N° D'ORDRE 06/2005-M/IN

REBUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE D'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE DES SCIENCES ET DE LA TECHNOLOGIE

« HOUARI BOUMEDIENE »

FACULTE D'ELECTRONIQUE ET D'INFORMATIQUE

MEMOIRE

Présenté pour l'obtention du diplôme de MAGISTER

En : INFORMATIQUE

Spécialité : Programmation et Systèmes

Par : CHENAIT MANEL

SUJET

La sécurité dans le protocole Mobile IP: Un nouveau schéma d'authentification pour l'environnement Mobile IP

Soutenu Le 02/07/2005 , devant le jury composé de :

Mr. A. AISSANI	Professeur, USTHB,	Président
Mr. N. BADACHE	Professeur, USTHB,	Directeur de thèse
Mme Z. ALIMAZIGHI	Professeur, USTHB,	Examinateur
Mr S. LARABI	Maître de conférences, USTHB,	Examinateur
Mr. D. TANDJAOUI	Attaché de recherche, CERIST,	Co-rapporteur

Dédicaces

Je dédie ce travail à tous ceux qui me sont chers…

Ma mère;
Mon père;
Mes frères et sœurs;
Tous mes amis.

Manel

Remerciements

Je tiens à remercier mon Dieu, le tout puissant, de m'avoir donné le courage et la patience jusqu'à l'achèvement de ce travail.

Je tiens à remercier mon directeur de thèse D^R Nidjib BADACHE, de m'avoir fait confiance en me proposant ce sujet.

J'exprime ma profonde reconnaissance et mes vifs remerciements à mon encadreur M.Djamel TANDJAOUI pour les lectures attentives de mes rapports et pour les critiques et suggestions qui ont été d'un grand apport pour la finalité de ce travail.

Je remercie M^{me} A. AISSANI, M^{me} Z. ALIMAZIGHI et M. S.LARABI d'avoir accepté de juger ce travail.

J'adresse également mes sincères remerciements à Madame Hassina ALIANE, responsable du laboratoire de logiciels de base (C.E.R.I.S.T), pour sa compréhension, et pour tous les moyens qu'elle a mis à ma disposition.

Un grand MERCI, aux membres de ma famille et à mes très chers amis pour leurs encouragements, leur patience et leur amour.

Sommaire

CHAPITRE V: Démarche et résultats d'analyse.

Introduction générale

Les réseaux IP ont été mis en place initialement par l'interconnexion d'hôtes fixes reliés par un réseau filaire. L'objectif était d'offrir une communication rapide à haut débit. De nos jours, on essaye de plus en plus de rendre ces équipements IP mobiles. Différentes technologies de communication sans fil (IEEE 802.11, HiperLAN/2) sont en train de voir le jour. Elles offrent des débits suffisants pour la connexion d'hôtes mobiles à des réseaux IP.
La mobilité dans l'Internet a été introduite par l'organisme de standardisation IETF (*Internet Engineering Task Force*). Cet organisme s'est principalement penché sur la gestion des déplacements d'un ordinateur mobile sur l'Internet, c'est-à-dire du passage d'un réseau à un autre réseau, ce qui a permis de définir plusieurs protocoles parmi lesquels le protocole Mobile IP.

Mobile IP est un protocole standard placé au-dessus du protocole IP qui offre une simple gestion et rend la mobilité transparente aux applications. Néanmoins, autoriser une machine à se connecter sur un réseau puis à se déplacer de réseau en réseau entraîne de nombreux risques de sécurité: vol de sessions, l'écoute, la localisation, etc.
Il est donc indispensable que les acteurs sachent s'authentifier et s'identifier les uns les autres.

Beaucoup de travaux ont été proposés pour améliorer la sécurité de l'authentification du protocole Mobile IP[RFC2002][ZAO97][RFC2977], mais qui restent insuffisants en matière de sécurité et de performance. L'authentification standard [RFC2002] considère la pré-existence des liens de confiance entre les acteurs Mobile IP. Cette solution s'est avérée insuffisante à cause de la non scalabilité et l'absence d'une entité digne de confiance qui se préoccupe de la gestion des clés entre ces acteurs. Zao [ZAO97] a proposé l'utilisation des cryptosystèmes à clé publique pour résoudre le problème de la scalabilité de l'authentification standard: chaque entité possède une paire de clé publique et privée utilisée pour chiffrer et signer. C'est une solution qui garantit essentiellement la non-répudiation, mais elle reste théorique en particulier pour les nœuds mobiles puisque les algorithmes à clé publique nécessitent une grande puissance en capacité et en temps de calcul.
Le schéma d'authentification Mobile IP/AAA [RFC2977] est venu remédier à l'absence de l'outil de gestion de clés dans l'authentification standard, le home server (AAAH) est devenu l'entité responsable de la gestion sécurisée des clés. Cette entité se charge de générer et de distribuer les clés de communication grâce aux associations de sécurité statiques existantes entre le AAAH et les acteurs Mobile IP. Néanmoins, ce mode d'authentification comporte essentiellement deux points faibles: Le premier est la centralisation de l'outil de gestion de clés ; dans ce schéma il y a que le home server qui se charge de la gestion sécurisée des clés de tout le système (génération, chiffrement, déchiffrement, distribution) ce qui augmente la charge sur ce serveur. De plus si jamais cette entité tombe en panne tout le système sera exposé aux attaques. Le second problème apparaît lorsque le nœud mobile effectue un intra domain handover

(migration vers un foreign agent dans le même domaine que l'ancien), dans ce cas précis le nœud mobile effectue l'authentification des entités en gardant *les anciennes clés de communication* (déjà partagées lors d'une ancienne session MIP/AAA). Cela pose un problème en cas où les clés sont découvertes ou cassées.
Dans ce travail, nous proposons un nouveau schéma d'authentification pour Mobile IP. Ce schéma introduit des améliorations à l'ancien modèle d'authentification Mobile IP/AAA. Nous avons opté de continuer l'exploit et l'amélioration de ce schéma essentiellement parce qu'il est renforcé en matière de sécurité par rapport aux autres schémas grâce à la collaboration des structures AAA qui se préoccupent des opérations cryptographiques indépendamment des acteurs du protocole. Notre schéma est composé de deux étapes essentielles: la certification des serveurs locaux et la gestion des clés à partir de ces serveurs. L'idée de base est de re-générer de nouvelles clés pour l'authentification même lors d'un intra domaine handoff; les acteurs Mobile IP partagent trois nouvelles clés de communication à chaque déplacement du mobile dans le même domaine. De cette manière, on évite le grand risque en l'usages des anciennes clés, en particulier si elles sont découvertes ou cassées. Ces clés seront régénérées par les serveurs locaux certifiés au lieu du home server, de cette manière le flux de messages de demande et de réponse d'enregistrement ne sera pas transmis jusqu'au domaine mère, ce qui diminue considérablement la latence du handover.

Ce document est composé de cinq chapitres :
Le premier chapitre est une présentation générale des caractéristiques des environnements mobiles à savoir la connexion sans fil et la mobilité.

Le second a été principalement axé sur la mobilité IP ainsi que le fonctionnement du protocole Mobile Ipv4 (la découverte des agents, l'enregistrement et le tunneling), on y trouve aussi une description de son successeur Mobile IPv6.

Le troisième chapitre est une étude de la sécurité du protocole Mobile IP : les différentes attaques enregistrées sur ce protocole ainsi que les besoins de sécurité que doit assurer un système sécurisé dans un environnement mobile. Ce chapitre contient aussi les différents travaux qui ont fais l'étude de la sécurisation de la procédure d'authentification dans Mobile IP.

Le quatrième chapitre consiste à décrire le nouveau schéma d'authentification (Local MIP/AAA) que nous proposons.

Et enfin le cinquième et dernier chapitre est une étude de performance du protocole proposé par analyse. Dans ce chapitre, on trouve une description de la démarche d'analyse et une présentation des résultats obtenus.

Chapitre I *Généralités sur les environnements mobiles.*

1.1Introduction

Les évolutions techniques dans le développement des ordinateurs portables et le déploiement rapide de la technologie des réseaux sans fil fournissent la base pour un nouvel environnement, appelé *environnement mobile* ou *nomade*.

En utilisant conjointement ces ordinateurs portables et les médiums de communication sans fil (ondes radiofréquence, ondes lumineuses), il devient possible de rester connecté á son réseau habituel et de communiquer avec les autres machines mobiles tout en se déplaçant soi-même. Les utilisateurs mobiles sont capable de communiquer, d'accéder á l'information n'importe où et n'importe quand.

Ces développements ont cependant un prix, Les nouvelles contraintes introduites par l'environnement mobile font qu'il est nécessaire de réviser les mécanismes des systèmes répartis classiques. Ces contraintes découlent d'une part de la mobilité, qui induit que le travail ne s'exécute plus seulement sur un réseau statique mais aussi avec des machines qui se déplacent, ce qui complique considérablement les exécutions réparties. D'autre part, l'architecture des systèmes supportant des ordinateurs mobiles est différente de celle des réseaux fixes. Il peut en effet être nécessaire de supporter la notion cellule de communication sans fil (zone au sein de laquelle la communication sans fil est possible), de station support (station du réseau fixe qui a la charge d'une cellule de communication sans fil), etc. [BAG95]. De plus, les communications sans fil créent des problèmes de déconnexion, de faible largeur de la bande passante ou de besoins de communication extrêmement variables. Enfin, la nécessité de portabilité du matériel induit de nombreuses limitations et oblige à gérer la consommation d'énergie, les problèmes de stockage, etc. L'impact du nouvel environnement de calcul est donc important, tant au niveau du réseau que des applications et des systèmes.

Ce chapitre a pour but de présenter l'environnement mobile, et les principaux concepts liés à ce nouvel environnement : architecture, types de réseaux sans fil ainsi que les caractéristiques des environnements mobiles.

1.2 Architecture d'un système distribué avec sites mobiles

Le terme "*mobile*" implique être capable de se déplacer tout en restant connecté au réseau [IOA91]. Le modèle de système distribué comprenant des sites mobiles est composé de deux ensembles d'entités distincts (Figure 1.1) : les sites fixes d'un réseau de communication filaire classique et des sites mobiles [BAD95]. L'entité qui relie les deux parties, fixe et mobile, du réseau en transformant les signaux entre les deux médiums est appelé *station de support mobile (MSS – Mobile Support Station)*. Les

MSS(s) sont munies d'interface de communication sans fil et la zone géographique couverte par une *MSS* est appelée *cellule*. Tout *site mobile (MH – Mobile Host)* est initialement enregistré dans une et une seule *MSS* appelée *station d'enregistrement (ou Home base)* [ALE00]. Ceci n'empêche pas le libre déplacement de celui-ci entre les différentes cellules en qualité de 'visiteur'. Un site mobile ne peut communiquer avec d'autres entités du réseau que par l'intermédiaire d'une *MSS*. Un site mobile peut se déplacer d'une cellule á une autre cellule. Dans un tel cas, la *MSS* de l'ancienne cellule cède les responsabilités de communication du *MH* á la *MSS* de la nouvelle cellule.

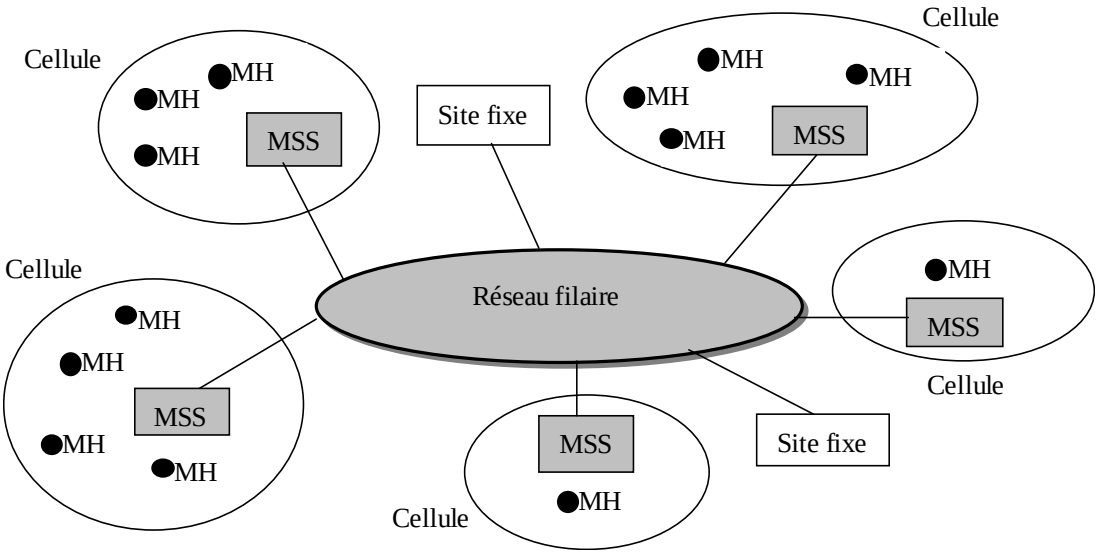

Figure 1.1: Architecture d'un système mobile.

1.3 Modes de fonctionnement des mobiles

Dans un système réparti sans ordinateur mobile, une machine ne peut travailler que dans deux modes différents, soit connectée au réseau, soit totalement déconnectée. Par contre en environnement mobile, il existe des degrés variés de déconnexion [PIT93]. Le degré de déconnexion est relatif à la largeur de bande passante disponible allouée à la liaison sans fil.

Un site mobile dispose donc de davantage de modes de travail. Actuellement, nous dénombrons quatre modes de fonctionnement différents employés sur les sites mobiles, nous les définissons dans ce qui suit:

1.3.1 Mode connecté

Dans ce cas de figure, le mobile dispose d'une connexion normale au réseau, à la manière d'une station classique. La connexion est réalisée par une interface de communication sans fil, qui fournit des débits plus faibles qu'une liaison câblée.

1.3.2 Mode partiellement connecté

Pour communiquer avec le réseau, le mobile ne dispose que d'un lien à faible largeur de bande (connexion faible ou déconnexion partielle). Cette perte de capacité de la bande passante peut être due à des perturbations, à des surcharges de la station de base qui gère les communications des mobiles se trouvant dans sa cellule.

1.3.3 Mode veille

Ce mode est utilisé par les mobiles pour préserver leurs ressources énergétiques. La vitesse de l'horloge est alors réduite et les exécutions des applications de l'utilisateur sont suspendues. La liaison avec le réseau est malgré tout maintenue, le mobile n'envoie plus de messages, mais peut encore en recevoir et repasser ainsi en mode connecté.

1.3.4 Mode déconnecté

Un site mobile peut bien sûr se trouver totalement déconnecté du réseau, à la fois parce qu'il n'y est plus physiquement relié ou parce qu'il est impossible de maintenir une connexion sans fil (volontairement, du fait de fortes interférences ou de surcharges momentanées, par exemple).

1.4 Les types de réseaux sans fil

L'évolution des réseaux sans fil tend aujourd'hui à l'établissement de chaînes de mobilité capables de répondre au besoin croissant de connexion permanente des individus et des organisations dans l'ensemble de leurs déplacements. Pour les prochaines années, se dessine un scénario de complémentarité/concurrence où différentes technologies mobiles coexisteront au profit d'usages pluriels. Une complémentarité peut être envisagée entre :

- Les WWAN (Wireless Wide Area Network) : c'est des technologies associées à des services de pleine mobilité, qui offriront une couverture quasi-universelle et une continuité de communication grâce à leur fonction de roaming. Elles peuvent être classées en deux catégories : les technologies de la téléphonie mobile telles que (HSCSD, GPRS, EDGE, UMTS, et CDMA), et les technologies satellitaires telles que Globalstar, Ellipso, Intelsat, et thuraya
- Les WLAN (Wireless Local Area Network) : un WLAN est un système de communication de données pouvant être implémenté comme l'extension ou comme l'alternative à un réseau câblé dans un bâtiment. Il utilise comme vecteur de transmission la *lumière infrarouge* ou les *fréquences radios*. Les fréquences radio sont les plus utilisées en raison d'une portée plus longue, d'une bande passante supérieure et d'une couverture plus large. Généralement la portée d'un WLAN peut aller de dix à quelques centaines de mètres. Parmi les technologies utilisées citons la Wi-Fi IEEE 802.11 et l'hiperLAN.
- Et les WPAN (Wireless Personal Area Network) : se sont des réseaux sans fil individuels de faible portée (elle peut aller de 10 jusqu'à 30 mètres), mais qu'avec le temps devraient augmenter leurs débits et leurs portées pour devenir de

véritables concurrents des WLAN. Bluetooth est une des technologies les plus utilisées pour mettre en œuvre ce type de réseau.

Notons qu'une même unité mobile, pendant son déplacement, peut utiliser différents types de technologie à différents moments selon son emplacement et ses besoins.

1.5 Les caractéristiques des environnements mobiles

L'environnement mobile offre aux utilisateurs la capacité de pouvoir se déplacer tout en restant connecté au réseau et d'être indépendants de toute localisation. Pour permettre aux utilisateurs d'un tel environnement d'avoir un accès continu aux services et aux ressources du réseau, il est nécessaire de disposer d'interfaces de communication sans fil, à la fois sur certaines stations fixes du réseau et sur les mobiles.

Cependant de nouveaux problèmes peuvent apparaître causés par les nouvelles caractéristiques du système mobile. Ceci nécessite des mécanismes spécifiques pour s'adapter aux limitations qui existent, ainsi aux facteurs qui rentrent dans le jeu lors de la conception.

1.5.1 Les connexions sans fil

Les mécanismes permettant de mettre en œuvre les connexions sans fil sont multiples, ils impliquent la prise en compte de l'environnement qui interagit avec le signal, le bloque, ou introduit du bruit, de l'écho [BAG95]. Les communications sans fil sont donc de moins bonne qualité que les communications filaires : Les largeurs de bande sont plus réduites, les besoins très variables, les taux d'erreur plus élevés et les fréquentes déconnexions. Ces facteurs peuvent augmenter les temps de latence du aux retransmissions, aux délais d'attente entre ces retransmissions, aux exécutions de protocole de contrôle d'erreur et aux courtes déconnexions. Dans un environnement sans fil, les connexions peuvent être perdues ou dégradées du fait de la mobilité et du passage de cellule en cellule, ou suite à des interférences. A la différence des réseaux fixes, le nombre de machines connectées dans une cellule peut être très variable, et des concentrations importantes d'utilisateurs dans une même cellule peuvent surcharger le réseau [FOR94].

Les points qui suivent passent en revue les différents problèmes induits par l'utilisation de communications sans fil :

1.5.1.1 Les déconnexions

Contrairement aux réseaux fixes où les déconnexions sont considérées comme des pannes réseaux, dans un environnement mobile, une déconnexion est un événement normal qui peut se produire à tout moment. Dans les réseaux mobiles, la déconnexion d'une unité peut être volontaire ou involontaire, prévisible ou soudaine, de longue ou de courte durée [NOU01].

Dans le premier cas, déconnexions volontaires, c'est l'utilisateur qui décide de se déconnecter pour une raison ou une autre. Par exemple s'il détecte une faible connectivité [CON03], ou s'il sait qu'il va rentrer dans un endroit où les connexions

sans fil sont interdites, comme dans un avion, ou pour préserver sa batterie. Dans ce cas de déconnexion, plusieurs techniques et systèmes ont été proposés pour permettre à un utilisateur de travailler tout en étant déconnecté et ceci en faisant du pré-chargement de certaines entités sur le terminal mobile, et puis d'effectuer une réconciliation dés sa reconnexion.

Le second type de déconnexion ou déconnexions involontaires, sont généralement le résultat de coupures imprévisibles, comme par exemple, lors du passage de l'utilisateur dans une zone non couverte ou devant un obstacle qui coupe le signal. Ces déconnexions fréquentes et imprévisibles restent un des grands défis de l'environnement mobile et posent plusieurs problèmes au niveau de: la récupération des données, la récupération de l'état de la session, l'exclusion mutuelle, …etc.

1.5.1.2 La faible largeur de la bande passante

L'environnement de calcul mobile est davantage concerné par les problèmes de limitation et de consommation de largeur de bande passante que l'environnement fixe ; les réseaux sans fil ayant des largeurs de bande plus petites que les réseaux filaires. Les débits crête pour les communications sans fil sur portables atteignent seulement un Mega bit par seconde pour l'infrarouge, deux Mega bits par seconde pour la radio, neuf à quatorze Mega bits par seconde pour la téléphonie cellulaire, tandis qu'un réseau Ethernet fournit dix Mega bits par seconde, ATM cent cinquante cinq Mega bits par seconde, et même un réseau sans fil non portable comme le Motorola Altair fournit 5,7 Mega bits par seconde [FOR94].

En plus de ces limitations déjà existantes, rappelons que dans une cellule, la largeur de bande est partagée entre les différents utilisateurs. La largeur de bande disponible pour chaque utilisateur offre donc un meilleur aperçu de la capacité du réseau que la largeur de bande totale.

1.5.1.3 L'hétérogénéité des réseaux

Contrairement aux systèmes répartis classiques (fixes) où les machines sont connectées une fois pour toute à un réseau donné, dans un environnement mobile, se rencontre non seulement une multitude de types de sites mobiles mais également un grand nombre de réseaux à la fois avec ou sans fil. Les mobiles se retrouvent donc à naviguer dans un environnement hautement hétérogène et de même les réseaux risquent de voir passer un grand nombre de machines de tout ordre et d'utiliser un nombre important de protocoles d'accès différents.

Les interfaces de communication sans fil risquent également de changer lors de déplacements entre l'intérieur et l'extérieur. Par exemple, les infrarouges relativement sensibles aux rayonnements solaires sont plus facilement utilisés à l'intérieur. Et même si une interface radio est conservée, les protocoles sont susceptibles de changer lorsque nous passons d'une couverture cellulaire à une couverture satellite. La gestion de cette hétérogénéité implique des traitements plus complexes en environnement mobile q'en environnement traditionnel (fixe) [FOR94].

1.5.1.4 Les risques de sécurité

Précisément puisqu'il est facile de se connecter à un lien sans fil, la sécurité des communications sans fil peut être compromise bien plus facilement que celle des communications avec fils, tout spécialement lorsque les transmissions se font sur de très grandes distances (interception, génération de messages. Il est donc nécessaire d'inclure des mécanismes sécuritaires aux réseaux sans fil.

La sécurité sur ce type de communications est d'autant plus complexe si les utilisateurs sont autorisés à traverser des domaines de sécurité de différents pays.

Les problèmes rencontrés ont donc trait à l'usurpation d'identité, au refus de service, à l'écoute ou encore à la surveillance des déplacements des mobiles [MAR93]. A la fois les mobiles et les réseaux fixes qu'ils visitent, doivent donc être protégés contre tous ces problèmes. Cette protection passe à l'heure actuelle par deux principes, l'authentification et le respect de l'anonymat (confidentialité des informations).

1.5.2 La mobilité

Dans l'environnement mobile, la mobilité est une contrainte de base qui doit être prise en compte.

En informatique mobile, trois types de mobilités sont étudiés : la mobilité des applications, la mobilité du matériel, et la mobilité des utilisateurs [BAG95] :

- La mobilité des applications : cette mobilité permet à l'utilisateur d'avoir ses applications actives quelque soit sa localisation.
- La mobilité du matériel : dans ce type de mobilité, un appareil peut se déplacer tout en étant connecté au réseau. Ce qui lui permet de changer d'adresse dynamiquement.
- La mobilité des utilisateurs : ce type de mobilité permet à un utilisateur de se déplacer et d'accéder aux mêmes services depuis différents terminaux. Dans ce cas, les adresses des machines restent fixes.

La mobilité des utilisateurs conjointe à la mobilité du matériel constitue un des cas les plus étudiés dans l'informatique mobile et engendrent plusieurs problèmes:

1.5.2.1 La migration d'adresse et la gestion de localisation

Contrairement aux réseaux fixes où chaque station a une adresse fixe par la quelle elle se connecte au réseau. Les unités mobiles durant leurs déplacements auront à se connecter via différents point d'accès et donc différentes adresses. Ce qui a un effet direct sur :

1. La conception d'algorithmes distribués qui ne peut être basé sur une topologie fixe du réseau,
2. Les protocoles de routage existants qui ne peuvent être utilisés dans les réseaux à grande mobilité,
3. Le coût de communication qui est augmenté par le coût de localisation.

Cette migration dans le réseau doit respecter les points suivants :

- La migration dans un nouvel environnement doit se faire de façon transparente à l'utilisateur et au correspondants,
- Les mêmes services réseaux doivent être conservés quel que soit le point de rattachement,
- Disposer d'une continuité de service lors d'un déplacement en cours de communication.

1.5.2.2 Les informations de localisation

Dans les réseaux traditionnels où les ordinateurs sont fixes, les informations qui dépendent de leurs localisations telles que les imprimantes disponibles, le serveur de nom (DNS), la zone horaire, …etc., sont configurées de façon statique.

L'un des problèmes de l'environnement mobile est de détecter les changements dans la localisation, et de fournir des mécanismes pour obtenir les informations de configuration appropriées à l'endroit courant. Par exemple, un utilisateur rentrant dans un espace géographique, pourra savoir quels sont les services disponibles, détecter les équipements voisins et les périphériques présents : imprimantes, fax, etc.

En plus du problème de configuration dynamique, dans certains cas, les unités mobiles nécessitent l'accès à plus d'informations relatives à leur localisation et cela pour leur servir de guide.

Le défi majeur de l'environnement mobile dans ce contexte est de garantir un accès plus flexible à ses informations sans violer l'intimité des autres utilisateurs.

1.6 Conclusion

Ce chapitre a été principalement axé sur la définition de l'environnement mobile, ses caractéristiques et ses problèmes.

Tout d'abord, nous avons pu constater que, grâce à la communications sans fil, les sites mobiles disposent de davantage modes de fonctionnement par rapport aux stations fixes. Donc, en plus des modes connecté et déconnecté, un site mobile pourra également économiser de l'énergie en passant en mode veille, ou encore subir une chute de capacité de bande passante et ne plus opérer qu'en étant partiellement connecté. Enfin, nous avons passé en revue les problèmes causés par les nouvelles caractéristiques de l'environnement mobile à savoir la sécurité, l'hétérogénéité etc.

Dans le même contexte, le chapitre suivant est une étude sur la mobilité dans Internet et particulièrement la mobilité couche IP.

Chapitre II *La Mobilité IP.*

2.1 Introduction

Aujourd'hui la mobilité s'est imposée aux utilisateurs d'un système de communication comme une nécessité impérieuse. Il n'est donc pas étonnant que tous les réseaux existants se sont donné pour mission d'intégrer de nouvelles fonctionnalités permettant de proposer ce service. Néanmoins, le routage des paquets IP est basé sur le préfixe des adresses: chaque adresse IP est en fait implicitement attachée à un réseau. Ainsi, lorsqu'un mobile change de point d'attachement tout en conservant son ancienne adresse IP, les paquets ne pourront plus lui être adressés. De plus, afin de maintenir les connexions de niveau transport, un mobile doit conserver la même adresse IP. En effet, les connexions TCP sont indexées par un quadruplet contenant les adresses IP et les ports des hôtes source et destination. Si on change l'une de ces valeurs, la connexion est coupée. Avec ces caractéristiques, il est impossible d'être mobile (de réseau en réseau) tout en conservant une connexion de type TCP/IP. Donc pour être joignable, le mobile doit avoir une nouvelle adresse dans chacun des réseaux qu'il visite.

D'une manière générale, les spécifications minimales de la solution recherchée à ce problème sont les suivantes :
- Le déplacement d'un mobile ne doit pas provoquer des coupures de connexions ouvertes.
- L'opération doit être simple à mettre en œuvre et d'un coût raisonnable .
- L'accès aux ressources doit être transparent .
- La solution doit être compatible avec le protocole IP et en particulier avec les algorithmes de routage.
- Le support de la mobilité ne doit pas nécessiter la modification de tous les routeurs.

L'IETF (*Internet Engineering Task Force*) a proposé un nouveau protocole qui répond à ces besoins : Mobile IPv4.

Mobile IPv4 est un protocole standard placé au-dessus du protocole IP, il rend la mobilité transparente aux applications et il permet au mobile de posséder deux adresses: une adresse mère fixe et une autre temporaire qui change à chaque changement de point d'attachement. [RFC2002]
L'objectif de ce chapitre est d'étudier la mobilité IP avec le protocole Mobile IPv4, nous allons donc présenter ses acteurs ainsi que les étapes essentielles qui jalonnent son fonctionnement, nous allons présenter ensuite son successeur le protocole Mobile IPv6 , et ces fonctionnalités supplémentaires mises en places.

2.2 Le protocole IP

Le protocole IPv4 fait partie de la couche Internet de la suite de protocoles TCP/IP. C'est un des protocoles les plus importants d'Internet car il permet l'élaboration et le transport des datagrammes IP (les paquets de données), sans toutefois en assurer la "livraison". En réalité le protocole IP traite les datagrammes IP indépendamment les uns des autres en définissant leur représentation, leur routage et leur expédition.[RFC 791]. Le protocole IPv4 détermine le destinataire du message grâce à 3 champs:

- Le champ adresse IP : adresse de la machine
- Le champ masque de sous-réseau : un masque de sous-réseau permet au protocole IP de déterminer la partie de l'adresse IP qui concerne le réseau
- Le champ passerelle par défaut : Permet au protocole Internet de savoir à quelle machine remettre le datagramme si jamais la machine de destination n'est pas sur le réseau local.

Les données circulent sur Internet sous forme de datagrammes (on parle aussi de paquets). Les datagrammes sont des données encapsulées, c'est-à-dire des données auxquelles on a ajouté des en-têtes correspondant à des informations sur leur transport (telles que l'adresse IP de destination, ...). Les données contenues dans les datagrammes sont analysées (et éventuellement modifiées) par les routeurs permettant leur transit.

Le routage des datagrammes se fais au niveau de la couche IP, c'est sa tache la plus importante. Les datagrammes ne sont pas routés par des simples hôtes mais plutôt par des routeurs dont le rôles est de transmettre les datagrammes d'une interface à une autre.

D'un point de vue idéale, établir une route pour des datagrammes devrait tenir compte d'éléments comme la charge du réseau, la taille des datagrammes, le type de service demandé, les délais de propagation, l'état des liaisons, le trajet le plus court, etc.

2.2.1 IPv6: Le nouveau protocole et ses solutions

Cette nouvelle version du protocole IP apporte principalement la solution au nombre d'adresses mais apporte également un lot de nouveautés. IPv6, bien qu'encore non tout à fait terminé (il reste encore certains points de détails à revoir), fonctionne déjà bien [BAR04].

- Avec IPv6, le problème de pénurie d'adresse est largement écarté avec des adresses si grandes (128 bits).
- Les en-têtes des paquets IPv6 ont été fortement réduits par rapport à ceux d'IPv4; les diverses options ne sont plus contenues dans les en-têtes, mais dans le corps (partie données) du paquet. Cela a pour but d'accélérer la transmission des paquets, car les différents intermédiaires n'ont plus à analyser un en-tête compliqué.
- La découverte des voisins, grâce au protocole ICMPv6 (étroitement lié à IPv6) est un gros progrès. Le but est de permettre à un ordinateur de découvrir par lui-

même le réseau dans lequel il se trouve, ce qui lui permet de se configurer tout seul, sans intervention d'un administrateur.

L'autoconfguration permet à un ordinateur voulant s'intégrer à un réseau de le faire par lui-même, sans DHCP (Dynamic Host Configuration Protocol), bien que l'utilisation d'un serveur DHCPv6 soit possible ; on parle dans ce cas d'autoconfguration statefull.

2.2.2 Le problème de la mobilité IP

IPv4 identifie le point d'accès d'un nœud sur Internet d'une manière unique grâce à son adresse IP. Celle-ci se décompose en deux parties:

- Le préfixe qui détermine le sous réseau sur lequel la machine se trouve.
- L'identifiant de la machine sur son sous réseau.

Internet est un réseau de trop grande taille pour que chaque routeur puisse mémoriser une route vers toutes les machines qui y sont attachées. En fait, les routeurs ne stockent que des entrées correspondant à des sous réseaux, considérant que des datagrammes destinés à des machines ayant le même préfixe seront tous routés de manière identique.

La mobilité introduit un nouveau problème de routage : les mobiles se déplacent d'un sous réseau IP vers un autre sous réseau IP, mais en un mauvais préfixe sur le réseau destination. Par conséquent, un nœud doit être situé sur le réseau indiqué par son adresse IP afin de pouvoir recevoir les paquets qui lui sont destinés. Pour qu'un nœud puisse changer de point d'accès sans perdre la possibilité de communiquer, deux mécanismes peuvent être employés :

- Le nœud doit changer d'adresse IP à chaque fois qu'il change de point d'accès.
- Des chemins spécifiques à l'hôtes doivent être propagés dans presque toute la structure de routage d'Internet.

Ces deux alternatives sont souvent inacceptables. La première ne permet pas à un nœud de conserver des connexions au niveau de la couche transport ou couches supérieures lorsqu'il change de position. La seconde pose des problème de passage à l'échelle.

Un nouveau mécanisme flexible est nécessaire afin de s'adapter à la mobilité des nœuds sur Internet. Le protocole Mobile IP permet aux nœuds de changer de point d'accès sans changer leurs adresses IP.

2.3 Définitions

- Nœud mobile (Mobile Node ″MN″)

Hôte ou routeur qui change de point d'accès d'un réseau (ou sous-réseau) à un autre, il appartient initialement à un réseau appelé réseau mère (Home Network). [LEG01]

-Correspondant (″CN″)

Machine (mobile ou fixe) en communication avec le nœud mobile. [LEG01]

- Agent mère (Home Agent ″HA″)

Routeur sur le réseau , il met à jour les informations concernant la position du mobile et tunelle les datagrammes destinés à ce dernier. [LEG01]

- Agent étranger (Foreign Agent ″FA″)
Routeur sur un réseau visité par le nœud mobile, qui fournit des services de routage au mobile lors de son enregistrement. [LEG01]
- Care Of Adress (Adresse temporaire)
Adresse temporaire affectée au mobile par le foreign agent dans le domaine étranger. [LEG01]
- Co-located care-of-address
Adresse temporaire affectée au mobile d'une manière dynamique par un serveur DHCP (Dynamic Host Configuration Protocol) [LEG01]
- Point d'accès
Equipement intermédiaire entre le réseau filaire et le nœud mobile qui offre la connexion aux nœuds mobiles qui lui sont rattachés. [LEG01]
- Handoff
Le processus enclenché quand un mobile actif (en cour de communication) change son point d'attachement à Internet. [LEG01]
- La latence du handoff
Laps de temps entre le dernier moment où le mobile peut recevoir et émettre des paquets IP à travers l'ancien foreign agent et le premier moment où il peut recevoir et émettre des paquets à travers le nouveau foreign agent. [LEG 01]
L'architecture de base de ces équipements est présentée dans la Figure 2.1 :

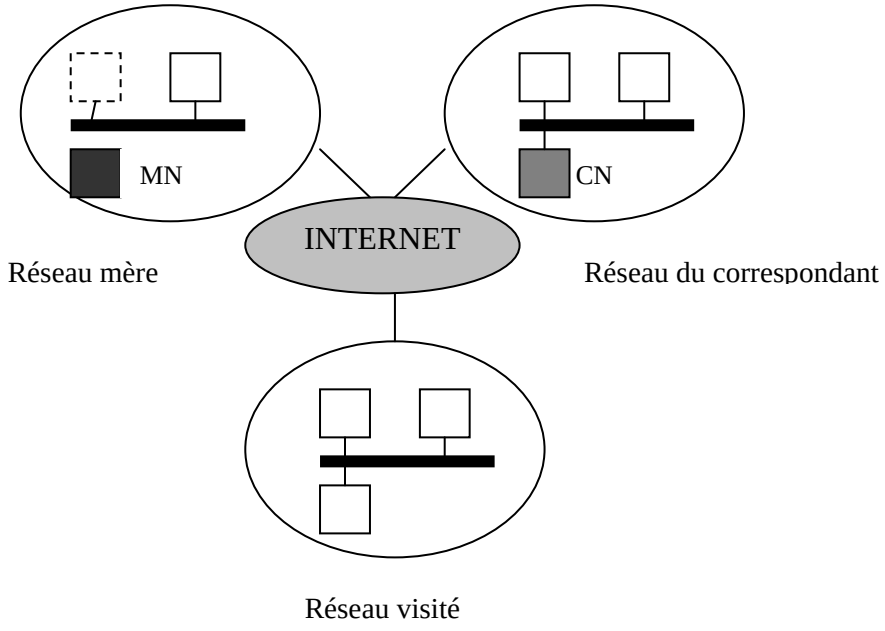

Figure 2.1 : Schéma des principaux acteurs de base de la mobilité

2.4 Le handoff dans l'environnement mobile

Le handoff est le processus enclenché quand un mobile actif (en cours de communication) change son point d'attache à Internet. D'après le modèle OSI, on peut découper un handoff de la manière suivante: handoff de niveau 3 (couche IP) et handoff de niveau 2 (couche liaison). Le handoff de la couche 2 est l'opération

effectuée par un nœud mobile qui change de point d'accès sans fil, c'est à dire que c'est le passage d'un point d'accès à un autre. Ce handoff peut engendrer ou non un handoff de la couche supérieure selon le lien filaire des points d'accès (si elles sont sur le même lien réseau ou non). Plus généralement, on distingue trois types de handoff : (Figure 2.2)

- **Handoff intra-routeur d'accès**: handoff généré par le changement d'interface réseau du routeur d'accès par laquelle il communique avec le mobile. L'adresse IP du mobile ne change pas.
- **Handoff à l'intérieur d'un réseau d'accès**: Opération effectuée quand le nœud mobile change de routeur d'accès en restant dans le même réseau d'accès. Ce handoff est invisible pour un point extérieur au sous-réseau et l'adresse du mobile ne change toujours pas, mais le chemin pour l'atteindre est modifié.
- **Handoff entre réseaux d'accès:** Déplacement du mobile hors du réseau d'accès; cette fois le MN a besoin d'acquérir une nouvelle adresse IP.

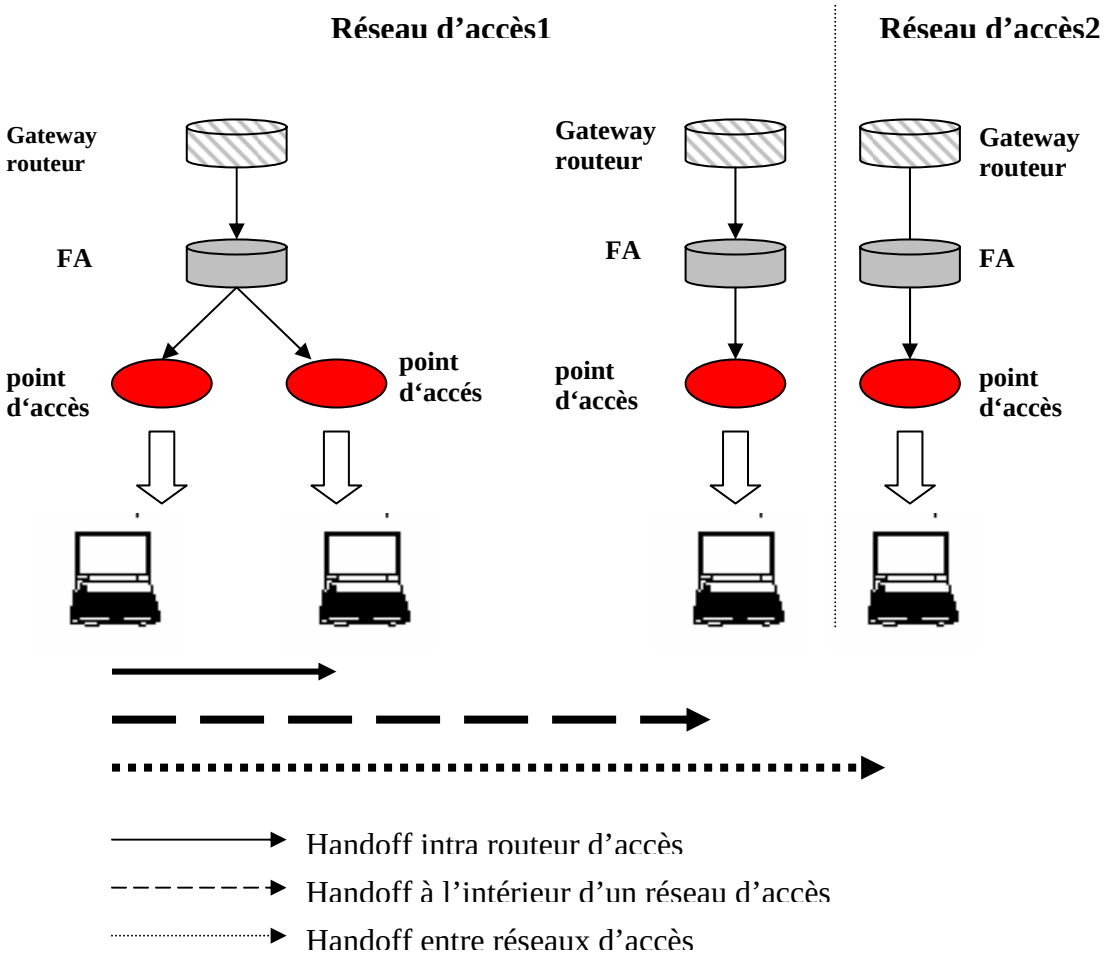

Figure 2.2 : Niveaux de handoff

2.5 Le fonctionnement du protocole Mobile IPv4

Le protocole Mobile IPv4 est un protocole de niveau réseau permettant à un mobile d'être joint et de communiquer (avec d'autres mobiles ou terminaux fixes) quelle que soit sa position géographique. [RFC2002].
Le protocole Mobile IP est fondé sur la division du réseau en sous-réseau en accord avec les préfixes et les règles de routage. Lorsqu'un utilisateur change de sous réseau, il est nécessaire de modifier son préfixe pour que les routeurs puissent acheminer l'information au nouveau sous-réseau.
Dans cette optique trois étapes essentielles jalonnent le fonctionnement de Mobile IP:

- **La découverte des agents** : C'est l'étape de la découverte des agents relais (Home Agents et Foreign Agents).
- **L'enregistrement :** Lorsqu'un mobile est hors de son réseau mère il enregistre son adresse temporaire avec son agent mère.
- **Le tunneling**: Les paquets destinés au mobile sont interceptés par l'agent mère et tunnelés jusqu'au mobile.

2.5.1 La découverte des agents

C'est l'étape de la découverte des agents relais et l'obtention d'une adresse temporaire (COA). Dans le réseau visité, le nœud mobile MN doit obtenir une adresse lui permettant de déclarer sa localisation à son HA. A cette fin, un agent étranger diffuse à intervalle régulier un message d'avertissement contenant les adresses temporaires proposées par le domaine visité. Par ailleurs, un nœud mobile ne désirant pas attendre un tel message, peut explicitement en demander un par l'émission d'un Agent de sollicitation (cas où l'agent tombe en panne par exemple). Ces messages seront authentifiés et envoyés en broadcast ou en multicast .
Les agents de mobilité (HA et FA) maintiennent une liste des nœuds mobiles qu'ils cogèrent. Cette liste appelée cache d'association associe l'adresse principale du mobile à son adresse temporaire, cette dernière peut être obtenue par l'une des techniques suivantes:

- **Co-located care-of-address**: Le mobile MN peut par exemple interroger un serveur DHCP (Dynamic Host Configuration Protocol) qui lui attribue une adresse IPv4 dynamiquement.
- **Foreign-Agent care-of-address**: le mobile MN n'a pas d'adresse propre. Son adresse temporaire correspond à l'adresse du FA. Le mobile émet des paquets avec son adresse principale comme adresse source.

2.5.2 L'enregistrement

Lors de son mouvement, le nœud mobile doit enregistrer sa localisation. La procédure d'enregistrement permet au réseau d'abonnement de transférer le trafic du nœud et de vérifier s'il détient les autorisations pour accéder au réseau visité.

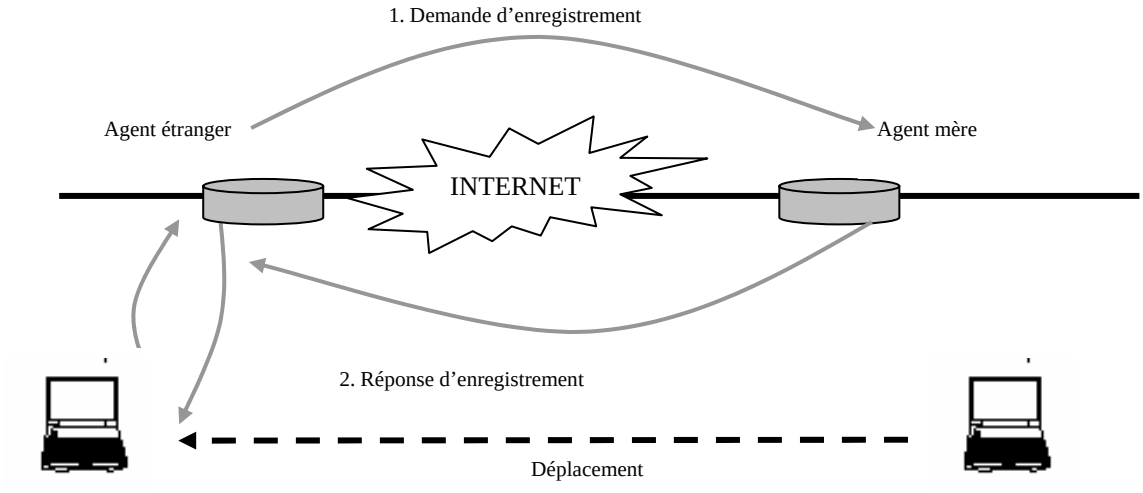

Figure 2.3 : La procédure d'enregistrement.

Lorsque le nœud mobile détecte qu'il a changé de sous réseau (a travers les messages d'enregistrement), il doit acquérir une nouvelle adresse temporaire et s'enregistrer auprès du HA et du FA .

La procédure d'enregistrement est résumée en quatre étapes : (Figure2.3)

- Demande d'enregistrement au FA *(Registration Request).*
- Traitement de la demande par le FA, puis transmission de la demande au HA.
- Notification d'acceptation ou de refus de prise en charge du mobile du HA au FA .
- Traitement de la notification par le FA et transmission de l'information au mobile .

La procédure d'enregistrement sera détaillée dans le chapitre III .

2.5.3 Le tunneling

Un correspondant instaure un trafic IP avec le nœud mobile, l'agent mère intercepte puis encapsule les paquets en provenance du correspondant. Un tunnel est ensuite créé entre le HA et le FA pour rediriger les paquets encapsulés vers le FA[AGA01]. A la réception, le FA décapsule l'information et la transfère au nœud mobile. (Figure 2.4)

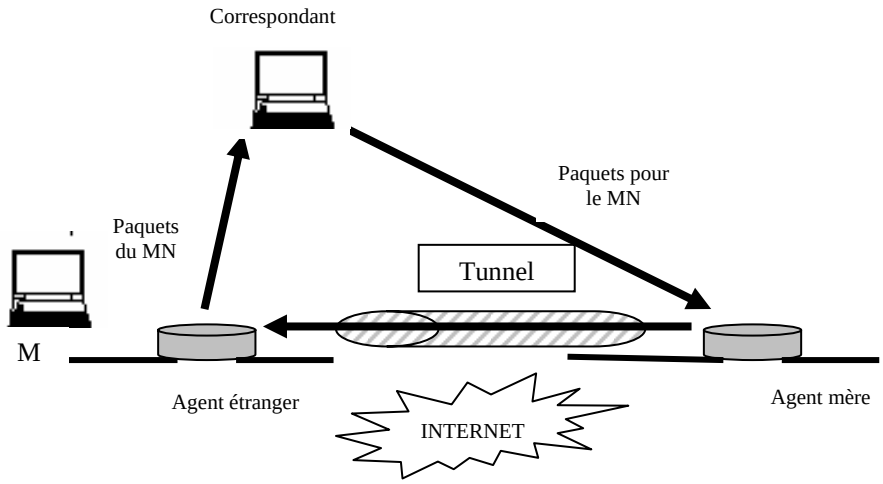

Figure2.4 : Le Tunneling

Un certains nombres d'algorithmes d'encapsulation existent, dont le plus simple est « IP dans IP ». La simplicité de l'algorithme d'encapsulation IP dans IP s'explique par son mode de fonctionnement, il ajoute un nouvel en-tête au paquet IP en dupliquant les données qu'il extrait de l'en-tête original.(Figure2.5)

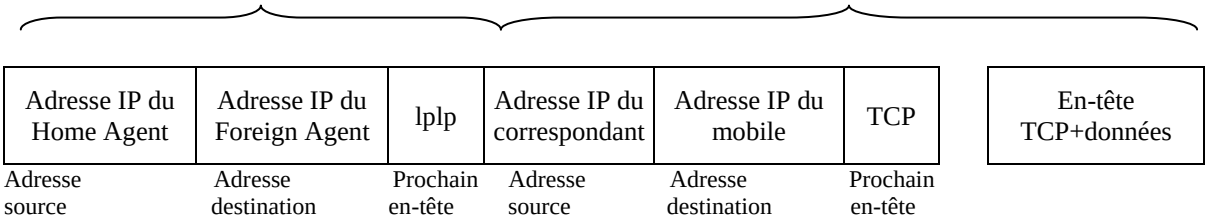

Figure2.5 : L'encapsulation IP dans IP

2.6 Le scénario de communication du Mobile IPv4

Nous allons considérer deux scénarios de communication dans Mobile IPv4**[**AGA01].

Premier scénario : (CN → MN).
Les informations sont transférées du correspondant CN au nœud mobile MN. Le CN ne connaît que l'adresse principale du MN, les paquets à destination du MN sont *toujours* envoyés dans le sous réseau mère du MN (Figure2.6).
- Si le MN ne s'est pas déplacé, les paquets lui sont livrés de la même manière qu'un nœud fixe (sans opérations supplémentaires).
- Sinon, si le MN est dans un sous réseau visité, le HA devra capturer tous les paquets destinés au MN et les lui transmettra à son adresse temporaire grâce à son cache d'association.

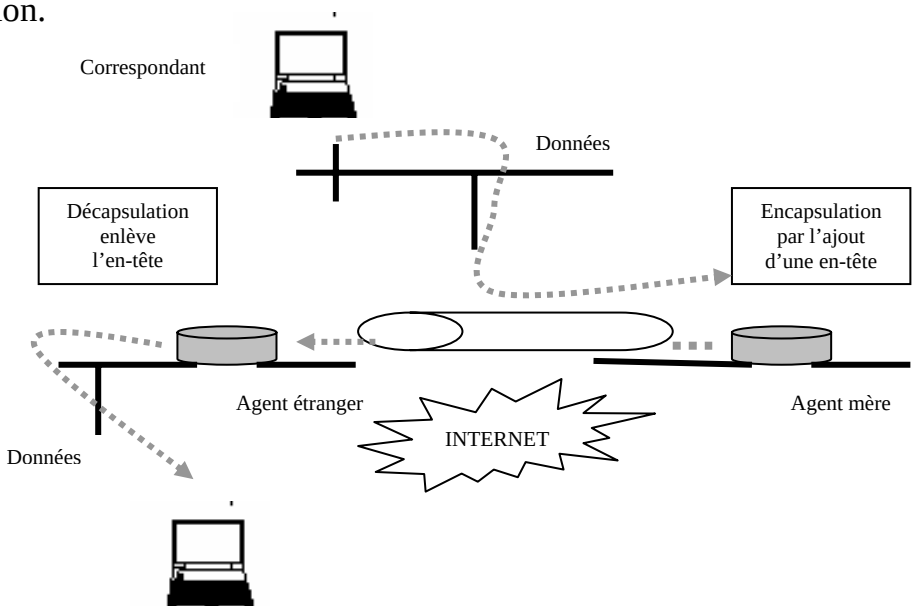

Figure2.6: Le routage triangulaire du correspondant au mobile

Deuxième scénario : (MN→ CN)
Les informations sont transférées du correspondant MN au nœud mobile CN. Les paquets envoyés par le MN ont l'adresse du correspondant comme adresse destination, et l'adresse principale du mobile comme adresse source. Ceci présente un problème au modèle de l'Internet puisque l'adresse source des paquets envoyés par le nœud mobile ne correspond pas au préfixe du sous réseau visité.
Les paquets devront alors obligatoirement passer par l'agent visité pour éviter qu'ils ne soient détruits (ingress filtering)[1]. Par contre, une fois que les paquets ont été routés hors du sous-réseau visité, ils vont directement du MN au correspondant sans passer par le réseau mère.

En effet, le MN qui se déplace dans le sous réseau visité informe son HA à travers une demande d'enregistrement (*Registration Request),* à la réception, le HA met à jour l'entrée pour ce MN, et fait la correspondance entre l'adresse IP du MN et son adresse MAC ainsi il peut intercepter les paquets à destination du mobile. Chaque paquet est encapsulé en ajoutant une entête avec l'adresse temporaire du mobile comme adresse destination et l'adresse du home agent comme adresse source avant de les tunneler au FA, enfin, chaque paquet est décapsulé (suppression de l'entête) et délivré au nœud mobile. (Figure2.7)

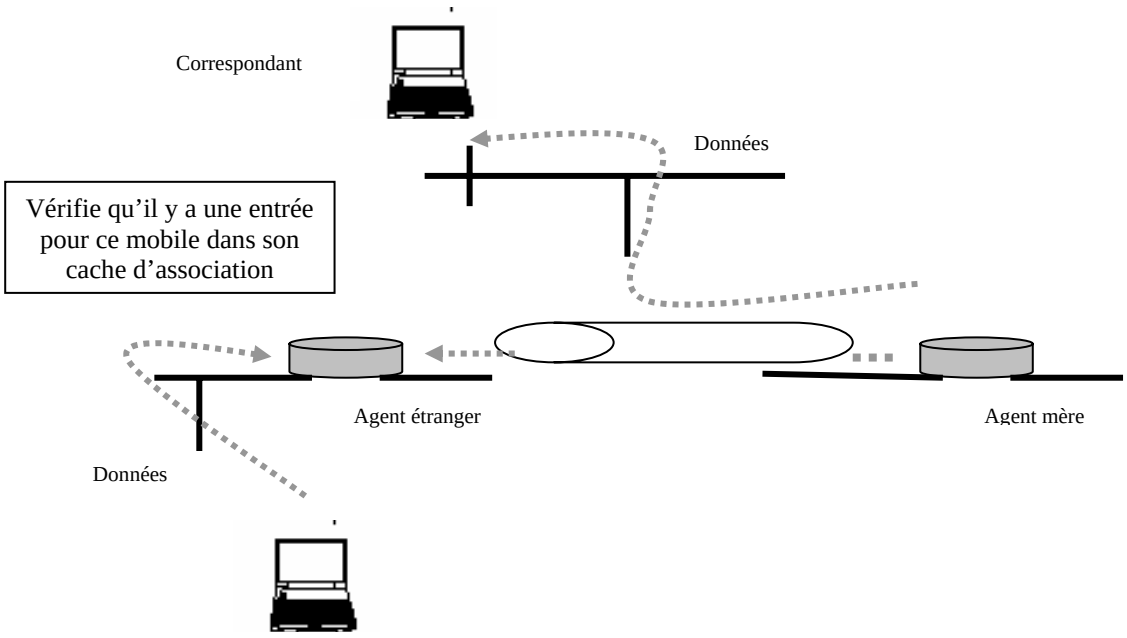

Figure2.7 : Le routage triangulaire du mobile au correspondant

[1] Ceci consiste à vérifier que les adresses d'émission des paquets reçus sont valides, c'est-à-dire qu'elles respectent la topologie du réseau : Quand un routeur reçoit un paquet sur une interface, il vérifie que l'adresse source du paquet appartient bien à un réseau connecté à cette interface.

2.7 Optimisation de route dans Mobile IP de base

Le protocole Mobile IP de base, permet à une unité mobile de se déplacer et de changer son point d'attachement à Internet tout en conservant son identité définie par l'adresse IP qui lui a été assigné par son réseau mère.
Les nœuds qui correspondent avec le mobile envoient à son adresse IP les datagrammes IP qui lui sont destinés. Cette façon de faire rend la mobilité transparente aux correspondants mais force tous les datagrammes dessinés à un nœud mobile à être routés par son agent mère, ainsi, les datagrammes destinés à un nœud mobile empruntent généralement des routes qui sont souvent longues et non optimales.
A titre d'exemple, si un nœud mobile visite un sous réseau loin de son réseau mère et communique avec un correspondant qui se trouve sur le même sous réseau visité, ce dernier sera obligé de router ses datagrammes jusqu'au home agent pour suivre le tunnel vers le sous réseau d'origine et en fin être délivrés au mobile. Ce routage indirect (triangulaire) peut retarder significativement les paquets destinés au mobile et place un fardeau supplémentaire sur les routeurs du réseau.
Pour cette raison, un ensemble d'extensions est apporté au protocole Mobile IP de base afin de permettre un meilleur routage où les datagrammes sont routés directement du correspondant vers le nœud mobile sans transiter par son agent mère.
Cet ensemble d'extension est appelé : *«optimisation de route»* [RFC2002][PER98]

L'optimisation de route apporté à Mobile IP de base comporte 3 parties essentielles:

- Utilisation des binding caches.
- Utilisation de smooth handoffs entre Foreign agents.
- Utilisation de tunnels spéciaux.

2.7.1 Le binding cache

Un binding cache (Figure 2.8) est une table qui contient une liste d'association de type (mobile, adresse temporaire) [PER00b]. Chaque nœud maintient son binding cache pour optimiser ses communications avec les autres nœuds. Pour envoyer des paquets au nœud mobile X, le correspondant consulte tout d'abord son binding cache pour vérifier si l'adresse temporaire du X existe. Si une telle adresse existe, le correspondant peut envoyer ses paquets directement au nœud sans transiter par son réseau mère, le correspondant utilise les mêmes techniques d'encapsulation que le Home Agent.

Mobile ID	**Adresse temporaire**
…	….
…	….
Mobile X	Adresse temporaire Y
…	…

Figure2.8 : format d'un binding cache

Lorsque l'agent mère intercepte un paquet contenant l'adresse IP du mobile X dans son réseau mère et l'encapsule pour ce nœud, il déduit que le nœud source du message ne possède pas une entrée pour X dans son binding cache. L'agent mère envoie alors un message BU (mise à jour du binding) au nœud source du message dont lequel il l'informe du l'adresse temporaire, ce dernier ajoute alors cette adresse temporaire à son binding cache. Ce message ne nécessite pas un accusé de réception, en effet à chaque fois que l'agent mère reçoit un message à tunnler vers un nœud mobile, il génère un message de binding update pour le nœud source du message.
La gestion de l'espace du cache est donc nécessaire, si une nouvelle entrée est ajoutée , le nœud peut supprimer d'autres entrées pour libérer de l'espace. La suppression est faite à l'aide de l'algorithme LRU (Last Recently Used). [PER00b]

2.7.2 Smooth handoff entre les foreign agents

Lorsqu'un nœud mobile se déplace et s'enregistre avec un nouveau foreign agent, le protocole Mobile IP de base ne prévoit pas de notifier l'ancien foreign agent. Les datagrammes IP interceptés par le home agent après le nouvel enregistrement du mobile sont tunnelés vers la nouvelle adresse temporaire.
Cependant, les datagrammes déjà en route, ceux qui ont été tunnelés vers l'ancienne adresse temporaire sont perdus et supposés retransmis par les couches de haut niveau du protocole.
L'optimisation dans ce cadre, fournit à l'ancien foreign agent du nœud mobile un moyen pour être notifier du point d'attachement du mobile. Ainsi, les datagrammes envoyés vers l'ancien foreign agent peuvent être redirigés par ce dernier vers la nouvelle adresse temporaire.
Cette notification permet aussi à tous les datagrammes tunnelés vers l'ancien foreign agent par un correspondant dont l'entrée du binding cache a expiré, d'être redirigés vers la nouvelle adresse temporaire.
Finalement, cette notification permet de libérer les ressources du nœud mobile au niveau de l'ancien Foreign agent immédiatement.
L'introduction de cette notification au niveau de l'enregistrement du mobile est dite *« smooth handoff »*. En effet, durant la procédure d'enregistrement le nœud mobile peut demander que son nouveau Foreign agent essaye de notifier son ancien foreign agent, pour cela, le nœud mobile inclut dans son message d'enregistrement envoyé au nouveau foreign agent une demande de notification de l'ancien foreign agent (c'est l'extension apporté à la procédure d'enregistrement). Le nouveau foreign agent construit alors un message Binding Update et l'envoie à l'ancien foreign agent en demandant un accusé de réception, ce message contient la nouvelle adresse temporaire qui permettra à l'ancien foreign agent de créer une entrée pour le mobile dans son binding cache qui servira comme pointeur de redirection. [PER00b]

2.7.3 Utilisation de tunnels spéciaux

Il peut arriver qu'un nœud reçoit un paquet tunnelé (encapsulé pour un mobile qui n'existe pas dans la liste des visiteurs (le nœud n'est pas le foreign agent du mobile).

Donc l'adresse temporaire utilisée par le nœud qui a envoyé le paquet est sûrement incorrecte et l'entrée du binding cache correspondante au mobile n'est pas mise à jour.
Si le nœud recevant le paquet encapsulé possède une entrée qui corresponde à la destination dans son binding cache, il doit renvoyer le paquet à l'adresse temporaire indiquée dans son binding cache.
Cependant, si le foreign agent recevra la paquet encapsulé ne possède pas une entrée correspondante à la destination dans son binding cache, il ne peut diriger le paquet vers sa destination, il doit cependant l'envoyer vers le home agent du mobile en utilisant une forme spéciale de tunnel où l'adresse IP destination (externe) de l'entête du paquet est identique à celle qui existe dans le paquet original. Donc, les adresses IP de destination interne et externe sont identiques et sont égales à l'adresse du home agent.
Lorsqu'un tel paquet arrive au niveau du home agent, se dernier doit décapsuler le paquet et l'envoyer à l'adresse temporaire correcte du mobile. Cependant, il doit d'abord vérifier que l'adresse temporaire en sa possession n'est pas l'adresse du foreign agent qui a tunnelé le paquet qu'il vient de recevoir. Si c'est le cas, le home agent en déduit que le foreign agent servant le mobile a perdu l'entrée correspondante au mobile dans sa liste de visiteurs (suite à une panne par exemple). Le home agent doit éliminer le paquet pour éviter une boucle infinie.
Si par contre, l'adresse temporaire courante est différente de l'adresse du nœud qui a tunnelé le paquet, le home agent envoie le paquet à l'adresse temporaire. Il envoie aussi des messages de « mise à jour de binding » au foreign agent qui a utilisé le tunnel spécial ainsi qu'au nœud source de massage.

2.8 Le protocole successeur: Mobile IPv6

Profitant de l'émergence du nouveau protocole IPv6, en 1994 Charles Perkins, David Johnson et Andrew Myles soumettent à l'IETF une proposition de protocole de mobilité sur IPv6 appelé *Mobile IPv6* qui décrit un moyen de gérer la mobilité de terminaux IPv6.[CHA02]
Cette mobilité permet qu'un terminal IPv6 soit toujours joignable, quelle que soit sa localisation dans l'Internet et que ses connexions en cours restent actives malgré ses déplacements. IPV6 introduit les notions de « découverte de voisins » et « d'auto configuration » deux outils permettant à un utilisateur d'obtenir une adresse. Il rend ainsi l'agent étranger sans aucun rôle et sera par conséquent supprimé. En remplacement des points d'accès, radio ou fixe, sont introduits, assurant l'accueil des visiteurs.
Le cœur du fonctionnement d'IP ayant été maintenu, la gestion de la mobilité par le biais des adresses temporaires COA et les protocoles d'encapsulation restent inchangés.
Ainsi, l'utilisateur à son arrivé à un réseau visité se met à l'écoute des messages IPV6 pour construire sa nouvelle adresse temporaire (COA), une fois cette adresse obtenue elle sera transmise à l'agent mère pour l'enregistrement. L'agent mère procède à l'encapsulation pour re router l'information de l'utilisateur à la destination. [AGA01]

Bien que MIPV6 reprenne les mécanismes de MIPV, de nombreuses fonctionnalités supplémentaires ont été mises en places.

2.9 Fonctionnalités requises

- Le correspondant doit disposer d'un cache d'associations tout comme l'agent mère dans ce cache sera stocké la correspondance entre l'adresse temporaire et celle principale.
- Le correspondant doit être capable de traiter les messages d'enregistrement émis par le MN.
- Le correspondant doit être capable d'effectuer le routage directement vers le MN *(Routing Header).*
- Le MN doit conserver la listes des correspondants auxquels il envoie un message d'enregistrement, et il doit être capable de décapsuler lui-même les paquets qui lui sont transmis.

2.10 Le scénario de communication du Mobile IPv6

Le principe de base de Mobile IPv6 est que le nœud mobile MN est toujours adressable par son adresse mère, qu'il soit sur son réseau mère ou sur un réseau visité. Dans le cas où MN est dans son réseau mère, le routage des paquets s'effectue d'une manière standard.

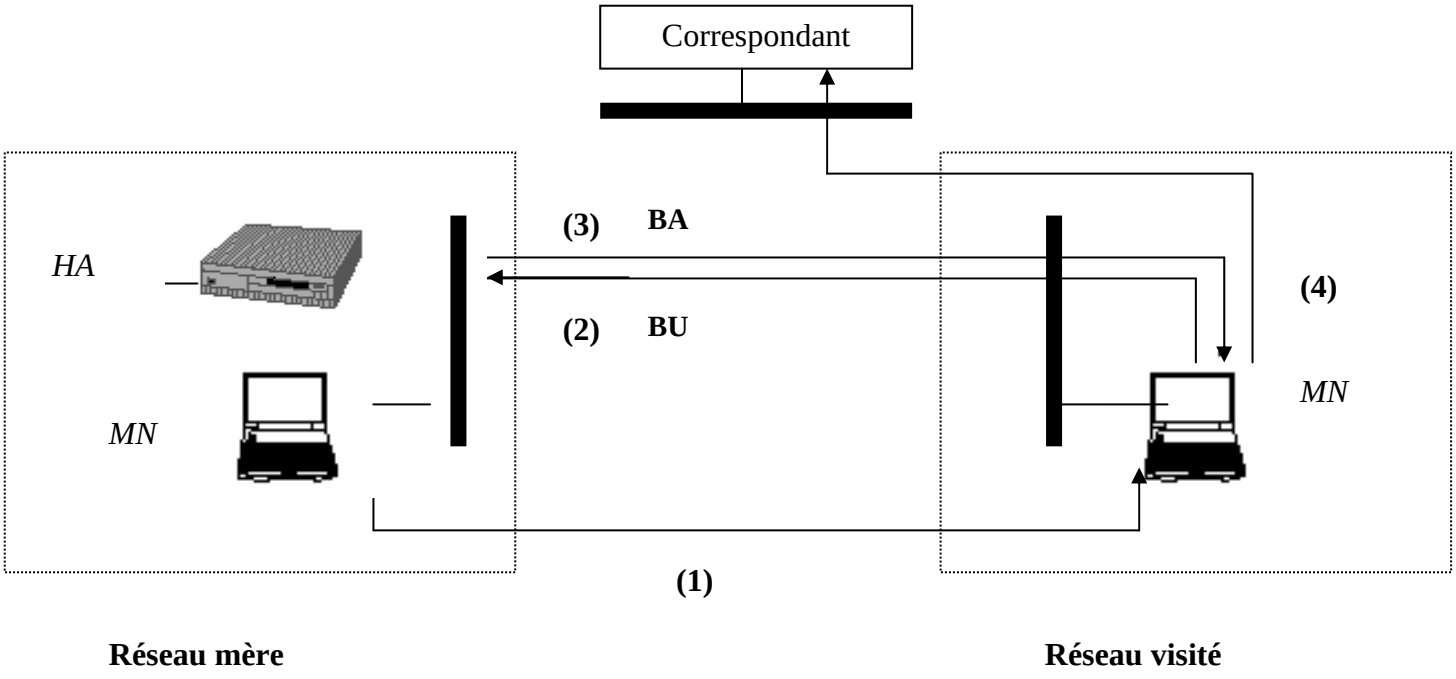

Figure 2.9: La communication dans Mobile IPv6

Dans le cas où le nœud mobile MN effectue un mouvement pour aller sur un réseau visité **(1)**, il récupère une adresse temporaire sur ce réseau, enregistre sa nouvelle position auprès de l'agent mère **(2)** grâce au message *Binding Update* (BU) qui contient les deux adresses temporaire et mère. Le HA confirme en envoyant le message *Binding Acknowledgement* (BA) **(3)**. (Figure2.9)

Par ailleurs, à l'inverse de Mobile IPv4, le nœud mobile MN dans Mobile IPv6 peut signaler sa nouvelle position **(4)** aux correspondants avec lesquels il était en communication toujours grâce aux messages *(Binding Update)* et *Binding Acknowledgement).*

2.11 Limites de Mobile IP (Solution de micro mobilité)

Mobile IP est conçu pour permettre aux nœuds de se déplacer d'un sous réseau IP à un autre; il résout le problème de « macro » mobilité mais il est moins bien adapté à la micro mobilité lorsque les mobiles effectuent les handoffs fréquents dans une même zone géographique.

Dans la version standard de Mobile IP, la nouvelle localisation d'un mobile est toujours signalée à son home agent. Ce dernier est ainsi averti de tous les déplacements des mobiles qu'ils gèrent. Ces opérations génèrent une grande quantité de signalisation de plus, les pertes de paquets pendant les handoffs peuvent être importantes puisque la procédure d'enregistrement est longue, en particulier si le home agent se trouve loin.

La micro mobilité représente donc la gestion de la mobilité locale. La gestion de la micro mobilité permet à des mobiles de s'enregistrer localement à l'intérieur du réseau qu'ils visitent, cet enregistrement locale réduit le délai de signalisation ce qui peut améliorer les performances des handoffs.

Pour des mobiles bénéficiant d'une certaine qualité de service, l'acquisition d'une nouvelle adresse temporaire pour chaque handoff implique de remettre en place des réservations entre le home agent et le nouveau foreign agent. Cependant, une grande partie du chemin entre le correspondant et le mobile risque d'être identique avant et après le handoff (si le mobile ne change pas de domaine).

Plusieurs solutions pour gérer la micro mobilité ont été proposées. Toutes reposent sur le principe suivant: le réseau visité par un mobile se charge des déplacements locaux ; le home agent n'est donc pas prévenu de tous les changements de localisation du mobile qu'il gère.

Mobile IP Hiérarchique, Cellular IP, HAWAII sont des exemples de protocoles de micro mobilité

2.12 Conclusion

Grâce à la popularité d'Internet, le protocole IP s'impose comme incontournable pour les futurs réseaux de télécommunication. Par ailleurs, la miniaturisation des équipements informatiques et le développement des réseaux et des services sans fil contribuent à développer les services de mobilité. L'IETF a standardisé le protocole Mobile IP pour intégrer le support de service de mobilité dans les réseaux IP étendus. Le protocole Mobile IP permet aux nœuds mobiles l'échange de données tout en étant mobile.

Cependant, Mobile IP souffre de plusieurs problèmes techniques empêchant son déploiement adéquat : la technique du routage triangulaire représentait la faiblesse majeure du protocole Mobile IPv4 [CHA97], en effet, lorsqu'un mobile hors de son sous-réseau mère cherche à joindre une machine sur le même réseau visité, les paquets doivent néanmoins transiter par le sous-réseau mère du mobile. Ce problème a été résolu avec le Mobile IPv6 en proposant d'ajouter des mécanismes supplémentaires sur les correspondants d'un mobile et de modifier la pile du protocole TCP/IP mais cette solution supprime la transparence du protocole par rapport aux utilisateurs, c'est à dire qu'un correspondant doit à présent savoir s'il dialogue avec une machine fixe ou mobile de plus ces opérations génèrent une grande quantité de signalisation.
La perte de paquets surtout pendant le handover est un autre problème de Mobile IP, il est dû à la longueur de la procédure d'enregistrement (la durée d'un handover peut atteindre plusieurs secondes dans l'Internet actuel) En particulier si le Home Agent se trouve loin du domaine visité.
Enfin, autoriser une machine à se connecter sur un réseau puis à se déplacer de réseau en réseau entraîne de nombreux risques (écoute, vol de session, intrusion, …).
Nous avons consacré le chapitre suivant à l'étude de la sécurité dans le protocole.

Chapitre III *La sécurité dans le protocole Mobile IP*

3.1Introduction

Aujourd'hui, l'idée d'utiliser les protocoles de mobilité IP pour assurer la gestion des mobiles dans les réseaux cellulaires est devenue rapidement évidente, le protocole Mobile IP fournit un mécanisme efficace pour passer d'un réseau à un autre. Néanmoins, cette mobilité pose de vrai risques de sécurité. En effet, le nombre incalculable d'attaques enregistrées (déni de service, analyse de trafic, écoute passive, …) montrent que Mobile IP est l'objet d'incessantes tentatives de fraude.
D'une manière générale il existe trois raisons majeures de fortes tentatives de fraudes et d'attaques sur les réseaux Mobile IP:

1. L'expérience acquise sur les réseaux IEEE802.11 qui révèle une activité frauduleuse élevée.
2. L'ouverture des protocoles et des terminaux.
3. L'accès physique des mobiles aux réseaux ouverts.

Par ailleurs, les victimes des attaques ne seront pas uniquement les mobiles, mais potentiellement tous les acteurs intervenant dans la communication du mobile: son correspondant, son agent-mère, son réseau mère, les autres mobiles du réseau visité, les machines opérant sur le réseau visité, etc.
Les nombreuses publications d'attaques sur les réseaux IEEE802.11b[BUT02] montrent que la pression des fraudeurs sur les réseaux nomades est forte. Le nombre incalculable d'attaques enregistrées laisse augurer qu'un réseau Mobile IP sera l'objet d'incessantes tentatives de fraude puisque les terminaux considérés soient des ordinateurs connectés à l'Internet à l'inverse du monde GSM où les protocoles, les terminaux et les interfaces sont très fermés aux utilisateurs. De plus, Mobile IP repose sur le protocole insécurisé et ouvert : le protocole IP.
Enfin, autoriser une machine à se connecter sur un réseau puis à se déplacer de réseau en réseau entraîne de nombreux risques qui n'existaient pas auparavant dans une architecture fixe. En effet, le mobile pourrait être victime des autres mobiles du réseau visité ou le réseau visité pourrait être l'objet d'une destruction de la part d'un des mobiles qu'il accueille.
Dans ce chapitre nous présentons quelques types d'attaques enregistrées sur Mobile IP, ainsi que les besoins de sécurité de ce protocole et plus précisément le besoin d'authentification. En plus, nous étudierons quelques travaux proposant des améliorations à la procédure d'authentification de ce protocole.

3.2 Attaques dans le monde mobile

3.2.1 Attaques sur les machines mobiles

- **L'écoute**

Le risque le plus présent à l'esprit des travailleurs nomades est certainement le vol d'informations sensibles. Aujourd'hui, il est couramment admis dans les usages d'établir un VPN[2] pour se connecter à un Intranet depuis l'extérieur de son entreprise, par exemple par une connexion modem. Demain, l'emploi des réseaux radio va accroître les points d'écoute, notamment sur la partie hertzienne de la connexion. Non seulement la radio permet un espionnage à distance, mais elle repose souvent sur un protocole à diffusion qui facilite l'écoute passive. Dans le même ordre d'idée, un réseau visité Mobile IP utilise aussi la diffusion et constitue donc aussi un support d'écoute facile.

- **Vol de session**

Le vol de session se trouve également facilité pour les mêmes raisons: réseaux à diffusion et utilisation fréquente de la radio. Le vol de session consiste pour un attaquant à se faire passer pour sa victime, le but étant de lui voler des informations, mais plus souvent de lui voler son accès à l'Internet. Dans le cas où l'usage des ressources est payant, un vol de session permet de gagner un accès au réseau en prenant la connexion d'une victime qui paye la ressource.

- **Localisation**

Certains experts considèrent que la connaissance même de la position du mobile constitue une information que l'on peut souhaiter vouloir cacher. Bien que ceci ne constitue pas un risque en soit pour le mobile, un correspondant qui connaîtrait la position d'un mobile pourrait en déduire des informations personnelles ou professionnelles importantes, par exemple sur quel réseau le mobile est venu se connecter et donc quel client, partenaire, fournisseur ou concurrent a été rencontré.

- **Intrusions**

Un protocole tel que Mobile IP conduira inévitablement à des situations où les machines d'utilisateurs concurrents (au sens économique ou commercial du terme) seront connectées simultanément au même réseau visité. Il convient de s'assurer que l'intrusion d'une machine sur une autre machine sera rendue la plus difficile possible.

3.2.2 Attaques sur l'agent mère et les correspondants

Le rôle principal de l'agent mère est d'enregistrer et de suivre les différentes positions du mobile [RFC2002]. Lorsqu'un mobile en déplacement reçoit du trafic à son adresse mère, l'agent mère doit l'intercepter et le retransmettre vers le mobile. Donc un usurpateur qui arriverait à se faire enregistrer à la place d'un mobile auprès de son

2 Un VPN est un système permettant d'interconnecter plusieurs ordinateurs distants avec la sécurisation des données en utilisant un réseau public (Internet). L'objectif est d'offrir le même degré de disponibilité, de performance et de sécurité qu'un réseau privé, mais sans les coûts prohibitifs et avec plus de maniabilité[BEN04].

agent mère recevrait tout le trafic normalement destiné à sa victime. Une attaque sur l'agent mère constitue par conséquent un moyen de réaliser une attaque de type vol de session ou vol de données. Ces attaques sont d'autant plus probables qu'il n'est pas toujours possible d'établir un lien de confiance aussi fort entre un mobile et un correspondant qu'entre un mobile et un agent mère. Il n'est pas raisonnable de supposer qu'il existe a priori un quelconque lien de confiance entre un terminal et un correspondant pris au hasard sur Internet. Par conséquent, une attaque en vol de session pourra profiter de cette faiblesse. D'autres attaques en déni de service sont également possibles en se faisant passer pour l'agent mère. Un attaquant pourrait ainsi intercepter les Binding Update émis par le mobile en direction de l'agent mère et acquitter ces messages au nom de ce dernier. De cette manière plus aucun message à destination du mobile ne lui parviendrait.

3.2.3 Attaques sur le réseau visité

Les réseaux visités pour les mobiles devront être ouverts et pouvoir accueillir des machines mobiles en provenance de différents réseaux. Même si ces machines sont parfaitement identifiées sur le réseau, rien ne les empêche d'exécuter des attaques sur les équipements du réseau visité (serveur d'authentification ou facturation, DNS ou serveur applicatif). Le risque est encore plus grand lorsque la technologie d'accès au réseau, au niveau 2, ne procède à aucun filtrage des mobiles. Par exemple, certaines architectures de mobilité sur IEEE802.11 permettent à n'importe quel mobile d'établir une connexion au niveau radio et, seulement après, de procéder à l'authentification au niveau IP. Cette première connexion libre préalable à l'authentification peut dans certains cas être suffisante pour lancer des attaques contre le réseau. On pourrait craindre par exemple des attaques en déni de service sur les équipements du réseau visité ou même des attaques sur les autres mobiles. Notons que les mobiles sont en vue directe les uns des autres sans firewall pour les isoler.

3.2.4 Attaques sur les autres machines de l'Internet

Les attaques en déni de service distribué (DDoS) consistent pour une machine attaquante à lancer un grand nombre de requêtes sur un grand nombre de serveurs en modifiant l'adresse source des paquets IP[CHA 02]: au lieu d'indiquer son adresse, elle donne celle de la victime.
Les serveurs vont alors tous répondre en même temps. Mais compte tenu de l'adresse source falsifiée, les messages se dirigeront vers la victime qui sera inondée. La parade consiste à vérifier que les adresses d'émission des paquets reçus sont valides, c'est-à-dire qu'elles respectent la topologie du réseau. C'est ce qu'on appelle l'ingress filtering: quand un routeur reçoit un paquet sur une interface, il vérifie que l'adresse source du paquet appartient bien à un réseau connecté à cette interface.

3.3 Les besoins de sécurité

Vu le grand nombre nombres d'attaques qui menacent Mobile IP, six besoins de sécurité sont devenues vitales, ils représentent les facteurs communs que doit assurer un système sécurisé dans l'environnement mobile[JAC97].

3.3.1 L'authentification

Permet de s'assurer de l'identité du correspondant, c'est à dire de vérifier qu'il est bien celui qu'il dit être[SCH02]. Lorsqu'un MN reçoit un message d'avertissement de la part d'un des foreign agents, il aura besoin de s'assurer que ce message provient d'un FA légitime. Sans authentification des acteurs de la communication, un FA malintentionné pourra facilement ″ voler ″ l'identité d'un FA légitime et prétendra être lui, de plus il pourra envoyer la demande d'enregistrement d'un nœud mobile avec une adresse autre que son adresse mère et de cette manière le nœud ne recevra jamais une réponse d'enregistrement de la part de son HA.
De la même manière, le FA et le HA doivent authentifier les nœuds voulant accéder au domaine étranger, le HA par exemple doit s'assurer que la demande d'enregistrement provient d'un nœud légitime sinon il va accepter l'enregistrement du nœud malveillant et il va lui envoyer par la suite les paquets sensés être destinés au vrai MN.

3.3.2 L'intégrité

Assure que les données transmises ne sont pas altérées au cours de la transmission. Chaque message envoyé entre le MN, le FA et HA doit rester intègre. Une attaque sur l'intégrité du trafic se fait par exemple en altération d'une réponse d'enregistrement d'une réponse positive en une autre négative[COM99].

3.3.3 L'autorisation (control d'accès)

L'objectif du contrôle d'accès est de vérifier qu'une entité a effectivement le droit d'accéder au réseau et d'exploiter ses ressources[COM99].

3.3.4 La confidentialité

Assure qu'une information transmise n'est accédée que par une personne autorisée[COM99].

3.3.5 La non-répudiation

L'émetteur du message ne doit pas nier l'envoi ou la réception d'un message. Lorsque le nœud mobile visite un domaine étranger, il consomme certaines ressources (paquets émis/reçus, paquets detunnelés par le FA, affectation d'une adresse IP), le FA pourra identifier les ressources exploitables par chaque MN pour effectuer sa comptabilité sauf si ce dernier nie sa visite à ce domaine ou son exploitation de ses ressources.

La signature numérique était la solution proposée pour palier à la répudiation[COM99].

3.3.6 La gestion des clés

Des techniques cryptographiques ont été conçu pur assurer l'authentification et l'autorisation des entités ainsi que l'intégrité et la confidentialité du flux transmis tel que les algorithmes à clé secrète, les algorithmes à clé publique, les fonctions de hachage, la signature numérique, etc. Toutes ces technique repose sur l'utilisation d'une ″clé″.

La gestion des clés est le point le plus critique de la cryptographie. En effet, la distribution ou l'échange non sécurisé de certaines clés cause la vulnérabilité de tous le système, donc il faut s'assurer que la génération, la distribution et l'échange des clés doit être adéquate.

3.4 Les schémas d'authentification proposés pour Mobile IP

L'authentification est considéré comme le service de sécurité le plus important [SCH 95], en effet, il faut s'assurer tout d'abord de la bonne identité des parties avant de leur permettre la communication et l'échange de données.
Selon les acteurs de Mobile IP, il est clair que les motivations d'authentification dans ce protocole se résume en trois relations: [SCH01]

1. *Authentification entre le MN et son réseaux mère :* pour interdire un nœud mal intentionné d'accéder au paquets IP dessinés à un nœud légitime.
2. *Authentification entre le MN et le réseau visité :* pour contrôler l'accès au ressources tout en assurant une comptabilité sécurisé (secure accounting).
3. *Authentification entre le réseau mère et le réseau visité :* pour contrôler les permissions d'accès aux ressources du réseau visité d'une part et de vérifier les droit d'accès des nœuds dans ce nouveau réseau d'une autre part. (Figure 3.1)

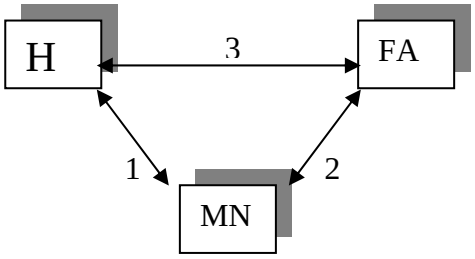

Figure 3.1 : Les motivations d'authentification MIP

Le principe commun entre toutes les propositions de sécurisation du protocole Mobile IP [BOU03][ZAO97][PAC02] repose sur *l'assurance des ces trois relations de confiance*.
Dans ce qui suit nous allons étudié quelques solutions proposée pour la sécurisation de MIP et en particulier la sécurisation de la procédure d'authentification.

3.4.1 L'authentification standard dans Mobile IP

L'authentification standard est une solution intégrante dans Mobile IP.
Le principe était simple: chaque entité signe le flux de messages qu'elle envoie et cela par l'ajout d'un condensât (signature) comme extension aux messages de contrôle. Le format de l'extension est comme suit: (figure3.2)

- *Le type* : indique le type de l'authentification : 32 pour l'authentification MN/HA, 33 pour l'authentification MN/FA et 34 pour celle FA/HA.
- *Length:* Indique la longueur de l'extension.
- *SPI (security parameter index):* Identifie l'association de sécurité établie entre les différentes parties avant l'enregistrement (l'algorithme choisi, la paire de clé publique /privé utilisée pour calculer le condensât,…)
- Authenticator: c'est le condensât ou le hachage du message d'enregistrement.

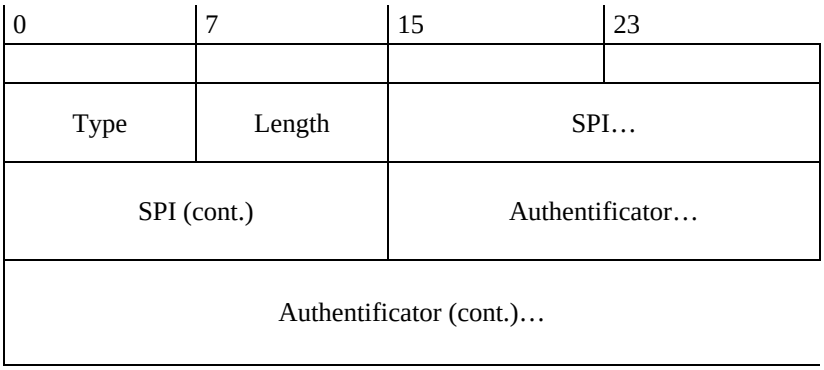

Figure 3.2 : Le format d'une extension d'authentification dans Mobile IP.

Voyons maintenant l'intégration des extensions aux messages d'enregistrement :
1) Un nœud mobile ″écoute″ les messages d'avertissement en provenance du FA , puis crée et envoie le message d'enregistrement (*RegReq*) au FA, ce message contient:

- Des drapeaux (*Flags*)
- La durée d'enregistrement (*Lifetime*)
- L'adresse mère du nœud mobile ($addr_{MN}$).
- L'adresse mère de l'agent mère ($addr_{HA}$).
- L'adresse temporaire du MN (*COA*).
- Un identificateur de la requête (*IdReq*) .
- Un identificateur d'accès au réseau /Network Access Identifier:(NAI_{MN})
- Une extension d'authentification (*Sig*) qui sera vérifiée par le HA, et une autre qui sera optionnellement vérifiée par le FA.

$$MN \rightarrow FA : \{RegReq, Flags, Lifetime, Addr_{MN}, Addr_{HA}, CoA, IdReq, NAI_{MN}, Sig_{MN, HA}, [Sig_{MN, FA}]\}$$

2) A la réception, le FA vérifie la validité de la signature $Sig_{MN, FA}$ (s'il elle existe) puis crée sa signature $Sig_{FA, HA}$ et l'envoie au HA.

$$FA \rightarrow HA : \{RegReq, Flags, Lifetime, Addr_{MN}, Addr_{HA}, CoA, IdReq, NAI_{MN}, Sig_{MN, HA}, [Sig_{MN, FA}], [Sig_{FA, HA}]\}$$

3) A son tour, le HA s'assure de l'authenticité du message par la vérification des deux signatures $Sig_{MN, HA}$ et $Sig_{FA, HA.}$ En cas de succès, le HA répond en envoyant un Registration Replay (*RegRep)* signé $Sig_{HA, FA}$

$$HA \rightarrow FA : \{RegRep, Code, Lifetime, Addr_{MN}, Addr_{HA}, IdRep, NAI_{MN}, Sig_{HA, MN}, [Sig_{HA, FA}]\}$$

4) Le FA vérifie que cette réponse provient effectivement du HA (vérification du la signature $Sig_{HA, FA}$), en cas de succès le FA ajoute sa signature $Sig_{FA, MN}$ puis envoie la réponse au nœud mobile.

$$FA \rightarrow MN: \{RegRep, Code, Lifetime, Addr_{MN}, Addr_{HA}, IdRep, NAI_{MN}, Sig_{HA, MN}, [Sig_{HA, FA}], [Sig_{FA, MN}]\}$$

5) Si le MN vérifie les extensions d'authentification et trouve que toutes les signatures sont valides et si le HA a accepté la demande d'enregistrement alors le MN s'est donc enregistré avec succès .
Notons que la signature est par définition le hachage du message chiffré avec la clé partagée entre l'émetteur et le récepteur [BID95]. Le récepteur effectue la même opération pour vérifier la validité de la signature c'est à dire qu'il hache le message reçu et il le chiffre à l'aide de la clé partagée, si les deux condensats signés sont égaux alors la signature est valide.
Au premier coup d'œil ce schéma parait suffisant pour réaliser les trois relations d'authentification citées dans le paragraphe 3.4. Néanmoins, il comporte plusieurs inconvénients : il considère l'existence d'une relation de confiance pré-établie entre les trois acteurs (MN, FA, HA). Cependant, il n'est pas raisonnable de supposer l'existence à priori de quelconque lien de confiance entre ces parties puisque n'importe quel acteur peut être lui-même un malveillant (voir §3.2), et même si on considère que les trois entités partagent des clés entre elles, cette solution reste inefficace en l'absence d'une entité responsable de la gestion des clés, en particulier lors d'un handoff inter-domaine où les opérateurs sont distincts. De plus, dans ce schéma, la clé secrète partagée entre le FA et le HA est établie à l'aide du standard IKE (Internet Key Exchange) d'IPsec [RFC2401][RFC2409] qui est un protocole à objectif très générique et qui nécessite plus d'efforts que le Mobile IP a besoin.

3.4.2 L'authentification basée sur les clés publiques

Ce schéma a été proposé par [ZAO97], il était parmi les premières tentatives de sécurisation du protocole Mobile IP. Les auteurs ont supposé que chaque entité possède une paire de clé publique/privé certifiée. Pour une assurer l'authentification mutuelle, les trois entités Mobile IP associent au messages échangés leurs signatures et certificats comme preuve d'identité (Figure3.3)

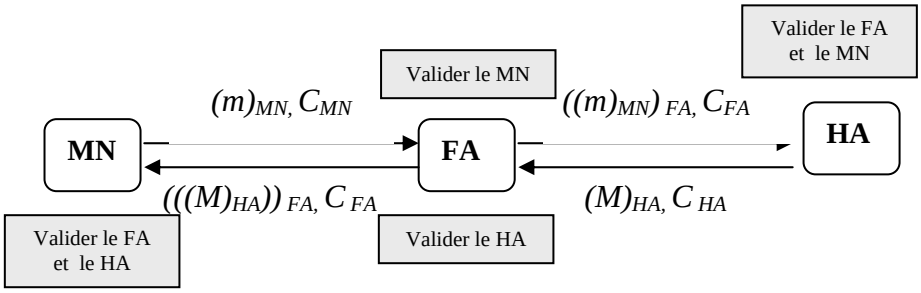

Figure 3.3: Authentification basée sur les clés publiques

Le principe est simple : le nœud mobile envoie au FA le message signé avec sa clé privée $(m)_{MN}$ et son certificat (C_{MN}). Le FA authentifie le nœud en vérifiant la validité de son certificat. Il signe à son tour le message reçu avec sa clé privée $((m)_{MN})_{FA}$, associe son certificat C_{FA} et envoie le tout a son home agent.
A la réception de ce message, le HA authentifie le FA et le MN et procède de la même manière, signe le message $(M)_{HA}$ et fait attacher son certificat $C_{HA,}$ le FA l'authentifie puis signe le message reçu $(((M)_{HA}))_{FA}$ et fait attacher associe son certificat C_{FA}, de cette manière le nœud mobile authentifie le FA et déduit l'authenticité du HA.

Ce schéma assure la non répudiation grâce à l'utilisation des certificats. De cette manière aucune entité ne peut nier l'émission ou la réception, de plus c'est un schéma scalable puisqu'il suffit qu'une nouvelle entité ait un certificat valide pour s'authentifier puis entrer en communication avec les autres entités. Néanmoins, ce mode d'authentification reste lourd en particulier pour les nœuds mobiles à cause de l'utilisation des algorithmes a clés publiques qui nécessitent une grande puissance de calcul.

Une amélioration a été proposée au schéma précédant en diminuant le nombre de certificats utilisés en admettant l'existence d'une certaine association de sécurité entre le nœud et son agent mère. De cette manière, c'est le HA qui authentifie le FA pour le nœud mobile. (Figure3.4)
L'inconvénient de cette solution est qu'il n'est pas raisonnable d'admettre l'existence d'une relation de confiance pré-établie entre les entités.

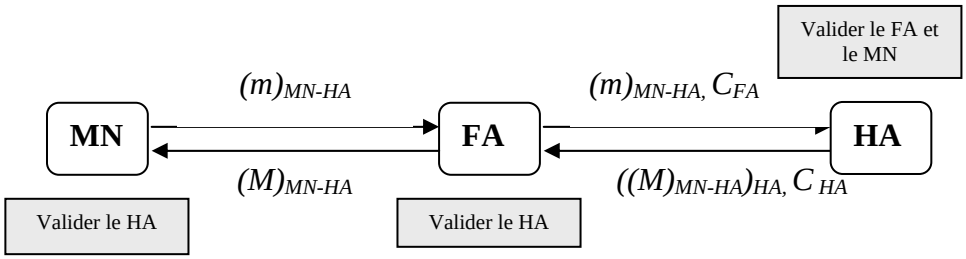

Figure 3.4: Authentification minimale basée sur les clés publiques

3.4.3 L'authentification Mobile IP/AAA

Un grand nombre des attaques pourraient être évitées si un contrôle strict des accès au réseau visité était effectué avant toute opération d'enregistrement à l'agent mère. Ce contrôle est assez facile pour des mobiles se connectant à un réseau visité de leur domaine administratif, autrement dit sous la même administration qu'eux même.

En effet, l'unicité du domaine permet d'établir un lien de confiance fort entre le mobile, le réseau visité et l'agent mère. Ce lien se matérialise généralement par le partage d'une association de sécurité IPsec entre ces équipements, c'est-à-dire une configuration commune d'IPsec qui permet au moins une authentification des données qu'ils échangent. Ainsi, lorsqu'un mobile arrive sur un réseau visité le simple fait qu'il parvienne à signer des paquets garantit qu'il appartient bien au domaine.

Le problème se complique considérablement lorsque les mobiles doivent pouvoir changer de domaine administratif. En effet, il faut fournir au réseau visité des moyens d'authentifier un mobile qui ne le connais pas, d'enregistrer des informations sur les ressources consommés par lui (temps de connexion, volume de données échangées, …) dans le but d'établir une facturation.
Ces fonctions d'Authentification, d'Autorisation et de comptabilisation sont réunis dans les services AAA (Authentication, Authorization and Accounting).
En l'an 2000, un groupe de travail de l'IETF a suggéré l'intégration des architectures AAA dans Mobile IP dans le but d'améliorer le niveau de sécurité de ce protocole.

Les éléments générique d'une architecture AAA sont: [RFC2977] (Figure 3.5)

- *Le demandeur* : c'est la machine qui cherche à se connecter, il est identifié par un NAI (Network Access Identifier) de la forme *utilisateur@domaine*.
- *Le vérificateur* : est l'équipement qui reçoit les demandes de connexion du demandeur. Son rôle est uniquement de recevoir les demandes, de les transmettre au AAAL et selon la réponse que ce dernier lui retourne, autorise ou interdit la connexion .

  Le vérificateur et l'AAAL font partie du même domaine administratif, il partage donc une association de sécurité entre eux qui leur permis le transfert sécurisé des données entre eux .
- *Le AAAL :* c'est le serveur AAA du réseau visité. Il ne peux pas authentifier le demandeur que si ce dernier appartient lui aussi au réseau visité .

Si ce n'est pas le cas, le AAAL transmet la demande au AAAH du domaine du demandeur (identifiable par la partie «@domaine» du Network Access Identifier (NAI).

- *Le AAAH :* est le serveur AAA du réseau mère du demandeur. Il est capable d'identifier le demandeur, et de transmettre ses droits au AAAL qui a son tour les transmettra au vérificateur

Les concepteurs ont remarqué qu'une telle architecture se calque également assez bien sur un réseau de mobilité IPv4, Le vérificateur est dans ce cas le foreign agent. (figure 3.5)

Lorsqu'un mobile se connecte au réseau visité, il envoie une demande d'enregistrement (1) au Foreign Agent en lui précisant son identifiant NAI de la forme *utilisateur@domaine*. Celui-ci transmet la demande (2) au AAAL qui, en fonction la partie domaine de l'identifiant du mobile, détermine vers quel AAAH il doit transmettre la demande (3). Le AAAH, une fois la demande reçue, effectue la vérification de l'identité de l'utilisateur et de ses droits.

Si l'utilisateur est autorisé, le AAAH transmet la demande de connexion (4) à l'agent mère qui enregistre la nouvelle position du mobile et répond par le même chemin.

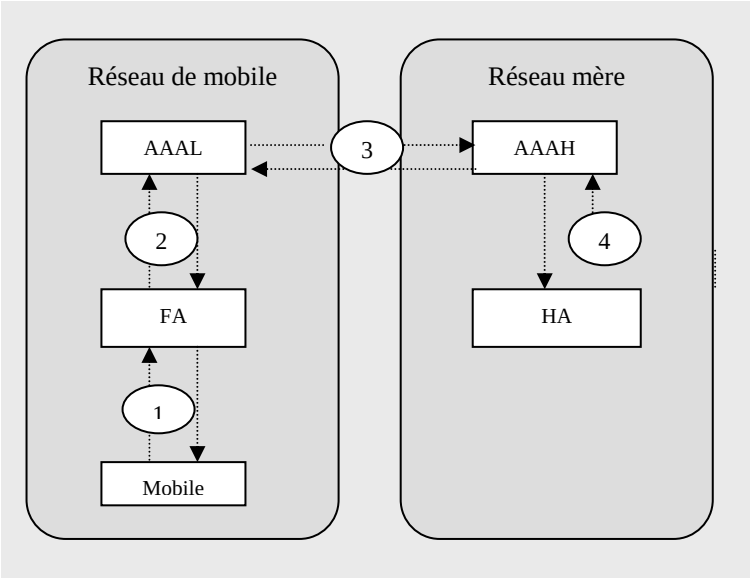

Figure 3.5 : Les architectures AAA et la mobilité IPv4

3.5 Le protocole Diameter

Diameter est un protocole permettant à des domaines administratifs différents de collaborer pour réaliser les fonctionnalités AAA [BOU03], il a été proposé par l'IETF au début de l'année 2000.
Il est constitué d'un protocole de base qui définit
- Le format des messages (comment ils sont transportés).
- Les messages d'erreurs
- Les services de sécurité.

Le protocole de base Diameter est un protocole extensible à ajouter d'autres applications (*Diameter Extensible Authentication Protocol (EAP) Application, Diameter CMS Security Application, Diameter Network Access Server Application,…).*
Diameter /Mobile Ipv4 est une des applications de ce protocole. L'idée générale est que Diameter permet d'authentifier un utilisateur avant de lui permettre l'accès à des ressources, cet accès pouvant être restreint à certains services. Il faut qu'il existe des accords entre ces domaines. Ainsi, si l'opérateur A a des accords avec l'opérateur B, les clients de A peuvent obtenir des services de B et inversement.

3.5.1 Les acteurs de Diameter dans Mobile IP

Les acteurs sont les acteurs déjà cité dans le paragraphe précédant, mais cette fois nous allons les présenter relativement au protocole Diameter.
L'architecture préconisée dans Diameter dans un environnement de mobilité IPv4 fait intervenir les acteurs suivants: (Figure 3.6)[RFC2977]

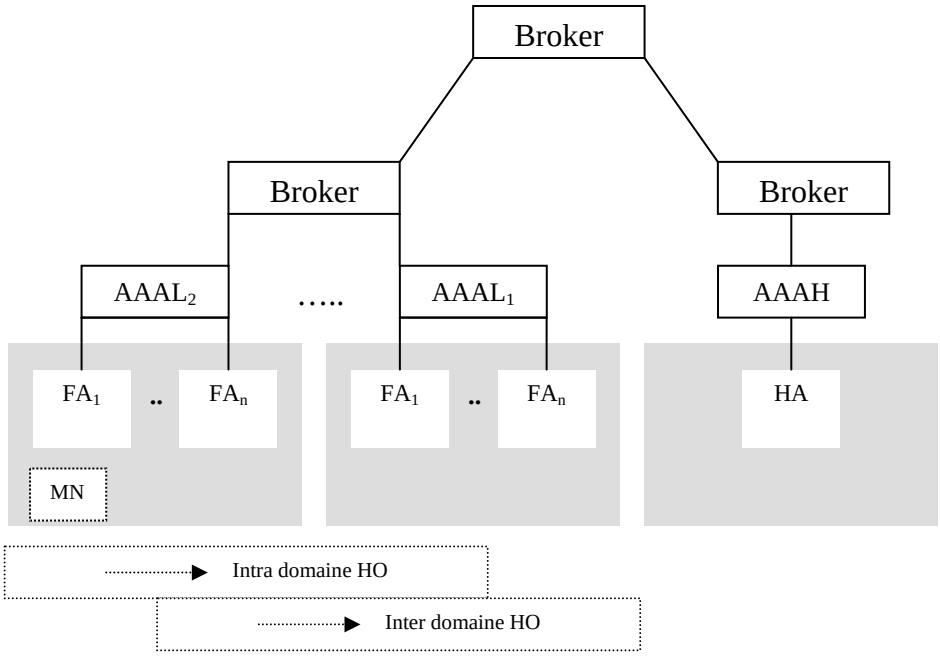

Figure 3.6: Les acteurs de Diameter dans MIPv4

- ***Home AAA (AAAH)*** *(ou Home Diameter Server)* : authentifie et autorise un mobile à s'enregistrer auprès d'un HA spécifique. Il peut servir de centre de distribution de clés et de créer des clés temporaires pour protéger le trafic entre les différents acteurs .
- ***Home Agent (HA)*** : rend les mêmes fonctions que l'agent mère défini dans mobile IPv4 : enregistre l'adresse courante du mobile, redirectionne les paquets vers le mobile et gère l'attribution des adresses mères.
- ***Foreign AAA (AAAF)*** *(ou Local Foreign Server AAAL)* : relaye les demandes d'authentification en provenance de l'un des FA(s) au serveur AAAH approprié.
- ***Foreign Agent (FA) :*** rend les mêmes fonctions que l'agent visité dans Mobile IPv4: possibilité d'enregistrer la correspondance entre l'adresse courante et l'adresse mère mais participe encore à l'authentification du mobile. Pour cela, il peut envoyer un challenge au mobile lorsque ce dernier s'enregistre, ce qui permet de se prémunir des attaques par replay. Il devra ensuite transmettre la réponse du mobile au serveur AAAL pour vérification de sa validité.
- ***Mobile Node (MN) :*** garde en mémoire la correspondance entre l'adresse courante du mobile et son adresse mère. Il s'authentifie en répondant au challenge du FA.

Une fois l'enregistrement et l'authentification effectués, seul le FA, le HA et le MN interviennent comme dans un contexte de mobilité IPv4.

Il existe un autre acteur appelé *Broker AAA* qui intervient lorsqu'un AAAL ne partage pas de secret avec le AAAH. Le Broker AAA qui doit partager une association de sécurité avec chacun des serveurs AAAH et AAAL peut alors mettre en relation AAAH et AAAL de façon sécurisée en certifiant à ces deux serveurs l'identité de l'autre. Les communications entre AAAL et AAAH peuvent être soit relayées par le

Broker AAA, soit directe une fois qu'une clé de session commune est établie. Des certificats[3] peuvent être émis par le Broker AAA pour tous les serveurs AAA.
La figure 3.6 montre que
- Les secteurs en commun représentent les domaines administratifs des entités du réseau .
- Chaque domaine administratif contient un ou plusieurs AAAL et multiples FA(s).
- Les serveurs AAA des différents domaines s'interagissent directement à travers les Broker AAA - Le domaine mère d'un nœud mobile contient un AAAH et un ou plusieurs HA.
- Le MN effectue soit un *inter-domaine handover* (déplacement d'un domaine à un autre) , soit un *intra-domaine handover* (déplacement dans le même domaine). (figure3.6)

3.5.2 Le fonctionnement de Diameter dans Mobile IPv4

Dans le cadre du protocole Diameter, il est nécessaire que ses modules partagent des associations de sécurité (SA)″ *statique* ″ représentées dans la figure3.7 par des lignes continues et qui sont établies entre :
- FA et AAAL (SA_1).
- MN et AAAH (SA_2).
- HA et AAAH (SA_3).
- AAAL et AAAH (SA_4). Ce qui évite la dégradation des performances liée à l'implication des Brokers
- Serveurs AAA et un ou plusieurs Brokers (s'il n'y a pas une association de type SA_4).

Les liens dynamiques devrant être établies sont présentées par des pointillé dans la (Figure 3.7)

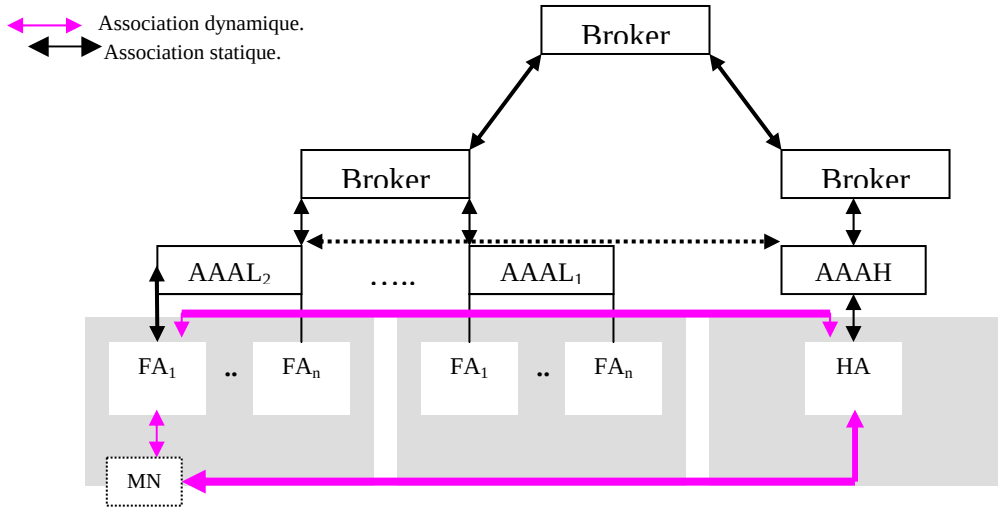

Figure 3.7 : Les associations de sécurité statiques et dynamiques dans Diameter.

Le flux de messages d'authentification dans Diameter est montré dans la figure3.8[SCH02]

[3] Le certificat numérique est un fichier de un millier d'octets qui prouve un lien entre un individu et sa clé publique, il contient d'abord, en clair, son identité et sa clé publique**. [SCH 02]**

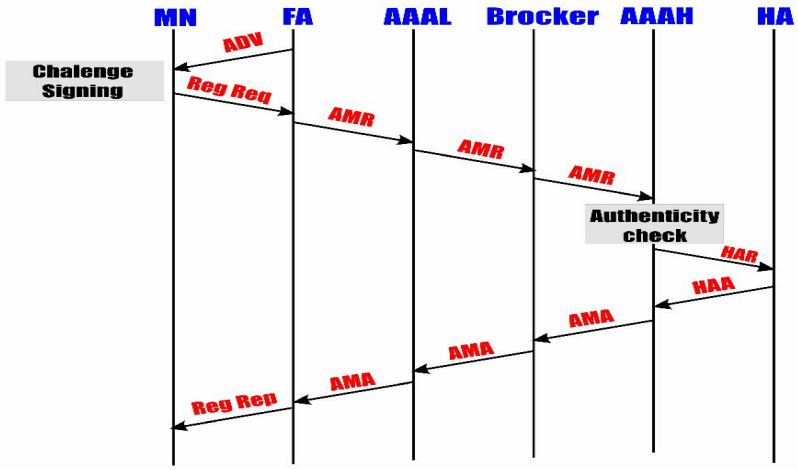

Figure 3.8: Le flux de messages d'authentification dans Diameter

1) Tous les FA(s) envoient périodiquement des messages d'avertissements contenant le NAI qu'il les identifie et un challenge qui contient un nombre aléatoire x_{FA}.

$$FA \rightarrow MN : \{Advertisement,\ldots, NAI_{FA}, x_{FA}\}$$

2) Le MN stocke le NAI reçu du FA, crée un message d'enregistrement Mobile IP *(RegReq*)qui contient le nombre aléatoire x_{FA}, son NAI_{MN} et une signature qui doit être vérifiée par le AAAH ($Sig_{MN, AAAH}$), ce message est envoyé au FA.

$$MN \rightarrow FA : \{RegReq,\ldots, x_{FA}, NAI_{MN}, Sig_{MN, AAAH}\}$$

3) Le FA crée un message d'enregistrement AMR qui contient la demande d'enregistrement du MN et l'envoie à son AAAL.

$$FA \rightarrow AAAL :\{AMR,\ldots, \ldots RegReq,\ldots, x_{FA}, NAI_{MN}, Sig_{MN, AAAH}\}$$

4) Le AAAL envoie de sa part ce message directement ou indirectement (sans l'utilisation des Brokers) au AAAH qui peut être connu par le $NAI_{MN.}$

$$AAAL \rightarrow AAAH:\{AMR,\ldots, \ldots RegReq,\ldots, x_{FA}, NAI_{MN}, Sig_{MN, AAAH}\}$$

5) Le AAAH vérifie la signature $Sig_{AAAH, MN}$ du mobile, si la signature est valide le AAAH déduira que c'est bien le MN qui a crée le message d'enregistrement.

Le AAAH crée maintenant un nouveau message HAR qui contient le message de registration original du MN, une clé de session $K_{MN, HA}$ qui va être partagée entre le MN et HA, une autre clé $K_{FA, HA}$ qui va être partagée cette fois entre le FA et le HA. Ces deux clés sont chiffrés avec une clé secrète $K_{AAAH, HA}$ partagée entre le AAAH et le HA.

De plus, le AAAH fait la même chose pour le MN, il inclut deux clés de session $K_{MN, FA}$ et $K_{MN, HA}$ pour être distribué au MN. De la même manière ces deux clés seront chiffrées avec la clé secrète $K_{MN, AAAH.}$

$$AAAH \rightarrow HA:\{HAR,\ldots,RegReq,\ldots NAI_{MN,}\{K_{MN, HA,} K_{FA, HA}\} K_{AAAH, HA},\{K_{MN, FA,} K_{MN, HA}\}K_{MN, AAAH,} Sig_{AAAH,HA}\}$$

6) A la réception de ce message le HA vérifie la validité de la signature, enregistre le nœud mobile avec l'adresse temporaire contenue dans le message de registration, il décrypte et stocke les deux clé de session $K_{MN, HA}$ et $K_{FA, HA}$, il crée par la suite une réponse d'enregistrement (*RegRep*) qui contient aussi les clés de session telle qu 'elles ont été envoyées par le AAAH, puis il signe le tout avec $Sig_{HA, MN.}$
Le message (*RegRep*) est inséré dans une réponse HAA et envoyé au AAAH, confirmant ainsi le succès de l'enregistrement du MN.

$$HA \rightarrow AAAH : \{HAA,\ldots, (RegRep,\ldots,\{K_{MN, FA}, K_{MN, HA}\}K_{MN, AAAH,} Sig_{HA, MN}), Sig_{HA,AAAH}\}$$

7) Le AAAH crée sa réponse d'enregistrement AMA qui contient le (*RegRep*) inclue dans le message HAA. Si le nœud mobile s'est enregistré chez le HA avec succès, le AAAH inclue une clé de session au FA , tout ce message est signé puis envoyé au AAAL.

$$AAAH \rightarrow AAAL : \{AMA,\ldots,x_{FA,} \{K_{MN, FA}, K_{FA, HA}\}K_{AAAH, AAAL,} (RegRep,\ldots,\{K_{MN, FA}, K_{MN, HA}\}K_{MN, AAAH}, Sig_{HA,MN}), Sig_{AAAH, AAAL}\}$$

8) Le AAAL vérifie la validité des signatures, extrait les clés du FA, puis il les rechiffre à l'aide de $K_{FA, AAAL}$.

$$AAAL \rightarrow FA :\{AMA,\ldots, x_{FA,} \{K_{MN, FA}, K_{FA, HA}\}K_{FA, AAAL} ,(RegRep,\ldots,\{K_{MN, FA}, K_{MN, HA}\} K_{MN, AAAH}, Sig_{HA, MN}) Sig_{AAAL, FA}\}$$

9) A la réception de ce message, le FA vérifie la signature du message puis il commence le traitement du AMA: si le AMA signale le succès de l'enregistrement du MN le FA déduit que le MN a signé correctement le nombre aléatoire envoyé à l 'étape 2.
Le FA décrypte et stocke les deux clés $K_{MN, FA}$ et $K_{FA, HA}$ puis envoie le (*RegRep*) au MN.

$$FA \rightarrow MN :\{RegRep,\ldots,\{K_{MN, FA}, K_{MN, HA}\}K_{MN, AAAH}, Sig_{HA, MN}\}$$

10) Le MN décrypte les deux clés de session envoyées par le AAAH, il les stocke puis utilise la clé $K_{MN, HA}$ pour vérifier la signature $Sig_{HA, MN}$ qui a été crée dans la sixième étape .
Si toutes les vérifications se terminent avec succès , cela veut dire que le FA a bien authentifié et accepté l' enregistrement du nœud mobile MN.

Notons que dans le cas où le nœud mobile voudrait ré-enregistrer (par exemple après expiration du Lifetime), il va utiliser les mêmes clés de session obtenues lors d'une ancienne session Mobile IP/AAA.

On remarque que le schéma d'authentification Mobile IP/AAA a résolu le problème de la génération et de distribution des clés grâce au serveur AAAH qui se charge de faire cette tache d'une manière sécurisé. Néanmoins, ce schéma comporte encore quelques problèmes en terme de sécurité et de performance:
- Le grand nombre de d'entités impliqué dans ce schéma rend l'analyse de la sécurité plus difficile.[SCH02]
- La réponse au challenge du FA est distribuée le FA fournit un nombre aléatoire (le chalenge), mais il ne peut vérifier la réponse du challenge il doit faire confiance au AAAH du nœud mobile.
- D'une autre part, le AAAH peut vérifier la réponse du challenge, mais il ne peut pas déduire ″la frecheur″ (the freshness) de ce challenge du moment que ce dernier n'a pas été crée par le AAAH lui-même.
- Le message *Registration Request* envoyé par le mobile à son foreign agent est un message Mobile IP non chiffré. Le fait que ce message ne soit pas chiffré implique qu'un intrus sur le lien pourra obtenir des informations sur le nœud ou sur son domaine mère .

3.6 Conclusion

Apres avoir expliquer le fonctionnement du protocole Mobile IP, nous nous sommes intéressés dans ce chapitre à l'étude d'un aspect important de la qualité de service de ce protocole qui est la sécurité et plus précisément la sécurité de la procédure d'authentification.
L'idée principale de l'authentification dans Mobile IP est de s'assurer tout d'abord de la bonne identité des parties avant de leur permettre l'accès, la communication et l'échange de données dans le réseau visité.
Les tentatives de sécurisation du protocole Mobile IP sont variées mais nous avons constaté que le point commun entre elles est de garantir trois relations de confiance de base : entre le home et le foreign agent, entre le home agent et le nœud mobile et entre le nœud mobile et le foreign agent.
La première proposition de sécurisation avec du protocole Mobile IP appelée ″authentification standard″[RFC2002] était une partie intégrante du protocole lui-même, en effet pour prouver son identité, chaque entité signe numériquement ce qu'elle envoie (messages de control, acceptation, refus, …) et cela à l'aide de la clé partagée avec l'entité réceptrice.

Malgré que cette solution soit simple et facile à implémenter mais elle s'est avérée insuffisante en l'absence d'une entité de gestion de clés. De plus, la solution est non scalable du moment que le nœud mobile doit gérer lui-même le grand nombre de clés partagées avec l'ensembles des home et foreign agent(s).

[ZAO97] a proposé l'usage des algorithmes cryptographiques asymétriques comme solution aux problèmes de distribution des clés de session. Bien que cette solution garantisse la non-répudiation et diminue le nombre de clés partagées (une seule paire pour chaque entité), elle manque d'un centre de certification des clés asymétriques.
Le schéma d'authentification Mobile IP/AAA proposé par l'IETF a donné un autre vision à l'étude de l'authentification: Pourquoi ne pas profiter du niveau de sécurité élevé fourni par les structures AAA pour sécuriser Mobile IP ?. En effet, ce schéma résolu le problème d'absence de l'entité responsable de gestion des clés puisque le home server dans cette architecture est dédié pour cette tâche. Le protocole Diameter, dédié au structures AAA permet aux opérateurs une authentification sûre des utilisateurs ayant souscrit un abonnement auprès d'un autre opérateur. Néanmoins, cette proposition comporte aussi plusieurs inconvénient telle que l'augmentation du temps du handover puisque la demande d'enregistrement passent par plusieurs entités intermédiaires (serveurs AAA, brokers, …), la centralisation de l'outil de gestion de clé (une seule entité gérante de clés) et le problème de l'authentification locale.
Dans le chapitre suivant, nous proposerons un nouveau schéma d'authentification pour Mobile IP qui repose sur l'authentification AAA et qui essaye de résoudre les problèmes posés dans ce mode d'authentification.

Chapitre VI *Un nouveau schéma d'authentification pour le protocole Mobile IP*

4.1 Introduction

Dans les chapitres précédents nous avons vu que beaucoup de travaux ont été proposés pour améliorer la sécurité de l'authentification du protocole Mobile IP[RFC2002] [ZAO97][RFC2977], mais qui restent insuffisants en matière de sécurité et de performance. L'authentification standard [RFC2002] considère la pré-existence des liens de confiance entre les acteurs Mobile IP. Cette solution s'est avérée insuffisante à cause de la non scalabilité et l'absence d'une entité digne de confiance qui se préoccupe de la gestion des clés entre ces acteurs. Zao a proposé l'utilisation des cryptosystèmes à clé publique pour résoudre le problème de la scalabilité de l'authentification standard[ZAO97]: chaque entité possède une paire de clé publique et privée utilisée pour chiffrer et signer. C'est une solution qui garantit essentiellement la non-répudiation, mais elle reste théorique en particulier pour les nœuds mobiles puisque les algorithmes à clé publique nécessitent une grande puissance en capacité et en temps de calcul.

Le schéma d'authentification Mobile IP/AAA est venu remédier à l'absence de l'outil de gestion de clés dans l'authentification standard. Le home server (AAAH) est devenu l'entité responsable de la gestion sécurisée des clés dans ce schéma. Cette entité se charge de générer et de distribuer les clés de communication grâce aux associations de sécurité statiques existantes entre le AAAH et les acteurs Mobile IP. Néanmoins, ce mode d'authentification comporte essentiellement deux points faibles: Le premier est la centralisation de l'outil de gestion de clés ; dans ce schéma il y a que le home server qui se charge de la gestion sécurisée des clés de tout le système (génération, chiffrement, déchiffrement, distribution) ce qui augmente la charge sur ce serveur. De plus si jamais cette entité tombe en panne tout le système sera exposé aux attaques. Le second problème apparaît lorsque le nœud mobile effectue un intra domain handover (migration vers un foreign agent dans le même domaine que l'ancien), dans ce cas précis le nœud mobile effectue l'authentification des entités en gardant *les anciennes clés de communication* (déjà partagées lors d'une ancienne session MIP/AAA). Cela pose un problème en cas où les clés sont découvertes ou cassées.

Dans ce chapitre, nous allons définir un nouveau schéma d'authentification pour le protocole Mobile IP. Ce schéma propose des améliorations à l'ancien modèle d'authentification Mobile IP/AAA. Nous avons opté de continuer l'exploit et l'amélioration de ce schéma essentiellement parce qu'il est renforcé en matière de sécurité puisque les structures AAA se préoccupent des opérations cryptographiques indépendamment des acteurs du protocole.

4.2 Le problème de la ré-authentification locale dans le schéma Mobile IP/AAA

Rappelons que lors de la dernière étape du schéma d'authentification Mobile IP/AAA (§3.4.3) les trois acteurs Mobile IP partageaient trois clés de communication ($K_{MN,\ FA}$, $K_{MN,\ HA}$, $K_{FA,HA}$), ces clés ont été générées puis distribuées par le AAAH en toute sécurité (Figure 4.1).
Par exemple, si le FA reçoit un message crypté à l'aide de la clé $K_{HA,\ FA}$, s'il arrive à le décrypter, il sera sûr de l'authenticité du HA puisqu'il est le seul à partager cette clé avec lui.

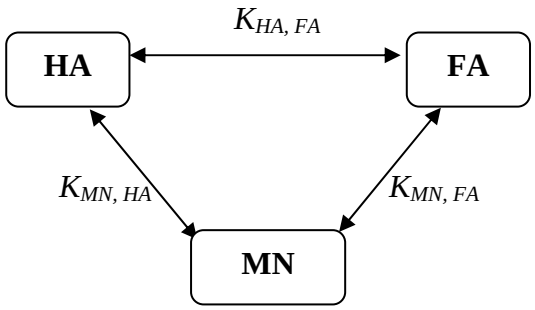

Figure 4.1: Les clés partagées lors de l'authentification Mobile IP/AAA.

Tant que le mobile n'a pas changé de cellule, le home agent, le foreign agent et le nœud mobile, continuent à partager les trois clés de communication :
- $K_{MN,HA}$:entre le nœud mobile et son home agent.
- $K_{MN,FA}$:entre le nœud mobile et le foreign agent.
- $K_{HA,FA}$:entre les deux agents.

Dans le cas où il effectue un intra domain handover, le nœud mobile continuera à utiliser *les mêmes clés* pour éviter de demander de nouvelles auprès du AAAH et d'augmenter la latence du handover (Figure 4.2).

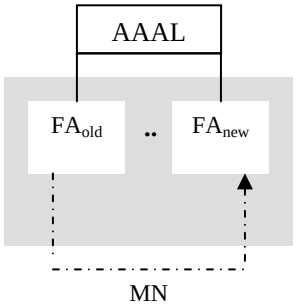

Figure 4.2 : Intra domain handover

En effet, la procédure d'enregistrement est comme suit:
1) Le FA_{new} envoie périodiquement des messages d'avertissements qui contiennent l'identificateur du nouveau foreign agent (Network Access Identifier) NAI_{FAnew} ainsi qu'un nombre aléatoire x_{FAnew} qui doit être signé par le mobile.

$$FA_{new} \rightarrow MN: \{Advertisement,\ldots,NAI_{FAnew}, x_{FAnew}\}$$

2) Le MN crée une demande d'enregistrement qui contient le nombre aléatoire reçu, l'identificateur du nœud NAI_{MN} et celui de l'ancien foreign agent (NAI_{FAold}) et une signature ($Sig_{MN,HA}$), qui va être vérifiée par le home agent et une autre $Sig_{MN,FAold}$ qui va être vérifiée par le FA_{old}.

$$MN \rightarrow FA_{new}: \{RegReq\ldots, x_{FAnew}, NAI_{MN}, NAI_{FAold}, Sig_{MN,HA}, Sig_{MN,FAold}\}$$

3) Le FA crée un message d'enregistrement AMR qui contient le (*RegReq*) et envoie ce message tel qu'il est au AAAL.

$$FA_{new} \rightarrow AAAL: \{AMR,\ldots,RegReq,\ldots,x_{FAnew}, NAI_{MN}, NAI_{FAold}, Sig_{MN,HA}, Sig_{MN,FAold}\}$$

4) Le AAAL vérifie s'il peut accorder la clé de session ($K_{MN,FAold}$) au nouveau FA.

$$AAAL \rightarrow FA_{new}: \{AMA,\ldots, x_{FAnew}, \{K_{MN,FAold}, K_{FAold,HA}\} K_{FAnew,AAAL}\} Sig_{AAAL,FAnew}$$

5) A la réception de ce message, le FA_{new} décrypte les clés de session et grâce à la clé $K_{MN,FAold}$ partagée, il vérifie la signature. Si la signature est valide il continuera l'enregistrement à partir de la deuxième étape de l'authentification standard (§3.4.1).

Cette solution est performante puisqu'elle évite de contacter le domaine mère à chaque demande d 'enregistrement, donc elle évite d'augmenter la latence du handover mais elle déclenche un nouveau problème de sécurité puisque pour s'authentifier en local les trois entités gardent *les anciennes clés de communication* ce qui présente un problème en cas où les clés sont découvertes ou cassées.

Pour cette raison, nous proposons un nouveau schéma d'authentification inspiré du modèle Mobile IP/AAA, où nous avons englober les deux buts: Une meilleure performance et une meilleure sécurité.

4.3 Présentation générale du protocole (Local MIP/AAA)

L'idée de notre proposition est de re-générer de nouvelles clés pour l'authentification tout on évitant de contacter le domaine mère à chaque changement de cellule puisque les clés seront régénérées par le serveur local AAAL et non pas par le home server AAAH[CHE04].
L'architecture proposée est composée d'un domaine mère qui contient le home serveur AAAH, le home agent HA et le nœud mobile MN, et d'un ensemble de domaines étrangers où chaque domaine est composé d'un ou plusieurs AAAL et de multiple foreign agents FA (Figure4.3).

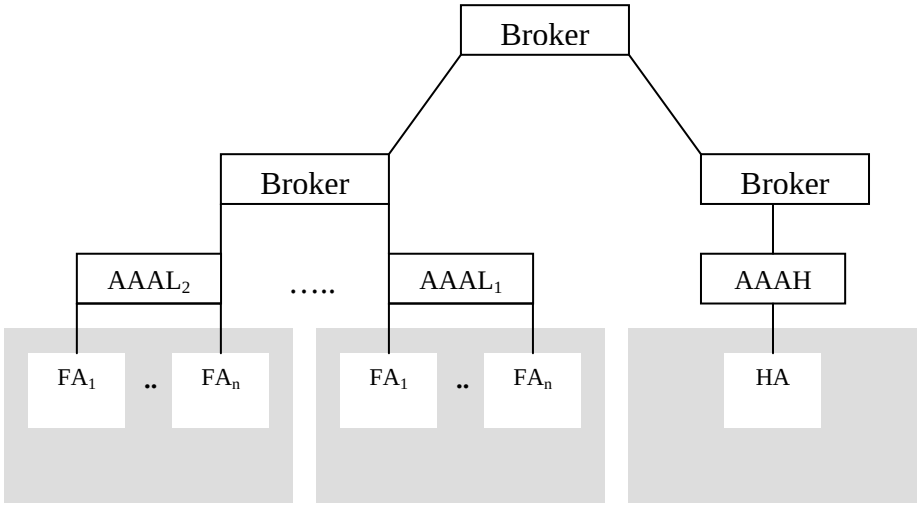

Figure 4.3: Les acteurs de Local MIP/AAA

Notre solution se résume en deux phases importantes:
La première phase: La certification des serveurs locaux AAAL(s) par le brocker (Figure4.4).
La deuxième phase: La génération et la distribution des nouvelles clés au nœud mobile au home agent et au foreign agent, ces clés sont générées et distribuées par les serveurs locaux certifiés (AAAL(s))(Figure4.5).

4.3.1 La certification du serveur local

C'est une phase préliminaire qui s'effectue une seule fois pour initialiser les serveurs.
Son but est double:

- Le premier est la certification des serveurs locaux pour leur permettre la création et la distribution des clés, rôle affecté uniquement au serveur AAAH dans le mode d'authentification MIP/AAA.
- Le second est d'éviter la participation du AAAH lors de la procédure d'authentification.

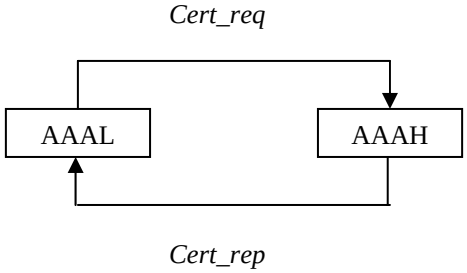

Figure4.4 : La phase de certification

On considère que chaque serveur local AAAL possède un certificat signé par le broker père qui se trouve juste au-dessus dans l'hiérarchie. Un message de demande de certification (*Cert_req*) et le certificat du AAAL ($Cert_{AAAL}$) sont envoyés au home server. Ce message sera crypté par la clé publique du home server (k_{pub_AAAH})

$$AAAL \rightarrow AAAH : \{ Cert\_req, Cert_{AAAL}, \ldots \} k_{pub\_AAAH}$$

A la réception, si la vérification du certificat s'est effectuée avec succès, le AAAH signe à son tour le certificat et renvoie le message au serveur local.

AAAH → AAAL: {Cert_rep, Cert $_{AAAL}$, …. }

Ainsi, le serveur local pourra générer et distribuer des clés puisqu'il a reçu une réponse positive à sa demande.

4.3.2 La génération et la distribution des nouvelles clés

Une fois certifié, le AAAL jouera le rôle d'un home server en générant et en distribuant les clés de session au nœud mobile, au home agent et au foreign agent. (Figure4.5).

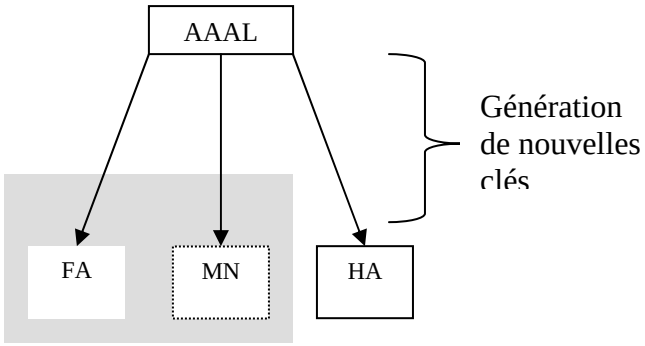

Figure4.5 : Génération et distribution de clés

4.4 Schéma descriptif de la proposition

Dans ce qui suit nous allons décrire le schéma d'authentification que nous proposons pour Mobile IP selon le déplacement du nœud mobile en dehors de son domaine mère
En effet, on considère trois types de handover:

- **TypeI** (*First Inter domain handover*): se déroule lorsque le nœud mobile sort pour *la première fois* de son domaine mère vers un autre étranger. (Figure4.6)
- **TypeII** (*Intra domain handover)*: se déroule lorsque le nœud mobile se déplace à une nouvelle cellule dans le même domaine étranger. (Figure 4.8)
- **TypeIII** *(Inter foreign domain handover)*: se déroule lorsque le nœud mobile migre vers une nouvelle cellule d'un autre domaine étranger. (Figure4.10)

4.4.1 Le handover de Type I (First Inter domain handover)

Dans le premier type de handover, on enregistre *la première migration* du nœud mobile de son domaine mère vers un autre étranger. (Figure4.6)

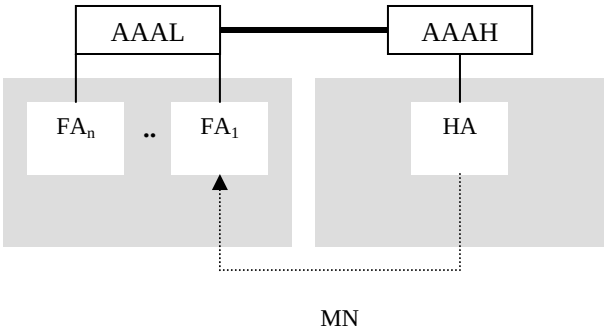

Figure4.6 : First Inter domain handover (Type 1)

Dans ce type de handover, les trois premiers messages échangés sont les mêmes que dans le schéma Mobile IP/AAA (Figure4.7).

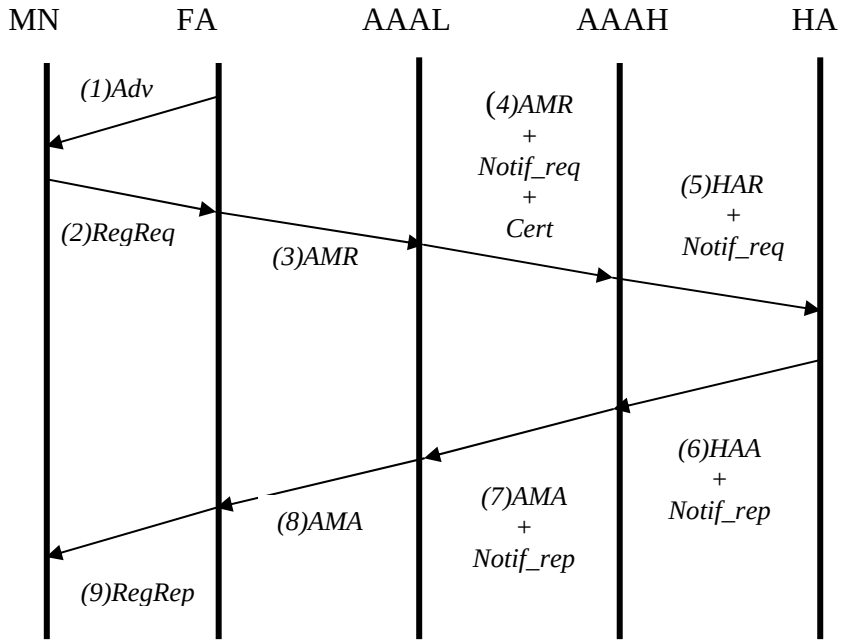

Figure4.7 : Flux de messages durant le First Inter domain handover (TypeI)

1) Tous les FA(s) envoient périodiquement des messages d'avertissements contenant le NAI Identifiant ces FA(s) et un challenge qui contient un nombre aléatoire (x_{FA}).

$$FA \rightarrow MN : \{Advertisement,\ldots, NAI_{FA}, x_{FA}\}$$

2) Le MN stocke le NAI reçu du FA, crée un message d'enregistrement Mobile IP qui contient le nombre aléatoire (x_{FA}), son (NAI_{MN}) et une signature qui doit être vérifiée par le AAAH, ce message est envoyé au FA.

$$MN \rightarrow FA : \{RegReq,\ldots, x_{FA}, NAI_{MN}, Sig_{MN, AAAH}\}$$

3) Le FA crée un message d'enregistrement *(AMR)(§3.5.2)* qui contient la demande d'enregistrement du MN et l'envoie à son AAAL.

$$FA \rightarrow AAAL : \{AMR,\ldots, \ldots RegReq,\ldots, x_{FA}, NAI_{MN}, Sig_{MN, AAAH}\}$$

4) Le AAAL envoie de sa part ce message au AAAH approprié (connu grâce au (NAI_{MN})). A ce stade, le AAAL demande une notification concernant les informations du HA et du MN, on lui associant son certificat ($Cert_{AAAL}$).

$$AAAL \rightarrow AAAH : \{AMR,\ldots, \ldots RegReq,\ldots, x_{FA}, NAI_{MN}, Sig_{MN, AAAH}\} \oplus Notif\_req \oplus Cert_{AAAL}$$

5) A la réception de ce message, Le AAAH vérifie la signature ($Sig_{AAAH, MN}$) du mobile. Si la signature est valide le AAAH déduira que c'est bien le MN qui a crée la demande d'enregistrement et vérifie aussi la validité du certificat du AAAL.
Le AAAH crée un message (*HAR)* qui contient le message d'enregistrement, crée une clé de session ($K_{MN, HA}$) à partager entre le MN et HA, et une autre clé ($K_{FA, HA}$) à partager entre le FA et le HA. Ces deux clés sont chiffrées avec une clé secrète ($K_{AAAH, HA}$) partagée entre le AAAH et le HA. De même le AAAH inclut deux clés de sessions pour le MN ($K_{MN, FA}$) et ($K_{MN, HA}$). Ces deux clés sont chiffrées avec la clé secrète ($K_{MN, AAAH}$). Enfin, le AAAH demande au HA de lui envoyer les informations d'identité du MN (*Notif_req).*

$$AAAH \rightarrow HA : \{HAR,\ldots, RegReq,\ldots NAI_{MN}, \{K_{MN, HA}, K_{FA, HA}\} K_{AAAH,HA}, \{K_{MN,FA}, K_{MN, HA}\} K_{MN, AAAH}, Sig_{AAAH, HA}\} \oplus (Notif\_req)\ Sig_{AAAH, HA}$$

6) A la réception de ce message, le HA vérifie la validité de la signature ($Sig_{AAAH, HA}$), enregistre le nœud mobile avec l'adresse temporaire contenue dans le message d'enregistrement, il décrypte et stocke les deux clés de session ($K_{MN, HA}$) et ($K_{FA, HA}$), crée par la suite une réponse d'enregistrement (*RegRep*) qui contient aussi les clés de session envoyées par le AAAH, puis il signe le tout avec ($Sig_{HA,MN}$).
Le message (*RegRep*) est inséré dans une réponse (*HAA)*, et envoyé au AAAH, confirmant ainsi le succès de l'enregistrement du MN. De plus, le HA répond par un *(Notif_rep)* qui contient les informations d'identité du nœud mobile.

$$HA \rightarrow AAAH : \{HAA,\ldots, (RegRep,\ldots, \{K_{MN, FA}, K_{MN, HA}\} K_{MN, AAAH}, Sig_{HA, AAAH}\} \oplus (Notif\_rep)\ Sig_{HA,AAAH}$$

7) Le AAAH vérifie les signatures ($Sig_{HA,AAAH}$), si le MN s'est enregistré chez le HA avec succès, le AAAH crée sa réponse d'enregistrement (*AMA*) *(§3.5.2)* et crée les clés de session du FA et du MN.
Dans notre schéma, le AAAH associe à ce message la réponse de notification cryptée par la clé publique du AAAL *(Notif_rep)*$k_{pubAAAL}$

$$AAAH \rightarrow AAAL : \{AMA,\ldots, x_{FA}, \{K_{MN, FA}, K_{FA,HA}\} K_{AAAH, AAAL}, (RegRep,\ldots, \{K_{MN, FA}, K_{MN, HA}\} K_{MN, AAAH}, Sig_{MN,AAAH}\}\ k_{pubAAAL} \oplus (Notif\_rep) k_{pubAAAL}$$

8) Le AAAL extrait les clés propre au FA ($K_{MN, FA}$, $K_{FA, HA}$), les rechiffre à l'aide de la clé ($K_{FA, AAAL}$) puis envoie ce message au FA et garde la réponse de notification à son niveau *(Notif_rep)*.

$$AAAL \rightarrow FA :\{AMA,\ldots, x_{FA}, \{K_{MN, FA}, K_{FA, HA}\}K_{FA,AAAL}, (RegRep,\ldots, \{K_{MN, FA}, K_{MN, HA}\}K_{MN, AAAH}, Sig_{MN, AAAH}) Sig_{AAAL, FA}\}$$

9) A la réception de ce message, le FA vérifie la signature du message et traite le message *(AMA)*: si le *(AMA)* signale le succès de l'enregistrement du MN, le FA déduit alors que le MN a signé correctement le nombre aléatoire envoyé à l 'étape 2, il décrypte et stocke par la suite les deux clés ($K_{MN, FA}$) et ($K_{FA, HA}$) et envoie (*RegRep*) au MN.

$$FA \rightarrow MN :\{RegRep,\ldots,\{K_{MN, FA}, K_{MN, HA}\}K_{MN, AAAH}, Sig_{MN, AAAH}\}$$

10) Le MN décrypte et stockent les deux clés de session ($K_{MN, FA}$, $K_{MN,HA}$) envoyées par le AAAH puis il utilise la clé ($K_{MN, HA}$) pour vérifier la signature ($Sig_{HA, MN}$) créee dans la sixième étape .
Si toutes les vérifications se terminent avec succès, cela veut dire que le FA a bien authentifié et accepté l'enregistrement du nœud mobile MN.

Ainsi, le AAAL est devenu le nouveau centre de gestion des clés, il crée et gère les nouvelles clés de session pour les trois entités.

4.4.2 Le handover de Type II (Intra domain handover)

Se déroule lorsque le nœud mobile se déplace à une nouvelle cellule dans le même domaine étranger. (Figure4.8)

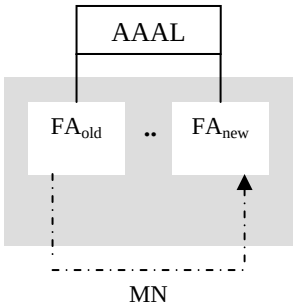

Figure4.8 : Intra domain handover (Type 2)

Dans ce cas, les étapes d'authentification sont comme suit: (Figure4.9)

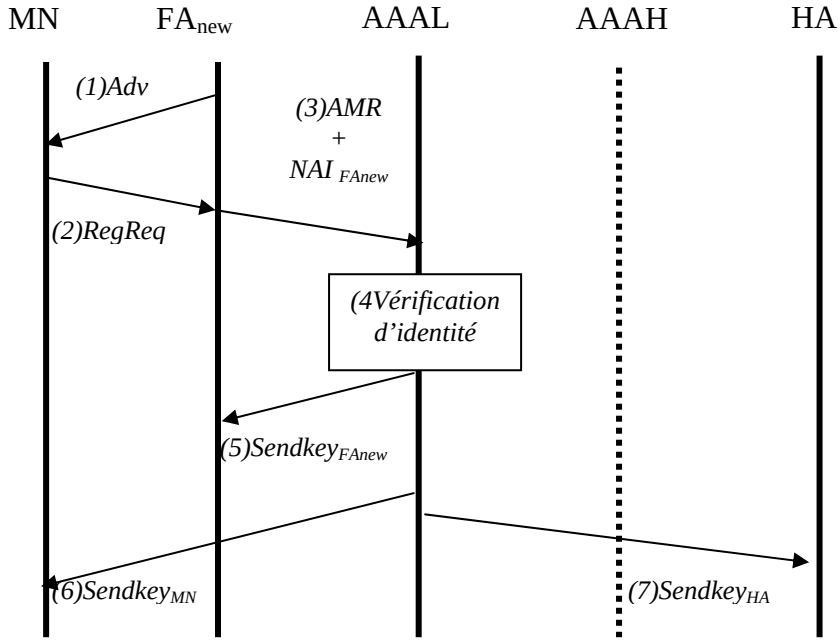

Figure 4.9 : Flux de messages durant l'Intra domain handover (TypeII)

1) Le FA envoie périodiquement des messages d'avertissement qui contiennent le NAI du nouveau FA, (NAI_{FAnew}).

$$FAnew \rightarrow MN : \{ advertissement, NAI_{FAnew} \}$$

2) Le MN crée une demande d'enregistrement ordinaire (*RegReq)* cryptée par la clé publique du AAAL ($k_{pubAAAL}$).

$$MN \rightarrow FA_{new}: \{ Regreq, NAI_{MN}, NAI_{FAnew}, addr_{HA,\ldots} \} k_{pub\_AAAL}$$

3) Le nouveau FA envoie à son AAAL le message (2) en lui associant l'identificateur (NAI_{FAnew}) et tout le message crypté avec (k_{pub_AAAL}).

$$FA_{new} \rightarrow AAAL:[\{Regreq, NAI_{MN}, NAI_{FA}, addr_{HA},\ldots\},\{NAI_{FAnew}\}]k_{pub\_AAAL}$$

4) Le AAAL vérifie l'identité du MN et du HA en comparant le message (3) avec la réponse de notification (*Notif_rep)* envoyé dans le message (7) durant le premier intra-domain handover et vérifie l'identité du (FA_{new}), si la vérification s'est terminée avec succès, le AAAL générera les trois nouvelles clés de session ($K'_{FAnew, HA}$) , ($K'_{MN, HA}$) et ($K'_{FAnew, MN}$).

5) Le AAAL distribue les deux clés ($K'_{FAnew, MN}$) *et* ($K'_{FAnew, HA}$) au (FA_{new}), il envoie aussi son certificat signé avec la clé privée du AAAH ($k_{privAAAH}$) prouvant ainsi qu'il un est un serveur digne de confiance

$$AAAL \rightarrow FA_{new} : \{Send\_key(K'_{FAnew, MN}, K'_{FAnew, HA}) \} + [Cert_{AAAL}] k_{\mathbf{privAAAH}}$$

6) Le AAAL distribue les deux clés ($K'_{FAnew, MN}$) et ($K'_{MN, HA}$) *au MN*, il envoie aussi son certificat signé avec la clé privée du AAAH ($k_{privAAAH}$)

$$AAAL \rightarrow MN : \{ Send\_key(K'_{FAnew, MN}, K'_{MN, HA})\} + [Cert_{AAAL.}]\ \mathbf{k_{privAAAH}}$$

7) Le AAAL distribue les deux clés ($K'_{FAnew, HA}$), ($K'_{MN, HA}$) *au HA*, il envoie aussi son certificat signé avec la clé privée du AAAH ($k_{privAAAH}$)

$$AAAL \rightarrow HA : \{ Send\_key(K'_{Fanew, HA}, K'_{MN, HA})\} + [Cert_{AAAL.}]\ \mathbf{k_{privAAAH.}}$$

Enfin ,Chaque entité vérifie la validité du certificat du AAAL, puis extrait ses clés pour communiquer en toute sécurité.

4.4.3 Le handover de Type III (Inter foreign domain handover)

Se déroule lorsque le nœud mobile migre vers une nouvelle cellule d'un autre domaine étranger.(Figure4.10)

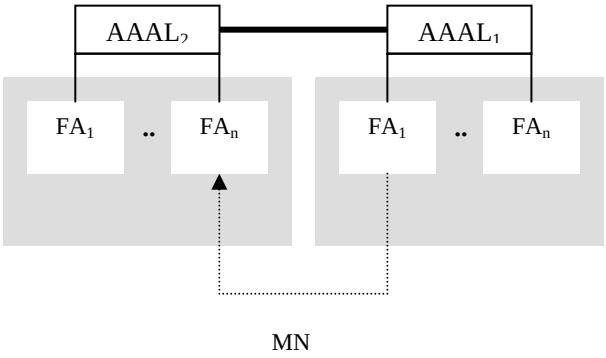

Figure4.10 : inter foreign domain handover (TypeIII)

Les trois premiers messages [1,2,3] sont les mêmes que dans le type précédant (Type II). En effet, le FA transmis des avertissements au nœud mobile qui lui envoie à son tour la demande d'enregistrement. Le FA transmis cette demande au $AAAL_1$ (le serveur local approprié) (Figure4.11)

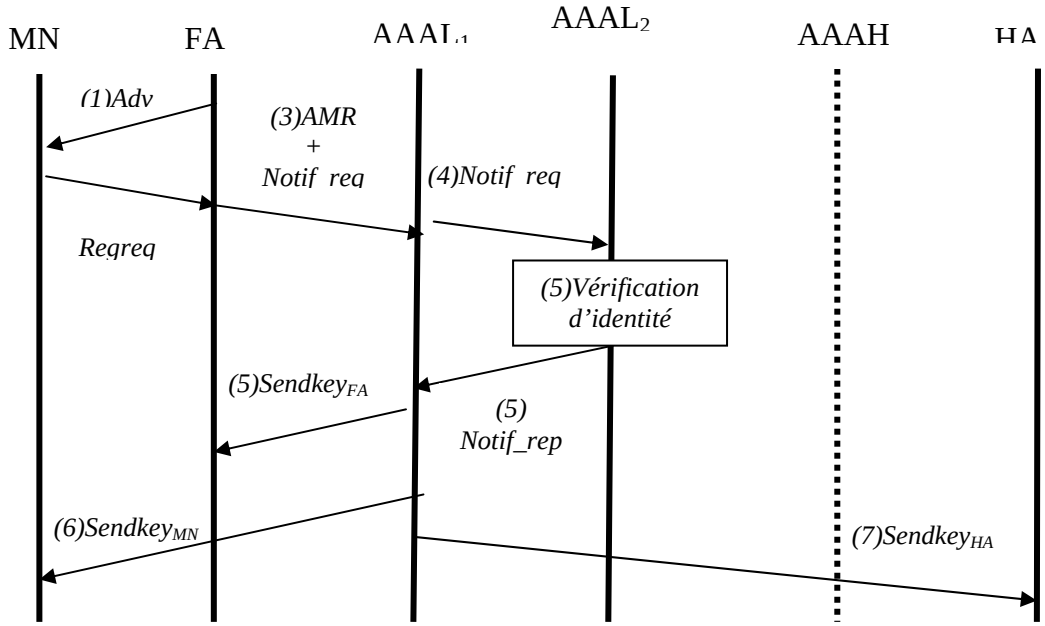

Figure4.11 : Flux de messages durant Inter foreign domain handover (TypeIII)

4) Le $AAAL_1$ contacte l'ancien serveur local $AAAL_2$ (qui possède une réponse de notification) et il lui envoie le message *(AMR)* qui contient la demande d'enregistrement reçue par le FA cryptée avec la clé publique du $AAAL_1$ ($k_{pubAAAL2}$) et son certificat ($Cert_{AAAL1}$)

$$AAAL_1 \rightarrow AAAL_2 : \{AMR,\ldots, \ldots RegReq,\ldots, x_{FA}, NAI_{MN} \oplus Notif\_req\}\ k_{pubAAAL2} \oplus Cert_{AAAI.1}$$

5) A la réception, le $AAAL_2$ décrypte le message à l'aide de sa clé privées, vérifie la signature du $AAAL_1$, puis envoie la réponse à la demande de notification (*Notif_rep)* ainsi que le certificat ($Cert_{AAAL2}$)

$$AAAL_2 \rightarrow AAAL_1 : \{Notif\_rep\}\ k_{pubAAAL1} \oplus Cert_{AAAL2}$$

Le $AAAL_1$ effectuera par la suite les échanges déjà expliqués lors d'un intra domain handover (TypeII); les étapes [5,6,7].

4.5 Avantages et inconvénients de la solution

Notre schéma présente des avantages et des inconvénients que nous citons:

4.5.1 Avantages

- **Décentralisation de la gestion des clés** : la gestion des clés (génération, distribution, chiffrement, déchiffrement) est partagée entre plusieurs entités (solution distribuée).
- **Tolérance au panne** : grâce à la décentralisation du processus de gestion des clés, le système continue à authentifier les acteurs même dans le cas où le home server tombe en panne.
- **Scalabilité :** notre système reste opérationnel même en l'augmentation exponentielle du nombre de nœud mobile en vu d'authentification.
- **Fusion de plusieurs étapes** : et cela dans le but de diminuer la latence du handoff lors de l'authentification, par exemple l'étape de la certification des serveurs et celle de la génération et distribution des clés sont traitées au même temps.
- **Choix adéquat des cryptosystèmes cryptographiques:** utilisation des cryptosystèmes à clé secrète rapide et moins coûteux en temps de calcul pour les acteurs Mobile IP (HA, FA, MN) et utilisation des algorithmes à clé publique plus sécurisés mais qui nécessitent plus de temps de calcul et de capacité mémoire pour les serveurs du système.

4.5.2 Inconvénients

- Chaque nœud mobile doit connaître au préalable la clé publique du serveur local qui correspond au nouveau FA (handoff du Type II) pour pouvoir envoyer sa demande d'enregistrement.

- Utilisation des associations de sécurité statiques lors du handoff de Type 1 entre le serveur AAA et les acteurs Mobile IP.

4.6 L'algorithme

Dans cet algorithme nous définissons les variables suivantes :

HO: type de handover (type1,2 ou 3).
First_HO: booléen (initialisé à FALSE).
RegReq: demande d'enregistrement délivrée par le nœud mobile.
RegRep: réponse d'enregistrement reçue par le nœud mobile.
Notif_req: demande de notification.
Notif_rep: réponse de notification.
@X: Adresse IP mère.
$k_{x,y}$: Clé secrète partagée entre les deux entités X et Y.
k_{pubX} :Clé publique de l'entité X.
$k_{priv\ X}$: Clé privée de l'entité X.
$Cert_x$:Certificat numérique de X.
[Px] :Paquet signé.

Le Programme principal

```
BEGIN
{
If (HO==1) then
{
   If (First_HO==TRUE)
            then handover_type1()
            else handover_type2()
}
else
   If (HO==2) then handover_type3()
}
END
```

Procedures

handover_type1()
Begin
{
Send (FA, MN, *Advertisements*)
When MN receive *advertisements*
Sig (MN, *RegReq*, $k_{MN,AAAH}$)
Send (MN,FA, *[RegReq*])
End

When FA receive [RegReq]
Create (FA, *AMR*)
P1= AMR⊕ [RegReq]
Send (FA, AAAL, *P1*)
End

When AAAL receive (*P1*)
Create *(Notif_req)*
L_AMR=P1⊕ Notif_req⊕ $Cert_{AAAL}$
Send (AAAL, AAAH, *L_AMR*)
End

When AAAH receive (*L_AMR*)
Verif_Sig (AAAH,MN, *[RegReq*], $K_{MN,AAAH}$)
If (Verif_Sig==Successful)
Then
{
Create (AAAH, *HAR*)
Create_key ($K_{MN,HA,}$ $K_{FA,HA}$)
KE1=Encrypt (AAAH, ($K_{MN,HA,}$ $K_{FA,HA}$), $K_{AAAH,HA}$)
Create_key *(*$K_{MN,FA,}$ $K_{MN,HA,}$*)*
KE2=Encrypt (AAAH, *(*$K_{MN,FA,}$ $K_{MN,HA,}$*)*, $K_{AAAH,MN}$)
L_HAR= HAR⊕[RegReq]⊕ Notif_req⊕ KE1⊕ KE2
Sig (AAAH, L_HAR, $K_{AAAH, HA}$)
Send (AAAH, HA, [L_HAR])
}
Else break
}
Else break
End if
End
When HA receive ([L_HAR])
Verif_Sig (HA, [L_HAR], $K_{AAAH,HA}$)
If (Verif_Sig==Successful)
then
{// Faire la correspondance entre l'adresse //principale et temporaire
Correspond (@MN, CoA)
Decrypt (HA, KE1, $K_{AAAH,HA}$)
Store ($K_{MN,HA,}$ $K_{FA,HA}$)
Create (HA, HAA)
Create (Notif_rep)
Sig (HA, Notif_rep, $K_{AAAH,HA}$)
P4= HAA⊕ [RegRep] ⊕ [Notif_rep]⊕ KE2
Sig (HA, P4, $K_{AAAH,HA}$)
Send (HA,AAAH,[P4])
}
end if
End

When AAAH receive ([P4])
Verif_Sig (AAAH, [P4], $K_{AAAH,HA}$)
If (Verif_Sig==Successful)
then
{
Create_key ($K_{MN,FA}$, $K_{FA,HA}$)
KE3=Encrypt (AAAH, ($K_{MN,FA}$, $K_{FA,HA}$), $k_{pubAAAL}$)
E1=Encrypt (AAAH, *Notif_rep* $k_{pubAAAL}$)
E2=Encrypt (AAAH, *RegRep*, $k_{pubAAAL}$)
Create (AAAH, *AMA*)
P5= AMA⊕ E1⊕ E2⊕ KE3
Send (AAAH, AAAL, *P5*)
}
end if
End

When AAAL receive *(P5)*
Decrypt (AAAL, *KE3*, $k_{privAAAL}$)
// extraire les clés du FA
KE4=Encrypt (AAAL, ($K_{MN,FA}$, $K_{FA,HA}$), $K_{AAAL,FA}$)
// clés du FA cryptés
Decrypt (AAAL, *E2*, $k_{privAAAL}$)
// décrypte la demande d'enregistrement
Sig (AAAL,*RegRep*, $K_{AAAL,FA}$)
// signe la demande d'enregistrement
Store (*Notif_rep*)
P6=AMA⊕KE4 ⊕ [RegRep]
Send (AAAL, FA, *P6*)
End
When FA receive (*P6*)
Verif_Sig (FA, [*P6*], $K_{AAAL,FA}$)
If (Verif_Sig==Successful)
then
{
Decrypt (FA, *KE4*, $K_{AAAL,FA}$)
Verif_Sig (FA, [*RegReq*], $K_{AAAL,FA}$)
If (Verif_Sig==Successful)
then
{
P7=RegRep⊕KE2
Send (FA, MN, *P7*) //RegRep et les clés du MN
}
end if
}end if
End
When MN receive (P7)
Decrypt (FA, KE2, K AAAH,MN)
Successful registration
End
}
END //fin type1

handover_type2()
Begin
{
Send (FA, MN, Advertisements)
When MN receive advertisements
E6=Encrypt (MN, RegReq, kpub_AAAL)
Send (MN,FA, E6)
End
When FA receive (E6)
E7=E6⊕NAIFAnew
Send (FA, AAAL, E7)

}

End

When AAAL receive *E7*
If (E7== *Notif_rep*) // Comparaison d'identité du HA et du MN
Then
{
Create_key ($K'_{FAnew, HA}$, $K'_{MN, HA}$, $K'_{FAnew, MN}$)
Send (AAAL, FA, ($K'_{FAnew, HA}$⊕ $K'_{FAnew, MN}$⊕ $Cert_{AAAL}$))
Send (AAAL, MN, ($K'_{FAnew, MN}$⊕ $K'_{MN, HA}$⊕ $Cert_{AAAL}$))
Send (AAAL, HA, ($K'_{FAnew, HA}$⊕ $K'_{MN, HA}$⊕ $Cert_{AAAL}$))
}
else break
End

When FA receive *($K'_{FAnew, HA}$⊕ $K'_{FAnew, MN}$⊕ $Cert_{AAAL}$)*
Verify_cert ($Cert_{AAAL}$)
Store ($K'_{FAnew, HA}$, $K'_{FAnew, MN}$)
End

When MN receive *($K'_{FAnew, MN}$⊕ $K'_{MN, HA}$⊕ $Cert_{AAAL}$)*
Verify_cert ($Cert_{AAAL}$)
Store ($K'_{FAnew, MN}$, $K'_{MN, HA}$)
End

When HA receive *($K'_{FAnew, HA}$⊕ $K'_{MN, HA}$⊕ $Cert_{AAAL}$)*
Verify_cert ($Cert_{AAAL}$)
Store ($K'_{FAnew, HA}$, $K'_{MN, HA}$)
End
}
END //fin type2

handover_type3()
Begin
{
Send (FA, MN, *Advertisements*)
When MN receive *advertisements*
Sig (MN, *RegReq*, $k_{MN,AAAH}$)
Send (MN,FA, *[RegReq*])
End
When FA receive *[RegReq]*
Create (FA, *AMR*)
P8= AMR⊕ [RegReq]
Send (FA, $AAAL_1$, (*P8*))
End

When $AAAL_1$ receive *(P8)*
KE5 =Encrypt ($AAAL_1$, *P8⊕ Notif_req*, $k_{pubAAAL2}$)
P9=KE5⊕ $Cert_{AAAL1}$
Send ($AAAL_1$, $AAAL_2$, *P9*)
End
When AAAL2 receive (P9)
Verify_cert *($Cert_{AAAL1}$)*
Decrypt ($AAAL_2$, *KE5*, $k_{pubAAAL2}$)
Create (*Notif_rep)*
KE6=Encrypt ($AAAL_2$, *Notif_rep*, $k_{pubAAAL1}$)
P10= KE6⊕ $Cert_{AAAL2}$
Send ($AAAL_2$, $AAAL_1$, *P10*)
End
When $AAAL_1$ receive *(P10)*
// même flux que dans
le type 1
End
}
END // fin type 3

Autres Procédures

La signature numérique:
Sig (signataire :X, message à signer :msg, clé de signature :K)
{
// Appliquer une fonction de hachage SHA-1 au message à signer et obtention du condensât (hash)
hash =Sha-1(X, msg)
encrypt (X, hash, K)
}

La verification de la signature numérique:
Verif_Sig (verification Y , message signé:[msg] , clé de signature)
{
hash' =Sha-1(Y, msg)
Encrypt (Y, hash', K)
if (hash'== hash)
Then verification is successful
}

Envoi de messages
Send (emmeteur, recepteur, message)

Création de messages
Create (message)

Création de clés
Create_key (Keys)

4.7 Conclusion

Dans ce chapitre, nous avons proposé un nouveau schéma d'authentification pour Mobile IP. Ce schéma a été suggéré après l'étude des différentes propositions de sécurisation de la procédures d'authentification dans Mobile IP. Nous avons remarqué que les systèmes proposés[RFC2002][ZAO97] restent insuffisants en matière de sécurité en l'absence d'un outil efficace de gestion de clés. Pour cela, nous supposons dans notre schéma l'existence d'une entité (le home server) qui se charge de gérer les clés distribuées dans tout le système, et pour plus de performance nous avons supposé qu'une gestion local des clés est toujours possible. En effet, lorsque un nœud mobile voulait se re-authentifier (en cas d'expiration du lifetime ou en cas de changement de cellule) il peut se re-authentifier au niveau de son serveur local certifié sans passer par toute l'architecture AAA. De cette manière, on évite la grande surcharge sur le home server et on assure la continuité du service dans le cas où le home server tombe en panne.
Dans le chapitre suivant nous allons analyser puis comparer les performances des deux schéma d'authentification : Mobile IP/AAA et notre schéma Local Mobile IP/AAA.

Chapitre V *Démarche et résultats d'analyse..*

5.1 introduction

Nous avons vu dans le chapitre précédant que notre contribution a touché principalement deux points: Le premier est la génération de nouvelles clés lors d'un intra domain handover et le second est la génération et la distribution des clés à partir des serveurs locaux certifiés AAAL(s) à la place du home server AAAH. Dans ce qui va suivre, nous allons voir l'impact de l'ajout de ces contraintes sur la sécurité et la performance du processus d'authentification.
Pour cela, nous estimerons puis nous comparerons le temps complet d'authentification dans les deux schémas : Mobile IP/AAA et notre schéma Local Mobile IP/AAA en ces trois types.

5.2 Délai d'authentification dans le schéma Mobile IP/AAA

On considère que le temps complet d'authentification (T_{full_auth}) est la somme de deux temps: le temps de transfert du flux de messages ($T_{transfert}$) (différence entre le temps de recevoir la réponse d'enregistrement par le MN et celui de l'envoie de la demande d'enregistrement) [SCH01] et le temps nécessaire pour effectuer les opérations cryptographiques (chiffrement, déchiffrement et signature) pour chaque entité (T_{crypto}).

$$T_{full\_auth} = \Sigma T_{transfert} + \Sigma T_{crypto} \qquad (1)$$

Notons que nous considérons, dans tout le reste de ce chapitre, la même architecture ainsi que les mêmes algorithmes cryptographies décrit dans [SCH01].

5.2.1Temps de transfert

On considère une architecture composée d'un domaine mère qui contient le home serveur AAAH, le home agent HA et le nœud mobile MN, et d'un ensemble de domaines étrangers où Chaque domaine est composé d'un ou plusieurs AAAL et de multiples foreign agents FA (Figure5.1). Dans cet environnement, on considère les paramètres suivants [SCH01]:

- MN⇔FA via un lien sans fil de (2Mo/s).
- FA⇔AAAL via un lien local de (2Mo/s).
- AAAL⇔AAAL via un lien de (100Mo/s).
- AAAL⇔Broker via un lien de (100Mo/s).
- Broker ⇔AAAH via un lien de (100Mo/s).
- AAAL⇔AAAH via un lien de (100Mo/s).
- AAAH⇔HA via un lien local de (2Mo/s).

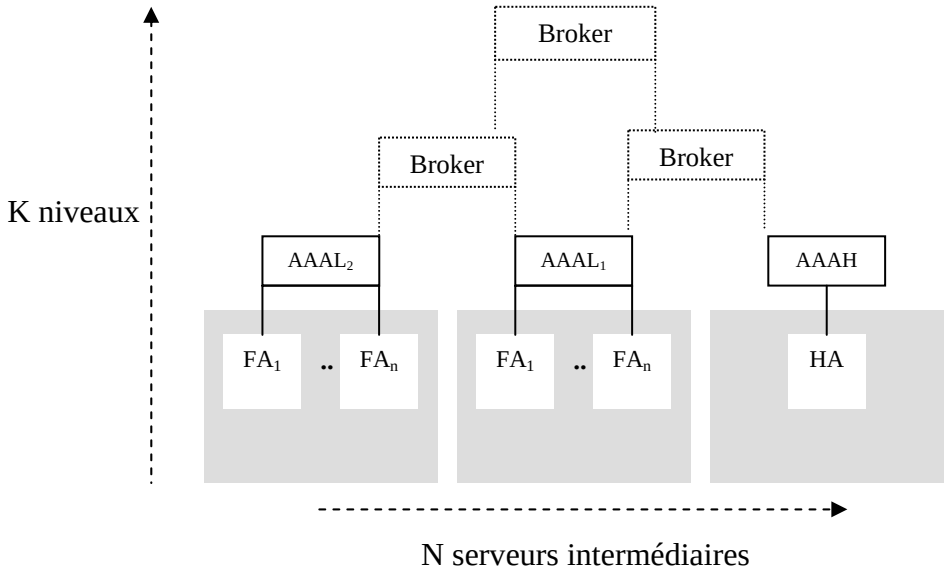

Figure5.1 Environnement d'analyse.

Le tableau 5.1 montre la longueur et le temps de transfert da chaque message du flux Mobile IP/AAA en supposant l'existence d'un lien filaire directe entre le home et le local server (sans brokers intermédiaires).

Lien	Messages	Longueur (octets)	Temps de transfert (µs) (sans brokers intermédiaires)
MN→FA	RegReq	90	42,91
FA→AAAL	AMR	436	207,88
AAAL→AAAH	AMR	436	4,142 (T_{AMR})
AAAH→ HA	HAR	532	253,65
HA→AAAH	HAA	492	234,58
AAAH→AAAL	AMA	476	4,522 (T_{AMA})
AAAL → FA	AMA	476	226,95
FA → MN	RegRep	130	61,98
			$\Sigma=T_0=1036.614\mu s$

Tableau 5.1: Le temps de transfert du flux Mobile IP/AAA sans brokers.

Généralisation

Pour n brokers intermédiaires, on remarque que le temps de transfert ($T_{transfert}$) est la somme de trois temps: T_1, T_2 et T_3.

T_1 est le temps de transfert du flux entre les n brokers (B_1,...,B_n).

T_2 est le temps de transfert du flux entre le AAAL et le premier broker B_1 et entre le dernier broker B_n et le AAAH.

T_3 est le temps de transfert du flux sans brokers intermédiaires moins le temps de transfert d'un AMR et un AMA échangés entre un AAAL et un AAAH.

$$T_{transfert}=T_1+T_2+T_3.$$

$$T_{transfert}= [(n-1)(T_{AMR}+ T_{AMA})]+[2(T_{AMR}+ T_{AMA})]+ [T_0-(T_{AMR}+ T_{AMA})]$$

$$T_{transfert}= T_0+n* (T_{AMR}+ T_{AMA}) \qquad (2)$$

Tel que:
n :est le nombre de brokers intermédiaires.
T_0 : est le temps de transfert du flux Mobile IP/AAA sans brokers intermédiaires.
T_{AMR} : est le temps de transfert d'un message AMR entre deux serveurs AAA, ou entre deux brokers, ou entre un serveur AAA et un broker.
T_{AMA}: est le temps de transfert d'un message AMA entre deux serveurs AAA, ou entre deux brokers, ou entre un serveur AAA et un broker.

Nombre de brokers	Temps de transfert (µs)
0	1036,614
1	1045,278
2	1053,942
3	1062,606
4	1071,27
5	1079,934
6	1088,598

Tableau 5.2 : Le temps de transfert en fonction du nombre de brokers.

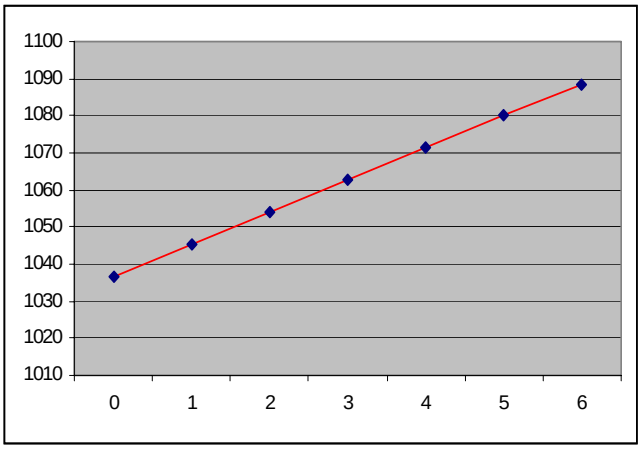

Figure5.2 : Le temps de transfert en fonction du nombre de brokers.

On remarque (tableau 5.2) que le temps de transfert du flux augmente proportionnellement par rapport au nombre de sauts effectués (nombre de brokers intermédiaires).

5.2.2 Temps des opérations cryptographiques

Le temps consacré au opérations cryptographiques (chiffrement, déchiffrement, signatures) dans le schéma d'authentification Mobile IP/AAA est la somme des temps nécessaires pour cette opération au niveau de chaque entité .

$$T_{op\_crypto}(MIP/AAA)= \Sigma T_{op\_crypto}(entité_i) \qquad (3)$$

Elle est égale (sans brokers intermédiaires) à T'_0 =1158µs (0.001158s) [SCH01].
Notons que nous utiliserons dans la suite de ce chapitre les mêmes algorithmes cryptographiques utilisés dans [SCH01] qui sont DES et MD5.

Généralisation :
Si on considère l'existence de n brokers intermédiaires, il faut ajouter pour chaque broker le temps de chiffrement de deux messages AMA ($2*T_{cryp\_AMA}$) et le temps de déchiffrement de deux messages AMR ($2*T_{cryp\_AMR}$).
pour n brokers cette durée est égale à (n*730)µs.

$$T_{op\_crypto}(MIP/AAA) = T'_0 + 2n(T_{cryp\_AMR} + T_{cryp\_AMA}) \quad (4)$$

Tel que
T'_0 : est le temps nécessaire pour effectuer toutes les opérations cryptographiques sans brokers intermédiaires (1158µs).
T_{cryp_AMR} :est le temps de déchiffrement d'un message AMR (190µs) [SCH01].
T_{cryp_AMA}: est le temps de chiffrement d'un message AMA (175µs) [SCH01].
Le tableau 5.3 montre le temps nécessaire pour effectuer des opérations cryptographiques dans ce schéma en fonction du nombre de brokers.

Nombre de brokers	Temps nécessaire pour les opérations cryptographiques[µs]
0	1158+0*730=1158
1	1158+1*730=1888
2	1158+2*730=2618
3	1158+3*730=3348
4	1158+4*730=4078
5	1158+5*730=4808
6	1158+6*730=5538

Tableau 5.3 : Durée des opérations cryptographiques en fonction du nombre de brockers dans le schéma MIP/AAA

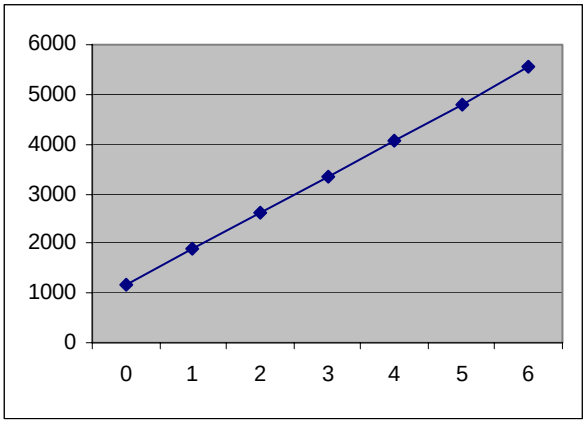

Figure5.3: Durée des opérations cryptographiques en fonction du nombre de brockers dans le schéma MIP/AAA

On remarque que le temps nécessaire pour effectuer des opérations cryptographiques pour Mobile IP/AAA est proportionnel au nombre de sauts effectués(Figure 5.3).

5.2.3 Délai complet d'authentification

La durée complète d'authentification Mobile IP/AAA est :

$$T_{full\_auth} = \Sigma T_{transfert} + \Sigma T_{crypto}$$

$$T_{full\_auth}(MIP/AAA) = [T_0 + n*(T_{AMR} + T_{AMA})] + [T'_0 + 2n*(T_{cryp\_AMR} + T_{cryp\_AMA})]$$

$$T_{full\ auth}(MIP/AAA) = T_0 + T'_0 + n*[T_{AMR} + T_{AMA} + 2(T_{cryp\ AMR} + T_{cryp\ AMA})] \quad (5)$$

On remarque que le délai complet d'authentification Mobile IP/AAA est proportionnel au nombre de sauts effectués. (Figure 5.4)

Nombre de brokers	Temps complet d'authentification[µs]
0	2194,614
1	2933,278
2	3671,942
3	4410,606
4	5149,27
5	5887,934
6	6626,598

Tableau 5.4 : Délai complet d'authentification (MIP/AAA).

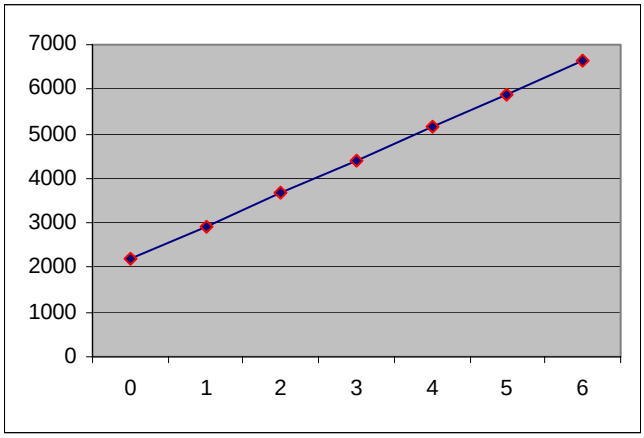

Figure5.4: Délai complet d'authentification (MIP/AAA).

5.3 Délai d'authentification dans le schéma Local Mobile IP/AAA

5.3.1Premier cas : handover de Type I

Rappelons que lors d'un handoff de Type I, le nœud mobile sors la première fois de son domaine mère vers un autre étranger.

5.3.1.1 Temps de transfert du flux

On considère les hypothèses suivantes sur la longueur des messages supplémentaires que nous utilisons dans notre schéma, la longueur des autres messages restera la même que dans Mobile IP/AAA.

- (Notif_req) sur 16bits (2octets).
- Le certificat (Cert) sur 1024 bits (128octets).
- (Notif_rep) sur 24bits (3 octets).

Le tableau 5.5 montre la durée de transfert du flux durant le handover de Type I.

Lien	Messages	Longueur (octets)	Temps de transfert (µs)
MN→FA	RegReq	90	42,91
FA→AAAL	AMR	436	207,88
AAAL→ AAAH	AMR+ Cert+ Notif_req	566	5,37
AAAH→ HA	HAR+Notif_req	534 (532+2)	254,61
HA → AAAH	HAA+ Notif_rep	495 (492+3)	236,01
AAAH → AAAL	AMA+Notif_rep	479 (476+3)	4,55
AAAL → FA	AMA	476	226,95
FA → MN	RegRep	130	61,98
			$T_0=\Sigma=1040,26\ \mu s$

Tableau5.5 : La durée de transfert du flux durant le handover de Type I.

Généralisation

Pour n brokers intermédiaires, on remarque que le temps de transfert ($T_{transfert}$) est de:

$$T_{transfert}= [(n-1)(T'_{AMR}+ T'_{AMA})]+[2(T'_{AMR}+ T'_{AMA})]+ [T_0 -(T'_{AMR}+ T'_{AMA})]$$

$$T_{transfert} = T_0 + n * (T'_{AMR} + T'_{AMA}) \quad (6)$$

Tel que:
n :est le nombre de brokers intermédiaires.
T_0 : est le temps de transfert du flux LMIP/AAA/TypeI sans brokers intermédiaires (1040,26µs).
T'_{AMR} : est le temps de transfert d'un message (AMR, Cert et notif_req)(5,37µs).
T'_{AMA}: est le temps de transfert d'un message (AMA, notif_rep)(4,55µs).

Nombre de brokers	Temps de transfert (µs)
0	1040,26
1	1050,18
2	1060,1
3	1070,02
4	1079,94
5	1089,86
6	1099,78

Tableau 5.6 : Le temps de transfert en fonction du nombre de brokers(typeI)

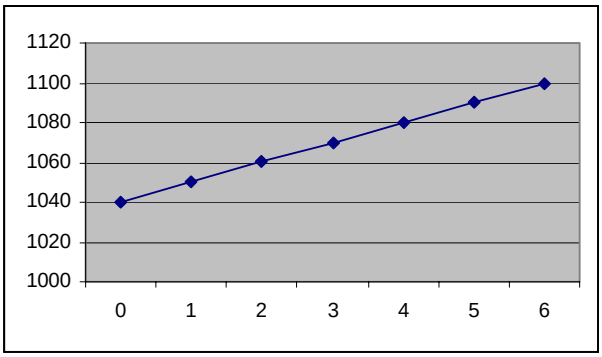

Figure5.5 : Le temps de transfert en fonction du nombre de brokers(TypeI)

On remarque que le temps de transfert du flux lors d'un handoff de type I est proportionnel au nombre de sauts effectués.

5.3.1.2 Temps des opérations cryptographiques

Le tableau 5.7 récapitule le temps nécessaire pour effectuer toutes les opérations cryptographiques durant un handoff du Type I.

Entité	Action	Durée (µs) DES/MD5
MN	RegReq(E+S) RegRep(D)	3 5
FA	AMR(E+S) RegRep(D)	88 100
AAAL	AMR+ Notif_req (E+S) AMA(D)	175,79 190
AAAH	HAR+Notif_req (E+S) AMA+Notif_rep (D)	195,73 196,22
HA	HAA+ Notif_rep (E+S)	208,26
		$\Sigma = T_0 = 1162\mu s$

Tableau5.7 : Durée des opérations cryptographiques durant un handoff de Type I.

Généralisation :
Si on considère l'existence de n brokers intermédiaires, il faut ajouter pour chaque broker le temps de chiffrement de deux messages (AMA, notif_rep) ($2*T'_{cryp\_AMA}$) et le temps de déchiffrement de deux messages (AMR, notif_req) ($2*T'_{cryp\_AMR}$).

$$T_{op\_crypto}(\ typeI\ ) = T'_0 + 2n(T'_{cryp\_AMR} + T'_{cryp\_AMA}) \quad (7)$$

Tel que:
T'_0 : est le temps nécessaire pour effectuer toutes les opérations cryptographiques sans brokers intermédiaires (1162µs).
T'_{cryp_AMR} :est le temps de déchiffrement d'un message (AMR, notif_req) (175.79µs)
T'_{cryp_AMA}: est le temps de chiffrement d'un message (AMA, notif_rep)(196.22µs)

Le tableau 5.8 montre le temps nécessaire pour effectuer des opérations cryptographique dans ce schéma en fonction du nombre de brokers.

Nombre de brokers	Temps nécessaire pour les opérations cryptographiques[µs]
0	1162
1	1906,02
2	2650,04
3	3394,06
4	4138,08
5	4882,1
6	5626,12

Tableau 5.8: Durée des opérations cryptographiques en fonction du nombre de brockers (typeI)

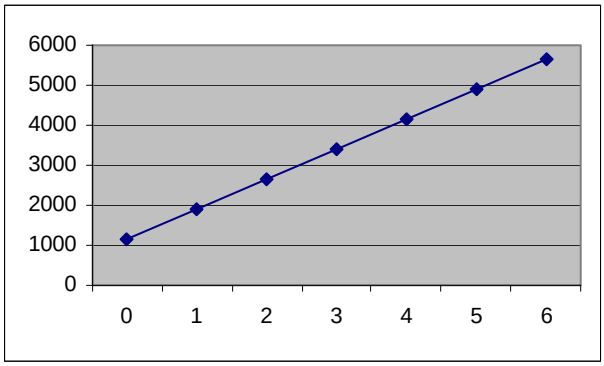

Figure5.6: Durée des opérations cryptographiques en fonction du nombre de brockers (typeI)

5.3.1.3Délai complet d'authentification

La durée complète d'authentification lors d'un handoff de TypeI est (Figure 5.7)

$$T_{full\_auth} = \Sigma T_{transfert} + \Sigma T_{crypto}$$

$$T_{full\_auth}(TypeI) = [T_0 + n*(T'_{AMR} + T'_{AMA})] + [T'_0 + 2n*(T'_{cryp\_AMR} + T'_{cryp\_AMA})]$$

$$T_{full\_auth}(type\ I) = T_0 + T'_0 + n*[T'_{AMR} + T'_{AMA} + 2(T'_{cryp\_AMR} + T'_{cryp\_AMA})] \quad (8)$$

Nombre de brokers	Temps complet d'authentification[µs]
0	2208,06
1	2956,2
2	3710,14
3	4464,08
4	5218,02
5	5971,96
6	6725,9

Tableau5.9 : Délai complet d'authentification (typeI).

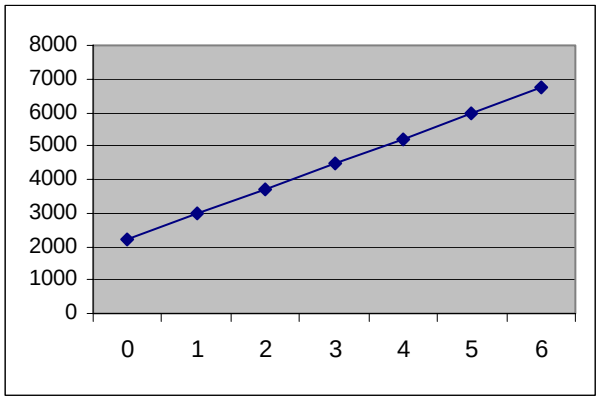

Figure5.7: Délai complet d'authentification (typeI).

On remarque que le délai complet d'authentification est proportionnel dans ce type de handoff au nombre de sauts effectués.

5.3.2 Deuxième cas : handover de Type III

Rappelons que le handover de Type III se déroule lorsque le nœud mobile migre vers une nouvelle cellule d'un autre domaine étranger.
Le tableau 5.10 montre le temps de transfert du flux durant le handoff de Type III.
Le AAAL cherchant à authentifier les acteurs demande dans notre schéma des informations d'identification auprès d'un serveur proche et ayant authentifié les acteurs lors d'une session précédente. Pour cela, il envoie son certificat et la demande de notification au serveur en question et reçoit la réponse suite à la vérification du certificat.

5.3.2.1 Temps de transfert du flux

Lien	Messages	Longueur (octets)	Temps de transfert (µs)
MN→FA	RegReq	90	42,91
FA→AAAL	AMR	436	207,88
$AAAL_1 \rightarrow AAAL_2$	AMR+ Cert+ Notif_req	436+128+2=566	5,37
$AAAL_2 \rightarrow AAAL_1$	Cert+ Notif_rep	128+3=131	1,24
$AAAL_1 \rightarrow FA$	AMA	476	226,95
$FA \rightarrow MN$	RegRep	130	61,98
			Σ=547,33µs

Tableau5.10 : Le temps de transfert du flux durant le handoff de Type III.

5.3.2.2 Temps des opérations cryptographiques

Le tableau 5.11 montre le temps des opérations cryptographiques durant un handoff du Type III.

Entité	Action (DES/MD5)	Durée (µs)
MN	RegReq(E+S) RegRep(D)	3 5
FA	AMR(E+S) RegRep(D)	88 100
$AAAL_1$	AMR+ Notif_req(E+S) Notif_rep (D)	175,79 1,19
$AAAL_2$	Notif_rep (E+S)	0,8
HA	Keys (D)	0,54
		Σ= *374,32µs*

Tableau5.11 : Durée des opérations cryptographiques durant un handoff de Type III.

5.3.2.3 Délai complet d'authentification

La durée complète d'authentification LMIP/AAA(Type III) est :

$$T_{full\_auth} = \Sigma T_{transfert} + \Sigma T_{crypto}$$

Elle est égale à 921.65µs (*547,33µs+374,32µs*), sans brokers intermédiaires.
Si au pire des cas, il n'ya pas de serveur proche et certifié et qui a déjà authentifier ces acteurs, on se ramène à une authentification due type MIP/AAA/TypeI où on demande l'authentification au serveur AAAH.

5.3.3Troisième cas : handover de Type II

Rappelons que dans cette étape nous avons proposé que le AAAL certifié, génère trois nouvelles clés à partager entre les acteurs Mobile IP (MN, HA, FA) et cela à chaque intra domain handover(§4.2.2).
Ce processus supplémentaire va sûrement augmenter le délai complet d'authentification lors de ce type de handoff puisqu'il augmente le temps des opérations cryptographiques. En effet, nous essayons de rendre la durée de cette phase supplémentaire la plus petite possible en choisissant un algorithme symétrique robuste et rapide pour la génération des clés. Pour cela, nous allons comparer quelques algorithmes symétriques selon plusieurs critères (longueur de clé, temps de génération de clés, rapidité) et choisir l'algorithme le plus adéquat pour notre schéma.

5.3.3.1 Estimation du temps de génération/chiffrement des nouvelles clés

Le but est d'estimer le temps de la génération de ces clés puis comparer les résultats obtenus pour chacun des algorithmes robustes et de différentes tailles [ICH02]: MARS, RC6, Rijndael, Serpent et Towfish.

Le tableau 5.12 présente chacun de ces algorithmes, sa longueur de clé ainsi que le temps nécessaire pour générer cette clé[ICH02].

Algorithme symétrique (X)	Longueur de clé (bits)	Temps de génération de clé $T_{Gen\_sym}(X)$ (µs)
DES	64	4,830
3-DES	128	14,490
MARS	128	1,741
RC6	256	2,1123
Rijndael	256	0,05734
Serpent	256	0,11407
Towfish	256	0,01638

Tableau5.12 : Temps de génération de clés symétriques.

Le temps nécessaire pour un serveur AAAL pour générer et chiffrer trois clés de session:

$$T_{Gen\_chiff}=(T_{Gen\_sym}(X)+T_{chiff})*3 \quad (9)$$

Tel que :

$T_{Gen\_sym}(X)$ le temps nécessaire pour générer une clé à l'aide de l'algorithme symétrique X.

T_{chiff} Le temps nécessaire pour un chiffrement DES/MD5 (chiffrement d'un octet en 0.36 µs) [SCH 01]

Le tableau 5.13 montre les différents résultats obtenus

Algorithme symétrique (X)	Longueur de clé (bits)	$T_{Gen\_sym}(X)$ (µs)	T_{chiff} (DES/MD5) (µs)	T_{Gen_chiff} (3clés)(µs)	Rapidité (Mo/s)
DES	64	4,830	2,94	23,31	21,34
3-DES	128	14,490	5,88	61,11	9,84
MARS	128	1,741	5,88	19,38	27,91
RC6	256	2,1123	11,76	37,39	37,814
Rijndael	256	0,05734	11,76	34,45	48,229
Serpent	256	0,11407	11,76	35,39	21,091
Towfish	256	0,01638	11,76	35,32	31,411

Tableau 5.13 :Rapidité des clés symétriques

Discussion :
Le temps de la génération de trois nouvelles clés lors du handover de Type II est une étape supplémentaire par rapport au schéma Mobile IP/AAA, c'est à dire qu'elle s'ajoute au temps complet d'authentification Mobile IP/AAA. D'où la nécessité de la rendre la plus petite possible. Pour cela, il faut choisir l'algorithme le plus rapide pour exécuter la génération de ces clés en moins de temps.
Le temps de génération et de chiffrement de clé augmente selon la longueur de cette clé, d'où l'obligation de choisir un algorithme dont la clé est de taille raisonnable bien que cela diminue le niveau de sécurité.

5.3.3.2 Temps de transfert de flux

De la même manière que dans les Types précédents:

Lien	Messages	Longueur (octets)	Temps de transfert (µs)
MN→FA	RegReq	90	42,91
FA→AAAL	AMR	436	207,88
AAAL→ FA	AMA+K_1	732	292,18
AAAL→ MN	K_2	256	102,18
AAAL→ HA	K_3	256	102,18
			$\sum=T_0=747,33$

Tableau 5.14: Le temps de transfert du flux durant le handoff de Type II.

La durée du transfert est fixe (indépendante du nombre de brokers puisque on effectue un intra domain handoff)

5.3.3.3 Temps des opérations cryptographiques

Le tableau 5.15 est un tableau comparatif entre le temps nécessaire pour effectuer les différentes opérations cryptographiques (chiffrement, déchiffrement, signature) dans le schéma d'authentification Mobile IP /AAA [SCH01] et, par conséquent, celui de notre schéma (Local Mobile IP /AAA):
On considère les notations suivantes :
-E: chiffrement (Encryption).
-D: déchiffrement (Decryption).
-S: signature (Signing).
- Keys(G+E): Génération et Chiffrement de clés (§5.3.3.1)

Entité	Action (DES/MD5)	MIP/AAA (Type II)	LMIP/AAA (Type II)
MN	RegReq(E+S) RegRep(D)	3µs 3µs	3µs 3µs
FA	AMR(E+S) RegRep(D+S)	48µs 69µs	48µs 69µs
AAAL	AMR(D+E+S)	-	-
	AMA(E+S)	112µs	112µs
	Keys(G+E)	-	**X**
		Σ=235µs	Σ=(235 +X) µs

Tableau 5.15 : Temps nécessaire pour effectuer les différentes opérations cryptographiques dans les deux schémas.

Dans notre schéma d'authentification en local, nous utilisons les mêmes opérations cryptographiques que celles employés dans le schéma Mobile IP/AAA plus l'opération supplémentaire qui est celle de la génération et le chiffrement de trois nouvelles clés.

$$T_{full\_auth(LMIP/AAA)} = T_{full\_auth(MIP/AAA)} + T_{Gen\_chiff\ (X)} \qquad (10)$$

$T_{full\_auth(LMIP/AAA)}$: Durée complète d'authentification dans notre schéma.
$T_{full\_auth(MIP/AAA)}$: Durée complète d'authentification dans le schéma MIP/AAA (235µs).
$T_{Gen\_chiff\ (X)}$: Temps nécessaire pour générer puis chiffrer trois clés de Type X

Le tableau 5.16 montre le temps complet des opérations cryptographiques lors d'un handover de Type II, selon le type de l'algorithme symétrique choisi pour effectuer la génération des clés.

Algorithme symétrique (X)	Temps des opérations cryptographique (type II)(µs)
DES	235,25
3-DES	296,11
MARS	254,38
RC6	272,39
Rijndeal	269,45
Serpent	270,39
Towfish	270,32

Tableau 5.16:Temps des opérations cryptographiques (type II) en fonction des algorithmes symétriques.

Discussion:
On remarque que l'algorithme DES effectuera cette tache en moins de temps par rapport aux autres algorithmes, mais avec 64 bits, il est beaucoup moins sécurisé par rapport au autres algorithmes.
L'Algorithme MARS est plus adéquat donc, puisque il effectuera la génération en un temps raisonnable, et permet un chiffrement symétrique rapide (nécessaire pour la communication HA, FA, MN).

5.3.3.4 Délai complet d'authentification

La durée complète d'authentification LMIP/AAA(Type II) est :

$$T_{full\_auth} = \Sigma T_{transfert} + \Sigma T_{crypto}$$

La durée complète d'authentification LMIP/AAA (Type II) est une durée fixe (747.33µs) indépendante du nombre de brokers.
Notons que lors de l'expiration du délai d'enregistrement dans le modèle Mobile IP/AAA (TypeII), le nœud mobile recontactera le AAAH pour effectuer une authentification complète en passant par les brokers intermédiaires, alors que dans notre schéma l'authentification continue à s'effectuer localement.

5.4 Tableau récapitulatif

Le tableau suivant récapitule les résultats précédents:

Schéma	Nombre de brokers	Type de handoff	Temps de transfert (µs)	Temps des opérations cryptographiques (µs)	Délai d'authentification complète (ms)
MIP/AAA	0	**I**	1036,614	1158	*2,194*
	6	**I**	1088,598	5538	*6,626*
	0	**III**	1036,614	1158	*2,194*
	0	**II**	747,33	235	*0,982*
	6	**II**	1036,614	1158	*2,194*
LMIP/AAA	0	**I**	1040,26	1162,38	*2,208*
	6	**I**	1099,78	5626,12	*6,725*
	0	**III**	547,33	374,32	*0,921*
	0	**II**	747,33	254,38	*1,001*
	6	**II**	747,33	254,38	*1,001*

Discussion:
Le tableau récapitulatif synthétise les temps nécessaires pour l'authentification dans les deux schémas: Mobile IP/AAA (Type I et III) et Local Mobile IP/AAA (Type I, II, III).
Pour Un handoff de Type I:
Nous remarquons que le temps complet d'authentification dans MIP/AAA/TypeI augmente proportionnellement par rapport au nombre de brokers intermédiaires entre le AAAL et le AAAH, cela est dû à l'ajout du temps de transmission supplémentaire entre les serveurs et les brokers et entre les brokers eux mêmes, ainsi qu'à l'ajout du temps de calcul cryptographique de ces entités.
De même, pour le temps d'authentification LMobileIP/AAA/TypeI qui augmente aussi proportionnellement par rapport au nombre de brokers intermédiaires, mais qui est légèrement lent par rapport au Mobile IP/AAA/Type I (6.725ms pour LMIP/AAA/TypeI et 6.625ms pour MIP/AAA/Type1). Cela est dû à l'ajout de quelques messages (demande et réponse de notification) qui nécessitent un temps supplémentaire de chiffrement, déchiffrement et de transfert. Cette différence ne pose pas de problème puisque le handoff de Type I dans notre schéma ne s'effectue qu'une fois (lors du *premier* handoff du mobile de son domaine mère vers un autre étranger).

Pour Un handoff de Type III:
Pour diminuer le délai d'authentification lors d'un inter- domain handoff (Type III), Nous avons proposé de demander les informations d'authentification auprès du serveur AAAL le plus proche et ayant déjà authentifié le MN et le HA associé 0.921ms.

En l'absence de cette amélioration dans le schéma Mobile IP/AAA/TypeIII, une authentification AAA complète (de Type I) s'effectue : 2.914ms au meilleurs des cas (c'est à dire sans brokers intermédiaires). Nous enregistrons donc un gain de 1.99ms.

Pour Un handoff de Type II:

Le temps d'une authentification lors d'un handoff de Type II est de 0.98ms pour le schéma Mobile IP/AAA et 1.00ms pour notre schéma. Cela est du à l'étape que nous avons rajouté dans notre schéma qui est celle de la génération et le chiffrement de trois nouvelles clés.

Le temps de transfert est le même dans les deux schémas (pas de sauts supplémentaires entre brokers, puisque le nœud mobile effectue un intra domain handoff). Le temps des opérations cryptographiques est plus important dans LMIP/AAA (0.254.38ms et 0.235ms pour MIP/AAA). Cela est dû à la phase supplémentaire que nous avons rajouté dans notre schéma (la génération de trois nouvelles clés).

Néanmoins, dans le cas d'expiration du délai d'enregistrement dans le modèle Mobile IP/AAA, le nœud mobile doit recontacter le AAAH pour effectuer une authentification complète en passant par les brokers intermédiaires (6.626ms pour 6 brokers intermédiaires), alors que dans notre schéma l'authentification continue à s'effectuer localement 1ms. nous enregistrons alors un gain de 5.626ms (cas de 6 brokers intermédiaires)

5.5 Conclusion

Dans ce chapitre, nous avons analysé l'impact de l'ajout de nos contraintes à l'ancien modèle d'authentification Mobile IP/AAA sur le délai complet d'authentification.

A partir des résultats de cette analyse, nous pouvons conclure que :

- Le temps d'authentification dans le schéma MIP/AAA/TypeI et MIP/AAA/TypeIII augmente proportionnellement par rapport au nombre de sauts effectués (nombre de brokers intermédiaires).
- De même, le temps d'authentification dans le schéma LMIP/AAA/TypeI augmente proportionnellement par rapport au nombre de sauts effectués.
- Le temps de la génération de trois nouvelles clés lors du handover de Type II est une étape supplémentaire par rapport au schéma Mobile IP/AAA, c'est à dire qu'elle s'ajoute au temps complet d'authentification Mobile IP/AAA. D'où la nécessité de la rendre la plus petite possible. Pour cela, il faut choisir l'algorithme le plus rapide pour exécuter la génération de ces clés en moins de temps et qui permet au même temps un chiffrement symétrique rapide (nécessaire pour la communication HA, FA, MN).
- Le temps de génération et de chiffrement de clé augmente selon la longueur de cette clé, d'où l'obligation de choisir un algorithme dont la clé est de taille raisonnable bien que cela diminue le niveau de sécurité.
- Notre schéma réduit aussi le délai d'authentification durant un inter domain handoff (Type III), grâce à l'authentification des acteurs auprés d'un serveur local proche et certifié.

- Notre schéma réduit considérablement le délai d'authentification Type I grâce à la gestion locale proposée où nous évitons de passer par plusieurs brokers intermédiaires pour atteindre le AAAH.

Conclusion générale

Le fait que Mobile IP permet de se déplacer d'un réseau à un autre tout en se reposant sur un protocole ouvert et universel : Le protocole IP, rend Mobile IP vulnérable à de nombreuses tentatives de fraudes. Il faut dans certains cas pouvoir authentifier l'utilisateur avant de lui permettre l'accès au réseau.
Nous avons vu que beaucoup de travaux ont été proposés pour améliorer la sécurité de la procédure d'authentification du protocole Mobile IP [RFC2002][ZAO 97][RFC2977], mais qui restent insuffisants en matière de sécurité et de performance. L'authentification standard [RFC2002] considère la pré-existence des liens de confiance entre les acteurs Mobile IP. Cette solution s'est avérée insuffisante à cause de la non scalabilité et l'absence d'une entité digne de confiance qui se préoccupe de la gestion des clés entre ces acteurs. Zao [ZAO97] a proposé l'utilisation des cryptosystèmes à clé publique pour résoudre le problème de la scalabilité de l'authentification standard: chaque entité possède une paire de clé publique et privée utilisée pour chiffrer et signer. C'est une solution qui garantit essentiellement la non-répudiation, mais qui reste théorique en particulier pour les nœuds mobiles puisque les algorithmes à clé publique nécessitent une grande capacité de calcul.

Le schéma d'authentification Mobile IP/AAA est venu remédier à l'absence de l'outil de gestion des clés dans l'authentification standard, le home server (AAAH) est devenu l'entité responsable de la gestion sécurisée des clés. Cette entité se charge de générer et de distribuer les clés de communication grâce aux associations de sécurité statiques existantes entre le AAAH et les acteurs Mobile IP. Néanmoins, ce mode d'authentification comporte essentiellement deux points faibles: Le premier est la centralisation de l'outil de gestion de clés; dans ce schéma, il y a que le home server qui se charge de la gestion sécurisée des clés de tout le système (génération, chiffrement, déchiffrement, distribution) ce qui augmente la charge sur ce serveur de plus si jamais cette entité tombe en panne tout le système sera exposé aux attaques. Le second problème apparaît lorsque le nœud mobile effectue un intra domain handover (migration vers un foreign agent dans le même domaine que l'ancien), dans ce cas précis le nœud mobile effectue l'authentification des entités en gardant *les anciennes clés de communication* (déjà partagées lors d'une ancienne session MIP/AAA). Cela pose un problème en cas où les clés sont découvertes ou cassées.

Dans cette thèse, nous avons proposé un nouveau schéma d'authentification pour le protocole Mobile IP. Ce schéma propose des améliorations à l'ancien modèle d'authentification Mobile IP/AAA. Nous avons opté de continuer l'exploit et l'amélioration de ce schéma essentiellement parce qu'il est renforcé en matière de sécurité par rapport aux autres schémas grâce à la collaboration des structures AAA qui se préoccupent des opérations cryptographiques indépendamment des acteurs du protocole.

Notre contribution se résume en deux points essentiels :

- La certification des serveurs locaux : c'est une étape préliminaire durant laquelle les serveurs AAAL envoient leurs clés publiques pour être signer par le broker approprié.

Un serveur certifié d'une entité digne de confiance aura l'avantage de générer et distribuer les clés de communication entre les acteurs Mobile IP.

- La génération et la distribution des clés: le serveur étranger certifié pourra générer et distribuer les clés de session ou de communication suite à une demande d'enregistrement Mobile IP, rôle affecté dans l'ancien schéma MIP/AAA au AAAH. Le but principal de cette phase est la décentralisation du processus de gestion des clés, le système continue à authentifier ces acteurs même dans le cas où le AAAH tombe en panne.

En effet, nous avons considéré trois types de handoff, selon le déplacement du nœud mobile :

- Handoff Type I: se déroule lorsque le nœud mobile sort pour la première fois de son domaine mère vers un autre étranger.
- Handoff Type II : se déroule lorsque le nœud mobile se déplace à une nouvelle cellule dans le même domaine étranger.
- Handoff Type III : se déroule lorsque le nœud mobile migre vers une nouvelle cellule d'un autre domaine étranger.

Dans le premier type de handoff, nous enregistrons la première migration du mobile vers un domaine étranger où le serveur local demande une notification auprès du AAAH concernant l'authenticité des acteurs, le AAAH envoie la réponse suite à la vérification du certificat du AAAL.
Le temps complet d'authentification augmente proportionnellement par rapport au nombre de brokers intermédiaires entre le AAAL et le AAAH, cela est dû à l'ajout du temps de transmission supplémentaire entre les serveurs et les brokers et entre les brokers eux mêmes, ainsi qu'à l'ajout du temps de calcul cryptographique de ces entités.
Le délai d'authentification lors du handoff de Type III (inter domain handoff) est diminué par rapport à l'ancien modèle MIP/AAA, puisque nous suggérons de demander les informations d'authentification au serveur AAAL le plus proche et ayant déjà authentifié le MN et le HA associé.

Pour palier au problème de la re-authentification locale dans MIP/AAA/Type II où les clés de session ne sont pas renouvelées, nous avons proposé la regénération de ces clés à chaque intra domain handoff. Et puisque cette phase est supplémentaire par rapport au schéma initial, nous avons choisi l'algorithme MARS qui génère ces clés en un temps raisonnable et qui assure une communication rapide entre les acteurs Mobile IP.

Nous enregistrons un gain important en le délai complet d'authentification en particulier en cas d'expiration du délai d'enregistrement dans le modèle Mobile IP/AAA où le nœud mobile doit recontacter le AAAH pour effectuer une authentification complète en passant par les brokers intermédiaires, alors que dans notre schéma l'authentification continue à s'effectuer localement.

Nous envisageons des perspectives qui se dessinent sur deux axes : la sécurité et la gestion de la mobilité:

- Essayer de trouver un moyen de communication normalisé entre le MN et le FA (puisque ce dernier ne peut pas vérifier la validité de la réponse du challenge immédiatement, il doit faire confiance au AAAH du MN).
- Utiliser d'autres algorithmes plus robustes et plus rapides dans le but de réduire le temps de chiffrement et par conséquent le délai complet d'authentification.
- Etendre l'application de notre proposition pour le protocole Mobile IPv6.
- Etendre cette étude pour être applicable même lors d'une authentification dans un environnement de micro mobilité.

Bibliographie

[AGA01] Khaldoune Al aga , Guy Pujolle, Guillaume VIVIE, «Réseaux de mobiles et réseaux sans fil », Edition Eyrolles 2001.

[ALE00] N. Aleb, «Spécification des Systèmes en Environnement Mobile à l'aide du Pi-calcul », Thèse de Magister, USTHB, Octobre 2000.

[ALI00] Aliouane Lynda , Chenait Manel, «Le paiement électronique sécurisé », Mémoire de fin d'étude pour l'obtention du diplôme d'ingénieur d'état en informatique , USTHB 2000.

[BAD95] N. Badache, « La Mobilité dans les Systèmes Répartis », Publication Interne IRISA n° 962, Octobre 1995.

[BAG95] Baggio, «Environnements Mobiles : Etude et Synthèse Bibliographique» DEA de Systèmes Informatiques, Laboratoire MASI, Université Pierre et Marie Curie, 1995.

[BAR04] Cédric Barboiron, Xavier Chouteau, Naïme El Mimech, « Les protocoles IPv4 et IPv6 », février 2004.

[BEN04] Minna Ben haddou, Wilfried Duquenne, « système repartis », Master TIIR, université de Lille1, 2004.

[BER01] Laurent Bernat, « dossier de la balise: Glossaire », 2001

[BID95] C. Bidon & V. Issamy, «Un aperçu des problèmes de sécurité dans les systèmes informatiques », IRISA (Institut de Recherche en Informatique et Systèmes Aléatoires)- Publication interne N°959, octobre 1995, France.

[BLU03] Gwenael Blum ,Florian Lasowy, Cyril Guerin, Cédric Pfeiffer, « Protocole AAA principes et implantations », 2003.

[BOU01] Julien Bournelle .Maryline Laurent-Maknavicius, «Etat de l'art de AAA et Diameter», Département logiciels –Réseaux (LOR). Institut national des télécommunication , France 2001

[BOU03] Julien Bournelle .Maryline Laurent-Maknavicius, «Adaptation et implémentation de Diameter/AAA pour Mobile IPv6 », Département logiciels – Réseaux (LOR). Institut national des télécommunication , France 2003

[BUT02] L. Butti ,O. Charles, « Wireless LAN security », Séminaire WLAN, Direction de l'innovation de France Télécom, mars 2002.

[CAL01] P. Calhoun, H. Akhtar, J. Arkko, E. Guttman, A. Rubens,G. Zorn, « Diameter Base Protocol », Internet Draft, work in progress, June 2001, draft-ietf-aaa-diameter-06.txt.

[CAL02] R. Calhoun , Tony Johansson, Charles E. Perkins., «Diameter Mobile IPv4 Application», draft-ietf-aaa-diameter-mobileip-13.txt.

[CHA02] Olivier CHARLES, «Sécurité et mobilité : panoramas des problèmes de sécurité de la mobilité sur IPV6 », Ecole Supérieure d'Informatique et Applications de Lorraine, 2002

[CHE04] Manel Chenait, Djamel Tandjaoui, Nadjib Badache, «New Authentication Scheme in Mobile IP», First Ifip International conference on wireless and optical communications networks WOCN, Sultan Qaboos University Muscat, Oman, 2004.

[CIR97] S. Jacobs, G. Cirincione, «Security of current Mobile IP solutions», Proc. of IEEE MILCOM'97, Monterey, CA, USA, 1997.

[COM99] COMBES Jean-Michel, «Etudes des failles de sécurité des protocoles de mobilité dans l'Internet Nouvelle Génération », Rapport de Soutenance de

Projet de Fin d'Etudes, Projet réalisé au CNET à Issy-Les-Moulineaux (DTL/SSR),1999.

[CON03] Denis Conan, Sophie Chabridon, Olivier Villin, and Guy Bernard, «Domint: A Platform for Weak Connectivity and Disconnected CORBA Objects», 2003.

[DAI04] Wei Dai , «Crypto++ 5.2.1 Benchmarks», 2004

[DAV97] D.W. Davies & W. Price, «Sécurité dans les réseaux informatiques », 1997

[FOR94] G. Forman, J. Zahorjan, «The Challenges of Mobile Computing», Computer Science & Engineering, University of Washington, US, IEEE Computer, pages 39-47, April 1994.

[GUS01] Ulf Gustafson, Jan Forslöw, «Network design with Mobile IP» INET, Stocholm, Sweden, 2001.

[ICH02] Tetsuya ICHIKAWA, Tomomi KASUYA, Mitsuru MATSUI, «Hardware Evaluation of the AES Finalists », Mitsubishi Electric Corporation, 2002.

[IOA91] J. Ioannidis, D. Duchamp, G. Q. Maguire, «IPbased Protocols for Mobile Internetworking», Proc. of ACM SIGCOMM Symposium on Communication, Architectures and Protocols, pages 235–245, September 1991.

[KIS92] James J.Kistler and M. Satyanarayanan, «Disconnected Operation in the Coda File System», ACM Transactions on Computer Systems 10(1), February, 1992.

[KLE00]] Matthieu KLEIN, «PGP et applications cryptographiques», Rapport de licence EEAsur les techniques de chiffrement, 2000.

[KLE96] M.KLEIN, «PGP et applications cryptographiques», 1996

[LEG01] M. Gwendal LE GRAND, «Qualité de service dans des environnements Internet mobile » Thèse de doctorat de l'Université Pierre et Marie Curie, 2001.

[LEV99] T.L.ABEGNOLY, «Une infrastructure PKI pour la sécurité accrue », Revue 01 Réseaux n°73, 1999

[MAK01] Julien Bournelle, Maryline Laurent-Maknavicius, «Critiques et améliorations possibles de Diameter», Institut national des télécommunication , France 2001

[MAR93] B. Marsh, F. Douglis, R. Cáceres,«System Issues in Mobile Computing "Matsushita Information Technology Laboratory, Technical Report MITL-TR-50-93, February 1993.

[MON01] Nicolas MONTAVONT, «La mobilité dans les réseaux IP», Rapport du DEA en informatique , Université Louis Pasteur de Strasbourg , 2001

[NAH95] Erich Nahum, Sean O'Malley, Hilarie Orman_ , Richard Schroeppel, «Towards High Performance Cryptographic Software» University of Massachusetts, 1995.

[NOU01] N. Nouali, « Impact de la mobilité sur les modèles de transactions », Publication Interne, Cerist, Janvier 2001.

[PAC02] Sangheon PACK, Yanghee CHOI, «Fast inter-AP handoff using predictive authentication scheme in a public wireless LAN», School of computer science and engineering , Seoul national university, Seoul , Korea, 2002.

[PER00a] C. Perkins, «Mobile IP Joins Forces with AAA», IEEE Personal Communications .vol7 Issue 4 August 2000.

[PER00b] Charles E. Perkins, «Route optimisation in Mobile IP», draft-ietf-mobileip-optim-10, 2000.

[PER96] C. Perkins, «IP Mobility Support», RFC2002, Network Working Group, October 1996.

[PER96] C. Perkins, R. Calhoun, «AAA Registration Keys for Mobile IP», Mobile IP Working Group, Internet draft, Nokia Research Center draft-ietf-mobileip-aaa-key-11.txt

[PER98] C.Perkins, « Mobile IP : Design Principles and practice », Addison-Wesley Longman, 1998

[PIT93] E. Pitoura, B. Bhargava, «Dealing with Mobility: Issues and Research Challenges», Technical Report TR-93-070, Department of Computer Science, Purdue University, November 1993.

[RAM01] Barandharan RAMAN, «Security in wireless networks», Department of Computer Science, Texas A&M University, December 2001.

[RFC2002] C.Perkin , «IP Mobility Support», Network Working Group ,1996.

[RFC2401] S. Kent, R. Atkinson , «Security Architecture for the Internet Protocol», November 1998.

[RFC2409] D. Harkins, D. Carrel, «The Internet Key Exchange (IKE) », November 1998

[RFC2977] S. Glass, T. Hiller, S. Jacobs, C.Perkin, «Mobile IP Authentication, Authorization, and Accounting requirements », Network Working Group ,1996

[RFC791] Darpa Internet program Protocol specification , «Internet Protocol », September 1981

[SAA00] Saadi Rachid, Berbar Ahmed, « la protection de la messagerie électronique par des méthodes cryptographiques», Mémoire de fin d'étude pour l'obtention du diplôme d'ingénieur d'état en informatique , USTHB 2000.

[SAT90] Satyanarayanan, M., Kistler, J.J., Kumar, P., Okasaki, M.E., Siegel, E.H., Steere, D.C. «Coda: A Highly Available File System for a Distributed Workstation Environment», IEEE Transactions on Computers 39(4), April, 1990.

[SCH01] G. Schäfer, A. Festag, H. Karl, «Performance Evaluation of AAA / Mobile IP Authentication», Telecommunication Networks Group, Technical Report TKN-01-012, 2001.

[SCH02] G. Schäfer, A. Festag, H. Karl, «Current Approaches to Authentication in Wireless and Mobile», Telecommunication Networks Group, Technical Report TKN-01-002, 2002.

[SEB02] Abderrazek SEBA, «Optimisation de route dans Mobile IP» , Mémoire de fin d'étude pour l'obtention du diplôme d'ingénieur d'état en informatique , USTHB 2002.

[SUD03] Sudha Sudanthi, «Mobile IPv6 security», GSEC, 2003

[TAN03] Jin Tang, «Authentication in Mobile IP», Communications Systems Center; Georgia Institute of Technology, 2003

[TEW02] H. Tewari, D. O'Mahony, «Lightweight AAA for Cellular IP», Computer Science Department Trinity College, Irland, 2002.

[THO02] Thomas NOEL, «Apports de la mobilité IPv6 par rapport à la mobilité IPv4», LSIIT, 2002

[TON02] Toni SOUEID, «Présentation de Mobile IPv6», 2002

[TUQ99] Gloria Tuquerres, Marcos Rogério Salvador and Ron Sprenkels, "Mobile IP: Security and application", Telematics Systems and Services - Centre for Telematics and Information Technology University of Twente,1999

[VEN02] Håkan Ventura, «Diameter next generation's AAA protocol», Master thesis in Information theory at Linköpings Tekniska Högskola, Sweden, 2002

[WAN00] Hsiu-Chiung Wang, «Speed Improvement for the RSA Encryption Method», Thesis for master, Philosophy of computer department in Napier University.

[WON01] Duncan S. Wong, Hector Ho Fuentes, Agnes H. Chan, «The Performance Measurement of Cryptographic Primitives on Palm Devices », College of Computer Science, Northeastern University, USA 2001.

[ZAO97] J. Zao, S. Kent, J.Gahm, «A Public-key based secure Mobile IP»,Proc of 3rd Annual ACM/IEEE Intl Conference, MobiCom'97, Budapest, Hungary.

[ZIM98] P. Zimmerman, «Introduction à la cryptographie», 1998