Internet Engineering Task Force
Internet-Draft
Intended status: Standards Track
Expires: September 24, 2010

J. Espi
R. Atkinson
University of Strathclyde

March 23, 2010

Proactive Route Optimization for FMIPv6
draft-espi-ietf-mipshop-profmipv6-00.txt

Abstract

The Fast Handovers for Mobile IPv6 (FMIPv6) protocol was developed from the experience of MIPv6 and the facilities provided by link layer triggers, allowing for a proactive approach to handover that minimises packet exchange delay and packet loss. On completion of handover, the mobile node engages MIPv6 procedures in to update the Home Agent with the mobile node's new location. Subsequently, the mobile node may carry out Return Routability with the correspondent node(s) for route optimization. However, this method leaves scope to optimize handover delays derived from the signalling message exchange.

This document proposes an enhancement to FMIPv6, the Proactive Route Optimization for FMIPv6 (PRO-FMIPv6) protocol, which aims to further reduce the signalling load thereby improving the overall performance of the handover process.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

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

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

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

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on 24th September 2010.

Table of Contents

1. Introduction

The process of leaving a network link to join another is referred to as handover. Fast Handovers for Mobile IPv6 (FMIPv6) [RFC5568] enables a proactive approach to handover: before handover, the mobile node (MN) forms a new care-of address and solicits the present/ previous access router to start forwarding packets to that address at the next/new access router's link. As a consequence, the communication disruption is limited to the link layer procedures, i.e., synchronizing to the new access point (AP). Subsequently, the FMIPv6-enabled MN updates the binding cache of its home agent (HA) with its new care-of address (NCoA) and, optionally, the correspondent node (CN)'s binding cache for optimal routing via the Return Routability procedure [RFC3775].

The standard procedures based on FMIPv6 handover and route optimisation leave scope to reduce the handover delays and the signalling latency [RFC4651]. This document introduces Proactive Route Optimization for FMIPv6, namely, PRO-FMIPv6, which reduces this latency by carrying out the signalling towards route optimization proactively.

More specifically, this specification suggests using cryptographically generated addresses to bind the home address (HoA) and the previous care-of address (PCoA) to the NCoA. The signalling exchange between MN and CN, carried out proactively, allows the CN to check the validity of the new care-of address through a cryptographic route test.

PRO-FMIPv6 is independent of the link-layer technology. The document updates the format of the "(Proactive) Home Address Test Initiation (PHoTI)" message, "(Proactive) Care-of Test Initiation (PCoTI)" message and "Fast BU (FBU)" message. It also defines a new type of Mobility Header-based option; the "Binding Update Info (BUInfo)".

The handovers defined in this specification can interwork with MIPv6/ FMIPv6 enabled networks as they are backwards compatible.

1.1. Language Requirements

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119]. The use of the term, "silently ignore" is not defined in RFC 2119. However, the term is used in this document and can be similarly construed.

The following terminology and abbreviations are used in this document

in addition to those defined in [RFC3775, RFC5568].

Proxy Binding Update (PrBU): It is a BU sent on behalf of the MN by any other network entity.

Token Table: It is kept by the CN. It contains the MN's HoA, PCoA and tentative NCoA, the two tokens used for route optimization security check and the NAR's prefix.

2. Protocol Overview

The proposed protocol aims to integrate a novel signalling scheme for route optimization within the FMIPv6-provided facilities.

As in FMIPv6, through the "Router Solicitation for Proxy Advertisement (RtSolPr)" and "Proxy Router Advertisement (PrRtAdv)" messages, the MN also formulates a prospective new CoA (NCoA) when it is still present on the PAR's link. This address can be used immediately in the new subnet link when the MN has received a "Fast Binding Acknowledgment (FBack)" (see Section 6.2.3 in [RFC5568]) message prior to its movement. In the event it moves without receiving an FBack, the MN can still use the NCoA after announcing its attachment through an "Unsolicited Neighbor Advertisement (UNA)" message (with the 'O' bit set to zero) [RFC4861]; the NAR may respond to this UNA message if it wishes to provide a different IP address to use. In this way, NCoA configuration latency is reduced.

The information provided in the PrRtAdv message can be used even when DHCP [RFC3315] is used to configure an NCoA on the NAR's link. In this case, the protocol supports forwarding using PCoA, and the MN performs DHCP once it attaches to the NAR's link. The MN still formulates an NCoA for FBU processing; however, it MUST NOT send data packets using the NCoA in the FBU.

Like FMIPv6, the MN generates the NCoA from the NAR's prefix, included in the PrRtAdv message. However, additionally, the MN generates two random numbers (tokens). The NCoA is form as shown in equation (1).

NCoA = NAR_prefix | hash (HoA | token1 | token2) (1)

Each of the tokens (token1 and token2) is included in a Mobility Header-based message (PHoTI and PCoTI) that traverse different paths to the CN. The PHotI message is sent to the CN via the HA just like the HoTI message in standard MIPv6, and the PCoTI message is sent via the NAR. The CN receives both packets (PHoTI and PCoTI) from the home and care-of addresses respectively. This requires both the HA

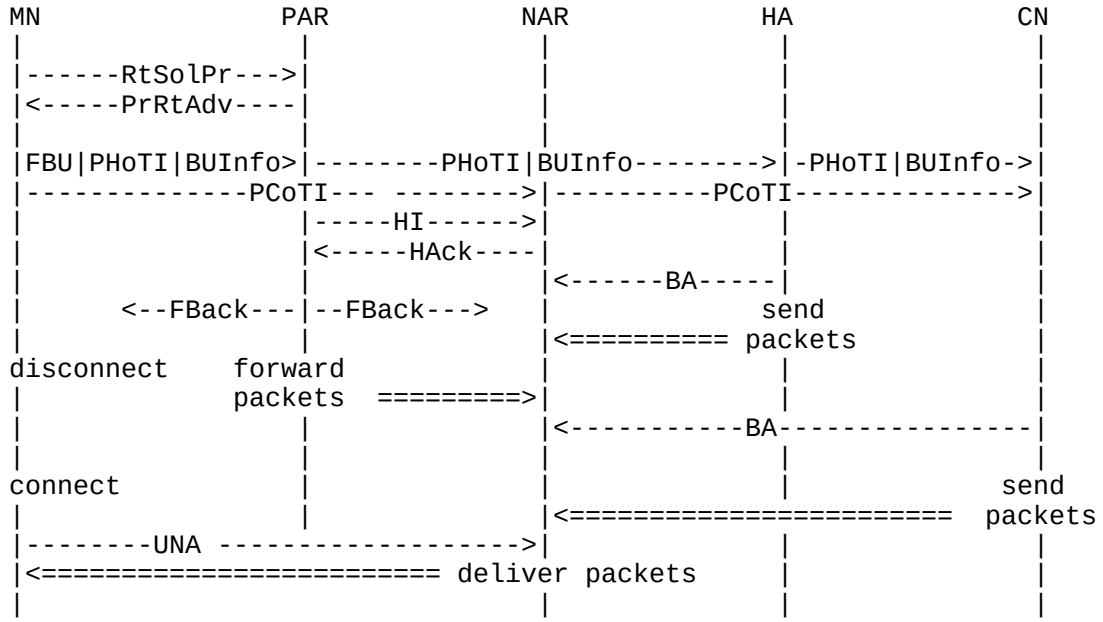
and the NAR to proxy those packets, i.e., the HA has to set the IPv6 source address field in the PHoTI packet to the home address, and the NAR has to set the PCoTI source address to the new care-of address. Moreover, the PAR and the HA update their MN's NCoA entries with the NCoA included in the PHoTI message.

On receipt of the two tokens, the CN is able to check whether the home and care-of addresses fit with that in equation (1). If the NCoA is valid, the CN updates its binding cache and replies with a BA. However, if the check is not valid, the packets are silently discarded.

Immediately after sending FBU | PHoTI and PCoTI, the MN starts layer 2 handover. After joining the new link, the MN announces its attachment with a UNA message that instructs NAR to forward packets to the MN.

The MN MUST receive a FBack message from the PAR indicating the tunnel is correctly set. The MN MUST receive at least one FBack since this message is bicasted from the PAR to both the PCoA and NCoA.

Likewise, the MN MUST receive a BA from the HA acknowledging the MN's NCoA. Also, if the CN's validity check is met, the CN MUST send a BA to the NCoA.



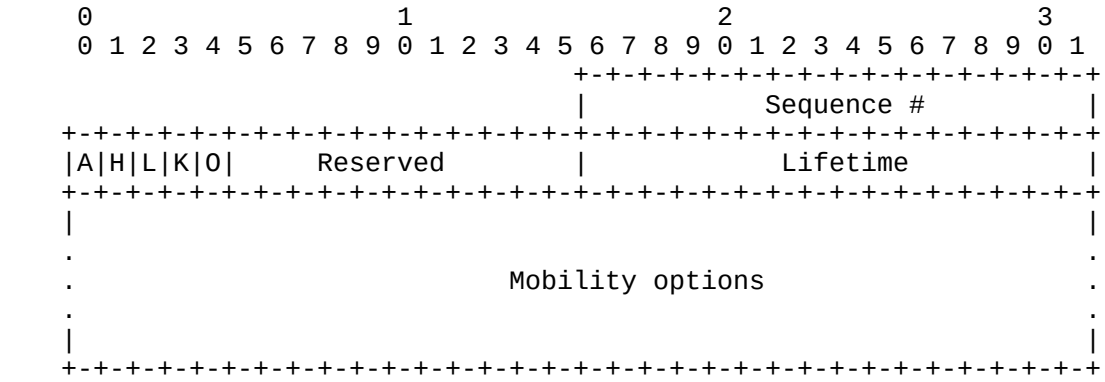
PRO-FMIPv6 signalling.

3. Message Formats

3.1. Modifications to MIPv6 and FMIPv6 Mobility Header-based messages

3.1.1. Modified FBU Mobility Message Format

The 'O' flag has been added as follows.



Modified FBU Mobility Message.

IP Fields:

Source Address: The PCoA

Destination Address: The IP address of the Previous Access Router.

'A' flag: See [RFC5568].

'H' flag: MUST be set to one. See [RFC3775],[RFC5568].

'L' flag: See [RFC3775].

'K' flag: See [RFC3775].

'O' flag: The Proactive Route Optimization ('O') is set by the MN to request the PAR to forward the enclosed mobility options to the HA.

Reserved: This field is unused. MUST be set to zero.

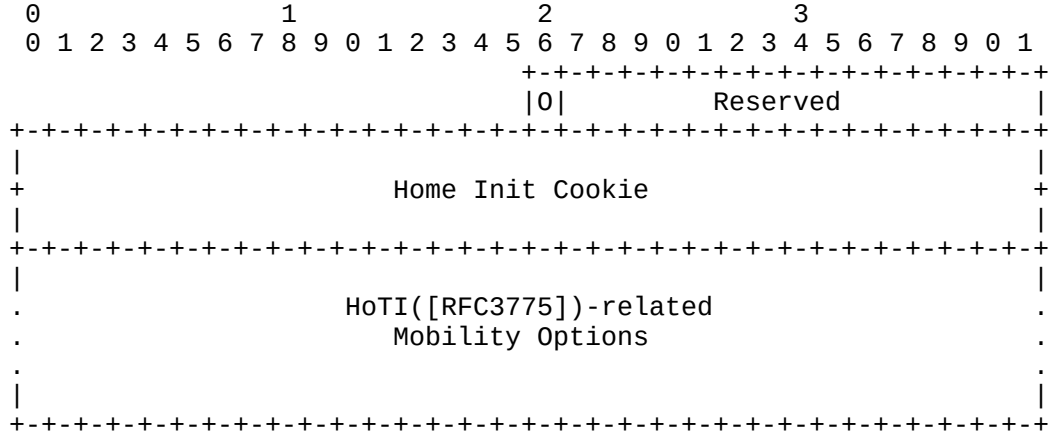
For descriptions of other fields present in this option header, refer to Section 6.2.2 of [RFC5568].

The FBU message is sent by the MN using its PCoA to the PAR's IP address

3.1.2. Proactive HoTI Message

In [RFC3775] the HoTI message is designed to initiate the return routability procedure and request a home keygen token from a correspondent node. The Proactive Home Test Init message is forwarded by the HA to the CN using the MH Type value 1.

The HoTI message has been modiffied including the 'O' flag to indifcate proactive optimization. When this value is indicated in the MH Type field, the format of the Message Data field in the Mobility Header is as follows:

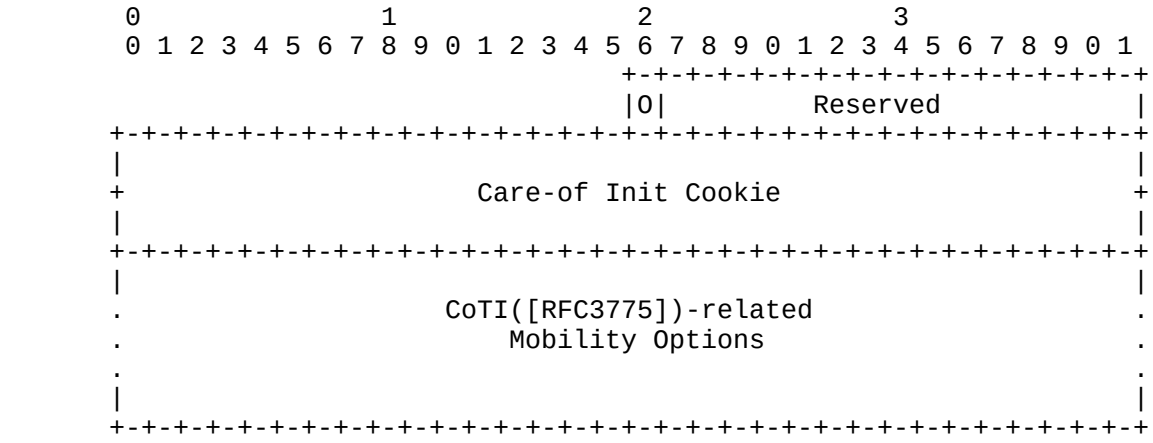


Proactive HoTI.

3.1.3. Proactive CoTI Message

In [RFC3775] the CoTI message is used to initiate the return routability procedure and request a care-of keygen token from a correspondent node. The Proactive Care-of Test Init message is forwarded by the NAR to the CN using the MH Type value 1.

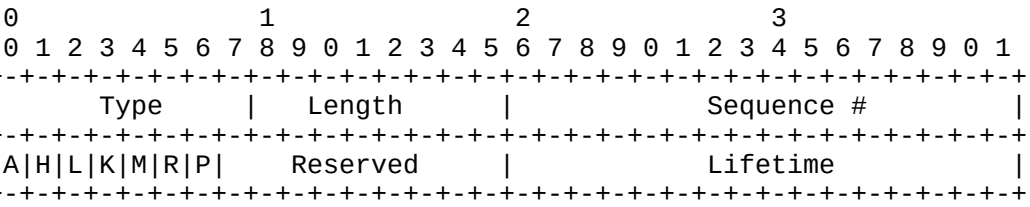
The CoTI message has been modified including the 'O' flag to indicate proactive optimization. When this value is indicated in the MH Type field, the format of the Message Data field in the Mobility Header is as follows:



Proactive CoTI.

3.2. New Mobility Options

3.2.1. BU Info Option



BU Info.

The BU Info option header is equivalent to the BU message [RFC3775]. The flags remain the same as in [RFC3775], including those defined in [RFC3963], [RFC4140] and [RFC5213] ('R', 'M' and 'P' respectively).

Type: 28

For descriptions of other fields present in this option header, refer to Section 6.1.7 of [RFC3775].

4. Protocol Details

4.1. Corrrespondent Node Operation

4.1.1. Data Structures

In addition to a Bining Cache, the CN MUST maintain a Token Table, where the CN keeps track of the tokens received and mobility related information from the MN. Each MN already contacting the CN towards route optimization has one entry. Each entry has five fields:

HoA: obtained at session set up

NCoA: retrieved from PHoTI (IP in IP encapsulation) and PCoTI messages

Token1: token included in PHoTI message

Token2: token included in PCoTI message

NAR's prefix: retrieved from PCoTI message

This Token Table MAY be implemmented in any manner consistent with the behaviour described in this document.

4.1.2. Route Optimization Signalling

4.1.2.1. Receiving PHoTI and PCoTI

The CN, on receipt of either the PHoTI or the PCoTI message, MUST create an (incomplete) entry in the Token Table. This entry will be kept until the second message is received or MAX_TOKEN LIFETIME seconds are elapsed. The MAX_TOKEN LIFETIME timeout period is devised to prevent memory exhaustion due to the size of the CN's Token Table.

If both messages are correctly received within a MAX_TOKEN LIFETIME seconds time frame, then the CN will MUST validate the following tests:

NCoA MUST be a unicast routable address.

PHoTI and PCoTI MUST have same nonce index.

Fields in the Token Table MN's entry (NAR's prefix, tokens 1 and 2, Home Address) MUST meet equation (1).

If the tests are met, then the CN processes the BUInfo option (included in the PHoTI message) as described in RFC 3775, Section 9.5.1. Next, the CN sends a BA to the MN's NCoA according to RFC 3775, Section 9.5.4.

If the tests are not met, the MN's entry is removed from the Token Table.

4.1.2.2. Sending Binding Acks

Refer to RFC 3775, Section 9.5.4.

4.1.2.3. Sending Binding Refresh Requests

This document does not address refreshing bindings.

4.2. Home Agent Operation

The Home Agent operation is largely based on [RFC3775]. On receipt of a PHoTI message, the Home Agent checks the validity of the enclosed BU Info option. If the validity check is successful, the Home Agent MUST send a BA to the MN's NCoA. Next, the Home Agent forwards the PHoTI message to the CN's address.

However, if the validity check fails, the Home Agent silently ignores the PHoTI message.

The Binding Cache entry is to last MAX_RR_BINDING LIFETIME seconds. In the eventuality of expiration of the Binding Cache entry, the Home Agent operates as in [RFC3775].

4.3. New Access Router Operation

The NAR MUST behave as stated in [RFC5568].

Prior to handoff, the MN sends the PHoTI and the PCoTI messages, that traverse different paths towards the CN. The PCoTI message is routed along the PCoA-NCoA-CN path. The NAR, on recepit of the PCoTI message, MUST forward it to the CN, including the PCoA as a home address option (defined in [RFC3775]).

4.4. Previous Access Router Operation

The PAR MUST behave as stated in [RFC5568]. Additionally, of receipt of the PoTI message, it MUST forward it to the HA, including the PCoA as a home address option ([RFC3775]).

4.5. Mobile Node Operation

The protocol begins when the MN sends the RtSolPr to its PAR to resolve one or more Access Points Identifiers to subnet-specific information. In response, the PAR sends the PrRtAdv containing one or more [AP-ID, AR-Info] tuples [RFC5568].

From the information received in the PrRtAdv message, the MN generates a prospective NCoA using equation (1). In order to do so, the MN generates two random tokens that it concatenates to the HoA and applies a SHA1 hash function to the result.

The MN will then send two messages, the FBU and the PCoTI.

The FBU message comprises a PHoTI message and a BUInfo option enclosed in a MIPv6 FBU message. The MN sends this message to the PAR. In the BUInfo option, bit 'A' MUST be set.

The PCoTI message is sent to the NAR, that will forward it to the CN (IPv6 encapsulation).

Next, the MN performs handover to the NAR. After the attachment, the MN should receive two acknowledgements, specifically, from the PAR and the HA. The MN may receive a third acknowledgement from the CN, in the special case wherethe CN is PRO-FMIPv6 enabled.

5. Configurable Parameters

Mobile nodes rely on the configuration parameters defined in section 12 of [RFC3775] and section 9 of [RFC5568]. Each mobile node MUST have a configuration mechanism to adjust the parameters.

In addition, the value of MAX_TOKEN LIFETIME ([RFC3775]) is reduced to 3 seconds. The rationale behind this is that the MN sends both the PHoTI and PCoTI messages simultaneously and therefore the CN expects to receive them at approximately the same time.

6. Security Considerations

Firstly, a malicious MN may try to redirect traffic from his HoA or PCoA to a NCoA. E.g., if a MN is connected with a server through a high-speed connection, the MN could redirect the stream towards a low-speed NAR (in terms of processing or link capacity).

PRO-FMIPv6 precludes MN from carrying out this kind of attacks: The NAR can voluntarily discard the PCoTI message if the QoS required for the MN is too high, if the proposed NCoA is not acceptable, if the source PCoA or HoA is from a domain not accepted, if the NAR does not have any established trust relationship with the PAR, if the demanded buffer size is too high or if the access control parameters do not meet the security requirements. The NAR retrieves information on all the previously mentioned issues from the HI message.

Even if this kind of Denial of Service (DoS) attack could be effectively carried out, the malevolent MN would not be capable of specifying any concrete IPv6 address. The rationally behind that is that it would be virtually impossible for a MN to find two random numbers such that the result of equation (1) is equivalent to the target IPv6 address.

Secondly, a malicious 3rd party may try to steal a node's (either mobile or fixed) IPv6 address by creating a binding cache entry at the CN. PRO-FMIPv6 prevents attackers from doing this. In case a HA receives a PHoTI message for whose HoA has no administrative agreement, it silently ignores it.

Thirdly, one or more attackers may want to consume all the memory available in the CN's tokens table by sending a number of PHoTI or PCoTI messages. In any case, every time a CN receives a BU|t1 or BU|t2 the CN overrides the correspondent HoA or NCoA respectively, so therefore there is only one entry at the tokens table for each MN, independently of how frequently performs the signalling towards route optimization. Moreover, registers in the token table are only kept for MAX_TOKEN LIFETIME seconds.

Finally, the protocol inherits the vulnerabilities identified in [RFC5568] for the RtSolPr, PrRtAdv and FBU messages.

7. IANA Considerations

TBD

8. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[RFC3775] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[RFC3963] Devarapalli, V., Wakikawa, R., Petrescu, A., and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol", RFC 3963, January 2005.

[RFC4140] Soliman, H., Castelluccia, C., El Malki, K., and L.

Bellier, "Hierarchical Mobile IPv6 Mobility Management (HMIPv6)", RFC 4140, August 2005.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.

[RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.

[RFC5568] Koodli, R., "Mobile IPv6 Fast Handovers", RFC 5568, July 2009.

Authors' Addresses

Jorge Espi
University of Strathclyde
Glasgow,
UK

Phone: +44 0141 548 2527
Email: jorge.espi@eee.strath.ac.uk

Robert C. Atkinson
University of Strathclyde
Glasgow,
UK

Phone: +44 0141 548 2879
Email: r.atkinson@eee.strath.ac.uk