Titre: Title:	History based anchor selection mechanism in hierarchical mobile IP
Auteur: Author:	Seyedeh Moloud Mousavi
Date:	2005
Type:	Mémoire ou thèse / Dissertation or Thesis
Référence: Citation:	Moloud Mousavi, S. (2005). History based anchor selection mechanism in hierarchical mobile IP [Master's thesis, École Polytechnique de Montréal]. PolyPublie. https://publications.polymtl.ca/7653/

UNIVERSITÉ DE MONTRÉAL

HISTORY BASED ANCHOR SELECTION MECHANISM IN HIERARCHICAL MOBILE IP

SEYEDEH MOLOUD MOUSAVI
DÉPARTEMENT DE GÉNIE INFORMATIQUE
ÉCOLE POLYTECHNIQUE DE MONTRÉAL

MÉMOIRE PRÉSENTÉ EN VUE DE L'OBTENTION
DU DIPLÔME DE MAÎTRISE ÈS SCIENCES APPLIQUÉES
(GÉNIE INFORMATIQUE)

NOVEMBRE 2005

Your file Votre référence
ISBN: 978-0-494-16821-9
Our file Notre référence
ISBN: 978-0-494-16821-9

UNIVERSITÉ DE MONTRÉAL

ÉCOLE POLYTECHNIQUE DE MONTRÉAL

Ce mémoire intitulé :

HISTORY BASED ANCHOR SELECTION MECHANISM IN HIERARCHICAL MOBILE IP

présenté par : MOUSAVI Seyedeh Moloud

en vue de l'obtention du diplôme de : Maîtrise ès sciences appliquées

a été dûment accepté par le jury d'examen composé de :

M. CHAMBERLAND Steven, Ph.D., président

M. QUINTERO Alejandro, Doct., membre et directeur de recherche

M. PIERRE Samuel, Ph.D., membre

ACKNOWLEDGEMENT

I would like to take the opportunity to thank people who guided and supported me during my study. First, I would like to thank my advisor, Dr. Alejandro Quintero. He has been so kind, patient and helpful whenever his guidance and assistant were needed. I am also grateful to Dr. Samuel Pierre who gave me the chance to be admitted for Master's studies. I have also been so fortunate to have support of my friends, Meral Shirazipour and Eva-Maria Garcia. Their suggestions and comments encouraged me a lot.

And at the end, I would like to express my sincere gratitude to my family specially my mother, and to my brother, Fariborz, for their forever emotional support, love and guidance. Without their encouragements, I could never be strong enough to overcome difficulties.

ABSTRACT

Domain oriented mobility management schemes like "Hierarchical Mobile IP" (HMIP) reduce the overwhelming binding updates signaling of a standard Mobile IP. A substitute of home agent, "Mobile Anchor Point" (MAP) in each domain of the network hides user's mobility from the "Home Agent" (HA). The MN informs its peers of its movement from the home network to a visitor network via a global "Binding Update" (BU) to HA and accordingly through a "Regional Binding Update" (RBU) to the anchor agent. Thus the signaling messages in macro aspect get reduced as long as the MN stays in a specific domain. But there are still many deficiencies associated with the structure itself. The standard hierarchical structure depends on a single MAP for all users of the domain without considering their mobility patterns. Consequently, the system has to fall back to the Mobile IP structure, if MAP functions improperly. To make it brief, system performance and reliability is under direct influence of the anchor choice. Moreover vague definition of domain's boundary and ignoring users' traffic behavior are among the most addressed problems. The objective of this research is to propose a new scheme which is built on top of the hierarchical architecture of HMIP. It tries to find for each individual mobile user its appropriate anchor point regarding its history of activities.

The idea of the scheme is based on three issues: micro mobility, dynamic aspect of the network and user mobility pattern. The anchors represent the resources which are requested by the MNs. The resource allocation problem, which in our case is selection of the best anchor, is a dynamic issue. In fact the roaming MNs with variable required service cause different situation in the network. Consequently the imposed load on the anchors can be considered as a time variant parameter. Moreover, an adaptive and dynamic view of the system takes into consideration the individuals' characteristic, accordingly resources can be shared efficiently and in an optimized manner. The movements in the network can be predicted using the fact that most subscribers have a

daily basis schedule. Based on their daily activities, the movements' pattern can be defined and some classifications are possible. Hence the system can behave for each category in respect to its properties and can save the signaling messages load, leading to the minimal cost. Therefore the proposed scheme takes into consideration the above mentioned issues.

The analytical model which functions based on the probability of the movement out of a domain, allows us to evaluate the scheme. The scheme has been compared with the conventional approach (centralized scheme) as well as the other two published models. The results demonstrate a definite improvement in respect to the centralized scheme, and promising regarding to the other compared schemes.

CONDENSÉ

Les réseaux d'accès mobiles de nouvelle génération (3G et plus) évoluent rapidement vers une définition de réseau entièrement IP (tout-IP). Ces réseaux, synonymes de services à valeur ajoutée, doivent offrir l'évolutivité requise pour satisfaire aux exigences du futur trafic IP en terme de nouveaux services multimédias et applications à temps réel, tout en assurant une gestion efficace de la mobilité des usagers.

Ce qui rend un réseau mobile avantageux sur le réseau fixé est la liberté pour l'utilisateur de bouger comme il le désire. Donc, pour fournir aux utilisateurs le service souhaité, le réseau devrait être informé du statut actuel de l'usager en ayant sa trace partout. Évidemment, une telle capacité provoque l'échange de plus de messages parmi les éléments de réseau. Pour maintenir la connexion IP existante, l'IP doit voir la même adresse du point de chaque noeud d'attachement, tandis que cela contredit la perception de noeud mobile. IP Mobile a été proposé pour implémenter la mobilité transparente dans le monde Internet.

Dans IP mobile, on permet qu'un MN ait deux adresses IP, une statique que l'on appelle "Home Address" et une dynamique, "Care of Address" (CoA), qui change chaque fois que le nœud mobil (MN) se promène et fait partie d'un nouveau point d'attachement. "Home Agent" (HA), un noeud de réseau origine, sera chargé d'intercepter le trafic entrant destiné au MN et de le livrer à son endroit actuel dans le réseau visité (Foreign Network). Le MN devrait informer son HA de son mouvement ou bien son nouveau CoA, donc le HA est capable de réexpédier les paquets de MN à son point actuel d'attachement. Par conséquent le HA transforme l'adresse de destination des paquets reçus au CoA d'un MN particulier et les réexpédie au réseau visité.

Avec la demande importante pour le trafic en temps réel comme la voix sur IP, la perte de paquet et la relève douce acquièrent une valeur significative. La latence de relève, un tournant dans le concept de mobilité, dépend de la latence de "Binding Update" (BU) ainsi que la latence de la connexion IP (en incluant la détection de

mouvement, la configuration d'adresse IP et la mise à jour de la localisation). De plus, la nature de liens sans fil implique des risques de sécurité inévitables. L'authentifiant BU garantit la sécurité d'opération de protocole de la piraterie, des attaques de reproduction et les messages simulés, ce qui prolonge à son tour la période de mise à jour.

Le protocole de gestion de IPv6 Mobile traite des chemins de routage entre un noeud mobile et les "Corresponding Node" (CN) via l'expédition de BU au HA et à tout CN avec lequel il communique. Il y a toujours quelques restrictions inhérentes aux optimisations de trajet. Les problèmes exposés dans le domaine de IP Mobile peuvent être considérés sous deux aspects, la gestion de mobilité macro et la gestion de mobilité micro. IP Mobile a été optimisé pour la mobilité macro et spécialement pour les hôtes qui bougent relativement lentement. Pour avoir localisé le domaine de réseau, la charge des signaux produite par la mise à jour de la localisation est restreinte et élimine ainsi l'élément de retard supplémentaire à partir de la période de relève critique de temps. Les usagers dans chaque domaine actualisent leur mouvement avec leur ancre de domaine. Ainsi l'ancre reprend de la responsabilité de HA pour sa propre région et cache le déplacement des nœuds mobiles du CN et du HA.

Quelques solutions ont été proposées dans la littérature comme IP cellulaire, HAWAII et IP Mobile Hiérarchique pour s'occuper de l'aspect de mobilité micro de IP Mobile et améliorer sa performance. Bien qu'HAWAII et IP Cellulaire soient de différentes approches, ils sont comparables à HMIPv6 qui est basé sur le concept de l'ancre. En considérant le cas particulier de HMIPv6 proposé par IETF, bien qu'il surpasse IPv6 Mobile dans le sujet de relève rapide par "Fast Mobile IPv6" (FMIPv6), quelques problèmes demeurent:

- L'architecture de réseau est centralisée, ce qui fait de l'ancre le seul point d'échec de l'architecture;
- La frontière des régions n'est pas facile à définir;
- Le comportement du trafic des usagers et le patron de mobilité ne sont pas fixés.

En bref, HMIPv6 qui propose un schéma rigide de la performance de système et de l'intégrité, est sous l'influence directe du choix de l'ancre.

L'objectif principal de ce travail est de proposer un schéma qui trouve le meilleur point d'ancrage dans la structure hiérarchique d'IP Mobile. En tenant compte des manques intrinsèques du protocole original, l'algorithme proposé doit diriger la mobilité dans le domaine micro et réduire la charge des signaux. La distribution (l'anticipation de tolérance de panne), l'aspect dynamique (la caractéristique de réseau en temps réel) et la qualité de service (la classification du trafic, le partage de ressource) sont parmi les paramètres les plus importants adressés dans la proposition conçue. Ainsi, les objectifs essentiels de la recherche sont les suivants:

- Présenter et analyser les problèmes existants, et les travaux y relatifs;
- Concevoir une nouvelle méthode pour résoudre les problèmes mentionnés concernant l'aspect de mobilité micro;
- Vérifier et évaluer la performance de la nouvelle méthode proposée;
- Comparer le schéma proposé avec ceux qui existent déjà bien que la base soit la structure hiérarchique conventionnelle et à observer si une modification positive a été faite.

L'idée du schéma proposé est fondée sur trois sujets: la mobilité micro, l'aspect dynamique du réseau et le patron de mobilité de l'utilisateur. Le but dans le schéma de gestion de mobilité orienté domaine est la réduction de mises à jour écrasantes dans une gestion de mobilité d'IP standard. L'idée fondamentale de gestion de mobilité localisée est basée sur le remplacement de HA par un nouvel équipement que l'on appelle l'agent d'ancrage. De plus, le MN informe ses pairs de son mouvement du réseau principal vers un réseau de visiteur, via BU global au HA et en conséquence par un "Regional Binding Update" RBU à l'agent d'ancrage.

L'aspect dynamique du réseau est considéré comme un des points essentiels de cette recherche et son effet (surtout la complexité) sur le système est lui aussi pris en compte. Les ancres représentent les ressources qui sont demandées par les MNs. Particulièrement deux éléments relèvent du problème d'allocation de ressource, qui dans notre cas constitue la sélection de la meilleure ancre. Le premier élément est la charge sur les ancres qui est un paramètre variable dans le temps. Deuxièmement, les MNs se

promenant avec le service variable requis provoquent différentes situations dans le réseau. Il devrait être encore notifié que les changements inattendus dans l'environnement ou des directives globales modifiées provoqueront des re-calculs dynamiques et des modifications sur le comportement de l'ancre.

L'ancre individuelle, par rapport à sa responsabilité peut réaliser la tâche spécifiée et/ou accepter la charge d'expédition superflue et changer l'état de routage pour minimiser la probabilité de panne. Ainsi les ancres communiquent entre elles via les communications bilatérales pour compenser les déficiences et établir un système tolérant de panne. En conséquence, quelques liens de dépendance sont dynamiquement créés entre eux et les algorithmes de contrôle et de supervision assurent que ces dépendances ne se mêleront pas de l'accomplissement des objectifs. En bref, le partage des ressources et de l'allocation, l'exécution de la tâche et la planification correspondent aux contraintes du problème et aux objectifs.

Les mouvements dans le réseau peuvent être prédits en utilisant le fait que la plupart des abonnés ont un programme de base quotidien. Basé sur leurs activités quotidiennes, le patron des mouvements peut être défini et quelques classifications sont possibles. Par exemple un utilisateur de la classe ouvrière part à la maison à une certaine période le matin, fait ses travaux à certains endroits au cours de la journée et revient à la maison. Ainsi, les routeurs d'accès visitées restent les mêmes dans la vie quotidienne. De plus, les services demandés sont d'une manière ou d'une autre les mêmes. Dorénavant le système peut se comporter pour chaque catégorie dans le respect de ses propriétés et peut sauver la charge des signaux, au moindre coût. Un modèle d'utilisateur simple ou un ensemble d'utilisateurs groupés selon certains paramètres comme le taux d'arrivée des appels et le patron de mobilité peut être définis pour analyser la situation.

Afin de prévoir de façon précise le mouvement des usagers, deux types d'informations pourraient être collectées dans le réseau:

1. L'observation à long terme d'une activité d'utilisateur qui représente des changements lents au cours des mois ou des semaines;

2. Les activités de moyen ou court terme qui représentent le dernier comportement des utilisateurs, conduisant à plus d'exigence de mémoire et à l'augmentation de coût par profil d'utilisateur.

Le schéma traite de la gestion de mobilité par deux phases: le processus d'apprentissage de patron de mobilité et du protocole basé sur le profil qui est construit à partir des données obtenues auparavant. Ces phases sont réalisées en considérant les points ci-dessous mentionnés:

- Le MN devrait sauvegarder ses propres renseignements, afin de réduire la charge des signaux résultant de la trace des utilisateurs dans le réseau. Par conséquent l'exactitude et la résolution des données sont plus garanties. L'intervalle de répétition du patron de mobilité est considéré pour 24 heures (la période quotidienne). Le modèle d'apprentissage devrait être capable de découvrir la régularité de mouvements et construire une table d'ensemble des routeurs d'accès visités basés sur un temps quotidien. Aussitôt que le modèle découvre la stabilité dans les mouvements, alors le patron de mobilité est conçu et prêt à prévoir la meilleur ancre;
- Dans la phase d'apprentissage, le routeur d'accès observe sa capacité et les services demandés par les utilisateurs et aide le MN à se décider pour l'ancre la plus convenable. Le protocole profite du patron construit de lors la période d'apprentissage.

Ici le schéma ne passe pas par le détail de phase d'apprentissage. Quelques spécifications et les renseignements attendus à ce stade sont discutés.

Nous supposons que chaque région de service est divisée en cellules qui sont servies par les stations de base. Une agrégation d'un certain nombre de cellules dans lesquelles un utilisateur individuel bouge, forme un sous-réseau servi par un routeur d'accès. Un domaine est constitué de nombreux sous-réseaux. Pour chaque domaine, un point d'ancrage garde l'adresse et les autres renseignements pertinents concernant les utilisateurs qui résident dans sa région de charge. Le HA à son tour sauvegarde l'adresse de points servant d'ancrage pour chacun des utilisateurs (en fait la première ancre de la

chaîne est l'adresse de référence). Le MN continue à surveiller le signal de balise d'avertissement d'agent pour découvrir les routeurs d'accès et voir s'il est applicable à leur capacité. Comme MN change les routeurs d'accès, il s'actualise avec le nouveau routeur d'accès en service. Ensuite il enregistre l'adresse nouvellement obtenue avec son point d'ancre en service. Les aspects de la sécurité "Authentification, Autorisation and Accounting" (AAA) peuvent considérés à cette étape aussi.

Apparemment, la distribution de probabilité de l'activité de chaque utilisateur n'est pas uniforme durant la période d'observation. Pour fournir une vue meilleure et plus précise du patron de mobilité individuelle, deux dimensions sont considérées. La première dimension définit le profil d'utilisateur dans une approche presque déterministe comme le jour ouvrable, le jour férié et le week-end. La deuxième dimension suit le comportement de mobilité dans différents intervalles de temps pendant une journée.

Nous discutons du schéma proposé à partir de deux différents points de vue : la partie concernant l'utilisateur et la partie concernant l'équipement de réseau (le routeur d'accès).

Chaque utilisateur garde la trace et la QdS offerte par les routeurs d'accès et construit le patron. Finalement le modèle d'apprentissage établit une table dans laquelle les champs sont la période de temps considérée (intervalle de 24 heures), les deux ensembles de routeurs d'accès visités attendus dans chaque période spécifique, la probabilité de visiter chaque ensemble de routeurs d'accès, la QdS demandée par l'utilisateur dans chaque période et finalement l'ancre la meilleure parmi les routeurs d'accès visités. En conséquence après la collecte de renseignements sur l'utilisateur et la connaissance de ses habitudes, dès qu'il s'inscrit dans le réseau, en partant de son histoire, la meilleure ancre pour chaque période est connue au MN et il peut envoyer le message de mise à jour à l'ancre.

Concernant les ancres qui sont fondamentalement des routeurs d'accès, le paramètre important qui devrait être considéré est la capacité d'élément de réseau, et si elles peuvent prendre en main un nouvel utilisateur, en répondant à la QdS requise. Aussi longtemps que l'utilisateur conserve ses habitudes, l'ancre convenable de chaque

période est connue. Pour affaiblir la charge du signal au HA, la première ancre pourrait établir une chaîne vers les suivants. Un paquet entrant est envoyé du HA à la première ancre et suit la chaîne pour arriver à l'utilisateur. Un routeur d'accès enregistre la QdS demandée par l'utilisateur et la charge imposée dans un intervalle de choix du moment prédéterminé. Donc, il monte une table qui sauvegarde le résultat provenant de son activité. Les champs de cette table sont l'intervalle de temps dans lequel l'observation a été faite, la QdS demandée, la charge d'unité centrale et le nombre d'utilisateurs en service.

Comme il a été discuté auparavant, un paramètre de QdS (demandé, offert) fixé dans les messages d'échange d'enregistrement s'éclaircit si le routeur d'accès peut être un ancre de candidat, ou non. Mais le problème survient en considérant le fait que le routeur d'accès devrait être autorisé pour toute la période (le domaine) et non uniquement pendant le temps d'enregistrement. Donc le routeur d'accès devrait informer le MN de sa capacité pour ce domaine spécifique et pratiquement réserver la QdS promise pour l'intervalle de temps choisi. Autrement, la durée de vie détermine la période de validité de la capacité du routeur d'accès.

La question essentielle réside dans la façon de définir la période d'observation et la période convenable de MN. La façon de modéliser le moment où le MN passe d'un domaine à l'autre est fondée sur un travail déjà fait dans le domaine de "Personal Communications Service" (PCS). Cependant dans l'article mentionné, la charge sur l'équipement de réseau n'a pas été comptée. Pour définir la limite de chaque ancre, nous considérons :

- Le traitement de la charge sur chaque ancre: s'il excède le seuil prédéfini, et le prix de passage à l'ancre suivante inférieur à la charge imposée par le traitement ;
- Le temps de résidence dans le sous-réseau inscrit: si un MN demeure en quelque part plus que le temps moyen de résidence, le domaine sera terminé avec le sous-réseau mentionné. La valeur de seuil est définie par rapport à l'histoire de chaque utilisateur et est dorénavant unique à chaque utilisateur;

- Le taux d'arrivée d'appel: puisque le changement de domaine provoque une relève inter domaine au milieu de la durée d'appel, dorénavant ce serait mieux pour le MN d'être dans un état neutre avant la transition d'une ancre à la suivante.

Ainsi la chance qu'un MN bouge de son domaine régional d'après les paramètres mentionnés sera définie.

Chaque fois que MN change de sous-réseau, premièrement il inscrit son nouvel "Local Care of Address" (LCoA) dans l'ancre. Par conséquent l'ancre connait l'endroit précis où est localisé le MN et transmet le paquet directement à sa destination. Ce qui est obligatoire dans le cas des applications qui sont sensibles au délai, puis qu'il augmente la charge des signaux locaux. Autrement l'ancre peut juste garder des renseignements de localisation approximative du MN dans son domaine, cela signifie que le MN actualise avec l'ancre une fois quand il entre dans le domaine. Pour livrer un paquet adressé à un tel MN, l'ancre doit rechercher partout dans le domaine. Évidemment une telle option peut être plutôt proposée pour les applications où le temps réel n'est pas exigeant.

Dorénavant, selon la QdS désirée par le MN, ce dernier et l'ancre peuvent déduire si la pagination devrait être appliquée pour cet intervalle de temps donné. Mais pour être capable d'appliquer une telle stratégie, le MN devrait demander le même service dans les sous-réseaux entiers du domaine.

Dans le schéma proposé, l'échange des signaux reste essentiellement le même, sauf que chaque fois que l'utilisateur s'inscrit avec le routeur d'accès local, il négocie le service demandé pour vérifier si le routeur d'accès peut être son ancre convenable dans le future. La phase de négociation de QdS peut être implantée dans le message de l'enregistrement dans lequel le MN exige un type de QdS nécessaire et en réponse il reçoit la capacité de l'AR en fonction de l'offre du type de QdS.

Nous calculons la fonction de prix du schéma proposé à travers le développement d'un modèle analytique. Comme les autres travaux dans ce sujet, les mises à jour périodiques envoyées par un MN à son HA ou AR ne sont pas prise en compte. Il faut signaler que les calculs de prix sont valides juste pour un cas d'utilisateur individuel, puisque le patron de mouvement des abonnés est complètement indépendant.

Les métriques de performance considérées pour le prix total des signaux est la mise à jour de la localisation et la livraison de paquet. Le modèle analytique du schéma est comparé à deux propositions relativement semblables. La raison pour laquelle ces schémas-là sont choisis est qu'ils sont bien connus dans la littérature et sont basés sur l'analyse mathématique. De plus le schéma est comparé avec le concept général de la structure d'enregistrement régionale d'IP Mobile. Dans un système centralisé le domaine ne change jamais, peu importe comment les utilisateurs spécifiques se promènent et il reste le même dans toutes les conditions. L'autre propriété d'un tel système est que seule une ancre simple est responsable du domaine.

D'ailleurs, le schéma a été analysé et vérifié par une boîte à outils pour la validation et la vérification de systèmes en temps réel. La vérification formelle de protocoles passe par différents stades:

- La modernisation du système: une description du système;
- La définition des propriétés du système: les caractéristiques du system;
- Vérification: si un modèle correspond aux propriétés du système et aux contraintes.

Dans notre cas, le modèle du système est fondé sur les transitions dans lesquelles un processus commence d'un état initial et passe par les étapes intermédiaires. Un modèle d'automate chronométré, la boîte à outils vérifiante UPPAAL, est choisi pour vérifier la validité du modèle proposé.

"QoS binding", "QoS paging", et le mécanisme d'ajustement d'ancrage sont les cas qui ont été modelés et vérifiés. Les propriétés classiques qui sont d'habitude vérifiées sont: la sûreté, la vivacité, l'accessibilité et l'absence de blocage. La sûreté assure qu'aucune anomalie inattendue n'arrivera dans le système. La vivacité suppose que sous certaines conditions, le système devrait arriver à un état spécifique. Par exemple, cette propriété peut être utilisée pour vérifier si le système est capable de répondre dans un temps fini. Évidemment, l'accessibilité vérifie si une situation est accessible ou non. Finalement le système devrait être libre de tout blocage.

Les résultats montrent une amélioration importante par rapport au schéma centralisé et prometteuse par rapport à d'autre schémas.

Nous avons visé l'amélioration de la structure hiérarchique traditionnelle d'IP Mobile et les résultats analytiques semblent raisonnables et prometteurs. Mais nous avons observé quelques difficultés qui constituent des limites à notre travail. D'abord, le schéma est fondé sur l'histoire de chaque utilisateur qui n'est pas en réalité exécutée. Dorénavant nous entrons dans un monde inconnu, dont les déficiences affectent directement la performance de notre modèle. Deuxièmement, l'aspect de sécurité et la confidentialité des données relatives aux utilisateurs imposent des fardeaux. Le client devrait être assuré que sa vie privée ne sera jamais manipulée.

L'implémentation du projet à partir d'un instrument de simulation et une mise à l'essai de son efficacité dans un environnement réel de la collaboration avec un opérateur peut constituer la prochaine étape de ce travail.

TABLE OF CONTENTS

TABLE OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

AR	Access Router
CAP	Candidate Anchor Point
CAR	Candidate Access Router
DAD	Duplicate Address Detection
DMA	Domain Mobility Agent
FBACK	Fast Binding Update Acknowledgement
FBU	Fast Binding Update
FNA	Fast Neighbor Advertisement
GFA	Gateway Foreign Agent
HACK	Handover Acknowledge
HLR	Home Location Register
HI	Handover Initiate
ICMPv6	Internet Control Message Protocol Version 6
LCoA	Local Care-Of-Address
MA	Mobility Agent
MAP	Mobile Anchor Point
MCoA	Multicast Care of Address
MMD	Micro Mobility Domain
MSS	Mobile Service Station
NAR	New Access Router
PAR	Previous Access Router
RCoA	Regional Care-Of-Address
PrRtAdv	Proxy Router Advertisement
RtSolPr	Router Solicitation for Proxy
SA	Subnet Agent
UDP	User Datagram Protocol

CHAPTER I

INTRODUCTION

"Internet Protocol" (IP) convergence shapes the future of communications. But with the deployment of all-IP network, more problems should be solved. With evolution in mobile service through IP connectivity, handhelds, and digital cellular phones are offering more than basic voice service. What makes a mobile network advantageous over the fixed network is the user freedom to move wherever he likes. Therefore to deliver the required service to the users, the network should be informed about the current status of the user via tracing him everywhere. Obviously such ability causes the exchange of more signaling messages among the network elements. To maintain the existing IP connection, the IP needs to see the same address for each node's point of attachment, while this contradicts the perception of mobile node. Mobile IP was proposed to implement the transparent mobility in the Internet world. Mobile networking, the dream of yesterday and the reality of today, have some technical obstacles in its way to be popular in the world. This work follows the objective of optimization in mobility management of Mobile IP. Basic concepts of Mobile IP will be discussed first, and then it continues with introducing of some existing problems in this domain which give the idea of research, its objectives and at the end the plan of research will be presented.

1.1 Basic definitions and conceptions

We define in advance some phrases in mobile IP network, which clear the vague points and help to follow the succeeding chapters easily.

Home Agent (HA), a router on a mobile node's (MN) home network that tunnels packets to the mobile node while it is away from home. It keeps current location information for registered mobile nodes through *mobility binding*.

Home address, an IP address that is assigned for an extended time to a mobile node. It remains unchanged regardless of node's current point of attachment.

Care-of Address (CoA), whenever an MN visits a foreign network, it obtains a new address which identifies its new point of attachment.

Correspondent Node (CN), an MN's communication peer. A correspondent node may be either stationary or mobile.

Binding update (BU), a binding update informs the relevant entities of a mobile node's new CoA. The binding update contains the Mobile Node's home address, new CoA, and a new registration lifetime.

Registration, the process by which the mobile node informs its care-of address to the Home Agent while it is away from home. Registration may happen directly from the mobile node to the Home Agent or through a Foreign Agent.

Tunnel, the path followed by a packet while it is encapsulated from the Home Agent to the mobile node. The model is that, while it is encapsulated, a packet is routed to a knowledgeable decapsulating agent, which decapsulates the datagram and then correctly delivers it to its ultimate destination.

Handover (HO), the process of changing from one access point to the other one. Whenever an MN changes its radio access point but stays in the same network, the handover is the layer 2 handover. In case of layer 3 handover, the MN changes the network as well; consequently it has to obtain a new IP address. Hence due to the necessary signaling exchange, the MN suffers service interruption, so called *HO latency* in its communication.

Mobility Management (MM) covers protocol and resource reservation schemes for mobile terminals with certain mobility. In a composite radio environment, the MM needs to consider: registration/paging in the switching subsystem, resource reservation and management in the radio subsystem.

Macro Mobility, communication across different administrative domains, in which HA receives signals known as "Binding Updates" (BUs).

Micro Mobility, communication limited to a single administrative domain in which a substitute of HA (Gateway Agent) receives the signals known as "Regional Binding Updates" (RBUs).

A mobile node is supposed to maintain the existing communications while changing its point of attachment. According to the nature of Internet Protocol, the IP address should be the same during the whole communication, which cause a dilemma in mobile connectivity. A node in movement has to change its IP address, which in turn terminates the on-going sessions while the nomadic user seeks for convenience of seamless roaming. Mobile IP is a solution for heterogeneous and homogenous mobility. In mobile IP, an MN is allowed to have two IP addresses, a static one which is called home address and a dynamic one, CoA which changes whenever the MN roams and attaches to a new point of attachment. The HA, a network node in the home network, will be responsible to intercept the incoming traffic destined for the MN, and delivers them to its current location in "Foreign Network". The mobile should inform its home agent of its movement and its new care of address, hence home agent is able to redirect MN's packets to its current point of attachment. Consequently the home agent transforms the received packets' destination address to the mobile care of address, and redirects them to mobile visiting network. MN and CN can communicate via different ways in Mobile IP. Below they are discussed.

- Mobile IP with triangular routing

MN initiates communications with CN on the Internet by sending a packet which has its home address as sender address. Obviously with routing protocol, the CN replies a packet back to the sender address which is MN's home address. The HA encapsulates the intercepted packet and inserts MN's care of address as the destination address, and establish a tunnel to the FA. The FA ignores the tunnel header and directs the rest to MN. Triangular routing is not an optimum implementation of Mobile IP (see figure1.1).

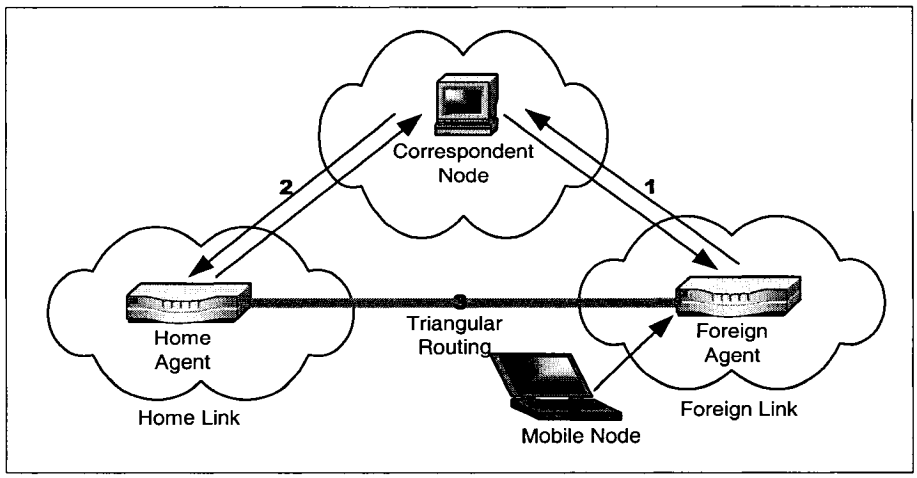


Figure 1.1 Triangular routing in Mobile IP

- Mobile IP with optimized (reverse) routing

If the MN directly informs its current care of address either to its HA and CN, then the CN will be able to deliver the packets destined to MN without HA intervene. Comparing with triangular routing, in which the binding information is in HA, the optimized routing generates security risks and administration difficulties (see figure 1.2).

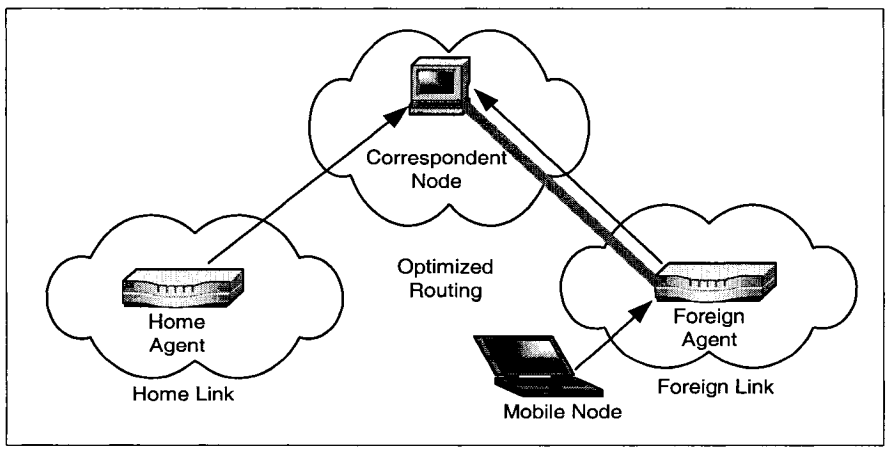


Figure 1.2 Optimized routing in Mobile IP

- Mobile IP with collocated care-of address

With elimination of FA, the MN new care of address will be provided by a DHCP. Consequently the MN has to extracts the encapsulated packet coming from HA (see figure 1.3).

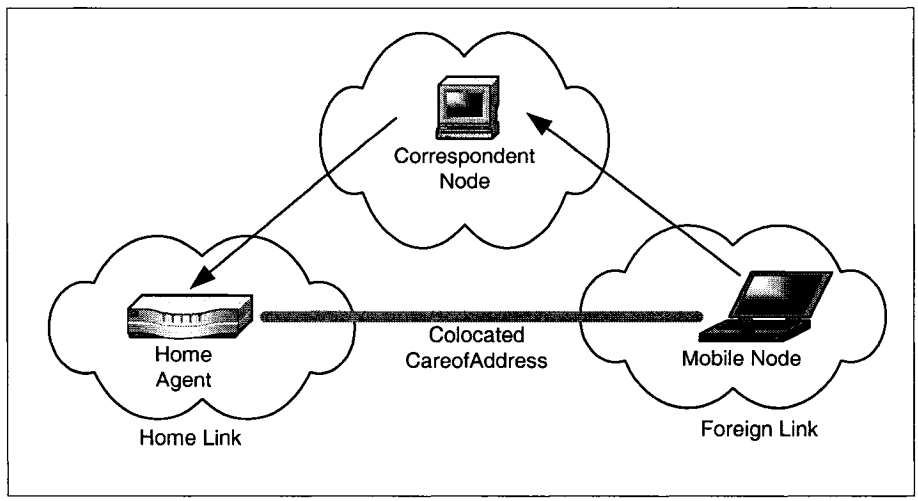


Figure 1.3 Collocates care of address in Mobile IP

1.2 Elements of problems

With overwhelming demand for real time traffics such as voice over IP, packet loss and smooth handover get a significant value. Handover Latency, a turning point in mobility concept, depends on the "Binding Update" (BU) latency along with IP connectivity latency (including movement detection, IP address configuration, and location update). Moreover, the nature of wireless links implies inevitable security risks. Authenticating BU ensures the security of protocol operation from hijacking, active replay attacks, and bogus messages, which in turn prolongs the updating period.

The Mobile IPv6 mobility management protocol deals with routing paths between a mobile node and the correspondent nodes via sending BU to the HA, and to the all CNs it communicates with. There are still some limitations inherent in route

optimizations. The facing problems in Mobile IP can be considered in two aspects: Macro Mobility Management, and Micro Mobility Management.

The mobile IP has been optimized for macro mobility and relatively slow moving mobile hosts. By having localized domain, the signaling load produced by location update is restricted thus eliminates the additional delay element from the time-critical handover period. Users in each domain update his movement with its domain gateway. Thus the gateway takes over the responsibility of HA for its own region and hides mobiles location from CN and HA while using mobile IPv6 route optimization.

Some solutions in literature like cellular IP [4], HAWAII [5] and Hierarchical Mobile IP [6] were proposed to deal with micro mobility aspect of mobile IP and to enhance its performance; though HAWAII and Cellular IP are different approaches comparing to HMIPv6 which is a gateway centric scheme.

Considering a particular case of HMIPv6 proposed by IETF, even though it outperforms mobile IPv6 in fast handover issues, but still it has some problems:

- The network architecture is centralized, which makes the gateway the single point of failure of the architecture;
- The regions' boundary is not easy to define;
- Users' traffic behavior and mobility pattern is not fixed, while HMIPv6 is a rigid scheme.

To make it brief, system performance and reliability is under straight influence of the gateway choice.

1.3 Research objectives

The main objective of this work is to propose a scheme which finds the best anchor point in the hierarchical structure of Mobile IP. Taking into account the intrinsic deficiencies of original protocol, the novel algorithm is to manage mobility in micro based domain and reduce signaling load. Distribution (fault tolerance anticipation), dynamic aspect (real time network characteristic), and quality of service (traffic

classification, resource sharing) are among the most important issues addressed in devised proposal. To enumerate the gist of research objectives, it:

- Presents and analyses the existing problems and the proposed solutions and related work;
- Designs a new method to solve the mentioned problems in micro mobility aspect;
- Verifies and evaluates the performance of the new proposed method;
- Compares the proposed scheme with the existing ones (though the base is conventional hierarchical structure) to observe if any positive modification has been done.

1.4 Research plan

Second chapter will analyze the different methods of related work. The third chapter proposes the new strategy of management of mobility in MIPv6. The fourth chapter verifies the new idea and analyzes the result. Finally, the last chapter will sum up the steps taken, the burdens and limits, and indicates the path of future work.

CHAPTER II

DYNAMIC-DISTRIBUTED SYSTEM

The ever increasing demand for mobile communications makes it important to eliminate its existing deficiencies and to improve its performance. Being mobile means the user should have the ability to be omnipresent, ideally, and maintains his connectivity while roaming among different networks. The point is being able to resume the ongoing connection with acceptable delay. In rough definition, a set of techniques to find mobile user's current point of attachment in the network means mobility management.

Since IP protocol has the capability to make an optimized converged network out of nowadays heterogonous network, it also attracts more and more attention in mobile communications. Standardized Mobile IP by IETF was the very first solution to mobility problem in IP world. Though basically it provides a transparent connection to all executing applications, it still suffers many lacks. Through the years mobile IP improved in many aspects, from triangular routing to optimized one, and more enhancement brought by its new version, "Mobile IPv6" (MIPv6). With Mobile IPv6, there is no need to have foreign agents in visited network, besides that binding updates from the mobiles are also directly destined to CN to keep them informed without HA intervene; thereby it results in having less signaling load in the network. Lots of article have been presented to improve different aspect of Mobile IP's deficiencies like high latency during its location update (registration), which consequently generates long delays in handovers (The ideal is fast, seamless handover), and lack of quality of service provisioning which renders the protocol paralyzed for real time applications.

Here after a short reintroduction to MIP, we discuss some of the most frequently addressed micro mobility protocols in literature in the next five sections. Next a comparison between some popular micro mobility protocols is made. And finally the

rest of the chapter is focused on some of the most relevant schemes which consider the dynamic and distributed aspect of micro mobility subject.

2.1 Basic mobile IP and micro mobility extension

As it mentioned earlier in the first chapter, the home network assigns a permanent IPv6 address (home address) to each belonging MN. While the user visits a foreign network, it attains a temporary IP care of address which represents its current point of attachment. The binding process which is the association of the home address with the user's CoA makes the MN reachable for HA. Hence the user should inform its new CoA to the HA whenever the visiting access router (AR) is changed. The peer node, CN, forwards the packet to MN's home address. HA in its turn intercepts incoming packets destined for MN, and encapsulate the packets to the MN's CoA.

Domain based mobility management aims to reduce the binding update and packet delivery delay [18]. The idea is to limit the signaling messages locally within the domain; hence the user's movement in domain is hidden to HA (see figure 2.1).

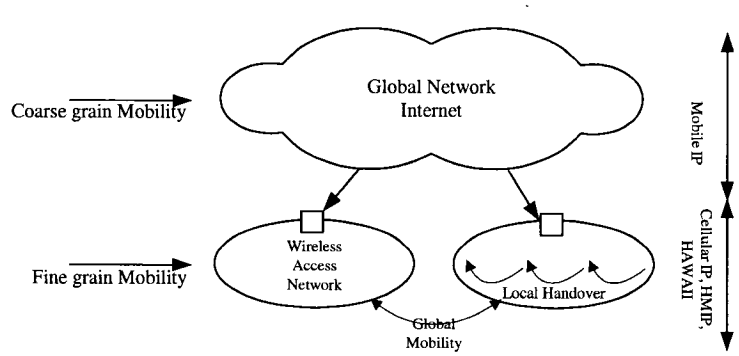


Figure 2.1 Micro mobility versus macro mobility

The MN is known by two addresses: "Local CoA" (LCoA), which addresses the MN's current AR, and "Regional CoA" (RCoA), which relates it with the domain's gateway.

According to [5] there are two types of micro mobility protocol: tunneled based and routing based scheme. Mobile IP regional registration and "General Packet Radio System (GPRS) Tunneling Protocol" (GTP) are tunnel-based schemes, in which a

"Gateway Foreign Agent" (GFA) builds a hierarchical mobility structure. HAWAII [5] and "Cellular IP" (CIP) [4], the routing based schemes use conventional IP forwarding in micro mobility domain. The common point of all these protocols is to enhance micro mobility vision of Mobile IP and to handle its intrinsic pitfalls. Unfortunately all described protocols are susceptible to the HA or GFA failure. As it is recommended in literature, the usual solution proposed in [4] and [5] is either application of a dynamically assigned home agent, and having redundancy, which consequently renders the HA robust to failures [3].

2.2 Hierarchical Mobile IPv6 (HMIPv6)

Mobile IP maintains the ongoing session between MN and CN via sending binding updates from roaming MN to HA and CNs. Authenticating procedure of binding updates between the MN and each CN is time consuming which requires nearly 1.5 round trip times. Moreover the HA update time which is one round trip should also be added to the above mentioned time (though it can be done simultaneously with CN update). Consequently such a mechanism causes service disruption during handover and the mobile IP performance decreases due to such mobility signaling and its following delay.

2.2.1 HMIPv6 overview

Hierarchical Mobile IP [6] as an extension to Mobile IP adds a strategic node, Mobile Anchor Point, which localize the mobility signaling to a specific region and functions as a local HA in its domain. Not merely does such a hierarchical mobility management reduces the signaling load but also attains seamless mobility through Fast Mobile IPv6 handover. Two simplistic view of HMIPv6 structures are shown in figure 2.2 and 2.3.

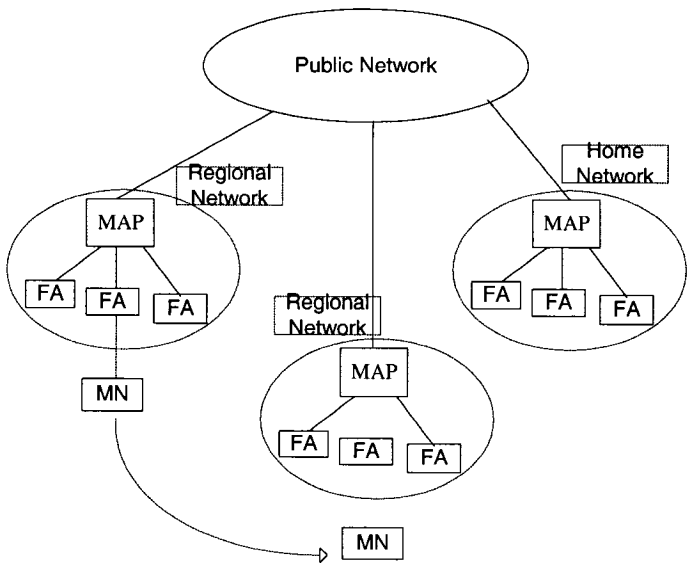


Figure 2.2 IETF regional registration [19]

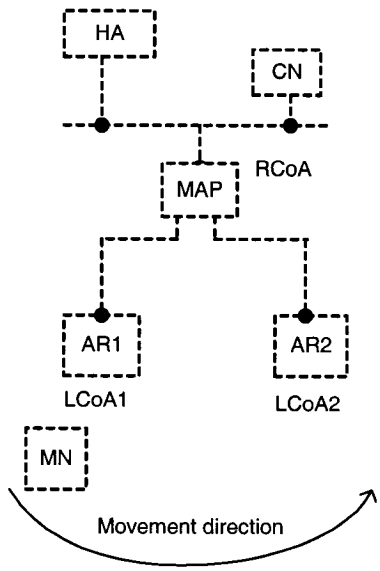


Figure 2.3 HIMPv6 schematic view [6]

The MAP can be placed in any level of hierarchical structure of network, and should serve an optimized number of subnets. Therefore the MAP role can be distinguished in the following way:

- Binding updates are sent from MN directly to MAP rather than HA and all CNs, meaning that MN's exact position is hidden from outer region;
- One and just one update message is sent from MN to MAP.

In the first place, the MN receives the local MAP's "Router Advertisement" (RA) message containing some needed information on its existence. Next, the MN binds its Local CoA, with an address of the MAP's subnet, RCoA. Accordingly the MAP takes the responsibility of local HA for the registered MN in the region and the incoming packets for MN will be intercepted by MAP and then tunneled to MN's corresponding AR. Therefore whenever MN roams in MAP's domain, there is no need to inform the HA or CNs, it only requires the new address registration with the MAP.

The MN discovers the global address of a MAP through the received RA, since this address is saved in RA messages. The above mentioned mechanism is called MAP discovery and it continues as MN moves from one subnet to the other one. After every movement, MN checks whether it is still in the same MAP domain. If any alteration in the advertised MAP's address is found, then the MN should register its new RCoA with HA. To trace the MN, the MAP saves the MN's LCoA in its binding cash during registration process. Thus the MN's movement as long as it wanders in the region will be transparent to HA and CNs.

2.2.2 HMIPv6 discussion

There are some concerns about HMIPv6. The MN should be able to detect HMIPv6 in the region which is MAP discovery phase. Moreover the decision whether to register with MAP or to be connected directly to the HA affects protocol performance.

The Achilles' heel of HMIPv6 is its MAP too, since it creates a single point of failure in the network, and turns to be a bottleneck in the public network. Thus it reduces the quality of service. In addition as it mentioned in literature [5], though hierarchical mobile structure eases seamless handover, the main deficiency with such a scheme remains its lack of flexibility and its rigid structure. Size optimization of each domain

means a lot, since in the case of inter region handover the increased signaling load impacts the performance even more.

2.3 Fast Mobile IPv6 handover

To compensate the delay generated by Mobile IPv6 mechanism which consists of movement detection, new CoA assignment, and binding update, a new protocol was devised. Fast Mobile IPv6 [11] is to improve the handover delay and subsequently renders Mobile IPv6 an efficient protocol for real-time traffic such as voice over IP, and also for throughput sensitive application. The idea behind fast handover is to provision layer 3 handover occurrences and forward the packets to MN's new location in advance.

As soon as the MN handovers to new subnet link and is IP-capable, it sends a binding update to HA and the involved CNs. After successful binding updates with the correspondents which is called Return Routability Procedure, the MN will be able to receive new packets.

2.3.1 FMIPv6 overview

The MN can discover the new subnet by link layer specific mechanism, and then requesting the information about the available ARs. Via "Router Solicitation for Proxy Advertisement" (RtSolPr), and "Proxy Router Advertisement" PrRtAdv the MN provisions the "New AR" (NAR) when it is still attached to the "Previous AR" (PAR). Thus it eliminates the new prefix discovery latency which is due to handover. Next the MN sends a "Fast Binding Update" (FBU) message to authorize PAR through binding the old CoA with NCoA and accordingly to forward incoming packets towards NAR.

FBU's response, "Fast Binding Acknowledgment" (FBack) can be received by MN either when it is still attached to its PAR, or already left the PAR, and proceeds with appropriate tunneling method. The sequence of fast handover while still the MN is attached to the PAR and is moving toward the NAR is as following:

- MN gets a new CoA from new AR, though it is still attached to PAR.
- If NCoA is applicable with NAR, while the MN is attached to PAR, sends a Fast Binding Update (F-BU) to NAR, to keep PAR's cache updated.

- The PAR redirects MN's incoming packets to the NCoA from NAR. (If NCoA is not relevant, the PAR establishes a tunnel to NAR.)
- If NCoA is not applicable at NAR, then MN sends F-BU after moving to NAR, to keep PAR's cache updated.

When attachment to the new AR is done, the MN knows the new router's triplet (the prefix, L3 address, and L2 address). But it does not mean that the MN is able to receive new packets, unless NAR can detect the MN's presence. Via "Fast Neighbor Assignment" (FNA) MN informs its attachment to NAR, and assures use of NCoA whether FBACK is not received by MN. The ARs exchange the network resident contexts, such as access controls, QoS, header compression through "Handover Initiate" (HI) and "Handover Acknowledge" (HAck).

a. Network vs Mobile initiated handover

Based on received information (triggers) from link layer, either MN or PAR initiates the fast handoff process. If MN receives the triggers, it sends a PrRtSol message to PAR. Otherwise the PAR spreads PrRtAdv to the correspondent MN. Once the MN receives L2 handover information, it sends RtSolPr to PAR, which in turns makes PAR send PrRtAdv. The RtSolPr message originated from MN contains "Medium Access Layer" (MAC) address or NAR's identification.

The MN attains NCoA while still attached to PAR through information found in RA of NAR. Next the PAR verifies the obtained NCoA with NAR via transmission of HI message to NAR. According to HAck response, the PAR decides if it should establish a tunnel to NCoA (means that the new address is applicable) or to NAR's address (means that the new address is not applicable). In the latter case, the NAR generates a host route for the MN via its old CoA. In case of network initiated handover, the new CoA can be configured in two ways, stateless or stateful.

b. Stateless NCoA configuration

Whenever the PAR detects the movement towards the NAR, the old router generates a new address based on the MN's MAC address and the NAR's prefix. Then

the generated NCoA will be sent to L3 and L2 address of NAR via PrRtAdv message. At the same time, the PAR sends HI to the NAR to inform him the new and old MN's address. The NAR checks if the NCoA is applicable. If it was acceptable, the NAR appends the address in cache and sends a HAck. Otherwise, it sends HAck announcing that handover is accepted, but not with the new assigned address. Figure 2.4 represents the signaling flow.

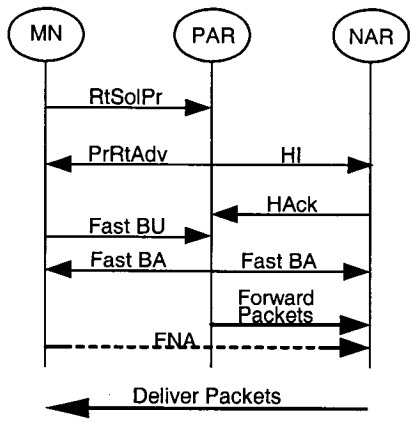


Figure 2.4 Stateless NCoA configuration in FMIPv6

c. Stateful NCoA configuration

In this case, the PAR sends HI message before PrRtAdv message. Via HI message the PAR demands for the MN's new temporary address, opposing the case for stateless in which HI requests if the assigned address is valid. NAR responds to PAR with HAck containing a valid address as MN's NCoA which can be used in PrAdv.

The main difference between the stateless and stateful configuration is in the latter case HI/HAck precedes PrRtAdv of PAR to MN. While the rest of procedure remains intact. Signaling flow is shown by figure 2.5.

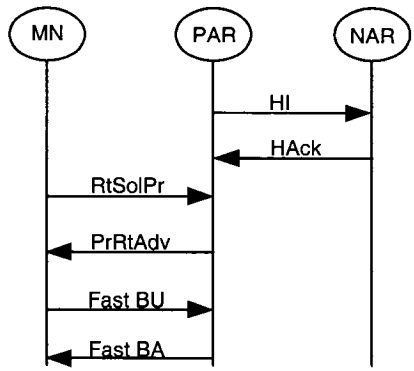


Figure 2.5 Stateful NCoA configuration in FMIPv6

2.3.2 FMIPv6 discussion

FMIPv6 has its own limit in handling the MNs with fast speed, though its name can induce false impression of its positive capability. An exceptional case of fast movement is ping pong while a MN moves back and forth between two subnets.

The other problem is the result of link layer idiosyncrasies which leads to receiving erroneous information on MN's movement, either the MN moves to a different AR, or it totally abandons the movement. In such a case, since the packets are forwarded to a not suitable AR, the impact is usually restricted to packet loss.

Another problem with FMIPv6 arises due to IP layer limits in handling fast MNs. There should be a concordance between L3 handover duration and MN's functionality to updates binding of HA and CNs. Fast moving MN does not let the signaling procedure to be completed and causes packet loss.

2.3.3 FMIPv6 and HMIPv6 integration

Integration of HMIPv6 and Fast Handover is possible in two ways, either AR, or the aggregated AR functions as MAP. Placing MAP in an aggregation router makes efficient use of bandwidth and saves delays. In this case, the HI/HAack messages exchange between MAP and NAR are to verify whether the new CoA is applicable. So basically the procedure remains intact, but MAP takes PAR's place. Signaling flow is shown in figure 2.6.

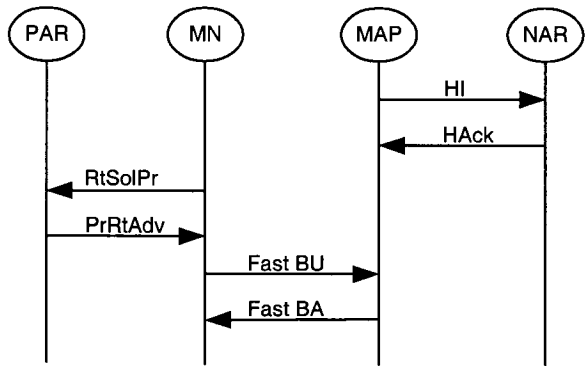


Figure 2.6 FMIPv6 based on HMIPv6

The challenging point is to decide when to forward the incoming packets to the MN's new location. If the time to detach from the PAR and to attach to NAR is not adjusted, then the packets will be lost.

2.4 Intra-Domain Mobility Management Protocol (IDMP)

IDMP [1] [2] aims at reduction of handover latency and mobility signaling load in 4^{th} generation environment. Like the other micro mobility protocols, it localizes the signaling to the domain itself. Each domain possesses a "Mobility Agent" (MA) which functions as the same way of a GFA in Mobile IP regional registration scheme. Subnet mobility is achieved by "Subnet Agents" (SA). Under IDMP, an MN obtains two concurrent CoAs: local care of address (domain wide), and global care of address (resolving address up to domain granularity).

2.4.1 IDMP overview

IDMP deploys the proactive method to minimize service interruption during the handoff process. Once the MA receives *MovementImminent* message either from MN or the old SA, the MA multicasts all incoming traffic to the entire set of neighboring SAs. Each of these candidate SAs caches the inbound packets in per-MN buffers, thus minimizing the loss of in-flight packets during the handoff transitional state.

A unique identifier, "Paging Area Identifiers" (PAIs), is assigned to a group of SAs which form "Paging Area" (PA). Listening to the identifiers enables MN to detect

changes in its current PA. A *PageSolicitation* packet is multicasted by MA to all subnets belonging to the MN's current PA to find an MN with invalid LCoA. Once the MN registered with the MA, the buffered packets are directed to the destined MN.

2.4.2 IDMP discussion

Like IETF proposal, IDMP is fixed centralized scheme. Consequently the same problems remain unsolved: its reliability is under doubt, since a single point of failure element exists in each domain. Moreover to place an agent in a domain is another issue. Fast handoff and paging operations are handled by lots of multicast addresses which waste resources and QoS issue is not considered [8].

2.5 Handoff Aware Wireless Access Internet Infrastructure (HAWAII)

Another micro mobility protocol which enhances Mobile IP to overcome its intrinsic limitations is HAWAII [5]. As it has been mentioned in literature, handover latency, signaling overhead due to continuous update of HA and CNs, and besides that establishment of "Resource Reservation Protocol" (RSVP) path after each roaming, are considered as mobile IP's draw backs.

These problems are addressed in HAWAII through setting up a path per MN in network domains' routers, therefore it conceals the user mobility from HA and CNs. Briefly HAWAII peruses the following features in wireless network:

- Fewer service disruption;
- Controls routing and tunneling, which results in efficient resource handling;
- Supports more number of mobile users through less HA updates which make it a scalable protocol;
- Presents QoS via less reservations and path reestablishment caused by user movement;
- And reliability via addition robustness mechanism.

2.5.1 HAWAII overview

Hierarchical structure of protocol resembles the autonomous system hierarchy in Internet. Each domain is served by a domain root router and presumably a mobile user has an IP address and a home domain. The domain root router receives the incoming packets destined to its subnet address and routes them to a visiting user in its domain through a pre-established dynamic path along the domain routers.

Once the user powers up and joins a domain, it sends a *path setup power up* message. The passage of this message over the intermediate hops towards the root router, establishes the host specific route in the domain. Altogether the paths from domain root router to the mobile hosts generate a virtual tree overlay. To increase the robustness of protocol, the path state in routers is considered soft-state meaning that the mobile host transmits periodic *path refresh* message to its attached base station to keep the host-based entries updated. Subsequently the base station and the intermediate routers, in turn, send periodic *aggregate hop-by-hop* refresh message towards the domain root router.

a. Handover mechanism

The mobile host sends *path setup* message via its attached base station. Next the base station forwards the message over the upstream routers towards the root to set up path state. Each intermediate router caches the user IP address and the receiving interface to be able to forward user's incoming packet in reverse path.

When the packets are forwarded from the old base station to the new, the path setup message is considered as forwarding schemes, whereas in the non-forwarding schemes, they are diverted at the crossover router. The latter scheme is based on the wired link to buffer packets and forward them to new base station while the former scheme keeps the previous and new connections to make a seamless handover.

"Multiple Stream Forwarding" (MSF) and "Single Stream Forwarding" (SSF) are two variation of forwarding scheme. MSF during handoff causes disordered streams and routing loops, though it provides simplicity and no packet loss. By using interface-based forwarding technique during handoff, the SSF forwards packets from previous

base station to the new one in a single stream. Apart from its high performance, its implementation is sophisticated.

Based on wireless network capability, there are two kinds of the non-forwarding scheme. Where the mobile host in a network is able to listen/transmit to two or more base stations simultaneously for a short duration, the "Unicast Non-Forwarding" (UNF) scheme is devised. Examples are aWaveLAN or "Code Division Multiple Access" (CDMA) network. While in the case of a "Time Division Multiple Access" (TDMA) network, the mobile host is able to listen/transmit to only one base station and the "Multicast Non-Forwarding" (MNF) scheme is optimized.

2.5.2 HAWAII discussion

HAWAII makes routing updates close to the access points, which results in localized update processing at the cost of possibly non-optimal routing. The other potential concern is the number of mobile hosts that can be attached to and supported by a single domain; consequently the domain root router can become a processing bottleneck. The final arguing point is the impact of failure of home agents (domain root router). Though a backup is suggested, but still there would be no connectivity during swap.

2.6 Cellular IP (CIP)

"Cellular IP" (CIP) [3] is a micro mobility protocol proposed by IETF to handle local mobility and handover support for frequently moving hosts in a simple and scalable manner. Its integration with Mobile IP provides wide area mobility support. The four main aspects of the protocol conception are [9]:

- Using distributed databases to store location information (via two types of caches) engages a large number of users roaming in the network without rendering the location management overloaded;
- The usual IP datagram initiating from MN generates and updates the location information;

- The routing entries (location information) have soft state, meaning that they are not valid after expiration of a certain time;
- Idle mobiles possess their specific location management isolated from active hosts.

A CIP domain resembles a tree based network. The root of tree, domain gateway plays domains' HA role and does registration management in addition to its traditional routing task. The CIP differs from the other micro mobility solution in two aspects [4]. Firstly, it is an operationally scalable protocol from small office systems to large area networks. Secondly, exploiting an effective location management and tracing scheme render cheap passive connectivity possible, a mechanism similar to cellular telephony.

2.6.1 Cellular IP overview

The registration process commences with an update message which is initiated from MN and goes through base station and uplink nodes towards the root (domain gateway), establishing the routing path. The MN identifies an available base station via reception of periodic beacon signal. The hops along the path keep a host-based routing cache, which maps the MN's IP to the incoming interface at nodes. Once the gateway receives the routing update message, it discards the message and learns how to reach to that specific MN.

To keep routing information updated, the MN (no matter if it is an idle one or not) refreshes routing cache via sending dummy packets sporadically. There are some conflicting views on dealing with timers. Since the mapping are not explicitly cleared after each handover, the routing path to the previous base station stays valid for a while. During this period the incoming packets are forwarded to the both (previous and new) base stations, which results in waste of resource. Choosing small timeout interval causes a significant load of dummy packet transmission by MNs. To master such a problem, each node can keep paging cache for idle MNs, and separate routing cache for active ones. Thus the timeout interval for idle MNs are set based on their movement frequency while for the active MNs is set according to the packet time scale.

a. Paging mechanism

Each idle MN sends a short control packet named paging-update packet. These packets are received by the nearest available base station and then forwarded hop by hop to the gateway. During its path, the nodes supplied by paging cache refresh their map database. The idle MN's incoming packets are queued by gateway and a paging packet is routed based on paging caches. In case the intermediate hop does not maintain paging cache, it simply forwards to all outgoing ports. Once the idle MN receives the paging packet, it generates a route update packet to establish the routing path to gateway and acquires the queued incoming packets.

b. Routing mechanism

The functional structure of routing is nearly the same as paging. The routing path is established from MN hop by hop along the uplink neighboring nodes and consequently incoming data traverses the reverse path to reach to MN.

c. Handover mechanism

Hanover in CIP is always initiated by the MN. CIP supports two kinds of handover algorithms: Hard and Semi-Soft handover. In the former case the MN moves from a wireless link (Base Station) to the other immediately. In the latter case, while the MN is attached to the new base station sends a route update message marked with a semi-soft handover and then comes back to its previous base station to receive the incoming packets. The route update message updates the path from the gateway to cross over hop where the path divides between the previous and new base station to maintain both connections.

2.6.2 Cellular IP discussion

The main argue about cellular IP is related to mobile host number [10] whether the protocol is able to scale to support high throughput with very large numbers of mobile hosts. The growth of active mobile hosts has a direct impact on routing tables in the access network. An efficient lookup in routing cache is needed for each data packet

forwarded by a base station. Whenever search in routing cache fails, the paging cache will be searched for the delivery of downlink packets.

Therefore to handle excessive overhead of host-based forwarding entries in the access routers, appropriate sizing of the domain and carefully selection of routers that are updated during mobile host's hand off are the MUST.

The other concern [5] is gateway issue. In addition to reliability subject, since outer world does not say any difference between mobile users and tunnels all packets to the same gateway, QoS management will not be an easy task.

2.7 Comparison of micro mobility protocols

As it has been noticed so far, the various micro mobility protocols have some characteristic in common [15].

- Micro Mobility Domain: A set of ARs form a region in which the MNs just inform the designated router (GFA, MAP) from their local movement. Once the MN changes its domain, MIP provide the mobility support; HA and CNs should be updated;
- The presence of a designated router, which acts like a local HA and conceals the MN's movement inside the domain from outer world.

Since domain conception impacts the performance of a micro mobility protocol, the importance of dynamic and distributed aspect of micro mobility is evident. Table 2.1 [12] compares different micro mobility protocols in two major groups: tunneled based versus routing based schemes.

Table 2.1 Comparison of micro mobility protocols [12]

	Routing-based schemes		Tunnel-based scheme	
	Cellular IP	**HAWAII**	**Regional registration/hierarchical Mobile IP**	**IDMP**
Domain root router	GW	Domain root router	The highest level of GFA in the hierarchy	MA
Additional cost	Propagating route information in routers		Tunneling overhead at each hierarchy	
Gradual deployment	Difficult		Easy	
Reliability	Rely on root (gateway) router		Rely on mobility agents at each hierarchy	

2.8 Dynamic, distributed hierarchical structure

A dynamic domain scheme has a unique property due to:

- Domain design cannot be based on network's topological scheme;
- The popularity of mobile network which affects tomorrow's connections;
- Dynamic user mobility pattern;
- Aggregate user mobility pattern versus individual pattern.

Two types of distributed system can be considered: fixed, and dynamic. A fixed regional network size is not flexible while in the dynamic one the region size can differ according to users' mobility pattern and traffic load.

Distribution and dynamic concept are two independent issues [19]. The former means that GFA's ability is shared among FAs, while the latter means that domain size is a time variant parameter. The possible cases [19] are presented in table 2.2.

Table 2.2 Micro mobility structure [19]

System Architecture	Regional Network Size	Comments
Centralized	Fixed	IETF Mobile IP regional registration is an example
Centralized	Dynamic	FA decides to send registration request to GFAs based on network specifications (difficult to implement)
Distributed	Fixed	
Distributed	Dynamic	[19]

The proposed anchor selection algorithm in HMIPv6 chooses the anchor with furthest distance and according to the preference field. In case of large number of subscribers, the selected anchor gets overloaded, and besides that as it mentioned in RFC itself, the choice of farthest anchor is not an optimal decision considering the mobility pattern of MN's particularly their speeds [7].

Unfortunately the proposed algorithm to define the size of a "Location area" (LA) in "Personal Communication Systems" (PCS) to obtain the minimum location update cost and terminal paging cannot be reused in Mobile IP case. The rationality to explain why are [19]:

- The cellular network is geographic-oriented while Internet is more spatial oriented. Structured cell configuration (mesh, or hexagonal) is far from subnet abstract;
- In Internet, distance is a virtual concept, since it is measured by hops, while in PCS, the distance between two cells are geographical issue;
- Paging cost in cellular network is comparable with triangular routing cost in Mobile IP. In PCS, a mobile phone is paged in all existing cells of a LA, while the routing path for incoming packet from CN to MN is known through HA and GFA.

Here we discuss other micro mobility schemes and some of the proposed solutions in literature to the distributed and dynamic aspect of micro mobility protocols.

2.8.1 Robust hierarchical mobile IPv6 (RH-MIPv6)

Survivability as an important point in QoS has been addressed by this article; particularly a fault tolerant and robust Hierarchical Mobile IPv6 is modeled to overcome HMIPs' fragile reliability. The essential idea of RH-MIPv6 [3] is placing two MAPs in each domain. Thus a mobile user receives two regional address, primary (P-RCoA) and secondary (S-RCoA) at the end of registration with different MAPs. In case of any fault detection, a mechanism has been provisioned to switch the connection from one to the other.

According to the article, the already proposed solutions in literature can be categorized in two classes: redundancy based and refresh based. In case of former one, multiple mobility agents are available. The primary and backup should exchange periodic synchronization message to keep each other updated. While in the latter case, a periodic binding update in a refresh time interval proposed to recover from HA or FA database crash.

As it has been acknowledged in literature in HMIPv6 case, HA and MAP are two points of failure and potential performance bottleneck. For example a "Denial of Service" (DoS) can interrupt the functionality of MNs visiting a region served by faulty MAP. In first place a distributed MAP environment replaces the basic one MAP structure of HMIPv6. They can be located in any level of hierarchy including AR, and they can function independently in a single domain.

Once an MN enters a domain, it receives RA message with MAP option from all existing domain's MAPs. Binding update message in RH-MIPv6 has a P flag to distinguish the message destined to each MAP. The binding update message with primary MAP exploits a P flag set to one, and with the second one the P flag is unset. Thus MNs and CNs maintain binding information of MN's primary and secondary RCoA.

a. Failure recovery mechanism

The valid life time in MAP option is used to discover MAP failure in HMIPv6. Since the RA interval is set to few seconds, therefore failure discovery takes too much time and results in service disruption. In RH-MIPv6 different failure detection scenarios have been considered: MAP failure detection by CN, and MN.

If CN does not receive any response from MN's serving MAP via "Internet Control Message Protocol Version 6" (ICMPv6), it deduces MAP failure. Next it searches for second binding entry in its binding cache, and forwards the packets to the secondary MAP. Whenever the MN receives the packets from new MAP, it sends a binding update message with the secondary RCoA to HA and CN. The MN detects fault the same way through ICMPv6 message.

Through analytical and simulation results, the authors show that RH-MIPv6 has 60% faster recovery time than HMIPv6. In HMIPv6, an MN reconfigures a new RCoA after failure detection, which consequently takes time, leads to service disruption and "Duplicate Address Detection" (DAD). Though a distributed MAP hierarchy is considered, and enhances the survivability issue (single point of failure case in traditional HMIPv6), but still like HMIPv6 it assumes a fixed region for MAPs. Moreover the mechanism how to place them in a domain, and how they are selected are not discussed at all.

2.8.2 Multicast-based mobility (M&M)

A new proposed handover management scheme which points to improve Mobile IP performance [13]. In each domain the visiting mobile attains a multicast address in addition to its regional care of address. Hence the handover is accomplished based on multicast join/prune mechanism. Two different approaches are presented: mobility proxy approach, and algorithm mapping. The algorithm mapping is proved to be more scalable and robust. Once a mobile enters a new domain, it obtains a new unique unicast address known as RCoA and a multicast care of address (MCoA). The RCoA can be assigned from any subnet in the domain. The scope of MCoA is local to the domain;

therefore the user does not acquire a new CoA with every subnet change in the domain. Incoming packets destined to MN are routed to the RCoA through Internet and then redirected within the domain by MCoA.

As it mentioned in the article, the IP mobility using multi-cast based mobility approach is not appropriate for inter domain mobility. First, today's internet cannot handle the ubiquitous multicast deployment. Second, it is due to huge amount of multicast state proportional to the number of users. Third, the need of global multicast address allocation scheme which wastes multicast resources, and finally the security overhead is more crucial with multicast than unicast systems.

The simulation results have been compared with CIP. In case of proactive handover M&M and CIP show lower handover delay and packet reordering than HAWAII, while for reactive handover and coverage gaps, it surpasses CIP and HAWAII.

a. Proxy-based architecture

The MN sends a *request* message through the serving AR to "Mobility Proxy" (MP) to obtain a MCoA. Subsequently the MN registers its address as CoA for the MN's home agent, then specifies a MCoA and sends a *reply* message to MN, and finally maintains the established mapping. The visiting MN joins the assigned multicast (G), and sends the join to the proxy-group pair (MP, G). The join is processed as per the underlying multicast routing.

b. Algorithmic mapping architecture

Algorithmic mapping architecture was devised to overcome the shortcoming of proxy based architecture like scalability, complex robustness algorithm, MP's survivability issue (single point of failure), and finally the need for a multicast address allocation scheme. Through scheme modification, with addition of an algorithmic mapping, the AR can derive the multicast address for the MN from the obtained unicast address. The AR then triggers a *join* message for MCoA to set up the multicast tree.

c. M&M handover framework

According to definition smooth handover is a result of beforehand knowledge of the future-be serving AR. In proactive handover, smooth handover is achieved through tunneling or bi-casting to both previous and new AR since the MN knows the identification of the new AR before detachment from previous AR; while in reactive handover, a sudden disconnection from the previous AR causes handover (ex. Handover in IEEE802.11). Hence prediction of new AR and path establishment proactively is a must in second case.

Since M&M is an intrinsic multicast protocol, is able to send packets to multiple ARs simultaneously and minimizes packet loss. A potential set of adjacent routers to the serving router is defined as "Candidate Access Router" (CAR-set). The CAR-set handover algorithm does proactive route repair by initiating multicast join from the old AR before link level handover. All member routers of the CAR-set join the multicast tree corresponding to the mobile's MCoA.

Apart from its better performance in case of reactive handover, M&M can deal the presence of multiple border routers in a domain, while CIP fails. In case of proxy-based architecture, the MP is considered to be placed at the border of the domain, or at the center of the network. But there is not an explicit algorithm on dynamic MP aliveness and election mechanism. The reader has been addressed to [14].

2.8.3 A dynamic micro-mobility domain construction scheme

To reduce the signaling cost with a low complexity, the article [15] proposes a dynamic "Micro Mobility Domain" (MMD). For simplifying the task of a network operator, some assumptions have been taken:

- Operator decides the number of domains beforehand (k);
- K routers are designated as seed by operator too.

During algorithm execution, the free routers join the seeds and set up a domain. The selection of a seed is based on the evaluation of signaling cost; the seed with the

least cost will be considered to be joined. Whenever an AR is part of a domain, its state is *joined*, and otherwise *independent.*

The metric used to measure the traffic between ARs is the number of registered MNs (CoA). Each AR can be part of domain in a predefined time (lifetime). After lifetime expiration, the AR is independent to choose a new domain based on the new network traffic pattern.

As it mentioned in the article, the MMD construction problem can be proven to be a NP-hard problem, hence the proposed scheme is not designed to provide the optimal performance. The solution can be considered as a sub-optimal one with a low complexity which is applicable by operators. Besides that the logical distance between routers is based on hops, causing delay in an ordinary transmission. Moreover, though the assumption made by the article simplifies the case, but this supposal is at the price of precision.

2.8.4 Dynamic hierarchical mobility management strategy (DHMIP)

The article addresses the Hierarchical Mobile IPv6 problem in GFA selection and its reliability [17]. According to the proposed mechanism, different hierarchies are dynamically setup for different users, hence distributes the signaling burden equally in the network. The signaling cost of scheme has been evaluated through a development an analytical model. The scheme outperforms the IETF HMIPv6 in terms of the overall signaling cost.

In DHMIP, as MN moves among subnets, it registers its new CoA with previous FA, hence reduces location update signaling message. The incoming packets for each individual user is intervened and retunneled along the hierarchy of FAs which are established for each user. Packet traversing through the chain of FA causes some delay which is not acceptable for real time application. Thus a threshold is set for each user which restrains the level of hierarchy. The threshold is defined based on user mobility pattern and traffic load. Whenever the threshold is reached, the MN updates the HA with its new CoA directly. The intercepted packets by HA are forwarded to the FA which has been updated as user's anchor point last time. Then the packets move along the FAs

chain to reach to the destined user. The optimal value of hierarchy level can be computed in different occasions, every time the MH enters a new subnet, or whenever the previously calculated threshold is reached, or it can be periodically adjusted. There is a tradeoff between the accuracy of the value and computation cost for MN.

a. Improvements to DHMIP

State activation and loop removal are some elaboration to the protocol.

- State activation

Based on Cellular IP's paging functionality in which HA has rough information about an idle user, enhanced DHMIP has been proposed. In the scheme, an idle MN does not receive packets for a system predefined period; hence the hierarchy level (k) can be set to a relatively large constant number. Consequently the MN energy consumption reduces. Once the MN receives packet, immediately it updates its address with HA, and recalculates (k).

- Loop removal

Sometimes user moves in a limited area, meaning that he revisits the already have seen subnets, and according to the defined scheme of DHMIP, loop may form in FA's chain. To avoid such a problem, whenever a user enters a new subnet, the new FA verifies the hierarchy list of MN if its address (FA) has been already recorded there. If that is the case, it removes the subsequent FA addresses for that user without updating the old FA. The obtained results show that there is no optimal threshold for an MN. Obviously a higher threshold value yields a higher performance, while at the same time large threshold consequences to long packet delivery delay for the first packet. Thus, there is a trade off between signaling cost and QoS that should be observed by operator.

The other point is hierarchy level value (k) impact on the performance according to the Call to Mobility Ratio. Whenever CMR is high, no matter which value the k has, the performance is not influenced. That is due the fact that in MN's active state, the HA should be kept updated.

2.8.5 Improved distributed regional location management scheme for mobile IP

Since in IETF centralized regional registration scheme, the domain's border is vague, it is usually difficult to determine the regional network size. The proposed distributed network architecture in literature [19], addresses this problem which sets up the domains based on individual user's mobility pattern. Hence the signaling traffic can equally be spread among the networks. Though in both cases, since the serving FA is not the GFA, so there would be always an extra packet delivery cost.

This paper [16] develops a system model to analyze the distributed scheme performance. In addition it also advises an improved distributed scheme. The idea resembles the distributed scheme, yet it counts user state too. If the user is in idle state, it does not receive or transmit any packet and the distributed system remains intact. Once the user receives or transmits a packet, it changes its state to active.

In active state, without considering the evaluated regional network size, the MN updates the current FA's new CoA with HA. As long as the MN is in active state and with every movement, it updates again the new CoA with HA. It means that the regional network size is fixed. Therefore whenever MN is in active state, its serving FA is also its GFA, which leads to less packet delivery cost with no increase in location update cost.

As it has showed in the article, the distributed network architecture with fixed regional size can have saving only when the CMR is small. With CMR increment, the dynamic scheme has a better performance than the fixed one and will never generate more traffic load than the basic mobile IP scheme.

Since the idea is built on [17] and it does not change whenever the MN is in idle state, so still it has the same disadvantage.

2.8.6 Dynamic & distributed domain-based mobility management method

The article [18] is another study on dynamic and distributed aspect of micro mobility management issue. The scheme has been simulated to compare with basic Mobile IPv6 mobility management and it shows the reduction of the binding update and packet delivery latency and traffic. The taken approach is based on individual MN's mobility pattern and its packet arrival. Besides that the mobility agent is not restricted to

just one router, and it is distributed among all of them. Thus the distributed view can deconcentrate network's load, and alleviate management problems in case of failure in domain mobility agent.

As the other domain-based mobility management, the MN obtains two care of address; one from its serving AR (LCOA) and the other (FCoA) from domain mobility agent. Hence the user performs the local binding to its DMA and registers with HA whenever he moves to the other domain. For each MN, case by case, domain is defined according to his mobility pattern and traffic load. To achieve a dynamic domain, all ARs possess a list of routers within the distance threshold from each AR. The distance is calculated based on the number of hops between two ARs. The so called domain list shows the domain range of a specific AR.

Network topology affects the distance threshold of each AR. The first visiting router is the user's first DMA. As MN proceeds and receives the other router's advertisement message, it checks its buffered domain list to see if the new AR's information is already there. If not, the MN updates its buffer with new AR's domain list and registers the new acquired FCoA with HA and the new AR acts as new DMA too. If the new AR's IP address is found in MN's buffered domain list, there will not be need to update its domain list and also it maintains the already assigned DMA. Once incoming packets destined to a user is intercepted by the MN's home agent, they are tunneled to the MN's FCoA, found in HA's binding cache. DMA obtains the packets and decapsulate them to the destined user.

AR's dynamic domain may cause packet loss. Such a packet loss is due to dynamic change in domain list. Hence to prevent the effect of domain change, each MN considers a life time for its domain list. Whenever it expires, it asks for an updated domain list from DMA. If it differs with its own, the MN has to send binding update to the HA.

The MN's speed has a direct impact on network performance. The more mobile speed is, the bigger the domain size should be to achieve a better performance. And on contrary higher packet arrival rate makes the domain size smaller.

The work can be seen as a study in Mobile IPv6. The simulation result has been analyzed in comparison with Mobile IPv6 and not Hierarchical Mobile IPv6. Since for sure domain based mobility has its own advantages and disadvantages in comparison with traditional Mobile IPv6. But it could make more sense to examine with the other similar proposed schemes.

2.8.7 A distributed dynamic regional location management

Another interesting article [19] which discusses the dynamic and distribution aspect in domain-based mobility based on the up-to-date mobility and traffic load for each individual terminal. It addresses the intrinsic deficiencies of Mobile IP regional registration like being centralized which leads to sensitivity to GFA's failure, and its vague definition of region. Besides that it aims at optimized system configuration, signaling load reduction, and system robustness enhancement through a discrete analytical model.

- Distributed vision of network

According to the user mobility pattern, each FA can be considered as GFA or FA. Once the MN enters a regional network, the first serving FA takes the role of GFA for that specific user. The GFA keeps a visitor list and updates it according to incoming registration request which indicates the MN's movement in regional network, and as usual it transfers home registration request to HA too.

- Dynamic vision of network

The number of FA under control of a GFA varies based on incoming packet arrival rate and user mobility pattern, hence optimized for all and each user in the network. An IP address list of all present FAs exist in each mobile. Whenever the MN enters to a new domain, it adds the new GFA's address into its list and updates the HA with its new RCoA via the new GFA. The calculation of optimal number of FA for a domain is performed according to MN's parameters. This value is a length threshold of MN's buffer.

Once the MN detects a new subnet, it sends a regional registration message to its GFA (the first visited FA). Then it compares the address of new serving FA with already saved addresses in its buffer. It adds the address in case it cannot be found in the list. Otherwise it ignores the FA. The MN is in a new domain whenever the address in the list exceeds the threshold. Because of threshold value and the taken strategy on address addition to the buffered list, the back and forth movement does not generate zigzag effect.

According to [15] the proposed scheme imposes a high complexity on operator's network. Firstly, each router has dual functionality of GFA, and AR. Secondly, the scheme is based on individual mobility pattern, hence a large number of subscribers put a large burden on network operator!

2.8.8 Architecture for mobility and QoS support in all-IP wireless networks

The article [8] proposes a modified version of forwarding chain in MIP domain which supports fast handoff, fast location lookup, and resource reservation.

Two types of forwarding schemes have been considered: *region based* and *movement-based* schemes. In the region-based forwarding (abbreviated as R-FCAR), the forwarding paths for an MN is limited to be within the same PA. The renewal happens whenever MN handoffs to the other PA, subsequently the new visited SA in the new PA is chosen as new anchored SA. In the movement-based forwarding (abbreviated as M-FCAR), the maximal length of the forwarding chain (in terms of the number of movements) is fixed to a certain threshold. Passing the threshold makes the renewal of chain.

Fast Handoff is similar to fast handoff mechanism in IDMP. While in IDMP during handoff serving MA sends the buffered packets, in this proposal old SA takes the role. By sending *MovementImminent* message to the old SA from MN, the old SA redirects all MN's incoming packets to neighboring SAs via the subnet paths. The neighboring SA caches inbound traffic in its per-MN buffers. After MN registration with new SA, then MN sends a forwarding request message to the old SA (via the new SA). As soon as the old SA receives the forwarding request message, it directs future packets

directly to the new SA via the subnet path, instead of sending them to the neighboring SAs.

Fast Location Lookup is to prevent MIP's triangular routing which causes a long call setup delay in the voice over IP applications. It is due to the fact that only HA is aware of MNs' movement. The idea presented is based on cellular networks which reduce the call setup delay by replication the address mapping of an MN (MN's home address, MN's GCoA) in the HA to the MAs. Thus the local MA can deliver a call for the remote access network's MN by looking up the replica in the remote MA without sending any query to the HA.

Since the connection path between anchored SA and CN (intra domain) is less probable to be altered, so RSVP's per-flow resource reservation can be employed at anchored SA. For HA - MA connection, and also the connection between the MA and the anchored SA, RSVP over IP tunnels are applied. The end-to-end QoS is satisfied since the forwarding chain to trace the terminal mobility is set up over subnet paths with preconfigured resources, therefore the resource preparation can be rapidly and conveniently broadened from the anchored SA to the MN's current SA.

Forwarding and anchoring concepts are to reduce the signaling traffic due to location registration; however they may impose additional delays during location retrievals. The two approaches show different degrees of performance improvement according to call to mobility ratio.

2.8.9 Load-balanced location management for cellular mobile systems using quorums and dynamic hashing

The article [20] proposes a new distributed location management in personal cellular system (PCS). Fast location update, and query, load balancing among location servers and scalability are the achieved points. Location updates and queries for an individual are multicasted to a time variant subset of location servers, based on the MN's and query node's location, and load on the server.

According to the introduced distribution location management, the MN's information are cached at O (radical N) location servers (where N is the total number of

location servers in the system). The scheme's round trip message delays for location query shows improvement over hierarchical structure in the worst case. Besides that it eliminates the placement of HLR, and VLR in network.

The system model is constituted of "Mobile Service Station" (MSS) serving as a base station to each cell, Registration area composed of a cluster of neighboring cells, and zone formed by one or more RAs. Location servers considered for RAs and zones keep MN's location information. The employed mechanism for fast update and query is a distributed concept. Determining the location servers of an MN is not based on MN's location to prevent overloading a specific area's server. Hence a function (h) of the MN as well as the current cell of MN defines the subset of servers which maintains the MN's information. Therefore function h (.) defines the MN's update set as long as it moves, and the query set to fetch MN's location. Since network load varies in time as the mobiles move, a uniform hashing function that guarantees load balancing in a specific time cannot respond according to situation. To overcome such a problem a dynamic hashing whose value range shrink or extend in time variant system load is proposed.

The discussed idea seems quite interesting. To achieve robustness and scalability, the system is basically distributed. Though dynamic load sharing among the servers are fulfilled but the policy to determine the size and layout of registration areas are predefined and considered solved issue.

2.8.10 Load balancing hierarchical model for micro mobility

The scheme [7] proposes a new load balancing hierarchical model for micro mobility management, using an anchor selection algorithm which is based on the MN's traffic QoS class and mobility characteristic. Moreover, robustness, scalability, and fast handoff are some strong points of the presented model.

The scheme is inspired by the 3rd generation of UMTS network model. "Radio Access Network" (RAN) and "Domain Access Network" (DAN) separate the network into regions. Each paging area, as a group of access points, is connected to "Paging Access Router" (PAR) by IP tunnels. The PARs, the root in RAN and leaf in DAN, traces all mobile stations, and handles paging function and handoff management for the

MN's within the RAN. "QoS-aware Anchor Agents" (QANAs), form the hierarchical layers of DAN. From the highest layer to the lowest one, the QANAs are named: Gold, Silver, and Bronze. The anchor selection algorithm helps each mobile to choose a suitable QANA. Consequently the MN is assigned an IP address for global registration, authentication, and data packet exchanges. Whenever the MN roams from its serving (home) QANA domain to the new one (inter anchor mobility), the algorithm reselects a new QANA.

In addition to multiple gateway routers implementation, overlapping the domains of QANAs of the same layer can alleviate the single point of failure problem.

a. Anchor selection algorithm

The PAR collects MN's demanded services and its characteristic, then performs anchor selection procedure and selects the suitable QANA on behalf of MN. A QANA selection matrix and a QANA cache table (maintaining all QANAs in charge of PAR) are resident in each PAR. As the matrix is composed of QoS and mobility pattern, hence the concept of QoS classification and mobility characteristic are turning points. The four main QoS classes have been derived from UMTS definitions: conversation class (VoIP, video conference), streaming class (video on demand), interactive class (web browsing, database retrieval), background class (FTP, Email).

Also, mobile wireless applications are considered to be: movable (pedestrian scenario), slow ($\leq$ 36 km/h, main road scenario), and fast (highway scenario). Each PAR requests the status of its attached QANA to keep its cache table real time and updated. Each entry of QANA cache table has two fields: preference field and valid lifetime field. The former indicates the load information of QANA and the latter shows the validity of information. Finally higher level anchor is chosen for delay sensitive applications which provide them with optimal routing path and lower delay in domain. On the contrary lower level anchors are selected for data integrity sensitive applications to get enough buffer resources for mobility management. Different service classes are presented in table 2.3.

Table 2.3 QANA selection matrix [7]

QoS + Mobility	Fast	Slow	Movable
Conversation class	Gold	Gold	Silver
Streaming class	Gold	Silver	Bronze
Interactive class	Silver	Bronze	Bronze
Background class	Bronze	Bronze	Bronze

The idea of QANA selection algorithm seems genuine, since the QoS affects directly the choice of appropriate MAP, along with each individual MN's QoS traffic class and mobility characteristics parameters. Hence the MN's registration load and mobility management are distributed to all the QANAs in the domain. In my point the only issue which needs reconsideration is the fixed MAP hierarchical structure, in other words the anchor's known placement in hierarchy.

2.8.11 Multilevel hierarchical mobility management scheme in complicated structured networks

The article [21] aims at HMIPv6 mobility management enhancement through decentralizing the load of mobility management with various levels of MAPs. In fact it continues the authors' previous work [22] with some improvement to select a suitable MAP for the MN in a complicated hierarchical structure by adjustment of selection criteria at a particular place.

Basically the MN assignment to a hierarchical MAP is done based on the speed of MNs. A higher mobility MN is managed via a MAP with a wider domain, located in a higher level of hierarchy, and slow mover MNs are assigned to a lower level MAPs with narrow domain. To alleviate the single point of failure problem, the MAP domains situated in the same level of hierarchy should overlap each other in a densely meshed tree topology.

To realize the idea, a database named "Selection Table" (ST) resides in each AR, gives the visitor MN's information about candidate MAPs. A list of pairs of speeds representing as minimum and maximum thresholds of speed, and a list of corresponding

MAPs are included in each ST. Therefore the MN will be able to select its MAP based on its historically estimated speed and the content of ST in visited AR. Since the network structure and mobility pattern affects the choice of suitable MAP for each MN, hence a single distribution criterion is not enough.

At first place the MN selects a MAP with the smallest domain among the available MAPs with MN's mobility attitude consideration. Then the ST configuration adjustment tries to configure different contents of ST at each AR. Based on MAP's domain size, its initial value of maximum threshold of speed can be set. The management load on neighboring MAPs adjusts the threshold at each AR periodically in an autonomous way.

Though the scheme goes far beyond the rough and simple method of HMIPv6 anchor selection, it still has some deficiencies. The adjustment algorithm makes decision based on MAPs' loads and mobile subscribers' speed. In addition to insufficient consideration of subscriber's mobility pattern (speed represent all MN's aspect), no means is recommended to calculate the MAP's load and the related affecting parameters. Having MAP with fixed domain size, makes the procedure easy and at the same time not pragmatic.

2.9 The other related work

Chu and Weng [23] propose a scheme in which MN exploits a cascaded tunneling strategy in a mobile IP network, called "Pointer Forwarding MIPv6 Mobility Management" (PFMIPv6). Upon MN's movement into a new domain instead of registration with HA, a tunnel is established between the old PFMA and the new one.

The authors in [24] present a combination of pointer forwarding and caching method. A chain of anchors connects each mobile to the HA (the first anchor). The authors assume a correlation between communication cost and geographic distances.

Chen and Boult [25] focus on mobile IPv4, and propose simultaneous binding with two or more HAs to provide seamless HA handover. Since HA is not static any more, the "Network Access Identifier" (NAI) or "Full Qualified Domain Name" (FQDN) is used rather than home address.

A hierarchical architecture is proposed in [26] to improve the performance of Mobile IP in GSM networks regarding fast intra domain handover and latency reduction. Each roaming MN obtains two care of addresses, one link local address to use in a region of a specific BSC and one site local address which identifies a MSC's region. HA and CN communicate with MN through the MSC's IP address.

To alleviate the FA's bottleneck in hierarchical structure, a new micro mobility management for a metro sized network is advised in [27]. Connecting all the MNs on a single ring network which covers a metropolitan area generates a flat network structure. The ring is composed of "Mobility Switches" (MSW) which maintains registration information of MNs and a "Gateway" (GW) which handles a bidirectional connection with the outer network.

Onwuka and Niu [28] combine the idea of distributed hierarchical location directory with prefix routing to gain a balanced loading of network nodes in a MIPv6 access networks. A dynamic domain, based on Internet administrative domain structure, is constituted of a "Domain Router" (DR) and AR. Access network nodes are arranged in a logical tree hierarchy and a block of globally routable IPv6 address space is assigned to each domain. In [31], they compare the multi level hierarchy with flat (fixed) hierarchy, and draw the conclusion that scalability and delay performance of mobile network improve under multi-level hierarchy structure. Finally it concludes that hierarchical design based on addressing structure may scale better for it does not generate bottleneck problem on root node!

To eliminate the load of packet processing at MAP and to do packet deliverance from CN to MNs without MAP intervene, a new scheme is proposed in [29]. Each MAP manages the mobility profile for MNs of its administrative domain. If the MN's average residence time in subnet (domain) is less than a threshold, it registers the LCoA with the CNs. Hence CNs can forward packets directly to MN through optimized route.

The authors in [30] discuss the MN's ability on the selection of a suitable mobility management mechanism (MIPv6 and HMIPv6) for each CN according to MN's mobility pattern (speed and traffic intensity).

CHAPTER III

ANCHOR SELECTION ALGORITHM AND MODEL

This chapter presents a novel approach which focuses on mobility management issue in mobile networks. It builds on top of the hierarchical architecture of HMIPv6 and tries to find the most suitable anchor point based on users' mobility history.

The goal is to establish a scalable, distributed network of modular entities. The important facts are the limited amount of sharing resources and the ever changing characteristic of network. It leads to rising of continuous modifications according to the new encountered real time conditions. As it mentioned in the second chapter, several proposed schemes consider the dynamicity in micro mobility and try to solve the complex issues. Most common points in all those schemes are the user mobility pattern and the call arrival rate which restrain the depth of domain. On the other hand, the optimal number of access routers under control of an anchor is obtained according to the mobility characteristic of each user. However the individual mobility history in none of them was taken into consideration.

The rest of the chapter is organized as follows. First we present the principal concepts of the proposed model, and then the following section introduces the proposed architecture. The detailed description of the model and the algorithm come next. Finally, the signaling cost and delay of scheme will be compared with the other proposed one, basically HMIP.

3.1 Basic concepts and principles

The idea of the proposed scheme is based on three issues: micro mobility, dynamic aspect of the network, and user mobility pattern. Hence each of them is discussed in more detail to give a view for the rest of the chapter, specifically to make the model more comprehensive.

3.1.1 Micro mobility

The goal in a domain oriented mobility management scheme is reduction of overwhelming binding updates signaling in a standard IP mobility management. Having a substitute of home agent in the network which is called anchor agent is the basic idea of localized mobility management. Thus the signaling messages get reduced as long as the MN stays in a specific domain. Moreover the MN informs its peers of its movement from home to a visitor network via a global BU to HA and accordingly through an RBU to the anchor agent.

According to HMIP structure, the network is divided in domains in which an anchor limits the outgoing signaling to HA. But some problems coexist with the nature of protocol:

- The centralized architecture causes single point of failure;
- The fixed boundary (region size) which ignores the real time change of mobile environment.

3.1.2 Dynamic aspect of the network

Dynamic aspect of the network is considered as one of the main point of this research and as corollary its affect (mainly the complexity) to the system. Generally a perfect, pragmatic structure of resource allocation in time variant environment is known with certain characteristics like:

- Scalability, and flexibility of procedures;
- Robust interactive between network elements;
- Real time restructuring whenever changes arise (dynamic situation);
- Reliability in case of disruption of communications.

The anchors represent the resources which are requested by the MNs. Particularly two facts signify the resource allocation problem, which in our case is selection of the best anchor. The first fact is the load on the anchors which is a time variant parameter. Second, the roaming MNs with variable required service cause different situation in the network. It should be once more notified that unexpected

changes in the environment or modified global directives will initiate dynamic recalculations and modifications to anchor behavior as well.

Individual anchor based on their responsibilities may fulfill specified job and/or accept the extraneous forwarding load and routing state to minimize the outage probability. Thus the anchors communicate among themselves via two-way communications to compensate the deficiencies and establish a fault tolerant system. In consequence some links of dependency are dynamically created between them, and supervisory control algorithms insure that these dependencies will not interfere with the completion of the objectives. In brief the allocation and resource sharing, task execution and planning corresponds to the problem constraints and objectives.

3.1.3 History and user profile patterns

The current trend in mobile communications is to provide customized services while saving the system resources. Meaning that an adaptive and dynamic view of the system takes into consideration the individuals' characteristic, consequently resources are shared efficiently and in an optimized manner. The movements in the network can be predicted using the fact that most subscribers have a daily basis schedule. Based on their daily activities, the movements' pattern can be defined and some classifications are possible. If mobile user's movements are considered stochastic, then Markov model represents them efficiently, but regularity is part of human's life and consequently a random process cannot be a good model for user movement's behavior.

Hence the system can behave for each category in respect to its properties and can save the signaling messages load, leading to the minimal cost. Either a single user model or a set of users grouped by their call arrival and mobility pattern can be defined to analyze the situation.

To have a precise prediction of user movement, two types of information need to be collected in the network:

a) Long term observation of a user activity which represents slow changes in weeks or month period.

b) Short or medium term activities represent the last behavior of users, leading to more memory requirement and per user profile updating cost.

3.2 System description

We assume that each service region is divided into cells which are served by base stations. An aggregation of a number of cells, in which an individual user moves, forms a subnet served by an access router. A domain is constituted of many subnets. Per each domain, one anchor point keeps the address and the other relevant information of users who are residing in its charge area. The HA in turn stores the address of serving anchor points for each users (in fact the first anchor of the chain is the reference address). The MN keeps monitoring the beacon signal of agent advertisement to discover the access routers. As MN changes the access routers, it updates itself with the new serving access router. Next it registers the newly obtained address with its serving anchor point. Security aspects (AAA: authentication, authorization, and accounting) can be addressed at this stage as well.

The scheme addresses the mobility management issue through two phases: the learning process of mobility pattern and the profile based protocol which is built from the previously obtained data. These phases are fulfilled via considering the below mentioned points:

- The MN should cache its own history information, to reduce the signaling load due to tracking the users in the network, as a result the accuracy and resolution of the data is more guaranteed. The mobility pattern repetition interval is considered for 24 hours (daily period). The learning model should be able to detect the regularity of movements and build a daily time based visited access routers. As soon as the model discovers the stability in the movements and following the same habitude, then the mobility pattern is devised and ready to predict. Building history is accomplished in two phases. During the first phase the regularity of movement (the visited routers pattern) is detected, thus the time intervals are defined. Then the addressed QoS offered by routers are defined for each time interval. Here the scheme does not go through the learning phase detail. Some specifications and the expected information

which can be acquired from this stage are discussed. In the learning phase, the access router observes its capability and the requested services by users, and helps the MN to decide on the most suitable anchor.

- The protocol makes use of the built pattern of learning period.

Some hypothesis and constraints on the IP mobility proposals, which affect directly the effectiveness of the protocol, are addressed below as well:

- Round trip time latency between MN and the anchor increases as MN passes many domains during its journey. The upper bound is the round trip time between the anchor and the HA;
- All traffic destined to the MN are routed to the domain anchor, hence the anchor should guarantee the optimal path;
- The exchanging message between anchor and MN, the anchor and HA (the BU/RBU message) can be extended via sub-options. Thereby a trade off between the functionality of anchor and the signaling message overhead is recommended;
- A real network is in ever-changing state in term of the number of users. Hence scalability should be provisioned in advance. Moreover a uniform distribution of anchors in a domain is a MUST, which prevents extra loads and hot spot creation in network;
- Fault tolerance mechanism for anchor should be provided to lessen service disruption. Meaning that the anchor functionality should not be intervened by any topological changes in network (addition or deletion of any network elements). It can be an advantage to able the anchors to reconfigure themselves after any change automatically;
- The MN shouldn't get involved in complex task of load balancing, anchors selection or such other mechanism. The MN functionality is to pertain to the case of small mobile device and wireless environment;
- As an important issue in scalability to have the best performance, it is better to minimize the routing state. Besides that the functionality of an anchor should not interfere with the dynamic routing functionality of core network;

- The interoperability of extensions to micro mobility protocol with the base IP mobility protocol as well as each other is an asset. In case of cooperation between two protocols, the compatibility in their signaling interactions to cover each others' deficiency is essential;
- Security issue is another important aspect in IP mobility management. The anchor can be mostly attacked by denial of service and message replay. But to avoid latency and scalability problem, the point to point security issue (between MN and its peers) should be transparent to the anchors functionality.

3.3 Scheme overview

Considering the above mentioned facts, the proposed scheme makes use of the regular pattern of users in network. For example a working class user leaves home at a certain period of time in the morning and does his jobs at certain places in the course of the day and returns home. Hence usually the visited access routers stay the same in daily life. Moreover his requested services are somehow the same during his movement pattern. Figure 3.1 shows a simplified view of user's mobility movement pattern. It should be noted that for the sake of simplicity, each hexagon represents a subnet which is served by an access router.

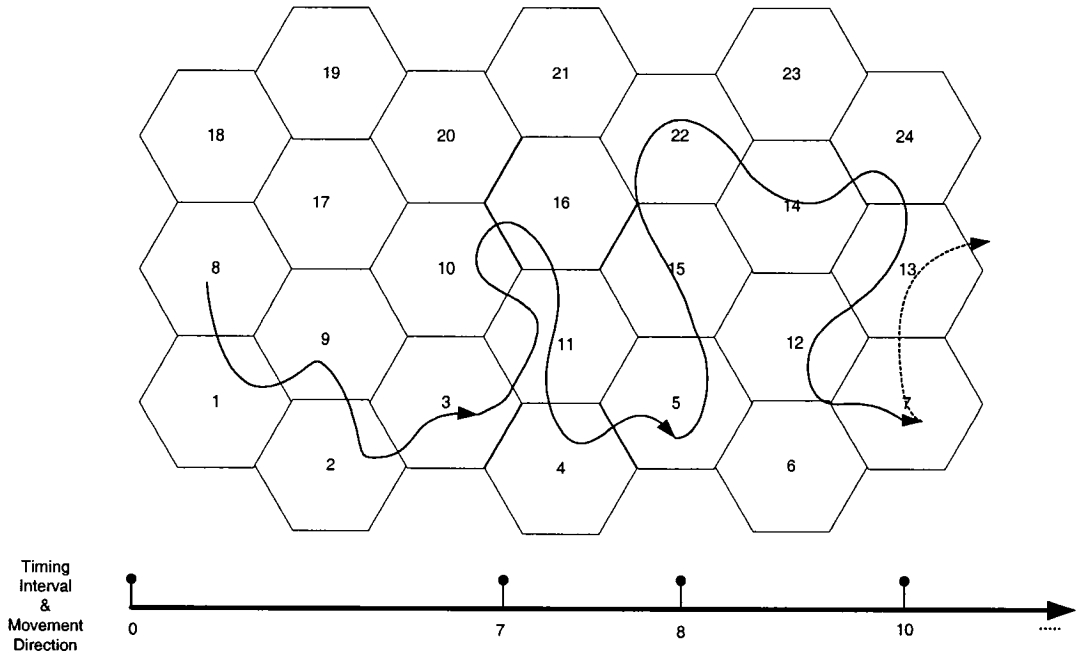


Figure 3.1 A schema of user's movement path

Apparently the probability distribution of each user's activity is not uniform in the observation period. To provide a better, more precise view of the individual mobility pattern, two dimensions are considered. The first dimension defines the user profile in a quasi deterministic approach like working day, holiday, and weekend. The second dimension follows the mobility behavior in different time interval during course of a day.

We discuss the proposed scheme from two different points of view: Mobile user's part and network equipment (access router) part.

3.3.1 User point of view

Each mobile user keeps track of its own movement and the offered QoS by the access routers and builds the pattern. Finally the learning model sets up a table in which the fields are the period of time (24 hours interval), two sets of the expected visiting access routers in each specific period of time, the probability of visiting each set of access routers, the QoS requested by user in each period and finally the best chosen anchor among the visiting access routers (see table 3.1).

Hence after a while collection of user information and learning the users' habitude, as soon as a user registers with the network, in the case of following his history, the best anchor for each period of time is known to the MN and it can send update message to the anchor as well.

Table 3.1 An individual user's daily schedule, totally can be different from weekend and holidays

Time Interval	Set of Visited ARs	The probability (%)	Requested QoS	CAP/ Next CAP
7-9	1,2,4,6,7	80	Type II	6/8,6
	1,2,3,4,5	20	Type I	4/8,6
9-12	4,6,8	86	Type II	8/11,12
	5,6,7	14	Type II	6/11,12
12-14	8,11,13,15	89	Type III	11/17,18
	8,12,13,14	11	Type III	12/17,18
14-17	14,15,17,20	97	Type II	17/22
	13,15,18,20	3	Type II	18/22
17-19	21,22,23,24	64	Type II	22/18,2
	19,20,22,24	36	Type II	22/18,2
19-21	17,18,19,20	58	Type I	18/8,9
	1,2,12,13,14	42	Type I	2/8,9
21-24	5,8,9,10	56	Type II	8/2
	6,8,9,11	44	Type II	9/2
0-7	1,2,3	91	Type I	2
	1,2,4	9	Type I	2

3.3.2 Network elements point of view

Concerning the anchors which are basically the access routers, the important parameter which should be considered is network element's capability, as if they can handle a new coming user, fulfilling its requested QoS. For each most probable set of visiting access routers, a suitable anchor is chosen (one for each set). The update with HA happens just once whenever the user joins to the network, and the HA knows the first anchor which serves the user. As long as user follows his habits, so each period's suitable anchor is known. To make the load of signaling to HA even less, the first anchor establishes a chain to the next ones. An incoming packet is forwarded from HA to the first anchor and follows the chain to reach to the user (see figure 3.2).

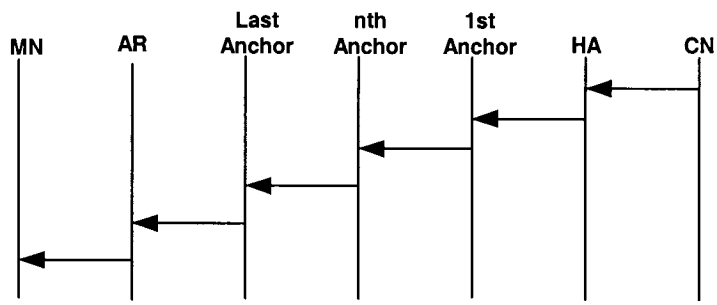


Figure 3.2 Incoming packet delivery sequence

3.3.3 Suitable anchor selection mechanism

As mobile user thoroughly observes its activity, so does an access user. An access router tracks the QoS requested by user and the load charge in a pre-defined timing interval. So it sets up a table which saves the monitoring result of its activity. The table's fields are time interval, in which the monitoring was done, the requested QoS, CPU load, and the number of serving users (see table 3.2).

Table 3.2 Access router's monitoring table

Time Interval	Served QoS	CPU Load	# of users
0-1	Type I	40%	50
1-2	Type II	64%	670
2-3	Type I	57%	240
3-4	Type III	69%	750
4-5	Type I	85%	1000
⋮			⋮
23-24	Type I	75%	821

During the observation period to build the history table, the user collects the info from the visiting access router in each time interval. For example, take a set of most probable visiting access router be: 1, 2, 3, 6, 7 in the morning period between 7 and 9. The user notice that most of the time (ex. 74 %) access router 2 handles the user requested QoS efficiently, and 26% the access router 7 does so. Hence it learns that the suitable anchor for this period of time is access router 2. In case of tie between access routers, the one with the highest valid preference value should be selected.

In simple terms, the steps in selection algorithm are (in case the MN follows its history):

1. The MN must define the most probable movement path along with needed QoS requirement history in a period of time (a set of visited access routers and the requested service from each access router).
2. The QoS aware access router monitors its capability in a predefined set of time as well.
3. MN receives and parses the access routers' capability in term of QoS. Hence MN marks the two most qualified access routers for that specific period based on the AR's life time. AR's life time should be comparable with domain's timing

interval and it goes without saying that the provided capability should stay the same during this period.

4. A chain is established which starts from the first anchor and goes to the next period's selected anchor.
5. As soon as an MN enters a domain, it registers with the new subnet and the domain anchor.

3.3.4 Design scenarios

Here some of the most vital cases in the scheme are discussed: the power-up sequence, the default scenario and the fault tolerance case.

a. Power-up sequence

As soon as the MN powers up, it looks up its table (filled according to history) and identifies the predefined anchor for the time interval. The router advertisement signal acts as verification if the registered router belongs to the identified interval. Figure 3.3 presents an algorithmic view of the sequence.

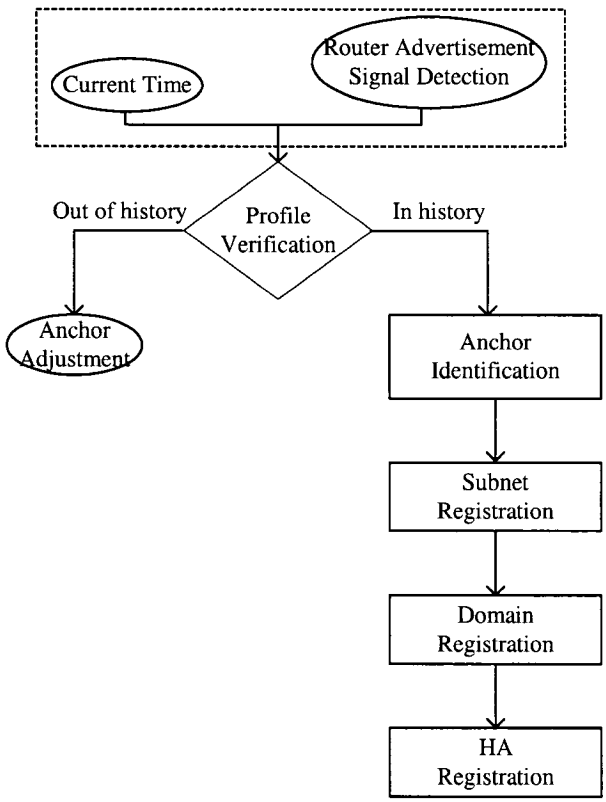


Figure 3.3 MN power up schema

b. Default case

Each MN keeps (and expects to visit) two sets of the most probable access routers and their corresponding "Candidate Anchor Points" (CAP). Generally to overcome the situation where the suitable anchor point is not defined, a long term observation is recommended. But in case when MN cannot register with any expected CAP, a reference anchor point is considered. The reference anchor point is the long term selected anchor. Therefore the default case is still the hierarchical structure with one of the previous high probable selected anchor and not the Mobile IP. Figure 3.4 presents an algorithmic schema of the case.

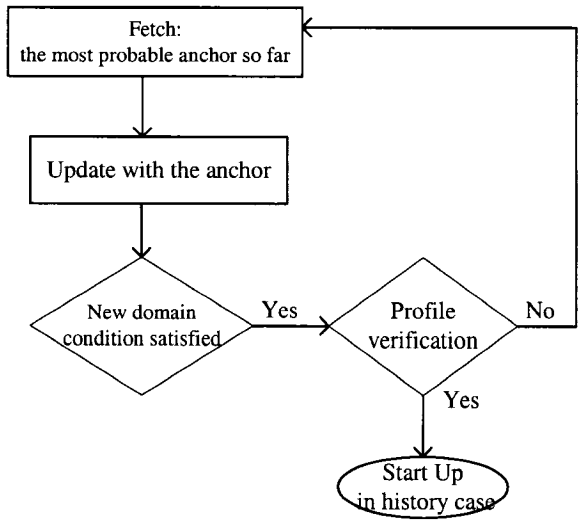


Figure 3.4 Default case schema

c. Anomaly case: Fault tolerance consideration

One of the main deficits of the IETF hierarchical architecture is the anchor point's (MAP) single point of failure issue. To avoid such a problem, here the scheme considers the anomaly case, and the recover strategy. In case of any anomaly which can happen unpredictably in network, the MN should know how to act automatically to recover the failure.

Since in each time interval out of two sets of most probable visiting access routers, the best ones are chosen as the anchors, hence there are two anchors which serve the user at each period. In case the primary option anchor cannot serve anymore the second choice will take the responsibility. As it mentioned before, a forwarding pointer establishes a chain among the chosen anchors as the user moves in time intervals. Considering the case when one of the middle time interval anchors cannot work properly, then the chain is broken. To handle such a problem, the suggestion is to set up multiple chains among the anchors of different levels (see figure 3.4). Having high reliable access routers will end up the extra cost of double chain.

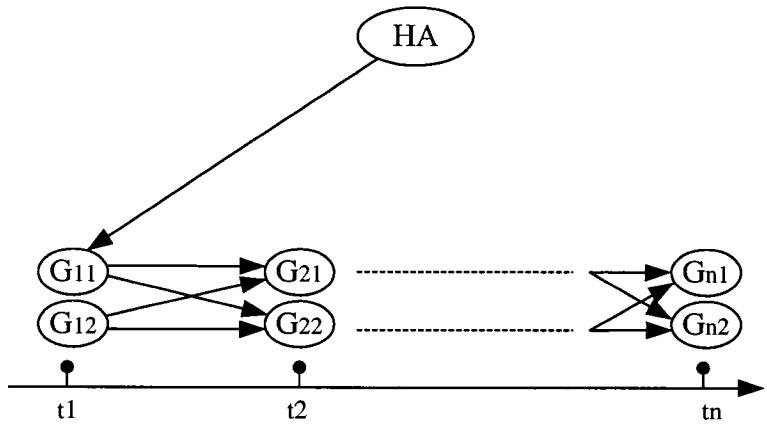


Figure 3.5 Anchor chain establishment

3.4 Protocol design issues

Some of the main points of the scheme are discussed in this section: QoS definition, the preference value consideration to select the most suitable anchor, and the implementation of QoS in signaling flow.

3.4.1 QoS types and preference value

At the time of registration, the MN queries the access router to find out its capability. Moreover it demands its needed service and negotiates with the mentioned access router. Whenever MN terminates a time interval (ex. 7 a.m.-9 a.m.) based on the queried access routers' capability, it designates the most suitable one as its anchor for that specific interval. The QoS definition (traffic classifications) can be categorized according to a set of parameters:

- Delay
- Bandwidth
- Distance between access router and MN's HA

Since transmission cost is a part of total cost, therefore the distance between the access routers and HA is an important parameter to choose the right anchor. If we consider that each packet goes through a specified path, then the number of hops is fixed. Though in reality the path varies according to network situation, we can define a boundary based on time-to-live (TTL) field of IP packet header.

Based on certain threshold for each set of parameters, a QoS type is identified (see table 3.3). In negotiation phase of registration sequence to be brief just type number will be indicated.

Table 3. 3 UMTS QoS type definition

QoS Type	Application Example	Traffic Classification	Delay/Jitter	Bandwidth
Type I	Voice	Conversation class (real time)	Low	Low
Type II	Email	Background class (best effort)	High	Low
Type III	Streaming Video	Streaming class (real time)	Low	High
Type IIII	Web Browsing	Interactive class (best effort)	Medium	Medium

The preference value for each anchor will be defined based on their available resources, which can guarantee a minimum service. Thus according to their preference value, the two most acceptable routers are CAPs.

Let's consider that a low number for preference value represents better choice to select. Therefore for each router in MN's cache table, a preference field is associated.

3.4.2 Signaling exchange sequences

As it is known in Hierarchical Mobile IP, whenever MN moves into a new anchor domain, it receives agent advertisement messages containing information on locally available anchors. Then the update sequences are executed in two levels: local and remote. The local registration updates the address in domain access router level and the remote one updates the anchor address with the HA (see figure 3.6).

In the proposed scheme the signaling flow basically remains the same, except that whenever the user registers with the local access router, it negotiates on the requested service to verify if the access router can be its future suitable anchor.

The QoS negotiation phase can be implemented in two different ways:

Either, implicit notification in which the MN caches AR's QoS capability and tries to deal with the attached router:

- Subnet registration request contains the QoS-specific extensions (measured parameters come later). It indicates the service requested by the user;
- Subnet request reply should notify the MN if the requested service can be provided.

Or, explicit notification in which MN rejects the ARs which are incapable to fulfill its demanded service:

- Agent Advertisement message can be extended to inform the MN of router's capability.

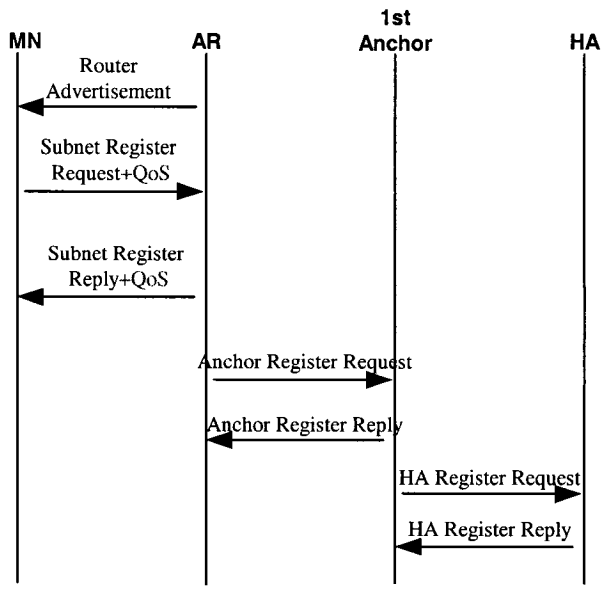


Figure 3.6 Home location registration

3.4.3 Message packet format

As it mentioned earlier, routers' QoS parameters verification can be implemented via either agent advertisement message (explicit way) or registration messages (implicit way).

a. QoS embedded in agent advertisement message

The agent advertisement is the ICMPv6 periodic message destined to (224.0.0.1) in case of multicast addressing, and to (255.255.255.255) for broad cast addressing. The Router Address fields are filled in with the address(es) of the agent.

The Agent Advertisement is basically an ICMP router advertisement message. In addition to the conventional fields, one or more extensions are added to the message format. There are three extensions specified: *the Mobility Agent Advertisement Extension, Prefix-Lengths Extension, and One-Byte Padding Extension.* The extension type 16 determines the mobility agent advertisement.

As figure3.7 shows, there is a single byte of reserved field which can be used as an indication of router's QoS capability.

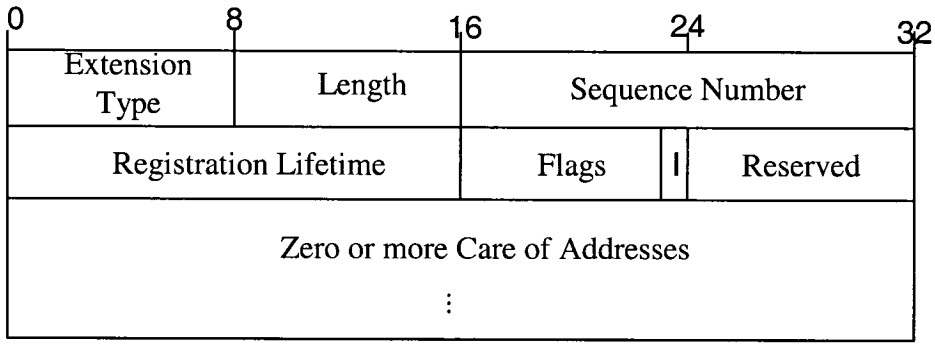


Figure 3.7 Mobile IP mobility agent advertisement extension format

A three bits sequence can handle all the considered QoS levels for each router (see table 3.4).

Table 3.4 QoS indication in registration message format

b1 b2 b3	Indication
000	QoS cannot be met at all
001	Type I
010	Type II
011	Type III
110	Type IIII

b. QoS embedded in registration message

In contrast to agent advertisement which is an ICMP message, the registration messages are carried in the payload of a "User Datagram Protocol" (UDP) message. Therefore, registration is technically performed at a higher layer than the rest of Mobile IP communication. Agents listen for registration requests on well-known UDP port #434, and respond back to mobile nodes using whatever temporary assigned port the node used to send the message. A registration request message is distinguished from registration reply message by the type field. If it is set to 1, it indicates a request, and for the reply message it is set to three. The one byte flag field has two reserved bits at the 6^{th} and 8^{th} place, but unfortunately it cannot be enough in our case (see figure 3.8). Therefore to address all QoS options, the extension field can be used. In the response the same technique specifies whether desired QoS indicated by request message can be fulfilled. The registration message format is presented in figure 3.9. The QoS types are defined based on the same bit structure of table 3.4.

Simultan -eous Binding (S)	Broad -cast Data- Grams (B)	Decap by Mobile Node (D)	Minimal Encap. (M)	GRE Encap. (G)	Reserved (r)	Reverse Tunnel -ing (T)	Reserved (x)

Figure 3.8 Mobile IP registration message: Flag subfield

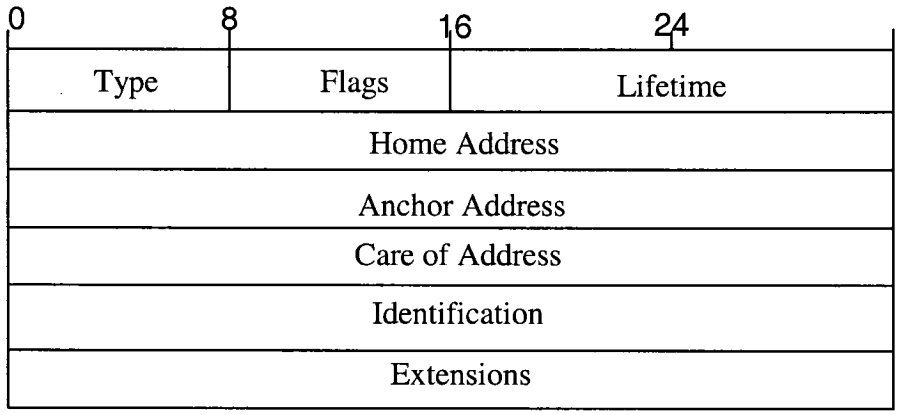


Figure 3.9 Mobile IP registration request message format

3.5 The process of changing history in long term observation

The dynamic characteristic of network causes different situation in long term and consequently affects the choice of best anchor point and the sequence of anchor point's chain. Hence the MN's mobility pattern and the access routers' capability should be observed even after the learning phase. As MN proceeds in the network and registers with new access router, it verifies to find out if the new serving access router matches with the expected access router list in its history. Therefore one by one the actual path's visiting access routers are compared with the built in known path. If it follows the history, then the CAP choice suits well the set of visiting access routers.

3.5.1 Changing the suitable anchor

If MN does not follow its history and deviates from the expected path, then the history based calculated anchor point will not remain the same. Take a sequence of access routers saved by the MN in its history presented in figure 3.10:

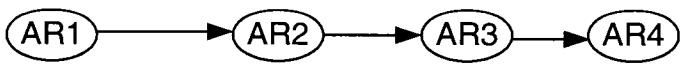


Figure 3.10 An example of an individual MN's history (visited access routers)

And the deviated sequence is considered according to figure 3.11:

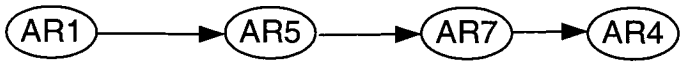


Figure 3.11 The deviated sequence of visited access routers for the same MN

Moreover the selected anchor point for the path is AR4.

According to example, the MN registers with the first access router AR1, and since it matches its history, the algorithm proceeds normally. As it moves, it has to register with the next access router AR5, which is a deviation from what it expected, AR2. Hence the MN saves the provided QoS by the access router and access router's capability in its actual path field. Next it visits AR7 which presents the other deviation and does the same, meaning that MN keeps the deviated access routers' capability and the provided QoS. Changing two access routers in the expected set causes AR4 not to be considered as the suitable anchor. Thus the MN compares the previous anchor point AR4 capability (preference value) and life time with the new visited access routers' one (in this case AR5, and AR7), and takes the one with the highest preference value and agreeable life time . In long term if the probability of the new selected AR increases (passes a certain threshold), then it will turn to be the new designated anchor of the set In figure 3.12 anchor (AR) counts the number of times the AR has been qualified as the anchor during the specified time interval. The mentioned AR will be the new anchor of domain, if the condition [Anchor(AR) > Threshold] is satisfied; which in fact it shows the AR's high probability of being suitable anchor.

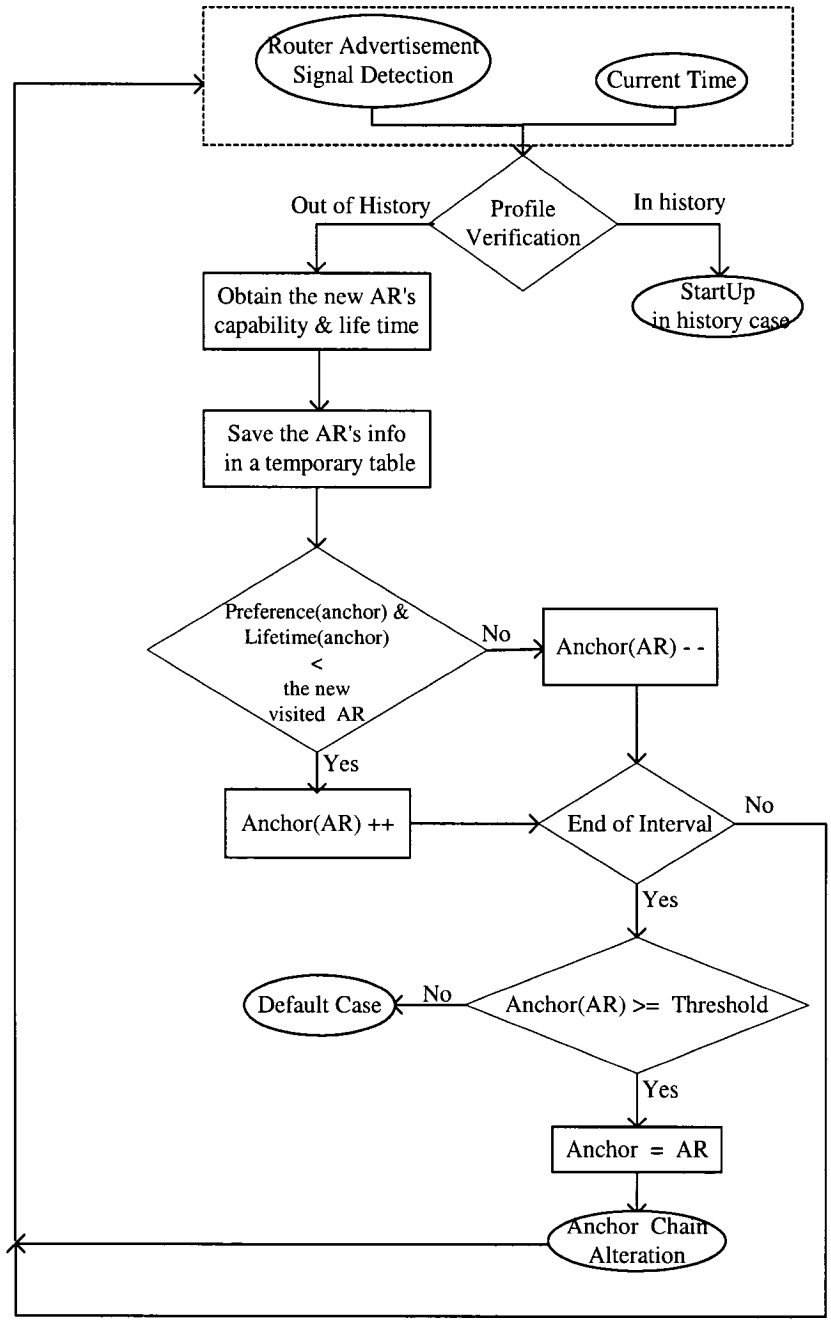


Figure 3.12 Anchor adjustment schema

3.5.2 Changing the anchor chain sequence

Whenever a new access router is designate as the new suitable anchor, then the MN should update itself with the new anchor point for that specific period of time. The

new anchor point sends a signal to the previous and the next anchor to establish a new chain. Otherwise the previous anchor looses the next anchor of the chain. The MN should carry the last anchor point's address in its table to inform the new anchor point about the previous anchor. Otherwise the new anchor cannot find the previous ring of the chain (see figure 3.13).

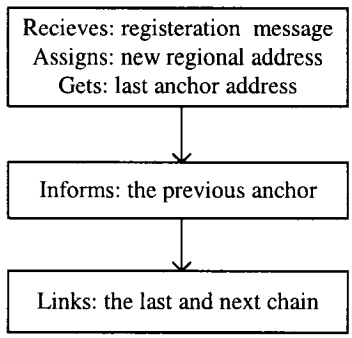


Figure 3.13 Anchor chain alteration schema

In signaling sequence the new anchor informs the last visited (previous) anchor point and in reply gets the next anchor's address to insert itself in the ring (see figure 3.14).

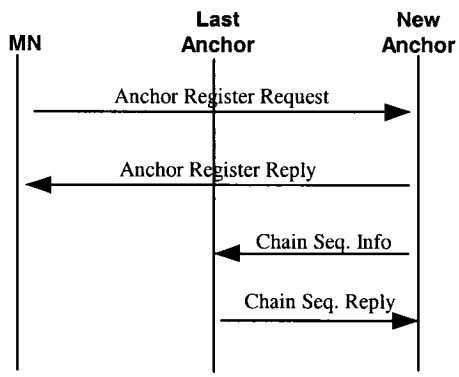


Figure 3.14 Chain establishment signaling flow

3.5.3 Message format

As it mentioned in previous section, in case of deviation from the predefined history path, the new selected anchor should be inserted in the chain and the previous

(disqualified) anchor is supposed to be discarded as well. Below the exchanged message formats are discussed:

a. The anchor registration message format (request & reply)

The message format is presented in figure 3.15. It consists of:

Type: identifies if the message is the anchor register request or reply.

Lifetime: as usual represents the message validity period.

Reserved field: is considered for future needs.

Home Address: specifies the MN's home address.

Care of Address: with the home address identifies the MN to the anchor.

Last Anchor Visited Address: the address of the last serving anchor. In case of the anchor registration reply, it assigns a new regional address to the MN.

Identification: protects against replays and allows the acknowledgment to be associated with a pending message.

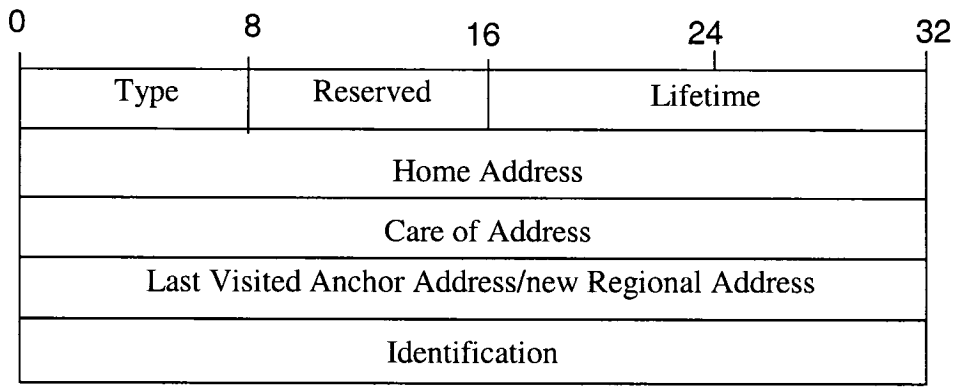


Figure 3.15 Anchor registration format

b. Chain sequence info and chain sequence reply message format

The only difference with the anchor registration is the Next Anchor Address field. In case of info type it just informs the last anchor of its address while reply message contains the next expected anchor address (see figure 3.16).

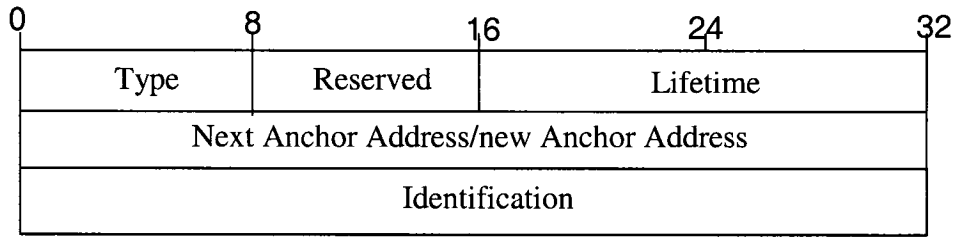


Figure 3.16 Chain sequence message format

3.6 Possible performance improvement

Some points can be involved directly in performance improvement of the proposed scheme: forwarding pointer loop removal, domain update criteria, and QoS based paging.

3.6.1 Loop removal

As it was supposed that mobile users move in a limited area, and sometimes they back and forth due to geographical restraints, or some other temporary demands (traffic or constructions,...), in consequence a loop may form which leads to delay in packet exchange to MN, more signaling cost and also more load on the AR. For example take CAP1, CAP2, CAP3, CAP2, CAP4, and CAP4, a sequence of the most suitable anchor points of an individual user in a sequential time interval. Hence the user movement form two loops, between CAP2, and CAP3, and the other is a self-loop on CAP4. Figure 3.17 is to give a clear view of the observed problem.

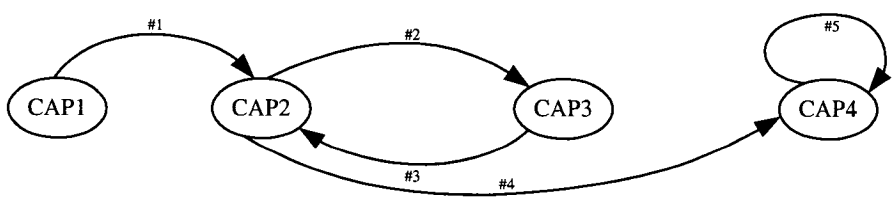


Figure 3.17 Loop creation among the candidate access points

One way to remove such a loop is to ignore the intermediate movements which terminated with the starting point. Meaning that in case of CAP2, CAP3, and CAP2, CAP3 is ignored and just CAP2 will be in the next CAP of the MN's table.

3.6.2 Domain update criteria

How to define the monitoring period and MN's suitable period of time? As it discussed before, a QoS parameter (requested, offered) embedded in registration exchange messages clears if the router can be a CAP, or not. But the problem arises considering the fact that the router should be qualified for the whole period of time interval (domain), and not just during registration time. So the router should inform the MN of its capability for that specific domain, and practically reserve the promised QoS for the time interval. Otherwise, a life time shows the validity period of router's capability.

The idea how to model the moment that MN leaves a domain for the next one is based on [33]. But in the mentioned article the load on the network equipment was not counted. To define each anchor's boundary we count on:

I) Processing Load on each anchor: If it exceeds a pre defined threshold and the cost of traversing to the next anchor is less than processing load.

P_i $[L>L_{th}]$ signifies the probability that processing load of the i^{th} anchor passes the amount of threshold.

II) Resident time in the registered subnet: If an MN stays there more than the average resident time, then the domain will be terminated with the mentioned subnet (see figure 3.18). The threshold value t_r is defined based on each user's history, and hence is unique to each mobile user.

P_r $[t_i> t_r]$ signifies the probability that an MN resides more than usual.

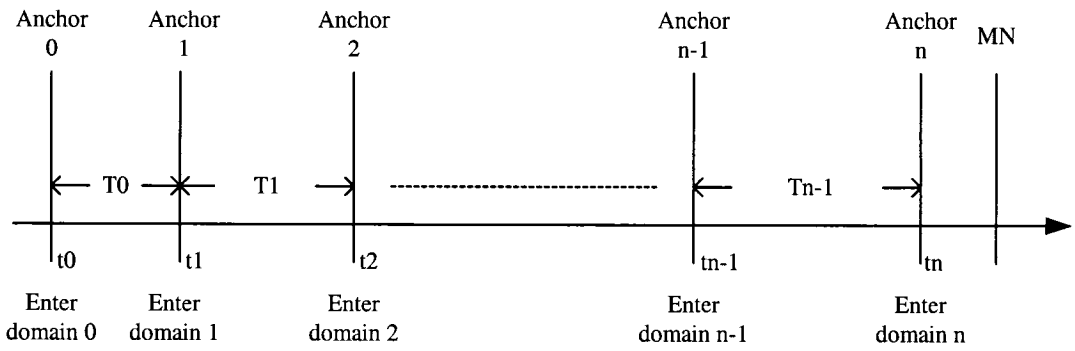


Figure 3.18 Timing diagram 1

III) The call arrival rate: Since changing domain (and consequently anchor) provokes an inter domain handover in the middle of call duration, hence it would be better for the MN to be in idle state before transition from one anchor to the new one (see figure 3.19).

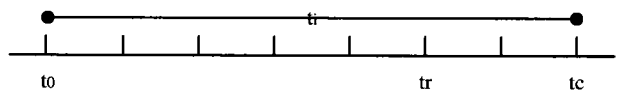


Figure 3.19 Timing diagram 2

P_r $[t_i < t_c]$ signifies the probability of any time when there is not any active session.

So the probability that an MN moves out of its regional domain according to the above mentioned parameters will be:

$P_t = P_r [t_i > t_r] * P_r [t_i < t_c] * P_i [L > L_{th}]$

3.6.3 QoS based paging

Basically MN registers with the anchor its new obtained LCoA whenever it changes the subnet. As a result the anchor knows the MN's precise location and forwards the packet directly to its destination. In case of delay sensitive application, local update is a must, though it increases local signaling load. Otherwise the anchor can just keep approximate location information of MN in its domain, meaning that the MN updates with the anchor once when it enters the domain. In order to deliver a packet

addressed to such an MN, the anchor has to page all over the domain. Obviously such an option can be rather proposed for the time trivial applications (see figure 3.20).

Hence, according to the MN's desired QoS, the MN and the anchor can deduce if the paging should be applied for that specific time interval. But to be able to apply such a strategy, the MN should demand for the same service in the whole subnets of the domain.

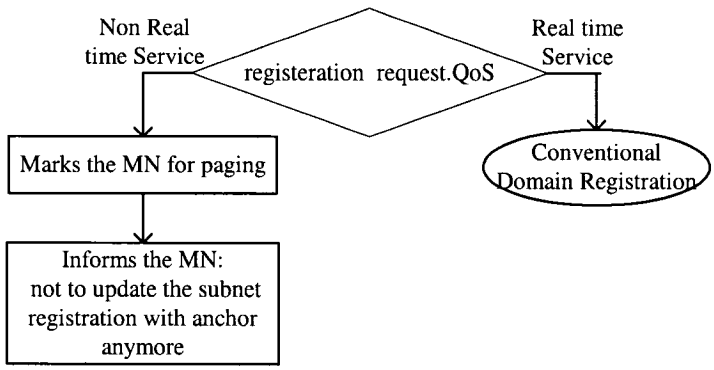


Figure 3.20 QoS based paging

3.7 The achieved design's goals

Certain features were pointed out by the proposed scheme:

- Distributed database: each MN keeps its own location information path and each access router monitors and keeps track of its activity. No centralized structure which avoids single point of failure issue. Moreover in each time interval a specific region is formed for the user (according to its profile), hence a dynamic, time variant region structure is the result. And since different mobile users have their own appropriate anchors, consequently the mobile host's registration load and mobility management load are distributed;
- The data are stored as soft state: since the AR's state is periodically updated in MN's cache via either above mentioned ways (see section 3.3.1), consequently a robust protocol is achieved;
- MN does not need to know about network topology, it learns the profile of each user through its history;

- Scalability: as it is based on HMIPv6, the HA and CN are unaware of users' movement thus signaling updates reduction to HA make the scalability easier, and more mobile users can be served by HA;
- QoS: in best anchor selection, as it mentioned in section 3.3.2, efficient use of access routers' resource is as important as its ability to provide a certain level of satisfying service (bandwidth, delay ...) to the mobile user;
- Load Balance: It consists of data flows being redirected to vacant anchors (mobility agent) rather than packets being de queued and moved among them. Hence it eliminates the overwhelming a specific anchor;
- Reliability: CAPs are obtained via two sets of the most probable path taken by MN.

To summarize, a satisfying performance balance (to reach higher bandwidth utilization, throughput, and lower delay) among the network involved equipments in a dynamic environment is the demanding part of the scheme.

3.8 Analytical model

In this section, we calculate the cost function of the proposed scheme through an analytical model development. Like the other works in this subject [17] [19], the periodic binding updates sending by an MN to its HA or AR are not taken into account. It should be noticed that the cost calculations are valid just for an individual user case, since the subscribers' movement pattern are completely independent.

Furthermore the scheme supposes that MN just once updates itself with the new anchor whenever it moves to the new domain, meaning that it just informs the anchor of its entrance. Consequently there is no need to register its LCoA with the anchor while it changes the subnet in the same domain. At the packet delivery time, the anchor reaches the destined MN through paging to all the served MNs of its domain.

3.8.1 Scheme cost

The performance metrics considered for total signaling cost are location update and packet delivery.

a. Location Update Cost

Location update is done in two levels, from the anchor to the HA and from the subnet AR to the suitable anchor. Obviously the domain size affects the location update cost. In IETF Mobile IP regional registration, the number of home registration increases as a result of small domain. In case of our scheme the small domain causes chain traversing cost.

A set of parameters are defined to calculate the location update cost:

P: probability that the MN follows its history

λ_r: mean time a user resides in a given subnet

$C_{tot.}$: total location update cost

$C_{prof.}$: location update cost in case the MN moves according to its profile

$C_{non\text{-}prof..}$: location update cost in case the MN derives from its history

a_h: location update processing cost at HA

a_f: location update processing cost at AR

a_g: location update processing cost at anchor

C_{hg}: traversing cost from HA to the first anchor

C_{gf}: traversing cost from first anchor to the AR

C_{fm}: update cost from MN to the new subnet

C_{gg}: traversing cost from one anchor to the next one

The total location update cost for an individual user is:

$$C_{tot} = P.\, C_{prof.} + (1\text{-}P).C_{non\text{-}prof} \quad (3.1)$$

The location update cost in case of following the history is composed of three parts; the home registration cost, the domain-wide local registration cost, and the cost that comes from moving along anchor chain:

$$C_{prof} = C_{Uh} + \sum_i C_{Uri} + \sum_i C_{anchor\, i} \quad (3.2)$$

Let C_p denote the anchor's total location update cost which is composed of the processing cost at anchor, and traversing chain cost:

$$C_{pi} = a_{gi} + C_{ggi} \quad (3.3)$$

$$\sum C_{anchor} = P_{t0} \cdot C_{p0} + P_{t1} \cdot C_{p1} + P_{t2} \cdot C_{p2} + \ldots + P_{tn} \cdot C_{pn} \quad (3.4)$$

What we are looking for is to define the P_{ti}, the probability of occurrence of the set $\{t_0, t_1, t_2, \ldots, t_n\}$, which denotes the changing domain time for each user. Though is suggested to make a daily anchor chain, but in reality it affects the packet delivery cost. Therefore the chain is established alternatively, meaning that the length of the chain is always 1.

Suppose the residence time of an MN in a subnet and the call arrival rates are both Poisson processes and respectively the density function of t_r and t_c are:

$$f_c(t) = \lambda_c e^{-\lambda_c t}, \; f_r(t) = \lambda_r e^{-\lambda_r t} \quad (3.5)$$

Then,

$$P_r[t_i > t_r] = \int_0^{t_i} \lambda_r e^{-\lambda_r t_r} dt_r = 1 - e^{-\lambda_r t_i}, \; P_r[t_i < t_c] = e^{-\lambda_c t_i} \quad (3.6)$$

Moreover, let assume that signaling load on each anchor is of exponential distribution:

$$f_i(t) = \frac{1}{\beta} e^{-\frac{t}{\beta}}, \quad (3.7)$$

where β is the mean load value which can be defined per anchor capability, and is user specific and in a more complicated case can be time variant parameter. And finally,

$$P_{ti} = P_r[t_i > t_r] * P_r[t_i < t_c] * P_i[L > L_{th}] \quad (3.8)$$

$$\sum_i C_{anchor\,i} = \sum_i (P_r[t_i > t_r] \cdot P_r[t_i < t_c] \cdot P_i[L > L_{th}]) . Cp_i \quad (3.9)$$

Therefore each time stamp t_0, t_1, ... signifies the case in which P_t happens with high probability.

Consequently, according to the signaling message flows for location registration, the bottom line is:

$$C_{prof} = C_{Uh} + \sum_i C_{Uri} +$$

$$\sum_i (P_r[t_i > t_r] \cdot P_r[t_i < t_c] \cdot P_i[L > L_{th}]) . Cp_i \quad (3.10)$$

Though the t_i value represents the continuous daily time interval, but here we assume as soon as the MN registers with new subnet, it resets the timer. Hence with changing each subnet, the new subnet residential time is taken into account.

It is obvious that the higher probability that an MN sticks to its profile, the more the total cost depends on C_{prof} value. This is what we expect to see in most of the cases.

According to the formula introduced in [19], the upper bound of the total location update cost per unit time is:

$$C_{LU} \leq \frac{E(M).C_{ur} + C_{uh}}{E(M)tr} \tag{3.11}$$

where E(M) is the expectation of the moment at which an MN moves out of regional network. In our case such an expectation is calculated:

$$E(M)= \lambda_r . P_r [t_i > t_r] + \lambda_c . P_r [t_i < t_c] + (\text{number of subnets in the domain}).P_i [L > L_{th}] \tag{3.12}$$

And C_{Ur}, C_{Uh} are home location and regional costs:

$$C_{Ur}= 2.[a_f+C_{gf}+C_{fm}]+a_g \tag{3.13}$$

$$C_{Uh}=2.[C_{hg}+ a_g]+a_h \tag{3.14}$$

b. Packet delivery cost

The cost of routing a tunneled packet from the HA to its destination MN forms the packet delivery expense in the network.

Suppose,

V_h: packet delivery processing cost at the HA

V_g: packet delivery processing cost at the anchors

T_{hg}: traversing cost of packet delivery from HA to the first anchor

T_{gf}: traversing cost of packet delivery among the anchors

Based on [17] and [19] the packet delivery cost is:

$$C_{PD} = T_{hg} + T_{gf} + V_h + V_g \tag{3.15}$$

The processing cost at HA is:

$$V_h = \eta.\lambda_c \tag{3.16}$$

where η is packet delivery processing constant cost at HA, and λ_c is packet arrival rate.

The packet processing load of the anchor is directly under effect of the number of visiting users in the total subnets of domain (K). Hopefully in case of distributed system, the load is evenly scattered among the different anchors.

$$V_g = \varsigma K \,.\, \lambda_c.(\alpha\omega + \beta \log(K)) \tag{3.17}$$

(3.16) presents the packet delivery cost function at the anchor, where $\varsigma, \omega, \alpha, \beta$ respectively are constants related to bandwidth allocation cost, the number of users in each subnet, and weighting factors of visitor list and routing table lookups.

CHAPTER IV

ANALYSIS OF RESULTS

So far we have seen the intrinsic problems associated with hierarchical mobile IP structure. These problems are due to the usual deficits of centralized architectures. Then in the previous chapter a distributed dynamic structure was proposed which is based on the individual user's mobility pattern and its long term history of activity. The performance and suitability of the proposed scheme is to be evaluated in this chapter. The scheme has been analyzed and checked by a tool box for validation and verification of real-time systems called UPPAAL. The second part of evaluation is through analytical comparison of the scheme with the other two distributed dynamic structures in the literature. Shortly we go through an introduction to UPPAAL, and then the modeled timed automata with the verified properties are presented. At the end, the analytical results are discussed.

4.1 Validation tool box: UPPAAL (UPPsala-AALborg university)

Formal verification of protocols goes through different stages:

- Modeling system: a description of system;
- Definition of system's properties: what a system is expected to handle;
- Verification: Whether a model corresponds to the system's properties and constraints.

In our case the system's model is based on transitions in which a process starts at an initial state and goes through intermediate steps via transitions. A timed automata model checking toolbox, UPPAAL, is chosen to verify the validity of the proposed model.

UPPAAL is known as «an integrated tool environment for modeling, simulation and verification of real-time systems» [32].

It is composed of three modules:

I) A description language which explains characteristic of systems through non-deterministic guarded commands with the help of clock and data variables.

II) A simulator which examines the system and detects the possible faults in system behavior.

III) A model-checker explores the state-space of the system to verify the stated constraints and properties through exhaustive search. It is supposed to deal with all possible dynamic characteristics of the system.

UPPAAL is finite state machine with clocks to deal with time. Time is a continuous global variable which proceeds for the whole system at the same pace. Concurrent processes, each as an automaton form a system in UPPAAL. To model graphically a system, the automaton should be placed. The transition from a location to the other one is controlled though guards and synchronization. Usually a guard applies a condition on the variables and clocks to handle transitions. At transition time, handshaking style synchronization can be applied through globally introduced channels to verify the cooperation between different elements of the system.

4.2 Models, properties and verifications of the system

QoS binding, QoS paging and anchor adjustment are the cases which have been modeled. The modeling is based on the system description of third chapter.

The classical properties which are usually verified are: safety, liveness, accessibility, and the absence of deadlock. Safety property assures that unexpected anomaly case will not happen in the system. Liveness observes that with certain conditions, the system should reach to a specific state. For example this property can be used to check if the system is able to respond in a finite time. Obviously accessibility verifies if a situation is accessible or not. Finally the system should be deadlock free.

4.2.1 QoS Binding

I) The model

It is based on the signaling exchange sequence of section (3.4.2) in the previous chapter. Figure 4.1 shows the timed automata of QoS binding.

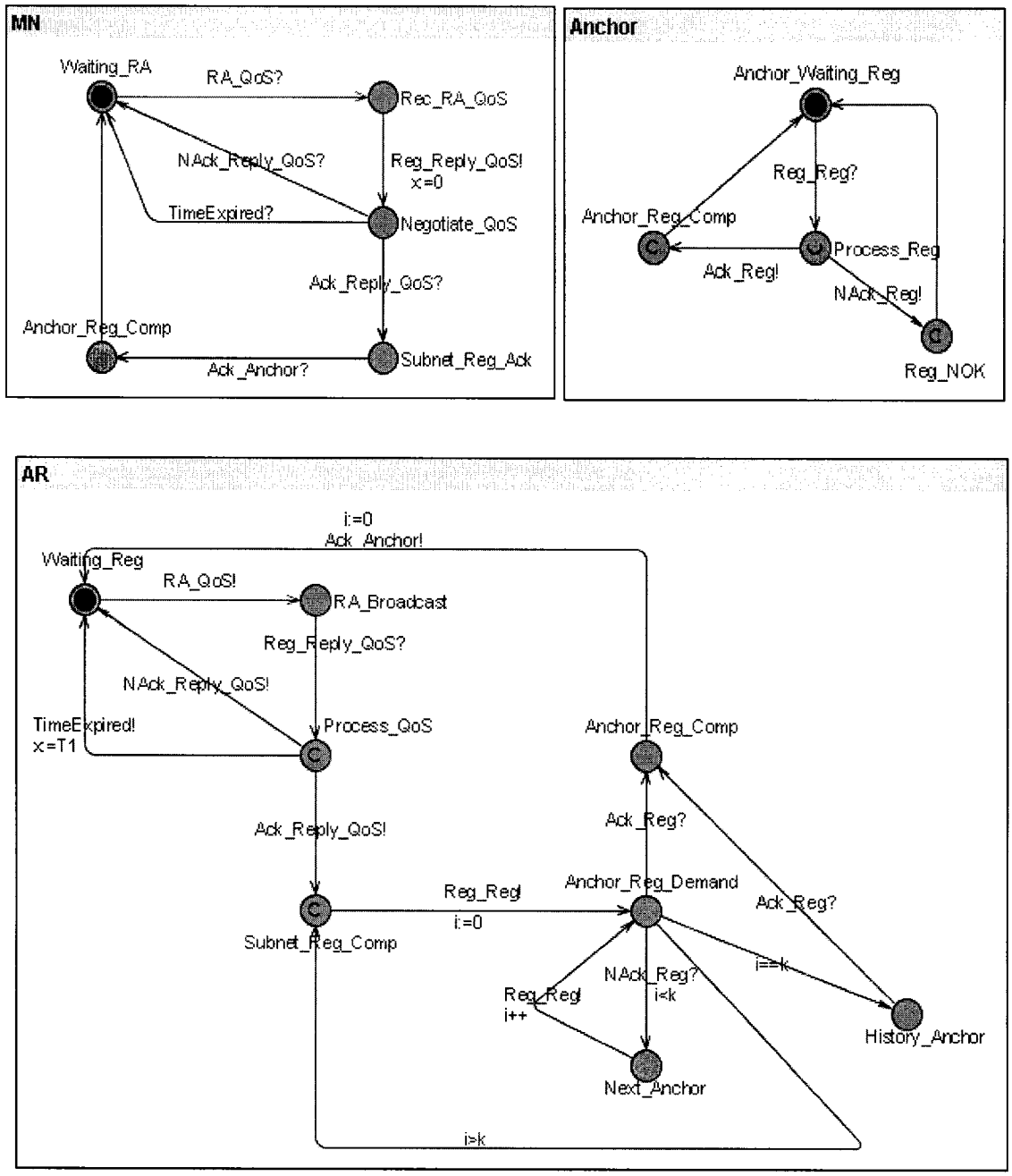


Figure 4.1 QoS binding timed automata

II) The properties

Safety: The MN should register with one anchor, either according to its profile or the most visited anchor during its activity (whenever the MN does not follow its profile).

Liveness: The MN's request to register with the subnet should be responded in a finite time from the involved access router's side.

Accessibility: The stages of system should be visited even once.

Deadlock: There is a predefined syntax in the UPPAAL.

III) Verification

Figure 4.2 shows that the above mentioned properties are satisfied.

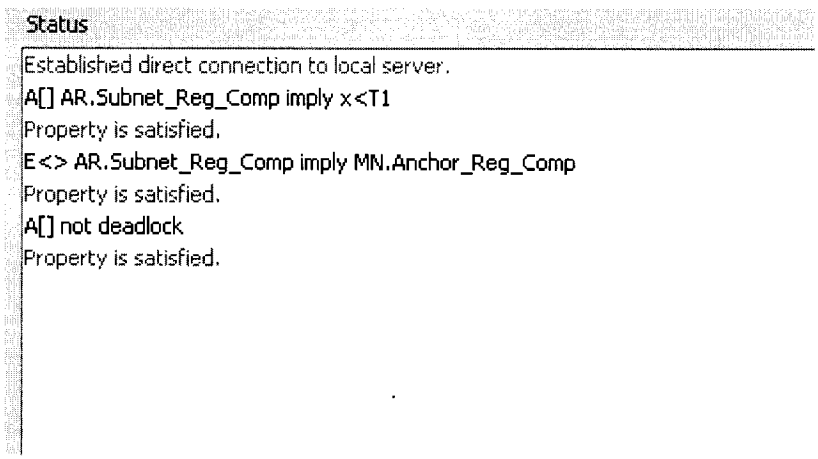


Figure 4.2 QoS binding: a view of verified properties

4.2.2 QoS Paging

I) The model

It is based on the description of section 3.6.3 of the previous chapter. Figure 4.3 shows the timed automata of the process.

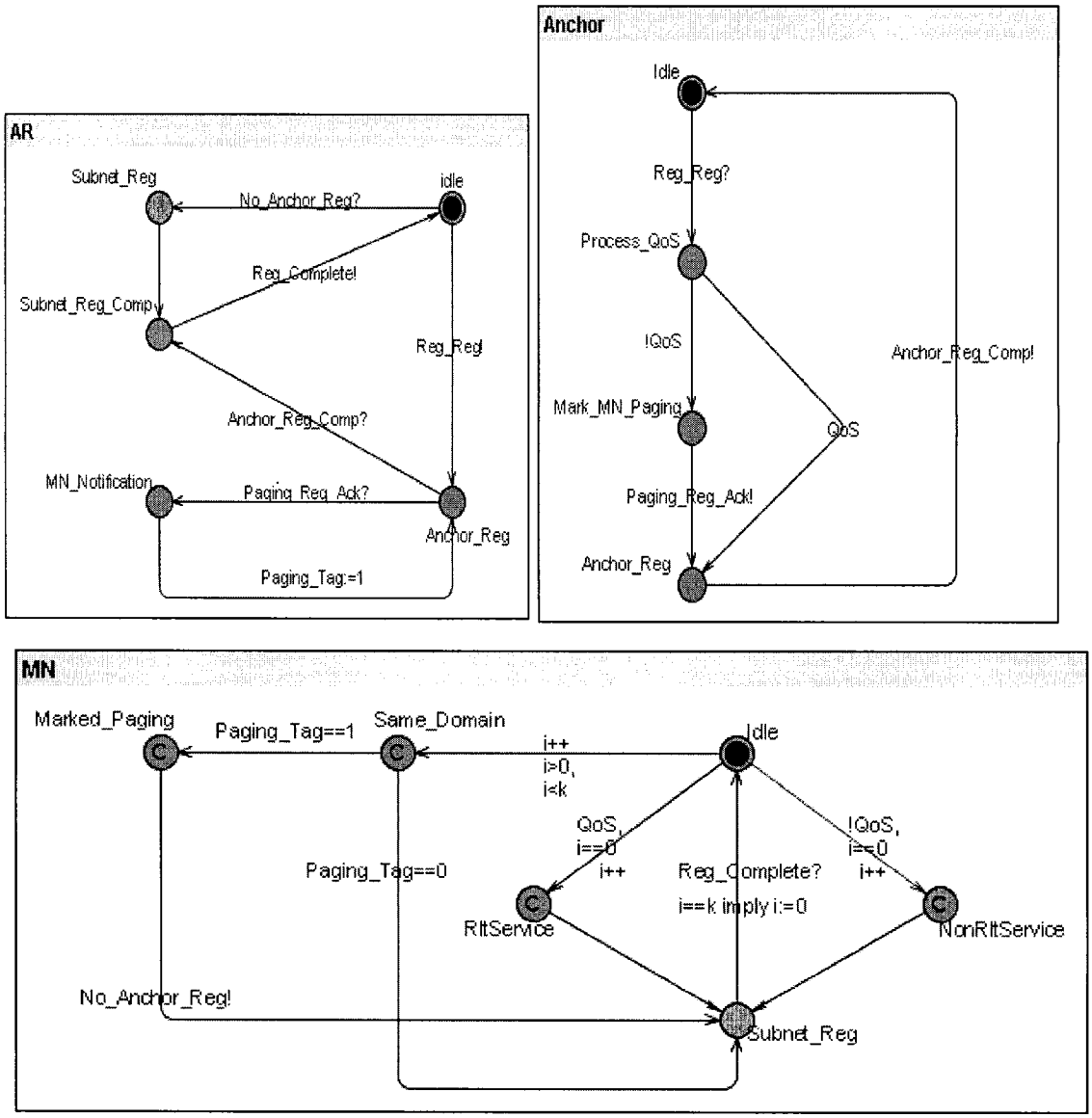


Figure 4.3 QoS paging timed automata

II) The properties

Safety: the state when the MN is out of domain (starts a new domain), but still is judged based on its previous domain's service request.

Liveness: As long as the MN stays in the same domain, its service request represented by paging_tag never changes.

III) Verification

Figure 4.4 shows that the above mentioned properties are satisfied.

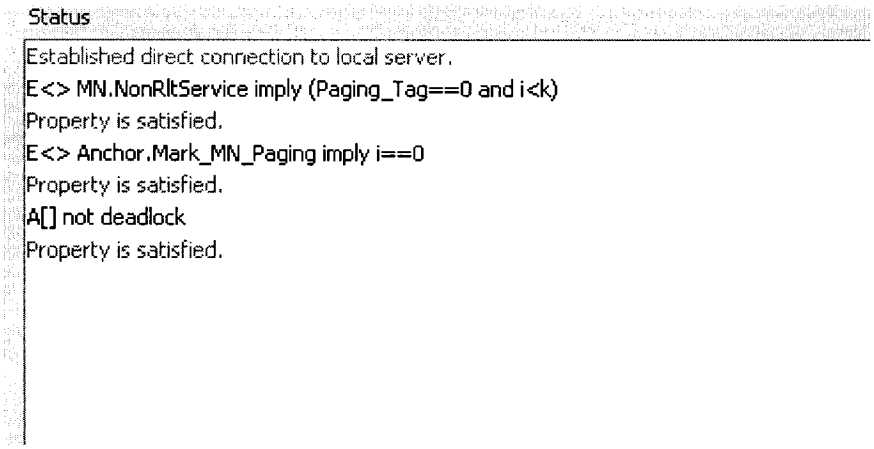
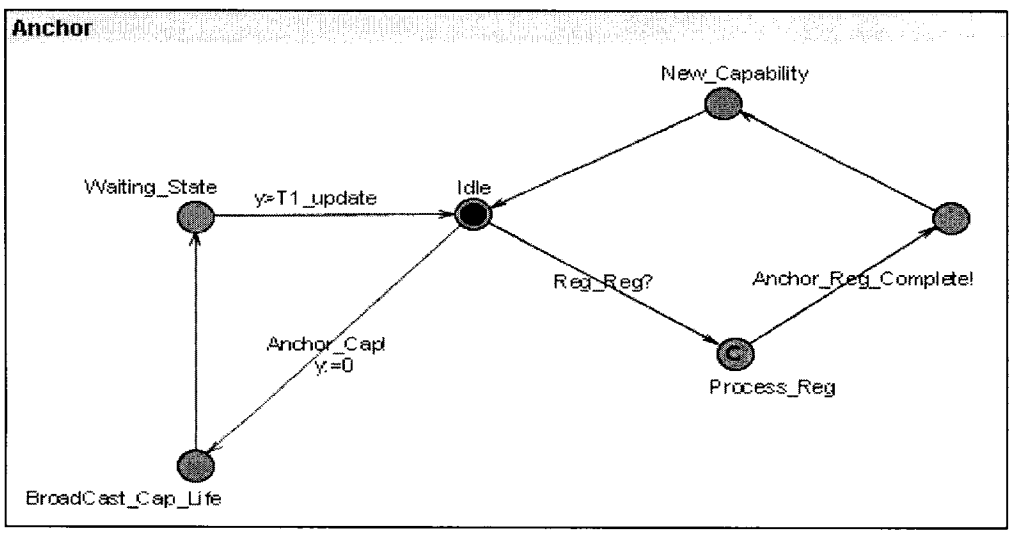


Figure 4.4 QoS paging: a view of verified properties

4.2.3 Anchor adjustment

I) The model

It is based on the description of section 3.5.1 of the previous chapter. Figure 4.5 shows the timed automata of the process.



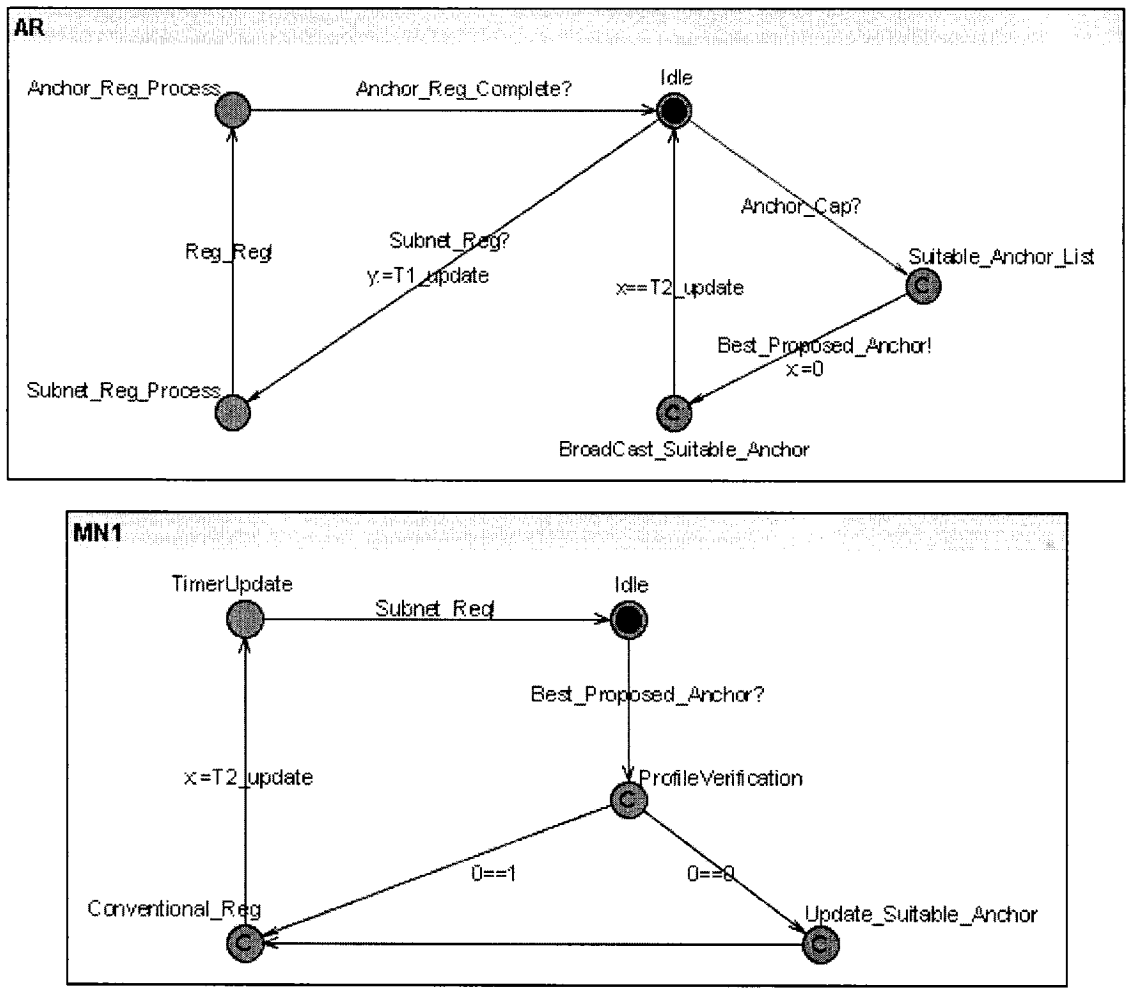


Figure 4.5 Anchor adjustment timed automata

II) The properties

Safety: The MN should register with the most updated suitable anchor.

Liveness: The MN should decide if it following the history or not in a bounded time delay (T2_update).

III) Verification

Figure 4.6 shows that the above mentioned properties are satisfied.

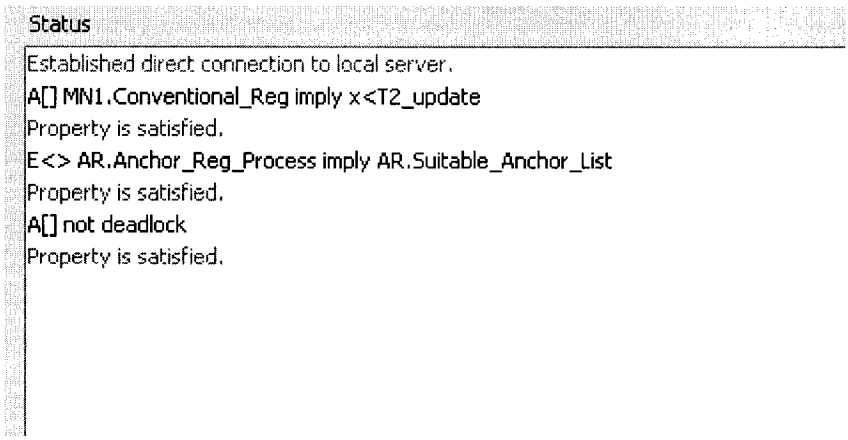


Figure 4.6 Anchor adjustment: a view of verified properties

4.3 Performance evaluation and results

The analytic model of the scheme is compared with two relatively similar proposals:

1) Dynamic Hierarchical Mobility Management Strategy for Mobile IP Networks[17]
2) A Distributed Dynamic Regional Location Management Scheme for Mobile IP[19]

The above mentioned schemes (DHM and DDR) are quite well known in literature and both outperform HMIP in terms of location update cost and packet delivery cost. Hence the proposed scheme (HBAS) can be justified according to the defined measurement parameters and formulas. Moreover the scheme is compared with the general concept of Mobile IP regional registration structure. In fact the centralized system as a traditional reference point gives a general view, though the architecture is completely different. The article's schemes are discussed in detail in chapter 2, sections 2.8.4 and 2.8.7 respectively. Here we just have a brief look at the centralized scheme and the articles' idea once more.

In this chapter the centralized scheme represents the notion of Mobile IP regional registration structure in which the domain never changes no matter how specific users wander and remain the same under all conditions. The other property of such a system is that just one single anchor is in charge of the domain. That is why it is referred as a

centralized scheme. In contrast the proposed scheme can be categorized under distributed and dynamic system in which every characteristic of the domain is adjusted based on individual user movement. Figure 4.7 shows a simplified topology of the centralized scheme and the proposed one. The very first difference is the update sequence which in case of the proposed structure does not have to be done with the HA whenever the MN updates itself with a new domain. Furthermore the domain definition is not fixed for the different users in our proposed system.

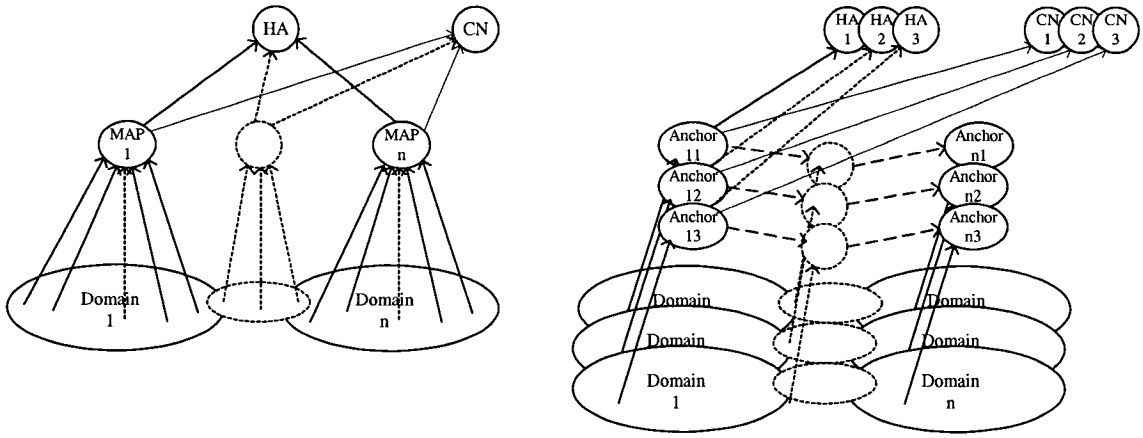


Figure 4.7 Abstract view of centralized and proposed scheme

According to the first article (we call it DHM), the MN updates itself with the first "Foreign Agent" (FA) of domain designated as the anchor agent (in the article called "Gateway Foreign Agent", GFA). Then it visits K different FA which represents domain's size (see figure 4.8). Each new FA registers the new visited MN's address with the previous one, and sets up a hierarchy of FAs. Though the scheme proves to be better than the other one in one aspect, it has its own specific week point as well, which will be analyzed later in sections 4.3.3 and 4.3.4.

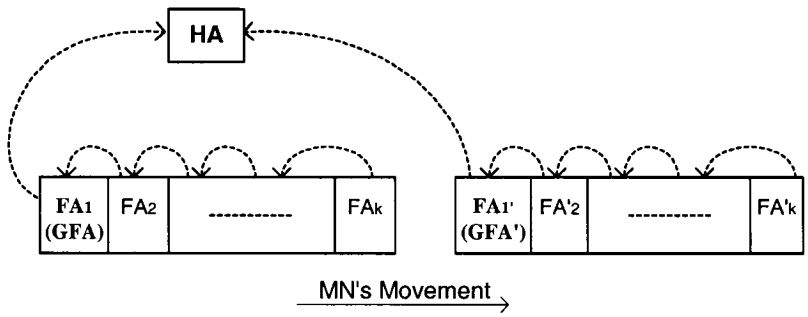


Figure 4.8 DHM scheme view

In the second article (we call it DDR), like the previous one, the first encountered FA of the network is designated as MN's anchor. Here again the individual user passes K number of subnet, hence the domain boundary is defined by the number of visited FA (see figure 4.9).

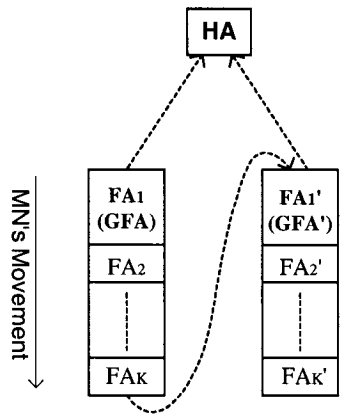


Figure 4.9 DDR scheme view

In both cases the optimal number of subnets which is called K_{opt} in the domain is defined based on each individual mobility pattern. K_{opt} is obtained via an iterative algorithm which tries to minimize the cost function. It can be updated every time MN enters a new subnet, or when the previously calculated threshold is reached or the MN calculates it periodically. Therefore the turning point in both those two models, DHM and DDR is the optimal number of visited FA under control of each domain, K_{opt}.

Moreover though the structures of the two mentioned articles seem simple, but the main part which is calculation of K_{opt} makes the task difficult for the network operators.

4.3.1 Analysis parameters

Here are the parameters used for cost calculation of all schemes:

Table 4.1 The parameters' value for performance analysis

Processing Cost			Transmission Cost				Pkt Delivery Constants					# of subnets
a_h	a_g	a_f	C_{hg}	C_{gf}	C_{ff}	C_{fm}	α	β	# of MNs in a subnet (ω)	η	γ	N
25	15	10	400	200	50	20	0.3	0.7	15	0.01	0.15	50

where a_h , a_g , and a_f are packet processing cost of HA, anchor, and access router respectively. C_{hg} , C_{gf} , C_{ff} , and C_{fm} in the order given are transmission cost between HA and anchor, anchor and access router, two neighboring access routers and one access router with its attached MN. α , β are weighting factors of visitor list and routing table lookups and η is packet delivery processing cost constant at HA. γ is location update loading weight at anchors.

Figure 4.10 shows the effect of different transmission cost. As it is expected the graph is shifted up and down in respect to the increase and decrease of the value. Changing the processing cost demonstrate in the same way less severe impact. For the rest of this chapter the values presented in the table will be the reference value.

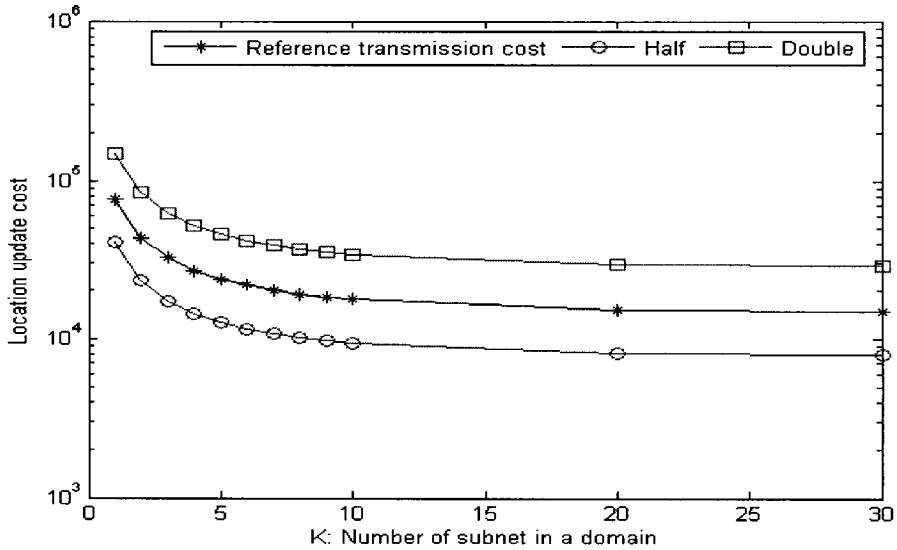


Figure 4.10 The effect of different transmission cost on location update cost

4.3.2 Expectations

As it mentioned in previous chapter, according to [19] the expectation of the moment at which an MN moves out of a domain has a defining role in location update cost formula. For different schemes the following formula is used:

$$E(M) = 1 + (N-1)/(N-K), \quad \textit{for centralized structure} \tag{4.1}$$

$$E(M) = 1 + (N-1)\sum_{i=1}^{K} 1/(N-i), \quad \textit{for DDR} \tag{4.2}$$

$$E(M) = \lambda_r * P_r [t_i > t_r] + \lambda_c * P_r [t_i < t_c] + K * P_i [L > L_{th}], \quad \textit{for HBAS} \tag{4.3}$$

$$\alpha(i) = \frac{(1-g)^2 g^{(i-1)}}{\rho}, \quad \textit{for DHM} \tag{4.4}$$

The authors in [19] propose a general formula (4.2) for the case in which the anchor changes for each user of the domain and does have a dynamic boundary respect to each user movement (called distributed system). We devised our own formula (4.3) driven from [33] which considers the load on the anchors and decides to start a new domain

based on MN's residence time, and call arrival rate. According to [17], $\alpha(i)$ denotes the probability that an MN crosses i subnets between two consecutive packet arrivals, and calculates the signaling costs respectively. In the above mentioned formula (4.4), g represents subnet residence general density function and ρ is the MN's CMR. For the sake of integrity, we take the DDR's formulas as the reference point, since it is more comprehensive than DHM's.

Figure 4.11 shows that the expectation of DDR, DHM and HBAS is obviously larger than the centralized scheme. It should be noted that centralized scheme expectance is a constant value related to the number of visited subnets. That is due to the fact that the scheme's architecture is fixed. The number of subnet in a domain (K) affects the expectation of (4.2) in a linear way; while in (4.3) K impacts the location update load processing at the anchor in an exponential probability function. That is why after a while HBAS' expectation is stabilized and the other two schemes always increase. Any how the advantage is that the number of home registration per unit time in a distributed system like HBAS is less than a centralized scheme.

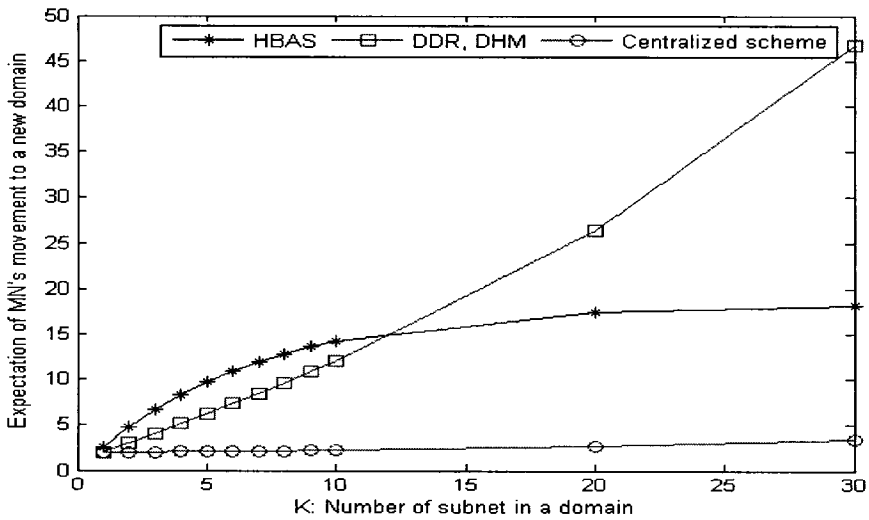


Figure 4.11 Comparison of different scheme's expectation under variable subnet number

4.3.3 Location update cost

According to [19], (4) is a general formula which gives the upper bound of total location update cost per unit time:

$$C_{LU} \leq \frac{E(M) * C_{ur} + C_{uh}}{E(M)tr} \quad (4.5)$$

Obviously each scheme's expectation and home, regional registrations result in different values as location update cost.

$$C_{Uh}=2[C_{hg}+ a_g]+a_h \quad (4.6)$$

$$C_{Uh}=2[C_{hg}+ a_g + C_{fm}]+a_h \quad (4.7)$$

$$C_{Uh}=2[a_f +C_{hg}+ a_g + C_{hg}+C_{fm}]+a_h \quad (4.8)$$

$$C_{Ur}= 2[a_f+C_{gf}+C_{fm}]+a_g \quad (4.9)$$

$$C_{Ur}= 2[C_{ff}+C_{fm}]+3a_f \quad (4.10)$$

$$C_{Ur}= 2C_{fm}+a_g \quad (4.11)$$

The formulas indicated by (4.5), (4.8) are the home location and regional registration costs for HBAS. Moreover, (4.6), (4.8) and (4.10) address the same costs for DDR. It should be noticed that regional registration in this case is a bit different when the MN roams in the anchor's subnet comparing to the conventional case. Finally (4.7) and (4.9) give the same costs for DHM.

Since in HBAS the MN just update itself once with the HA, and the other times a chain is established between the anchors, so two scenarios are considered for location update cost.

I) The first time when the MN registers itself for the first time with the HA.

II) When the MN moves out of the domain. In this case, MN in both other schemes does a home location update again while HBAS establishes a chain between the anchors.

Moreover we can analyze system behavior in two different aspects, either based on the number of subnets in the domain, or the individual user's average residence time.

a. Location update cost versus the number of subnet in a domain

Figure 4.12 shows that HBAS is as good as DDR, while DHM gives better results than the other two schemes. DHM has a relatively low regional registration cost with relation to the other schemes, therefore it does affect the location update cost impressively. In other words, that is because DHM never updates itself with the far away anchor; in contrast it updates itself with the previous FA. The competency between the HBAS and DDR is defined by the average residence time. As it shows in figure 4.13, with the increase of λ_r (average residence time) the location update cost of HBAS and DDR both gets decreased. The reason is as long as the MN stays in the same subnet, the signaling cost resulted from changing consequent subnet will be less. But in the case of HBAS, since the domain size is directly defined by time residence probability, the effect is more.

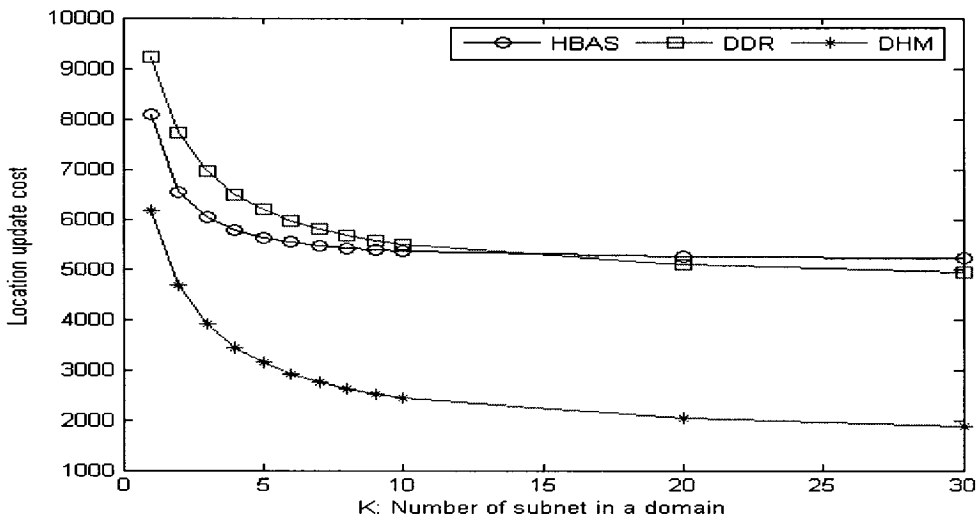


Figure 4.12 Different schemes' location update cost under variable subnet number, scenario i

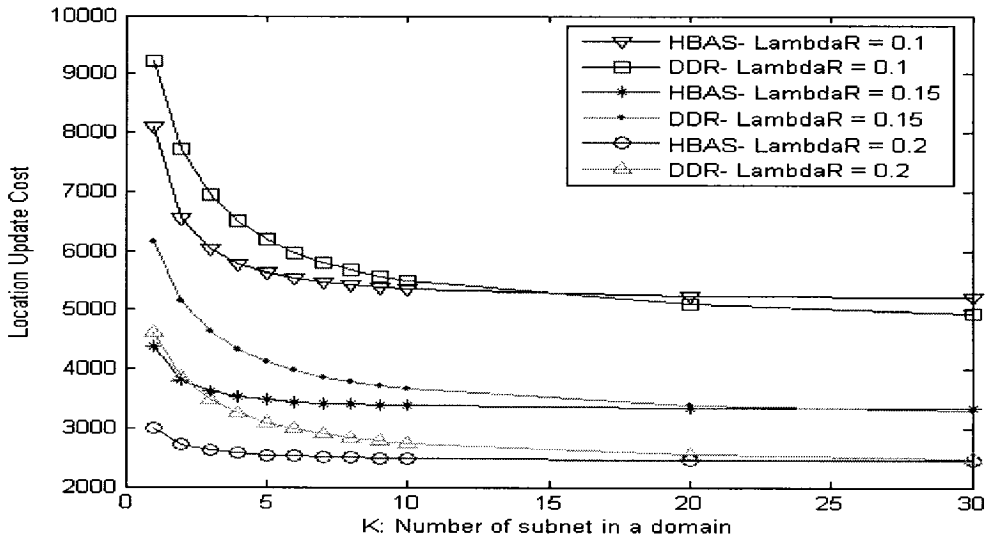


Figure 4.13 Impact of average resident time on HBAS and DDR

Evidently with the increase of K which means having a bigger domain, the location update cost should decrease. As it mentioned earlier the expectation of the movement from the previous domain in the centralized scheme is a linear function of K, while in the case of HBAS is an exponential function. Figure 4.14 demonstrates the above mentioned fact.

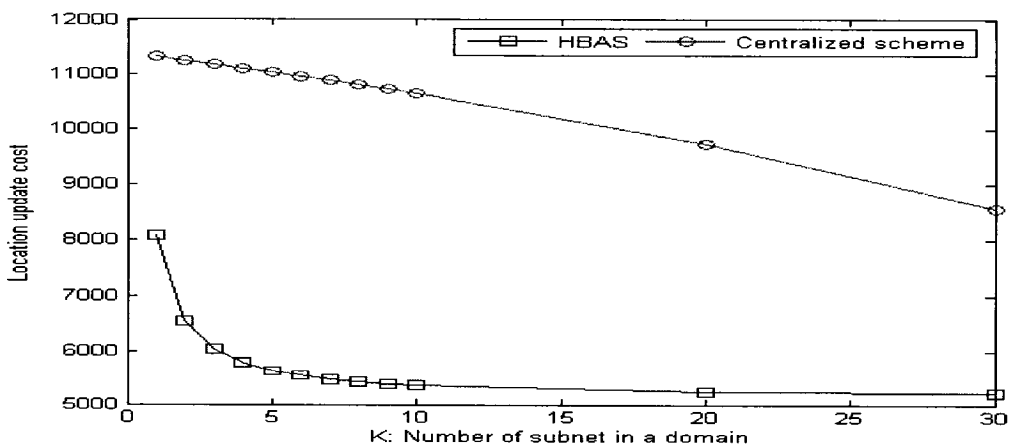


Figure 4.14 Comparison of location update cost between HBAS and centralized scheme, scenario i

Eventually in the case of second scenario, HBAS gets better because as soon as the MN enters to the new domain, it has to update itself with the previous anchor, while an MN in DDR system has to be updated with the HA which costs more. But since the cost of chain establishment among the FAs is less expensive than chain establishment among the anchors, hence DHM still presents better results (see figure 4.15).

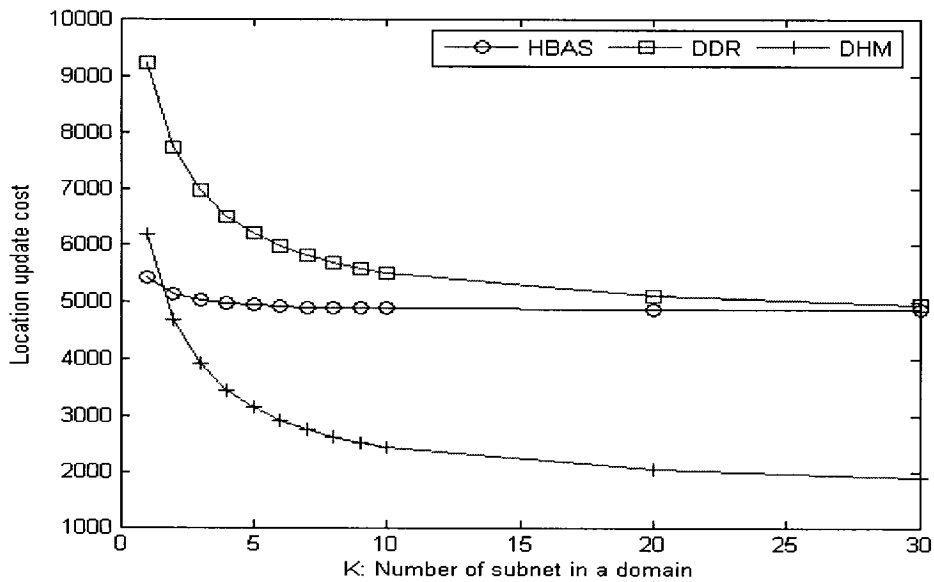


Figure 4.15 Different schemes' location update cost under variable subnet number, scenario ii

As for comparison between the centralized scheme and HBAS, since the cost of chain establishment is less that update with the HA which the case for centralized scheme, therefore the proposed scheme demonstrates even better result than the first scenario (see figure 4.16).

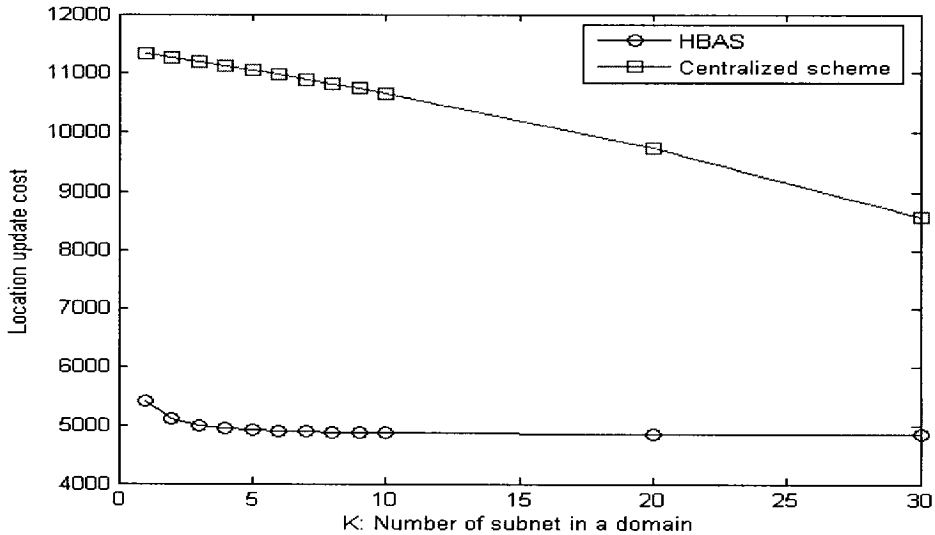


Figure 4.16 Comparison of location update cost between HBAS and centralized scheme, scenario ii

b. Location update cost versus time variant residence time

Figure 4.17 demonstrates the effect of an individual user's time variant residence time on its location update cost. The residence time of the MN, T_f is considered an exponential distribution:

$$f(T_f) = \frac{1}{\lambda_r} e^{-T_f / \lambda_r} \tag{4.12}$$

It explains that when the user stays in the same subnet longer, evidently the anchor point does not change. Therefore in this case there is no need to register with the HA and consequently the location update cost reduces.

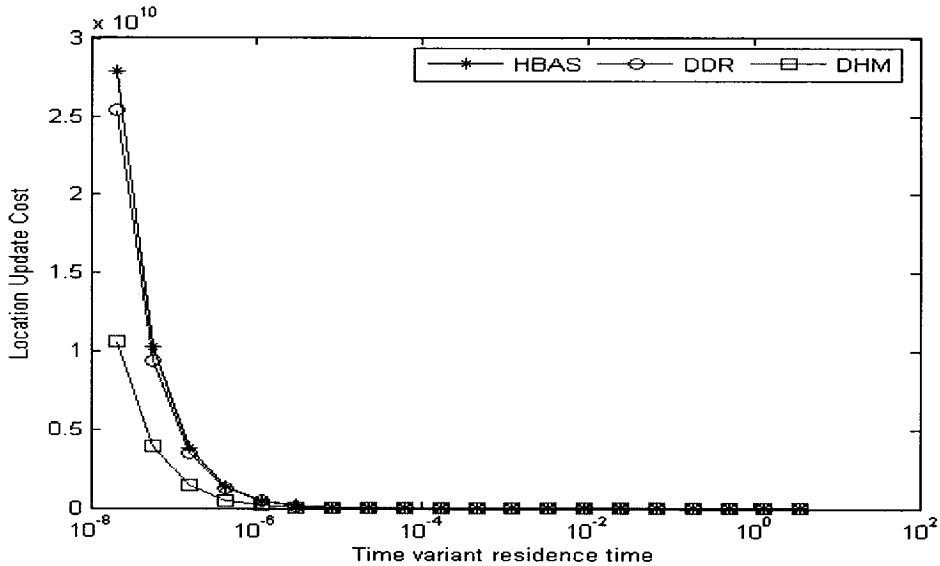


Figure 4.17 Impact of time variant resident time on different schemes

The same logic is applicable to the centralized fixed structure as well. But as it is expected, HBAS seems less expensive than the centralized scheme (see figure 4.18).

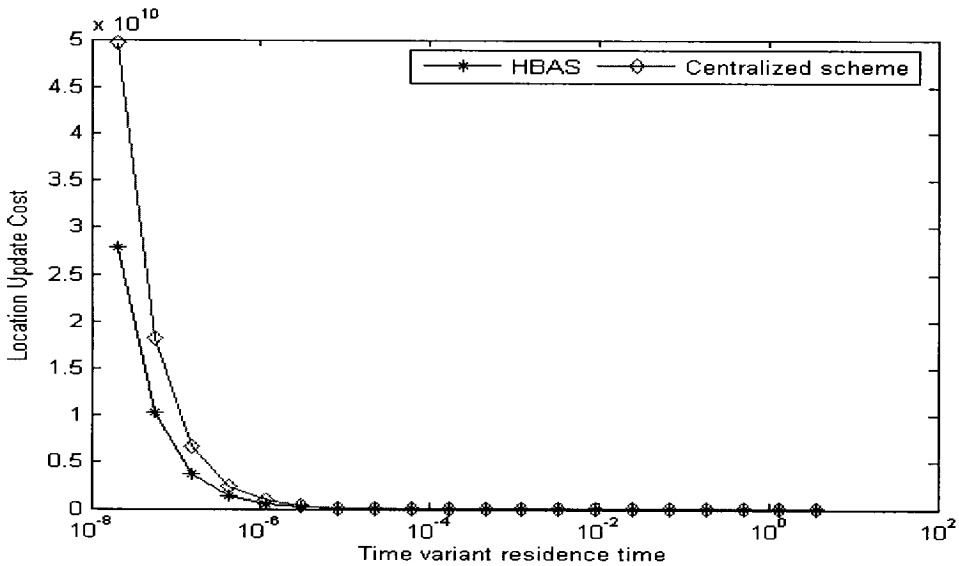


Figure 4.18 Impact of time variant resident time on HBAS and centralized scheme

4.3.4 Packet delivery cost

The analytical model used for packet delivery cost is extracted from [19]. As the anchor receives the packets from the HA, it decapsulates the tunneled IP packets and then looking up in its visitor table to find the exact location of the MN. Consequently the packet should be encapsulated again and sent to its destination. Hence an increase in the number of user in each subnet and totally in the domain causes a bigger table, which takes more time to look up. Moreover the network bandwidth is affected by the overwhelming packet flow to the anchor. Hopefully in our case in which the anchors are distributed, the performance degradation is less. In other words the load is supposed to be distributed per individual user among different anchor, and not just one.

$$C_{PD} = T_{hg} + T_{gf} + V_h + V_g \tag{4.13}$$

$$C_{PD} = T_{hg} + T_{gf} + V_h + V_g + (T_{ff} + V_f) \tag{4.14}$$

The above statements (4.13) and (4.14) are the general packet delivery cost respectively for HBAS (same as DDR), and DHM. The difference signifies the addition cost of traversing along the chain in each domain for DHM.

$$V_h = \eta * \lambda_c \tag{4.15}$$

$$V_g = \varsigma K * \lambda_c * (\alpha\omega + \beta \log(K)) \tag{4.16}$$

where η is packet delivery processing constant cost at HA and λ_c is packet arrival rate. $\varsigma, \omega, \alpha, \beta$ are respectively constants corresponding to the bandwidth allocation cost, the number of users in each subnet, weighting factors of visitor list and routing table lookups.

The logarithm of the length of the routing table K presents the complexity of IP address lookup at each anchor. The implementation is based on Patricia trie [34].

$$V_g = \varsigma K * \lambda_c * (\alpha\omega K + \beta \log(K)) \tag{4.17}$$

The (4.17) formulates the cost at the anchor in case of centralized fixed scheme. The difference ($\alpha\omega K$) signifies that the anchor in responsible for all the users of the domain.

Here like location update cost we can analyze packet delivery cost with respect to the number of subnet in the domain and the average packet arrival rate.

a. Packet delivery cost versus the number of subnet in the domain

Figure 4.19 shows the difference in cost between our scheme and the centralized one. As it is expected from (4.17), a single and central anchor in a centralized scheme has to deal with more users and subnets than the case in which the load processing is distributed among different anchors. In fact both schemes, centralized and HBAS have the same logarithmic shape, but in the case of centralized scheme the cost gets higher sooner than the HBAS.

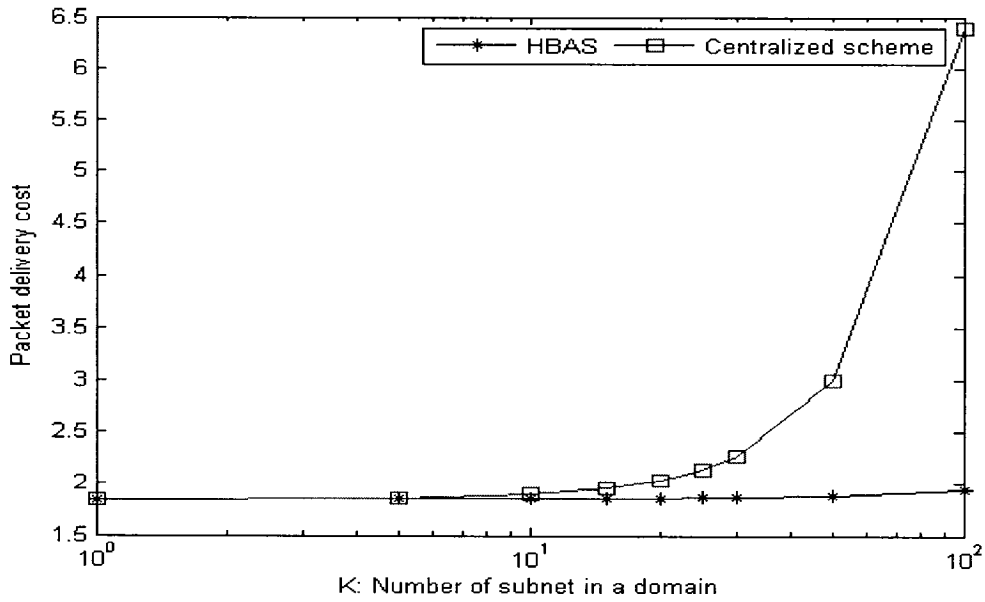


Figure 4.19 Comparison of packet delivery cost between HBAS and centralized scheme under variable subnet number

Figure 4.20 demonstrates the packet delivery cost of DHM scheme, which is proportional to the number of subnet in the involved domain. The extra cost is due to the chain establishment among FAs. Though a larger domain size results in the less number of location updates, it has the disadvantage of more delay in packet delivery processing. Here, with the increase in number of subnet, the packet delivery cost for HBAS and DHM both increase as well, but the increase rate of DHM scheme is faster than HBAS. Since DDR represents the same characteristic as HBAS, just one of them is presented.

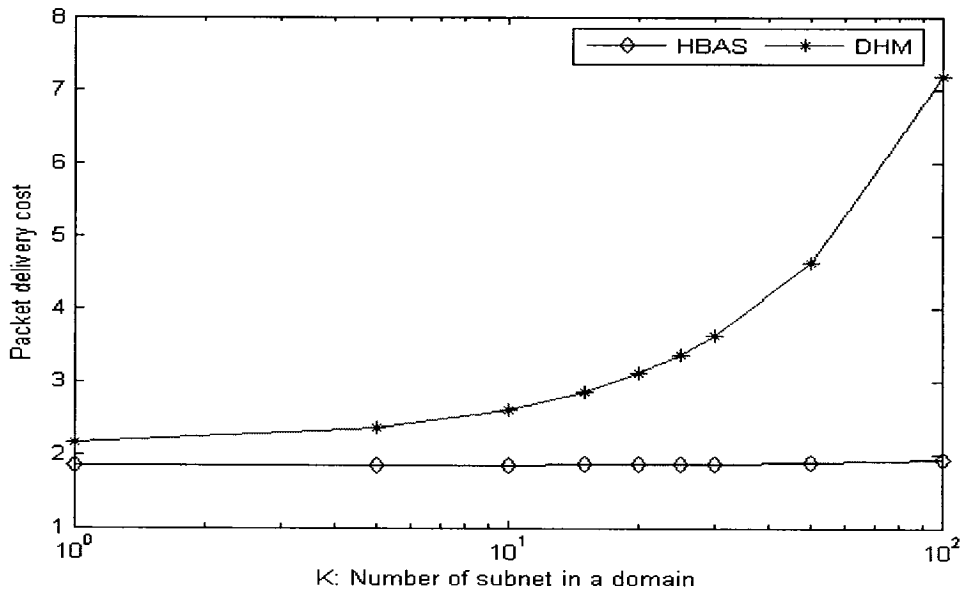


Figure 4.20 Different schemes' packet delivery cost under variable subnet number

b. Packet delivery cost versus time variant packet arrival rate

Due to high packet arrival rate, accesses to lookup table and visitor list get increased which consequently affects the packet delivery cost. The last two graphs examine the impact of time variant packet arrival rate for each individual user. Let suppose that packet arrival rate of the MN is of exponential distribution:

$$f(\lambda_f) = \frac{1}{\lambda c} e^{-\lambda f / \lambda c} \tag{4.18}$$

Figure 4.21 compares the result between the HBAS and DHM. Here again the DDR represent the same graph as HBAS, therefore just HBAS has been compared with the centralized scheme and DHM. Logically since the packet addressed to MN in DHM scheme has to follow the chain, hence the delivery cost increases more. While in case of centralized scheme with packet arrival increase the anchor has to handle more processing than the anchors in HBAS (see figure 4.22).

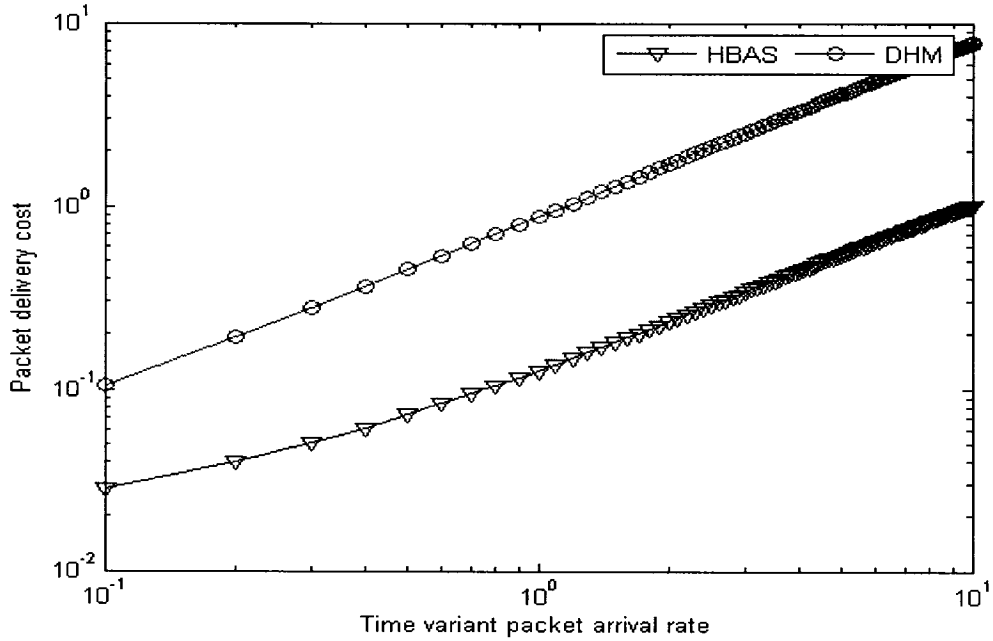


Figure 4.21 Impact of time variant packet arrival rate on packet delivery cost

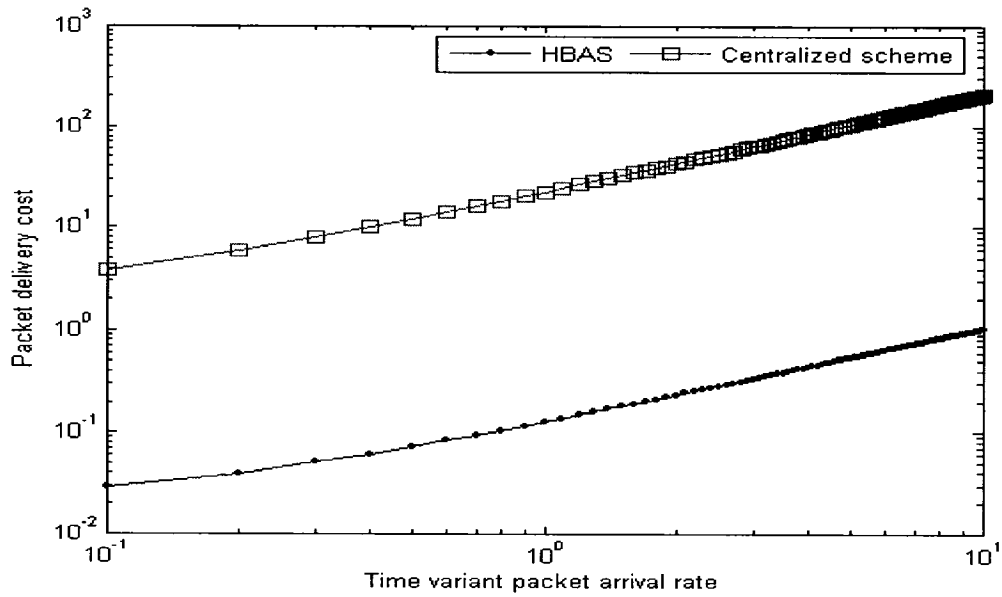


Figure 4.22 Comparison of packet delivery cost between HBAS and centralized scheme under impact of time variant packet arrival rate

4.4 Conclusion

In the first part of this chapter, some aspects of the proposed scheme, HBAS have been verified by a verification toolbox named UPPAAL. Then in the second part, the HBAS was analyzed and compared with the traditional centralized scheme, as well as the other two extracted schemes from the published articles [17] [19], briefly called DDR, and DHM. The analytical model is mainly based on the domain boundary definition which in case of HBAS has been inspired by the idea from [33]. But as a new parameter the number of subnets of a domain (domain size) was considered also.

The comparison between different schemes has been done based on two measurement parameters: Location update cost and packet delivery cost. The obtained results show that location update cost of HBAS is definitely better than the centralized scheme, and is so close to DDR. Though DHM yields better results in case of location update, but its packet delivery is more expensive than the HBAS.

To summarize, counting the fact that the number of subnet in case of DDR, and DHM should be calculated whenever the need arises (it is not mentioned precisely in the articles), makes the system more complex than HBAS which is based on the long term history of individual user.

CHAPTER V

CONCLUSION

During the last four chapters, we introduced some intrinsic problems of conventional mobile IP regional structure, then tried to find a solution and to show its effectiveness comparing to the other existing proposals. In the first section of this chapter, a synthesis of the project is to present. Then some limitations related to the proposed scheme will be discussed. And finally we terminate this chapter by having a look at the future aspect of the proposal.

5.1 Synthesis of work

Domain oriented mobility management schemes like "Hierarchical Mobile IP" (HMIP) reduce the overwhelming binding updates signaling of a standard Mobile IP. But in reality there are still many deficiencies associated with the structure itself. "Mobile Anchor Point" (MAP) as the single point of failure in the network, the vague definition of domain's boundary and finally ignoring the user's traffic behavior are among the most addressed problems.

In this project, the proposed scheme, "History Based Anchor Selection Mechanism" which we simply call it "HBAS", pinpoints the above mentioned insufficiencies and tries to clear them through a new scheme.

The proposed model functions based on the users' history of activity and their mobility patterns. A long term built history unfolds users' attitude in terms of their required services, the visited access routers along their habitual path. HBAS makes use of this fact, and suggests to each user to know the best serving access router and select it as its anchor. In contrast to the traditional hierarchical structure which revolves around a single anchor for the whole domain, such a consideration renders the system a distributed structure. Therefore it eliminates the single point of failure problem of HMIP.

Moreover the domain boundary is defined by the user's residence time in each subnet, the call inter arrival time, and the imposed load by location update and packet processing on the anchors.

An analytic model is introduced based on the proposed idea, and then it is compared with two different schemes which have their own solution to the same problems. Specifically the examined measurement parameters are location update and packet delivery cost. According to our study the growth of number of subnet in each domain results in larger expectation value in case of distributed system, which consequently leads to less home location update cost. And HBAS particularly outperforms the HMIP structure. Next the effect of time variant residence time on the location update cost is studied. The obtained results demonstrate HBAS reasonable performance relative to the other schemes. Second part of analytical study is focused on packet delivery cost which is examined through time variant call arrival rate and the number of domain's subnet. As it was expected, there is a definite improvement comparing to the HMIP structure and it yields also better result respect to one of the referenced scheme.

In addition to analytical study, some parts of the scheme are modeled, and verified. The system's model is based on transitions in which a process starts at an initial state and goes through intermediate steps via transitions. A timed automata model checking toolbox, UPPAAL, is chosen to verify the validity of the proposed model.

5.2 Limitations of work

We aimed for improvement of the traditional hierarchical structure of Mobile IP and the analytical results seem reasonable and promising. But we observed mainly two difficulties to be perfect in our path. First, the scheme is based on each user's history which in reality is not implemented. Hence we set foot in an unknown world, where its related facts and deficiencies directly affect the performance of our model. Second, we could not find any suitable simulator to study the efficiency of the scheme more in detail. On the other hand, many simulators do not support mobile IP or still have not released their final version. Hence the same problem applies to HMIP more severely. In

fact the only simulator which can support HMIP through some outdated patch is "Network Simulator" (NS-2). Unfortunately NS-2 is known as an unstable simulator which cannot be handled easily.

Moreover the confidentiality and security of each individual's personal data are the other aspect of limitation to the work. The traced users should be assured that their privacy will not be violated.

5.3 Future work

Users' movement trace illustrates network characteristic which in consequence helps to plan a more efficient network and gets the most out of the existing equipments. Many researches have been done on this subject particularly in cellular domain, though they mostly study the theoretical aspects of the issue. While in reality, network operators use tools to trace users and to optimize their networks. Hence it could be fascinating to have a joint project with a network operator, and to look for a pragmatic conclusion of users' attitude. Afterwards it will be possible to simulate and implement the individual user's mobility pattern based on the acquired data. Neural network can be used to generate the learning model and to produce different profiles (in three dimensions) based on the real collected data. In addition to users' attitude, specifically in the case of our scheme, the network equipment resources should be monitored and simulated as well.

Probably based on the obtained results, one will be inspired to imply them in different situations.

REFERENCES

[1] S. Das, et al., "IDMP: an intra-domain mobility management protocol for next generation wireless networks," *IEEE Wireless Communications*, vol. 9, no. 3, pp. 38-45, June 2002.

[2] A. Misra, et al., "IDMP-Based fast handoffs and paging in IP-based 4G mobile networks," *IEEE Communications Magazine*, vol. 40, no. 3, pp. 138-145, March 2002.

[3] T. You, S. Pack, and Y. Choi, "Robust hierarchical mobile IPv6 (RH-MIPv6)," *The 58th IEEE Vehicular Technology Conference*, vol. 3, pp. 2014 – 2018, October 2003.

[4] A. Valko, "Cellular IP: a new approach to Internet host mobility," *ACM SIGCOMM Computer Communication Review*, vol. 29, no. 1, pp. 50-65., January 1999.

[5] R. Ramjee, et al., "HAWAII: a domain-based approach for supporting mobility in wide area wireless networks," *IEEE/ACM Transaction on Networking*, vol. 10, no. 3, pp. 396 – 410, June 2002.

[6] H. Soliman, C. Castelluccia, K. El-Malki et L. Bellier, "Hierarchical mobile IPv6 mobility management (HMIPv6)," IETF Mobile IP Working Group, draft-ietf-mobileip-hmipv6-08.txt, July 2003.

[7] J. Li, and S. Sampalli, "A load balancing hierarchical model for micro mobility," *The 13th International Conference on Computer Communications and Networks Proceedings*, pp. 347 - 351, 2004.

[8] S. Lo, G. Lee, W. Chen and J. Liu, "Architecture for mobility and QoS support in all IP wireless networks," *IEEE Journal on Selected Area in Communications*, vol. 22, no. 4, pp. 691 – 705, May 2004.

[9] B. Rozsas, and S. Imre, "Improving quality of service in cellular IP domains," *The 7th International Conference on Telecommunications-ConTEL*, vol. 2, pp. 497 – 504, June 2003.

[10] A. T. Campbell, et al., "Design, implementation, and evaluation of cellular IP," *IEEE Personal Communications*, pp. 42-49, August 2000.

[11] R. Koodli, "Fast handovers for mobile IPv6," IETF Mobile IP Working Group, draft-ietf-mipshop-fast-mipv6-01.txt, January 2004.

[12] I. F. Akyildiz, J. Xie, and S. Mohanty, "A survey of mobility management in next generation all IP based wireless systems," *IEEE Wireless Communications*, vol. 11, no. 4, pp. 16-28, August 2004.

[13] A. Helmy, M. Jaseemuddin, and G. Bhaskara, "Multicast-based mobility: a novel architecture for efficient micro mobility", *IEEE Journal on Selected Area in Communications*, vol. 22, no.4, pp. 677 – 690, May 2004.

[14] D. Estrin, M. Handley, A. Helmy, P. Huang, and D. Thaler, "A dynamic bootstrap mechanism for rendezvous-based multicast routing," in *Proc. IEEE INFOCOM'99*, vol.3, pp. 1090–1098, March 1999.

[15] X. He, D. Funato, T. Kawahara, "A dynamic micro-mobility domain construction scheme," *The14 th IEEE 2003 International Symposium on Personal, Indoor, and Mobile Radio Communication Proceedings*, vol. 3, pp. 2495-2499, September 2003.

[16] W. Ma and Y. Fang, "Improved distributed regional location management scheme for mobile IP," *The 14th IEEE 2003 International Symposium on Personal, Indoor and Mobile Radio Communications Proceedings*, vol. 3, pp. 2505 - 2509 September 2003.

[17] W. Ma and Y. Fang, "Dynamic hierarchical mobility management strategy for mobile IP networks," *IEEE Journal on Selected Area in Communications*, vol. 22, no.4, pp. 664 - 676, May 2004.

[18] C.W. Pyo, J. Li, and H. Kameda, "Dynamic and distributed domain-based mobility management method for mobile IPv6," *The 58th IEEE Vehicular Technology Conference*, vol. 3, pp. 1964 - 1968, October 2003.

[19] J. Xie, and I. Akyildiz, "A distributed dynamic regional location management scheme for mobile IP," *IEEE INFOCOM*, vol.2, pp. 1069 - 1078, June 2002.

[20] R. Prakash, Z. Haas, M. Singhal, "Load-Balanced location management for cellular mobile systems using quorums and dynamic hashing," *ACM/Baltzer Wireless Networks (WINET) Journal*, vol. 7, no. 5, pp. 497-512, September 2001.

[21] K. Kawano, K. Kinoshita, and K. Murakami, "Multilevel hierarchical mobility management scheme in complicated structured networks," *The Proceedings 29th Annual IEEE International Conference on Local Computer Networks*, pp. 34 – 41, November 2004.

[22] K. Kawano, K. Kinoshita, and K. Murakami, "A study on estimation of mobility of terminals for hierarchical mobility management scheme," *IEICE Transaction Communications*, vol. E87-B, no.9, September 2004.

[23] C. Chu, and C. Weng, "Pointer forwarding MIPv6 mobility management," *IEEE Global Telecommunications Conference, GLOBECOM'02*, vol.3, pp. 2133 – 2137, November 2002.

[24] Y. Bejerano, I. Cidon, "An anchor chain scheme for IP mobility management," *The Proceedings 19th Annual Joint Conference of the IEEE Computer and Communications Societies*, vol. 2, pp. 765 - 774, March 2000.

[25] Y. Chen, T. Boult, "Dynamic home agent reassignment in mobile IP," *Wireless Communications and Networking Conference*, vol. 1, pp. 44 – 48, March 2002.

[26] R. Shah, and M. Chatterjee, "A hierarchical architecture to integrate GSM and mobile IPv6," *Wireless Communications and Networking Conference*, vol. 1, pp. 138 – 143, March 2004.

[27] H. Yokota, et al, "Metro mobile ring for high-speed and scalable micro mobility management," *The 13th IEEE Workshop on Local and Metropolitan Area Networks, LANMAN*, pp. 151 – 156, April 2004.

[28] E.N. Onwuka and Z. Niu, "CHIMA: a distributed hierarchical location directory approach to mobility management in a cellular mobile Internet," *The 9th Asia-Pacific Conference on Communications, APCC 2003*, vol. 1, pp. 157 - 162, September 2003.

[29] S. Hwang, B. Lee, Y. Han, and C. Hwang, "An adaptive hierarchical mobile IPv6 with route optimization," *The 57th IEEE Semiannual Vehicular Technology Conference*, vol.3, pp. 1502 – 1506, April 2003.

[30] X. Peng, H. Zhang, J. Hu, and S. Zhang, "Modeling in hierarchical mobile IPv6

and intelligent mobility management scheme," *The 14th IEEE 2003 International Symposium on Penonal, Indoor and Mobile Radio Communication Proceedings*, vol. 3, pp. 2823-2827, September 2003.

[31] E.N. Onwuka and Z. Niu, "A study of the scalability and performance of multi-level hierarchy for scalable mobility management in wireless IP networks," *The 14th IEEE 2003 International Symposium on Personal, Indoor and Mobile Radio Communication Proceedings*, vol. 1, pp. 465-469, September 2003.

[32] http://www.uppaal.com

[33] D. Ou et al., "An adaptive direction based location update scheme for next generation of PCS networks," *Proceedings of the 13th International Conference on Database and Expert Systems Applications*, pp. 413-422, 2002.