Internet Research Task Force (IRTF)
Request for Comments: 5726
Category: Experimental
ISSN: 2070-1721

Y. Qiu
Institute for Infocomm Research
F. Zhao, Ed.
Google
R. Koodli
Cisco Systems

February 2010

Mobile IPv6 Location Privacy Solutions

Abstract

Mobile IPv6 (RFC 3775) enables a mobile node to remain reachable while it roams on the Internet. However, the location and movement of the mobile node can be revealed by the IP addresses used in signaling or data packets. In this document, we consider the Mobile IPv6 location privacy problem described in RFC 4882, and propose efficient and secure techniques to protect location privacy of the mobile node. This document is a product of the IP Mobility Optimizations (MobOpts) Research Group.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for examination, experimental implementation, and evaluation.

This document defines an Experimental Protocol for the Internet community. This document is a product of the Internet Research Task Force (IRTF). The IRTF publishes the results of Internet-related research and development activities. These results might not be suitable for deployment. This RFC represents the consensus of the IP Mobility Optimizations Research Group of the Internet Research Task Force (IRTF). Documents approved for publication by the IRSG are not a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc5726.

Table of Contents

1. Introduction

The IP address location privacy problem is concerned with unwittingly revealing the current location of a mobile node to eavesdroppers and to communicating parties. In the presence of mobility as specified in Mobile IPv6 [6], there are two related problems: disclosing the care-of address to a correspondent node, and revealing the home address to an eavesdropper (please see the terminology below). A detailed description of the location privacy problem can be found in RFC 4882 [11]. This document assumes that the reader is familiar with the basic operation of Mobile IPv6 specified in RFC 3775, as well as the location privacy problem described in RFC 4882.

In order to protect location privacy, a mobile node must not disclose the binding between its care-of address and its home address. In this document, we propose a set of extensions to the Mobile IPv6 specification to address the IP address location privacy problem. Related to the IP address location privacy is "profiling", where the activities of a mobile node are linked and then analyzed. Profiled activities may contribute to compromising a mobile node's location privacy, especially when combined with additional information. Furthermore, once location privacy is compromised, it may lead to more targeted profiling. Solutions to thwart profiling are important; however, they are not central to this document. We discuss profiling in the appendix.

We propose two IP address location privacy solutions in this document. With the first solution (as described in Section 5), the mobile node can communicate with the correspondent node by using the real home address without location privacy being breached by eavesdroppers. This is done by using parameters generated during the return routability procedure to mask the real home address, which provides an evolution towards location privacy protection based on return routability messages already specified in RFC 3775. With the second solution (as described in Section 6), an IPsec tunnel mode security association with a non-null encryption algorithm is negotiated to encrypt signaling messages (including the real home address therein) exchanged between the mobile node and the home agent, for example, during the home binding update procedure. Furthermore, during the return routability procedure and the correspondent binding update procedure, a "pseudo home address" (the definition of this new term and many other commonly used mobility related terms is provided in Section 2) is used to replace the real home address in various messages, which allows the mobile node to hide its real home address from both the correspondent node and eavesdroppers without the need for additional extensions to the correspondent node. Moreover, the mobile node may mask the pseudo

home address by using the mechanism specified in Section 5 to further enhance location privacy protection. Each of these two solutions can be implemented on its own without relying on the other.

The solutions presented in this document are designed based on the following assumptions. First, we focus on location privacy issues arising when the mobile node attaches to a foreign link; location privacy issues when the mobile node attaches to its home link, if any, are outside the scope of this document. Second, we assume that IPsec [2] is used to secure mobility signaling messages exchanged between the mobile node and the home agent; therefore, location privacy solutions when other security mechanisms are used are beyond the scope of this document. Third, we assume that eavesdroppers are passive attackers, e.g., an eavesdropper along the path traversed by traffic flows from or to the mobile node. We make this assumption because messages generated by active attackers can either be discarded based on local policy at a mobile node or the mobile node could choose to treat such messages like those of any other correspondent nodes. Thus, specific threats to location privacy posed by active attackers are also beyond the scope of this document. Fourth, in order to simplify analysis, we assume that both the correspondent node and the home agent are fixed nodes; if either is mobile, the same analysis and solutions for the mobile node may also apply. Finally, the same solution applies to each of the care-of addresses if a mobile node maintains more than one care-of address.

This document represents the consensus of the MobOpts Research Group. It has been reviewed by the Research Group members active in the specific area of work. At the request of their chairs, this document has been comprehensively reviewed by multiple active contributors to the IETF Mobile IP related working groups.

2. Conventions and Terminology

2.1. Conventions

The keywords "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 [1].

2.2. Terminology

In this document, we introduce two new terms, "pseudo home address" and "encrypted home address". The definition of these two terms is provided in the following.

- Pseudo Home Address (pHoA): A unicast IPv6 address formed to replace the real home address used in certain Mobile IPv6 signaling or data packets. Without explicit indication, the pseudo home address looks like a regular IPv6 address [5].

- Encrypted Home Address (eHoA): The output when applying an encryption algorithm to the real home address or the pseudo home address with additional inputs, e.g., a key. The real home address can be recovered from the encrypted home address by using a decryption algorithm.

In addition, we use commonly adopted mobility-related terms as defined in [6] and [11] throughout this document. Some of these terms are provided below for easier reference. Nevertheless, we assume that readers are familiar with the basic operation of the Mobile IPv6 protocol as defined in RFC 3775 [6], RFC 3776 [7], and RFC 4877 [8].

- Mobile Node (MN): A Mobile IPv6 compliant mobile node that can roam on the Internet

- Correspondent Node (CN): An IPv6 node that communicates with the mobile node

- Home Network: The network where the mobile node is normally present when it is not roaming

- Visited Network: The network that the mobile node uses to access the Internet when it is roaming

- Home Agent (HA): A router on the mobile node’s home network that provides forwarding support when the mobile node is roaming

- Home Address (HoA): The mobile node’s unicast IP address valid on its home network

- Care-of Address (CoA): The mobile node’s unicast IP address valid on the visited network

- Return Routability (RR): A procedure which enables secure binding between the care-of address and the home address when no pre-existing security association exists between the mobile node and the correspondent node

- Home Test Init (HoTI) / Home Test (HoT) / Care-of Test Init (CoTI) / Care-of Test (CoT): Messages used during the return routability procedure

- Binding Update (BU): A message used by the mobile node to securely bind its care-of address to its home address at the correspondent node or the home agent

- Binding Acknowledgement (BA): A response to the Binding Update

- Message Authentication Code (MAC): The value, which is computed using HMAC_SHA1 in this document, that protects both a message's integrity and its authenticity

- Route Optimization: A mechanism that allows direct routing of packets between a roaming mobile node and its correspondent node, without having to traverse the home network

- Reverse Tunneling or Bidirectional Tunneling: A mechanism used for packet forwarding between a roaming mobile node and its correspondent node via its home agent

3. Requirements

In this section, we describe the requirements that should be met by the Mobile IPv6 location privacy solutions, hereafter referred to as "the solution". These are some of the basic requirements set forth in order to make the solution readily implementable by those familiar with Mobile IPv6 and the related security protocols used with it (such as IKEv2 [4] and IPsec).

R01: The solution must follow the framework and architecture of IPv6 and Mobile IPv6 (as specified in RFC 3775, RFC 3776, and RFC 4877).

R02: The solution must not interfere with the operation of IPsec. This means that the principles and the operation specified in RFC 3776 and RFC 4877 need to be followed. For example, the IPsec security association and policy must be identified by the real home address.

R03: The solution should provide back-compatibility in order for different Mobile IPv6 entities to work together even though they may have different capabilities. This requires the mobile node to be able to detect whether the home agent or the correspondent node supports the use of the location privacy solutions.

R04: The overhead resulting from the solution, in terms of payloads or messages transmitted and memory, should be kept minimal.

4. Solution Overview

The IP address location privacy solutions proposed in this document intend to conceal the binding between the mobile node's real home address and its care-of address from eavesdroppers and the correspondent node. In this section, we present an overview of the proposed solutions.

With the Mobile IPv6 specification, during the home binding update procedure, both the real home address and the care-of address are in the cleartext when either the IPsec tunnel mode or the IPsec transport mode is used with no encryption. As described in Section 6.1, the solution to prevent the real home address being leaked to eavesdroppers on the MN-HA path during the home binding update procedure is to set up an IPsec tunnel mode security association with a non-null encryption algorithm to encrypt home binding signaling messages and the real home address therein. This method is also used to enable location privacy protection during other mobility signaling message exchanges between the home agent and the mobile node, such as the prefix discovery procedure (see Section 6.4).

When communicating with the correspondent node with the reverse tunneling mode, the mobile node can hide its current location from the correspondent node and eavesdroppers along the HA-CN path, since the care-of address is not included in payload packets transmitted on that path. Also, an IPsec security association with a non-null encryption algorithm established between the mobile node and the home agent can conceal the real home address carried in payload packets from eavesdroppers along the MN-HA path.

In order to communicate with a correspondent node in the route optimization mode, the mobile node needs to perform the return routability procedure followed by the correspondent binding update procedure. With the current Mobile IPv6 specification, the real home address and the care-of address in the correspondent Binding Update message and payload packets are visible to eavesdroppers. Therefore, in order to send and receive packets through the optimized route and protect location privacy at the same time, the mobile node needs to disclose its care-of address and conceal its real home address. There are two different scenarios and we propose a different solution for each scenario.

One scenario is that the correspondent node is able to obtain the mobile node's real home address and initiates communication with the mobile node by using the real home address. In this case, the mobile node needs to continue to use the real home address with the correspondent node in order to maintain session continuity, and to

conceal the real home address from eavesdroppers. The solution for this scenario (hereinafter referred to as "reverse-tunneled correspondent binding update") is described in Section 5. With this solution, the mobile node exchanges the same return routability signaling messages as defined in RFC 3775 with the correspondent node and then derives a privacy management key from keygen tokens and uses this key to encrypt the real home address. Finally, it reverse-tunnels an extended correspondent Binding Update message via the home agent to register the encrypted home address and the real home address at the correspondent node. After the correspondent registration, the mobile node and the correspondent node use the registered encrypted home address, instead of the real home address in payload packets exchanged via the optimized route. The encrypted home address is different for different correspondent nodes since the privacy management key would be different.

The other scenario is that the mobile node prefers to conceal its real home address from both the correspondent node and the eavesdroppers (typically the mobile node initiates communication in this case, since the correspondent node does not know the real home address). The solution for this scenario is described in Section 6.2. With this solution, the mobile node first obtains a home keygen token generated based on the pseudo home address during the home address test procedure. Subsequently, the mobile node sends the correspondent Binding Update message to register the binding between the pseudo home address and the care-of address at the correspondent node via the optimized route. After the correspondent registration, the mobile node and the correspondent node use the registered pseudo home address, instead of the real home address, in payload packets exchanged via the optimized route. Note that the use of the pseudo home address is completely transparent to the correspondent node.

Furthermore, it is feasible to throttle "profiling" on the pseudo home address by using a combination of these two solutions. That is, the mobile node uses the pseudo home address in the extended home address test procedure to obtain a home keygen token; then, it uses the pseudo home address instead of the real home address in the reverse-tunneled correspondent binding update procedure. With this solution, the encrypted pseudo home address used in route optimized payload packets looks different to eavesdroppers each time, after a new round of the return routability procedure is completed.

Before a pseudo home address is used with a correspondent node, it MUST be registered with the home agent during the home registration procedure. The mobile node indicates the requested pseudo home address in a new mobility option, called the Pseudo Home Address option (see Section 7.3), carried in the home Binding Update message,

and the home agent indicates the status of pseudo home address registration in another new mobility option, called Pseudo Home Address Acknowledgement option (see Section 7.4), carried in the home Binding Acknowledgement message. The pseudo home address MUST be routable in order for the home agent to intercept packets destined at this pseudo home address. It is statistically difficult for other nodes to derive the real home address from the pseudo home address. A detailed description of pseudo home address generation is provided in Section 6.1.1.1.

With extensions introduced in this document, a mobile node is able to discover whether the home agent and the correspondent node support the location privacy solutions or not. When present in the home Binding Update message, the Pseudo Home Address mobility option indicates that the mobile node requests the use of the location privacy solutions. If such a Binding Update message is valid and the home agent supports the location privacy solutions for this particular mobile node, it responds with the Pseudo Home Address Acknowledgement mobility option in the Binding Acknowledgement message. Otherwise, if the home agent does not support the location privacy solutions, it does not include the Pseudo Home Address Acknowledgement mobility option in the Binding Acknowledgement message. Similarly, the presence of the Encrypted Home Address destination option in the correspondent Binding Update message indicates to the correspondent node that the mobile node requests the use of the location privacy solutions. If such a Binding Update message is valid and the correspondent node supports the location privacy solutions for this particular mobile node, it responds with the Encrypted Home Address routing header in the correspondent Binding Acknowledgement message to the mobile node. If the correspondent node does not support the location privacy solutions, it rejects the mobile node’s request by returning an ICMP Parameter Problem message with Code value set to 2. Furthermore, a home agent that recognizes such extensions but does not wish to provide location privacy protection MAY redirect the mobile node to another home agent. If the request for using the location privacy solutions is rejected, the mobile node may either proceed without location privacy protection, or try with a different home agent or a correspondent node, or abort the operation.

5. Reverse-Tunneled Correspondent Binding Update

In this section, we describe a solution that protects location privacy against eavesdroppers when the mobile node uses the real home address during communication with the correspondent node via the optimized route. Note that this solution does not require any change to return routability signaling messages. The detailed description is as follows.

5.1. The Procedure

After the return routability procedure is completed, if the mobile node needs to protect location privacy, and at the same time still uses the real home address with the correspondent node, the mobile node derives a privacy management key, Kpm, from the Kbm, where Kpm = HMAC_SHA1 (Kbm, 0). The mobile node uses Kpm to generate the encrypted home address as follows.

encrypted home address = Enc(Kpm, the home address)

Where Enc() is a symmetric key encryption algorithm. AES is the default encryption algorithm.

Kpm changes upon every change of Kbm, which itself changes when return routability is run (e.g., upon change of care-of address, expiry of keygen token, etc.). So, Kpm is not re-used when a care-of address changes.

The mobile node generates a correspondent Binding Update message and reverse-tunnels this message to the correspondent node via the home agent. The format of this message after encapsulation is:

```
IPv6 header (source = care-of address,
             destination = home agent)
ESP header in tunnel mode
IPv6 header (source = home address,
             destination = correspondent node)
Destination option header
    Encrypted Home Address option (encrypted home address)
Parameters:
    Alternative Care-of Address option (care-of address)
    sequence number (within the Binding Update message header)
    home nonce index (within the Nonce Indices option)
    care-of nonce index (within the Nonce Indices option)
    First (96, HMAC_SHA1 (Kbm, (care-of address | correspondent
        | BU)))
```

This packet is protected by the IPsec security association with a non-null encryption algorithm. If the home agent can process this packet successfully, it forwards the following packet to the correspondent node.

```
IPv6 header (source = home address,
             destination = correspondent node)
Destination option header
    Encrypted Home Address option (encrypted home address)
```

```
    Parameters:
        Alternative Care-of Address option (care-of address)
        sequence number (within the Binding Update message header)
        home nonce index (within the Nonce Indices option)
        care-of nonce index (within the Nonce Indices option)
        First (96, HMAC_SHA1 (Kbm, (care-of address | correspondent
            | BU)))
```

After receiving a reverse-tunneled correspondent Binding Update message, the correspondent node performs the operation as described in Section 5.5. If the correspondent Binding Update message is processed successfully and an acknowledgement is requested, the correspondent node constructs a Binding Acknowledgement message shown below.

```
    IPv6 header (source = correspondent node,
                 destination = home address)
    Encrypted Home Address routing header
        encrypted home address
    Parameters:
        sequence number (within the Binding Update message header)
        First (96, HMAC_SHA1 (Kbm, (care-of address | correspondent
            | BA)))
```

Upon receiving this Binding Acknowledgement message, the home agent applies the IPsec security association with a non-null encryption algorithm to this message and forwards the following packet to the mobile node.

```
    IPv6 header (source = home agent,
                 destination = care-of address)
    ESP header in tunnel mode
    IPv6 header (source = correspondent node,
                 destination = home address)
    Encrypted Home Address routing header
        encrypted home address
    Parameters:
        sequence number (within the Binding Update message header)
        First (96, HMAC_SHA1 (Kbm, (care-of address | correspondent
            | BA)))
```

The reverse-tunneled correspondent binding update procedure is completed after the mobile node processes the received Binding Acknowledgement message. Note that when the mobile node communicates with a different correspondent node, the encrypted home address looks different.

To delete an established Binding Cache entry at the correspondent node, the mobile node reverse-tunnels the following Binding Update message via the home agent. Note that the Encrypted Home Address option is optional during the correspondent binding de-registration and only the home keygen token is used to generate Kbm and Kpm, if needed, in this case.

```
IPv6 header (source = care-of address,
             destination = home agent)
ESP header in tunnel mode
IPv6 header (source = home address,
             destination = correspondent node)
Destination option header (optional)
    Encrypted Home Address option (encrypted home address)
Parameters:
    Alternative Care-of Address option (care-of address)
    sequence number (within the Binding Update message header)
    home nonce index (within the Nonce Indices option)
    care-of nonce index (within the Nonce Indices option)
    First (96, HMAC_SHA1 (Kbm, (care-of address | correspondent
        | BU)))
```

If an acknowledgement is requested, the correspondent node returns the following Binding Acknowledgement message to the mobile node.

```
IPv6 header (source = correspondent node,
             destination = home address)
Encrypted Home Address routing header (optional)
    encrypted home address
Parameters:
    sequence number (within the Binding Update message header)
    First (96, HMAC_SHA1 (Kbm, (care-of address | correspondent
        | BA)))
```

Since the destination IP address in this message is the home address, the home agent will receive this message and forward it to the mobile node via the reverse tunnel.

5.2. Route-Optimized Payload Packets

After the correspondent registration is completed successfully, subsequent payload packets are exchanged via the optimized route between the mobile node and the correspondent node. In such packets, only the encrypted home address carried in the Encrypted Home Address destination option and the Encrypted Home Address routing header are visible to eavesdroppers.

The format of payload packets sent from the mobile node to the correspondent node is:

```
IPv6 header (source = care-of address,
             destination = correspondent node)
Destination option header
    Encrypted Home Address option (encrypted home address)
Payload
```

The format of payload packets sent from the correspondent node to the mobile node is:

```
IPv6 header (source = correspondent node,
             destination = care-of address)
Encrypted Home Address routing header
    encrypted home address
Payload
```

5.3. Mobile Node Operation

5.3.1. Conceptual Data Structures

The Binding Update List entry for the correspondent registration is extended with a new field to store the current encrypted home address used with a particular correspondent node. The encrypted home address is stored when the mobile node sends a reverse-tunneled correspondent Binding Update message, and the state of the corresponding Binding Update List entry is updated when the mobile node successfully processes the correspondent Binding Acknowledgement message. Note that the encrypted home address field is not valid in the Binding Update List entry for the home registration.

Given that the encrypted home address is 128 bits long, it is expected that each encrypted home address or the combination of the encrypted home address and the correspondent node's IP address stored in the Binding Update List is unique. Therefore, the mobile node can use the encrypted home address (or use it together with the correspondent node's IP address) as a primary key to look up the Binding Update List.

5.3.2. Reverse-Tunneled Correspondent Binding Update to the Correspondent Node

After the return routability procedure, if the mobile node chooses to use the location privacy solution with the correspondent node, e.g., based on the mobile node's configuration, it generates the encrypted home address, updates or creates a new correspondent Binding Update List entry to store the encrypted home address, then forwards the

correspondent Binding Update message through the reverse tunnel established with the home agent. Note that the MAC is generated in the same way as specified in RFC 3775, and it does not cover the encrypted home address.

5.3.3. Reverse-Tunneled Correspondent Binding Acknowledgement from the Correspondent Node

When the mobile node receives a Binding Acknowledgement message from the correspondent node in response to a previously sent reverse-tunneled correspondent Binding Update message, if this Binding Acknowledgement message contains an Encrypted Home Address routing header, the mobile node considers that the correspondent node supports the location privacy solution. The mobile node authenticates this message based on RFC 3775. If authentication is successful, the mobile node decrypts the encrypted home address and compares the result with the real home address, or compares the encrypted home address with the one stored in the Binding Update List entry. If they match, the mobile node considers that the correspondent registration is successful and updates the state of the corresponding Binding Update List entry. If they do not match, the mobile node MAY start the correspondent binding update procedure again.

5.3.4. Route-Optimized Payload Packets

In order to maintain session continuity, upper layers of the IP stack in the mobile node still use the real home address, even after the reverse-tunneled correspondent registration.

A possible way of implementation is as follows. When the Mobile IP sublayer at the mobile node receives a packet from the upper layer, the normal processing as specified in RFC 3775 is performed. Subsequently, the Home Address option is replaced with the Encrypted Home Address option carrying the encrypted home address stored in the corresponding Binding Update List entry, and then the mobile node forwards the packet to the correspondent node via the optimized route.

On the other hand, when the mobile node receives a payload packet carrying the Encrypted Home Address routing header, the mobile node uses the encrypted home address (optionally together with the IP address of the correspondent node) to look up the Binding Update List. If an entry is found, the mobile node accepts this packet, replaces the Encrypted Home Address option with the Home Address option carrying the real home address, and continues with processing based on RFC 3775. If no entry is found, the mobile node silently drops the received packet.

5.3.5. Receiving ICMP Error Message

The mobile node may receive an ICMP Parameter Problem, Code 2, message forwarded by the home agent via the bidirectional tunnel, for example, when the correspondent node does not support the use of the Encrypted Home Address option. If such a message is received, the mobile node SHOULD not attempt to use the location privacy solution with the correspondent node. The mobile node may choose either not to communicate with the correspondent node, or to communicate without location privacy protection.

5.3.6. Binding Error from the Correspondent Node

When the mobile node communicates with a correspondent node by using the encrypted home address, a Binding Error message with the Status field set as 1 (unknown binding for Home Address destination option) may be received by the mobile node if there is no valid Binding Cache entry established at the correspondent node. Note that we do not specify a new Status value to be used in this case because the implementation of the Binding Update List entry can contain an indication of whether an encrypted home address is currently used with the correspondent node. Upon receiving the Binding Error message, the mobile node can find out which encrypted home address is invalid by looking at the Home Address field of the Binding Error message. The mobile node may then perform the correspondent binding update procedure to establish a valid binding for the encrypted home address.

5.3.7. Binding Refresh Request from the Correspondent Node

When the mobile node receives a Binding Refresh Request message sent from the correspondent node and forwarded by the home agent via the bidirectional tunnel, the mobile node needs to perform the correspondent binding update procedure to refresh the binding for the encrypted home address at the correspondent node.

5.4. Home Agent Operation

With the solution described in this section (i.e., Section 5), there is no new home agent operation to be specified. That is, the home agent behaves based on RFC 3775 when processing signaling or data packets.

5.5. Correspondent Node Operation

5.5.1. Conceptual Data Structures

The Binding Cache entry is extended with a new field to store the current encrypted home address used with a particular mobile node. The encrypted home address is stored when the correspondent node successfully processes a reverse-tunneled correspondent Binding Update message.

Given that the encrypted home address is 128 bits long, it is expected that each encrypted home address or the combination of the care-of address and the encrypted home address stored in the Binding Cache entry is unique. Therefore, the correspondent node can use the encrypted home address (or use it together with the care-of address) as a primary key to look up the Binding Cache.

5.5.2. Reverse-Tunneled Correspondent Binding Update from the Mobile Node

When receiving a reverse-tunneled Binding Update message with the Encrypted Home Address option, if the correspondent node supports the location privacy solution, it verifies the message by using the same method as defined in RFC 3775. If this verification succeeds, the correspondent node generates Kpm and uses it to decrypt the encrypted home address, and compares the result with the source IP address. If they match, the correspondent node stores the encrypted home address in the corresponding Binding Cache entry.

5.5.3. Reverse-tunneled Correspondent Binding Acknowledgement to the Mobile Node

If an acknowledgement to the reverse-tunneled correspondent Binding Update message is requested by the mobile node, the correspondent node returns a Binding Acknowledgement message with the Encrypted Home Address routing header, if it supports the location privacy solution. The MAC in the Binding Acknowledgement message is generated in the same way as specified in RFC 3775 and does not cover the encrypted home address carried in the Encrypted Home Address routing header.

5.5.4. Route-Optimized Payload Packets

In order to maintain session continuity, upper layers of the IP stack in the correspondent node still use the real home address, even after the reverse-tunneled correspondent registration.

A possible way of implementation is as follows. When the IP layer at the correspondent node finishes processing the packet received from the upper layer based on RFC 3775, the Type 2 routing header together with the real home address therein is replaced with the Encrypted Home Address routing header with the encrypted home address found in the corresponding Binding Cache entry. Then, this packet is forwarded to the mobile node via the optimized route.

On the other hand, when the correspondent node receives a payload packet with the Encrypted Home Address option, it uses the encrypted home address (optionally together with the care-of address of the mobile node) to look up the Binding Cache. If there is an entry, the correspondent node replaces the Encrypted Home Address option with the Home Address option carrying the real home address before forwarding the packet to the upper layer. If no matching entry is found, the correspondent node sends a Binding Error message to the source IP address, i.e., the care-of address of the mobile node.

5.5.5. ICMP Error Message to the Mobile Node

When receiving a reverse-tunneled correspondent Binding Update message with the Encrypted Home Address option, if the correspondent node does not support location privacy extensions, it sends an ICMP Parameter Problem, Code 2, message to the source IP address (i.e., the home address of the mobile node) and the home agent then forwards this ICMP message to the mobile node via the bidirectional tunnel.

5.5.6. Binding Error to the Mobile Node

When the correspondent node receives a payload packet with the Encrypted Home Address option for which there is no valid Binding Cache entry, it returns a Binding Error message with the Status code set as 1 back to the source IP address of the packet. Furthermore, the Home Address field in the Binding Error message MUST be copied from the Encrypted Home Address field in the Encrypted Home Address destination option of the offending packet, or set to the unspecified address if no such option appears in the packet.

5.5.7. Binding Refresh Request to the Mobile Node

When the correspondent node realizes that a Binding Cache entry is about to expire, it sends a Binding Refresh Request message to the real home address of the mobile node stored in the Binding Cache entry.

5.6. Summary

With the solution in Section 5, the real home address is visible in the Binding Update and Binding Acknowledgement messages along the HA-CN path. Like Mobile IPv6 itself, it has not been designed to change the communications between the home network and the correspondent node; the same issues would affect non-mobile hosts as well. This solution meets all the requirements set forth for the location privacy solutions and provides a simple way to provide location privacy protection while allowing the use of the real home address with the correspondent node.

6. IP Address Location Privacy Solution Using the Pseudo Home Address

6.1. Home Binding Update

When the mobile node attaches to a foreign link, it first performs the home binding update procedure for the real home address with the home agent, as specified in RFC 3775. For hiding the real home address, we require the use of IPsec Encapsulating Security Payload (ESP) [3] in tunnel mode. In order to provide location privacy, a non-null encryption transform must be used so that the real home address is encrypted and encapsulated, and made invisible to eavesdroppers on the MN-HA path. The packet formats and processing rules are the same as specified in RFC 3775 and RFC 4877.

6.1.1. Pseudo Home Address Registration

6.1.1.1. Generation

To protect location privacy in the route optimization mode, the mobile node replaces the real home address used in certain signaling and payload packets with the pseudo home address. Different from the encrypted home address, the pseudo home address needs to be routable so that the home agent can intercept packets with the pseudo home address used as the destination address. The pseudo home address is generated by concatenating one of the home network prefixes with a random bit string. There are many ways to generate such a random bit string, for example, by using a random number generator or a secure encryption or hash algorithm.

Using the pseudo home address instead of the real home address even in return routability and binding update to the correspondent has the following advantages. First, the pseudo home address does not reveal the identity of a mobile node since it is not (or should not be) publicly known. Hence, the signaling on the HA-CN is path is more secure since attackers will not be able to determine the identity of the mobile node based on the pseudo home address. Second, the mobile

node can communicate with a correspondent without disclosing its real home address. Finally, the chosen pseudo home address can be different with different correspondents for both signaling and data traffic purposes.

The prefix used to form the pseudo home address MUST be managed by the same home agent so that it can forward the return routability messages. Even though it does not have to be the same as that used in the real home address, the prefix is highly recommended to be different. For instance, a home agent may use a different prefix pool for location privacy purposes for a set of mobile nodes. This ensures that the real home address and the pseudo home address are not co-related (assuming the mobile node chooses different interface identifiers (IIDs)).

6.1.1.2. Registration

The mobile node MUST register the pseudo home address to be used with the home agent before actually using it with a correspondent node. To do so, the mobile node indicates a pseudo home address in the Pseudo Home Address mobility option in the Binding Update message sent to the home agent. If the home agent supports the location privacy solution, it performs the Duplicate Address Detection to detect whether this pseudo home address conflicts with other pseudo home addresses submitted from different mobile nodes. Based on the result, the home agent indicates whether to accept the pseudo home address by setting the appropriate status code in the Pseudo Home Address Acknowledgement option in the Binding Acknowledgement message. If the home agent prefers the use of a different home network prefix from that of the requested pseudo home address, the home agent returns the new pseudo home address in the Pseudo Home Address Acknowledgement mobility option to the mobile node.

The mobile node MAY register the pseudo home address when it is about to communicate with a correspondent node with location privacy protection. The default lifetime of registered pseudo home addresses is the same as the Home Binding Cache entry; however, a mobile node may choose any value and a home agent may grant any value. The mobile node can add or delete any pseudo home address by using the Pseudo Home Address mobility option in the home Binding Update message. The home agent does not have to recover the real home address from the pseudo home address.

6.1.2. Home De-Registration

When the mobile node returns to its home link, the home de-registration procedure is the same as specified in RFC 3775, i.e., the real home address is used as the source IP address in the Binding

Update message and the destination IP address in the Binding Acknowledgement message. The de-registration of the real home address results in automatic de-registration of all pseudo home addresses. When the mobile node decides to disconnect from the home agent while at its foreign link, the format of the Binding Update and Acknowledgement is the same as that defined for the home registration, except that the Lifetime field is set to zero. The home agent deletes the corresponding Binding Cache entry including the registered pseudo home address, if any.

6.2. Correspondent Binding Update Using the Pseudo Home Address

6.2.1. Return Routability Procedure

The location privacy solution specified in this section does not introduce any change to the care-of address test procedure as specified in RFC 3775. In the following, we highlight the extensions to the home address test procedure, during which the mobile node obtains a home keygen token generated based on the pseudo home address.

The mobile node generates and sends a Home Test Init message to the home agent. The format of this message is:

```
IPv6 header (source = care-of address, destination = home agent)
ESP header in tunnel mode
IPv6 header (source = home address, destination = correspondent)
Mobility Header (HoTI)
    Home Init Cookie
    Pseudo Home Address mobility option (pseudo home address)
```

The difference from what is specified in RFC 3775 is that the mobile node includes a Pseudo Home Address mobility option (see Section 7.3) in the Home Test Init message. A new option for carrying the pseudo home address is necessary because the security association between the mobile node and the home agent is based on the real home address. The pseudo home address contained in the Pseudo Home Address option is selected by the mobile node from a set of pseudo home addresses that have been registered with the home agent during the home registration procedure. Note that the Home Test Init message is protected by an IPsec security association in the ESP tunnel mode with a non-null encryption algorithm and a non-null authentication algorithm, as specified in RFC 3776.

When receiving a Home Test Init message, the home agent performs the operation as specified in Section 6.6.4. If this operation succeeds when the Pseudo Home Address mobility option is present in the Home Test Init message, the home agent generates a Home Test Init message

and forwards it to the correspondent node. As shown in the following, the pseudo home address carried in the Pseudo Home Address mobility option is used as the source IP address in the forwarded Home Test Init message.

```
    IPv6 header (source = pseudo home address,
                 destination = correspondent)
    Mobility Header (HoTI)
        Home Init Cookie
```

The forwarded Home Test Init message looks the same to the correspondent node as what is specified in RFC 3775 and the correspondent node does not realize that the pseudo home address is used, and just generates a home keygen token using the same algorithm as specified in RFC 3775.

```
   home keygen token =
       First (64, HMAC_SHA1 (Kcn, (pseudo home address | nonce | 0)))
```

The correspondent node then replies with a Home Test message. As shown in the following, the format of this message is the same as that specified in RFC 3776, and the pseudo home address is used as the destination IP address.

```
    IPv6 header (source = correspondent,
                 destination = pseudo home address)
    Mobility Header (HoT)
        Home Init Cookie
        Home Keygen Token
        Home Nonce Index
```

When the home agent intercepts the Home Test message using proxy Neighbor Discovery, it performs the operation as specified in Section 6.6.5. If this operation succeeds, the home agent generates the following Home Test message and forwards to the mobile node.

```
    IPv6 header (source = home agent, destination = care-of address)
    ESP header in tunnel mode
    IPv6 header (source = correspondent, destination = home address)
    Mobility Header (HoT)
        Home Init Cookie
        Home Keygen Token
        Home Nonce Index
        Pseudo Home Address Acknowledgement mobility option
           (pseudo home address)
```

When the mobile node receives the Home Test message, it performs operation as specified in Section 6.5.5. If such operation succeeds, the mobile node obtains a home keygen token computed using the pseudo home address. After the care-of address test is completed, the mobile node hashes the care-of keygen token and the home keygen token together to generate Kbm using the same method as specified in RFC 3775.

6.2.2. Route-Optimized Correspondent Binding Update

In this procedure, the mobile node MUST use the same pseudo home address used during the home address test procedure. The pseudo home address is carried in the Home Address option in the correspondent Binding Update message.

```
IPv6 header (source = care-of address,
             destination = correspondent)
Destination option header
    Home Address destination option (pseudo home address)
Parameters:
    sequence number (within the Binding Update message header)
    home nonce index (within the Nonce Indices option)
    care-of nonce index (within the Nonce Indices option)
    First (96, HMAC_SHA1 (Kbm, (care-of address | correspondent
    | BU)))
```

When the correspondent node receives the Binding Update message, it performs the same operation as specified in RFC 3775. If such operation succeeds and an acknowledgement is requested by the mobile node, the correspondent node replies with the following Binding Acknowledgement message.

```
IPv6 header (source = correspondent,
             destination = care-of address)
Parameters:
    sequence number (within the Binding Update message header)
    First (96, HMAC_SHA1 (Kbm, (care-of address | correspondent
    | BA)))
```

After the mobile node receives the Binding Acknowledgement message indicating that the correspondent registration succeeds, the mobile node can now use the pseudo home address for communicating with the correspondent node.

Such a Binding Update message may also be used by the mobile node to delete a previously established binding at the correspondent node. In this case, similar to what is specified in RFC 3775, Kbm is generated exclusively from the home keygen token that is based on the pseudo home address.

6.2.3. Reverse-tunneled Correspondent Binding Update

The mobile node may choose to use reverse tunneling for sending the Binding Update. The format of messages during such a procedure is similar to what is described in Sections 5 and 6.2.1, except that a pseudo home address is used in place of the real home address. The Encrypted Home Address destination and the Encrypted Home Address routing header SHOULD be used to carry the encrypted pseudo home address.

6.2.4. Using Different Pseudo Home Addresses with Different Correspondent Nodes

Based on its configuration and policy, the mobile node can choose to use the same or different pseudo home addresses when communicating with different correspondent nodes. Using a different pseudo home address with each correspondent node may help prevent the mobile node's activities from being linked and correlated. To do so, the mobile node selects a different but already registered pseudo home address and repeats the return routability procedure and the correspondent binding update procedure with each correspondent node.

In addition, if the mobile node prefers, it MAY use different pseudo home addresses for different sessions with the same correspondent node. This typically requires additional configuration at the mobile node that associates a specific session (for example, identified by the port number and the protocol number, among others) with a specific pseudo home address. This document does not address details of this solution.

6.3. Payload Packets

6.3.1. Reverse Tunneling Mode

The format of payload packets reverse-tunneled via the home agent is the same as that specified for the home address test procedure in Section 6.2.1.

6.3.2. Route Optimization Mode

When the route-optimized correspondent binding update procedure is performed, the format of payload packets exchanged between the mobile node and the correspondent node is the same as specified in RFC 3775. The operation of the mobile node when communicating with the correspondent node via the route optimization mode is described in Section 6.5.6.

When the reverse tunneled correspondent binding update procedure is performed, the format of payload packets exchanged between the mobile node and the correspondent node is the same as specified in Section 5, except that the encrypted pseudo home address SHOULD be included in the Encrypted Home Address destination option and the Encrypted Home Address routing header.

6.4. Prefix Discovery

The solution to protect location privacy during the prefix discovery procedure is similar to that used during the home binding update procedure.

6.5. Mobile Node Operation

In this section, we describe the mobile node’s operation when the location privacy solution is used.

6.5.1. Conceptual Data Structures

6.5.1.1. Pseudo Home Address Table

We introduce a new data structure, called Pseudo Home Address table, to record the information of pseudo home addresses. The mobile node may maintain a Pseudo Home Address table for each home agent it registers with. Each entry in the table contains a pseudo home address and its associated state, i.e., "unconfirmed" or "confirmed". The mobile node creates or updates entries in the Pseudo Home Address table when sending the home Binding Update message or receiving the home Binding Acknowledgement message. The pseudo home address can be used as a key to search the table. There MUST NOT be any duplicated pseudo home addresses stored in the Pseudo Home Address table.

6.5.1.2. Binding Update List

The Binding Update List entry is extended with a field, called Pseudo Home Address. This field MAY be implemented as a pointer that points to a corresponding entry in the Pseudo Home Address table. This pointer is initialized as NULL when the Binding Update List entry is

created (for example, when the mobile node sends a Binding Update message or a Home Test Init message to the home agent). For the binding sent to a specific home agent, the Pseudo Home Address field points to the first entry in the Pseudo Home Address table (or NULL if the table is empty), so that the mobile node can access all the pseudo home addresses registered at this home agent; on the other hand, for the binding sent to a specific correspondent node, the Pseudo Home Address field points to the Pseudo Home Address table entry that contains the actual pseudo home address used with this correspondent node (or NULL if no pseudo home address is used with this correspondent node).

6.5.2. Binding Update to the Home Agent

The mobile node may decide to perform the home registration with location privacy protection, for example, when it attaches to a foreign link or when it needs to extend the lifetime of a registered home binding.

Since IPsec tunnel mode is used, the mobile node MUST negotiate a non-null encryption algorithm (for example, during the bootstrapping) and use it to protect the home Binding Update message as specified in RFC 3775 and RFC 4877. In addition, the mobile node can register a pseudo home address as described above. If the mobile node does not wish to register the pseudo home address at this point, but wishes to discover whether the home agent supports the location privacy solution, the mobile node includes a Pseudo Home Address mobility option without the Pseudo Home Address field in the Binding Update message sent to the home agent.

After sending the home de-registration binding update message, in addition to the operation specified in RFC 3775, the mobile node MUST stop using any data structure specific to the location privacy solution and MAY delete them after the Binding Acknowledgement message is processed successfully.

6.5.3. Binding Acknowledgement from the Home Agent

With IPsec tunnel mode, the mobile node follows the rules specified in RFC 3775 and RFC 4877 to process the Binding Acknowledgement message.

In addition, if one or more Pseudo Home Address Acknowledgement mobility options are present in the Binding Acknowledgement message, the mobile node checks the Status field in each option. If the Status field in one option is 0 (Success), the pseudo home address, if not already present, is added into the Pseudo Home Address table, and the state of the corresponding entry is set to "confirmed".

Otherwise, the mobile node deletes any existing pseudo home address with the "unconfirmed" state (i.e., either an error code or no acknowledgement for such a pseudo home address is received) from the Pseudo Home Address table.

The mobile node considers that the home agent supports the location privacy solution, if a valid Pseudo Home Address Acknowledgement mobility option with or without a Pseudo Home Address field is received.

Note that the mobile node MUST determine whether the home registration succeeds or not based on what is specified RFC 3775.

6.5.4. Home Test Init to the Home Agent

To enable location privacy protection during communication with the correspondent node in the route optimization mode, the mobile node generates a Home Test Init message based on what is specified in RFC 3775 and RFC 3776. In addition, if the return routability procedure is for a new session with the correspondent node, the mobile node selects any pseudo home address from those already registered with the home agent and stored in the Pseudo Home Address table; otherwise, the mobile node must use the same pseudo home address as used with the same correspondent node before. The selected pseudo home address is carried in the Pseudo Home Address mobility option of the generated Home Test Init message. This Home Test Init message is protected by an IPsec security association with a non-null encryption algorithm.

After sending the Home Test Init message to the home agent, if there is no Binding Update List entry existing for the correspondent node, the mobile node creates one entry that points to the pseudo home address used; otherwise, the mobile node updates the existing entry.

6.5.5. Home Test from the Home Agent

When the mobile node receives a Home Test message from the home agent, it processes the packet based on processing rules specified in RFC 3775 and RFC 3776. If this is a valid packet and there is a Pseudo Home Address Acknowledgement option included, the mobile node examines the Status field inside this mobility option as follows:

- If the Status field indicates that the home address test procedure using the pseudo home address succeeds (the Status field is 0), in addition to what is specified in RFC 3775, the mobile node prepares to use the pseudo home address carried in the Pseudo Home Address Acknowledgement option for the correspondent registration.

- If the Status field indicates that the home address test procedure using the pseudo home address fails (the Status field is larger than 127), the mobile node can take steps to correct the cause of the error and retransmit the Home Test Init message, subject to the retransmission limit specified in RFC 3775. If this is not done or it fails, then the mobile node SHOULD record in its Binding Update List that the future home address test procedure SHOULD NOT use the pseudo home address with this correspondent node.

6.5.6. Route-Optimized Payload Packets

After the mobile node completes the route-optimized correspondent registration procedure using the pseudo home address, payload packets are sent to the correspondent node with the pseudo home address in the Home Address destination option.

The packet processing rules when sending and receiving route-optimized packets are the same as in RFC 3775 except that pseudo home addresses are used. In addition, if encrypted pseudo home addresses are used, both the mobile node and the correspondent node need to replace the encrypted address with the pseudo home address before passing them to the upper layers.

In the case that the mobile node masks the pseudo home address and uses the reverse-tunneled correspondent binding update procedure, the mobile node performs the operation specified in Section 5.3.4, except that the pseudo home address rather than the real home address is expected.

6.5.7. Receiving Binding Refresh Request

When the Mobile Node receives a Binding Refresh Request message from a correspondent node, the destination IP address may be the pseudo home address. In this case, the mobile node needs to check the corresponding Binding Update List entry for the correspondent node. If the pseudo home address is invalid, the mobile node silently discards this message. Otherwise, the mobile node refreshes the binding with the correspondent node by using the same pseudo home address.

6.6. Home Agent Operation

In this section, we describe the home agent’s operation when the location privacy solution is used.

6.6.1. Conceptual Data Structures

The Binding Cache entry is extended with a field that points to a list of currently accepted pseudo home addresses. Note that each registered pseudo home address MUST be unique and all the registered pseudo home addresses SHOULD be organized in such a way that the associated Binding Cache entry can be quickly located when a pseudo home address is used as the key to look up the Binding Cache.

6.6.2. Binding Update from the Mobile Node

If the received Binding Update message contains one or more Pseudo Home Address mobility options, the home agent MUST ignore such an option if it does not recognize it. If the home agent recognizes such an option, a Pseudo Home Address Acknowledgement mobility option is generated and some fields therein are set as follows:

- If the Pseudo Home Address field received is empty, the Status field is set to 0 (Success), and the Pseudo Home Address field is empty.

- If the Pseudo Home Address field received is set to all zero, the Status field is set is 0 (Success), and a pseudo home address SHOULD be included in the Pseudo Home Address field, if the home agent supports the dynamic pseudo home address assignment; otherwise, the Status field is set to 132 (Dynamic pseudo home address assignment not available) and the Pseudo Home Address field is empty.

- The Pseudo Home Address field received may contain an IPv6 address. If the format of such an IP address is incorrect, the Status field is set to 130 (Incorrect pseudo home address). If such an IP address is invalid, for example, the prefix is not a valid home network prefix or this is detected as a duplicated IP address, the Status field is set to 131 (Invalid pseudo home address). In both cases, the Pseudo Home Address field is empty. If the home agent suggests a different pseudo home address, the Status field is set to 0 (Success), and the new pseudo home address is included in the Pseudo Home Address field. Otherwise, if the home agent accepts the requested pseudo home address, the Status field is set as 0 (Success), and the same IP address is included in the Pseudo Home Address field.

- If the home agent does not allow the mobile node to use the pseudo home address with the correspondent node, the Status field SHOULD be set as 129 (Administratively prohibited) and the Pseudo Home Address field is empty.

- o In case that the home agent does not accept the Pseudo Home Address mobility option for all other reasons, the Status field SHOULD be set as 128 (Failure, reason unspecified) and the Pseudo Home Address is empty.

When receiving a Binding Update message protected with the IPsec tunnel mode, the home agent performs the operation specified in RFC 4877.

When receiving and successfully processing a Binding Update message for de-registration from the mobile node, in addition to what is specified in RFC 3775, the home agent MUST delete data structures related to the location privacy extension.

6.6.3. Binding Acknowledgement to the Mobile Node

When sending a Binding Acknowledgement message protected with the IPsec tunnel mode, the home agent performs the operation specified in RFC 4877.

The processing rules related to the Pseudo Home Address Acknowledgement mobility option are described in Section 6.6.2.

6.6.4. Home Test Init from the Mobile Node

When receiving a Home Test Init message from the mobile node, the home agent first verifies this message based on the IPsec processing rules as specified in RFC 3776. If the verification fails, the home agent acts based on such IPsec processing rules. Otherwise, if the Pseudo Home Address option does not exist in the Home Test Init message, the home agent performs the operation as specified in RFC 3775. Otherwise, the following operation is performed.

1. The home agent looks up its Binding Cache by using the real home address as a key. If the pseudo home address carried in the Pseudo Home Address option does not match any pseudo home address associated with the corresponding Binding Cache entry (including when the Pseudo Home Address field is set as zero), it MUST reject the Home Test Init message by sending back a Home Test message including the Pseudo Home Address Acknowledgement option with the Status field set as 131 (Invalid pseudo home address).

2. Otherwise, the home agent constructs a Home Test Init message with the pseudo home address as the source IP address, and forwards the Home Test Init message to the correspondent node.

6.6.5. Home Test to the Mobile Node

When the home agent intercepts a Home Test message using proxy Neighbor Discovery, if the destination IP address matches with one of the real home addresses, the home agent performs the operation as specified in RFC 3775. Otherwise, the home agent uses the destination IP address to look up the Binding Cache to find if there is a matched pseudo home addresses. If not, the home agent discards this message silently. When a matching pseudo home address is found, the home agent generates a Home Test message with a Pseudo Home Address Acknowledgement option and sends it to the mobile node. Inside the Pseudo Home Address Acknowledgement option, the Status field is set to zero (Success) and the Pseudo Home Address field is filled with the found pseudo home address.

6.7. Correspondent Node Operation

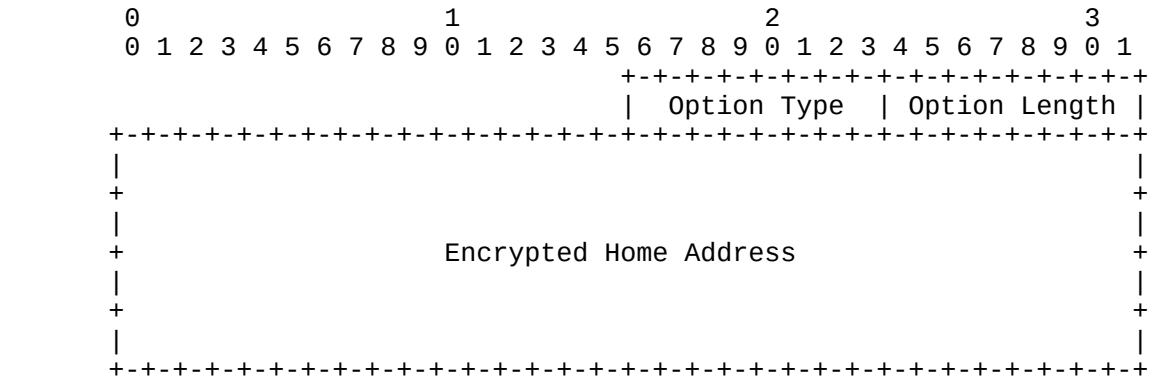
With the solution described in this section, when the correspondent node is involved in the route-optimized correspondent binding update procedure, there is no new operation if only pseudo home addresses are used without encryption. This specification recommends using encrypted pseudo home addresses to thwart revealing any prefix information about a mobile node. The additional operations are the same as specified in Section 5.5, except that the pseudo home address, instead of the real home address, is used.

7. Extensions to Mobile IPv6

This section describes the experimental extensions to Mobile IPv6 used in this document. For experimentation purposes, the experimental IPv6 Option Type, the experimental IPv6 Routing Header Type, and the experimental Mobility Option Type as defined in RFC 4727 [12] and RFC 5096 [13] can be used in the Encrypted Home Address destination option, the Encrypted Home Address routing header, the Pseudo Home Address mobility option, and the Pseudo Home Address Acknowledgement mobility option. In the following, we describe the format of each extension for illustration purpose.

7.1. Encrypted Home Address Destination Option

This option is used in the Destination Option extension header (Next Header value = 60).



Option Type

A type for identifying the use of the encrypted home address in this option. Implementations of this RFC can use the value 0xFE. This value is reserved in RFC 4727 for all experiments involving IPv6 destination options.

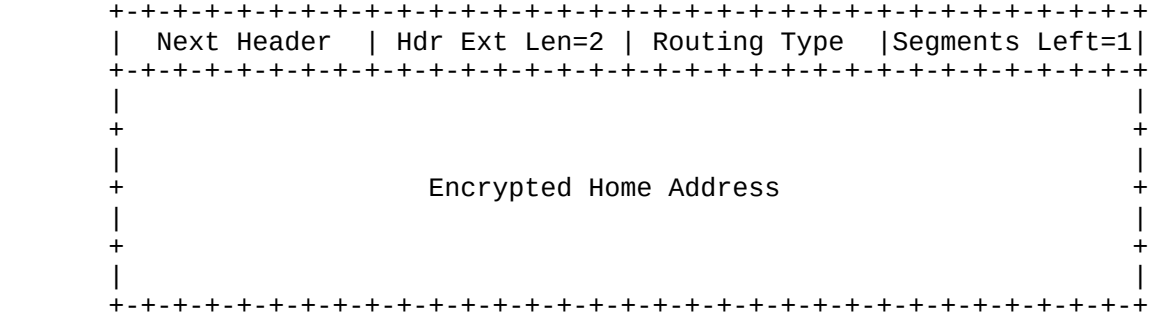
Encrypted Home Address

The encrypted home address generated from a either real or pseudo home address.

The processing of other fields in the Encrypted Home Address option is the same as that of those fields in the Home Address option described in RFC 3775. Note that if the Encrypted Home Address option is present in a packet, the encrypted home address therein MUST NOT be treated as the real source IP address by the receiver.

7.2. Encrypted Home Address Routing Header

The encrypted home address is carried in this routing header.



Routing Type

A type for identifying the use of the encrypted home address in this option. Implementations of this RFC can use the value 0xFE. This value is reserved in RFC 4727 for all experiments involving IPv6 routing header.

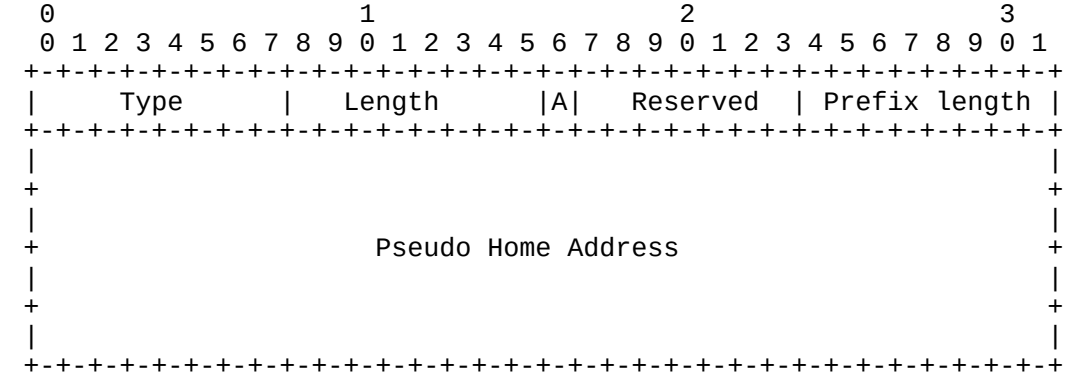
Encrypted Home Address

The encrypted home address generated from a either real or pseudo home address.

The processing of other fields in the Encrypted Home Address routing header is the same as described in RFC 3775. Note that if this routing header is present in a packet, the encrypted home address therein MUST NOT be treated as the real destination IP address by the receiver.

7.3. Pseudo Home Address Mobility Option

This mobility option is included in the mobility header, including the Binding Update message and the Home Test Init message, and carries zero or one pseudo home address. The alignment requirement for this option is 4n.



Type

A unique type (together with the 'A' bit in the Reserved field) for identifying the Pseudo Home Address Acknowledgement mobility option. For experimental purpose, the value of this type is 18 as reserved in RFC 5096.

Length

The length of the Pseudo Home Address mobility option excluding the Type field and the Length field. It MUST be 2 when the Pseudo Home Address field is not present; otherwise, it MUST be 18.

Reserved Field

The 'A' bit, which MUST be set to zero to indicate that this is a Pseudo Home Address mobility option. The rest of bits MUST be set as zero by the sender and ignored by the receiver.

Prefix Length

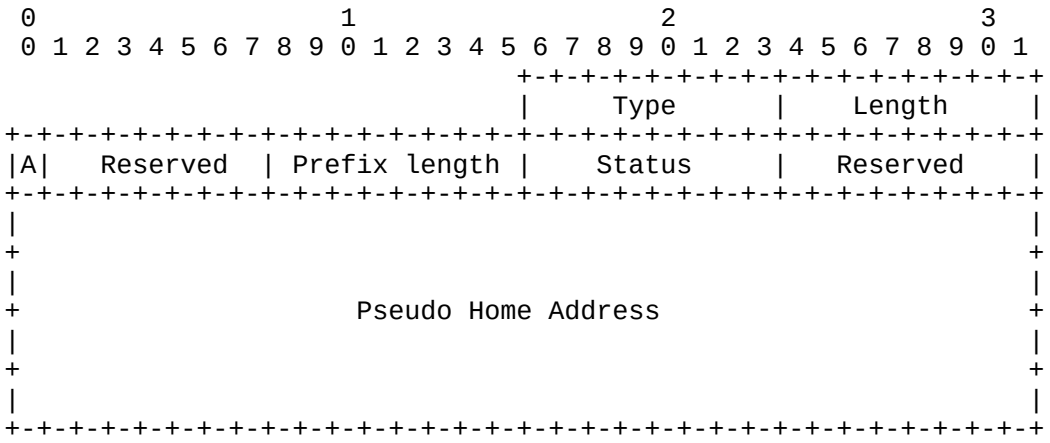
The length of the home network prefix of the included pseudo home address. When the Pseudo Home Address field is not present, the Prefix Length field MUST be set as zero.

Pseudo Home Address

If present, the field contains a pseudo home address that the mobile node wants to use for location privacy protection or zero if the mobile node requests a pseudo home address from the home agent. This field is not present if the mobile node only intends to discover whether the home agent supports the location privacy solutions. The Length field is used to detect whether the Pseudo Home Address field is present in the Pseudo Home Address mobility option.

7.4. Pseudo Home Address Acknowledgement Mobility Option

This mobility option is included in the mobility header, including the Binding Acknowledgement message and the Home Test message sent to the mobile node, and carries zero or one pseudo home address. This mobility option is used to indicate the status of the pseudo home address registration and/or whether the home agent supports the location privacy solutions. The alignment requirement for this option is 2n.



Type

A unique type (together with the 'A' bit in the Reserved field) for identifying the Pseudo Home Address Acknowledgement mobility option. For experimental purpose, the value of this type is 18 as reserved in RFC 5096.

Length

The length of the Pseudo Home Address Acknowledgement mobility option excluding the Type field and the Length field. It MUST be 4 when the Pseudo Home Address field is not present; otherwise, it MUST be 20.

Reserved

The 'A' bit, which MUST be set to one to indicate that this is a Pseudo Home Address Acknowledgement mobility option. The rest of bits MUST be set as zero by the sender and ignored by the receiver.

Prefix Length

The length of the home network prefix of the included pseudo home address. When the Pseudo Home Address field is not present, the Prefix Length MUST be set as zero.

Status

It indicates the status of the pseudo home address registration. Values from 0 to 127 indicate success. Higher values indicate failure. The following values are reserved:

0 Success
128 Failure, reason unspecified
129 Administratively prohibited
130 Incorrect pseudo home address
131 Invalid pseudo home address
132 Dynamic pseudo home address assignment not available

Reserved

This field is reserved for future use. It MUST be set to zero by the sender and ignored by the receiver.

Pseudo Home Address

If present, the field contains a pseudo home address that the home agent registers for the mobile node to use for location privacy protection. This field is not present when the home agent only needs to indicate that it supports the location privacy solutions as a response to the query from the mobile node. The Length field is used to detect whether the Pseudo Home Address field is present in the Pseudo Home Address Acknowledgement mobility option.

8. Security Considerations

The solutions proposed in this document address one of the security issues in the mobile environment, i.e., location privacy. Throughout the document, we provide a detailed analysis of how the proposed solutions address the location privacy problem. We carefully design such solutions to make sure that they fit well into the Mobile IPv6 framework; therefore, the same threat analysis, security mechanisms (such as IPsec, the sequence number in binding signaling messages, the return routability procedure), and considerations as described in RFC 3775 still apply. Nevertheless, in the following we provide an in-depth analysis on security threats involving the use of the location privacy solutions and demonstrate that the proposed solutions do not introduce any new vulnerability or weaken the strength of security protection of the original Mobile IPv6 protocol.

8.1. Home Binding Update

Given the strong security of the cryptography algorithm used to generate the encrypted home address, eavesdroppers are unable to derive the real home address from the encrypted home address and thus to correlate the care-of address with the real home address. Moreover, the encrypted home address can be updated to prevent eavesdroppers from linking the mobile node’s ongoing activities.

During the pseudo home address registration, the home agent verifies that the requested pseudo home address is not in use by other mobile nodes; therefore, the other mobile node cannot, inadvertently or maliciously, intercept ongoing sessions of a victim mobile node by registering the same pseudo home address.

A mobile node may attempt to register a large number of pseudo home addresses that may exhaust the pool of available pseudo home addresses and prevent other mobile nodes using location privacy protection. The home agent MUST limit the number of pseudo home addresses that can be requested by a mobile node. Also, with the IPsec security association between the home agent and the mobile node, if any misuse of the pseudo home address registration is detected, the home agent can identify the malicious mobile node and take further actions.

8.2. Correspondent Binding Update

The return routability procedure using the pseudo home address follows the same principle of the original return routability procedure, i.e., the message exchange verifies that the mobile node is reachable at both the pseudo home address and the care-of address (this is because the pseudo home address is required to be routable). Furthermore, the extended return routability procedure also utilizes the same security mechanisms as defined in RFC 3775, such as the nonce, the node key, and the sequence number, to protect against attacks. Overall, it provides the same security strength as the original return routability procedure.

The reverse-tunneled correspondent binding update procedure does not weaken security either. Although the real home address is transferred in cleartext on the HA-CN path, eavesdroppers on this path can already perform more serious attacks against the mobile node with the Mobile IPv6 protocol.

8.3. Route-Optimized Payload Packets

Using the Encrypted Home Address option in route-optimized packets results in the same security implications when the Home Address option is used in such packets. For example, the Encrypted Home Address option may be used by attackers to launch reflection attacks, e.g., by indicating the IP address of a victim node in the Encrypted Home Address option. Similar to the processing rule for the Home Address option specified in RFC 3775, this document restricts the use of the Encrypted Home Address option: it can be used only if there is an established Binding Cache entry containing the encrypted (pseudo) home address.

With the proposed location privacy solutions, the Encrypted Home Address routing header is used to carry the encrypted (pseudo) home address. The same threats specified in RFC 3775 for the Type 2 routing header are also possible when the routing header carries the encrypted (pseudo) home address. Similar processing rules are also used in this document to address such a threat: if the encrypted (pseudo) home address in the Encrypted Home Address routing header does not match with that stored in the Binding Update List entry, the packet will be dropped.

9. Related Work

Our work benefits from previous work and discussion on this topic. Similar to the concept of the pseudo home address, many documents have proposed using a temporary identity to replace the mobile node's home address in the IPsec security association, Mobile IPv6 signaling messages, and data packets. However, the details of how to generate and update this identity are absent. In the following, we provide a survey of related work.

RFC 4941 [10] specifies a mechanism to generate randomized interface identifiers, which can be used to update the care-of address and the home address. However, with our solution, the prefix of a pseudo home address can be different from that of the real home address and other pseudo home addresses, which prevents eavesdroppers from correlating and analyzing IP traffic based on a common prefix. Furthermore, we also discuss the interval of IP address update in the mobility scenario in order to resist the profiling attack both effectively and efficiently.

In [16], the authors propose using a temporary identity, called the Temporary Mobile Identifier (TMI), to replace the home address, and discussed the feasibility of utilizing the Crypto-Based Identifier (CBID), Cryptographically Generated Addresses (CGA), or Mobility Anchor Point (MAP) to further protect location privacy. However, as a 128-bit random number, the TMI is not routable; therefore, it is not suitable to be the source IP address in the Home Test Init message forwarded by the home agent to the correspondent node. Otherwise, the home agent cannot receive the Home Test message from the correspondent node. Furthermore, the document does not specify how to update the TMI to address the profiling attack.

In [14], the authors propose a mechanism that uses an identity as the home address and periodically updates such an identity by using a key and a previous identity as inputs to a cryptography algorithm.

In [15], the authors propose to update the mobile node's home address periodically to hide its movement. The new home address is generated from the current local network prefix, the Binding Update session key, and the previous home address, and updated every time when the return routability procedure is performed. The generated home address is random, routable, recognizable, and recoverable.

In [18], the authors propose a mechanism to achieve both route optimization and location privacy at the same time. This is done by discovering a tunneling agent near the correspondent node and bidirectionally tunneling data traffic between the mobile node and the tunneling agent.

10. IANA Considerations

This document creates a new registry "Pseudo Home Address Acknowledgement Status Codes" for the Status field in the Pseudo Home Address Acknowledgement mobility option. The current values are described in Section 7.4 and are the following:

0 Success

128 Failure, reason unspecified

129 Administratively prohibited

130 Incorrect pseudo home address

131 Invalid pseudo home address

132 Dynamic pseudo home address assignment not available

11. Conclusion

In this document, we have proposed solutions to address location privacy issues in the context of mobility. The main idea is to hide the binding between the home address and the care-of address from eavesdroppers and the correspondent node. We have described two methods. The first method extends the return routability to hide the real home address in Binding Update and data packets. This method uses the real home address in return routability signaling, and does not require any changes to the home agent. The second method uses pseudo home addresses starting from return routability signaling, and requires some extensions to the home agent operation. This method protects revealing the real home address on the HA-CN path. The two methods provide a means to hide the real home address from eavesdroppers, and the second method can also hide it from the correspondents.

The solutions we have proposed are for the basic Mobile IPv6 protocol as specified in RFC 3775. Recently, many extensions to Mobile IPv6 have been proposed, such as the NEMO Basic Support protocol [19], Dual Stack Mobile IPv6 Support [20], Multiple Care-of Addresses Registration [21], Binding Revocation [22], Generic Signaling Message [23]. It is expected that the proposed location privacy solutions can be applied with some modifications, if needed, to address location privacy issues when these extensions are used. One of our future works is to clarify related issues, if any, when the location privacy solutions are used with new Mobile IPv6 extensions.

12. Acknowledgements

The authors would like to thank the co-authors of previous documents from which this document is derived: Vijay Devarapalli, Hannu Flinck, Charlie Perkins, Feng Bao, Robert Deng, James Kempf, and Jianying Zhou. In addition, sincere appreciation is also extended to Claude Castelluccia, Francis Dupont, Gabriel Montenegro, Greg Daley, Kilian Weniger, Takashi Aramaki, Wassim Haddad, Heejin Jang, and Michael Welzl for their valuable contributions, review, and discussion. Work by Fan Zhao was done while he was at University of California, Davis and Marvell Semiconductor, Inc.

13. References

13.1. Normative References

[1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[2] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[3] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.

[4] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.

[5] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[6] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[7] Arkko, J., Devarapalli, V., and F. Dupont, "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents", RFC 3776, June 2004.

[8] Devarapalli, V. and F. Dupont, "Mobile IPv6 Operation with IKEv2 and the revised IPsec Architecture", RFC 4877, April 2007.

[9] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, February 2006.

[10] Narten, T., Draves, R., and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 4941, September 2007.

[11] Koodli, R., "IP Address Location Privacy and Mobile IPv6: Problem Statement", RFC 4882, March 2007.

[12] Fenner, B., "Experimental Values in IPv4, IPv6, ICMPv4, ICMPv6, UDP, and TCP Headers", RFC 4727, November 2006.

[13] Devarapalli, V., "Mobile IPv6 Experimental Messages", RFC 5096, December 2007.

13.2. Informative References

[14] Bao, F., Deng, R., Kempf, J., Qiu, Y., and J. Zhou, "Protocol for Protecting Movement of Mobile Nodes in Mobile IPv6", Work in Progress, March 2005.

[15] Bao, F., Deng, R., Kempf, J., Qiu, Y., and J. Zhou, "Protocol for Hiding Movement of Mobile Nodes in Mobile IPv6", Work in Progress, March 2005.

[16] Castelluccia, C., Dupont, F., and G. Montenegro, "A Simple Privacy Extension for Mobile IPv6", Work in Progress, July 2006.

[17] Daley, G., "Location Privacy and Mobile IPv6", Work in Progress, January 2004.

[18] Weniger, K. and T. Aramaki, "Route Optimization and Location Privacy using Tunneling Agents (ROTA)", Work in Progress, October 2005.

[19] Devarapalli, V., Wakikawa, R., Petrescu, A., and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol", RFC 3963, January 2005.

[20] Soliman, H., "Mobile IPv6 Support for Dual Stack Hosts and Routers", RFC 5555, June 2009.

[21] Wakikawa, R., Devarapalli, V., Tsirtsis, G., Ernst, T., and K. Nagami, "Multiple Care-of Addresses Registration", RFC 5648, October 2009.

[22] Muhanna, A., Khalil, M., Gundavelli, S., Chowdhury, K., and P. Yegani, "Binding Revocation for IPv6 Mobility", Work in Progress, October 2009.

[23] Haley, B. and S. Gundavelli, "Mobile IPv6 Generic Signaling Message", Work in Progress, August 2008.

Appendix A. Profiling Attack: Discussion

Profiling attacks pose a significant threat to user privacy. By collecting and analyzing (either online or offline) IP traffic, attackers can obtain sensitive user information. In the context of mobility, although the profiling attack does not directly lead to compromise of location privacy in the way the disclosure of the binding between the home address and the care-of address does, attackers can infer the mobile node's roaming and track its movement (i.e., handover) by profiling the mobile node's communication based on certain fields in IP packets, such as a constant IPsec SPI used during the home registration. The more information collected, the higher probability location privacy is compromised, which in return results in more targeted profiling.

We have taken the profiling problem into consideration when designing the solution to IP address location privacy; however, not all aspects of profiling attacks are addressed since the profiling problem spans multiple protocol layers. In the following, we provide a broad discussion on the profiling attack and protection mechanisms. Our discussion is organized based on how profiling attacks can be performed. Note that the following sections are not sorted based on any criteria or may not exhaustively list all the possible attack means (for example, profiling attacks based on upper-layer payloads in data packets are not discussed).

A.1. The Care-of Address

Eavesdroppers on the MN-HA path and/or the MN-CN path can profile the mobile node's communication by collecting packets with the same care-of address. It is recommended that the mobile node periodically updates its care-of address by using DHCPv6 or IPv6 address privacy extension, even if it does not change its current attachment point. Furthermore, it is even better to change the network prefix of the care-of address periodically, since eavesdroppers may profile IP packets based on the common network prefix.

Since the binding update procedure needs to be performed once the care-of address is changed, in order to reduce signaling overheads, the mobile node may choose to change its care-of address when the Binding Cache entry at the home agent or the correspondent node is about to expire.

A.2. Profiling on the Encrypted Home Address

Generated from either a real or pseudo home address, the encrypted home address can be dynamically updated, because a new key is generated when a new round of the return routability procedure is

performed, which makes the encrypted home address look different in subsequent Binding Update and Acknowledgement messages. Nevertheless, the same encrypted home address is used in payload packets forwarded via the optimized route before the next round of the return routability procedure. Given the cost and overhead of updating the encrypted home address, the proposed location privacy solutions still provide a reasonable level of protection against such profiling attacks.

A.3. The IPsec SPI

Eavesdroppers on the MN-HA path can profile the mobile node's communication based on the SPI of an IPsec security association that is for protecting the home Binding Update and Acknowledgement message or for protecting bidirectional-tunneled payload packets.

To resist this kind of profiling attack, the IPsec SPI needs to be periodically updated. One way is that the mobile node and the home agent rekey the IPsec security association or perform re-authentication periodically. This may result in more signaling overhead. Another way is that the mobile node or the home agent generates a new SPI and then notifies each other by exchanging the Binding Update and Acknowledgement messages protected by an existing IPsec security association with a non-null encryption algorithm. In this way, the information of the new SPI is hidden from eavesdroppers. The new SPI MUST not conflict with other existing SPIs; and if the conflict is detected on one end point, another SPI MUST be generated and be synchronized with the other end point. The new SPI is applied to the next packet that needs to be protected by this IPsec security association. This solution requires close interaction between Mobile IP and IPsec. For example, when the home agent receives a new SPI suggested by the mobile node, it needs to change the corresponding Security Association Database (SAD) entry.

A.4. The IPsec Sequence Number

The IPsec sequence number is required to be larger than that in the previous valid IPsec packet if the anti-replay service is enabled. However, if the increment of the IPsec sequence number is fixed (for example, the IPsec sequence number is sequentially increased), it is possible for eavesdroppers to identify a sequence of IPsec packets that are from/to the same mobile node and to track the mobile node's activities. One possible solution is to randomize the increment of the IPsec sequence number on both end points (i.e., the mobile node and the home agent) of the IPsec security association. The algorithm to generate randomness is implementation specific. It can be, for example, any random number generator, and independently chosen by each end point.

A.5. The Regular Interval of Signaling Messages

As described in RFC 3775, certain signaling messages may be exchanged on a regular basis. For example, the correspondent registration needs to be performed every MAX_RR_BINDING_LIFETIME seconds and the home binding update procedure needs to be performed regularly, if the lifetime of the home Binding Cache entry is fixed. Such timing allows eavesdroppers to perform traffic analyses and correlate different messages. Due to background traffic and routing dynamics, the timing of messages observed by an eavesdropper at a certain vantage point may be irregular. Nevertheless, a better solution is to randomize the lifetime of the Binding Cache entry in the home agent and the correspondent node.

A.6. The Sequence Number in the Binding Update Message

RFC 3775 requires that the sequence number in the Binding Update message be larger than that in the previous valid Binding Update message for a particular mobile node. However, if the increment of the sequence number in the home or correspondent Binding Update message is fixed (for example, the sequence number is sequentially increased), it is possible for eavesdroppers on the MN-HA or MN-CN path to identify a sequence of Binding Update messages that are from the same mobile node and to track the mobile node’s movement. One possible solution is that the mobile node randomizes the increment of the sequence number used in subsequent Binding Update messages. The algorithm to generate randomness is implementation specific. It can be, for example, any random number generator. Note that such an algorithm is not needed when the sequence number is encrypted, for example, when the home Binding Update message is protected by an IPsec tunnel mode security association.

A.7. Multiple Concurrent Sessions

It is possible for (colluded) eavesdroppers to correlate the mobile node’s different sessions with the same or different correspondent nodes, for example, based on the same pseudo home address and/or the same care-of address. A possible solution is to use different pseudo home addresses and different care-of addresses in different sessions. Note that the mobile node may also use the same pseudo home address with different correspondent nodes, if the pseudo home address is masked by different privacy management keys generated during the return routability procedure with different correspondent nodes. In this way, the encrypted pseudo home addresses used with different correspondent nodes look different to eavesdroppers.

A.8. Summary

As discussed above, there exist multiple means for eavesdroppers to correlate observed activities. For example, some IP fields, which contain certain constant values and remain unchanged for a long time, allow eavesdroppers to identify and link the mobile node's activities deterministically. Other means may be less reliable when used for traffic analysis and correlation; nevertheless, they provide additional hints to malicious attackers.

The solution to the profiling attack is to update certain IP fields periodically. Generally, the more frequently, the higher the probability that the profiling attack is resisted and also the higher the cost in terms of communication and processing overheads and complexity. As eavesdroppers can profile activities based on multiple fields, it may not be cost-effective to update some fields more frequently than others. Furthermore, it may reduce some overheads, if all the related IP fields are updated together with the same frequency.

The profiling attack is a complicated issue. A complete solution would have to consider tradeoffs of many different factors, such as complexity, effectiveness, and efficiency.

Authors' Addresses

Ying Qiu
Institute for Infocomm Research, Singapore
1 Fusionopolis Way
#21-01 Connexis (South Tower)
Singapore 138632

Phone: +65-6408 2053
EMail: qiuying@i2r.a-star.edu.sg

Fan Zhao (editor)
Google Inc.
1600 Amphitheatre Parkway
Mountain View, CA 94043
US

EMail: fanzhao@google.com

Rajeev Koodli
Cisco Systems

EMail: rkoodli@cisco.com