La mobilité dans COPS

Alain RINGAPIN[1,2], Jalel Ben-Othman[1], Pascal Urien[2]

[1]Laboratoire PRiSM, Université de Versailles
45, av. des Etats Unis
78035 – Versailles – France
{ringap, jbo}@prism.uvsq.fr

[2]SchlumbergerSema
36-38 rue de la princesse
78431 – Louveciennes – France
{Purien, Aringapin}@.slb.com

Résumé

Les services mobiles connaissent un succès grandissant auprès des usagers. Lancés par le GSM, on présage aisément de l'avenir de ce type de services, notamment avec les futurs réseaux de 4ième génération. Il est alors envisageable que les usagers mobiles exigeront un niveau de qualité de service similaire à celui des usagers fixes. Dans les réseaux mobiles, les mécanismes de sécurité et de **Q**uality **o**f **S**ervice (**QoS**) utilisés dans les réseaux fixes ne sont pas adaptés. Cet article décrit une approche pour la gestion des déplacements des usagers ainsi qu'aux moyens de mise en œuvre de la QoS liée à cette mobilité. La QoS est faite au niveau de la signalisation grâce à une extension du protocole **COPS** (**C**ommon **O**pen **P**olicy **S**ervice).

Mots clefs : COPS, mobilité, QoS, sécurité, carte à puce.

Introduction

Avec le succès d'Internet, le nombre de réseaux ne cesse d'augmenter. Une conséquence directe de cet état de fait est la difficulté de configurer les équipements au cœur des réseaux (routeurs, passerelles, …). Pour simplifier et automatiser la configuration de ceux-ci, une approche de gestion de réseaux grâce à des politiques émerge. Les politiques peuvent être définies comme un ensemble de règles capables de gérer et contrôler l'accès aux ressources d'un réseau. Ces règles peuvent concerner des domaines aussi divers que la QoS, la sécurité, la mobilité, … Pour normaliser cette approche, l'IETF a spécifié un protocole extensible : COPS (Common **O**pen **P**olicy **S**ervice). Plusieurs extensions de COPS concernant la QoS, la sécurité, … sont proposées dans des réseaux fixes mais peu en revanche dans un contexte mobile. Nous proposons une extension de COPS pour gérer la QoS et l'authentification des usagers dans un contexte mobile.

Cet article est divisé en trois parties : la première présente un état de l'art sur le protocole COPS, dans la deuxième, nous décrivons les problèmes liés à la mobilité dans les réseaux sans fils, et la dernière présente notre contribution pour résoudre les problèmes énoncés.

1. Etat de l'art

a) Présentation de COPS

Le protocole COPS, spécifié par l'IETF dans [1], décrit un modèle extensible pour l'échange d'informations d'administration réseau entre un serveur et ses clients (routeurs, commutateurs, ...).
Ce protocole est constitué de deux principaux éléments :

- Le **PDP** (**P**olicy **D**ecision **P**oint) est responsable des prises de décision (comportement sur un flux ou des paquets) pour la gestion d'un domaine. Il peut émettre un ordre de sa propre initiative ou après avoir été sollicité par des PEP (**P**olicy **E**nforcement **P**oint). Il doit également gérer les ressources en déterminant les règles à appliquer aux PEP. Il convertit les règles de politique dans un format adapté (sous forme de **P**olicy **I**nformation **B**ase, **PIB**) et garanti leur acheminement aux PEP.

- Le **PEP** (**P**olicy **E**nforcement **P**oint) est un équipement du réseau (routeur, passerelle, …) où sont mises en application les règles de politique (QoS, sécurité, mobilité, …) définies par le PDP. Les fonctions principales du PEP consistent d'abord à faire la correspondance entre les règles définies dans les PIB et

la configuration des équipements réseaux ; puis d'exécuter les décisions du PDP et de l'en informer via des rapports.

Ce protocole possède une architecture centralisée qui permet le stockage des politiques, la prise de décision et la distribution de paramètres de configuration aux équipements. Il autorise également une gestion centralisée car, comme le décrit la Figure 1, le PDP possède une vue globale de toutes les ressources disponibles (bande passante, …) dans chaque PEP à l'intérieur du domaine qu'il administre.

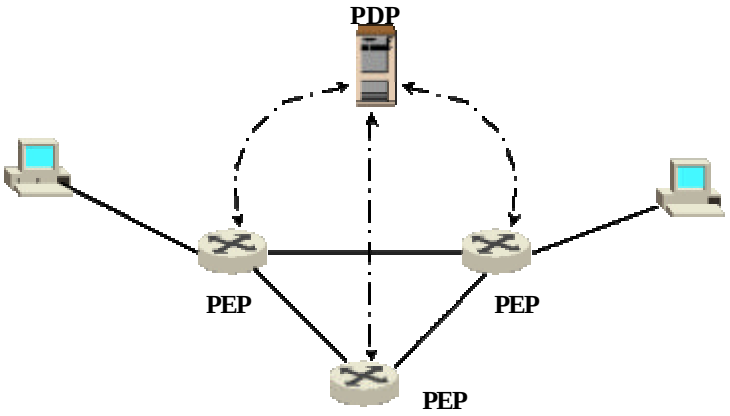

Figure 1: Architecture de COPS

COPS a aussi la possibilité de stocker les politiques. Pour cela, il convertit les règles sous forme de PIB accessible aux PDP et PEP.
La gestion du réseau s'effectue selon deux modèles :

- le modèle 'outsourcing" dans lequel le PEP fait appel au PDP pour réagir face à une situation pour laquelle il ne dispose pas des règles adéquates. Cette approche est particulièrement adaptée à des protocoles de signalisation de bout en bout de type Ressource reSerVation Protocol (COPS-RSVP défini dans [3]), Multi Protocol Label Switching défini dans [4], ...
- le modèle "provisionning" suppose que le PDP configure les PEP à partir de nouvelles règles d'utilisation du réseau (date, heure, règles de gestion, …) sans avoir été sollicité. Ce modèle est utilisé pour contrôler l'utilisation du réseau pour les protocoles non signalés, comme Diffserv ; ou pour configurer les équipements. L'usage de **COPS** for policy **PR**ovisionning (COPS-PR) est défini dans [2].

b) Les extensions de COPS

Dans la suite, nous présentons les différentes extensions existante de COPS. On les différencient selon trois critères : les politiques de QoS, les politiques de mobilité et celles de la sécurité.

☞ Les politiques de QoS

- COPS-PR

COPS for **PR**ovisioning décrit les mécanismes et conventions de communication entre PDP et PEP indépendamment des politiques mises en œuvre. Son utilisation est préconisée pour la gestion de la signalisation dans le modèle « provisioning ». COPS-PR, par le biais du PDP, transmet les politiques nécessaires aux PEP afin de conditionner leurs réactions à des évènements extérieurs. Il est également utilisé pour mettre en œuvre la gestion de réseaux Diffserv.

- COPS-RSVP

COPS-Ressource re**S**er**V**ation **P**rotocol est la première extension normalisée par l'IETF. Elle décrit les mécanismes et conventions de communication entre PDP et PEP indépendamment des politiques mises en œuvre. Son utilisation est préconisée pour la gestion de la signalisation dans le modèle « outsourcing ». Lorsqu'un flux RSVP est détecté par un PEP dans son voisinage, il en extrait les objets et les acheminent,

dans une requête, vers le PDP. Ce dernier décide si le message doit être acheminé vers le PEP suivant ou être supprimé. Le but de COPS-RSVP est d'offrir une meilleure QoS que le best-effort. Il est également utilisé pour mettre en œuvre des réseaux de type Intserv qui réservent des ressources pour fournir de la QoS.

- négociation de la QoS

COPS-Service **L**evel **S**pecification [5] est une extension de COPS qui permet une négociation de la QoS. Cette extension propose de positionner le PEP au niveau des équipements terminaux (passerelle d'un réseau local, équipement connecté par modem, …). Un SLS est un ensemble de paramètres et valeurs qui définissent le service offert à un flux de données. Dans ce modèle, le PEP peut négocier la QoS auprès du PDP en envoyant le SLS souhaité à son serveur. Ce dernier peut accepter, rejeter ou proposer un autre SLS au client. Cet échange prend fin lorsqu'une proposition est acceptée par les deux parties ; le PEP peut effectuer cette négociation pour lui-même ou au nom d'autres entités. COPS-SLS met en œuvre deux phases : une phase de configuration pendant laquelle le PDP utilise le modèle provisioning et installe dans le PEP les politiques permettant de négocier le SLS ; puis une phase de négociation qui gère l'échange d'informations sur l'accord d'un SLS entre le PEP et le PDP. Les informations relatives aux SLS, échangées entre les PDP et PEP, sont représentées dans une PIB.

☞ Les politiques de mobilité

Les travaux de mobilité sur COPS considèrent essentiellement deux types de mobilité : les déplacements des terminaux et ceux des usagers. La mobilité de l'usager permet à un utilisateur d'accéder aux services auxquels il a souscrit, indépendamment du terminal utilisé ; ceci, sous réserve que le terminal possède les fonctionnalités requises par les services. Autrement dit, l'utilisateur est libre d'utiliser un terminal différent à chacune de ses connexions. Il est toutefois nécessaire pour accomplir cela d'identifier de façon unique l'usager (login/mot de passe, carte à puce, …). La mobilité du terminal a pour but d'assurer la continuité d'une connexion pendant son changement de point d'attachement au réseau. Cependant, si on considère les services mobiles, les deux aspects sont liés : un usager ne peut se déplacer sans un terminal. Dans les réseaux GSM, la liaison entre les deux types de mobilité est assurée par le biais de la carte SIM.
Il existe deux extensions de COPS pour l'utiliser dans un contexte mobile : la première gère la mobilité des terminaux en adaptant Mobile IP pour COPS ; la seconde gère la mobilité des usagers dans COPS.

Le travail le plus abouti définit **COPS-M**obile **IP,** une extension de COPS pour Mobile IPv4 décrite dans [6]. Dans ce draft, les rôles de **H**ome **A**gent (HA) et **F**oreign **A**gent (FA) sont tenus par des PEP. Chaque PEP étant sous l'administration d'un PDP, on obtient donc pour le Home Network un Home Policy Decision Point et un Home Policy Enforcement Point (assimilé au HA). Dans le Foreign Network, on a un Foreign Policy Decision Point et un Foreign Policy Enforcement Point (assimilé au FA). La Figure 2 représente le schéma d'établissement de connexion lors de l'arrivée d'un mobile dans un Foreign Network.

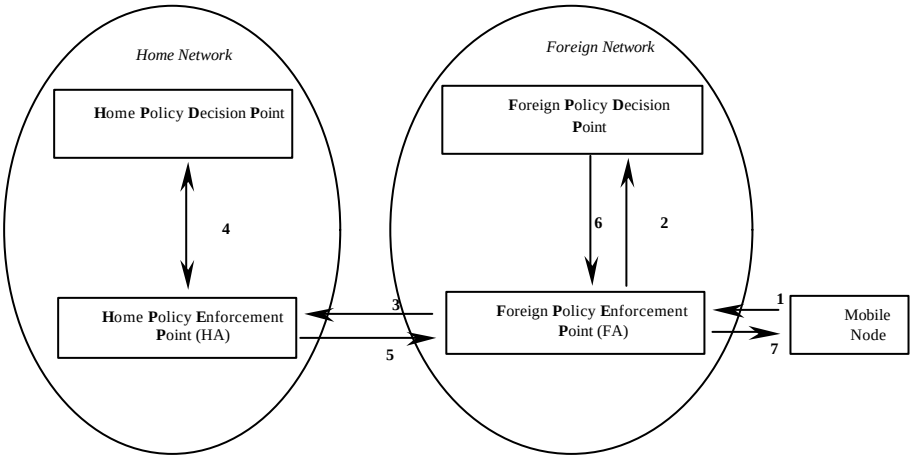

Figure 2 : Procédure d'enregistrement d'un nœud mobile

1 : Le **M**obile **N**ode (MN) envoie une requête d'enregistrement au **F**oreign **A**gent (FA).
2 : Le FPEP et le FPDP interagissent pour décider des politiques à appliquer sur la demande d'enregistrement.
3 : Le FA relaie la demande d'enregistrement du terminal au **H**ome **A**gent (HA).
4 : Le HPEP et le HPDP interagissent pour décider des politiques à appliquer sur la demande d'enregistrement.
5 : Le HA envoie la réponse d'enregistrement au FA.
6 : Le FPEP et le FPDP interagissent pour décider des politiques à appliquer sur la réponse d'enregistrement.
7 : Le FA fait suivre la réponse d'enregistrement au Mobile Node

[14] définit **COPS-M**obile **U**ser (COPS-MU) pour la gestion de la mobilité des usagers dans COPS. Cette extension présente l'avantage, par rapport à COPS-MIP, d'être utilisable aussi bien sur des réseaux IPv4 que IPv6. Pour assurer la mobilité des usagers et des terminaux, cette architecture représente le réseau selon deux points de vue. Elle distingue la vision de l'utilisateur décrite sur la Figure 3 et celle du terminal décrite sur la Figure 4. Les éléments concernant le terminal sont précédés du **T** de **T**erminal et ceux concernant l'usager sont précédés du **U** de **U**ser.

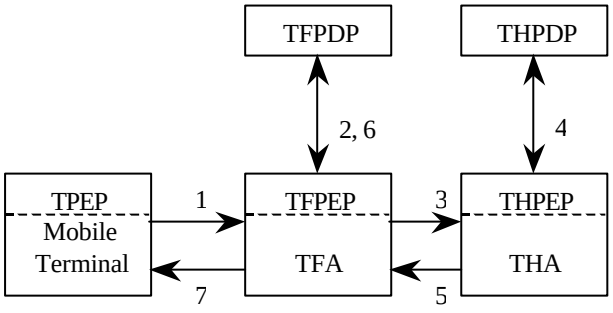

Figure 3: Enregistrement d'un terminal

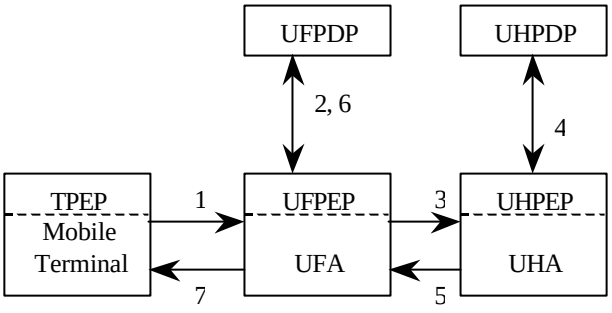

Figure 4: Enregistrement d'un utilisateur

Les procédures d'enregistrement sont symétriques dans les deux cas. Nous allons donc présenter seulement celle de la Figure 3.

1 : Le **M**obile **T**erminal (MT) envoie une requête d'enregistrement au **T**erminal **F**oreign **A**gent (FA).
2 : Le TFPEP et le TFPDP interagissent pour décider des politiques à appliquer sur la demande d'enregistrement.
3 : Le TFA relaie la demande d'enregistrement du terminal au **T**erminal **H**ome **A**gent (THA).
4 : Le THPEP et le THPDP interagissent pour décider des politiques à appliquer sur la demande d'enregistrement.
5 : Le THA envoie la réponse d'enregistrement au TFA.
6 : Le TFPEP et le TFPDP interagissent pour décider des politiques à appliquer sur la réponse d'enregistrement.
7 : Le TFA fait suivre la réponse d'enregistrement au Mobile Terminal

L'enregistrement d'un terminal s'effectue seulement si ce dernier est situé dans un réseau étranger. Par contre, celui de l'utilisateur doit se faire dans tous les cas de figure. L'enregistrement du terminal met à jour une association dans le THA (**T**erminal **H**ome **A**gent) entre l'adresse du terminal ou CoA (**C**are **o**f **A**dress) et son adresse d'origine (Home Adress). L'enregistrement de l'usager établit une association dans le UHA (**U**ser **H**ome **A**dress) entre l'identificateur de l'usager et l'adresse IP du terminal qu'il utilise.
COPS-MU permet également d'assurer la portabilité des services ainsi que la négociation de la QoS. Cette QoS comprend les paramètres usuels : bande passante, retard, gigue et perte de paquet. Elle contient, de plus, deux nouveaux paramètres pour la gestion de la mobilité : perte de paquet due au handoff et la probabilité de blocage.

☞ Les politiques de sécurité

Dans le domaine de la sécurité, deux approches se distinguent dans COPS : la première a pour but de sécuriser les données transmises par les PEP, et la seconde de sécuriser la transmission des politiques du PDP vers les PEP.

Dans le premier cas de figure, les règles sont transmises aux PEP par l'intermédiaire du PDP. [12]spécifie un ensemble de classes pour configurer la politique IPsec sur des équipements ayant cette fonctionnalité. Les instances de ces classes sont virtuellement contenues dans une IPsec Policy Information Base (IPsec PIB). Le protocole COPS-PR est utilisé pour transmettre les informations contenues dans la IPsec PIB aux équipements adéquats (passerelles de sécurité, …). La sécurité mise en œuvre dans cette approche ne concerne que les données transmises par les PEP. De plus, cette politique ne peut être mise œuvre que chez des clients de type COPS-PR IPsec.

La deuxième approche sécurise la transmission des politiques du PDP vers les PEP. [11] préconise l'utilisation de COPS au dessus de **T**ransport **L**ayer **S**ecurity (TLS). Il standardise **S**ecure **S**ocket **L**ayer (SSL) et fournit plusieurs mécanismes de sécurité (unidirectionnel ou bidirectionnel) tels que l'authentification, les clefs de session dynamique, les flux de données privés et l'intégrité des données. La transmission de politiques de façon sécurisée implique l'authentification du PDP et des PEP. Cela est mis en œuvre par l'utilisation de certificats X.509 v3. La démarche de vérification est celle utilisée par **P**ublic **K**ey **I**nfrastructure (PKI).

2. Problèmes liés à la mobilité

Nous allons dans cette partie décrire les problèmes de mobilité du terminal et de l'usager ainsi que l'évolution des contraintes de QoS et de sécurité.

a) mobilité de l'usager et du terminal

Comme il a été vu précédemment dans cet article, on différencie essentiellement deux types de mobilité : la mobilité de l'utilisateur et celle du terminal. La mobilité de l'usager est soumise à certaines contraintes. Un usager ne peut utiliser ses services sans un terminal. Il doit donc y avoir une correspondance entre l'utilisateur et le terminal. Cela implique également que la mobilité d'un usager est réduite à la mobilité d'un terminal pendant l'utilisation d'un service. Pour se libérer de cette contrainte, l'usager devra changer de terminal. Or, d'un point de vue pratique, il est difficile pour un usager de changer de terminal en cours de communication.

De notre point de vue, la mobilité de l'usager ne doit être prise en compte que pendant la phase d'initialisation de la communication. C'est à ce moment que doit s'effectuer la correspondance entre l'usager et le terminal qu'il souhaite utiliser. Pendant la phase de communication, seule la mobilité du terminal sera prise en compte dans notre approche.

b) sécurité des usagers

Pour utiliser un service, un utilisateur doit d'abord s'y abonner. L'accès au service souscrit n'est possible qu'une fois que l'utilisateur s'est authentifié. Cette démarche permet à l'utilisateur de ne pas se faire usurper le service. Elle permet également au fournisseur de services de répertorier les utilisations de son abonné et d'évaluer le tarif de ses prestations.

Cette démarche soulève plusieurs problèmes. Le premier problème est celui du moyen d'identification. Il faut définir, pour chaque utilisateur, un identifiant unique et accessible depuis tous les points d'accès du réseau. Le deuxième problème est celui du stockage de l'identificateur. Pour éviter d'être protéger, cet identifiant doit se trouver sur un support portable et sûr. Ce support ne peut en aucun cas être le terminal car la mobilité de l'usager serait alors remise en cause. Le troisième problème est de sécuriser la procédure de communication. Un hacker peut écouter les transmissions et récupérer les informations nécessaires à l'authentification des usagers. Il aurait ainsi la possibilité d'utiliser les services en utilisant l'identité de l'usager espionné.

Dans le cas des réseaux mobiles, un problème supplémentaire apparaît lors des handoffs. Il est nécessaire d'effectuer une phase d'authentification à chaque changement de cellule.

c) QoS et mobilité

La QoS est un sujet de recherche très actif. Si beaucoup de travaux ont été réalisés dans les réseaux fixes, peu en revanche se placent dans le contexte d'un réseau mobile. Dans les réseaux fixes, sous le terme de QoS, sont regroupés quatre paramètres : la bande passante, la gigue, le taux d'erreur et le délai de transmission. Dans les réseaux mobiles, ces critères ne sont pas suffisants, on rajoute donc la perte de paquet due au handoff (changement de cellule) et la probabilité de blocage. Les besoins de QoS des usagers s'expriment sous forme de contraintes plus ou moins fortes sur ces paramètres.

Le principal inconvénient pour fournir de la QoS à l'heure actuelle, vient essentiellement de la difficulté d'administrer et de contrôler les ressources du réseau. En effet, pour garantir de la QoS, il est nécessaire d'avoir une connaissance de toutes les ressources du réseau afin d'être capable d'en réserver pour des applications prioritaires.

Lorsqu'on associe une QoS à un terminal ou application, on l'associe en général à son adresse IP. Cette association permet de localiser le terminal et de réserver les ressources réseau pour acheminer les données avec les contraintes de QoS requises de bout en bout. Cette démarche est tout à fait valide dans les réseaux fixes. Dans les réseaux mobiles, par contre, le déplacement du terminal provoque un changement d'adresse IP en effectuant un handoff entre deux réseaux distincts. Dans ce cas de figure, il faut alors mettre à jour la correspondance entre la QoS et l'adresse IP du mobile à chaque changement. Plus encore, lors d'un handoff, le mobile change de point d'accès au réseau, il faut donc réserver de nouvelles ressources satisfaisant aux contraintes de QoS spécifiées par le mobile et libérer les ressources inutiles. Si le nouveau réseau d'accueil du mobile ne peut le prendre en charge, il devra alors en être informé. Les applications nécessitant de fortes contraintes de QoS (les applications temps-réel par exemple) impliquent une faible durée de la phase d'initialisation lors d'un handoff.

3. Contribution

Dans cette partie nous présentons notre approche basée sur le protocole COPS. L'extension que nous proposons permet de gérer la mobilité ainsi que l'authentification et le maintient de la QoS lors du déplacement des usagers. Elle est divisée en trois sous-parties : la première présente les composants de notre approche ; la seconde notre mécanisme de prévention des handovers dans COPS et la troisième décrit notre approche pour satisfaire aux exigences de QoS dans un contexte mobile.

a) Composants de notre architecture

Notre approche répond aux besoins de QoS et authentification pour des usagers mobiles. Pour cela, nous avons intégré les composants **N**ext **F**oreign **P**olicy **D**ecision **P**oint (**NFPDP**), **N**ext **F**oreign **P**olicy **E**nforcement **P**oint (**NFPEP**) répondant aux besoins de mobilité et une carte à puce comme support d'authentification des usagers dans l'architecture de COPS-MIP. La Figure 5 présente note architecture.

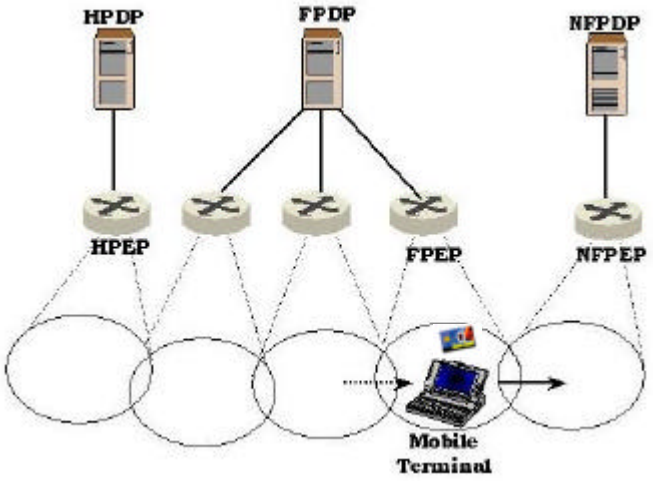

Figure 5: Composants de notre architecture

Examinons plus en détail les fonctions de chaque composant :

HPEP : Le PEP situé dans le réseau d'origine du terminal assure la fonction de Home Agent.
HPDP : Le serveur de politique du réseau d'origine du terminal qui est responsable de l'enregistrement du terminal.
FPEP : Le PEP situé dans le réseau étranger du terminal qui assure la fonction de Foreign Agent.
FPDP : Le serveur de politique du réseau étranger du terminal.
NFPEP : Le PEP situé dans le prochain réseau du terminal et qui assure la fonction de Next Foreign Agent.
NFPDP : Le serveur de politique du prochain réseau du terminal.
Carte à puce : Support sûr et fiable contenant l'identifiant de l'usager.
Mobile Terminal : Le terminal d'accès de services d'un usager en déplacement.

Dans la suite nous décrivons les différents composants de notre architecture, nous allons voir comment gérer de façon préventive les handoffs dans COPS.

b) La gestion préventive des handoffs dans COPS

Notre approche suggère une gestion préventive de l'enregistrement d'un mobile en déplacement. Nous considérons qu'il existe un PEP qui sert de station de base par cellule. Le mobile ne gère plus la phase d'enregistrement mais la délègue au NFPEP. Un PEP devient un NFPEP lorsqu'il détecte dans son voisinage un mobile qu'il ne gère pas. Il effectue alors les demandes d'enregistrement et d'authentification auprès de son NFPDP et du HPEP pour prendre en charge la gestion du mobile. Nous expliquerons plus en détail ces procédures dans la section suivante. Deux choix sont alors possibles. Le Next Foreign network peut gérer le mobile et effectuer la réservation de ressources ; ou, s'il ne peut le faire, il informe le mobile de son incapacité. Ainsi, lorsque celui-ci effectuera son handoff du HPEP au FPEP, sa connexion ne souffrira pas de la latence de l'enregistrement. La procédure est illustrée sur la Figure 6.

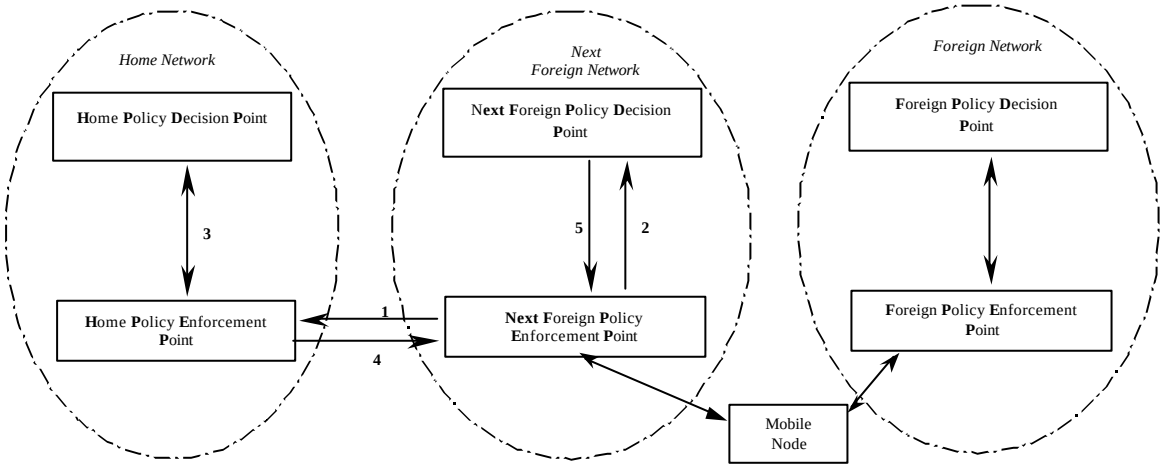

Figure 6 : Changement de réseaux d'un nœud mobile

Ce mécanisme de prévention des handoffs permet de réserver des ressources de façon préventive. Cette démarche supprime la possibilité de latence lors de la procédure de soft handover.

Nous avons préciser dans la section 2 que la mobilité de l'usager se réduisait à celle du terminal lorsque l'utilisateur utilise un service : c'est une mobilité de session. Lorsque l'usager désire changer de terminal, nous utilisons un mécanisme de correspondance : la carte à puce. C'est un support sûr , portable et fiable sur lequel on stocke l'identifiant de l'usager. Lorsqu'un usager se connecte à un nouveau terminal, la carte à puce permet à l'utilisateur de se faire identifier de façon unique sur le réseau.

c) La QoS dans COPS

Pour fournir de la QoS, il est nécessaire d'être capable d'administrer toutes les ressources du réseau. Le protocole COPS effectue, grâce au PDP, une gestion centralisée de tous les équipements du réseau (PEP). De ce fait, le PDP a une vue globale des ressources du réseau qu'il administre. On peut donc définir des règles de gestion, utilisées par le serveur de politiques, qui attribuent des priorités à des flux et réservent des ressources. Ces règles seront utilisées pour configurer les PEP par le serveur. C'est donc une architecture adaptée pour la gestion de la QoS.

L'association de la QoS à une adresse IP est très pratique pour déterminer la route que vont emprunter les données, et pouvoir plus facilement réserver les ressources. Dans les réseaux sans fil, l'adresse IP du mobile varie d'un réseau à l'autre. On ne peut donc plus associer la QoS à une adresse IP. Dans notre vision, nous stockons les paramètres de QoS sur la carte à puce. Il suffit alors de gérer une table de correspondance entre la carte à puce et sa localisation. Les caractéristiques de QoS étant stockées au niveau du terminal, les NFPDP sauront, dès son arrivée, s'ils ont la capacité de gérer les besoins de QoS requis par l'usager avant d'entrer en communication avec le HPDP.

Les applications nécessitant de fortes contraintes de QoS impliquent une faible durée pendant la phase d'initialisation au moment d'un handoff. Si ce temps de latence, dû à l'enregistrement du terminal et aux réservations de ressources du réseau, est trop important, alors la QoS sera dégradée. Notre solution basée sur la prévention des handoffs, remédie à ces problèmes.

La réservation de ressource est effectuée avec des minuteries. Pour maintenir la réservation, il envoie périodiquement des messages sur les équipements requis. Si les messages ne sont plus émis, les ressources sont libérées. Dans notre extension de COPS, le NFPDP se charge d'effectuer la réservation de ressource auprès des PEP. La tâche consistant à rafraîchir les réservations est déléguée au terminal, qui accomplit ce travail avec l'émission de données ou des messages de rafraîchissement si il n'a rien à émettre.

Si lors de son déplacement, le terminal mobile se trouve à proximité de plusieurs réseaux, tous les NFPEP des réseaux voisins font des demandes de ressources. Elles seront restituées lorsque le terminal ne sera plus à proximité.

d) La sécurité dans COPS

L'organe principal de la sécurité dans notre vision de COPS est la carte à puce. Nous allons détailler ses fonctions dans notre architecture.

Lorsqu'un utilisateur s'abonne à un service, il obtient un identifiant. Cet identifiant permet à l'utilisateur de pouvoir se faire authentifier auprès du fournisseur d'accès et ainsi d'utiliser le service souscrit. Pour éviter de se faire usurper cet identifiant, nous le stockons dans la carte à puce. Cette solution présente l'avantage pour l'utilisateur d'avoir des services indépendants du terminal et de pouvoir les transporter facilement. Si on place les informations d'authentification dans le terminal, on remet en cause la mobilité de l'usager et la confidentialité de l'identifiant. Lors d'un handoff, la ré-authentification de l'usager se fait de façon totalement transparente pour l'utilisateur comme le décrit la Figure 7.

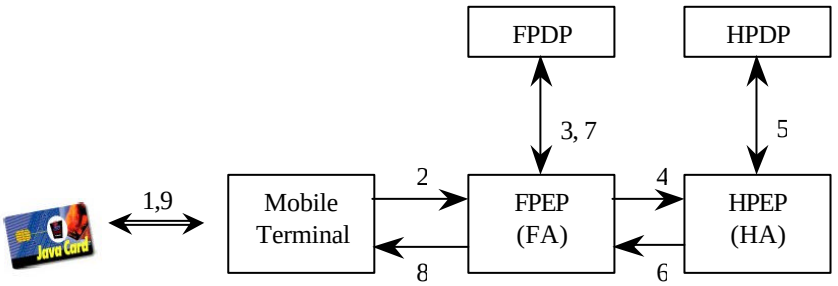

Figure 7: Enregistrement et authentification de l'utilisateur

Voici le détail de la procédure :

1 : La carte à puce fournit les informations d'authentification au **M**obile **T**erminal (MT).
2 : Le **M**obile **T**erminal (MT) envoie une requête d'enregistrement au **F**oreign **A**gent (FA).

3 : Le FPEP et le FPDP interagissent pour décider des politiques à appliquer sur la demande d'enregistrement.
4 : Le FA relaie la demande d'enregistrement du terminal au **H**ome **A**gent (HA).
5 : Le HPEP et le HPDP interagissent pour décider des politiques à appliquer sur la demande d'enregistrement.
6 : Le HA envoie la réponse d'enregistrement au FA.
7 : Le FPEP et le FPDP interagissent pour décider des politiques à appliquer sur la réponse d'enregistrement.
8 : Le FA fait suivre la réponse d'enregistrement au Mobile Terminal.
9 : La carte à puce vérifie si la réponse obtenue n'a pas été altérée depuis son émission.

On ajoute un mécanisme d'authentification de l'usager sur la carte à puce pour palier à des problèmes de vol ou de perte.

Le dernier point sur la sécurité concerne les échanges de messages entre l'utilisateur et le FPEP. Si un hacker réussit à obtenir le numéro d'identifiant d'un usager, il peut alors usurper son identité. Pour résoudre à ce problème, nous utilisons la carte à puce pour signer tous les messages que l'utilisateur émet. Le FPEP aura alors la possibilité d'authentifier les données émises par l'usager. Plus encore, le FPEP signe toutes les informations qu'il transmet. Donc, lorsque le terminal reçoit des messages d'un FPEP, la carte à puce vérifie leur intégrité.

Conclusion

Avec l'arrivée des futurs réseaux mobiles comme ceux de 4^{ième} génération, la QoS dans un contexte mobile semble promise à un bel avenir. Nous avons présenté dans cet article une proposition pour satisfaire une demande de QoS dans un réseau mobile. Après avoir énumérer les problèmes de QoS et de mobilité, nous avons montré la nécessité de mécanismes sécurisés pour la facturation de services mobiles nécessitant de la QoS. Nous proposons une extension du protocole COPS pour résoudre les problèmes énoncés. Nous avons utilisé pour la gestion de la mobilité et la sécurité des informations une carte à puce comme support de stockage. La validation de ce protocole est en cours d'implémentation sur un réseau sans fil 802.11.
Cet axe de recherche nous semble prometteur. C'est d'ailleurs dans ce sens que le projet MMQoS [15] converge. Dans nos futurs travaux, nous utiliserons pour la gestion de la sécurité sur carte à puce l'architecture SIM-IP.

Références

[1] Boyle, J., R. Cohen, D. Durham, S. Herzog, R. Raja, et A. Sastry, *The COPS (Common Open Policy Service) Protocol*, RFC 2748, Janvier 2000.

[2] Chan, K., J. Seligson, D. Durham, S. Gai, K. McCloghrie, S. Herzog, F. Reichmeyer, R. Yavathar, A. Smith, *COPS Usage for Policy Provisionning (COPS-PR)*, RFC 3084, Janvier 2000.

[3] S. Herzog, J. Boyle, R. Cohen, D. Durham, R. Rajan, A. Sastry, *COPS usage for RSVP*, RFC 2749, Janvier 2000.

[4] F. Reichmeyer, S. Wright, M. Gibson, *COPS usage for MPLS/TE*, draft-franr-mpls-cops-00.txt, Juillet 2000.

[5] T.M.T. Nguyen, G. Pujolle, N. Boukhatem, COPS Usage for SLS negotiation, draft-nguyen-rap-cops-sls-00, juin 2001.

[6] M. Jaseemuddin, A. Lakas, *COPS usage for Mobile IP*, draft-jaseem-rap-cops-mip-00.txt, Octobre 2000.

[7] A. T. Campbell, Gomez, J., Kim, S., Turanyi, Z., Wan, C-Y. and A, Valko *Comparison of IP Micro-Mobility Protocols*, IEEE Wireless Communications Magazine, Vol. 9, No. 1, February 2002

[8] C. E. Perkins, *Mobile Networking Through Mobile IP*, IEEE Internet Computing, January 1998.

[9] Andrew T. Campbell, Javier Gomez, Andras G. Valko, *An Overview of Cellular IP*, IEEE Wireless Communications and Networking Conference (WCNC'99), New Orleans, September 1999.

[10] R. Ramjee, T. La Porta, S. Thuel, K. Varadhan, L. Salgarelli, IP micro-mobility support using HAWAII, Internet Draft, draft-ietf-mobileip-hawaii-00, Work in progress, Mars 2000.

[11] J. Walker A. Kulkarni, *COPS over TLS*, draft-ietf-rap-cops-tls-02.txt.

[12] A. Doria, D. Arneson, J. Jason, C. Wang, M. Li, *IPsec Policy Information Base,* draft-ietf-ipsp-ipsecpib-03.txt.

[13] *Internet 3*, http://i3.prism.uvsq.fr.

[14] N. Boukhatem, B. Campedel, H. Chaouchi, V. Guyot, F. Krief, T. M. T. Nguyen, G. Pujolle, *I3- Une nouvelle génération intelligente de Réseaux IP*, GRES'01.

[15] *Maitrise de la mobilité et de la qualité de service dans la 4ème génération de mobiles*, http://mmqos.org.

[16] A. Fasbender, F. Reichert, E. Gueulen, J. Hjelm, T. Wierelemann, *Any Network, Any Terminal, Anywhere*, IEEE Personal Communications Journal, 1999.