# Local-area Mobility Support through Cooperating Hierarchies of Mobile IP Foreign Agents

**Ayman Abdel-Hamid** **Hussein Abdel-Wahab**

Department of Computer Science, Old Dominion University

Norfolk, VA 23529, USA

{hamid, wahab}@cs.odu.edu

## Abstract

*Mobile IP presents an efficient solution to the wide-area host mobility problem in the Internet. Nevertheless, its home registration process introduces an overhead in the local-area mobility case. A Mobile Host is required to register with its possibly distant Home Agent, whenever it changes its point of attachment to the network. Foreign Agent hierarchies have been introduced to perform Regional Mobile IP registration to minimize the home registration signaling overhead. In this paper, we propose a novel configurable architecture to organize cooperating Foreign Agent hierarchies in the foreign domain. An attempt is made not to change the Mobile Host home registered care-of address as long as it is within the foreign domain. In such manner, home registration signaling overhead is minimized, and the Home Agent is isolated from any local-area movement by the Mobile Host.*

## 1 Introduction

The ubiquity of wireless communication technologies and the proliferation of portable computing devices have made possible a mobile computing era in which users, on the move, can seamlessly access network services and resources, from any-where, at any time.

An IP address reflects a host's point of attachment to the network. A mobile host continuously changing its network point of attachment creates a serious problem for a TCP/IP based Internet. During an active TCP session, if the source IP address or the destination IP address changes, due to a change of point of attachment, the TCP session breaks. If no special handling is provided to deal with host mobility, packets addressed to a mobile host will be routed to the mobile host's home network, not to its current location. This problem occurs because an IP address serves a dual purpose: a *routing directive* in the network layer and an *end point identifier* in the transport layer [4].

Mobile IP presents a network layer solution to the host mobility problem in the Internet for both wired and wireless networks. For wireless networks, it assumes that the Mobile Host (MH) is properly equipped to communicate over a wireless link with a *Base Station* (BS). BSs are statically connected to the Internet by means of a fixed wired networking infrastructure. Mobile IPv4 [10] uses a two level addressing architecture, and deploys *Mobility Agents* (MA) in the home network, and the visited network. The MH is associated with two IP addresses: its permanent home IP address which serves as an end point identifier, and a transient care-of IP address which reflects its current point of attachment, and serves as a routing directive at the network layer. The care-of address can be the address of a *Foreign Agent* (FA) in the visited network, or can be a co-located care-of address, which the mobile host acquires on the visited network. The FA is a router in the foreign network that acts as a mobility agent. Whenever a mobile host is away from home, it registers its current care-of address with its *Home Agent* (HA). The HA is a router that acts as a mobility agent in the home network, and intercepts any datagrams destined to the mobile host's home address, and tunnels them to the registered care-of address. A host in the Internet communicating with the MH is termed a *Correspondent Host* (CH).

Mobile IP[1] can handle wide-area mobility, and local-area mobility. Although, it is more suitable to handle wide-area mobility since a mobile host is required to register with its, possibly distant, HA whenever it changes its point of attachment. This results in a large registration signaling overhead, and large handoff latencies in the local-area mobility case. Minimizing handoff latency is crucial in wireless networks with small sized cells, where the MH crosses cell boundaries very often resulting in frequent handoffs. One solution to handle local-area mobility in Mobile IPv4 deploys FA hierarchies within the foreign domain [9].

In this paper, we present a novel architecture, within Mobile IPv4 framework, to organize and operate *FA Hierarchies* within the foreign domain. FA hierarchies cooperate in a configurable manner to keep the MH home registered mobility-binding current. The proposed architecture minimizes the handoff delay by isolating the effects of the MH's movement within the foreign domain from the HA. If possible, the MH keeps the same its home registered care-of address, even if it moves across FA hierarchies within the same foreign domain. In addition, the format and processing of Mobile IP protocol messages is modified to account for the failure of the MH home registered care-of address inside the foreign domain, when the MH moves between FA hierarchies. The proposed architecture

[1] Throughout the paper, the term "Mobile IP" refers to Mobile IPv4.

along with Mobile IP protocol modifications maintain the same level of security as the base Mobile IP, by providing message authentication and replay protection of protocol messages.

The rest of this paper is organized as follows. Section 2 presents an overview of related work. Section 3 introduces the architecture of cooperating hierarchies of Mobile IP foreign agents. First, A general overview of the architecture is presented highlighting the motivation for such architecture. Second, the necessary extensions for Mobility Agents advertisements, and Mobile IP protocol messages are explained, along with the required processing. In addition, we show how replay protection, and fast handoffs can be implemented within our architecture. Finally the paper is concluded in section 4, along with future work.

## 2. Related Work

A number of proposals, within Mobile IP framework, exist to handle local-area mobility, without incurring any large handoff latencies [6, 9]. Other researchers have optimized their local-area mobility solutions towards the wireless network environment [5, 15, 16].

To alleviate the large Mobile IP home registration overhead, the *Regional Registration* approach introduced FA Hierarchies in the foreign domain [9]. A FA hierarchy (figure 1) is rooted by a *Gateway Foreign Agent* (GFA), which has a publicly routable IP address. The MH registers with its HA the GFA address as its care-of address. This care-of address will not change when the MH changes FA under the same GFA. After registering the GFA IP address with the HA as care-of address, the MH is allowed to perform regional registration within the FA hierarchy as long as its registration with the HA did not expire. Hence, part of the HA functionality is delegated to the GFA, and any of the FAs beneath the GFA in the hierarchy become *Regional FAs* (RFA), i.e. the target of a regional registration from the MH. Figure 1 illustrates an example of the MH's home registration, and regional registration.

A number of FA hierarchies might be deployed in the same foreign domain. Nevertheless, existing prototype implementations, and simulations have considered deploying only one FA Hierarchy in the foreign domain [8, 14]. The FA hierarchy approach is sensitive to FA failures. In addition, if one GFA exists in the domain, it is required to maintain a routing entry for every MH currently registered within the foreign domain, and act as a tunnel endpoint for all tunnels established with the MHs home agents. Moreover, security associations are required between each parent FA and its children FAs beneath it in the FA hierarchy. Nevertheless, the FA hierarchy approach is independent of any physical network placement of FAs and offers the same level of security as the base Mobile IP.

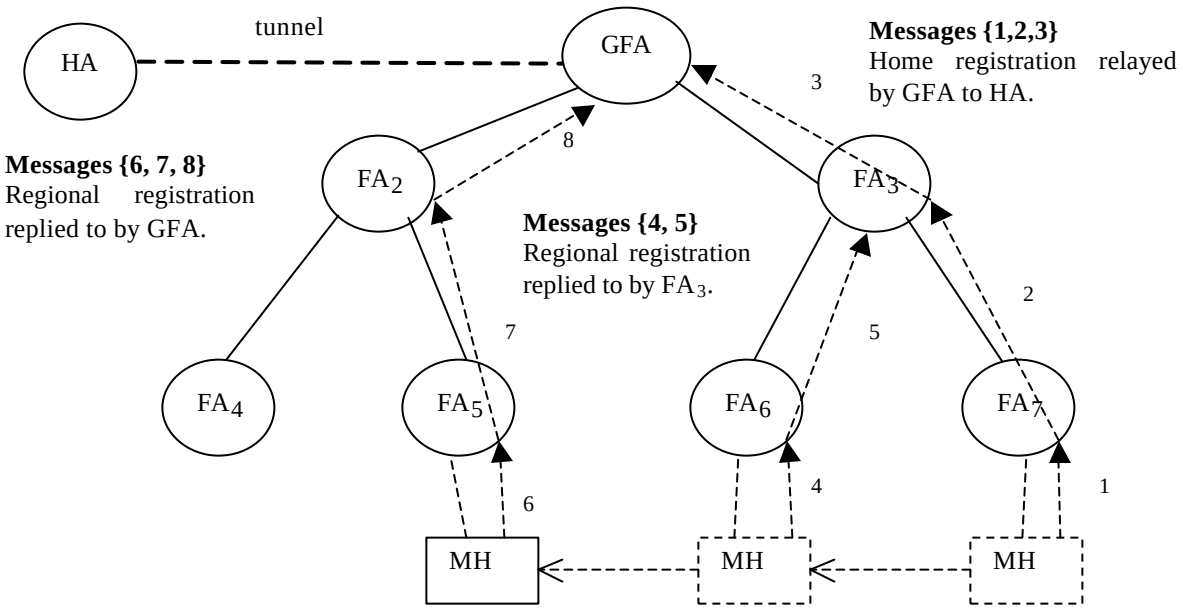


Figure 1: FA Hierarchy within a visited foreign domain.

The Anchor FA approach [6] introduces two registration methods to reduce handoff latencies within the visited domain: *local registration*, and *global indirect registration*. Either method requires the MH to perform a *global registration* (Mobile IP home registration) with its HA upon entering a visited *Zone*. The authors do not explain what constitutes a zone in a foreign domain. In the *local registration* method, it is assumed that the current FA and the MH establish a shared security association. Later on, the current FA acts as an *Anchor FA* for this MH, authenticating the MH while it moves within the same zone. When the MH changes FA within the same zone, the new FA performs local registration with the Anchor FA. The *global indirect registration* method is used when no security association could be established between the current FA and the MH, requiring the HA to always authenticate the MH registration. Any new FA directs the MH registration towards the Anchor FA, the Anchor FA relays the registration to the HA, which authenticates the registration. This approach has the disadvantage of requiring two shared security associations, one in each direction, between any two FAs within a zone. However, since any FA can become an Anchor FA, management of mobile hosts routing entries is distributed, and no one FA has to manage routing entries for the total number of MHs within the zone.

Caceres, and Padmanabhan [5] suggest the use of FA hierarchies but distinguish the *local mobility* case where an MH moves between BSs on the same IP subnet. The *Address Resolution Protocol (ARP)* proxy and gratuitous ARP messages are used in the IP subnet to maintain the illusion that the

MH resides on the wired link in this subnet. Movement between IP subnets is handled by *subnet FAs*. A MH uses a *domain FA* IP address as its care-of address in its home registration. Use of proxy and gratuitous ARP represents a potential security problem in this approach.

Cellular IP [16] suggests handling local-area mobility through a wireless access network. The access network is connected to the Internet through routers, called *gateway routers* (GW). The GW can act as a HA or FA. The wireless access network is partitioned into *Paging Areas*. BSs transmit which paging area they belong to as part of their periodic beacon signals. Packets addressed to a MH are routed to its current BS on a hop-by-hop basis where each node only needs to know on which of its outgoing ports to forward packets. To accomplish that, two types of caches are deployed within the access network: *Paging Caches* maintained for idle mobile hosts, and *Routing Caches* maintained for MHs currently receiving or expecting to receive data. Entries in the Paging caches are used to page the MH and alert it that data packets are to be transmitted to it. Entries in Routing caches are used to actually route any data packets to the MH. While idle, MHs are responsible for populating Paging caches by sending a specific control packet. Any data packets transmitted by the MH are used to update the Routing caches entries. In such approach, the GW presents a single point of failure. In addition, when the number of MHs increases, the number of control packets needed to keep the mappings current increases possibly overloading the wireless access network.

HAWAII [15] suggests partitioning the wireless access network into administrative domains with domain gateway routers named the *Domain Root Routers*. It uses specialized path setup schemes that install host-based forwarding entries in specific routers to efficiently support local-area mobility (Intra-domain). When a MH is moving within its home domain, it retains its IP address. Packets destined to the MH reach the Home Domain Root Router based on the subnet address of the domain and are forwarded over special dynamically established paths to the MH. In such manner, The HA functionality is not needed while the MH is moving within its home domain. When a MH is visiting a foreign domain it is required to obtain a co-located care-of address within the foreign domain. The MH keeps this care-of address as long it is within the same foreign domain. Nevertheless, it is required to register with a BS within the domain to better handle handoffs. The BS in turn informs the MH's HA about the MH's co-located care-of address through the Mobile IP registration process. The HA forwards any datagrams for this MH to its care-of address. These datagrams reach the foreign domain root router through normal IP routing, and are forwarded over dynamically established paths until they reach the MH. The problem we envision with such approach is the requirement that the MH must acquire a new co-located care-of address whenever it changes domains. This requirement stresses the

already depleted IPv4 address space. In addition, all the routers in the domain must maintain host-based entries to efficiently implement the path setup scheme. Nevertheless, the proposed approach takes into account the different types of wireless networks suggesting two corresponding path setup schemes.

# 3 Cooperating Hierarchies of Mobile IP Foreign Agents

Deploying one FA hierarchy in the foreign domain places a burden on the GFA. The GFA has to maintain a routing entry for every MH within the foreign domain. This becomes a drawback as mobility becomes the norm, rather than the exception. In addition, one GFA presents a single point of failure in such system. Although the regional registration approach [9] suggests that at least one GFA should be present in a domain, it does not allow cooperation between GFAs to maintain the current MH mobility-binding within the domain to further reduce any unnecessary registrations with a possibly distant HA. Nevertheless, it allows the MH to request regional registration with its known GFA, other than the one advertised by the current FA. Such regional registration can fail since the current FA may know nothing about the current MH's GFA, forcing the MH to send a home registration request changing its home registered care-of address to the new GFA. In addition, this approach requires security associations between FAs in different FA hierarchies, which might not be feasible if the FA hierarchies are controlled by different administrative entities within the same domain, or if even feasible increases substantially the required number of security associations. On the other hand, The Anchor FA approach [6] allows any FA to become an Anchor FA, requiring security associations between any two FAs. Management of such security associations can become cumbersome when the number of deployed FAs within a zone increases.

In order to further reduce any home registration signaling overhead while the MH is moving within the same foreign domain, and to minimize the required number of security associations between FAs, we suggest deploying in the foreign domain *multiple cooperating FA hierarchies.* Although, multiple FA hierarchies coexist in the foreign domain, they can cooperate in a configurable and scalable manner to maintain the MH home registered care-of address current, and the same as long as the MH is moving within the same foreign domain. Scalable cooperation in this context implies using the minimum number of security associations, and is achieved in our suggested architecture by allowing cooperation across FA hierarchies only between the roots of each hierarchy (section 3.2). We believe that the ability to partition the foreign domain into FA hierarchies gives great flexibility to network administrators. Each hierarchy can be managed independently from the other, while still not precluding

any possible cooperation among FA hierarchies. Across FA hierarchies, two security associations, one in each direction, are required between each 2 roots of such hierarchies. In addition, within the same FA hierarchy, security associations are required between each parent FA and its children FAs. The subsequent sections present the details of the suggested architecture.

### 3.1 Foreign Agent Hierarchies

The foreign domain is partitioned into *Routing Zones* (figure 2). Routing zones are non-overlapping in the sense that each routing zone constitutes an independent FA hierarchy. Special cases might arise when partitioning the foreign domain into routing zones such as a domain-wide routing zone, and single-FA routing zone. The domain-wide routing zone case implies deploying one FA hierarchy within the foreign domain. The single-FA routing zone case implies that the routing zone is constituted of only one FA, i.e. the FA hierarchy has been reduced to a single FA. If all the routing zones in the foreign domain are single-FA routing zones, then this foreign domain partitioning maps to the Anchor FA strategy of independent FA deployment within the foreign domain [6].

The root FA in a zone is termed the *Zone FA* (ZFA), and is required to have a publicly routable IP address. Each ZFA acts as a *Gateway Mobility Agent* for this foreign domain such that the ZFA IP address can be used by a MH as care-of address when registering with the HA. In this manner, different MHs may register different ZFAs as their care-of address depending on which routing zone the MH was in when it first entered the foreign domain. Hence, mobile hosts routing entries are distributed between ZFAs. Consequently, a single ZFA does not have to act as the HA tunnel endpoint for all MHs within the foreign domain. Neither the number of levels in any FA hierarchy, nor the number of FAs in any level is restricted. We adopt the terminology introduced in [9] and term any non-root FA within a FA hierarchy as a regional FA. FAs within a routing zone advertise two care-of addresses: their own IP address, and their corresponding ZFA IP address, respectively. We believe that an FA advertising its own IP address is crucial to the efficient operation of the *Previous FA Notification Extension*, in case smooth handoffs are requested by the MH [12]. In addition, the advertisement of the FA IP address, allows a MH to register with the FA directly according to the base Mobile IP protocol [10], if the MH is not equipped to deal with the FA hierarchy and the required protocol messages. Moreover, an FA does not advertise the FA hierarchy leading to its ZFA. In such manner, less bandwidth is required if the FA advertisement is to be transmitted over a wireless link, the structure of the FA hierarchy is hidden from the MH, and the structure of the FA hierarchy can change dynamically without having to alter the FA advertisement.

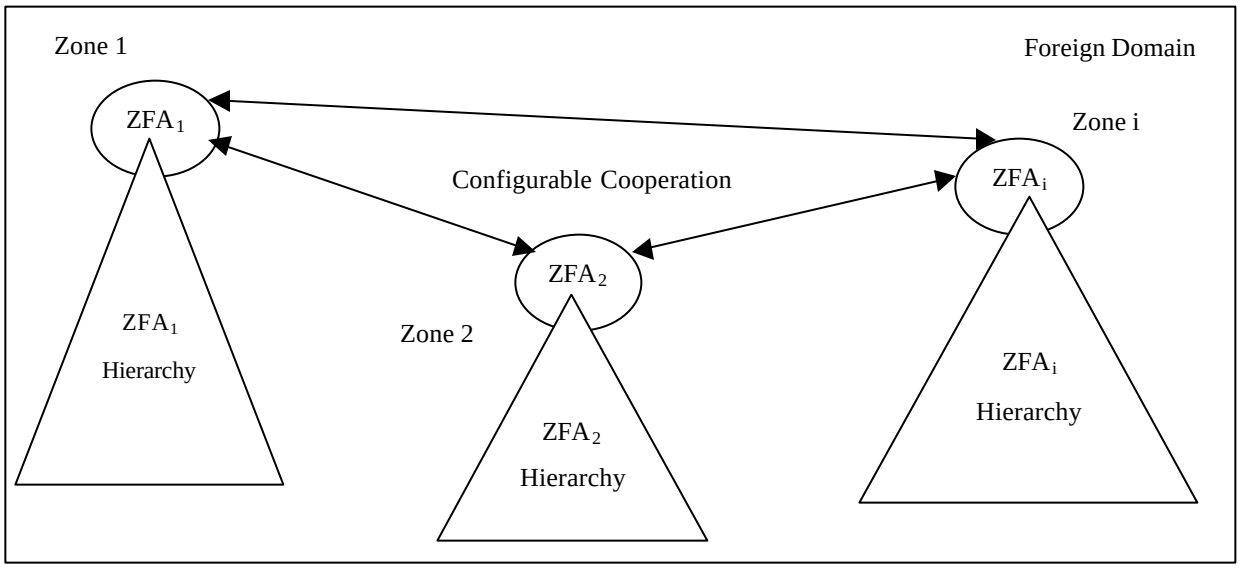


Figure 2: Routing Zones (FA Hierarchies) within the foreign domain.

The MH can detect that it has changed routing zones by examining the ZFA IP address advertised by the FA. ZFAs cooperate to maintain the mobility-binding of an MH current without having to register with its HA, unless deemed necessary by the MH, or by the current ZFA. To make such cooperation configurable and controllable by network administrators, any FA advertises two new options in its mobiltity agent advertisement extensions [10]. These options define whether this ZFA, the root of the current FA hierarchy, will permit the following: will this ZFA accept cooperation requests from other ZFAs?, and will this ZFA send cooperation requests on behalf of the MH?. For instance, if the MH has home registered $ZFA_1$ as its care-of address, and is moving into $ZFA_2$ hierarchy, cooperation can occur if $ZFA_2$ advertises the possibility of sending cooperation requests on behalf of the MH, and if $ZFA_1$ advertises the possibility of accepting cooperation requests from other ZFAs. Please refer to [1] for more specific details about the proposed additions to the Mobile IP agent advertisements to achieve this configurable cooperation. In addition, the FA advertises its *Network Access Identifier* (NAI) [2] in its agent advertisement message. This enables the MH to determine if it is in its home domain, or it is now in a visited foreign domain, and whether it has changed domains since its last registration. All FAs in all routing zones have the same realm in their NAI.

### 3.2 Operational Overview

When an MH first enters the foreign domain, it is required to perform a home registration with its HA. Assume that a MH first enters the foreign domain, and is located within the $ZFA_i$ hierarchy. We shall

focus hereafter on the case where the MH chooses to home register $ZFA_i$ as its care-of address. According to [13], The HA generates a *registration key*, and distributes it to both the MH, and $ZFA_i$. This registration key will be used to authenticate the MH within this foreign domain until it performs another home registration, and another registration key is generated and distributed by the HA. $ZFA_i$ in turn distributes this registration key down its own hierarchy to the regional FA that forwarded the home registration request. Note that the MH needs to remember that $ZFA_i$ is its home registered care-of address as long as it is within this foreign domain. $ZFA_i$ is termed the *Root ZFA* (RZFA) with respect to this MH, since it represents the root of the forwarding tree for this MH inside this foreign domain. Note that, different MHs might have different RZFA, according to which ZFA is their current home registered care-of address. This remains in effect until the MH decides to perform another home registration while within the same foreign domain or another ZFA decides that the MH must perform a home registration. This can be due to for example to the failure of the current RZFA ($ZFA_i$). The home registration process is illustrated in figure 3.

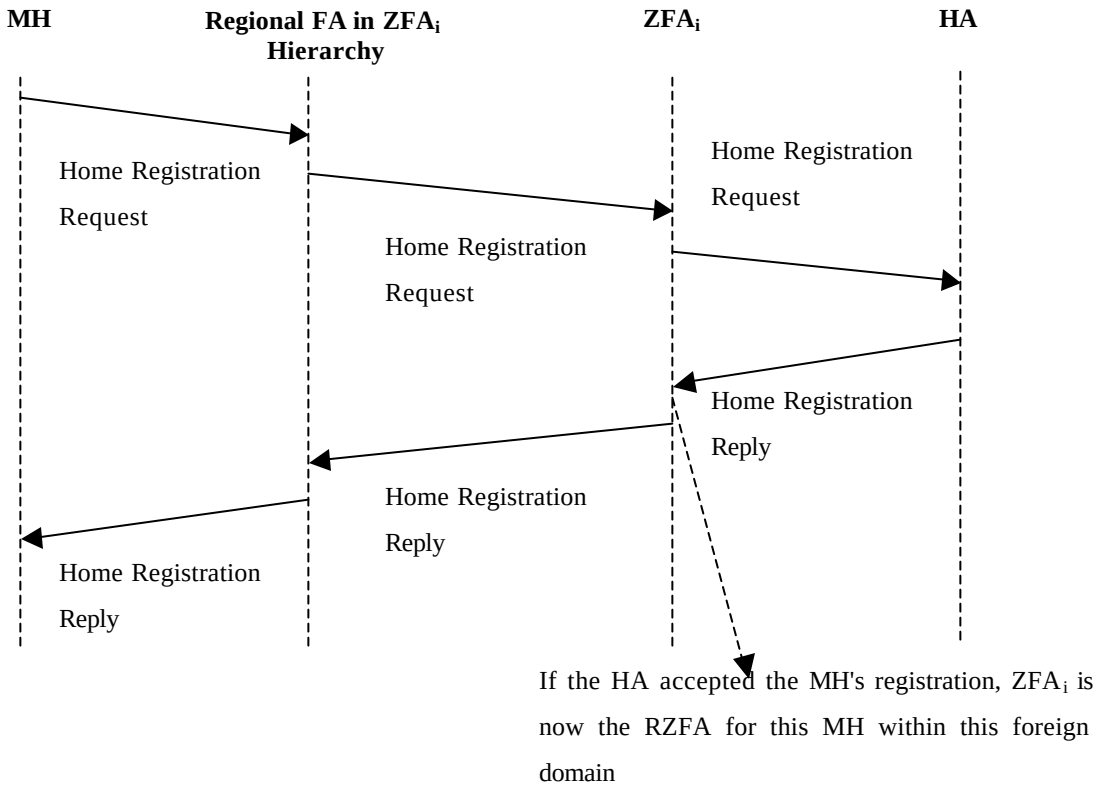


Figure 3: Home registration process.

When the MH moves to another FA hierarchy within the same foreign domain, e.g. changes location from within the $ZFA_i$ hierarchy to within the $ZFA_j$ hierarchy, it has two choices available. The first choice is to perform a new home registration changing its home registered care-of address to $ZFA_j$. Alternatively, it can inform $ZFA_j$ to cooperate with $ZFA_i$ to maintain its home mobility-binding current if both $ZFA_i$ and $ZFA_j$ allow such cooperation. This can be pictured as if $ZFA_i$ is dynamically acquiring a new child FA, $ZFA_j$. The MH can base its decision for example on the fact that it is active, sending or receiving datagrams, or currently idle, or based on the cooperation advertisements by both ZFAs. If the MH is active, then the obvious choice, to minimize the handoff latency, is to keep his home registered care-of address to be $ZFA_i$, meanwhile $ZFA_i$ tunnels any newly received datagrams to $ZFA_j$, which in turn tunnels them down its own FA hierarchy. If the MH is idle, it can choose to inform $ZFA_j$ that it needs to perform home registration, to minimize tunneling overhead within the foreign domain. Later on, if the MH changes location to within the $ZFA_k$ hierarchy, the same cooperation process repeats to establish a tunnel from $ZFA_i$ to $ZFA_k$, and the old tunnel from $ZFA_i$ to $ZFA_j$ is eventually removed (figure 4).

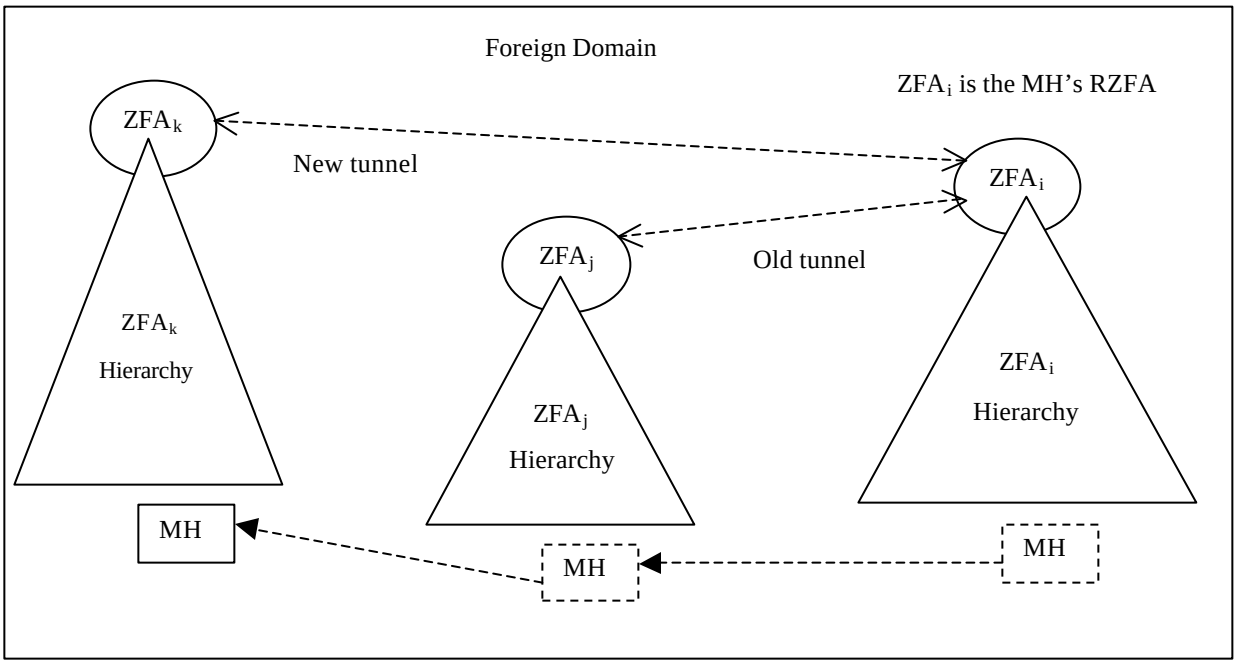


Figure 4: The MH moving between FA hierarchies within the foreign domain. $ZFA_i$ is the MH's RZFA. The MH moves to within the $ZFA_j$, $ZFA_k$ hierarchies, respectively.

In cooperation mode between $ZFA_j$ and $ZFA_i$, $ZFA_j$ relays the MH registration to $ZFA_i$. If $ZFA_i$ accepts the registration relayed by $ZFA_j$, it sends to $ZFA_j$ the registration key acquired from the HA, when the MH first entered the foreign domain. $ZFA_j$ in turn distributes this registration key down its own hierarchy. If for some reason, $ZFA_i$ failed, $ZFA_j$ receives an ICMP error while trying to contact $ZFA_i$, it may go ahead and perform a home registration on behalf of MH. In this case, the MH needs to have included its *Home Credentials* in the registration request to $ZFA_j$. The MH's home credentials are any registration information pertaining to its HA as defined in [10]. If the MH did not include its home credentials, $ZFA_j$ returns a registration reply to the MH containing an appropriate error code. The MH upon receiving this registration reply sends another home registration request choosing its care-of address as $ZFA_j$. In this case, further delay and potential packet loss is introduced by the fact that $ZFA_j$ sends a registration reply to the MH with an error code, and consequently the MH sending another home registration with either messages having to flow through the current FA hierarchy. Therefore, in this case we suggest formulating the home registration message in a new manner by adding a new Mobile IP extension [10] that carries regional registration information. The differently formulated home registration request represents a combined *home-regional registration* request. The home portion of the registration request serves to establish $ZFA_j$ as the new care-of address within the foreign domain, in case the current RZFA is not reachable. Meanwhile, the regional portion of the request provides the MH's regional contact information (the current RZFA) for the current ZFA. The current ZFA, upon receiving the home-regional registration request, attempts to contact the MH's current RZFA by using the regional registration information. If ICMP errors persist after a number of retries, the current ZFA uses the MH's home registration information to perform a home registration on behalf of the MH. In such manner, an attempt is made to account for the failure of the RZFA, and the MH's home mobility-binding is maintained current, while minimizing the incurred delay. The home-regional registration process is illustrated in figure 5.

As long as the MH is moving within its RZFA hierarchy, or within another ZFA hierarchy for which it had already sent a home-regional registration, the MH can perform regional registration to change FA within the same FA hierarchy. The regional FA generating the regional registration reply, sends a deregistration message to the old care-of address registered for that MH [9], unless the MH is requesting simultaneous binding within its registration request. The RZFA is the FA responsible for generating the deregistration message while responding to home-regional registration messages.

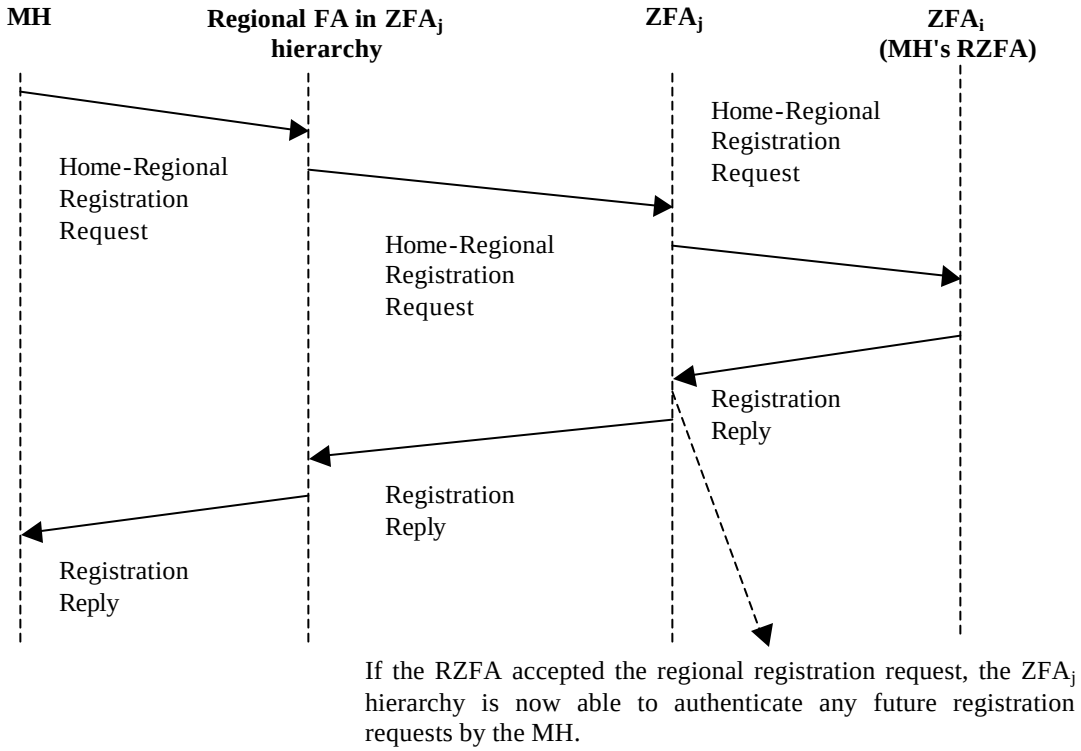


Figure 5(a): The home-regional registration process, in case the RZFA is reachable.

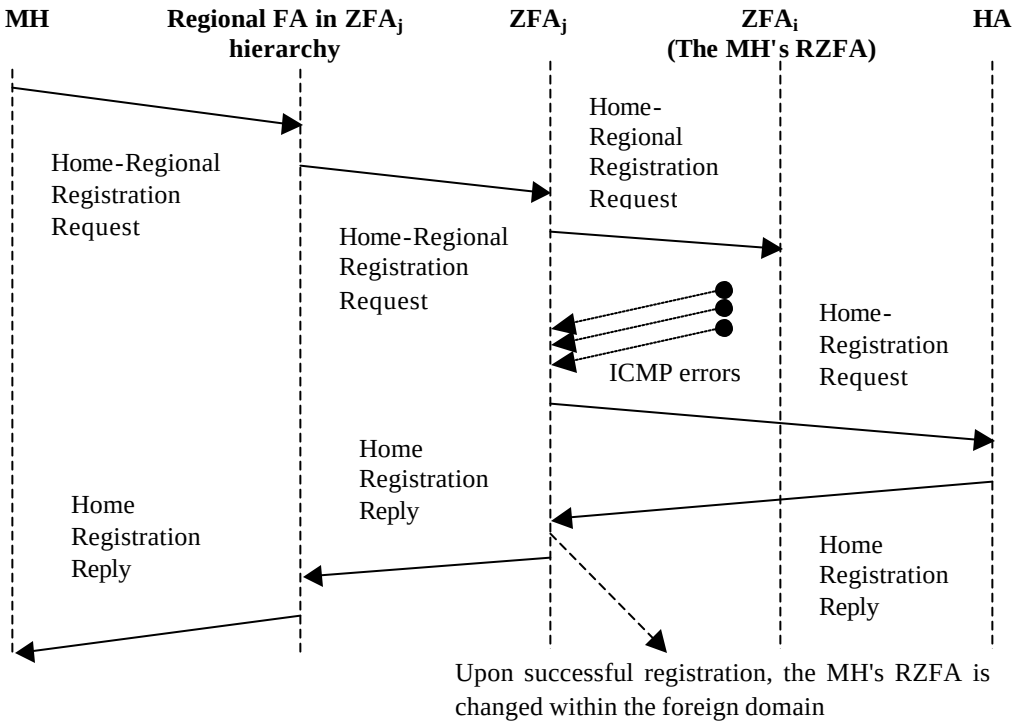


Figure 5(b): The home-regional registration process, in case the RZFA is not reachable.

## 3.3 Registration Messages and Processing

The following sections explain in more detail the different types of registrations used by the MH while moving between FA hierarchies within the foreign domain along with processing by the MH and the involved FAs. The registration types include home registration, regional registration, and home-regional registration.

### *3.3.1 Home Registration*

The MH is required to perform a home registration when it first enters the foreign domain. If the MH is able to acquire a co-located care-of address, it registers this address as its care-of address directly with its HA according to [10]. Alternatively, if registration with the foreign agent is required, the MH home registers the co-located care-of address through the current ZFA [9]. Otherwise, The MH formulates a home registration request using as care-of address the ZFA IP address, or the advertising FA IP address. The advertising FA upon receiving this registration request inspects the supplied care-of address. If the care-of address is its IP address, then this FA forwards the registration request to the MH's HA and acts according to [10]. Alternatively, if the MH is using the ZFA IP address as care-of address, this FA adds to the registration request a *Hierarchical Foreign Agent extension* [9] to include its own IP address, and relays the registration request to its upper FA. This information is authenticated to the upper FA in the FA hierarchy by including an *FA-FA Authentication extension* [9]. The authenticator value is computed based on the shared secret between the forwarding FA, and the upper FA (parent FA). Next, the registration request is relayed to the upper FA, which records the forwarding FA IP address as the tunnel endpoint for this MH. In addition, it removes the Hierarchical FA extension inserted by the forwarding FA, and inserts it own Hierarchical FA extension, and authenticates this information in the same manner to its upper FA. This repeats until the registration request reaches the current ZFA, which records the forwarding FA IP address as the tunnel endpoint for this MH. The current ZFA removes any present Hierarchical FA extension, and forwards this registration request to the MH's HA. Upon receiving a registration reply from the HA, the registration reply is forwarded to the MH using the same FA path that was setup when forwarding the registration request. The registration reply contains a registration key to the ZFA, and the MH. The ZFA distributes this registration key to its regional FA that previously sent the registration request. This process repeats until the registration reply reaches the MH. The MH is responsible for keeping his home registration current, by generating home registration renewals whenever the home registration is about to expire.

If the MH's home mobility-binding is about to expire, and it is just entering a FA hierarchy other than his RZFA hierarchy, the MH formulates a home-regional registration request by forming a home registration request addressed to his HA, with care-of address its RZFA. Next, the MH appends a regional data extension (the RZFA extension, see section 3.3.3) to this home registration request to provide information about its current RZFA. Intermediate FAs, recognizing that the care-of address in the regional extension is their ZFA IP address, forward the registration request upward in the FA hierarchy while adding the Hierarchical FA extension, and the FA-FA Authentication extension. The current ZFA inspects and records the information provided by the MH in the regional extension, and notes the intermediate FA that relayed this request, and relays the registration request to the RZFA. Since the care-of address in the original registration information is the RZFA, the current ZFA simply relays the registration request. In such case, the regional extension is provided to enable cooperation between the two FA hierarchies. The RZFA removes any unnecessary extensions and the regional extension, and records the sending ZFA before relaying the request to the MH's HA. If the RZFA is not reachable, a registration reply with appropriate error code is returned to the MH. In such case, the MH might formulate another home registration request with care-of address the current ZFA, changing its RZFA within the domain to be the current ZFA. In such manner, this home registration along with the regional extension serve to renew the home-registered care-of address, and to notify the current RZFA about the new care-of address for the MH inside the foreign domain.

If the MH's home mobility-binding is about to expire, and it has already established a mobility-binding within the current ZFA hierarchy, i.e., it has previously sent a home-regional registration request, the MH formulates a home registration request addressed to his HA, with care-of address its RZFA. In such case, the ZFA simply relays the registration request to the RZFA appending its hierarchical FA extension, authentication this request with the FA-FA Authentication extension. The regional extension need not be supplied in this case, since cooperation information had been previously exchanged between these two FA hierarchies.

### *3.3.2 Regional Registration*

The regional registration approach [9] defined regional registration request/reply messages to carry regional registration information. We suggest reusing these messages to perform regional registration in our proposed architecture. The ZFA IP address replaces the HA IP address in the regional registration request/reply message. The MH appends a *MH-ZFA Authentication extension* to the regional registration request to authenticate itself to the FA hierarchy. The MH-ZFA Authentication

extension is a new subtype of the generalized Authentication extension [11] similar to the *MN-GFA Authentication extension* defined in [9]. The authenticator value in this authentication extension is calculated based on the registration key that was forwarded to the MH as part of the home registration reply message.

If the MH is moving within its RZFA hierarchy, it generates a regional registration request targeted to the RZFA, with the care-of address set to the current announcing FA. When the MH changes FA hierarchies it registers with the new FA hierarchy by sending a home-regional registration request (see section 3.3.3). Afterwards, If the MH needs to change FA within this ZFA hierarchy, it generates a regional registration request targeted to the current ZFA, with the care-of address set to the advertising FA.

Regional registration replies are generated by the first intermediate FA that already has a mobility-binding for this MH. This intermediate FA will be the intersection point between the old and new registration path. In the worst case, the intermediate FA is the RZFA if the MH is within its RZFA hierarchy, or it is the current ZFA if the MH is moving within another FA hierarchy. In all cases, the lifetime field in the regional registration reply is set to the remaining lifetime of the MH home registration. The Starting lifetime for this remaining lifetime had been recorded from a registration reply previously sent by the RZFA.

### *3.3.3 Home-regional Registration*

Home-regional registration is performed when the MH discovers that it is changing FA hierarchies within the same foreign domain, i.e. the current FA advertisement contains a ZFA IP address different than the MH's RZFA. Home-regional registration attempts to combine the home and regional registration in one message to minimize any unnecessary delays faced while moving to a new FA hierarchy, in case the RZFA has failed. The home-regional registration request is basically a home registration request with a mandatory regional data extension.

The current FA is advertising its NAI, with the realm part of the NAI the same for all FA hierarchies within the foreign domain. Consequently, the MH can deduce that it is still within the same foreign domain, and needs to formulate a home-regional registration request, instead of a home registration request. In order to be able to carry home registration information, along with regional registration information in one message, a *RZFA extension* is defined to carry the regional registration information. The RZFA extension must exist in the home-regional registration message. Information in the RZFA extension is authenticated by the MH-ZFA Authentication extension. The RZFA extension

serves a dual purpose in the home-regional registration request. For the current ZFA, it provides information about the current mobility-binding between the MH and the RZFA such as the RZFA IP address, the style of replay protection currently in use between the MH and the RZFA along with the current identification value [10]. For the RZFA, it provides the current ZFA IP address, whether the MH is requesting simultaneous binding, the current identification value to validate this registration request, and the type of encapsulation to be used between the RZFA and this current ZFA if this registration request is accepted. Please refer to [1] for specific details about the format and data fields of the RZFA extension.

The current FA behaves the same as if it is receiving a home registration, and appends the Hierarchical FA extension and authenticates the request by the FA-FA Authentication extension. Each intermediate FA forwards the registration request upward in the FA hierarchy until it reaches the current ZFA. The current ZFA identifies this registration request as a home-regional registration request, and begins by processing regional registration information supplied in the RZFA extension. The current ZFA checks the RZFA NAI included in the ZFA extension to make sure that this RZFA is within the same domain. Next, The current ZFA appends to the registration request its own NAI, and authenticates this information by using an FA-FA Authentication extension. The authenticator value in the extension is computed based on an established security association between the current ZFA and the RZFA. The current ZFA supplies its own NAI such that the RZFA is able to make sure that this ZFA is within its same domain. Finally, The current ZFA forwards the registration request to this RZFA. The RZFA validates the registration request, and if successful records that the current regional care-of address for this MH is the forwarding ZFA. In addition, the RZFA returns a regional registration reply to the sending ZFA. The regional registration reply includes the MH's registration key encrypted using the shared security association. The ZFA, in turn, distributes this key down its own hierarchy, until the registration reply reaches the MH. In such manner, this new FA hierarchy is able to authenticate any future regional registration requests received from this MH.

If the current ZFA discovers the failure of the RZFA by receiving an ICMP error, it tries to forward the registration request for a predetermined number of times, afterwards it gives up and switches to performing home registration on behalf of the MH. The current ZFA strips the RZFA extension, and the MH-ZFA Authentication extension from the home-regional registration request, and might append any necessary authentication extensions to establish a security association between itself and the HA, and forwards the request to the HA. The HA identifies this request as a home registration request and

acts according to [10]. If the HA accepts the registration request, the MH's RZFA is changed within the foreign domain to be the current ZFA.

### 3.4 Replay Protection

This section explains how replay protection is provided between the MH and the set of FA hierarchies within the foreign domain. Since the MH and any ZFA will most likely not share a pre-established security association, then the replay protection style between the MH and the ZFA is not identified. The regional registration approach [9] introduced a *replay protection extension* that specifies what style of replay protection the MH desires for its regional registration, and provides an initial value to synchronize the replay protection mechanism. The MH adds this extension to the registration request. We propose reusing the same extension, to be supplied by the MH, whenever it changes RZFA within the foreign domain. If the MH changes RZFA, then it needs to supply its replay protection extension so that the new RZFA is able to perform the replay protection mechanism. In brief, the MH appends the replay protection extension to any new home registration request, or any home-regional registration request. In the case of a home-regional registration request, the RZFA extension supplies the type of replay protection currently in effect with the RZFA, and the current identification value. The current ZFA records the replay protection style, and the RZFA uses the identification value to validate the registration request.

Timestamp replay protection is processed according to [10]. Nevertheless, the FAs individual clocks along with the MH’s clock, used to generate the timestamps, need to be synchronized. In such case, any newly generated timestamps by intermediate FAs need not be distributed in the FA hierarchy.

Since our FA hierarchies only advertise the ZFA, but not the hierarchy itself, in the case of nonce replay protection the MH associates the identification value supplied within the registration reply with the current RZFA. Any intermediate FAs record the current nonce value for future use, if such intermediate FA is in a position to reply to a future regional registration request. If an intermediate FA generates a new nonce value, a mechanism is needed to disseminate this new nonce value to higher FAs in the hierarchy, since any of these FAs might be next to authenticate future registration requests from this MH. We propose that the FA generating the new nonce value, sends a *nonce-update message* upward in its FA hierarchy. The nonce-update message propagates upward all the way to this MH's RZFA. This new Mobile IP message contains the MH IP address, along with the new nonce value and is authenticated by means of a FA-FA authentication extension. Intermediate upward FAs in the path

towards the RZFA associate the new nonce value with the MH. In such manner, such FAs are capable of authenticating any future registration requests by the MH. Similarly, in case of timestamp replay protection, the same idea of propagating the generated timestamp, upward in the FA hierarchy can be equally applied, if general clock synchronization can not be achieved. In such case, a general *replay protection update message* is used to carry either the new timestamp value, or the new nonce value.

Alternatively, another solution to provide replay protection is through the announcing FA by means of a challenge-response mechanism [11]. In such case, timestamps or nonces are not needed between the MH and the RZFA.

### 3.5 Fast Handoffs

Fast handoffs within the regional registration approach were introduced in [7]. Using this approach, the MH anticipates its handoff to a new FA, and requests *simultaneous binding* when it detects a handoff-target FA. The handoff-target FA is a FA that the MH will most likely handoff to in the future. In such manner, when the MH actually handoffs to such FA, its datagram forwarding path is already setup and the MH faces no or minimum handoff delay. The MH requests simultaneous binding in its regional registration request. The intermediate FA, that sends a regional registration reply, notes the simultaneous binding request. Then, whenever any datagrams are available for this MH, the intermediate FA *simulcasts* each datagram to each existing mobility-binding for this MH.

This approach can equally be applied to our proposed architecture. The simultaneous binding option is available in regional registration requests. In addition, The RZFA extension includes an *S* bit, which is used by the MH to signal the need for simultaneous binding. Thus, fast handoffs are available to the MH if it is moving within the same FA hierarchy, or across FA hierarchies. In the worst case, the RZFA is the source of the simulcasting for this MH, if the MH has handoff-target FAs that are in a different FA hierarchy.

## 4 Conclusion and Future Work

In this paper, we presented a local-area mobility solution based on Mobile IPv4 FAs hierarchies, where a novel approach for configurable cooperation between FA hierarchies in the foreign domain was introduced. FA hierarchies within the same foreign domain cooperate to minimize any unnecessary home registration with a possibly distant HA. The required extensions and modifications in processing of Mobile IP protocol messages were presented. When the MH is moving across FA hierarchies, the processing of protocol messages accounts for the MH home-registered care-of address failure, such

that the handoff delay due to such failure is minimized. The proposed solution maintains the same security measures as the base Mobile IP protocol in providing message authentication and replay protection. Moreover, the required number of security associations between deployed foreign agents is minimal.

Future work includes simulating the proposed architecture using a network simulator such as ns2 [3]. Such simulation will allow measuring the effects of the introduced extensions and modifications on the handoff delay, and the registration signaling overhead incurred by the MH using a number of mobility scenarios. Furthermore, we intend to compare our approach, using simulation, to other existing approaches that deploy FA hierarchies in the foreign domain such as the regional registration approach [9]. In addition, we plan to investigate a dynamic mechanism to setup and manage FA hierarchies within the foreign domain. Finally, the issue of interoperability between FA hierarchies with different encapsulation, and compression capabilities needs to be fully investigated.

## References


[1] A. Abdel-Hamid, and H. Abdel-Wahab, "*A Generalized Foreign Mobility Agents Architecture*", Technical Report TR_2000_05, Department of Computer Science, Old Dominion University, Norfolk, VA 23529, USA, June 2000.

[2] B. Aboba, and M. Beadles, "*The Network Access Identifier*", Request For Comments (Proposed Standard) 2486, Internet Engineering Task Force, January 1999.

[3] University of California Berkeley, and Lawrence Berkeley National Laboratory, "*UCB/LBNL/VINT Network Simulator, ns (version 2)*", available at URL http://www.isi.edu/nsnam/ns.

[4] P. Bhagwat, C. Perkins, and S. Tripathi, "Network Layer Mobility: an Architecture and Survey", *IEEE Personal Communications*, Vol. 3, No. 3, pp. 54-64, June 1996.

[5] R. Caceres, and V. Padmanabhan, "Fast and Scalable Handoffs for Wireless Internetworks", *in Proceedings of 2nd IEEE/ACM International Conference on Mobile Computing and Networking (MobiCom)*, pp. 56-66, Rye, New York, 1996.

[6] G. Dommety, and T. Ye, "Local and Indirect Registration for Anchoring Handoffs", Internet Draft (Work in Progress), draft-dommety-mobileip-anchor-handoff-01.txt, July 2000.

[7] K. El Malki, and H. Soliman, "Fast Handoffs in Mobile IPv4", Internet Draft (Work in Progress), draft-elmalki-mobileip-fast-handoffs-03.txt, September 2000.

[8] D. Forsberg, J. T. malinen, J. K. Malinen, T. Weckstrom, and M. Tiusanen, "Disributing Mobility Agents Hierarchically under Frequent Location Updates", *in Proceedings of 6th IEEE*

*International Workshop on Mobile Multimedia Communications (MoMuC)*, San Diego, CA, USA, November 15-17, 1999.

[9] E. Gustafsson, A. Jonsson, and C. Perkins, "Mobile IP Regional Registration", Internet Draft (Work in Progress), draft-ietf-mobileip-reg-tunnel-03.txt, July 2000.

[10] C. Perkins (Editor), *"IP Mobility Support"*, Request for Comments (Proposed Standard) 2002, Internet Engineering Task Force, October 1996.

[11] C. Perkins, and P. Calhoun, "Mobile IPv4 Challenge/Response Extensions", Internet Draft (Work in Progress), draft-ietf-mobileip-challenge-13.txt, June 2000.

[12] C. Perkins, and D. Johnson, "Route Optimization in Mobile IP", Internet Draft (Work in Progress), draft-ietf-mobileip-optim-09.txt, February 2000.

[13] C. Perkins, and D. Johnson, and N. Asokan, "Registration Keys for Route Optimization", Internet Draft (Work in Progress), draft-ietf-mobileip-regkey-03.txt, July 2000.

[14] C. Perkins, and K.-Y. Wang, "Optimized Smooth Handoffs in Mobile IP", *in Proceedings of 4th IEEE Symposium on Computers and Communications (ISCC)*, pp. 340-346, Red Sea, Egypt, July 6-8, 1999.

[15] R. Ramjee, T. La Porta, S. Thuel, K. Varadhan, and S. Wang, "HAWAII: A Domain-based Approach for Supporting Mobility in Wide-area Wireless Networks", *in Proceedings of 7th IEEE International Conference on Network Protocols (ICNP)*, Toronto, Canada, 1999.

[16] A. Valko, "Cellular IP: A New Approach to Internet Host Mobility", *ACM Computer Communication Review*, Vol. 29, No. 1, pp. 50-65, January 1999.