Mobile IP Based Micro Mobility Management Protocol in The Third Generation Wireless Network

Status of this Memo

This document is an Internet Draft and is in full conformance with all provisions of Section 10 of RFC2026. Internet Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and 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 anytime. It is inappropriate to use Internet Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.
This document defines extensions to the Mobile IP protocol [1] to allow mobility management for the interface between a radio network and a packet data network in the third generation cdma2000 network.

Mobile IP requires link layer connectivity between the Mobile Node and the Foreign Agent. This draft proposes a protocol for achieving this when the physical layer terminates at a point distant from the FA. In particular, this protocol applies to cdma2000 networks where the physical layer terminates at a Radio Network Node (RNN) and the FA resides inside a separate Packet Data Serving Node (PDSN). The PDSN is responsible for establishing, maintaining, and terminating the link layer to the Mobile Node. A RNN is responsible for relaying the link layer protocol between a Mobile Node and its corresponding PDSN.

The interface between the RNN and the PDSN is called the RP interface. This interface requires mobility management for handling handoff from one RNN to another without interrupting end to end communication. It also requires the support of the link layer protocol encapsulation.

1. Introduction

This document defines extensions to the Mobile IP protocol [1] to allow mobility management for the interface between a radio network and a packet data network in the third generation cdma2000 network.

Mobile IP requires link layer connectivity between the Mobile Node and the Foreign Agent. This draft proposes a protocol for achieving this when the physical layer terminates at a point distant from the FA. In particular, this protocol applies to cdma2000 networks where the physical layer terminates at a Radio Network Node (RNN) and the FA resides inside a separate Packet Data Serving Node (PDSN). The PDSN is responsible for establishing, maintaining, and terminating the link layer to the Mobile Node. A RNN is responsible for relaying the link layer protocol between a Mobile Node and its corresponding PDSN.

The interface between the RNN and the PDSN is called the RP interface. This interface requires mobility management for handling handoff from one RNN to another without interrupting end to end communication. It also requires the support of the link layer protocol encapsulation.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC-2119].
3. cdma2000 Network RP Interface Overview

The high level architecture of a third generation cdma2000 network RP interface is shown in Figure 1.

```
+---------+    +---------+    +---------+
|         |    |         |    |         |
|   RNN   |----RP------|  PDSN   |---------|  HA     |
|         |    |         |    |         |         |
+---------+    +---------+    +---------+
/|
| Visited Access                Home Network |
| Provider Network               |
/|
| Mobile                         |
| Node                           |
+--------+

Figure 1: The Third Generation cdma2000 Network RP Interface
```

In above figure 1, the PDSN will be responsible for establishing, maintaining, and terminating the link layer to the Mobile Node. It initiates the authentication, authorization, and accounting for the Mobile Node and optionally, securely tunnels to the Home Agent.

The RNN is responsible for mapping the Mobile Node identifier reference to a unique link layer identifier used to communicate with the PDSN. RNN validates the Mobile Station for access service and manages the physical layer connection to the Mobile Node.

4. Mobile IP Extensions

This section describes extensions to the Mobile IP protocol for the RP interface within the third generation cdma2000 network.

4.1 Registration Request

In a cdma2000 network, the mobile node initiates a connection by sending a call setup indication to the RNN across the radio network. When this indication is received by a RNN, a Registration Request will be sent from the RNN to the PDSN to setup a new RP session.
A RNN MUST send a Registration Request with the GRE encapsulation and the reverse tunneling bit set. The Home Address field is set to zero. The Home Agent field will be assigned to the IP address of the PDSN and the Care-of Address field will be assigned to the IP address of RNN.

When a Registration Request is received by a PDSN, the information from the Session Specific Extension (see next section) will be used to identify a RP session. When a registration is accepted, a GRE tunnel will be created for this Mobile Node.

The fields of the Registration Request message are shown below:

```
  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      |S|B|D|M|G|V|T| |          Lifetime             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Home Address                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           Home Agent                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Care-of Address                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
+                         Identification                        +
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Extensions ...                                                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

<table>
<thead>
<tr>
<th>Type</th>
<th>1 (Registration Request)</th>
</tr>
</thead>
<tbody>
<tr>
<td>G</td>
<td>This bit MUST be set to 1 for GRE tunneling.</td>
</tr>
<tr>
<td>T</td>
<td>This bit MUST be set to 1 for reverse tunneling.</td>
</tr>
</tbody>
</table>

Home Address
The field is set to zero.

Home Agent
This field is assigned to the IP address of the PDSN.

Care-of Address
This field is assigned to the IP address of RNN.

Extensions
The Session Specific Extension as described in the next section MUST be included along with the ones described in RFC2002. Specifically, the MN-HA Authentication extension as described in RFC2002 MUST be included along with this extension.
4.2 Session Specific Extension

This extension is defined to carry information related to the session between a Mobile Node and its serving PDSN.

The detailed format of the extension is shown as follows.

```
+-----------------+------------------+------------------+-
<table>
<thead>
<tr>
<th>Type</th>
<th>Length</th>
<th>Protocol Type</th>
</tr>
</thead>
</table>
+-----------------+------------------+------------------+-
|                           Key                                 |
|-----------------|-----------------|-----------------|
+-----------------+------------------+------------------+-
|         reserved              |       MN Connection ID        |
|-----------------|-----------------|-----------------|
+-----------------+------------------+------------------+-
<table>
<thead>
<tr>
<th>MN ID Type</th>
<th>MN ID Length</th>
<th>MN ID</th>
</tr>
</thead>
</table>
+-----------------+------------------+------------------+-
|                           MN ID ...                          |
```

Type           TBD. Its value shall be in the range of 0 to 127.

Length         This is a one octet field and it indicates the length (in bytes) of the extension, NOT including the Type and Length fields.

Protocol Type  This is a two octet field. It indicates the type of the protocol to be tunneled across the RP interface. It is same as the Protocol Type field in the GRE header.

Key            This is a four octet value assigned by the RNN and inserted in every GRE frame across the RP interface during user data tunneling.

Reserved       This is a two octet field. It is not used and is set to zero.

MN Connection ID

Xu et al.               Expires 22 April 2000                       5

Internet Draft               3G Wireless              22 October 1999

This is a two octet field and it is used to differentiate the multiple sessions from the same Mobile Node. It is locally unique to a Mobile Node.

MN ID Type

This is a two octet field and it indicates the type of the following Mobile Node ID value. For example, value 1 defines IMSI (International Mobile Serial Identifier) and 2 Ethernet MAC
address.

**MN ID Length**
This is a one octet field and it indicates the length (in bytes) of the following Mobile Node ID field.

**MN ID**
This is the Mobile Node ID, which is globally unique. It is used to uniquely identify a Mobile Node.

This extension MUST be included in the Registration Request and Registration Update (see section 4.5) messages. It will be included before the MN-HA Authentication extension in the Registration Request message and before the Registration Update Authentication Extension in the Registration Update message.

The MN ID and the MN Connection ID together will uniquely identify a Mobile Session.

### 4.3 Registration Reply

The Registration Reply will be sent by a PDSN following the procedure as described in [1]. The Home Address field will be the same value as the Home Address field from the corresponding Registration Request message received by the PDSN.

### 4.4 Vendor/Organization Specific Extensions

Dommety [4] proposes two types of Vendor/Organization Specific extensions. These extensions will be used for carrying any third generation cdma2000 network specific information. They may appear in the Registration Request and Registration Update messages as needed.

### 4.5 Registration Update/Acknowledge

Two new messages are defined to support PDSN initiated RP tunnel tear down and to speed up resource reclamation on the RNN.

The Registration Update message is used for notification of the change of the registration associated with a call. It shall be sent by the PDSN to the previous RNN when a RNN to RNN handoff happens.

Both messages are sent with UDP using well-known port number 434.

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>++</td>
<td>++</td>
<td>++</td>
<td>++</td>
</tr>
<tr>
<td>Type</td>
<td>Reserved</td>
<td>Home Address</td>
<td>Home Agent Address</td>
</tr>
</tbody>
</table>
The format of the Registration Update message is illustrated above, and contains the following fields:

Type           TBD
Reserved       Sent as 0; ignored on reception.
Home Address   Sent as 0;
Home Agent Address
The IP Address of the PDSN.
Identification
A 64-bit number assigned by the node sending the Registration Update message. It is used to assist in matching requests with replies, and in protecting against replay attacks.
Extensions
Both Registration Update Authentication Extension (see section 4.6) and Session Specific Extension (see section 4.2) SHALL be included.

A Registration Update shall be sent by a PDSN to indicate the closure of a RP session. The RNN may reclaim the resource associated with that session.

A Registration Acknowledge message is used to acknowledge receipt of a Registration Update message. It MUST be sent by a node receiving a Registration Update message.
The format of the Registration Acknowledge message is illustrated above, and contains the following fields:

- **Type**: TBD
- **Status**: If the Status is nonzero, this acknowledgment is negative.
- **Reserved**: Sent as 0; ignored on reception.
- **Home Address**: Copied from the Registration Update message being acknowledged.
- **Care of Address**: The IP address of the RNN.
- **Identification**: Copied from the Registration Update message being acknowledged.
- **Extensions**: Registration Update Authentication Extension SHALL be included.

Allowable values for the Status include:

- 0  successful acknowledgement
- 128 reason unspecified
- 129 administratively prohibited
- 133 identification mismatch
- 134 poorly formed Registration Update

### 4.6 Registration Update Authentication Extension

Xu et al.  Expires 22 April 2000  8

Internet Draft  3G Wireless  22 October 1999

The Registration Update Authentication extension is used to authenticate the Registration Update and Registration Acknowledge messages. It has the same format and default algorithm support requirements as the authentication extension defined for Mobile IP protocol [1], but with a different type (TBD). The authenticator value is computed from the stream of bytes including the shared secret, the UDP payload all prior extensions in their entirety, and the type and length of this extension, but not including the authenticator field itself nor the UDP header. The secret used for computing the authenticator field is shared between the RN and PDSN. This extension is required in both Registration Update and Registration Acknowledge messages.

### 4.7 Summary
The extensions to Mobile IP include enabling the GRE encapsulation and reverse tunneling during Registration. A new extension called Session Specific Extension is defined and is mandatory in both Registration Request and Registration Update messages. The Home Address field MUST be set to zero in the Registration Request, Registration Reply, Registration Update and Registration Acknowledge messages.

Two new messages (Registration Update/Acknowledge) are defined to support the RP session disconnection in order to speed up resource reclamation.

5.0 GRE Encapsulation

GRE encapsulation as described in [3] shall be supported during user data transmission. A new protocol type might be required to support the link layer protocol defined for the third generation cdma2000 network. The Key field shall be required and its value shall be same as the one from the Session Specific Extension as described above. The sequence number may be required, depending on the requirement of the protocol encapsulated within the GRE frame.

During traffic tunneling, the sender will insert the Key value from the Registration Request message into the Key field of the GRE header. The receiver will use the Key value from the GRE header to decide where to forward the user data.

6.0 Security Considerations

The protocol presented in this draft is designed for use over a protected, private network between RNN and PDSN. Pre-arranged security associations in the style of Mobile IPv4 are assumed to exist among every (RNN, PDSN) pair that will form an RP connection. Also, it is assumed that the session specific information is authenticated by means outside the scope of this draft.

Several potential vulnerabilities exist if these assumptions are not met. First, if the network connecting the RNN and PDSN is accessible to an attacker, user traffic may be intercepted and/or spoofed if there are no other end-to-end security mechanisms in place. Second, the Mobile IP control messages must be authenticated, to prevent tunnel setup and tear down by unauthorized parties. Mobile IP Authentication Extensions are used to provide this additional protection for control messages. Finally, if session specific information is not authenticated, a denial-of-service attack is possible if a RNN unknowingly sends a registration request to the PDSN with a spoofed session specific extension. The PDSN would then send an explicit tunnel tear down to the previous RNN, causing user traffic to be misdirected to the new RNN. This would cause a loss of service and possibly interception of traffic, depending on what other security measures are in place.

References

Authors Addresses

Yingchun Xu                  Rajesh Bhalla
3Com Corporation             3Com Corporation
1800 West Central Rd.        1800 W. Central Road
Mount Prospect,              Mt. Prospect,
USA 60056                   IL 60056
Phone: (847) 342-6814        Phone: (847) 797-2618
Email: Yingchun_Xu@3com.com  Email: rajesh_bhalla@3com.com

Karl Freter                  Ed Campbell
3Com Corporation             3Com Corporation
1800 W. Central Road 1800 W. Central Road
Mt. Prospect, IL 60056       Mt. Prospect, IL 60056
Phone: (847) 222-2268        Phone: (847) 342-6769
Email: karl_freter@3com.com  Email: ed_campbell@3com.com

Xu et al.               Expires 22 April 2000                      10
Internet Draft               3G Wireless                       22 October 1999

Eileen McGrath Hadwen
Alcatel
PO Box 4442, Boulder CO 80306
Phone: 303 499 1496
Mobile: 303 517 0407
Email: mcgrath.hadwen@worldnet.att.net

Gopal Dommety                Kirit Joshi
Cisco Systems                Cisco Systems
170 West Tasman Drive        170 West Tasman Drive
San Jose, CA 95134           San Jose, CA 95134
Phone: (408) 525-1404        Phone: (408) 525 7367
Email: gdommety@cisco.com    Email: kjoshi@cisco.com

Parviz Yegani
Ericsson Wireless Communication Inc.
6455 Lusk Blvd.
San Diego, CA 92121
Phone: (858) 332-6017
Email: p.yegani@ericsson.com