Un Nouveau schéma d'authentification Pour le protocole Mobile IP

Chenait[1] Manel, Tandjaoui[1] Djamel, Badache[2] Nadjib
[1] CERIST,
E-Mail: m_chenait@mail.cerist.dz, dtandjaoui@mail.cerist.dz
[2]LSI, USTHB,,Alger
E-Mail: badache@wissal.dz

1. Introduction

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. 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 sera nécessaire de s'assurer de l'authenticité des mobiles avant de leur permettre de s'enregistrer auprès d'un réseau étranger.

Beaucoup de travaux ont été proposés pour améliorer la sécurité de l'authentification du protocole Mobile IP, mais qui restent insuffisants en matière de sécurité et de performance : L'authentification standard 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. L'utilisation des cryptosystèmes à clé publique a été proposée pour résoudre le problème de la scalabilité, mais ça reste une solution 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 mais il comporte deux points faibles qui sont : la centralisation de l'outil de gestion de clés et le non-renouvellement des clés de communication lors d'un intra-domaine handoff.

Notre article présente un nouveau schéma d'authentification pour Mobile IP qui propose des améliorations à l'ancien modèle d'authentification Mobile IP/AAA. L'idée de base est de re-générer de nouvelles clés pour l'authentification en local en évitant de contacter le domaine mère à chaque changement de cellule. En effet, les clés seront re-générées par les serveurs locaux certifiés et non pas par le home server. Ce nouveau schéma améliore l'authentification des nœuds mobiles dans le protocole Mobile IPv4 tout en diminuant la latence du handover.

2. Le protocole Mobile IP

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 (réseau mère et réseaux étrangers) 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.
On distingue entre les routeurs suivants: L'Agent mère (Home agent) qui est un routeur sur le réseau mère, il met à jour les informations concernant la position du mobile et tunelle les datagrammes destinés à ce dernier. Et l'agent étranger (Foreign Agent) qui est le routeur sur le réseau visité, il fournit des services de routage au mobile lors de son enregistrement.

D'une manière générale, trois étapes jalonnent le fonctionnement de Mobile IP:

- **La découverte des agents** : C'est l'étape de la découverte des agents (agent mère et agents étrangers).
- **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.

3. L'authentification dans le protocole Mobile IP

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.

D’une manière générale, Il est indispensable d’authentifier les acteurs avant de leur permettre de se déplacer d’un réseau à un autre.
Trois approches ont été proposées pour la sécurisation de la procédure d’authentification dans Mobile IP à savoir: l’authentification standard, l’authentification à clé publique et l’authentification Mobile IP/AAA.

3.1 Les schémas d’authentification proposés pour Mobile IP

3.1.1 L’authentification standard dans Mobile IP

L’authentification standard est une solution intégrante dans Mobile IP, son principe est 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.
Au premier coup d’œil ce schéma parait suffisant Néanmoins, il comporte plusieurs inconvénients : il considère l’existence d’une relation de confiance pré-établie entre les trois acteurs (MN, FA, HA) alors qu’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, et même si on considère que les trois entités partagent des clés entre elles, cette solution reste inefficace en l’absence d’un outil de gestion digne de confiance qui se charge de générer et de distribuer ces clés en toute sécurité et en particulier lors du déplacement des nœuds mobiles entre des réseaux gérés par des opérateurs distincts. En outre, la clé secrète partagée utilisée par le FA et le HA est établis à l’aide du standard du IPSEC le **IKE** (Internet Key Exchange) qui est un protocole à objectif très générique et qui nécessite plus d’efforts que le Mobile IP a besoin.

3.1.2 L’authentification basée sur les clés publiques

Ce schéma a été proposé par Zao[ZAO97], il était parmi les premières tentatives de sécurisation du protocole Mobile IP. L’auteur a supposé que chaque entité possède une paire de clé publique/privé certifiée.
Pour assurer l’authentification mutuelle, les trois entités Mobile IP associent aux messages échangés leurs signatures et leurs certificats comme preuve d’identité (Figure 1)

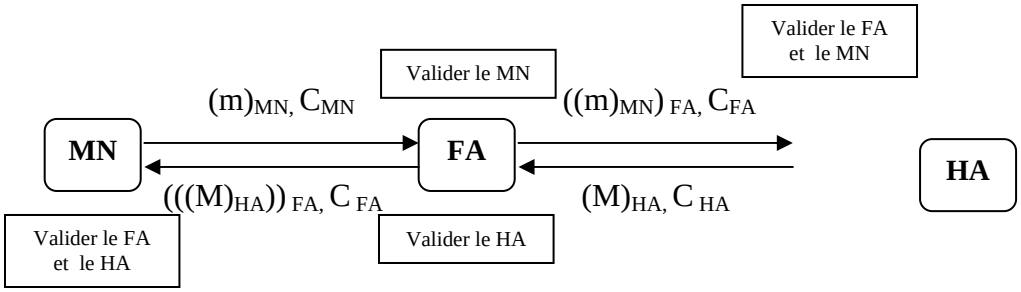

Figure 1 : Authentification basée sur les clés publiques

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 mobile à cause de l'utilisation des algorithmes a clés publiques qui nécessitent une grande puissance de calcul.

3.1.3 L'authentification Mobile IP/AAA

Un grand nombre d'attaque peut être évité si un contrôle strict des accès au réseau de visite était effectué avant toute opération d'enregistrement à l'agent mère, pour cela, 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.

L'architecture AAA 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

Des associations de sécurité « statiques » sont définies entre (Figure2)
- FA et AAAL.
- MN et AAAH.
- HA et AAAH.
- AAAL et AAAH.
- Serveurs AAA et un ou plusieurs Brokers.

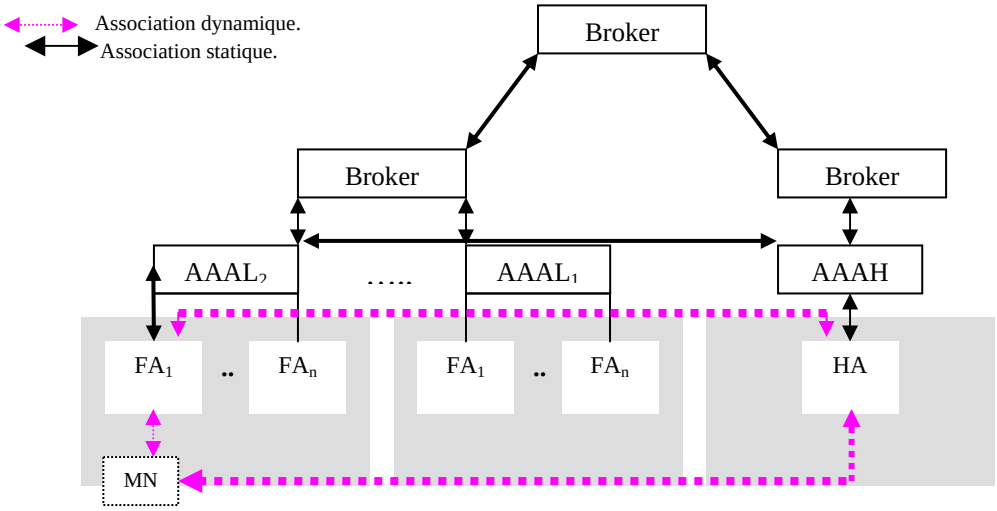

Figure 2 : Les associations de sécurité statiques et dynamiques dans Diameter.

Le flux de messages échangé est le suivant :

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}.

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

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.

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

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 chiffrées 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 clés 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 sécurisée. Néanmoins, ce schéma comporte encore quelques problèmes en terme de sécurité et de performance:

- Le grand nombre de d'entités impliquées dans ce schéma rend l'analyse de la sécurité plus difficile.[SCH 02]
- 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.

4. Un nouveau schéma d'authentification pour le protocole Mobile IP

4.1 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 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 3).

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.

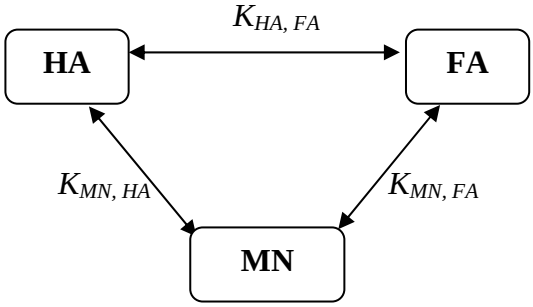

Figure 3 : Les clés partagées lors de l'authentification Mobile IP/AAA.

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 clés auprès du AAAH et d'augmenter la latence du handover

4.2 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].

Notre solution se résume en deux phases importantes:
La première phase: La certification des serveurs locaux AAAL(s) par le brocker.
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)).

4.3 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)
- **TypeII** (*Intra domain handover)*: se déroule lorsque le nœud mobile se déplace à une nouvelle cellule dans le même domaine étranger. (Figure5)
- **TypeIII** *(Inter foreign domain handover)*: se déroule lorsque le nœud mobile migre vers une nouvelle cellule d'un autre domaine étranger. (Figure6)

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

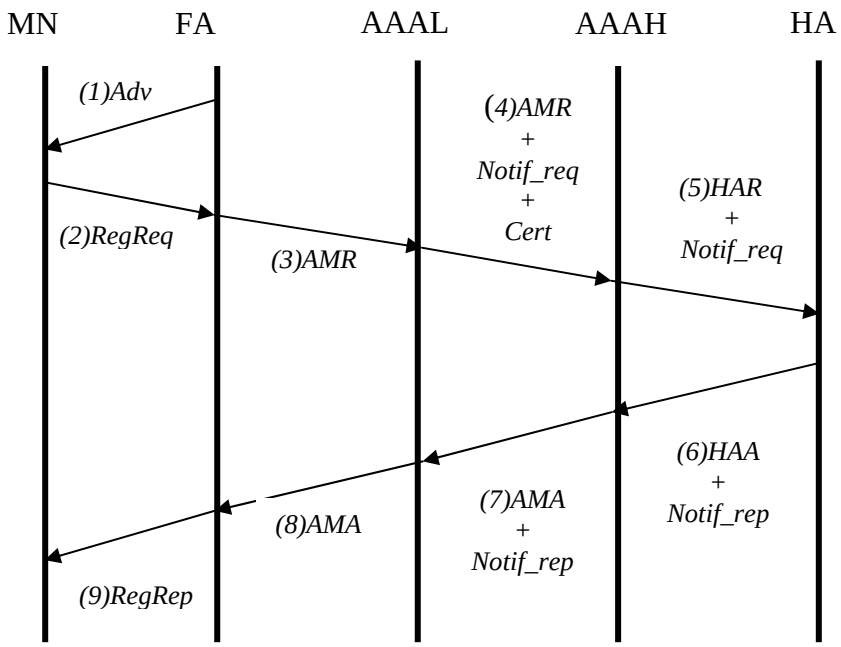

Figure 4 : Flux de messages durant le First Inter domain handover (TypeI)

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)* 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*) 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 propres 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 ($Sig_{HA,MN}$) créée 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.

4.3.2 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.

Dans ce cas, les étapes d'authentification sont comme suit: (Figure5)

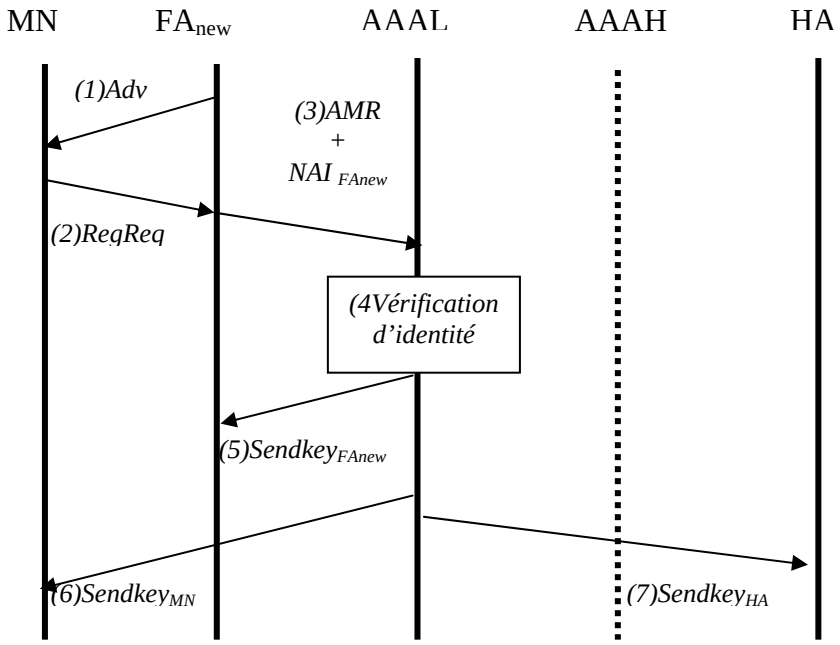

Figure 5 : Flux de messages durant l'Intra domain handover (TypeII)

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.

4.3.3 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(Figure6).

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)

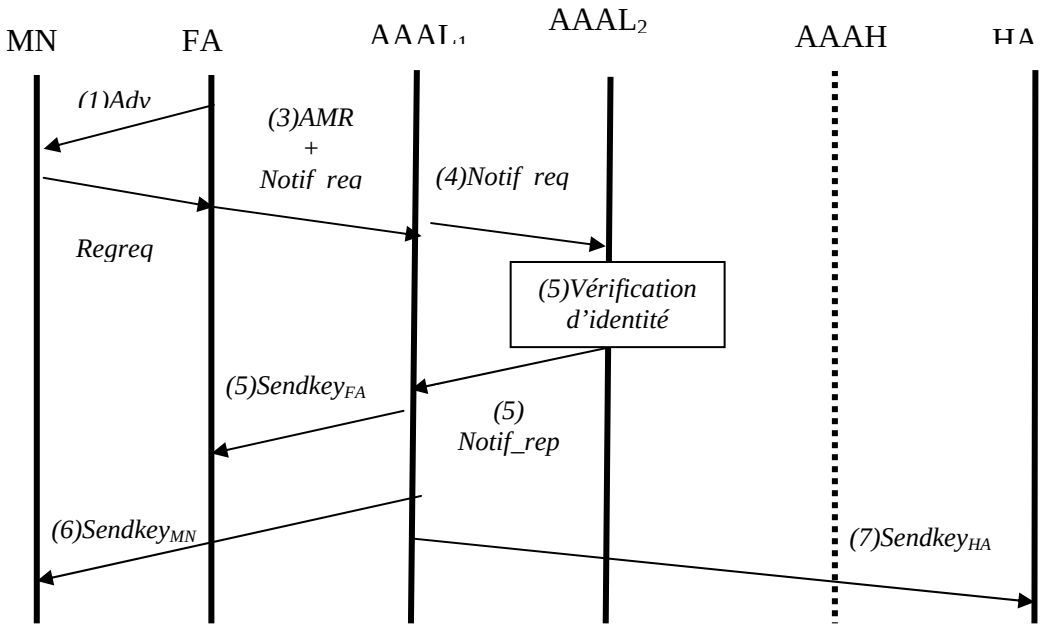

Figure 6 : Flux de messages durant Inter foreign domain handover (TypeIII)

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 $AAAL_1$ ($k_{pubAAAL2}$) *e*t son certificat ($Cert_{AAAL1}$)

$$AAAL_1 \rightarrow AAAL_2 : \{AMR,\ldots, \ldots RegReq,\ldots, x_{FA}, NAI_{MN} \oplus Notif\_req\}\ k_{pubAAAL2} \oplus Cert_{AAAL1}$$

5) A la réception, le $AAAL_2$ décrypte le message à l'aide de sa clé privée, 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].

4.4 Avantages et inconvénients de la solution

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

4.4.1 Avantages

- **Décentralisation de la gestion des clés** : la gestion des clés (génération, distribution, chiffrement, déchiffrement) est partagée entre plusieurs entités (solution distribuée).
- **Tolérance aux pannes**: 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 en 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.

4.4.2 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 I entre le serveur AAA et les acteurs Mobile IP.

5. Conclusion

Dans cet article, 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 procédure 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 locale des clés est toujours possible. En effet, lorsqu'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.

6. Références bibliographiques

[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.

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

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

[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.