Regional Aware Foreign Agent (RAFA) for Fast Local Handoffs
<draft-chuafoo-mobileip-rafa-00.txt>

Status of This Memo

   This document is a submission to the MobileIP Working Group of the
   Internet Engineering Task Force (IETF). Comments should be submitted
   to the mobile-ip@smallworks.com mailing list.

   Distribution of this memo is unlimited.

   This document is an Internet-Draft. Internet-Drafts are working
   documents of the Internet Engineering Task Force (IETF), its areas,
   and its working groups. Note that other groups may also distribute
   working documents as Internet-Drafts.

   Internet-Drafts are draft documents valid for a maximum of six months
   and may be updated, replaced, or obsoleted by other documents at any
   time. It is inappropriate to use Internet- Drafts as reference
   material or to cite them other than as ``work in progress.''

   To learn the current status of any Internet-Draft, please check the
   ``1id-abstracts.txt'' listing contained in the Internet-Drafts Shadow
   Directories on ftp.is.co.za (Africa), nic.nordu.net (North Europe),
   ftp.nis.garr.it (South Europe), munnari.oz.au (Pacific Rim),
   ftp.ietf.org (US East Coast), or ftp.isi.edu (US West Coast).

Abstract

   This document proposes an extension to the Mobile IP base protocol.
   The purpose of this extension is to solve the distant registrations,
   handoff latency, and key management problems among mobility agents.
   It provides a easy and robust solution for secure ubiquitous
   deployment of IP mobility while still maintaining interoperability
   with the base protocol.

Internet Draft   <draft-chuafoo-mobileip-rafa-00.txt>   November 1998

                              Contents

1. Introduction

   The base Mobile-IP scheme [1] provides a scalable mechanism for node
mobility within the Internet. However, there still exist some problems.
Firstly, it requires that a mobile node's home network be notified of
every change of location. As Perkins [2] addresses in the hierarchical
foreign agent model and M.C.Chuah [3] in the DREMIP model, in cases
where the home agent is far away, it may become too expensive or even
impossible to complete these frequent registrations. Furthermore, it
also adds more traffic to the wide-area portion of the internetwork.
Thus the current Mobile IP does not extend well to large numbers of
mobile nodes moving frequently between small wireless subnets.

   Secondly, the key management between the home and foreign agents, and
between the foreign agents and the mobile node is still a problem.
Mobile IP currently requires that registration messages between HA and
its MN be authenticated. Registration messages between an HA and an FA,
or between an MN and an FA, may be optionally authenticated. As more of
the networks MNs visit become wireless nets which are subject to
eavesdropping and unable to control actual attachment via physical
controls, authentication between FAs and HAs and between FAs and
MNs become mandatory for Mobile IP to succeed commercially.

   Thirdly, the Mobile-IP standard specifies a general handoff protocol
for both wired and wireless network. It incurs an intrinsic loss of data
up to a few seconds during handoff even in overlapping wireless subnets
due to the fact that the mobile node will only register with a new agent
if it fails to receive another advertisement from the current agent
within the specified lifetime. This often results in degraded throughput
which causes the handoff to be not as seamless. Thus, for mobile nodes
moving frequently between small wireless subnets, performance of future
IP applications such as IP telephony will be seriously affected.

   Fourthly, the base protocol does not require the mobile node to
inform the former foreign agent of the movement of the mobile node when
it moves from one foreign network to another. Thus, any correspondent
node in the former foreign network will not be able to route datagrams
to the mobile node until the registration lifetime of the binding has
expired which may take hundreds of seconds.

   In this draft document, we propose a new regional aware foreign agent
model as an extension to the base Mobile IP protocol to solve these
problems. Our proposed extension provides advantages over existing base
Mobile IP scheme while still maintaining interoperability.
   In particular, our proposed extension can
   a)   reduce frequent distant registrations during handoffs.
   b)   reduce the number of trusted entities in the network and hence
        enable us to minimise the key management problem.

c)   provide seamless handoff especially for small overlapping
         wireless cells to support multimedia data.

   d)   provide access control (authorization) in a foreign network and
        prevent an illegal mobile node from stealing services in a
        routing domain, and other services which may be very important
        for service providers so that gradual adoption is possible and
        might help in a more widespread deployment of Mobile-IP.
   e)   solve the inherent routing problem of the former foreign agent
        network as mentioned above when the MN moves to a new foreign
        agent network.
Importantly, the above advantage can be obtained without requiring any
changes in the base protocol implemented at the MN.

1.1. Requirements

   Any of the entities in the base protocol should be able to
interoperate with the new and enhanced entities in this regional aware
foreign agent (RAFA) model.

1.2. Architectural Entities

   The RAFA model introduces the following new architectural entities.

   Regional Aware Foreign Agent (RAFA)

      A host or router on a MN's visited routing domain which provides
      local registration service for an MN during handoff. It cooperates
      with the local foreign agents to allow the HA to have incomplete
      knowledgement of the MN's true point of attachment.

      It may be the tunnel endpoint of datagrams from the HA. It either
      extracts the datagrams and then tunnels datagrams to the local
      foreign agent for delivery to the MN or just acts as a simple
      router within a large routing domain.

      It therefore provides tunneling, registration and routing services
      to the MN while registered.

   Local Foreign Agent (LFA)

      It has the same functionality as the FA in the base protocol. It
      is a router on a MN's visited network which provides routing
      service to the MN while registered. It extracts and forwards
      datagrams to the MN.

      It has a security association with the regional aware foreign
      agent, and there is a slight modifications in the way it relays
      registration packets from the base protocol.

1.3. Terminology

   In addition to all the terminology in the base mobile-IP
specification, this document frequently uses the following terms:

   Anonymous Mobile Node

      A standard RFC2002 MN. However, with respect to the regional aware
      foreign agent, it is anonymous if the regional aware foreign agent
      does not have the information of the registration key shared
      between MN and HA.

   Registered Mobile Node

      A standard RFC2002 MN. However, with respect to the regional aware
      foreign agent, it is registered if the regional aware foreign
      agent has the information of the registration key shared between
      MN and HA.

   Enhanced Mobile Node

      A enhanced IETF base MN which is able to operate in two modes -
      IETF base mode and enhanced mode. Enhanced handoff feature is
      added to provide seamless handoff.

   Regionally Registered

      This means that the MN is a registered MN. It has a binding with
      the regional aware foreign agent. Datagrams from HA will be
      tunnelled to the regional aware foreign agent.

   Locally Registered

      This means that the MN is a anonymous MN. It has a binding with
      the local foreign agent. Datagrams from HA will be tunnelled to
      the local foreign agent.

2. Protocol Overview

   Using the proposed Regional-Aware Foreign Agent (RAFA) model,
latency incurred by the Registration process when a handoff occurs is
reduced as the MN would register with the regional aware foreign agent
which is nearer instead of its HA which may be far away. HA would only
know the regional aware foreign agent that is serving its MN. It does

not know its MN's true point of attachment.

2.1 Network Topology

   The network topology is shown in Fig 1 which consists of the
Home Agent (HA), Regional Aware Foreign Agent (RAFA), Local Foreign
Agent (LFA), Foreign Agent (FA) and Mobile Nodes (MN). Note that the HA,
FA and MN (base mode) are the entities in the base protocol, and we only
add two new entities - RAFA and LFA.
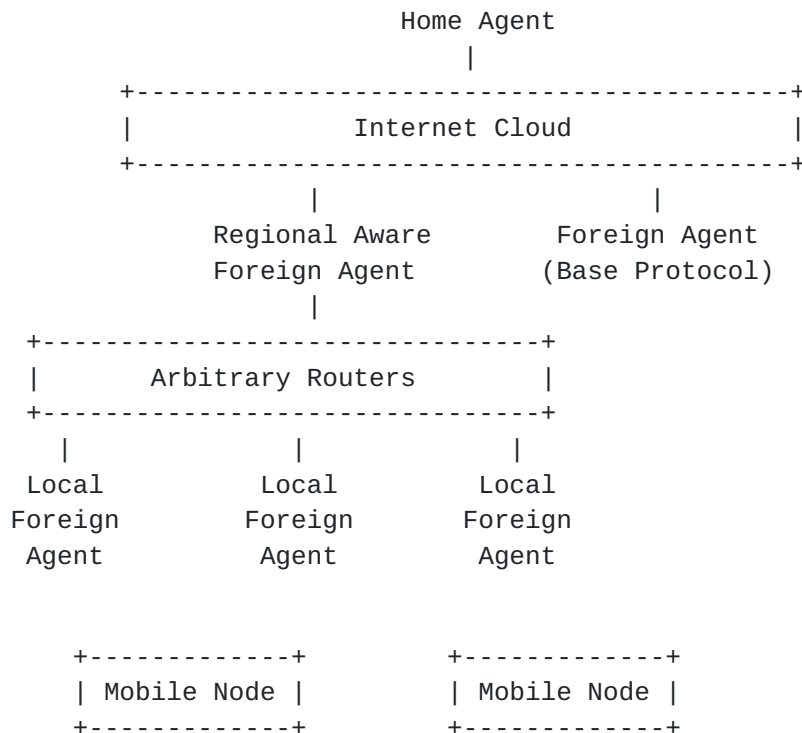
```
                          Home Agent
                              |
           +-------------------------------------------+
           |             Internet Cloud                |
           +-------------------------------------------+
                     |                        |
               Regional Aware           Foreign Agent
               Foreign Agent            (Base Protocol)
                     |
         +--------------------------------+
         |          Arbitrary Routers     |
         +--------------------------------+
            |              |              |
          Local          Local          Local
         Foreign        Foreign        Foreign
          Agent          Agent          Agent


         +-------------+          +-------------+
         | Mobile Node |          | Mobile Node |
         +-------------+          +-------------+


              Fig 1 : Network Topology
```

2.2 Agent Discovery

   MN detects a local foreign agent when it receives an agent
advertisement from it. This is equivalent to how the MN discovers an
agent in the base protocol.

2.3 Registration Process

   Under the RAFA model, depending on the handoff scenarios which can
take place between the networks of HA<->LFA, FA<->LFA and LFA<->LFA, the
Registration Request will either be directly relayed to the HA via the
local foreign agent if the MN is "locally registered" or via the
regional aware foreign agent if the MN is "regionally registered".

Likewise, the Registration Reply from the HA will be relayed to the MN
either via the local foreign agent if the MN is "locally registered" or
via regional aware foreign agent if the MN is "regionally registered".

2.3.1 **Processing of Registration Packets at LFA**

   During handoff, when the MN is not under the visitor list of a local foreign agent, the local foreign agent will relay the first-time Registration Request of the MN to the regional aware foreign agent. When the local foreign agent receives a reply with the proper authentication extension from the regional aware foreign agent, it will treat that the MN is "regionally registered" with the regional aware foreign agent. On the other hand, if it receives a reply directly from the HA, it will treat the MN as "locally registered".

   In the case of re-registration, if the MN is "regionally registered and has a binding with the regional aware foreign agent, the local foreign agent will relay the Registration Request to the regional aware foreign agent. If the MN is "locally registered" and has a binding directly with its HA, the local foreign agent will relay the Registration Request to the HA just like in the base protocol.

2.3.2 **Processing of Registration Packets at RAFA**

   Before the regional aware foreign agent relays the Registration Request from a MN, it will check whether it has the information on the shared registration key of the MN and its HA.

   If it has, it will relay the MN's Registration Request to its HA. The care of address field of the Registration Request is that of its care-of-of address instead of the care-of-address of the LFA. The HA will then have a mobility binding with the regional aware foreign agent.

   Otherwise, the regional aware foreign agent just forwards the Registration Request to the HA. The HA would then have a mobility binding with the local foreign agent instead.

2.4 **Typical Registration Scenarios**

   Different registration scenarios arise depending on whether

a) the regional aware foreign agent has the information of the shared
    registration key between HA and its MN
b) the MN is in the local foreign agent's visitor list or not
c) the MN handoffs from network of HA to LFA, FA to LFA, LFA to HA,
    LFA to FA or LFA to LFA

2.4.1   **MN handoffs from a FA network to a LFA network or**
        MN handoffs from a HA network to a LFA network.

   A first-time registration process at the local foreign agent consists
   of:

   a) MN receives a Mobility Agent Advertisement from a LFA
   b) MN sends a Registration Request to the LFA
   c) LFA forwards the received Registration Request to RAFA
   d) Depending whether RAFA has the information on the shared key, it
      either forwards or relays the Registration Request to the MN's HA.
      If RAFA has the shared key information, it changes the
      care-of-address field to its own care-of-address and relays to the
      HA without modifying the registration lifetime. Else, it merely
      forwards the Registration Request to the HA.
   e) HA processes the Registration Request in a similar way to that of
      the base protocol. It either sends a Registration Reply to RAFA if
      the care-of-address field in the Request is that of RAFA or to LFA
      if the care-of-address is that of LFA.
   f) If RAFA receives the Registration Reply from the HA, it updates
      its visiting MN list and relays the Reply to the LFA serving the
      MN. The LFA in turn updates the MN in its visitor list as
      "regionally registered" and sends the Reply to the visiting MN.

      In the case if HA sends a Registration Reply to LFA, upon
      receiving the reply, LFA updates the MN in its visitor list as
      "locally registered" and sends the Reply to the visiting MN.

For subsequent re-registration,

   a) For a "locally-registered MN", LFA relays the Registration
      Request to HA. HA will return a Registration Reply to the MN via
      LFA.

   b) For a "regionally-registered MN", LFA relays the Registration
      Request to HA via RAFA. HA will return a Registration Reply to the
      MN via RAFA and LFA

2.4.2   **MN handoffs from a LFA network to a FA network.**
        MN handoffs from a LFA network to a HA network.

   In this case, the Registration process follows that of the
Registration process in the base protocol.

2.4.3   **MN handoffs from a LFA network to a new LFA network within the same domain of a RAFA**

A first-time registration process at the new LFA consists of:

a) MN receives a Mobility Agent Advertisement from a new LFA
b) MN sends a Registration Request to the new LFA
c) The new LFA forwards the received Registration Request to the RAFA
d) Depending on whether MN is in its visitor list or not, RAFA either forwards the Registration Request to the MN's HA if MN is not in its visitor list or processes the Registration Request if MN is in its visitor list.

   If the MN is in its vistor list, RAFA updates the binding of the MN to the care of address of the new LFA. It will also send a Registration Reply on behalf of HA to the MN via the new LFA using the information of the shared registration key between HA and its MN.
e) When the new LFA receives the Registration Reply from either HA or RAFA, it updates its visiting MN list and sends the reply to the visiting MN. If it receives a Registration Reply from RAFA, the MN is "regionally registered". Else, the MN is "locally registered".

For subsequent re-registration,

a) For a "locally registered" MN, the new LFA relays the Registration Request directly to HA. HA will return a Registration Reply to the MN via the new LFA in a way similar to that in the base protocol.

b) For "regionally registered" MN, the new LFA relays the Registration Request to HA via RAFA. HA will return a Registration Reply to the MN via RAFA and then the new LFA.

2.5 **Datagram Routing**

Any packets addressed to the MN will be intercepted by its HA. The HA will tunnel the packets to the RAFA if the MN is "regionally registered". Otherwise, it will tunnel it to LFA/FA. Note that the registration process is transparent to the HA, and HA only tunnels datagrams to the MN according to the care-of-address of the MN's Registration Request as in the base protocol.

If the MN is "regionally registered", upon receiving the packets, RAFA refers to its visitor list and tunnels the packets to the appropriate LFA which is serving the MN. The LFA in turn forwards the packets to the MN. Else, LFA which receives packets directly from the HA

will just detunnel and forward packets as in the base protocol.

2.6 **Interoperability with the Base Protocol**

   The RAFA model is fully compatible with the base protocol as there
are no changes made in the MN and HA. Besides, it also supports all the
other implementations (related to Mobile-IP) such as route optimization,
simultaneous bindings at the HA etc. The network topology and operation
of the regional aware foreign agent and local foreign agent is totally
transparent to the MN and HA.

2.7 **Key Management/Distribution Scheme**

   The introduction of RAFA provides access control for the foreign
network and reduces frequent distant registrations during handoff. It
also reduces the number of trusted entities since the number of RAFA is
much less than the number of mobility agents and hence reduces the
severity of key management problem for Mobile-IP. In that sense, it is
more scalable. However, it requires the information on the shared
Registration key of HA and its MN. Note that even without the
information, handoff can still take place at the base protocol level in
our network topology. If the MN from some home network often visits a
routing domain under the RAFA, then the effort of creating such a
association will be worthwhile.

   Currently, besides manual configuration, there are many associated
key management/distribution approaches to solve this problem, and we can
do it either offline or dynamically. Doing it offline means that the
information of the shared key is distributed before the registration
process while doing it dynamically means that the information is
distributed during the registration process. But this requires slight
modification to the RAFA and LFA that we have described above, and the
RAFA must have a agreement with the HA about the distribution process.

   Two of these approaches can be employed to distribute (either offline
or dynamically) the shared Registration key of HA and MN to RAFA. They
are :

a) THE HA AS A KEY DISTRIBUTION CENTER (KDC)

   HA has a security association with RAFA. Using their shared key and
encryption, HA distributes its shared Registration key with its MN to
RAFA.

b) USING RAFA'S PUBLIC KEY

   HA uses the public key of RAFA and encryption to distribute its
shared Registration key with its MN to RAFA. RAFA can then use its
private key to obtain the shared Registration key of HA and MN.

MD5 can be used here for the purpose of transmitting registration
keys and secure eavesdroppers.

For offline distribution, RAFA and LFA work in the same way as described above. For dynamic distribution, this requires a bit of cooperation between the RAFA and LFA. When the RAFA receives a Registration Request, if it does not have the information of the shared key but has a agreement (security association) with the HA to distribute shared key information, it appends a Get Shared Key Notification extension in the Registration Request to be sent to the HA while notifying the LFA. The HA will then send the encrypted key to the RAFA using the agreed key distribution method with the RAFA, besides the normal Registration Reply to the LFA, which will treat the MN as "temporary locally registered".

When RAFA receives the information of the shared key, it will notify the LFA, which will then send the next Registration Request from the MN to the RAFA. RAFA with the information of the shared key will then proceed as described in the section on protocol overview. Note that in our description of the handoff scenarios, we do not elaborate the key distribution/management scheme as it is not part of the draft.

3. Local Foreign Agent (LFA) Considerations

The local foreign agent plays a mostly passive role just like the FA in the base Mobile-IP protocol. It functions almost exactly like the FA in the base protocol except the way it deals with Registration Request and Reply packets. It always sends the first Registration Request of a MN not in its visitor list to the regional aware foreign agent. It obtains the relevant information from the Registration Reply in order to decide whether to relay the subsequent Registration Request to the regional aware foreign agent or home agent.

3.1 Configuration and Registration Tables

Each local foreign agent has a security association with a list of regional aware foreign agents. In addition to the information maintained for the base protocol in the visitor list entry, the following information is also included - whether the MN is "regionally registered" at the care-of-address of the regional aware foreign agent or "locally registered" at its own care-of-address.

3.2 Receiving Registration Request

When the local foreign agent receives a Registration Request from an MN, it follows the base Mobile-IP protocol except when sending out the Registration Request. If the local foreign agent receives a Registration Request from a MN not in its visitor list, it will relay the first time Registration Request of the MN to the regional aware foreign agent

instead of the HA as specified in RFC2002. If the MN is in its visitor
list, it will check the list whether the MN is "regionally registered"

at the care-of-address of the regional aware foreign agent or "locally
registered" at its own care-of-address. If the MN is "regionally
registered", the local foreign agent will relay the Registration Request
packet to the regional aware foreign agent. Else, it will relay the
Registration Request to the HA as specified in the base protocol.

3.3 Receiving Registration Reply

   When the local foreign agent receives a Registration Reply, besides
following the base Mobile-IP protocol, it will check whether there is
a RAFA-LFA authentication extension with type 0x3. If yes, this means
that the MN is "regionally registered" at the care of address of the
regional aware foreign agent and the authenticator value in the
Registration Reply will be checked. The local foreign agent will update
its visitor list with the appropriate information that the MN is
"regionally registered" and will relay the Reply to the MN with all
the Extensions after the Mobile-Home Authentication Extension being
removed.

   If the authenticator is invalid, the local foreign agent will
silently discard the Reply and log the event as security exception. The
local foreign agent also will reject the MN's registration and send a
Registration Reply to the MN with Code 68. If no, this means that the MN
is "locally registered" at its own care-of-address. The local foreign
agent will update its visitor lists entry for the MN to reflect that the
MN is "locally registered" after doing the validity check and then it
forwards the Reply to the MN as specified in the base protocol.

3.4 Routing of Datagrams

   If the MN is "locally registered", the local foreign agent will
receive encapsulated datagrams from HA directly. Else, the local foreign
agent will receive encapsulated datagrams from the HA via the regional
aware foreign agent. The local foreign agent will decapsulate the
datagrams and forward them to the MN in exactly the same way as the FA
in the base protocol. Likewise, datagrams sent by the MN are generally
delivered to their destination using the standard IP routing mechanisms,
not necessarily passing through the regional aware foreign agent.

4. Regional Aware Foreign Agent (RAFA) Considerations

   The regional aware foreign agent plays a pro-active role in the
registration process. It performs local registration during handoff. It
is used to establish the local mobility binding of a MN. The local
mobility binding will enable it to tunnel the datagrams to the
respective local foreign agent which is serving the MN. Through the

registration process, it provides access control (authorization) over
the local foreign networks and prevent an illegal MN from stealing

services in a wider routing domain. It determines the services that the foreign network will provide for the MN.

4.1 Configuration and Registration Table

   Each regional aware foreign agent must be configured with a list of the local foreign agents which are under its routing domain with security associations. It may have information of the secret key shared between the MN and HA. In addition, for each pending or current registration, the regional aware foreign agent must maintain a visitor list entry containing the following information obtained from the MN's Registration Request.
- the IP Source Address (the mobile node's Home Address)
- the IP Destination Address
- the Home Agent address
- the care-of-address of the local foreign agent
- the Identification field
- the requested registration Lifetime
- the remaining Lifetime of the pending or current registration
The regional aware foreign agent may configure a maximum number of pending registrations that it is willing to maintain and additional registrations should then be rejected with code 66 just like that in the base protocol.

4.2 Receiving Registration Request

   When the regional aware foreign agent receives a Registration Request packet from the local foreign agent, it will perform the same validity check as that of the local foreign agent. If the regional aware foreign agent receives a Registration Request from a MN (via local foreign agent) in its visitor list, it will send a positive Registration Reply to the MN via local foreign agent using the information of the secret key shared by MN and HA. The Registration Reply contains the basic codes to inform the MN about the status of its Request plus a RAFA-LFA authentication extension to inform the local foreign agent that the MN is "regionally registered" or "locally registered", along with the lifetime granted by the regional aware foreign agent, which must not be great enough to last longer than time at which the binding at the HA would expire, as determined by the original lifetime granted by the MN's home agent in the last Registration Request approved by the HA.

    It must also update its record of the MN's mobility binding of which the care-of-address of the MN is the new local foreign agent and the Registration Request will then be silently discarded without forwarding to the HA. If the regional aware foreign agent receives a Registration Request from a MN not in its visitor list, it will check whether it has

the information of the secret key shared between the MN and HA, and
the care-of-address field of the Request is one of the local foreign
agent in its list. If there is information on the secret key and the

care-of-address is one of the local foreign agent, the regional aware
foreign agent will change the care-of-address field in the Registration
Request to its own care-of-address with a new MD5 authenticator [4]
being recomputed, and forward the Registration Request to the HA. It
must also record the new pending Request for the MN. If there is no
information of the secret key shared by MN and HA, the regional aware
foreign agent will relay the original Registration Request to the HA
without recording the pending Request if it allows services to an
anonymous MN of its local foreign agent network.

4.3 Receiving Registration Reply

   When the regional aware foreign agent receives a Registration Reply
message, it will search its visitor list for a pending Registration
Request with the same MN's home address as indicated in the Reply. If no
pending Request is found, the regional aware foreign agent will silently
discard the Reply. Else, it will forward the valid Registration Reply to
the local foreign agent after appending the RAFA-LFA authentication
Extension to the Reply using implicitly its own care-of-address as the
value for computed authenticator value. It then updates its visitor list
and resets its timer of the lifetime of the registration to the lifetime
granted in the Registration Reply like that of the FA in the base
protocol.

4.4 Routing of Datagrams

   The regional aware foreign agent has a binding for the mobile node
which shows that the MN is "regionally registered" at the
care-of-address of the next local foreign agent. Thus, a datagram
arriving from the home agent will be decapsulated and re-encapsulated
at the regional aware foreign agent with a new tunnel endpoint which is
the care-of-address of the local foreign agent which can deliver the
datagram to the mobile node. The actual decapsulation need not occur at
the regional aware foreign agent. Instead, the regional aware foreign
agent can merely change the source and destination IP addresses of the
encapsulating IP header. Note that the regional aware foreign agent is
not involved in any datagrams routing for MN which is "locally
registered" at the care-of-address of the local foreign agent.

4.5 Access Control (Authorization)/ Non-repudiation / Billing for
      Foreign Network

   The registration mechanism of which the local foreign agent always
relays the first Registration Request from the MN during handoff to the
regional aware foreign agent if MN is not in its visitor list provides
access control (authorization) over the visiting MNs for the regional

aware foreign agent. It can decide which MN is allowed visiting rights
and what network resources may be used by the visiting MN, whether it is

"regionally registered" or "locally registered". Priority can be given
to the MN which is "regionally registered" than one which is "locally
registered". Of course, the regional aware foreign agent can give equal
priority to all MNs but a "regionally registered" MN (registered MN)
will have better handoff performance than a "locally registered" MN
(anonymous MN).

   It can also control the number of visiting anonymous MNs. If the
traffic is low, the regional aware foreign agent may choose to provide
services for more anonymous MNs. If the traffic is high, it may even
choose to drop services for anonymous MN by sending a specific request
to the local foreign agent so that it can provide MNs which are
"regionally registered" with the scarce wireless network resources. Note
that the concept here is similar to the access control level allowed for
a host (anonymous login or user login) in any ftp session which is
commonly used in the Internet. For MN which is "regionally registered",
the regional aware foreign agent can also log some of its Requests so
that the MN cannot falsely deny that it originated the Requests at a
later time (non-repudiation). Likewise, it can log the Reply from the HA
so that the HA cannot falsely deny that it originated the Reply.
Nevertheless, it requires a trusted relationship between the HA and the
RAFA.

   The RAFA model also makes it easy for billing purposes when an MN
uses the precious wireless resources of a foreign network. Billing can
be easily done on a per RAFA basis (under the same administrative
domain) instead of per FA basis (may be under different administrative
domain).

   Hence, the RAFA model offers some kinds of security features, access
control and easy billing mechanisms that are especially important and
useful for commercial service providers. These are necessary for the
deployment of Mobile IP.

4.6 **Solving Inherent Functionality Problem of** Mobile IP

   The inherent functionality problem of any correspondent node in the
old foreign agent network will not be able to route datagrams to the MN
when it moves to a new foreign network until the registration lifetime
of the binding has expired which may take hundreds of seconds can be
easily solved in the RAFA model. The regional aware foreign agent may
send an explicit de-registration (preferably after a few seconds so as
to support simultanous bindings during the vulnerable period of handoff)
to the former foreign agent network to inform about the movement of MN.
This will enable the foreign agent to delete the MN's routing entry in
the routing table or release any resources (such as radio channel
reservations) consumed previously by an MN that is not in its network,

rather than waiting for its registration lifetime to expire.

4.7 Simultaneous Bindings

   The regional aware foreign agent can implicitly maintain multiple
simultaneous bindings for an MN, so that a copy of each datagram will be
tunneled to each active care-of-address of the local foreign agents
during handoff to the MN. Note that this simultaneous registration done
at the regional aware foreign agent (instead of HA in the base protocol)
is feasible as the duplication problem is not that severe since the
local foreign agents are normally just a few hops away from the regional
aware foreign agent.

4.8 Autonomous Mode Operation

   The RAFA model offers the possibility of autonomous mode operation
similar to that of the MOBITEX Network Architecture [5] if the link or
network connectivity between the regional aware foreign agent and MN's
HA is temporarily lost. This means that a MN can still communicate with
another MN if they are under the same local foreign agent or regional
aware foreign agent. The regional aware foreign agent can choose to
reply temporarily on behalf of the HA so that all the routing entries in
the local foreign agent and MN will remain intact for datagram routing
to take place. For a MN communicating with another MN under the same
local foreign agent, it will be able to do so as the route entry or
network resource is still available. However, for a MN communicating
with another MN under the same RAFA, LFA need to tunnel the packets from
the MN to RAFA which will then de-capsulated and tunnel the packets to
the appropriate LFA.

4.9 Multicast Data Routing Using the RAFA Model

   The RAFA model supports multicast services similar to the base
protocol. MN can either join the multicast group via a (local) multicast
router on the visited subnet or via a bi-directional tunnel to its home
agent. However, the RAFA model can reduce the multicast backbone traffic
compared to the base protocol. If more than one of its MNs which are
served by different FAs join the same multicast group, then the HA needs
only to send a single copy of the multicast to RAFA instead of multiple
copies of the multicast to the foreign agents. The reduction in backbone
traffic may be significant considering the fact that MNs of the same
multicast group have a tendency to be served by different FAs since they
may handoff to a foreign network frequently. Note that providing
multicast services for MNs that handoff frequently may be easy to do so
using the regional aware foreign agent as it is in charge of a larger
routing domain.

4.10 **Other Capabilities**

   The regional aware foreign agent can provide a mean for datagrams in
flight to the MN's previous local foreign agent to be forwarded securely
to its new local foreign agent. It can employ datagram buffering for
critical data at the local foreign agent serving the MN before a
handoff. It can then explicitly ask the local foreign agent to forward
the datagrams to another local foreign agent in a secure manner so that
there would be no loss of datagrams for the MN during handoff.
Simulation [6] has shown that buffering and forwarding last few packets
of the datagrams can significantly improve the TCP throughput during
handoff.

   Another capability of the RAFA model is that NAT and IP Masquerading
techniques in the RAFA model as the care-of-address of the local foreign
agent need not be real.

4.11 **Load balancing**

   Each of the regional aware foreign agent can occasionally probe their
regional aware foreign agent on the traffic load that each of them is
supporting. If the traffic load is high, it can order the local foreign
agent to forward new Requests to another regional aware foreign agent
with the least traffic.

5.   **Message Format and Extensions**

   There are a few new message formats and authentication Extensions in
the RAFA model.

5.1. **De-registration Request**

   De-registration Request is sent by the regional aware foreign agent
to the local foreign agent to delete the route entry of the MN when it
moves to a new local foreign agent network.
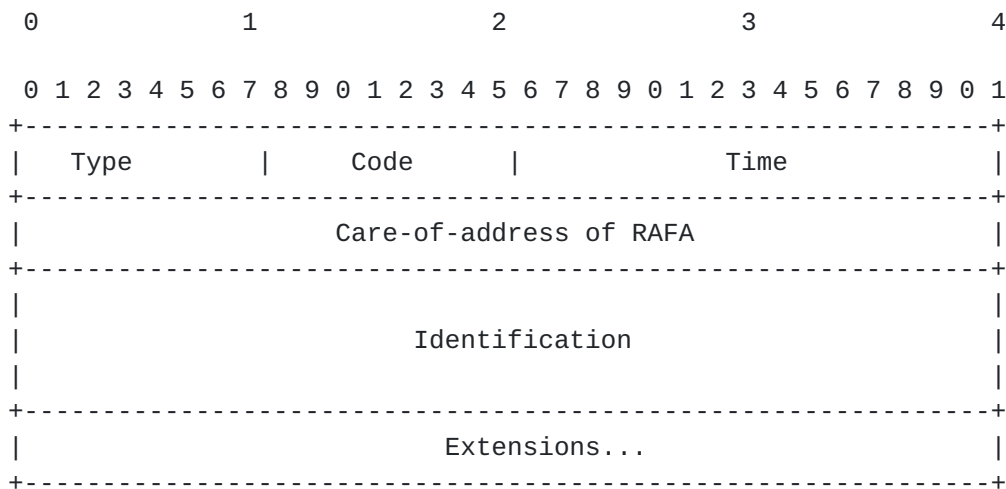
```
IP fields:
   Source Address        - The IP address of the regional aware foreign
                           agent
   Destination Address  - The IP address of the local foreign agent

UDP fields
   Source Ports          - Variable
   Destination Port     - 434
```

The UDP header is followed by the fields shown below

```
 0                 1                 2                 3                 4
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---------------------------------------------------------------+
|    Type       |     Code      |            Time               |
+---------------------------------------------------------------+
|                  Care-of-address of RAFA                      |
+---------------------------------------------------------------+
|                                                               |
|                      Identification                           |
|                                                               |
+---------------------------------------------------------------+
|                       Extensions...                           |
+---------------------------------------------------------------+
```

Type - 38

Code - 3 to indicate deletion

Time - The interval (seconds) needed to delete the route entry after
        receiving a de-registration request

Care-of-Address - IP address of the regional aware foreign agent

Identification - A 64 bit number used for protecting against reply
                 attacks of these messages

Extension - This is followed by the RAFA-LFA authentication Extension

5.2. Get Shared Key Notification Extension

   This extension is appended in the Registration Request message by the
RAFA so that the HA will send a encryted information of the shared key
of HA and its MN to it. Note that this extension is only required if we
want to support dynamic distribution of information of the shared key,
and may not be part of the RAFA model.

```
0               1               2               3               4

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---------------------------------------------------------------+
|   Type        |    Code       |             Lifetime          |
+---------------------------------------------------------------+
|                       RAFA's address                          |
+---------------------------------------------------------------+
|                                                               |
|                       Identification                          |
|                                                               |
+---------------------------------------------------------------+
|                       Extensions...                           |
+---------------------------------------------------------------+
```

Type - 11

Code - 5 to indicate the key distribution algorithm

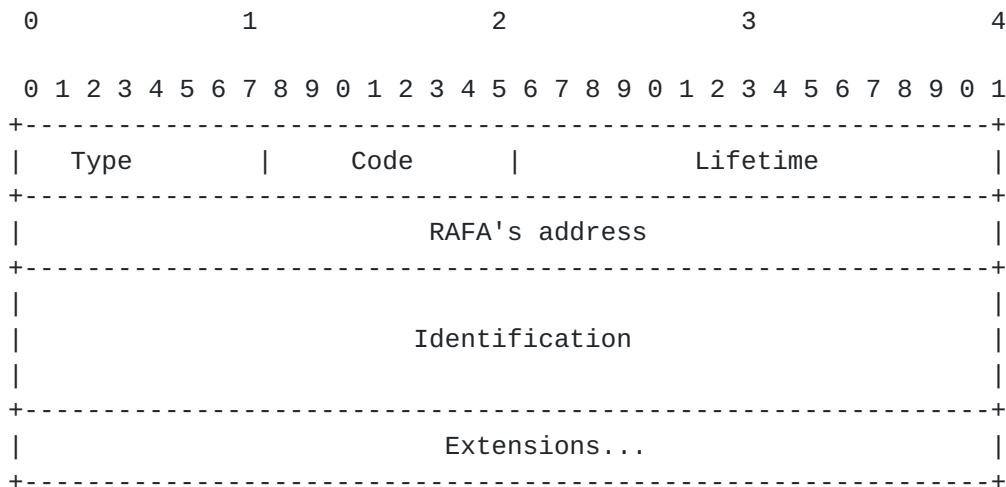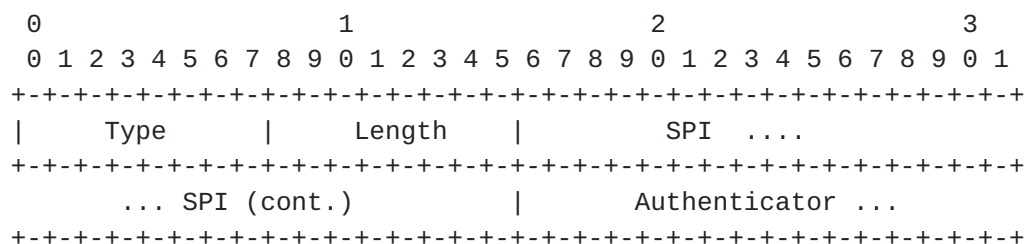Lifetime - time interval of which the Request is valid

RAFA's Address - IP address of the regional aware foreign agent

Identification - A 64 bit number used for protecting against reply
                 attacks of these messages

Extensions - followed by the HA-RAFA extension

5.3. RAFA-LFA Authentication Extension

   This extension is appended in the Registration Reply message by the
RAFA so that the LFA will know that the MN is "regionally registered".
The fields used are exactly the same as the base protocol except the
shared secret key is that between the RAFA and the LFA.

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |     Type      |    Length     |          SPI   ....
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
        ... SPI (cont.)            |       Authenticator ...
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

     Type   0x3

     Length   4 plus the number of bytes in the Authenticator.

     SPI   Security Parameter Index (4 bytes). An opaque identifier

Authenticator
                (variable length)

5.4. HA-RAFA Authentication Extension

This extension is appended in the Registration Request by the RAFA so
that the HA will send a encrypted version of the information of the
shared key to RAFA. It is required only if we want to distribute the
information of the shared key dynamically, and is not neccesary required
in the RAFA model.

```
  0                   1                   2                   3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |     Type      |     Length    |          SPI  ....
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |     ... SPI (cont.)           |       Authenticator ...
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

    Type   0x4

    Length   4 plus the number of bytes in the Authenticator.

    SPI   Security Parameter Index (4 bytes). An opaque identifier

    Authenticator
              (variable length)

6. Fast Handoff Considerations

The Mobile-IP base protocol standard specifies a general handoff
protocol for both wired and wireless networks. We believe that the
handoff protocol is more suited to handle portability and global
mobility (movement across different administrative domain) than local
mobility (within the same administrative domains where handoffs are
frequent like a network of wireless cells). In the Mobile-IP base
protocol, a handoff even in overlapping wireless small cells is not
seamless due to two main reasons - delay due to distant registration
and operational procedure of MN when it hears a new agent advertisement
(MN only registers with a new agent if it does not hear three
consecutive advertisements from the old FA which incurs a average delay
of 2.5 times the agent advertisement interval).

Using the RAFA model, we can reduce the delay due to distant
registration during handoff. To reduce the delay due to the
operational procedures of MN, we can either reduce the agent
advertisement interval or modify the handoff protocol of MN. We propose
a slight modification to the handoff protocol to provide seamless
handoff. However, it requires some minor changes in the LFA and MN. Note
that the changes in MN is to solve the handoff latency and is not

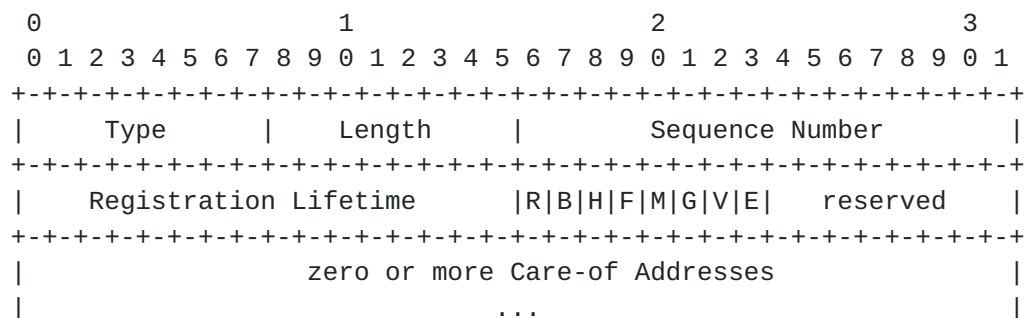necessarily required in the RAFA model.

   Instead of waiting for three consecutive missing advertisements in
the overlapping cells, the MN will immediately registers with the local
foreign agent once it hears a new advertisement. Note that this slight
modification is transparent to the HA and mobility agents in the base
protocol. This simple modification combined with simultaneous bindings
operation at the regional aware foreign agent will provide seamless
handoff between the local foreign agent networks which are overlapping.
Another option is to arrange the datagrams in flight when the MN moves
to be forwarded to the new LFA which will provide more seamless handoff.
In order to be interoperable with the base protocol, MN can operate in
two modes - base or enhanced mode according to the agent advertisement
it hears.

6.1 Local Foreign Agent (LFA) Considerations

   There is no modification to the way the LFA handles the Registration
Request and Registration Reply. Only the format of the agent
advertisement would be changed.

6.1.1 Sending Agent Advertisement

   A local foreign agent wishing to support the enhanced MN advertises
its services using the Mobility Extension to ICMP Router Advertisement
which is defined in the base Mobile-IP document. One bit (E) is added to
the flag bits in the Agent Advertisement message to indicate its
intention to support the enhanced MN with the modified handoff protocol.
(all other fields not defined here are unchanged from the definition
given in the base mobile-IP).


```
  0                   1                   2                   3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |     Type      |    Length     |        Sequence Number        |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |    Registration Lifetime      |R|B|H|F|M|G|V|E|   reserved    |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                   zero or more Care-of Addresses              |
 |                             ...                               |

    E               If set, the local foreign agent is advertising
                    its willingness to support the enhanced MN
```


6.2 MN considerations

   MN can operate in two modes - the base IETF mode and Enhanced Mode.

By default, the MN is operating in the base mode. It would only switch
to Enhanced mode if it receives an agent adevrtisement with the "E" bit
set.

6.2.1 Receiving Agent Advertisement

   When an MN receives an agent advertisement, it checks to see if the
"E" bit is set or not. If yes, the mobile node will switch from normal
base mode to Enhanced Mode. Instead of waiting for three missing
consecutive advertisements from the old FA before it sends its first
Registration Request, the MN will immediately send a Registration
Request.

6.3 Regional Aware Foreign Agent Considerations

   The regional aware foreign agent should support simultaneous bindings
if the local foreign agent supports the enhanced mode. A copy of each
datagram will be tunneled to each active care-of-address of the local
foreign agents to provide more seamless handoff to the MN.

References

[1] Charles Perkins, Editor, "IP Mobility Support", RFC 2002, October
    1996

[2] Charles Perkins, "Mobile-IP Local Registration with Hierachical
    Foreign Agents", Internet Draft,
    draft-perkins-mobileip-hierfa-00.txt, February 1996, Work in
    Progress

[3] M.C. Chuah, Y. Li, "Distributed Registration Extension to Mobile
    IP", Internet Draft, draft-chuahli-mobileip-dremip-00.txt", October
    1997

[4] R. Rivest, S. Dusse, "The MD5 Message-Digest Algorithm",
    RFC 1321, April 1992.

[5] Salkintzis, A.K. and Chamzas, C. "Mobile Packet Data Technology: An
    Insight into MOBILTEX Architecture", IEEE Personal Communications
    Mag, Feb 1997, pp. 10-18

[6] W. Woo, C.M Leung, "Handoff Enhancement in Mobile-IP Environment",
    Proceedings of ICUPC - 5th International Conference on Universal
    Personal Communications, 29 Sept. - 2 Oct. 1996

Author's Address

Dr K. C. CHUA
Deputy Director

Centre for Wireless Communications   Ph: +65 8729 030
20 Science Park Road   DID: +65 8709 222
#02-34/37, Teletech Park   Fax: +65 7795 441
Singapore Science Park II
Singapore 117674

Email: eleckc@leonis.nus.edu.sg
URL: www.cwc.nus.edu.sg

S. F. Foo
National University of Singapore
Department of Electrical Engineering
Lower Kent Ridge Cresent
Singapore 119260

Email: engp7498@leonis.nus.edu.sg   Ph: +65 8745 095