Internet Engineering Task Force   R. Ramjee / T. La Porta
INTERNET-DRAFT   S. Thuel / K. Varadhan
draft-ramjee-micro-mobility-hawaii-00.txt   Lucent Bell Labs
19 February 1999
Expires: 19 August 1999

IP micro-mobility support using HAWAII

Status of this memo

Abstract

In this contribution, we present HAWAII: a domain-based approach for supporting mobility. HAWAII uses specialized path setup schemes which install host-based forwarding entries in specific routers to support intra-domain micro-mobility and defaults to using Mobile-IP for inter-domain macro-mobility. These path setup schemes deliver excellent performance by reducing mobility related disruption to user applications, and by operating locally, reduce the number of mobility related updates. Also, in HAWAII, mobile hosts retain their network address while moving within the domain, simplifying Quality of Service support. Furthermore, reliability is achieved through the use of soft-state forwarding entries for the mobile hosts, and the elimination of foreign agents and, in some cases, the home agent.

Contents

1 Introduction

Mobile-IP is the current standard for supporting macro-mobility in IP networks [6]. Mobile-IP defines two entities to provide mobility support: a home agent (HA) and a foreign agent (FA). The HA is statically assigned to a mobile host based on the permanent home IP address of the mobile host. The FA is assigned to the mobile host based on its current location. The FA has associated with it an IP address called the care-of address. Packets sent to the mobile host are intercepted by the HA and tunneled to the FA at the care-of address. The FA then decapsulates the packets and forwards them directly to the mobile host. Thus, Mobile-IP provides a good framework for allowing users to roam outside their home networks. When Mobile-IP is used for micro-mobility support, it results in high control overhead due to frequent notifications to the HA. Also, in the case of a Quality of Service (QoS) enabled mobile host, acquiring a new care-of address on every handoff would trigger the establishment of new QoS reservations from the HA to the FA even though most of the path remains unchanged. Thus, while Mobile-IP should be the basis for mobility management in wide-area wireless data networks, it has several limitations when applied to wide-area wireless networks with high mobility users that may require QoS. Our aim is to extend Mobile IP to address these limitations using Handoff-Aware Wireless Access Internet Infrastructure (HAWAII).

1.1 Goals

We have three design goals:

- o Achieve good performance by reducing update traffic to home agent and corresponding hosts, avoiding triangular routing where possible, and limiting disruption to user traffic.
- o Provide intrinsic support for QoS in the mobility management solution, including allowing per flow QoS and limiting the number of reservations that must be re-established when hosts move.
- o Enhance reliability. We require HAWAII to be no less fault tolerant than existing Mobile-IP proposals, and we explore additional mechanisms to improve the robustness of mobility support.

1.2 Assumptions

Our proposal for supporting mobility hinges on the assumption that most user mobility is local to a domain, in particular, an

administrative domain of the network. Since an administrative domain is under the control of a single authority, it is possible to relax the assumption that there is no special support for mobility available in the domain infrastructure. Therefore, we consider optimizations in routing and forwarding in the domain routers for more efficient support of intra-domain mobility.

1.3 Terminology

Domain

A division of the wireless access network. It consists of one or more routers and multiple base stations. It will appear as a subnet to routers external to the domain.

Domain Root Router

The gateway router into a domain is called the domain root router.

Home Domain

Each mobile host is assigned a home domain based on its permanent IP address.

Foreign Domain

Any domain that is not the mobile host's home domain is referred to as its foreign domain.

Path Setup Scheme

A particular method of updating the routers in a domain so that connectivity to the mobile host is maintained across handoffs.

1.4 Design Overview

In this section, we present the architecture of HAWAII. There are three separate components to HAWAII: 1) To achieve maximum transparency in mobility, we consider a two-level hierarchy along domain boundaries, and define separate mechanisms for intra-domain mobility and inter-domain mobility. We conjecture that mobility across domains is likely to be a rare occurrence and default to using Mobile-IP for inter-domain mobility. To provide straight-forward QoS support, we assign a unique, co-located care-of address to the mobile host; 2) To maintain end-to-end connectivity with little disruption as the mobile host moves, we establish special paths to the mobile host; and finally, 3) To provide a degree of tolerance to router or link failures within the network, we use soft-state mechanisms for maintaining forwarding state. We discuss each of these issues separately in the following sections.

1.4.1 Network Architecture

```
                         ___             ___
                        |   | Internet  |   |
                        |   |  Core     |   |
                        |___|           |___|
                            x\         /
                             x\       /
                              x\ ____/
                               x|    |  Regular IP Packets      xxxxx
                                x    |  Encapsulated IP Packets @@@@@
                                |x___|  Domain Boundaries       *****
                                x /\
           ********************x /  \**************************
          *                   x /*  *\                        *
         *       Home        x /  **  \         Foreign        *
        *        Domain    _x_/   *    \ ___    Domain          *
       *         Root --->|x@@@@@@@@@@@@@@@ |<--Root             *
      *          Router   |x  |   *     | @ |   Router            *
     *                    |x__|   *     |_@_|                      *
    *  Home Domain         x      *       @      Foreign Domain     *
    *                    x x x    *      @@@                        *
    *                  x  x  x    *     @  @ @                      *
    *                x   x    x   *    @   @   @                    *
    *              x     x    x   *   @     @    @                  *
    *            x      x      x  *  @      @      @                *
    *         ___              x  *               ___               *
    *        |   |                *              |   | Mobile       *
    *        |   |                *              |   | Host         *
    *        |___|----->------->--*--->----->--->|___|              *
    *                             *                                 *
    * Movement        Movement across domains     Movement within   *
    * within domain   (HA notified of co-located  domain (no HA     *
    * (no HA involved)  care-of address)           notification)    *
```

Figure 1: Hierarchy

A common approach for providing transparent mobility to correspondent hosts is to divide the network into hierarchies. In HAWAII we define a hierarchy based on domains. The network architecture is illustrated in Figure 1. The gateway into each domain is called the

domain root router. Each host has an IP address and a home domain. For the moment, we defer the discussion of how this address could be assigned later (Section 5). When moving in its home domain, the mobile host retains its IP address. Packets destined to the mobile host reach the domain root router based on the subnet address of the domain and are then forwarded over special dynamically established paths to the mobile host. This allows the home domain to cover a large area made up of hundreds of base stations, thereby increasing the probability that a mobile host is in its home domain. For these mobile hosts, a home agent is not involved in the data path, resulting in enhanced reliability and efficient routing.

When the mobile host moves into a foreign domain, we revert to traditional Mobile-IP mechanisms. If the foreign domain is also based on HAWAII, then the mobile host is assigned a co-located care-of address from its foreign domain. Packets are tunneled to the care-of address by a home agent in its home domain. When moving within the foreign domain, the mobile host retains its care-of address unchanged (thus, the HA is not notified of these movements); connectivity is maintained using dynamically established paths in the foreign domain.

The design choices of using co-located care-of addresses and maintaining the mobile host address unchanged within a domain simplifies per flow QoS support as discussed in Section 4.2. This choice also eliminates the need for a FA in the domain, thereby enhancing reliability. Also, in Mobile-IPv6 [2], the FA is eliminated and the co-located care-of address option is used. One drawback of using the co-located care-of address option is the need for two IP addresses for each mobile host that is away from its home domain. This exacerbates the limited IP address availability problem. One possible optimization is to adapt the ``dialup'' model used by ISPs to wireless networks. This is discussed in Section 5.

1.4.2 Path Setup Schemes

As described above, HAWAII assigns a unique address for each mobile host that is retained as long as the mobile host remains within its current domain. In this context, maintaining end-to-end connectivity to the mobile host requires special techniques for managing user mobility. HAWAII uses path setup messages to establish and update host-based routing entries for the mobile hosts in selective routers in the domain so that packets arriving at the domain root router can reach the mobile host. The choice of when, how, and which routers are updated constitutes a particular path setup scheme. In Section 2, we describe two such path setup schemes.

One important question in using host-based forwarding in the domain routers is scalability. It is because of scalability considerations that we use Mobile-IP mechanisms for inter-domain mobility. In Section 4.1, we present a numerical example showing how a single domain in HAWAII can cover an area of approximately 1000Km2 without any difficulty in processing mobility related updates.

1.4.3 Soft-State

The notion of ``soft-state'' refers to state established within routers that needs to be periodically refreshed; otherwise, it is removed automatically when a preset timer associated with that state expires. The HAWAII path state within the routers is soft-state. This increases the robustness of the protocol to router and link failures.

Our protocol uses two types of control messages, updates and refreshes, to establish and maintain the soft-state respectively. Path setup updates are sent by the mobile host during power up and following a handoff. These messages are explicitly acknowledged by the recipient. Path setup refresh messages are sent periodically by mobile hosts. Aggregate refresh messages are sent periodically by base stations and routers in a hop-by-hop manner to the router upstream of the mobile hosts. As we shall see in the following sections, path messages are sent to only selected routers in the domain, resulting in very little overhead associated with maintaining soft-state.

2 Path Setup Schemes

Path setup update messages are sent by the mobile host during power up and following a handoff. We first discuss the update procedure for power up. We then describe two algorithms by which update messages in HAWAII are used to re-establish path state after handoffs.

When the mobile host powers up, it sends a path setup update message to its nearest base station. This message propagates to the domain root router. Each router in the path between the mobile host and the domain root router adds a forwarding entry for the mobile host. Finally, the domain root router sends back an acknowledgement to the mobile host. At this time, when packets destined for the mobile host arrive at the domain root router based on the subnet portion of the mobile host's IP address, the packets are routed within the domain to the mobile host using the host-based forwarding entries just established. Note that other routers in the domain have no specific knowledge of this mobile host's IP address. In the case of mobile to mobile communication, packets arriving at a router that has no specific host-based entry are routed using a default route. The packets eventually reach an upstream router (in the worst case, the domain root router) which has a forwarding entry for the mobile host.

We now describe the operations of two path setup schemes used to re-establish path state when the mobile host moves from one base station to another within the same domain. We assume a tree-based topology for the discussion although the path setup schemes work with any arbitrary topology. For the remaining subsections, let us define the cross-over router as the router closest to the mobile host that is at the intersection of two paths, one between the domain root router and the old base station, and the second between the old base station and the new base station. In both path setup schemes, forwarding entries during handoff are added so that packets are either forwarded from the old base station or diverted from the cross-over router to the new base station. This property ensures us against the possibility of persistent loops after the handoff update.

There are two variants of the path setup schemes, motivated by two types of wireless networks. The Forwarding scheme is optimized for networks where the mobile host is able to listen/transmit to only one base station as in the case of a Time Division Multiple Access (TDMA) network. The Non-Forwarding scheme is optimized for networks where the mobile host is able to listen/transmit to two or more base stations simultaneously for a short duration, as in the case of a WaveLAN or Code Division Multiple Access (CDMA) network. These are described below.

2.1   Forwarding Path Setup Scheme

In this path setup scheme, packets are first forwarded from the old base station to the new base station before they are diverted at the cross-over router.

The Forwarding scheme is illustrated in Figure 2. The forwarding table entries are shown adjacent to the routers. These entries are prepended with a message number indicating which message was responsible for establishing the entry (a message number of zero indicates a pre-existing entry). The letters denote the different interfaces. The path setup message is first sent by the mobile host to the old base station. The message contains the new base station's address. The old base station performs a routing table lookup for the new base station and determines the interface, interface A, and next hop router, Router 1. The base station then adds a forwarding entry for the mobile host's IP address with the outgoing interface set to interface A. It then forwards the message to Router 1 (shown as message 2 in Figure 2). Router 1 performs similar actions and forwards the message to Router 0. Router 0, the cross-over router in this case, adds forwarding entries that result in new packets being diverted to the mobile host at the new base station. It then forwards the message towards the new base station. Eventually the message reaches the new base station (shown as message 5 in Figure 2). The new base station changes its forwarding entry and sends an acknowledgement of the path setup message to the mobile host (shown as message 6 in Figure 2).

```
                                    |             (0):1.1.1.1->B
                                ---------         (3):1.1.1.1->C
                                |   A   |
                       ROUTER 0 |       |
                                | B   C |
                          @@@@@>--------- @@@@@
                          @     /  @@@@ \     @
                        3 @    /  @    @ \    @ 4
                          @   /  @      @ \   @
                          @  /   @      @  \  v
                ROUTER 1---------@      @--------- ROUTER 2
                        |   A   |@      @|   A   |
        (0):1.1.1.1->C  |       |@      @|       | (0):Default->A
        (2):1.1.1.1->A  | B   C |@      @| B   C | (4):1.1.1.1->B
                        ---------@      @---------
                          ^   |  @      @  |  @
                        2 @   |  @      @  |  @ 5
                          @   |  @      @  |  @
                          @   |  @      @  |  v
                   OLD BS -----<@       @  ----- NEW BS
                         /  A  \        @ /  A  \
        (0):1.1.1.1->B  |       |       @|       |  (0):Default->A
        (1):1.1.1.1->A   \  B  /        @ \  B  /   (5):1.1.1.1->B
                          -----       1 @  -----
                                       @     @  6
                                      @      @
                                   ---- <@@@@@
                           MOBILE /    \
                           USER   \    /
                                   ----
                               IP:1.1.1.1
```

Figure 2: Forwarding path setup scheme

Note that only the new and old base stations, and the routers connecting them, are involved in processing the path setup message. Also, only routers on the path between the new base station and the domain root router will receive the periodic refresh messages. Therefore, the entries in Router 1 and the old base station, which are no longer on this path, will time-out, while the entries in Routers 0 and 2, and the new base station will get refreshed.

2.2   Non-Forwarding Path Setup Scheme

```
                                    |             (0):1.1.1.1->B
                                ---------         (3):1.1.1.1->C
                                |   A   |
                       ROUTER 0 |       |
                                | B   C |
                          @@@@@@---------<@@@@@
                          @     /  @@@@ \     @
                        4 @    /  @    @ \    @ 3
                          @   /  @      @ \   @
                          v  /   @      @  \  @
                ROUTER 1---------@      @--------- ROUTER 2
                        |   A   |@      @|   A   |
        (0):1.1.1.1->C  |       |@      @|       | (0):Default->A
        (4):1.1.1.1->A  | B   C |@      @| B   C | (2):1.1.1.1->B
                        ---------@      @---------
                           @  |  @      @  |  ^
                         5 @  |  @      @  |  @ 2
                           @  |  @      @  |  @
                           v  |  @      @  |  @
                   OLD BS ----- @       @  ----- NEW BS
                         /  A  \        @ /  A  \
        (0):1.1.1.1->B  |       |       @|       |  (0):Default->A
        (5):1.1.1.1->A   \  B  /      6 @ \  B  /   (1):1.1.1.1->B
                          -----         @  --^--
                                       @@    @
                                      @      @ 1
                                   --v- @@@@@@
                           MOBILE /    \
                           USER   \    /
                                   ----
                               IP:1.1.1.1
```

Figure 3: Non-Forwarding path setup scheme

In this path setup scheme, as the path setup message travels from the new base station to the old base station, data packets are diverted at the cross-over router to the new base station, resulting in no forwarding of packets from the old base station.

The Non-Forwarding scheme is illustrated in Figure 3. In this case, when the new base station receives the path setup message, it adds a forwarding entry for the mobile host's IP address with the outgoing interface set to the interface on which it received this message. It then performs a routing table lookup for the old base station and determines the next hop router, Router 2. The new base station then forwards the path setup message to Router 2 (shown as message 2 in Figure 3). This router performs similar actions and forwards the message to Router 0. At Router 0, the cross-over router in this case, forwarding entries are added such that new packets are diverted directly to the mobile host at the new base station. Eventually the message reaches the old base station (shown as message 5 in Figure 3). The old base station changes its forwarding entry and sends an acknowledgement of the path setup message back to the mobile host (shown as message 6 in Figure 3).

3   Protocol Processing

In this section, we describe the protocol processing details of HAWAII path setup schemes. We first describe the format for the path setup update and refresh messages. We then present the processing at the mobile host and finally, the protocol processing at the base stations/routers.

3.1   Message Formats

The format of an update path setup message sent by a mobile host is shown below. The message is sent using the UDP protocol to a reserved port. Power up updates (type 1) are sent to the current base station. Handoff updates (type 2) are sent to the old base station in the case of the Forwarding scheme, and to the new base station in the case of the Non-Forwarding scheme. At present, we do not have a power down update as we rely on the time out of the soft state forwarding entries. It is conceivable to define an explicit tear down message to handle this case.

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Version| Type  |           Scheme              |    Reason     +
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                   Mobile Host Address                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                   Old Base Station                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                   New Base Station                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                      Timestamp                                +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Extensions ...
+-+-+-+-+-+-+-+-
```

```
Version                 1
Type                    1 (Power up update), 2 (handoff update),
                        3 (acknowledgement)
Scheme                  1 (Forwarding), 2 (Non-Forwarding)
Reason                  Used only for Type 3 messages
                        0   accepted
                        1   poorly formatted message
                        2   authentication failed
                        3   Scheme not supported
Mobile host Address     Home address in Home domain,
                        Care-of address in Foreign domain
Old Base Station        Old Base Station IP address for Type 2
                        0.0.0.0 for Type 1
New Base Station        New Base Station IP address for Type 2
                        Current Base Station for Type 1
Timestamp               Timestamp formatted as in
                        Network Time Protocol [3].
Extensions              Authentication field
                        Wireless link specific fields, for more study
```

The format for a refresh message is shown next. The message would contain only one entry when sent by a mobile host and could contain multiple entries as part of an aggregate refresh when sent by base stations and routers to their upstream router.

```
  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
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |Version|  Type |           Size                |     Reason    +
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                   Mobile Host Address[1]                      |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                                                               |
 +                      Timestamp[1]                             +
 |                                                               |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                             ...
                             ...
                             ...
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                   Mobile Host Address[N]                      |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                                                               |
 +                      Timestamp[N]                             +
 |                                                               |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 | Extensions ...
 +-+-+-+-+-+-+-+-
```

```
Version                 1
Type                    4 (refresh)
Size                    Number of mobile host entries
Reason                  0 (normal)
                        1 (triggered due to link/host failure)
Mobile host Address     Host-entry address
Timestamp               Host-entry timestamp
Extensions              Authentication field
```

3.2   Mobile Host Processing

The processing requirements for a mobile host depends on whether it is attached to its home domain or a foreign domain. When it is in its home domain, the mobile host executes a HAWAII client process. The operation of the HAWAII client is depicted in Figure 4.

When the HAWAII client process begins execution, it reads the host's configuration parameters (such as its IP address) and sends a power up update to the domain root router. It then waits for an acknowledgement in the INIT state. If an acknowledgment is received, the host enters the ATTACHED state, where it can send and receive packets. If an acknowledgment is not received after a certain period of time, the host resends the update message possibly multiple times until it finally receives an acknowledgement or decides to abandon executing the client process. If attachment is successful, the mobile host periodically sends a refresh message to the base station to which it is attached. The base station will, in turn, generate hop-by-hop refresh messages upstream, as described earlier.

```
                        On startup, send
              ++++++++  power up update  ++++++++  ____  On timeout,
             +        +---------------> +        +/    | resend power up
             +  NULL  +                 +  INIT  +     |   update
             +        + <---------------+        + <--/
              ++++++++  Give up resends  ++++++++
                                            ^ |
                 ^ Give up   Inter-domain   | | Receive ack from
                 | resends   handoff, send  | | domain root router
   On timeout,   |           power up update| |
   resend        |                          | v
   updates       |     Receive ack from     |
      ____  +++++++++    base station   ++++++++++  ____
     |    \+         +---------------> +          +/    | Send periodic
     |     + HANDOFF +                 + ATTACHED +     | refreshes
      \--> +         + <---------------+          + <--/
            +++++++++    Intra-domain   ++++++++++
                         handoff, send
                         handoff update
```

Figure 4: HAWAII Client State Diagram

When the mobile host moves to a new base station, if a domain boundary is crossed, the mobility client is notified that a inter-domain handoff has occurred and it is also informed of the new care-of address. The host then triggers the creation of host-based forwarding entries in the new domain through a power up update. If the mobile host moves to a new base station but does not cross a domain boundary, then the HAWAII client is notified of a intra-domain handoff. It is also informed of the IP address of the new base-station. The client then triggers a handoff update message and moves into the HANDOFF state. If the acknowledgement is received, the host returns to the ATTACHED state. If not, the host continues to send handoff update messages and wait for a reply until it succeeds in getting a reply or decides to abandon executing the client process.

There are several ways in which the handoff detection and notification may be implemented. A typical solution is to have the base stations send beacons periodically with their IP address and a domain identifier. A mobile client monitoring these beacons can then detect handoffs and it will have the necessary configuration information for its operation. If it is necessary to interoperate with existing base station beacons which do not contain information regarding IP addresses or domain identifiers, then it is possible to have the mobile client query the base station by sending link layer point to point messages. The details of different query response mechanisms are to be discussed.

As stated earlier, there are additional processing requirements when the mobile host is in a foreign domain. The mobile host needs a mechanism for acquiring a care-of address (such as a DHCP client) and a co-located foreign agent as in Mobile-IP [6]. The mobile host must first acquire its care-of address before the HAWAII client sends a power up update in the new domain. After the update processing is completed, the foreign agent will register the care-of address with its home agent.

3.3 Base Station/Router Processing

The pseudo-code for processing an power up update message in both the Forwarding and Non-forwarding schemes is shown in Figure 5. Each base station simply adds an entry for the mobile host and forwards the message to next hop router along its ``default'' route. Note that we assume that the default route is the same as the route to a domain root router (gateway). When the message reaches a domain root router, an acknowledgement is sent to the mobile host.

```
--------------------------------------------------------------------
Figure 5: HAWAII power up Update processing for both schemes
--------------------------------------------------------------------
1. Receive Power Up Update message from mobile host on Interface 1
2. Message contains MH IP ADDRESS, TIMESTAMP
3. Add/Update entry {MH IP ADDRESS -> Interface 1}, set timer
4. If I am the Domain Root Router
     Generate an acknowledgement back to the MH
   else
     Forward update to upstream neighbor along the default route
   endif
--------------------------------------------------------------------
```

The pseudo-code for processing an update message in the Forwarding and Non-Forwarding schemes is shown in Figure 6(a) and Figure 6(b) respectively. The processing of an update message is fairly simple: on receiving the message, modify the forwarding entry for the mobile host in the kernel and forward the update message towards its destination.

```
------------------------------------------------------------------
Figure 6(a): HAWAII handoff processing for the Forwarding scheme
------------------------------------------------------------------
1. Receive Update message from neighbor on Interface 1
2. Message contains MH IP ADDRESS, OLD BS ADDRESS, TIMESTAMP
3. If NEW BS ADDRESS matches one of my interface addresses then
     Let Interface 2 be my wireless interface
   else
     Look up routing table for NEW BS ADDRESS and determine
       next hop router and outgoing interface Interface 2
   endif
4. If TIMESTAMP is newer then
     Add/Update entry {MH IP ADDRESS -> Interface 2}, set timer
   endif
5. If NEW BS ADDRESS matches one of my interface addresses then
     Generate an acknowledgement back to the MH
   else
     Forward message to next hop router determined in step 3
   endif
------------------------------------------------------------------
Figure 6(b): HAWAII handoff processing for the Non-forwarding scheme
------------------------------------------------------------------
1. Receive Update message from neighbor on Interface 1
2. Message contains MH IP ADDRESS, OLD BS ADDRESS, TIMESTAMP
3. If TIMESTAMP is newer then
     Add/Update entry {MH IP ADDRESS -> Interface 1}, set timer
   endif
4. If OLD BS ADDRESS matches one of my interface addresses then
     Generate an acknowledgement back to the MH
   else
     Look up routing table to find next hop router for OLD BS ADDRESS
     Forward message to next hop router
   endif
------------------------------------------------------------------
```

The soft-state refresh messages are sent independently by each of the nodes on a hop by hop basis. The mobile host refreshes the base station every TH seconds. The base stations and routers send refreshes to their upstream routers (determined based on their default route to the domain root router) every TR seconds. Typically TH would be much larger than TR in order to conserve the limited wireless bandwidth. When the refresh message is received, the expiry timer corresponding to the refresh entry is updated. This involves no update to the kernel routing table and can be done very efficiently. Furthermore, a single refresh message can refresh several mobile hosts, thus amortizing on the cost of sending/receiving the message. The pseudo-code for processing a refresh message is shown in Figure 7. One important point to note is the need for a user-specific timestamp in the path setup messages. The timestamp guards against a potential race-condition involving a soft-state refresh from an old base station competing with a recent update message from a new base station.

```
--------------------------------------------------------------------
Figure 7: HAWAII refresh processing for both schemes
--------------------------------------------------------------------
1. Receive Refresh message from authenticated neighbor on Interface 1
2. Message contains multiple tuples of {MH IP ADDRESS, TIMESTAMP}
3. For each tuple do
     If entry exists for MH IP ADDRESS then
       If TIMESTAMP is greater than timestamp in the entry then
         If entry already has interface as Interface 1
            /* Most common case - no failure */
            reset timer on forwarding entry
         else
            /* interface changed failure,don't propagate up */
            update entry {MH IP ADDRESS -> Interface 1}, set timer
         endif
       endif
     else
       /* Non-existent MH entry failure, propagate up */
       Add entry {MH IP ADDRESS -> Interface 1}, set timer
       Send immediate update (batched) using the default route
     endif
4. Periodically send batch refresh upstream for all entries
5. When the default route changes
     send batch refresh upstream for all entries
-------------------------------------------------------------------
```

4 Design Implications

In this section, we illustrate the advantages of the HAWAII approach by studying the implications on scalability, QoS support, and reliability.

4.1 Scalability

In this section, we illustrate the advantages of HAWAII's local mobility through a numerical example. Consider a domain with configuration parameters as shown in Table 1. The domain is in the form of a tree with three levels: at the highest level there is a single domain router; at the second level there are seven intermediate routers; at the third and lowest level, there are 140 base stations (twenty per router). We also assume that the coverage area of a base station is a square with a given perimeter. For this configuration, we compute the rate of mobility related messages for two different approaches: 1) Mobile-IP approach where FAs are present at each base station and are served by a HA and 2) the HAWAII approach where the HA is at the domain root router.

Table 1: Domain Configuration values

Item	Type	Value
B	Base stations per domain root router	140
R	Second level router per domain root router=(B/S)	7
D	User density (active users)	39 per sq km
V	User speed	112 km/hr
TR	Router refresh timer for HAWAII	30 seconds
Y	No. of mobile host entries in refresh in HAWAII	25
TM	Mobile-IP binding lifetime	300 seconds
Z	Fraction of users in foreign domain in HAWAII	0.1
LB	Perimeter of base station	10.6 km
A	Coverage area of domain = B*LB*LB/16 =	980 sq km
LD	Perimeter of domain = SquareRoot(A)*4 =	125.2 km
LR	Perimeter of 2nd level router=SquareRoot(A/R)*4	47.3 km
N	Number of users in domain = B*D =	38,720

First note that the coverage area of this domain is quite large: A = 980km2. If we need to scale to larger areas, we would use Mobile-IP to handoff between these domains. The number of forwarding entries at the domain root router in the case of the HAWAII approach is the same as the total number of active users in the domain, and is N = 38, 220. This is well within the capability of a modern router. Furthermore, a majority of these entries are completely specified entries of hosts from a particular domain/subnet. In this case, perfect hashing is possible resulting in O(1) memory access for IP route lookup. Thus, route lookup for data forwarding can be done efficiently at the domain routers.

We now compute the impact of mobility-related messages for the two approaches. First consider a system based on Mobile-IP. Assuming the direction of user movement is uniformly distributed over [0,2pi] and using a fluid flow mobility model [5], the rate of mobile hosts crossing a boundary of perimeter l at a speed V is given by f(l)=(D*V*l)/(3600*pi). Since user handoffs between any two base stations in the domain generates an update registration at the HA, the number of mobility related updates at the HA from B base stations is f(LB)*B. The rate of registration renewals for N users is N/TM since every renewal period, each user send out one renewal request.

Now consider a system based on HAWAII. The domain root router, which houses the home agent, is the most heavily loaded router in this system as it has to process both path setup messages as well as Mobile-IP messages. The rate of Mobile-IP registrations, which occur only when user cross domain boundaries, is f(LD). The rate of Mobile-IP registration renewals, which are sent by only those users that are away from their home domain, is (Z*N)/TM. Path setup updates at the domain root router are generated whenever a user is handed off between base stations attached to two different second level routers. Thus, the rate of path setup updates is f(LR)*R. Path setup refreshes are aggregates, generated for each user. Thus, the rate of path setup refreshes is (Ceiling(N/Y)/TR).

Table 2: Frequency of Mobility related messages (per second)

Type	HAWAII at Domain Root Router	Mobile-IP at Home Agent
HAWAII update	127.8	0
HAWAII refresh	51.3	0
Mobile-IP registration	48.4	574
Mobile-IP renewals	12.7	127.4
Total	240.2	701.4

The frequency of various mobility related messages for the configuration shown in Table 1 is summarized in Table 2. The total number of control messages received by a HA in Mobile-IP (701.4) is almost three times the number of messages received by a domain root router in HAWAII (240.2).

4.2 Quality of Service Support

The fact that HAWAII maintains the IP address of the mobile host unchanged within a domain even as it moves simplifies the provision of flow-based QoS. In this section, we illustrate the ease with which the well-known resource reservation protocol, RSVP [9], is integrated with HAWAII.

```
                ________________
               |CORRESPONDENT   |---
               |HOST AS SENDER  |   |
               |________________|   ~
                IP:2.2.1.1          ~      [1.1.1.1->C]*** 1
                                    |                    * Asynchronous
                                ---------                v notification
                                |   A   |  {DEST, PHOP, NHOP}
                       ROUTER 0 |       |  {(0):2.2.1.1,A,B}
                                | B   C |  {(7):2.2.1.1,A,C}
                                ------+--<+++++
                                /    @ \      +
                               /      @ \     + 7
                              /      2 @ \    +
                             /          v \   +
                ROUTER 1---------        --------- ROUTER 2
                        |   A   |        |   A   |
           [1.1.1.1->A] |       |        |       | [1.1.1.1->B]
                        | B   C |        | B   C |
                        ---------        ---------   {DEST, PHOP, NHOP}
                            |             @  |  ^    {(2):2.2.1.1,A,-}
                            |           3 @  |  + 6  {(6):2.2.1.1,A,B}
                            |             @  |  +
                            |             v  |  +
                   OLD BS -----            ----- NEW BS
                         /  A  \          /  A  \
                        |       |        |       |
           [1.1.1.1->A]  \  B  /          \  B  /   [1.1.1.1->B]
                          -----       4    @-^--
                                     @@@@@@@ +      {DEST, PHOP, NHOP}
                                     @       + 5    {(3):1.1.1.1,A,-}
                                   --v- ++++++      {(5):1.1.1.1,A,B}
                      MOBILE HOST /    \
                      AS RECEIVER \    /           @@@@@> PATH
                                   ----            +++++> RESV
                               IP:1.1.1.1
```

Figure 8: RSVP flows when mobile host is a receiver

RSVP inherently assumes that hosts have fixed addresses, which is usually not the case for mobile hosts. When using Mobile-IP, the mobile host's home address is fixed, but its care-of-address changes. Since RSVP uses the destination address of the end node, i.e. the mobile host, for identifying a session, one has to redo the resource reservation along the entire path from the correspondent host (or HA) to the mobile host on every handoff of the mobile user. This must be performed even though most of the path is probably unchanged, as handoff is a local phenomenon. This results in increased reservation restoration latency and unnecessary control traffic.

In the case of HAWAII, support for QoS is straightforward since a mobile host's address remains unchanged as long as the user remains within a domain. The interaction between HAWAII and RSVP when the mobile host is a receiver is shown in Figure 8. The state in the square braces represents HAWAII forwarding state while the state in the curly braces represents RSVP state. After Router 0 processes a HAWAII path setup update, its RSVP daemon receives a path change notification (PCN) (message 1) using the routing interface for RSVP [8]. In standard RSVP, the router must now wait a time interval before generating the RSVP PATH message to allow the route to stabilize; this time interval is set to two seconds by default. In HAWAII, the RSVP PATH message (message 2) can be triggered immediately on receiving a PCN since the route to the mobile host is stable at that point. This allows for a faster reconfiguration due to mobility. The PATH message follows the new routing path (messages 2 and 3), installing PATH state on all the routers towards the new base station. When this PATH message reaches the mobile host, a QoS agent on the host generates an RSVP RESV message upstream that follows the reverse forwarding path (messages 5, 6, and 7). Router 0 stops forwarding the RESV messages upstream since there is no change in the reservation state to be forwarded. Thus, reservations are restored locally in a timely manner. The case when the mobile host is a sender is fairly simple. A RSVP PATH message is sent by the mobile host after handoff as soon as the HAWAII path setup is complete, resulting in reservations along the new path.

Note that the straightforward integration of RSVP and HAWAII is due to the fact that RSVP was designed to blindly follow the routing path established and maintained by an independent routing entity. The HAWAII path setup messages for a mobile host handoff are no different from any other routing changes to which RSVP was designed to respond. Thus, intra-domain handoffs in HAWAII are handled efficiently; since they are localized, they result in fast reservation restorations for the mobile user. In the case of inter-domain handoffs, since HAWAII defaults to Mobile-IP for mobility management, reservation restorations would follow along the procedures elaborated by the Mobile-IP working group.

4.3 Reliability

Failure of Home Agents is a concern for any approach that is based on Mobile-IP. In HAWAII as well as Mobile-IP, this failure could be tackled through the configuration and advertisement of backup home agents. Other approaches that rely on hot backups are also possible. However, recall that in HAWAII, in the common case of a mobile host not leaving its ``home'' domain, there is no HA involved. This greatly reduces HAWAII's vulnerability to HA failure as compared to the Mobile-IP schemes. Furthermore, HAWAII does not have any foreign agents inside the network architecture, eliminating another source of failure. Consequently, approaches in which the FA and the HA lie in the data path between the correspondent host and the mobile host suffer from reliability concerns not present in the HAWAII approach.

Link and router failures are handled through the soft-state refresh mechanism in HAWAII. The routing daemon running at each router would detect these failures and update its default route entry. This will trigger an immediate soft-state refresh of all its host entries to a new uplink router (see Figure 7 for details). This will result in further propagation of soft-state refresh messages until a router that has pre-existing entries for the affected mobile hosts is notified (this will be the domain root router in the worst case).

Finally, we need to address the issue of failure of HAWAII process itself without an accompanying router failure. To recover, the HAWAII process must simply be restarted as the subsequent soft-state refreshes correct the existing state. This may be addressed by several means. For instance, a process monitor resident in the same router as the HAWAII process could issue a restart upon detecting a non-responsive process.

5 Address Assignment

So far we have not made specific assumptions about how each mobile host acquires its IP addresses. In particular, we do not assume any correlation between the domain topology hierarchy and the actual address assignments to mobile hosts. Instead, we assume a flat address assignment algorithm in the domain. To put it another way, mobile hosts are assigned the next available address in the domain when they request one.

Recall that, in HAWAII, each host potentially needs two IP addresses: one to operate in its home domain, and (possibly) a second when it moves outside its home domain. The first address can be assigned statically by manual configuration, that then leaves open the question of how inter-domain mobility should be handled.

Alternately, and this is the approach preferred by HAWAII, we could use DHCP to acquire both the addresses dynamically. We explore each of these options in the following paragraphs.

An option is manual configuration of the home address, but this has implications when the host moves outside its home domain. In this situation, when the host moves outside its home domain, it has to either acquire a co-located care-of-address for itself through manual configuration or other means. Alternately, it might use a foreign agent in the new domain, and act as a ``vanilla'' mobile-IP agent; however, it then needs to attach itself to a new foreign agent every time it moves, even within the new domain, mitigating the gains possible in using HAWAII.

The other option is to acquire both the home address and the co-located care-of-address through DHCP [1]. The mobile can retain the home address for the duration of its lifetime; we call this the quasi-permanent address of the mobile. This domain also becomes the mobile host's home domain. Because mobile hosts typically act as clients, as they activate applications, their servers will learn their IP addresses. If the mobile host moves into a different domain while powered up, it is assigned a second IP address through DHCP in the new domain. This address becomes the mobile host's co-located care-of address. The mobile host still retains the quasi permanent address assigned in its home network, and packets are tunneled to/from a home agent in its home network to its current location. In this way, mobility is transparent to the corresponding servers and applications. When the host is powered down, it gives back all its assigned addresses (permanent address and care-of address, if any).

This requires modifying the client side of DHCP so that the client maintains leasing relationships with two different DHCP servers at the same time. The exact nature of this modification and its implications to DHCP are outside the scope of this specification.

The use of a quasi permanent address is similar to the ``dialup'' model of service provided by Internet Service Providers to fixed hosts. The difference is that the users in HAWAII are mobile and the home domain is determined by where the host is powered up rather than which modem access number is dialed. Apart from requiring fewer IP addresses, this optimization also results in optimal routing as long as the user does not move out of a domain while powered up.

6 Security

There are two issues in security: user authentication by the DHCP server during address assignment, that occurs during power up and inter-domain moves; and security and authentication related to HAWAII protocol messages.

This document does not specify solutions for addressing the security issues related to DHCP server authentication of a mobile user. Mechanisms such as the RADIUS protocol [7] could be used to perform the authentication. After the IP address assignment phase, a user specific key would be downloaded into the current base station.

A second issue is to disallow arbitrary users from sending path setup messages, thereby subverting another host's traffic. The path setup messages we propose can be made secure because they all require the old base station to cooperate. The new base station can ensure that all handoff update path setup messages are destined for some base station. When the mobile host is handed off to a new base station, the old base station approves of the path setup message only if the mobile host is able to authenticate itself in the path setup message. The user specific key can then be transferred from the user's old base station to the new base station. An advantage of this approach is that authentication is performed at the base stations (except during power up) in a distributed fashion. This approach also results in a natural protocol for key management where the user-specific key is handed off with the user from one base station to another. If the key management cannot be distributed, it is possible to have a centralized authentication server and have the base stations authenticate the path setup messages using this server.

Appendix A - Patent Issues

This is to inform you that Lucent Technologies has applied for and/or has patent(s) that relates to the attached submission.

This submission is being made pursuant to the provisions of IETF IPR Policy, RFC 2026, Sections 10.3.1 and 10.3.2.

Lucent Technologies Inc. will offer patent licenses for submissions made by it which are adopted as a standard by your organization as follows:

> If part(s) of a submission by Lucent is included in a standard and Lucent has patents and/or pending applications that are essential to implementation of the included part(s) in said standard, Lucent is prepared to grant - on the basis of reciprocity (grantback) - a license on such included part(s) on reasonable, non-discriminatory terms and conditions.

References

[1] R. Droms, `` Dynamic Host Configuration Protocol,'' Request for Comments 2131, Mar 1997.

[2] D. Johnson and C. Perkins, ``Mobility Support in IPv6,'' Internet Draft, Work in Progress, Nov 1998.

[3] G. Malkin, ``RIP Version 2 Carrying Additional Information,'' Request for Comments 1723, Nov 1994.

[4] D. Mills, "Network Time Protocol (Version 3): Specification, Implementation and Analysis", RFC 1305, Mar 1992.

[5] S. Mohan and R. Jain, ``Two User Location Strategies for Personal Communications Services,'' IEEE Personal Communications, Vol 1., No. 1, pp. 42-50.

[6] C.E. Perkins, ``IP Mobility Support,'' Request for Comments 2002, Oct 1996.

[7] C. Rigney, A. Rubens, W. Simpson, and S. Willens, ``Remote Authentication Dial in User Service (RADIUS),'' Request for Comments 2138, Apr 1997.

[8] D. Zappala and J. Kann., "RSRR: A Routing Interface for RSVP", Internet Draft, Jul 1998

[9] B. Braden et. al., ``Resource Reservation Protocol (RSVP) -
Version 1 Functional Specification,'' Request for Comments 2205,
Sep 1997.

Authors' Addresses

R. Ramjee, T. La Porta, S. Thuel, and K. Varadhan
Bell Labs, Lucent Technologies,
101 Crawfords Corner Road,
Holmdel, NJ 07733 (USA)
Phone: 732-949-3306
Fax: 732-949-4513
Email: {ramjee,tlp,thuel,kvaradhan}@bell-labs.com