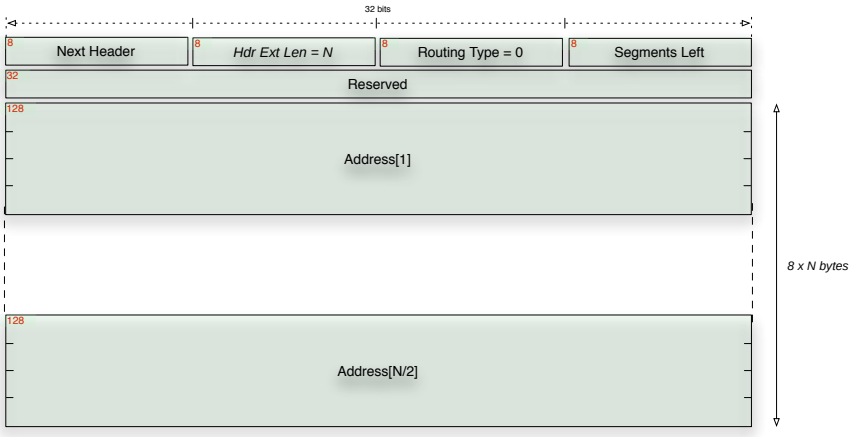

Fig. 2. Format des Routing Header Type 0

Chaque intermédiaire spécifié dans la liste utilise les valeurs des champs *Segleft* et *Hdr Ext Len* pour obtenir l'adresse de l'intermédiaire suivant. Il permute alors cette adresse avec celle présente dans le champ destination du paquet reçu.

Après avoir décrémenté la valeur du champ *Seg Left*, il reémet le paquet. Le destinataire final est celui qui reçoit le paquet avec un champ *Seg Left* à 0.

Mobile IPv6 définit un type spécifique, le type 2, version restreinte du type 0, limitant la liste des intermédiaires à une entrée. Les impacts de ce nouveau type en terme de sécurité sont détaillés par la suite.

Destination Options Header Ce type de header est utilisé pour transporter une information optionnelle devant être examinée uniquement par le noeud destination. Il est identifié par une valeur de 60 dans le champ *Next Header* du header précédent.

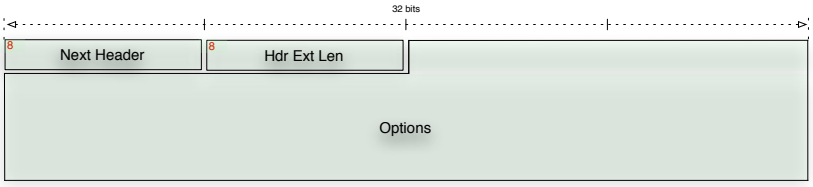

Fig. 3. Header IPv6

Le champ *Hdr Ext Len* indique la longueur de ce header en unité de 8 octets (celle-ci n'incluant pas les 8 premiers octets), le champ *Next Header* indiquant le type du header suivant, et le champ *Options* constituant un conteneur générique transportant un nombre variable d'options encodées sous forme de TLV[5].

3 Mobile IPv6

Le protocole Mobile IPv6 a été défini par le groupe de travail *mip6* de l'IETF dans [RFC3775]. Il autorise un hôte à utiliser une adresse IPv6 fixe indépendamment de ses déplacements. Il permet à la couche IP de masquer les effets de la mobilité aux protocoles supérieurs tels que TCP ou UDP et de fait aux applications les utilisant. Dans la terminologie MIPv6, l'hôte mobile est appelé Mobile Node (MN) et l'adresse unique Home Address (HoA). La figure 4 présente les différentes entités impliquées lorsque MIPv6 est utilisé par le MN pour communiquer. Le Home Agent (HA), le Correspondent Node (CN), et le MN utilisent des préfixes IPv6 différents.

Lorsqu'un noeud mobile se déplace, son sous-réseau d'attachement (réseau d'accueil) change, impliquant une modification de préfixe et donc plus généralement d'adresse IP. Ceci pose principalement deux types de problèmes :

[5] Type Length Value

1. les connexions existantes (connexions TCP, SA IPsec, ...) entre le noeud mobile et ses clients deviennent invalides ;
2. le noeud mobile n'est plus accessible à son ancienne adresse pour l'ouverture de nouvelles connexions.

Pour bien appréhender les problèmes associés à la mobilité IP et la solution apportée par Mobile IPv6, il est nécessaire de comprendre le double rôle que joue une adresse IP pour un noeud : elle est à la fois *identifiant pour le noeud* [6] ("Identifier") mais également *adresse pour le routage des messages jusqu'au noeud* ("Locator"). En raison de l'adressage hiérarchique utilisé dans IPv6, cette dernière peut être vue comme une information sur la position géographique du noeud.

3.1 Vue d'ensemble

Comme évoqué précédemment, Mobile IPv6 doit gérer dans le temps les associations entre les informations de position et d'identification pour le noeud.

A cet effet, le protocole définit la notion de **Home Address (HoA)** : il s'agit d'une adresse du réseau mère (classiquement, le réseau de son entreprise) du noeud mobile utilisée pour *identifier* le noeud. Cette adresse lui est associée quel que soit son réseau d'attachement.

Il définit également la notion de **Care-of address (CoA)**, qui est quant à elle l'adresse que possède le noeud dans son réseau d'accueil actuel. Elle ne joue aucun rôle en terme d'identification mais sert uniquement au routage des paquets jusqu'au site d'accueil du noeud.

Il n'existe pas de moyen de distinguer a priori une CoA, d'une HoA, d'une autre adresse IPv6 unicast globale. De plus, MIPv6 est transparent pour les correspondants du noeud mobile, aucune tâche particulière n'étant requise de leur côté[7] : il est ainsi impossible de distinguer un noeud mobile d'un noeud fixe.

Sur son réseau mère (Home Network), le noeud mobile possède un agent, appelé Home Agent (HA), dont le rôle est de tunneler les paquets pour le noeud mobile. Ce Home Agent intercepte les paquets des correspondants à destination du noeud mobile (de sa HoA) et les tunnelle vers l'emplacement courant du noeud (sa CoA), dans son réseau d'accueil. Le mécanisme inverse intervient lorsque le noeud mobile tunnelle un paquet à destination de son correspondant, via son Home Agent. *Le rôle principal du Home Agent est de maintenir la correspondance entre la la CoA et la HoA du noeud mobile*, i.e. entre l'adresse l'identifiant et son emplacement actuel. C'est ce que décrit la figure 4 :

Malgré tout, ce mode n'est pas optimal, les paquets à destination du noeud mobile transitant systématiquement par le Home Agent sur le réseau mère. Mobile IPv6 définit donc un mode optimisé appelé Route Optimization, évitant

[6] c'est par ce biais que le noeud est généralement désigné, comme fournisseur de certains services

[7] dans un mode non optimisé

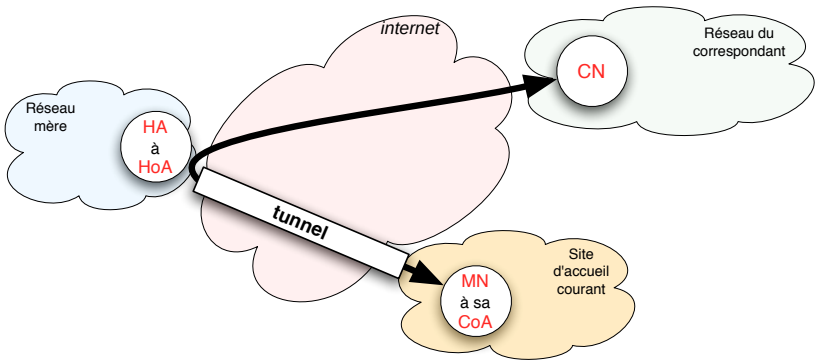

Fig. 4. Mobile IPv6 sans optimisation

ce routage triangulaire, cf. figure 5. Celui-ci ne fonctionne qu'avec les CN implémentant MIPv6. Cette optimisation de routage n'étant qu'optionnelle, il est possible pour les deux participants de la refuser tout en continuant à communiquer au travers du Home-Agent.

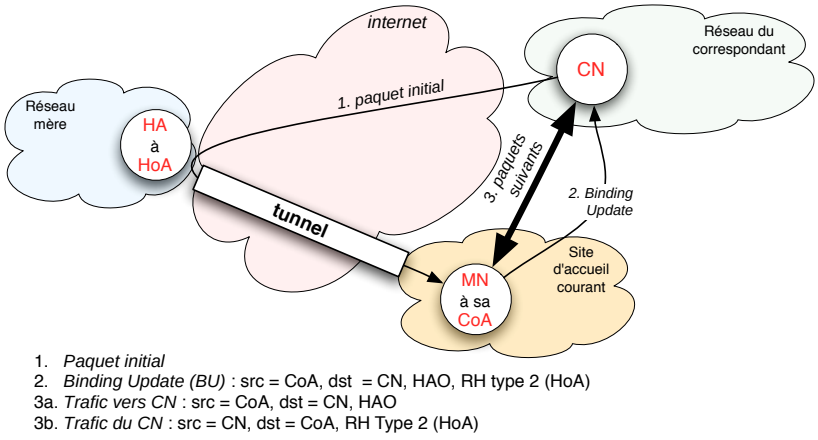

Fig. 5. Mobile IPv6 avec optimisation du routage

3.2 Détails

Mode non optimisé

Détection d'un nouveau point d'attachement Lorsqu'un noeud mobile change de point d'attachement, celui-ci reçoit un message Router Advertisement comportant un préfixe IPv6 différent de celui de sa CoA. A la réception de ce message, le noeud configure une nouvelle CoA appartenant au préfixe annoncé par le routeur d'accès. Afin de diminuer la durée d'un handover lors du passage d'un réseau à un autre, le noeud mobile peut soliciter le Router Advertisement en diffusant un message Router Solicitation comme dans la figure 6.

Procédure d'association Après configuration d'une nouvelle CoA, le noeud mobile s'associe avec son Home Agent. Pour se faire, il lui envoie un message Binding Update, BU. Ce message permet au HA de faire la relation entre la HoA et la CoA du noeud mobile. Celle-ci est stockée dans le *Binding Cache* du HA. Il s'agit d'une table de routage supplémentaire permettant de délivrer les paquets destinés à la HoA du noeud mobile à travers un tunnel IPv6-IPv6 établi entre le HA et la CoA du MN ; la HoA étant présente dans l'option Destination Option, et la CoA accessible directement dans le header IPv6 ainsi que dans l'option Alternate CoA des BU. A la reception du BU, le HA répond[8] par un Binding Acknowledgement, BA et établit le tunnel, comme dans la figure 6. La gestion des différentes erreurs est réalisée grâce aux messages Binding Error.

Mode optimisé

Le but de l'optimisation de routage est de permettre une connection directe entre le MN et le CN ne passant pas par le HA. Si la relation entre le MN et le HA dans un mode non optimisé a le mérite d'être simple, principalement du fait de leur connaissance préalable[9], celle liant un MN et un CN communiquant de manière directe est moins évidente.

Dans un mode optimisé, le CN se voit attribué une grande partie du rôle du HA, puisqu'il devient conscient de la CoA de son interlocuteur. Malgré tout, contrairement au HA, aucune information préalable permettant l'authentification du MN ne lui est disponible, a priori.

[8] le MN peut explicitement demander à ne pas recevoir de BA.
[9] secret partagé, voire certificats pour la protection par IPsec de leurs communications.

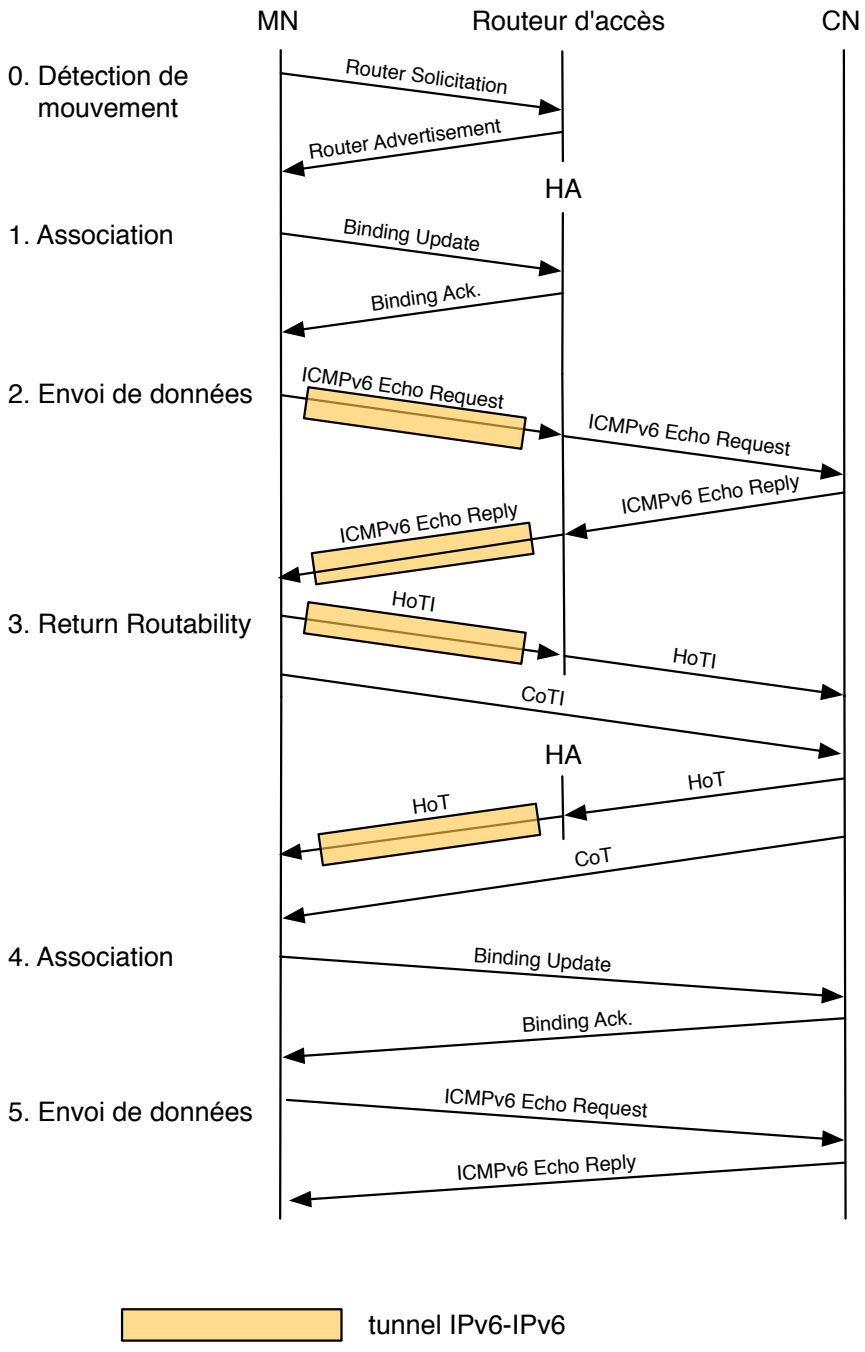

Fig. 6. Echanges de paquets dans Mobile IPv6

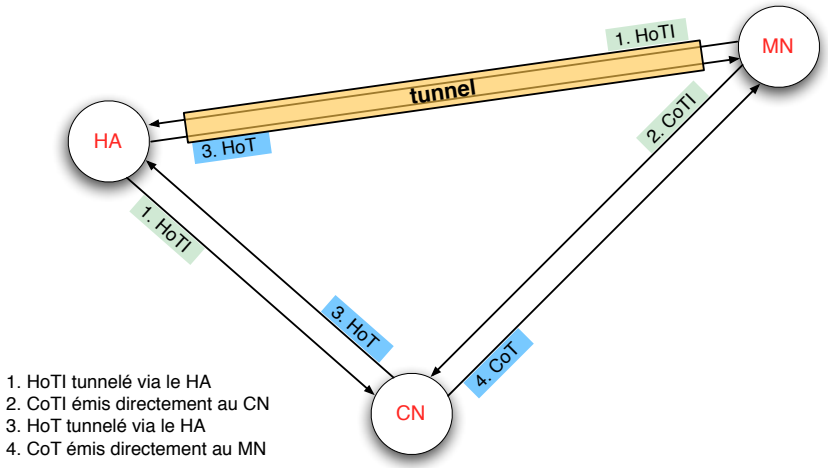

Fig. 7. Procédure de "Return Routability"

Il revient donc au MN de *prouver* à ses CN qu'il est bien possesseur des adresses auxquelles il prétend être joignable : sa HoA et sa CoA. Cette preuve est fournie si le MN est capable d'émettre et de recevoir du trafic depuis ces deux adresses : c'est le rôle de la "Return Routability Procedure"[10]. Dans les faits, la procédure est légèrement compliquée pour lui conserver son caractère *sans état* du point de vue du CN. Elle est basée sur l'échange de deux cookies, Care-of Init Cookie et Home Init Cookie, émis par le MN à destination du CN. Le premier est envoyé de manière directe avec la CoA du MN, et le second de manière indirecte avec la HoA du MN, en passant par le tunnel vers le HA. La réception de ces deux élements par le CN lui garantissent que le MN est bien capable de dialoguer avec sa CoA et sa HoA.

Ces deux cookies sont respectivement retournés dans les messages CoT et HoT émis par le CN au MN en réponse aux messages CoTI et HoTI reçus. Ils apportent alors au MN une garantie relative que les réponses proviennent d'une personne capable d'émettre avec l'adresse du CN et de recevoir à cette adresse des messages provenant du réseau d'accueil et du réseau mère du MN. Ils préviennent donc qu'un noeud présent sur le réseau d'accueil ou sur le chemin entre le MN et le CN puisse forger les réponses. Un tel attaquant doit également être capable d'obtenir le trafic émis du réseau mère vers le CN.
Cependant, cette utilisation de cookies n'apporte aucune solution face à un attaquant présent sur le réseau du CN capable d'accéder au trafic de celui-ci et d'en injecter en son nom. Ainsi, le niveau de sécurité est comparable à

[10] [RFC4225] décrit les problématiques et la section 15 de [RFC3775] les détails de la solution choisie.

celui d'une communication classique sur Internet entre deux clients quelconques.

De plus, deux types de Keygen Token (Care-of Keygen Token et Home Keygen Token), sont émis en réponse par le CN, respectivement à destination de la HoA du MN et de sa CoA. L'utilisation future de ces deux tokens pour authentification dans les messages de signalisation, i.e. Binding Update émis à destination du CN, permet de limiter la provenance aux personnes capables de recevoir du trafic à ces adresses.

La figure suivante synthétise les éléments échangés durant la Return Routability Procedure :

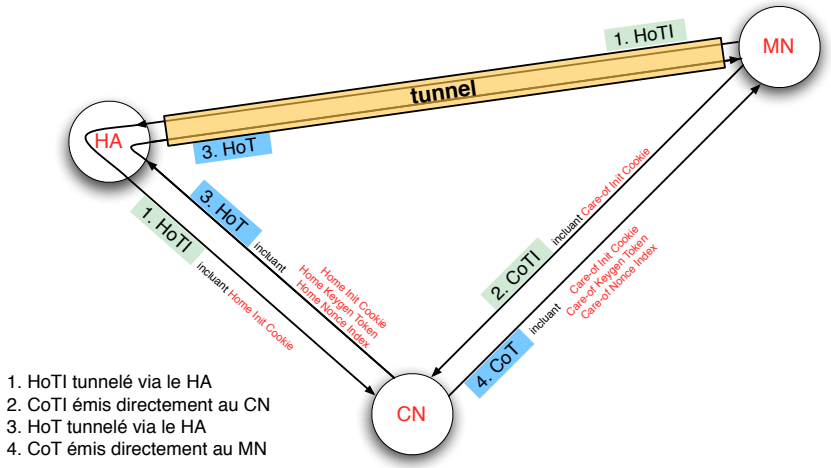

Fig. 8. Echange des éléments durant la "Return Routability Procedure"

3.3 La structure des paquets

Le trafic de signalisation de Mobile IPv6 se présente sous la forme d'un nouveau protocole identifié par le numéro 135 dans le champ Next Header de l'entête précédent. La figure 9 présente le format générique de ce Mobility Header. Le champ *Mobility Header Type* définit le type du message réellement transporté comme indiqué sur la figure 10.
De plus, ces différents messages peuvent comporter des options particulières au format. Ceci permet par exemple d'identifier la Care of Address du Mobile Node ou bien encore sa Home Address.

Les pseudo-paquets suivants représentent l'envoi de Binding Update et la réception du Binding Acknowledgement du Mobile Node vers le Home Agent et

le Correspondent Node. Seul les champs significatifs sont représentés.

1. Mode non optimisé

   - *Binding Update du MN au HA*

     ```
     IPv6(dst=HA, src=CoA)
              DestOpt(value=HoA)
                    MH(mhtype=5)
                           BindingUpdate()
                                 AlternateCareofAddress(value=CoA)
     ```

   - *Binding Acknowledgement du MN au HA*

     ```
     IPv6(dst=CoA, src=HA)
              RoutingHeader(type=2, value=HoA)
                                          MH(mhtype=6)
                                                  BindingAck()
     ```

2. Mode optimisé : Return Routability Procedure

   - *HoTI du MN au CN (via le HA)*

     ```
     IPv6(dst=CN, src=HoA)/MH(type=1)/HoTI()
     ```

   - *HoT du CN au MN (via le HA)*

     ```
     IPv6(dst=HoA, src=CN)/MH(type=3)/HoT()
     ```

   - *CoTI du MN au CN*

     ```
     IPv6(dst=CN, src=CoA)/MH(type=2)/CoTI()
     ```

– *CoT du CN au MN*

```
IPv6(dst=CoA, src=CN)/MH(type=4)/CoT()
```

– *Binding Update du MN au CN*

```
IPv6(dst=CN, src=CoA)
          DestOpt(value=HoA)
                    MH(mhtype=5)
                              BindingUpdate()
```

– *Binding Acknowledgement du CN au HA*

```
IPv6(dst=CoA, src=CN)
       RoutingHeader(type=2, value=HoA)
                                   MH(mhtype=6)
                                          BindingAck()
```

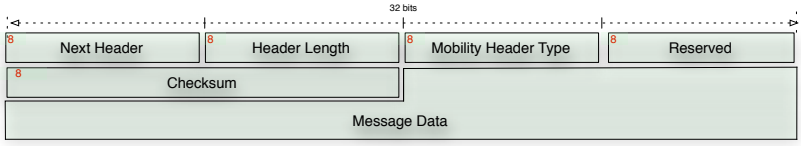

Fig. 9. Format du Mobility Header (MH)

Mobility Header Type	Mobility Message
1	Home Test Init
2	Care-Of Init
3	Home Test
4	Care-of Test
5	Binding Update
6	Binding Acknowledgement
7	Binding Error

Fig. 10. Mobility message et Mobility Header Type

Il est important de remarquer les deux points suivants :

- les paquets émis par le MN utilisent une option spécifique (HAO : Home Address Option, figure 11) du header Destination Option, permettant d'informer le récepteur de la HoA du noeud mobile.

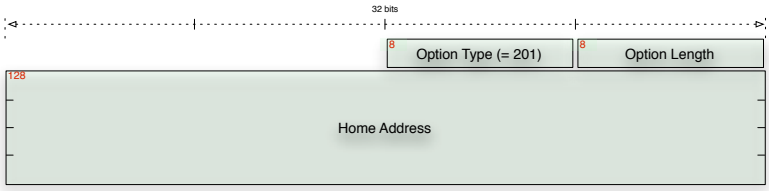

Fig. 11. Home Address Option (HAO)

- les paquets à destination du MN contiennent un Routing Header Type 2, transportant la HoA du noeud mobile. Il indique au MN que bien que le paquet doive être routé jusqu'à la CoA, il a réellement pour destination la HoA du noeud.

4 La sécurité dans MIPv6

Mobile IPv6 a la particularité de mettre en œuvre des communications entre trois participants : un CN, un MN et son HA. La sécurité de cette relation triangulaire entre les acteurs doit être étudiée en prenant en compte différents points de vue. Tout d'abord, chacun des participants doit être protégé d'éventuelles attaques pouvant survenir du fait de l'utilisation de Mobile IPv6. En pratique, chacun doit avoir la garantie que ses interlocuteurs sont bien ceux qu'ils prétendent être. De plus, les réseaux dans lesquels se situent les trois participants ne doivent pas être impactés par la présence de ceux-ci.

Enfin, l'utilisation des Routing Header et de l'option Home Address permettant de modifier les adresses destination et source des MN et CN[11] ne doivent pas fournir de nouvelles vulnérabilités.

4.1 Prise en compte des impacts sur Internet

L'une des recommendations fournie par l'IESG au Working Group Mobile IP était la suivante : "Do no harm to the existing Internet".

[11] et donc de passer outre les mécanismes d'Ingress filtering [RFC2827,RFC3704] éventuellement déployés sur Internet

La majorité des problématiques de sécurité soulevées par le protocole vis-à-vis d'Internet concerne la mise en œuvre de technologies permettant de modifier ses adresses sources et destination : il s'agit des mécanismes de *Routing Header Type 2* et de *Destination Header - Home Address Option*.

La problématique a été prise en compte dès les débuts du Working Group sur le sujet. Elle a notamment été formalisée dans [RHHASec][12].

- **Routing Header Type 2** : Le mécanisme de Routing Header intégré à IPv6 fournit dans sa version de base (Type 0) une fonctionnalité comparable aux options de source-routing disponible sous IPv4[13]. Sous IPv4, les implications de sécurité associées sont telles que la majorité des routeurs actuels désactivent par défaut le support de cette option.
  La prise en compte de cette problématique dans le cadre d'IPv6 a permis la définition d'un Routing Header d'un type spécifique (Type 2), utilisé uniquement dans le cadre du protocole et transportant une seule adresse (en pratique, la HoA du MN). Son interprétation est donc limitée aux seuls noeuds mobiles.
  Les conséquences liées à l'utilisation d'un nouveau type sont également importantes au niveau filtrage. Il devient possible d'adopter des politiques différentes pour les paquets incluant un Routing Header Type 0[14] et ceux incluant un Routing Header Type 2[15].

- **Destination Options Header - Home Address Option** : cette option du Destination Header, potentiellement impactante au niveau sécurité, est définie spécifiquement par Mobile IPv6. Elle n'a donc pas d'interprétation hors du cadre du protocole.
  En pratique, même si un paquet incluant cette option est reçue par une machine (du fait d'une absence de filtrage), celle-ci ne prendra pas en compte l'information transportée. En d'autres termes, elle ne réalisera pas la modification d'adresse source du paquet avec l'information présente dans l'option.
  De plus, l'utilisation d'IPsec sur le trafic de signalisation et plus particulièrement sur les messages incluant cette option (Binding Update et Mobile Prefix Solicitation), limite la prise en charge de celle-ci aux seuls HA et CN implémentant MIPv6.

Un autre point important dans le développement du protocole a également concerné les problématiques de DoS, que ce soit sur les participants ou sur l'infrastructure.

---

[12] Le document décrit notamment les problématiques d'ingress/egress filtering liées à l'utilisation potentielle des Routing Headers Type 0, avant la définition des Routing Header Type 2 proposée dans le document.

[13] *Loose and Strict Source Routing options*

[14] typiquement, les rejeter

[15] les accepter ou non en fonction de l'utilisation de MIPv6 sur le réseau

Comme dans le cas de TCP et d'autres protocoles de connexion, une répartition mesurée des messages et réponses associées a du être envisagée. Par exemple, [TA] décrit dans une optique historique les différentes étapes de sécurisation de la procédure de Binding Update (Return Routability Procedure). La complexité apparente de cette partie du protocole (Nonces, Cookies, Tokens), l'ordre des messages et leur nombre sont le résultat de longues réflexions visant à fournir une sécurité maximale pour le MN, le CN, en terme d'authentification, de prévention des DoS et de gestion des états dans les noeuds. C'est également le cas pour l'infrastructure concernant les Dénis de Service.

Sécurité dans les réseaux des participants

- ***Dans le réseau mère*** : Si tout a été mis en œuvre, suite aux recommandations de l'IESG, pour protéger l'infrastructure Internet existante, le déploiement éventuel du protocole à grande échelle est également lié aux impacts potentiels dans les réseaux des participants.
  En théorie, le HA est une cible de choix pour un attaquant. Il offre en effet un frontal sur Internet puisqu'il doit être accessible de tout point d'attachement de ses clients (il n'a pas de connaissance préalable des CoA utilisés par ses MN), mais également un point d'attachement sur un réseau interne.
  Dans les faits, la meilleure manière de considérer ce routeur est de le voir comme un concentrateur d'accès VPN. En effet, comme évoqué précédemment, la mise en œuvre d'un HA sans protection du trafic[16] ne peut être envisagée de manière sérieuse.
  Outre les extensions particulières liées à la mobilité, la problématique reste celle de la gestion de clients mobiles de type roadwarrior. Au final, en considérant les rôles de Mobile IPv6 et d'IPsec complémentaires, le rôle réel de MIPv6 dans le cadre de cette coopération consiste simplement à fournir le moyen de séparer les notions de Locator et d'Identifier evoquées précédemment.
  Les idées mises en œuvre et le travail réalisé au niveau de la différenciation des flux dans le protocole (Mobility Header, séparation des modes tunnel et transport, définition de Routing Header d'un type spécifique) fournissent les moyens de réaliser un filtrage et une protection précis.
  Dans cette optique, plusieurs types de flux sont à prendre en compte :

  1. Les flux protégés via IPsec provenant des MN (trafic IPsec protégeant la signalisation et les données des MN, montées de sessions IKE)
  2. Les flux entrants provenant des CN souhaitant contacter des MN associés au HA.

[16] La sécurisation du trafic par IPsec concerne à la fois la signalisation, mais également les données passant dans le tunnel entre le MN et le HA, même si les Security Policy pour ces types de trafics peuvent être différentes.

3. Les flux sortants provenant des MN et à destination de l'intérieur du périmètre de l'entreprise ou du domaine considéré.

4. Ces mêmes flux mais à destination de clients externes.

En pratique, la politique de sécurité du réseau mère impacte de manière directe le type de connexions que le noeud peut initier/recevoir. En entreprise, dans un premier temps, il est vraisemblable que le HA ne pourra pas être contacté par des CN externes, limitant ainsi l'intérêt de MIPv6 à la mise en place de connections avec des éléments du réseau interne (clients, serveurs, voire autres MN de l'entreprise). Hors contexte entreprise, il est possible que le déplacement progressif des éléments de sécurité (firewall, antivirus) sur les postes clients rende possible les réseaux ouverts dans lesquels le HA acceptera du trafic entrant pour ses clients. Le niveau de fonctionnalité est clairement lié au niveau de sécurité souhaité et aux objectifs à atteindre.
Pour autant et indépendamment des décisions prises concernant le filtrage, la complexité des protocoles rencontrés (Mobile IPv6, IKE[17], IPsec) pose deux problèmes majeurs :

– Le manque de maturité des implémentations : même si les démons IKE ne subissent pas des évolutions extrêmement importantes[18], que les piles IPsec ne sont également quasiment pas modifiées, le volume de code apporté par Mobile IPv6, la complexité des échanges assurent la découverte à venir de failles critiques. Pour contrebalancer ce point, il faut replacer le déploiement éventuel d'IPv6 en général et de solutions basées sur MIPv6 dans le temps. Lorsque ceci arrivera, les piles auront quelques années de maturité derrière elles.
– Les erreurs de configuration associées aux relations entre MIPv6, IPsec et IKE. Comme pour le point précédent, l'amélioration du support et l'expérience gagnée sur l'utilisation du protocole seront des points de passage obligés.

- ***Dans le réseau d'accueil*** : dans le réseau d'accueil, les possibilités d'impacts sont réduites, aucun déploiement spécifique d'éléments d'infrastructure ne venant potentiellement modifier la sécurité du réseau.
  Les seuls impacts potentiels sur le réseau sont liés à l'éventuelle mise en place de règles de filtrage pour autoriser IPsec, les Destination Options Header - Home Adress Option en entrée et les Routing Header Type 2 en sortie.

[17] Si le keying statique doit être supporté dans MIPv6, le Keying dynamique n'est qu'optionnel.
[18] Elles concernent majoritairement la prise en compte de l'extensions PF_KEY MIGRATE

Pour les Routing Header Type 2, le choix d'un type spécifique, la limitation à une adresse encapsulée et la portée réduite aux MN permettent un filtrage efficace et une utilisation sans crainte sur le réseau d'accueil.
De la même manière, la prise en compte du contenu de l'option HAO est intrinsèquement liée à l'implémentation et à l'activation du mode HA ou CN sur les entités du réseau d'accueil. Les deux bits de poids fort du type de l'option prenant la valeur 1, le comportement adopté par un hôte ne comprenant pas l'option consiste à rejeter le paquet, comme spécifié dans [RFC2460]. De plus, les gardes-fous placés sur son utilisation par le destinataire amènent aux mêmes conclusions que précédemment.
L'autorisation d'utiliser IPsec en sortie d'un réseau reste le point le plus controversé. En pratique, il semble évident, que les réseaux d'accueils desquels les invités auront accès seront séparés du coeur de l'entreprise. Dans les faits, l'exfiltration de données étant possible dès qu'une communication vers l'extérieur est réalisable, à travers proxy HTTP/HTTPS, sur DNS, les arguments associés à la capacité à surveiller les flux sortants ne tiennent déjà plus. Contrairement à TLS qui semble admis, peut-être du fait de son utilisation "grand public" une barrière doit encore être franchie pour le déploiement d'IPsec.
Du point de vue de la sécurité, de nouveaux deploiements de réseaux d'accueil séparés et ouverts sont envisageables. Ceux-ci permettent de laisser une liberté importante aux invités tout en assurant qu'aucune attaque ne puisse être montée depuis ceux-ci en utilisant le préfixe fourni par le site d'accueil. Dans cette optique, Mobile IPv6 peut servir de compromis au sein d'un réseau d'accueil pour permettre l'imputation des actions effectuées au préfixe du réseau mère du MN.

- ***Dans le réseau du correspondant*** : Dans le réseau du correspondant, les problématiques sont similaires à celles rencontrées dans le réseau d'accueil des noeuds mobiles. Elles sont même identiques dans le cas où le CN est également MN.
  Un élément est tout de même accentué lorsqu'on considère le cas du CN. Etant contacté par le MN, il doit être accessible depuis l'extérieur. Comme évoqué précédemment, la problématique de filtrage intermédiaire apparait peut-être moins sur les réseaux domestiques avec la mise en place d'éléments de protection directement sur les postes client.
  Dans un contexte plus restrictif, les correspondants des MN peuvent se voir limités au périmètre d'un domaine de confiance (autres noeuds de l'entreprise). Encore une fois, les choix effectués dépendent de manière directe des besoins de sécurité évalués.

4.2 Vulnérabilités côté client

L'utilisation de Mobile IPv6 sur un poste nomade peut poser de sérieux problèmes de confidentialité et d'anonymat. En effet, le noeud mobile étant toujours joignable à la même addresse, un attaquant peut ainsi harceler le

MN sans se soucier de ses déplacements. En fonction de la technologie d'accès du MN, un DoS peut donc avoir, à moindre coût pour l'attaquant, un effet dévastateur pour le noeud mobile.

Si l'on considère que le MN utilise un lien à faible débit, comme GPRS, l'attaquant pourra facilement empêcher le MN de communiquer en saturant son lien descendant. De la même façon, en considérant une technologie d'accès dans laquelle la facturation est basée sur le volume des données, l'attaquant peut nuire financièrement au MN. Dans ce type de configuration, la réception de trafic non solicité peut également représenter une menace envers le MN.

Afin de se prémunir de ce type d'attaques, il est envisageable de s'appuyer sur le réseau mère ainsi que sur le HA. Celui-ci possède vraisemblablement un lien plus rapide que le MN. Il sera donc plus à même de stopper le DoS et de prendre les messures adéquates pour en limiter les effets. Il est de plus possible d'effectuer du filtrage au niveau du HA afin de n'autoriser à destination du MN que les paquets en relation avec des connexions initiées par le MN.

Lorsqu'un noeud mobile désire effectuer une optimisation de route avec un CN présent dans un Hotspot non protégé, un attaquant peut compromettre les communications entre le CN et le MN. Il peut par exemple intercepter les messages échangés dans la procédure de Return Routability, et injecter de faux Binding Update. Bien que potentiellement dangereuse, cette attaque n'est pas engendrée par l'utilisation de Mobile IPv6 et reste similaire en terme d'impacts aux attaques que peut effectuer un attaquant présent sur le même lien que sa victime.

5 Retour sur les apports et contraintes d'IPsec

Dans de nombreux protocoles, l'argument de sécurité brandi est souvent l'utilisation proposée d'IPsec. Cet argument souvent fallacieux ne prend pas en compte la réalité des faits concernant IPsec, ses possibilités et les contraintes rencontrées.

Pour ce qui concerne Mobile IPv6, la **nécessaire** protection du trafic de signalisation entre le MN et le HA via IPsec n'est pas juste une proposition faite à la légère. Elle provient d'une véritable réflexion et de la disponibilité d'un environnement de mise en œuvre adapté. Outre l'intégration d'IPsec dans le standard, le sujet est également détaillé dans deux documents annexes ([RFC3776], [MIGRATE]).

Sous IPv6, de nombreux points favorisent la mise en œuvre d'IPsec. Les deux principaux sont certainement l'adressage global et la nécessaire implémentation du protocole au niveau des piles réseaux IPv6.

Le premier permet la mise en place de connexions sécurisées de bout en bout, sans subir la NAT ([RFC3947], [RFC3715][19], [RFC2709]).

Dans les cas rencontrés dans MIPv6 :

- l'utilisation du mode tunnel (pour la sécurisation du tronçon entre le MN et son HA lorsque celui-ci dialogue avec des CN) est des plus classiques. Les adresses des extrémités du tunnel sont la CoA au niveau du MN et l'adresse du HA.
  Il est à noter que le MN n'est pas vu comme un véritable roadwarrior bien que son adresse soit a priori inconnue du HA. Dans les faits, même si la SA du Home Agent vers le MN utilise la CoA courante comme destination, elle peut être initialisée à la valeur de la Home Address du noeud. Ensuite, cette adresse est mise à jour dans la SAD lorsque le noeud mobile se déplace (lors de la phase de "Binding"). La problématique de modification de la CoA lors d'un déplacement du noeud est traitée par la suite.

- l'utilisation du mode transport pour la sécurisation des Binding Update pourrait sembler problématique a priori, les paquets émis par le MN possédant une adresse source volatile mais compatible avec le réseau d'accueil (CoA). Dans les faits, le paquet est émis avec un header "Destination Options Header - Home Address Option" : une étape intermédiaire à la réception du paquet permet de replacer cette adresse dans le champ Destination Address du header IPv6. Au final, celle-ci est utilisée pour référencer la Security Policy associée. La protection appliquée au paquet est donc toujours réalisée avec la Home Address du noeud comme IP source, indépendamment des déplacements et ainsi des CoA rencontrées.

- l'utilisation du mode transport pour la sécurisation des Binding Ack (ou Binding Error) émis par le HA en réponse aux Binding Update reçus suit le même genre d'étape de routage intermédiaire. Cette fois-ci, l'adresse destination présente dans le paquet durant le routage est la CoA du MN, mais elle est échangée avec la Home Address de celui-ci présente dans un Routing Header Type 2.
  Dans ce cas, comme dans celui vu précédemment, bien que la phase de routage se réalise temporairement entre la CoA et l'adresse du HA, les destinataires finaux (donc ceux concernés par la Security Policy) sont bien la Home Address et l'adresse du Home Agent.

L'un des principaux problèmes que subit Mobile IPv6 et plus précisément IPsec dans la sécurisation du protocole tient en fait à une particularité de l'adres-

[19] comme évoqué dans le document, "The result is that IPsec-NAT incompatibilities have become a major barrier in the deployment of IPsec in one of its principal uses"

sage IP. En effet, une adresse IP est utilisée à la fois comme identifiant de routage et comme identifiant de noeud[20].

Pour cette raison, lorsque le noeud mobile change de réseau d'accueil, son identifiant de routage (sa CoA) change. Il devient nécessaire pour lui de mettre à jour les informations connues de ses correspondants ; HA et éventuellement, CN.

Ce problème touche en fait les SA IPsec négociées entre le MN et son HA et, dans le cas d'utilisation d'IKE la relation entre le démon IKE et la couche gérant Mobile IPv6. Seules les SA en mode tunnel sont impactées[21]. Elles font en effet intervenir la CoA du MN. Les SA en mode transport utilisant la Home Address du noeud pour le référencement et comme adresse des paquets ne sont pas impactées. Elles profitent des Routing Header Type 2 et de l'option HAO du Destination Options Header.

Une vision d'assez haut niveau de l'utilisation d'IPsec pour protéger Mobile IPv6 est fournie dans [RFC3775]. Les détails concernant la sécurisation via IPsec du lien entre le MN et son HA sont traités spécifiquement dans [RFC3776]. [MIGRATE] décrit une extension de l'interface PF_KEYv2 permettant la modification d'adresse au sein d'une SA en mode tunnel et permettant la survie de celle-ci aux déplacements. Pour des raisons de concision, le lecteur curieux est renvoyé vers ces documents pour les détails techniques.

Il est à noter qu'actuellement, les problématiques de protection via IPsec des relations entre le MN et le CN ne sont pas normalisées.

6 Implémentations

Mobile IPv6 étant standardisé ([RFC3775], [RFC3776]) depuis Juin 2004, plusieurs implémentations sont maintenant disponibles. Leur niveau de support varie principalement concernant l'intégration des mécanismes de sécurité permettant la protection du trafic de signalisation.

Un autre point de comparaison concerne les capacités de filtrage des différents systèmes vis-à-vis du trafic IPv6 en général et celui lié à Mobile IPv6 en particulier[22].

Cette section détaille ces points pour chacun des systèmes majeurs et des implémentations associées.

6.1 *BSD : SHISA

SHISA[23] est l'implémentation de Mobile IPv6 pour les plateformes *BSD. Il tire son nom d'une statue de lion ornant les toits de l'île d'Okinawa au sud

[20] il s'agit d'un des problèmes traités dans les groupes de travail sur le multihoming, notamment [monami6]

[21] Celles protégeant le trafic entre le MN et le CN via le HA, sur le tronçon entre le MN et le HA

[22] Il n'est pas abordé ici.

[23] `http://www.mobileip.jp`

de l'archipel nippon afin de protéger les habitations. Son développement a été effectué dans le cadre du projet WIDE[24] qui fut déjà à l'intiative de KAME[25], l'implémentation d'IPv6 faisant référence.

SHISA implémente Mobile IPv6 [RFC3775,RFC3776] ainsi que NEMO Basic Support [RFC3963]. Il permet donc de déployer des MN, des HA, des CN ainsi que des Mobile Router, MR. Bien que disponible pour les trois principaux BSD, OpenBSD, NetBSD, et FreeBSD, il est recommandé de le deployer en utilisant FreeBSD 5. Ce projet est désormais partie intégrante de KAME et peut être récupéré avec ses snapshots hebdomadaires.

En ce qui concerne IPsec, il est possible de protéger le trafic de signalisation et de données entre le MN et le HA à l'aide du static keying. Le dynamic keying est en cours d'implémentation mais ne sera plainement fonctionnel qu'avec le support de IKEv2 [RFC4306,MIP6IKEv2] dans racoon2.

6.2 Linux : MIPL

Sous Linux, le support de Mobile IPv6 est disponible sous forme d'un patch noyau[26] et d'une partie userland[27]. Le projet porte le nom MIPL : *Mobile IPv6 for Linux*. Les fonctionnalités de MN, CN et HA sont supportées.

Pour ce qui est du rôle de routeur IPv6 du HA, et notamment l'émission des *Routing Advertisement*, le logiciel **radvd** intègre maintenant dans sa version courante l'ensemble des extensions associées à MIPv6[28].

MIPL évoluant maintenant depuis quelques années (la version courante est la version 2.0), le support d'IPsec est actuellement disponible, au moins basiquement. Il permet la définition des flux à protéger sans avoir à spécifier l'ensemble des Security Policies à mettre en place, comme présenté figure 12.

Au niveau du noyau, en ce qui concerne IPsec, MIPL[29] ajoute notamment le support de l'API PF_KEY MIGRATE permettant la modification de la CoA utilisée dans les SA suite à l'émission et la réception d'un Binding Update.

Pour le keying dynamique, **racoon** offre un mode permettant le support de MIPv6 (option `support_proxy`). Ceci permet comme précisé dans [RFC3776], d'utiliser la CoA pour les échanges IKE tout en négociant les SA en utilisant la Home Address.

Dans les faits, le fonctionnement est encore balbutiant et les relations entre les trois composants — le démon IKE, MIPL et la SADB — sont encore incertaines.

[24] `http://www.wide.ad.jp`
[25] `http://www.kame.net`
[26] Actuellement pour 2.6.15
[27] Les deux étant téléchargeables sur `http://www.mobile-ipv6.org`
[28] permettant notamment d'utiliser des valeurs inférieures à certains timers utilisés par Neighbor Discovery
[29] plus généralement, il apporte la prise en charge des extensions des mobilité (Routing Header Type 2 et option HOA dans les Destination Option Header)

```
...
IPsecPolicySet {
        HomeAgentAddress ;
        HomeAddress /64;

        IPsecPolicy HomeRegBinding UseESP;
        IPsecPolicy TunnelMh UseESP;
}
...
```

Fig. 12. Un exemple de définition de la protection via IPsec de certains échanges sous MIPL.

Même si les cas simples fonctionnent, la gestion complète du keying dynamique avec certificats et la stabilité de l'implémentation restent encore à assurer.

6.3 Windows

En 2002, Microsoft mettait à disposition une version de test d'une implémentation Mobile IPv6 (suivant le draft 12 de [RFC3775]), faisant suite à un travail commun avec l'université de Lancaster.

Depuis le service pack 1, Windows XP intègre une implémentation offrant un support limité de MIPv6[30]. C'est également le cas de Windows Server 2003.

Le site de Microsoft annonce l'existence d'une version d'évaluation (Technology Preview) offrant l'ensemble des fonctionnalités de CN, MN et HA pour différentes versions de Windows. Sans raison évoquée, celle-ci est indisponible.

En ce qui concerne Windows Vista, le support de Mobile IPv6 n'est pas prévu à la sortie de cet OS mais sera disponible par la suite sous forme d'extension.

En pratique, la version disponible sous Windows XP n'est pas utilisable : elle n'implémente que la fonctionnalité de CN et suit une ancienne version du draft.

Pour ce qui est des CTP, Community Technology Preview, l'ensemble du code relatif à Mobile IPv6 a été désactivé (plus d'accès possible aux options de configuration par `netsh`).

Si les équipes de Microsoft travaillent actuellement sur IPv6 dans le cadre de la "Next Generation TCP/IP Stack", elles focalisent principalement leurs efforts sur d'autres technologies que Mobile IPv6 comme Teredo, le firewall IPv4/IPv6, le support complet d'IPsec, ou bien encore DHCPv6.

[30] uniquement la fonctionnalité de Correspondent Node telle que décrite dans le draft 13 de [RFC3775]

6.4 Cisco IOS

Les versions courantes d'IOS offrent un support d'IPv6, de nombreuses fonctionnalités ayant été progressivement ajoutées au fil des ans. Les extensions nécessaires à l'utilisation de Mobile IPv6 sont maintenant disponibles[31].

En pratique, les fonctionnalités de CN et MN ne sont pas disponibles sur IOS. Le système étant développé pour des routeurs, la non-disponibilité de ces fonctionnalités se justifie facilement.

Concernant la sécurisation, un des manques majeur qui limite l'intéret d'un Routeur Cisco en tant que Home Agent concerne la protection via IPsec du trafic entre le Home Agent et ses MN. Les mécanismes de sécurité décrits dans [RFC3776] ne sont pour le moment pas implémentés.

Aucune date n'est avancée sur la disponibilité de cette fonctionnalité indispensable à des déploiement sérieux.

Néanmoins, il semble que des développements soit en cours, poussés par des opérateurs de téléphonie mobile (notamment asiatiques), de manière à déployer dans des infrastructures spécifiques (contexte 3GPP2) des solutions de sécurité plus adaptées, comme celle définie par [RFC4285].

Finalement, les développement relatifs à Mobile IPv6 dans IOS évoluant avec les demandes du marché, le support actuel présente beaucoup moins d'intérêt que celui fournit par les équivalents disponibles dans le monde libre[32].

7 Conclusion

7.1 Sécurité

L'utilisation d'une adresse IPv6 en dehors de son site d'origine pose des contraintes complexes, aussi bien au niveau fonctionnel que concernant la sécurité. Après une longue période de gestation, Mobile IPv6 est depuis juin 2004 un protocole normalisé par l'IETF.

L'intégration de nombreux mécanismes de protection originaux a permis de prendre en compte les problématiques de sécurité sans pour autant restreindre les possibilités d'utilisation. La protection des communications entre le noeud mobile et son réseau mère s'appuyant sur IPsec, elle profite des facilités offertes au protocole de sécurisation dans le cadre d'IPv6 (connexion de bout en bout, disparition de la NAT).

En pratique, IPv6 est actuellement en phase de déploiement, même si aucune date concernant sa mise en œuvre massive ne peut être avancée. Son intégration et activation par défaut dans les prochaines version du système d'exploitation de Microsoft, comme c'est déjà le cas sur Mac OS, Linux et certains BSD, permettra certainement de pousser son déploiement.

Concernant Mobile IPv6, sa standardisation relativement récente et le déploiement d'IPv6 retardé par les mécanismes de NAT induit des

[31] disponibilité de la fonctionnalité Home Agent dans les 12.3(14)T, 12.4, 12.4(2)T et améliorations des ACL IPv6 depuis la 12.4(2)T

[32] as in beer

implémentations commerciales pour le moment assez limitées :

- Cisco n'inclut pour le moment pas la sécurisation via IPsec du lien MN-HA et travaille sur des mécanismes spécifiques à des infrastructures d'opérateurs mobiles ;
- Microsoft intègre une implémentation basée sur un draft dépassé dans Windows XP mais annonce MIPv6 sous forme d'extension après la sortie de Vista ;
- Apple ne prévoit pas l'intégration du protocole pour Léopard, mais le système étant basé sur FreeBSD, son portage par la suite bénéficiera certainement des avancées sur ce système.

Dans le monde libre, les BSD et Linux intègrent, pour le moment de manière externe, le code pour faire fonctionner le protocole. Même si la gestion de la protection via IPsec n'est pas encore complète, se limitant globalement à une gestion de clé statique, elle avance assez rapidement.

La volonté d'un déploiement à grande échelle du protocole et les objectifs importants concernant la protection des réseaux (Internet et des participants) et des clients ont amené à la mise en place de mécanismes de sécurité adaptés aux contraintes et utilisables (Return Routability Procedure).

L'utilisation d'IPsec/IKE a été étudiée de manière poussée, pour les relations entre le MN et le HA dans son réseau mère. Les extensions nécessaires à la gestion complète de la migration des extrémités de SA en mode tunnel sont en cours de normalisation [MIGRATE] et de tests.

Si les solutions proposées semblent robustes, un retour d'expérience reste encore à gagner sur le sujet :

- La stabilisation des relations entre les éléments présents dans les piles est en cours — au moins dans le monde libre — en attendant un déploiement éventuel à plus grande échelle après celui, progressif, d'IPv6.
- Certaines problématiques liées à la sélection d'adresse source — CoA ou Home Address – ne sont pour le moment pas résolues.
- De manière générale, le problème épineux de la séparation des rôles de "Locator"/"Identifier" pour l'adresse IP auquel MIPv6 apporte une solution est encore un sujet de recherche. Les questions de sécurité également.
- Concernant la mise en œuvre dans le cadre d'infrastructures spécifiques, comme celles des réseaux d'opérateurs mobiles, sur des équipements aux capacités plus limitées (puissance, batterie), d'autres solutions sont également en train de voir le jour.

Le point positif sur ce sujet est que le protocole bénéficie pour acquérir sa maturité du temps nécessaire à la mise en place progressive d'IPv6. Eventuellement, il fera partie des Killer Apps qui pousseront le déploiement d'IPv6.

7.2 Limitations

Dans le document, la sécurité de Mobile IPv6 a été décrite et analysée. Pour des raisons de concision, certains points concernant des mécanismes annexes ont été laissés de côté comme la protection des messages Mobile Prefix Solicitation ou Mobile Prefix Advertisement. D'autres, requiérant trop de détails, comme la procédure de Return Routability ou certains éléments sur IPsec/IKE ont été décrits de manière succinctes. Comme toujours, le diable étant dans les détails, les références bibliographiques permettront au lecteur curieux de répondre aux questions ouvertes.

Certains auraient certainement attendu de ce papier une partie comparative entre MIPv6 et MIPv4 [RFC3344]. La version IPv4 du protocole étant fondamentalement différente dans son fonctionnement, notamment du fait des problématiques dues à la NAT, elle n'a jamais été déployée à grande échelle. Egalement pour des raisons de concision, mais aussi de clarté, il a volontairement été décidé de ne pas l'évoquer pour se focaliser sur la version IPv6.

Le sujet de la mobilité a été restreint dans le document à Mobile IPv6, protocole adapté aux clients mobiles. D'autres protocoles comme NEMO [RFC3963] sont actuellement développés en parallèle, basées sur MIPv6, et permettant la mobilité de réseaux complets. Même si certaines contraintes de sécurité et donc certaines solutions apportées sont communes à celles étudiées ici, d'autres parties divergent sensiblement, imposant certains changements et restrictions. De la même manière, FMIPv6 [RFC4068] et HMIPv6 [RFC4140] n'ont pas non plus été abordés ici.

7.3 Intégration de Mobile IPv6 dans les VPN

Le lecteur attentif aura certainement remarqué que la sécurisation des communications entres le MN et ses correspondants a pour but de fournir un niveau équivalent à celui que le noeud mobile pourrait avoir dans son réseau mère et que le correspondant peut avoir vis-à-vis d'un client fixe. Peut-on faire mieux ?

En pratique, la possibilité, dans le cadre du mode optimisé de dialoguer de manière directe avec un correspondant en utilisant sa Home Address, sans pénalité de routage, offre de nouvelles perspectives. La mise en place de sessions sécurisées entre les noeuds mobiles d'un même réseau de confiance (domaine d'adressage, PKI), sans passage pénalisant par le réseau mère est une possibilité attractive. Elle permettrait la mise en œuvre de véritables VPN transparents, au dessus du réseau de routage IPv6, s'affranchissant d'une architecture en étoile pénalisante comme c'est le cas aujourd'hui.

Références

[RFC1958] B. Carpenter **"Architectural Principles of the Internet"** June 1996, informational

[RFC1883] S. Deering, R. Hinden **"Internet Protocol, Version 6 (IPv6) Specification"**. December 1995

[RFC2460] S. Deering, R. Hinden **"Internet Protocol, Version 6 (IPv6) Specification"**. December 1998

[RFC2461] **"Neighbor Discovery for IP Version 6 (IPv6)"**. December 1998, Standards Track

[RFC2709] P. Srisuresh **"Security Model with Tunnel-mode IPSec for NAT Doamins"** October 1999, Informational

[RFC2827] P. Ferguson, D. Senie **"Network Ingress Filtering : Defeating Denial of Service Attacks which employ IP Source Address Spoofing."** May 2000, Best Current Practice

[RFC3344] C. Perkins **"IP Mobility Support for IPv4"** August 2002, Standards Track

[RFC3439] R. Bush, D. Meyer **"Some Internet Architectural Guidelines and Philosophy"** December 2002, Informational

[RFC3704] F. Baker, P. Savola **"Ingress Filtering for Multihomed Networks"** March 2004, Best Current Practice

[RFC3715] B. Aboba, W. Dixon **"IPsec-Network Address TRanslation (NAT) Compatibility"** March 2004, Informational

[RFC3775] J. Arkko, V. Devarapalli and F. Dupont **"Mobility Support in IPv6"**. June 2004, Standards Track

[RFC3776] J. Arkko, V. Devarapalli and F. Dupont **"Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents"**. June 2004, Standards Track

[RFC3947] T. Kivinen, B. Swander, A. Huttunen and V. Volpe **"Negotiation of NAT-Traversal in the IKE"**. January 2005, Standards Track.

[RFC3963] V. Devarapalli, R. Wakikawa, A. Petrescu, P. Thubert **"Network Mobility (NEMO) Basic Support Protocol"**. January 2005, Standards Track.

[RFC4068] R. Koodli, Ed.**"Fast Handovers for Mobile IPv6"** July 2005, Experimental

[RFC4140] H. Soliman, C. Castelluccia, K. El Malki, L. Bellier **"Hierarchical Mobile IPv6 Mobility Management (HMIPv6)"** August 2005, Experimental

[RFC4225] P. Nikander, J. Arkko, T. Aura, G. Montenegro, E. Nordmark **"Mobile IP Version 6 Route Optimization Security Design Background"** December 2005, Informational

[RFC4285] A. Patel, K. Leung, M. Khalil, H. Akhtar, K.Chowdhury **"Authentication protocol for Mobile IPv6"** January 2006, Informational

[RFC4306] C. Kaufman **"Internet Key Exchange (IKEv2) Protocol"** December 2005, Standards Track

[RHHASec] P. Savola **"Security of IPv6 Routing Header and Home Address Options"** December 2002, draft-savola-ipv6-rh-ha-security-03.txt

[SALTZER] J.H. Saltzer, D.P. Reed, D.D. Clark **"End-To-End Arguments in System Design"** ACM TOCS, Vol 2, Number 4, November 1984, pp 277-288

[TA] Tuomas Aura **"Mobile IPv6 Security"** Microsoft Research Ltd

[MIGRATE] S. Sugimoto, F. Dupont and N. Nakamura **"PF_KEY Extensions as an Interface between Mobile IPv6 and IPsec/IKE"** Internet-Draft, draft-sugimoto-mip6-pfkey-migrate-02, Expires September 6, 2006.

[MIP6IKEv2] V. Devarapalli, F. Dupont **"Mobile IPv6 Operation with IKEv2 and the revised IPsec Architecture "** Internet-Draft, draft-ietf-mip6-ikev2-ipsec-05.txt

[monami6] **"IETF MONAMI6 (MObile Nodes And Multiple Interfaces in IPv6) Working Group"** `http://www.nautilus.org/ietf`