Proactive Route Optimization for Fast Mobile IPv6

Jorge Espi, Robert Atkinson, Ivan Andonovic and John Dunlop
Centre for Intelligent Dynamic Communications,
University of Strathclyde, Glasgow, UK

***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. After handover, 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 paper proposes an enhancement to FMIPv6, the Proactive Route Optimization for FMIPv6 (PRO-FMIPv6) protocol, which significantly reduces the signalling and thereby improves the overall performance of the handover process. Simulation results suggest a delay reduction up to 50% over other current proposals: the FMIPv6 protocol, Enhanced Route Optimization and Proactive Bindings for FMIPv6.**

***Keywords*—**Fast Mobile IPv6, latency, route optimization.

I. INTRODUCTION

The process of leaving a network link to join another is referred to as handover. Fast MIPv6 (FMIPv6) [1] 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 (PAR) to start forwarding packets to that address at the next/new access router's (NAR) 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 with its new care-of address and, optionally, the correspondent node's (CN) binding cache for optimal routing via the Return Routability procedure [2], as explained in Section II.A.

The standard procedures based on FMIPv6 handover and Return Routability route optimisation leave scope to reduce handover delays and overall route optimisation performance in terms of security. Security is not the primary focus in this paper as the Return Routability achieves security, in terms of authentication, comparable to the non-mobile Internet, however, overall signalling latency is the metric of interest.

Two relevant approaches to improved route optimisation will be reviewed and compared with the approach suggested in this paper: Proactive Bindings for FMIPv6 (PB-FMIPv6) [6] and Enhanced Route Optimisation for FMIPv6 (ERO) [7]. PB-FMIPv6 executes the MN's link layer handover while the NAR conducts signalling tasks, such that both processes are carried out simultaneously. ERO defines early binding update functionality, by which the CN updates its binding cache immediately after handover.

The approach suggested in this paper, Proactive Route Optimization for FMIPv6 (PRO-FMIPv6) takes advantage of cryptographically generated addresses to bind the previous care-of address to the new one. 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 combined routing-cryptographic test. The security analysis carried out confirms it is as secure as the Return Routability protocol. Furthermore, simulation results show a reduction of the overall handover signalling process up to 50% in comparison with the other protocols considered in this paper.

This paper is structured as follows. In Section II, the FMIPv6 and Return Routability protocols are introduced, and some other relevant approaches to route optimisation are discussed. In Section III the Proactive Route Optimization for FMIPv6 protocol is explained. Section IV shows the simulation results. In Section V a security analysis is performed. Finally, Section VI concludes the paper.

II. BACKGROUND

In the forthcoming discussion, three of the most relevant approaches for route optimization, namely, FMIPv6, PB-FMIPv6 and ERO, will be examined in turn.

A. FMIPv6 and Return Routability

FMIPv6 is a set of enhancements for MIPv6 that allows for a reduction in handover delays and a minimisation of packet loss for mobile users. The FMIPv6 handover procedure is shown in Fig. 1.

FMIPv6 assumes the MN discovers available APs using layer 2 specific mechanisms. However, to facilitate obtaining layer 3 information, such as IP prefixes, FMIPv6 provides the 'Router Solicitation for Proxy (RtSolPr)' and 'Proxy Router Advertisement (PrRtAdv)' messages to allow the MN to formulate a prospective new CoA (NCoA) prior to handover, while still attached to the PAR's link. This address is then passed to the PAR in a 'Fast Binding Update (FBU)' message, which is acknowledged by a 'Fast Binding Acknowledge (FBAck)' message at the MN. Thus, before handover the MN forms a NCoA that is valid in the new link.

FMIPv6 checks the validity and availability of the NCoA on the new link by means of the 'Handover Initiate (HI)' and 'Handover Acknowledge (HAck)' message exchange between the PAR and the NAR. Thus, after the MN passes its NCoA to the PAR while still in PAR's link, any packets addressed to MN in the PAR's link are forwarded to the NAR, which buffers them on behalf of the MN. When the MN attaches to the NAR's link, it sends a notification message to the NAR; the NAR can then forward the buffered packets to the MN. This approach minimises packet loss during link layer handover.

Next, the MN behaves as in [2] updating the home agent's (HA) binding cache with the NCoA through a 'Binding Update (BU)' message. On receipt of the 'Binding Acknowledgement (BA)' from HA, the MN may start the Return Routability procedure to establish direct communication with the CN. This direct path will generally be the shortest path between the nodes and may result in an

improvement in QoS (such as reduced jitter, delay and packet loss) [3].

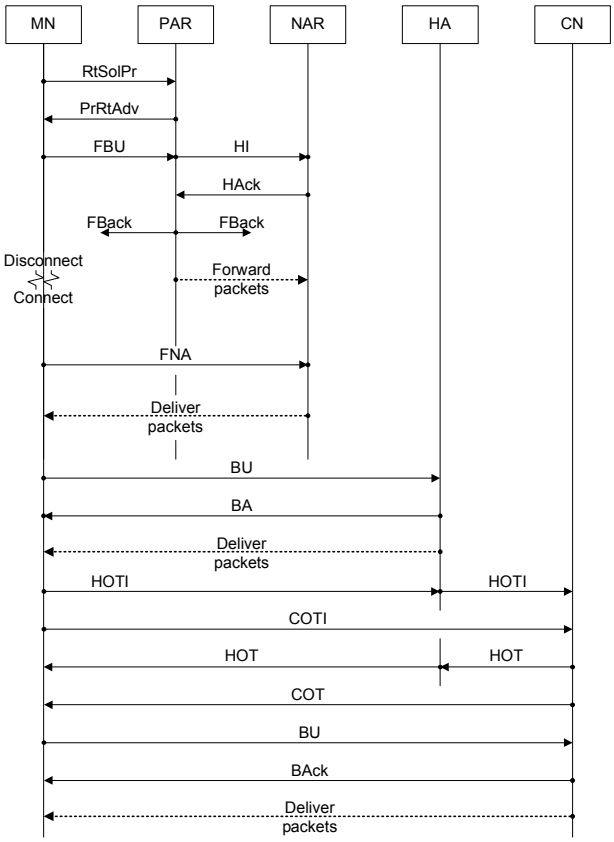


Fig. 1. FMIPv6 and Return Routability signalling

Updating both HA and CN with the NCoA is cryptographically secured. However, while Johnson et al [2] suppose an existing administrative association between HA and MN, the process of securing the communication between CN and MN is embodied in the Return Routability (RR) procedure.

While the HA may be assumed to have a pre-existing security association with the MN and can hence exchange BUs securely, the same cannot be assumed for the CN and the MN. The RR procedure is therefore designed to enable a CN to authenticate a BU (containing an NCoA) from the MN. RR does not provide strong authentication but can provide a degree of confidence (assuming a non-compromised Internet infrastructure) [4] that a BU received from a MN by the CN pertains to a pre-existing binding. The RR procedure operates as follows. The MN sends a Home Address Test Initiate (HOTI) message to the CN via its HA, and simultaneously sends a Care-of Address Test Initiate (COTI) message directly to the CN as shown in Fig. 1. These messages prompt a response in the form of a Home Address Test (HOT) and Care-of Address Test (HOT) from the CN to the MN, the former going via the HA; both the HOT and the COT contain cryptographically generated tokens. On reception of both the HOT and COT, the MN uses both tokens to form a key to sign a BU which consequently authenticates its identity. Note, authentication in this approach assumes that only the MN is able to receive both the HOT and COT messages and this can only be guaranteed if the paths taken by these messages are fully disjoint: this is unlikely to be the case in practice.

RR is the route optimization standard signalling scheme to prove ownership of the NCoA; however, it also introduces latencies for route optimized handover [5]. This paper will propose modifications to this approach to reduce these latencies. Two other approaches to reducing these latencies have been proposed: Proactive Bindings for FMIPv6 and Enhanced Route Optimization, and will be examined in the next sections.

B. Proactive Bindings for FMIPv6

In standard FMIPv6, after link layer handover has taken place, the MN must update the HA and, optionally, the CN(s) with its NCoA. In order to do so, the MN exchanges a BU and a BA with its HA, and subsequently initiates the RR procedure with its CN. These exchanges incur latencies.

Proactive Bindings for FMIPv6 (PB-FMIPv6) [6] aims to reduce the route optimisation signalling latency in FMIPv6 by delegating to the NAR the tasks related to NCoA registration with the HA and CN(s), i.e., the RR procedures (Fig. 2). These tasks are conducted while the MN is in the process of performing link layer handover. Consequently, this approach takes advantage of the simultaneous execution of RR and MN's link layer handover, and therefore, the overall latency of standard FMIPv6 handover may be reduced.

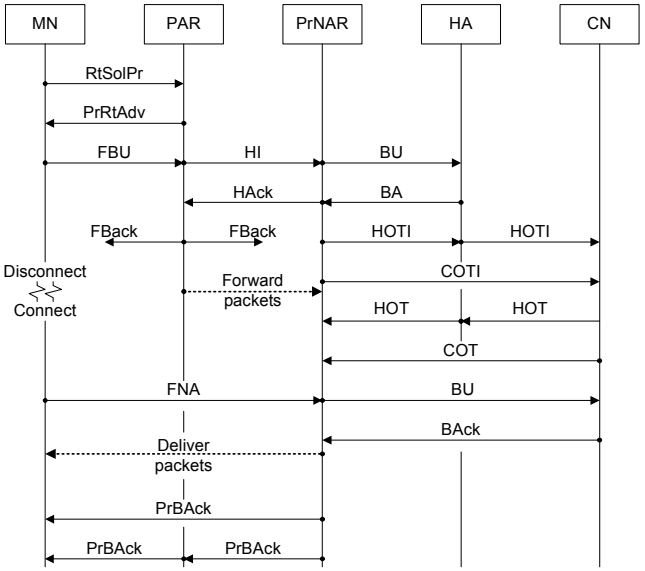


Fig. 2. PB-FMIPv6 signalling

PB-FMIPv6's NAR acts as a proxy on behalf of the MN to conduct the RR signalling tasks. In comparison with standard FMIPv6, this approach may be advantageous in those cases where the NAR receives the HI message before the MN joins the new link. This may occur depending on two factors: the end-to-end delay between PAR and NAR, and link layer handover delay. At the special case where the HI message arrives earlier than the MN at the new link, this approach represents an advantage in terms of overall signalling latency: while the mobile node is still carrying out link layer handover, the NAR performs route optimization.

Otherwise, in those cases where the link layer handover delay is lower than the message trip time from PAR to NAR, the MN will join the new link before the NAR has been triggered to start the signalling procedures, incurring in avoidable delays.

C. Enhanced Route Optimization

Enhanced Route Optimization (ERO) [7] specifies an enhanced version of the Mobile IPv6 RR procedure (Fig. 3). With ERO, the home address test is preformed proactively prior to handover hence avoiding the associated latency. The home address test provides strong authentication because the home address is a Cryptographically Generated Address (CGA). This type of address has the property of being verifiably bound to a public/private key pair. In this manner, the MN proves ownership of the home address by evidencing knowledge of the corresponding private key. These stronger security facilities preclude attacks from nodes on the home address test path (between MN and HA), permitting longer binding lifetimes and consequently reducing the signalling overhead.

ERO also considers the reliability of the communication. Relying on its trust relationship with the MN, the CN accepts a concurrent ('early') BU-BA exchange together with the care-of test, permitting immediate re-establishment of direct communication via the MN's new care-of address. This process makes use of 'credits' to temporarily limit the traffic volume between the CN and NCoA until the NCoA has been fully authenticated.

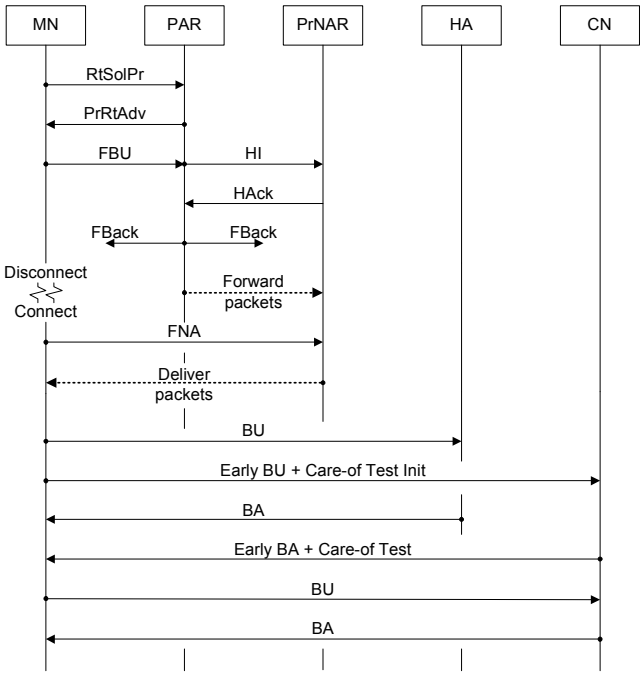


Fig. 3. ERO signalling

However, this approach introduces a significant limitation on the data transmission performance, as the CN has an upper bound for the packet transmission rate equal to the data reception rate from the MN. In cases where the communication is asymmetric, e.g. video- or audio-streaming, or file transfer, the MN will only communicate the CN to acknowledge the data received. The CN will then have a restricted transfer capability as long as the amount of data able to be sent to the MN is equal or lower than the addition of the acknowledgment packet payload sizes received from it. Alternatively, in those cases where MN and CN have established a bi-directional communication, e.g. VoIP, the MN will have to wait a RTT from its care-of to the correspondent address to start receiving packets and will impair perceived QoS.

For these reasons, the ERO credit-based system constrains the data throughput of the system.

III. PROPOSED SOLUTION

This paper proposes Proactive Route Optimization for FMIPv6, which provides lower handover delay than the protocols introduced in Section II, while maintaining the security requirements discussed in [5]. A detailed description of Proactive Route Optimization for FMIPv6 (PRO-FMIPv6) follows. Building on FMIPv6, the MN generates the NCoA from the NAR´s prefix, included in the PrRtAdv message. However, additionally, the MN produces two random numbers (tokens). The new care-of address is form as shown in equation 1.

$$New\ CoA = new\_net\_pref \mid hash\ (HoA \mid t1 \mid t2) \qquad (1)$$

Each one of the tokens (t1 and t2) is included in an FBU-based message (FBU | t1 and BU | t2) that traverse different paths to the CN. The CN receives both packets (BU | t1 and BU | t2) 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 IP packet to the home address, and the NAR has to set it to the new care-of address (Fig. 4). Moreover, the PAR updates its binding cache with the NCoA included in the FBU | t1 message and the HA updates its binding cache with the NCoA included in the BU | t1 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.

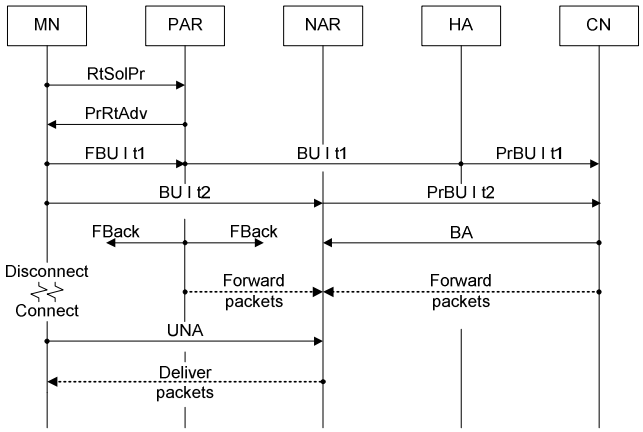


Fig. 4. PRO-FMIPv6 signalling

PRO-FMIPv6 does not check the validity of the NCoA in the new link prior to handover. Alternatively, Optimistic DAD is used.

FMIPv6 and PB-FMIPv6 enabled MNs are constrained by the need to update the CN(s) every 420 seconds. However, ERO relaxes this constraint by extending the update interval to 24 hours, as it relies on a strong home address authentication, and this reduces the overall signalling load. The signalling overhead in the proposed PRO-FMIPv6 solution is similarly reduced: giving rise to signalling loads significantly less than both PB-FMIPv6 and ERO approaches, and a time interval approximately equal to the mean connection time is used for binding refreshment of the CN(s).

Also, a packet loss characterization is relevant. However, FMIPv6-based protocols are not supposed to produce packet loss if the predictive mode of operation is being used [1], which is precisely the mode in which PRO-FMIPv6 procedures apply.

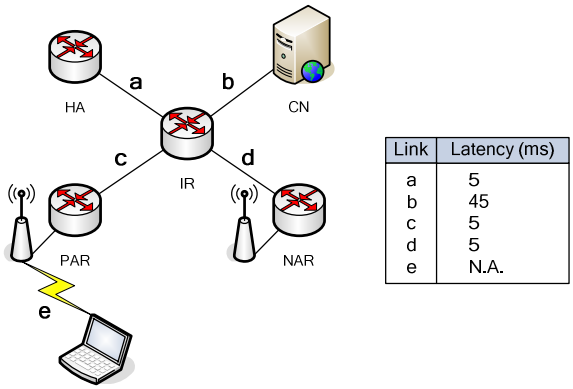
IV. EXPERIMENTAL RESULTS

Simulations have been conducted to estimate a range of parameters related to the overall handover signalling performance. Since the aim of the protocols discussed is to update the CN's binding cache, the time delay before communication through the optimised route can be re-established is the metric of interest.

It is recognised that packet reordering may occur as a result of flow diversion on PAR and HA and that this may have a negative impact on upper layer protocol performance. However, the effects of packet reordering are out of the scope of this paper.

The simulations have been carried out using the INET Framework for OMNeT++ [8].

Fig. 5 shows the system model from which network performance is evaluated. The network is composed by 6 participating nodes, and the links interconnecting them are described in terms of packet delivery latency [9] and throughput. Each of the links can be configured with a packet latency value to emulate the anticipated latencies in a real system between the CN, HA, MN, PAR, and NAR. The wired links are Gigabit Ethernet type, while the wireless link is 54 Mbps IEEE802.11b.



Link	Latency (ms)
a	5
b	45
c	5
d	5
e	N.A.

Fig. 5. System model

Four scenarios (A-D) are considered for each of the four schemes (FMIPv6, PB-FMIPv6, ERO, PRO-FMIPv6); the scenarios are differentiated by total link layer handover delay: 0s, 0.25s, 0.5s, and 1s respectively. Scenario A, corresponding to a handover delay of 0s, is of particular interest for two reasons: (1) from a theoretical perspective it provides an upper bound on the performance of each protocol, (2) from a practical perspective it provides a realistic assessment of the performance that may be expected where the MN were multihomed ([10], [11]) – this is particularly pertinent given the plethora of terminals with multiple interfaces on the market at present. The other scenarios permit comparative analysis for a range of handover delays since previous studies have demonstrated that relative performance is dependent on layer 2 handover latency. All scenarios assume an identical service: a stream of UDP packets sent from the CN to the MN at an interval of 20ms (consistent with standard VoIP codecs). At a predefined time a layer 2 hint [12] is simulated which initiates the handover process. In all cases proactive handover is assumed. On the simulation of the ERO protocol, the MN is considered to have performed the home test prior to handover, so the CN trusts the MN's reachability though its home address. On the simulation of the PRO-FMIPv6 protocol, Optimistic DAD is used (FBAck message functionalities are reduced to acknowledging the packet forwarding from PAR to NAR). This has no effect on the performance evaluation as for the other approaches DAD is carried out prior to handover and the route optimization signalling, through the HI and HAck messages. An extension of the PRO-FMIPv6 scheme to include DAD is explored in Appendix A.

As a consequence of path changes during handover, some packets sent along the new route may arrive earlier the MN than the last packet(s) sent along the previous, non-optimised route, causing reordering. Moreover, as a consequence of different delays assumed for each segment of the network, and the design of the signalling schemes, the binding updates will reach either the HA or the CN at different times, depending of the paths they traverse.

Fig. 6 illustrates the aforementioned effects on the system model depicted in Fig. 5.

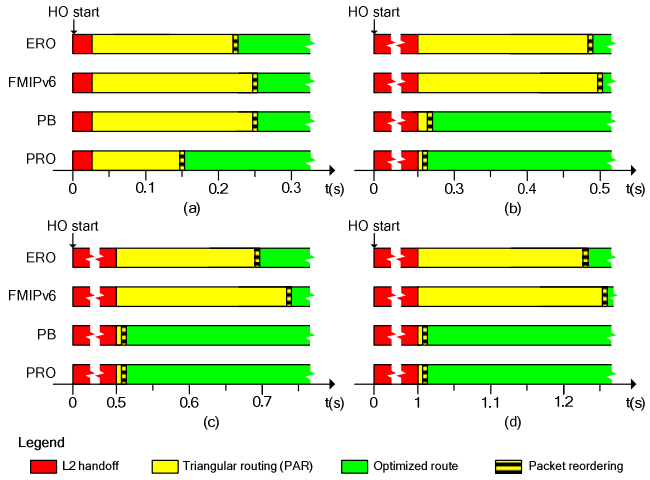


Fig. 6. Time elapsed until flow diversion **(a)** Scenario A – Negligible L2 handover delay **(b)** Scenario B – 0.25s L2 handover delay **(c)** Scenario C – 0.5s L2 handover delay **(d)** Scenario D – 1s L2 handover delay

Fig. 6 shows the performance of the four considered protocols in the scenarios A-D. Performance, in terms of latency, is measured as the delay from the start of the layer 2 handover until the establishment of direct communication between MN and CN (optimized route). Immediately after handover, and prior to establishing the optimized route, the mobile node receives packets along the path CN-PAR-NAR. This path is associated with higher packet latency than the optimized (CN-NAR) one.

In scenario A, the link layer handover delay is set to 0s. The results derived from this scenario set an upper bound to the performance of the ERO and FMIPv6 protocols. Given that they perform signalling tasks on the new link, having a 0s link layer handover delay, they don't suffer from additional delays from the link layer procedures. Meanwhile, PB-FMIPv6 and PRO-FMIPv6 take no advantage of the concurrent scheduling of tasks (route optimization signalling and link layer handover). There are notable differences on the performance, however, as result of the trip times of the signalling messages involved: ERO, FMIPv6, PB-FMIPv6 and PRO-FMIPv6 take 0.22s, 0.26s, 0.26s and 0.15s, respectively, to set the optimized route.

In scenarios B, C and D the link layer handover delay is set to 0.25s, 0.5s and 1s respectively. As ERO and FMIPv6 carry out signalling procedures in the new link after joining it, these delays are added towards the establishment of the optimized route. Alternatively, in both PB-FMIPv6 and PRO-FMIPv6, as the signalling mechanisms are performed in parallel while the MN is in the process of joining the new link, these latencies are therefore not cumulative.

In general, link layer procedures delay is additional to the overall signalling latency of ERO and FMIPv6. Making use of PB and PRO,

this delay just sets an upper bound on the performance. Table 1, obtained from the results on Fig. 6, corroborates this statement.

TABLE 1
DELAY TO SET OPTIMIZED ROUTE AFTER HANDOFF

HO delay (s)	0	0.25	0.5	1
ERO	0.215	0.221	0.228	0.202
FMIPv6	0.262	0.261	0.269	0.253
PB	0.262	0.025	0	0
PRO	0.150	0	0	0

For these reasons, the solution proposed in this paper performs better than the other protocols under consideration in the scenarios A and B. In the scenarios C and D, it performs as fast as the PB protocol. Consequently, a PRO-FMIPv6 enabled MN is expected to switch communications with a CN to the optimised route after handover faster than using the other approaches considered in this paper.

V. SECURITY DISCUSSION

Nikkander and Arkko [4] conjectured that the Return Routability procedure is vulnerable to attacks from nodes on the path between the CN and the MN. Under this premise, MIPv6 specifies that the packet payload should use end-to-end protection such as IP security (IPsec). However, MIPv6 MNs may still suffer denial of service or flooding. Hence, both FMIPv6-RR and PB-FMIPv6 are vulnerable to this kind of attack.

ERO aims to securely authenticate MNs without preconfigured credentials or public-key infrastructure. In order to do so, it relies on a secure exchange of a home address keygen token. The home address test also provides strong authentication because the home address is a Cryptographically Generated Address (CGA). This type of address has the property of being cryptographically and verifiably bound to a public/private key pair. In this manner, the MN proves ownership of the home address by evidencing knowledge of the corresponding private key.

PRO-FMIPv6 is as secure as the RR procedure, with the advantage that in cases where the IP addresses are spoofed, it is virtually impossible to redirect the traffic to any other node on the Internet. This is because the new IP address is composed from two randomly generated tokens. However, DoS is still a threat. ERO, despite being costly in terms of processing requirements, is the most secure protocol of the approaches considered.

VI. CONCLUSIONS

In this paper, the PRO-FMIPv6 protocol has been proposed. This signalling protocol allows for faster and more efficient FMIPv6 handovers because the MN updates the binding cache of the CN while the link layer handover procedures are being carried out, and makes use of a different approach than Return Routability for securing the home and care-of address checks.

The performance of this protocol has been measured in terms of route optimised handover latency. Simulation results confirm the PRO-FMIPv6 protocol achieves a reduction up to 50% in comparison with other relevant protocols: base Return Routability, Proactive Bindings and Enhanced Route Optimization, in cases where the link layer handover is either negligible or significant.

In those cases where link layer handover delay is significant, PRO-FMIPv6 is as efficient as PB-FMIPv6, while the other protocols under consideration affect negatively the packet reception at the MN.

A security analysis has been also carried out in this paper. Results point out that PRO-FMIPv6 is as safe as Return Routability or Proactive Bindings. Alternatively, Enhanced Route Optimization is safer than these other protocols, but it is also more computationally expensive.

REFERENCES

[1] Koodli, R., "Fast Handovers for Mobile IPv6", IETF RFC 5268, July 2005.
[2] Johnson, D., Perkins, C. and J. Arkko, "Mobility Support in IPv6", IETF RFC 3775, June 2004.
[3] Ng, C. and F. Zhao, "Network Mobility Route Optimization Solution Space Analysis", IETF RFC 4889, July 2007.
[4] Nikander, P. and J. Arkko, "Mobile IP Version 6 Route Optimization Security Design Background", IETF RFC 4225, December 2005.
[5] Vogt, C. and J. Arkko, "A Taxonomy and Analysis of Enhancements to Mobile IPv6 Route Optimization", IETF RFC 4651, February 2007.
[6] Yousaf, F.Z. and C. Wietfeld, "Proactive Bindings for FMIPv6", IETF Work in progress, May 2008.
[7] Arkko, J. and C. Vogt, "Enhanced Route Optimization for Mobile IPv6", IETF RFC 4866, May 2007.
[8] INET Framework for OMNeT++, OMNeT++ Community Site, http://www.omnetpp.org/
[9] Van Hanh, N. and S. Ro, "Simplified Fast Handover in Mobile IPv6 Networks", Computer Communications, 2008, doi: 10.1016.
[10] Abley, J. et al, "Goals for IPv6 Site-Multihoming Architectures", IETF RFC 3582, August 2003.
[11] Huston, G., "Architectural Approaches to Multihoming for IPv6", IETF RFC 4177, September 2005.
[12] The IEEE 802.21 Working Group, http://www.ieee802.org/21

APPENDIX A
NON-OPTIMISTIC-DAD PRO-FMIPv6 SIGNALLING

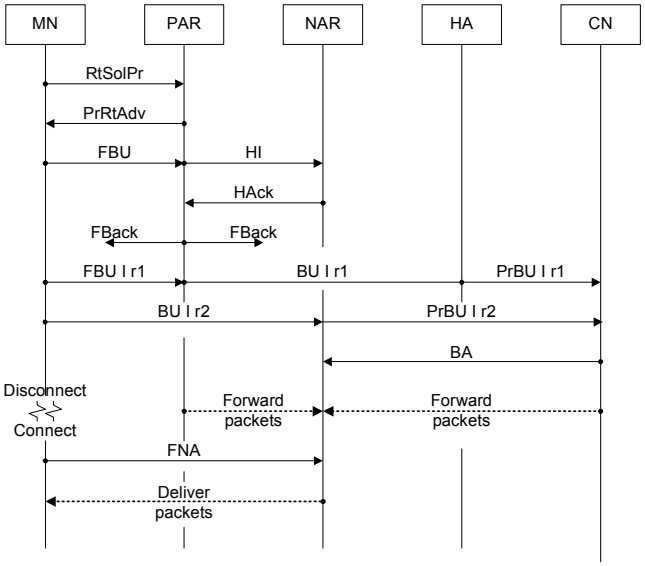


Fig. 7. Non-optimistic-DAD PRO-FMIPv6 signalling