MCMIPv6: Multicast Configuration-based Mobile IPv6 Protocol

Mohamed Oussama Cherif[1,3], Sidi Mohammed Senouci[2], Bertrand Ducourthial[3]

[1]Orange Labs, Core Network Laboratories, 2 Avenue Pierre Marzin, 22307, Lannion, France
[2]ISAT, University of Bourgogne, 49 rue Mademoiselle Bourgeois, BP.31, 58027, Nevers, France
[3]Laboratory CNRS Heudiasyc UMR6599, Centre de Recherche de Royallieu, B.P. 20529, Compiègne, France

Abstract – Mobile IPv6 (MIPv6) and its basic extension for network mobility NEMO were initially designed to manage the mobility of device users and networks respectively while maintaining a permanent IP address. Nevertheless, the different MIPv6's experiments have shown many lacks in case of high mobility of nodes such as in vehicular networks. To overcome these lacks, many solutions have been proposed by the research community. The most famous ones are HMIPv6 and FMIPv6 tackling each a specific issue. On the one hand, FMIPv6 introduces a solution to effectively minimize the L2/L3 latency and avoid the packets losses during the handover procedure. On the other hand, HMIPv6 is especially efficient in case of local mobility and permits in this case to minimize the signaling cost and improve the latency slightly. In this paper, we propose and evaluate a new vehicular mobility management protocol called MCMIPv6 (Multicast Configuration-based Mobile IPv6 protocol). MCMIPv6 is based on two main ideas: (i) definition of a new packet transmission way in visited networks based on a multicast communication and (ii) proposition of an efficient stateful configuration scheme to obtain addresses in visited networks. We used Qualnet simulator to compare the performances of our protocol, MCMIPv6, to those of existing solutions and show the different performance improvements in terms of handover latency and signaling cost.

Index Terms: **Mobile networks, Vehicular networks, Multicast, MIPv6, HMIPv6, FMIPv6.**

I. Introduction

One of the most interesting research topics in wireless networks is the optimization of the handover procedure. In fact, an IP address has a dual function: (i) unique identification of the mobile node (MN) in the network and (ii) localization of the MN in the network. This duality can not be guaranteed in case of node mobility. Indeed, when changing the associated access point (AP) in a handover procedure, the location of the node in the network changes, so, its address must change too. As this address is used to identify the node as packets' sender or receiver in the existing sessions, any address change leads to a session interruption. In case of mobile IPv6 networks, Mobile IPv6 (MIPv6) [1] brings a solution to this problem by defining two addresses for each mobile node (MN). One fix address, known by all the correspondents, associated with a home agent (HA) and called home address, and a care of address (CoA) that changes in proportion as the node moves between foreign networks. When a packet, sent by the correspondent node (CN) and is intercepted by the HA, it is immediately encapsulated using the CoA and sent to the MN through an IP tunnel.

Although MIPv6 gave a solution for address semantic duality, it still remains some problems related to it. In fact, MIPv6 suffers particularly from two problems: (i) high handover signaling costs and (ii) handover latency. This is accentuated especially in case of high velocity of mobile nodes (e.g. vehicular networks). With each handover, the new CoA has to be sent to the HA to permit it to update the matching (Home-Address/CoA) in its binding table. During this time, the node can neither send nor receive any application traffic.

On the one hand, to resolve the first problem, a hierarchical variant of MIPv6 (HMIPv6) [2] is proposed. It uses a new MIPv6 node called MAP (Mobility Anchor Point) to handle Mobile IP registration locally. On the other hand, to reduce the MIPv6 handover latency, the IETF has proposed Fast MIPv6 [3]. FMIPv6 focuses on reducing the CoA acquisition latency via an address pre-configuration method based on L2 signaling and by obtaining the network prefix information of the new access router (NAR) from the previous access router (PAR). The two protocols are described in the next section.

In this paper both macro-mobility and micro-mobility issues are tackled. We focus on the definition of a robust high mobility management scheme permitting to optimize the handover procedure in high mobile networks in general and particularly in vehicular networks. To this end, we present a new hard handover management protocol called Multicast Configuration-based MIPv6 protocol (MCMIPv6). MCMIPv6 uses multicast communication to send packets to more than one AR and defines a unique identifier for each mobile node to simplify the CoA configuration. MCMIPv6 is well suited for both delay-sensitive and data-loss-sensitive applications.

The rest of this paper is structured as follows. Section II details the function of HMIPv6 and FMIPv6 and other relevant related works. In Section III, we describe our proposed protocol MCMIPv6. After the presentation of the simulation results in Section IV, we conclude the paper and give some perspectives to our work in Section V.

II. Background

There are two manners to perform a handover between two visited networks: (i) hard handover: in which connectivity with the previous Access router (AR) is lost before establishing a new one with the new AR and (ii) soft handover: in which connectivity with the new AR is established before loosing a old one with the previous AR. In this section, we describe the function of two relevant hard handover management protocols: *Hierarchical MIPv6* (HMIPv6) and *Fast MIPv6* (FMIPv6), and give an overview of the other most relevant hard handover management protocols.

1) HMIPv6: Hierarchical MIPv6

HMIPv6 is an experimental handover management protocol that aims at: (i) reducing the signalization cost between the mobile node, its home agent (HA) and the correspondent node (CN) in a context of local mobility, and (ii) improving (slightly) the handover latency. In HMIPv6, the CN and the HA maintain the same functionalities as in MIPv6. The novelty is in the foreign network. Indeed, HMIPv6 proposes a hierarchical architecture for these networks. A node called Mobility Anchor Point (MAP) can be located at any level of this hierarchy to make the micro-mobility in its domain transparent for the upper located MAPs and the HA even if the MN changes its Access Router (AR) and then its Care of Address (CoA). When entering a new MAP domain, the MN receives a *Router Advertisement* messages containing the new MAP's information. Thus, the MN can create a couple of addresses: (i) Regional CoA (RCoA) that is still unchangeable as long as the MN is in the domain, and (ii) Local CoA (LCoA) that changes each time the MN changes the AR, even in the same domain. The MAP keeps a match (RCoA, LCoA) and sends the RCoA to the HA that keeps a match (Home-Address, RCoA). Then, a first IP tunnel is created between the HA and the MAP and a second IP tunnel is created between the MAP and the MN. When the HA receives a packet intended for the MN, it encapsulates it using the match (Home-Address, RCoA) and sends it to the MAP which decapsulates the packet, re-encapsulates it using the match (RCoA, LCoA) and sends it to the MN. We can notice that the MAP acts as a second HA (in the Foreign Network). HMIPv6 shows some deficiencies, especially when the user's mobility is not local. In this case, performance of HMIPv6, in terms of delays for packet delivery, is worse than that of MIPv6, due to the encapsulation processing by the MAP. As a result, packets must be encapsulated (IP-within-IP encapsulation) at each encapsulation level in the foreign network. This engenders some costs, extra overhead and especially higher delays. Many applications like video streaming and some transport protocols like TCP can not tolerate a great delay and interpret it as congestion indication.

2) FMIPv6: Fast MIPv6

Fast MIPv6 is an experimental handover management protocol. It aims mostly at improving the handover latency. To do that, FMIPv6 does not address any radio access discovery process. In fact, it exploits the L2 information to anticipate the selection of a New AR (NAR) and a New CoA (NCoA) while being connected to the Previous AR (PAR). The layer two (L2) received information permits to the Mobile Node (MN) to prepare for the imminent handover in advance. So, it sends a *Router Solicitation for Proxy Advertisement (RtSolPr)* to the PAR. The PAR, memorizing MAC addresses and subnet prefixes of the neighbouring ARs, assists the NCoA establishment by resolving subnet prefixes based on the reported L2 information before sending a *Proxy Router Advertisement (PrRtAdv)* to the MN. Therefore, the MN does not need to discover the available ARs by actively scanning all the communication channels. All it has to do is the sending of a *Fast Binder Update (FBU)* to the PAR in which it specifies the chosen NAR. Then, the handover could be initiated, in advance, by both the PAR and the NAR by establishing a NCoA for the MN and setting up an IP tunnel between the two ARs. When a handover must be set off, the PAR starts forwarding the MN's traffic to the NAR via the IP tunnel. After establishing link connectivity with the NAR, the MN sends a *Fast Neighbour Advertisement (FNA)* to notify the NAR of its presence. So, the NAR begins delivering the MN's traffic, received from the PAR during the handover, to the MN. At this time, the MN informs its HA about its NCoA and terminates the handover procedure. Thus, anticipating L2 handover in FMIPv6 permits to save a considerable amount of time which contributes significantly to the entire handover latency (in 802.11b, the L2 scan time is upper than 400ms).

Although the FMIPv6's handover anticipation method reduces effectively the handover latency, it still remains some difficulties related to this protocol: (i) contrary to HMIPv6, the handover procedure is not local; the HA must be informed each time the MN changes the AR and establishes a new CoA, (ii) the communication process (between PAR and NAR) that enables the construction of *PrRtAdv* messages is not specified for FMIPv6. To address this issue, the IETF SEAMOBY WG proposes Candidate Access Router Discovery (CARD) protocol [4], (iii) time required to prepare the FMIPv6 handover (*RtSolPr*, *PrRtAdv*, *FBU*) may be not long enough to anticipate the MN's mobility, and (iv) the MN may not move to the originally anticipated NAR's network. It may maintain the same AR or goes to another AR's area. This phenomenon known as *ping-pong* movement could lead, in case of FMIPv6, to important packet losses and long handover latencies.

3) Other hard handover management protocols

In addition to HMIPv6 and FMIPv6, other interesting handover management solutions have been proposed.

In [5], the authors proposed *Fast handover HMIPv6* (F-HMIPv6). F-HMIPv6 defines the same architecture as HMIPv6 and uses the same signaling messages as FMIPv6, but the handover IP tunnel is established between MAP and NAR, rather than between PAR and NAR. For this reason, the MN exchanges the handover's signaling messages with MAP, instead of PAR. Even if F-HMIPv6 permits to make the handover procedure local to the foreign network, other issue as IP-within-IP encapsulation, insufficient handover preparation time and ping pong movement's problem persist.

In [6], the authors proposed an extension of F-HMIPv6 called Fast handover Multi-tunnel HMIPv6 (FM-HMIPv6). The subjacent idea of FM-HMIPv6 is to not limit the IP tunnelling to one NAR. In fact, based on the exchanged signaling messages, the MAP could establish many IP tunnels with more than one hypothetical NAR. This solution permits to solve the ping pong movement's problem. In return, it introduces more cost in term of IP-within-IP encapsulation.

In the next section, we propose a new efficient hard handover management protocol: Multicast Configuration-based MIPv6 (MCMIPv6).

III. Multicast Configuration-based MIPv6

Multicast Configuration-based MIPv6 (MCMIPv6), the protocol proposed in this paper, aims to support an effective and optimized hard handover management.

A. *Principle*

If the mobile node (MN) changes its Access Router (AR) frequently, the overhead due to signaling messages introduced by non hierarchical mobility management protocols (Mobile IPv6, FMIPv6, etc.) increases. As HMIPv6, MCMIPv6 permits to manage the mobility locally. Then, it introduces a new conceptual entity, called "Rendez-Vous Point" (RVP), that permits to use the multicast communication to handle mobility management (see Figure 1). In fact, each RVP is associated to an RVP-domain and is in charge of managing a multicast tree that makes the mobility of each mobile node in this domain transparent for its home agent.

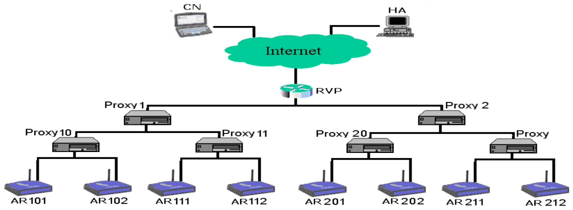

Figure 1. MCMIPv6 architecture

Initially, when joining its home network, each MN obtains a couple of home address "H_Addr" and group identifier "groupID". The group identifier is a 32-bit integer assigned to each MN by its home agent (HA). The HA has to ensure the uniqueness of this parameter. In [10], many procedures to create the group identifier are introduced. One of the described procedures proposes a match between the MAC address and the group identifier.

When the MN goes in a new RVP-domain, it sets off a procedure to obtain a couple of addresses (multicast address, CoA). This procedure, called *inter-RVP-domain handover*, is described in the next subsection.

B. *Inter-RVP-domain handover*

The inter-RVP-domain handover is illustrated in Figure 2. When attached to the PAR (Previous AR in the Previous RVP domain), the MN anticipates the handover procedure using *RtSolPr* and *PrRtAdv* to exchange New ARs (NARs) information with the Previous AR (PAR). After choosing the NAR to join, the MN sends a *BU* (Binder Update) message to the PAR. This message contains its current care of address (PCoA) and specifies the handover mode to "inter-RVP-domain". Then, the PAR can send a *HI* (Handover Initiation) message containing MN's information to the NAR. The NAR looks into the handover possibility. If it accepts the MN's handover it creates locally a New CoA (NCoA) as described in a next paragraph and can start the multicast address creation procedure .This procedure, based on the group identifier, is described later. When the multicast address is created, the NAR sends a *Hack* (Handover Acknowledgement) to the PAR. Then, the PAR can send a *BAck* (Binder Acknowledgement) to the MN in which it includes the NCoA and the multicast address. As the Mode value was set to "inter-RVP-domain" in *BU* message, the NAR uses the MLDv2 protocol [11] to inform the RVP of the joining of a new multicast group. To do that, the NAR broadcasts a *HearIPv6Multicast* (Hear IPv6 Multicast) message on the local link. The Proxy, situated in the next hierarchy level between the NAR and the RVP, subscribes itself as a receiver of the multicast packets; this process is reproduced at each level until reaching the RVP. Then, the RVP uses the PIM-SSM protocol [12] to join the HA. It sends a *PIM join* message to the HA. Therefore, an IP tunnel relating the HA and the RVP could be created and this latter could notify the MN, the NAR and the hierarchical proxies of the IP tunnel creation using a *MCast_Addr_Notif* (Multicast Address Notification). Thenceforth, both NAR and PAR receive the MN's packets via two different RVPs. When the MN gets the connection to the NAR, it sends a *RSol* (Router Solicitation) message including a fast neighbor advertisement to inform its presence. Then, the NAR will deliver the waiting packets to the MN and sends a *MCastQuitReq (Multicast Quit Request)* to the PAR to remove the old multicast link.

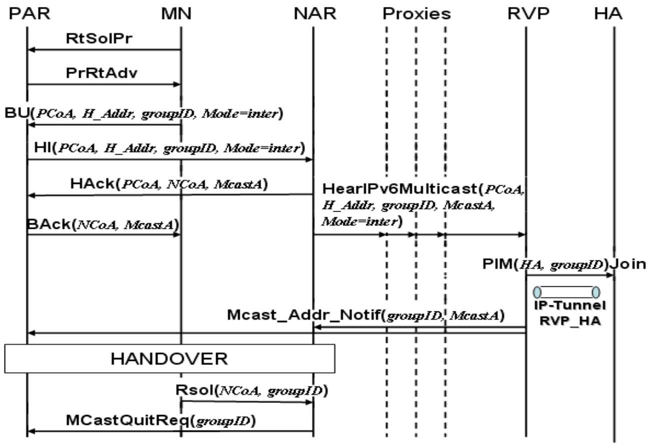
PAR
MN
NAR
Proxies
RVP
HA
RtSolPr
PrRtAdv
BU(PCoA, H_Addr, groupID, Mode=inter)
HI(PCoA, H_Addr, groupID, Mode=inter)
HAck(PCoA, NCoA, McastA)
HearIPv6Multicast(PCoA, H_Addr, groupID, McastA, Mode=inter)
BAck(NCoA, McastA)
PIM(HA, groupID)Join
IP-Tunnel RVP_HA
Mcast_Addr_Notif(groupID, McastA)
HANDOVER
Rsol(NCoA, groupID)
MCastQuitReq(groupID)

Figure 2. Inter-RVP-domain handover procedure

C. *Intra-RVP-domain handover*

In this subsection we describe briefly the handover procedure when the mobile node (MN) changes its associated Access Router (AR) within the same RVP-domain. The intra-RVP-domain handover is illustrated in Figure 3.

When a MN has to perform an intra-RVP-domain handover, the MN sends a *BU* (Binder Update) message to the Previous

AR (PAR). This message contains its current care of address (PCoA) and specifies the handover mode to "intra-RVP-domain". Then, the PAR can send a *HI* (Handover Initiation) message containing MN's information to the NAR. The NAR looks into the handover possibility. If it accepts the MN's handover, it creates locally a New CoA (NCoA) as described in the next paragraph, sends a *Hack* (Handover Acknowledgement) and broadcasts a *HearIPv6Multicast* (Hear IPv6 Multicast) message on the local link. If the NAR and the PAR are not attached to the same local link, the proxy situated in the next hierarchy level between the NAR and the RVP subscribes itself as a receiver of the multicast packets. This process is reproduced at each level until reaching a proxy that is already subscribed to the multicast packets. On the other hand, the PAR can send a *BAck* (Binder Acknowledgement) to the MN. When the MN gets the connection to the NAR, it sends a *RSol* (Router Solicitation) including a fast neighbor advertisement to inform its presence. Then, the NAR will deliver the packets to the MN and sends a *MCastQuitReq* (Multicast Quit Request), having the group identifier as parameter, to the PAR to remove the old multicast link.

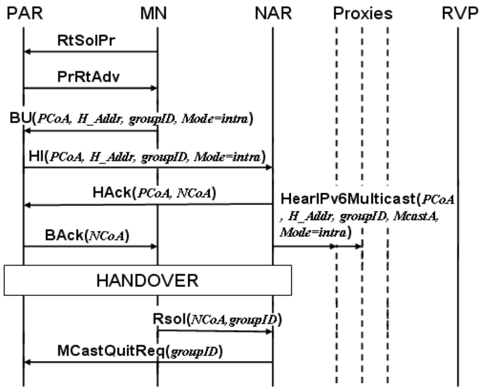
PAR
MN
NAR
Proxies
RVP
RtSolPr
PrRtAdv
BU(PCoA, H_Addr, groupID, Mode=intra)
HI(PCoA, H_Addr, groupID, Mode=intra)
HAck(PCoA, NCoA)
HearIPv6Multicast(PCoA, H_Addr, groupID, McastA, Mode=intra)
BAck(NCoA)
HANDOVER
Rsol(NCoA,groupID)
MCastQuitReq(groupID)

Figure 3. Intra-RVP-domain handover procedure

D. *Creation of CoA*

In our model we used a stateful address auto-configuration scheme. Each AR is in charge of the creation of CoAs of MNs joining its subnetwork. We proposed to reserve, at least, 32 bits for the interface identifier (in all unicast addressing architectures proposed in [13], 64 bits are reserved for the interface identifier). Therefore, the interface identifier field could contain the group identifier of the node. By this way, the group identifier uniqueness ensures the CoA uniqueness.

E. *Creation of multicast address*

There are two types of multicast addresses: (i) permanently-assigned IPv6 multicast addresses and (ii) non- permanently-assigned IPv6 multicast addresses. The main three classes of non-permanently-assigned IPv6 multicast addresses are: (i) Unicast-Prefix-based IPv6 Multicast addresses [9], (ii) Embedded-RP IPv6 Multicast addresses [8], and (iii) Source-Specific Multicast (SSM) addresses [9]. In case of MCMIPv6 we proposed using the Source-Specific Multicast addresses. The FF3X::/32 prefix is reserved for theses addresses, but the *Internet Assigned Numbers Authority* (IANA) suggests to use firstly the addresses derived from FF3X::/96 prefix. Then the format of Multicast Address assigned by an AR for a MN having a group identifier "groupID" is shown in Figure 4.

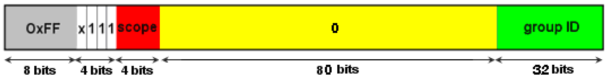

Figure 4. Multicast addresses format

IV. Performance Evaluation

To evaluate the performance of the proposed protocol (MCMIPv6), we used Qualnet Simulator [7]. The performances of MCMIPv6 are then compared to those of MIPv6, HMIPv6, FMIPv6 and FHMIPv6 in terms of handover delay and signaling costs.

A. *Simulation Setup*

In our 100-second simulations, the vehicles' velocities vary between 25 and 90 km/h and their communication range is about 150m. We used the network topology shown in Figure 5.

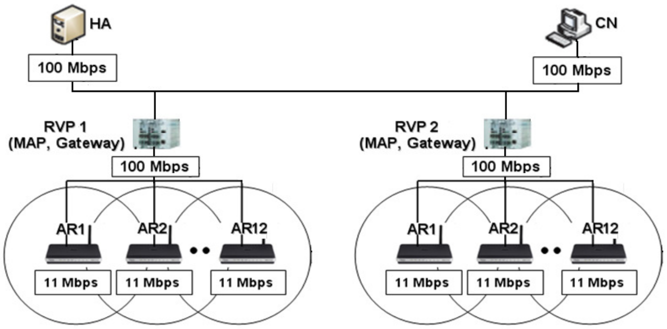

Figure 5. The simulation network topology

B. *Simulation results*

To evaluate the performances of our protocol, we focused on two performance metrics: (i) handover latency and (ii) handover signaling cost. The former represents the delay between the loss of connectivity with the PAR and the establishment of a new connectivity with the NAR. The latter shows the amount of the signaling exchanged packets.

1) *Handover latency*

Figure 6 shows the intra-domain handover latency (intra-RVP-domain for MCMIPv6 and handover between ARs in the same MAP domain for HMIPv6 and FHMIPv6) of the five simulated protocols. The localization of the handover process in the MAP domain permits to HMIPv6 to improve the MIPv6 latency (~ 48 ms). In fact, in case of HMIPv6, only the MAP has to be informed by the new LCoA (Local CoA) and there are no need to inform the HA. The anticipation of the handover preparation permits to reduce the latency efficiently by eliminating the L2 handover latency (~ 400 ms); then the handover latency in case of FMIPv6 is about 104 ms. In case of FHMIPv6, where the MAP hierarchical architecture is introduced, the handover is also prepared in advance, but in addition when obtaining a new CoA, only the MAP has to be informed by this new address. Hence, FHMIPv6 permits to decrease the FMIPv6 latency by 34 ms.

Our protocol, MCMIPv6, anticipates the handover preparation using the same mechanism as FMIPv6 and FHMIPv6. But, contrary to these two protocols, neither the HA nor the RVP has to be informed by the new CoA. Only a limited number of proxies in the foreign network have to subscribe to the multicast session. In our case, we obtained a handover latency of 23 ms.

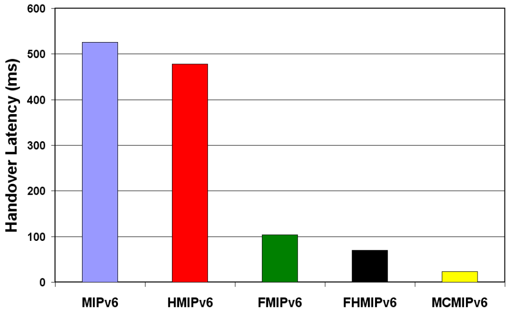

Figure 6. Intra-domain handover latency

Figure 7 shows the inter-domain handover latency (inter-RVP-domain for MCMIPv6 and handover between ARs in different MAP domains for HMIPv6 and FHMIPv6) of the five simulated protocols. In case of HMIPv6 and FHMIPv6, a couple (Regional CoA, Local CoA) has to be generated for the MN, then, the MAP has to inform the HA by the new RCoA. Hence HMIPv6 latency (540 ms) is greater than MIPv6 latency (526 ms) and FHMIP latency (109ms) becomes greater than FMIPv6 latency (104 ms). MCMIPv6 anticipates the obtainment of a multicast address and the establishment of a new multicast tree in the RVP-domain. So the handover latency still remains 23 ms.

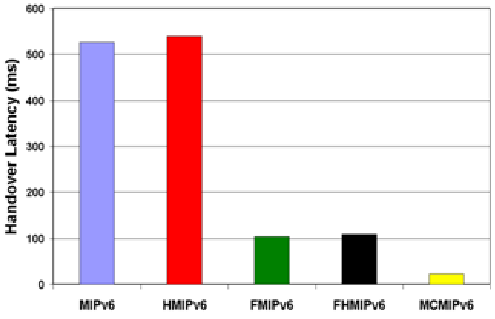

Figure 7. Inter-domain handover latency

2) *Handover signaling cost*

Figure 8 shows the signaling cost of the five protocols. MIPv6 and HMIPv6 procure the lowest handover signaling cost since no handover anticipation is needed. FMIPv6, FHMIPv6 and MCMIPv6 use more signaling traffic due to the handover anticipation signaling. The results obtained in case of MCMIPv6 are better than those of FMIPv6 and FHMIPv6 because the CN has not to inform the HA or the RVP each time it changes its CoA.

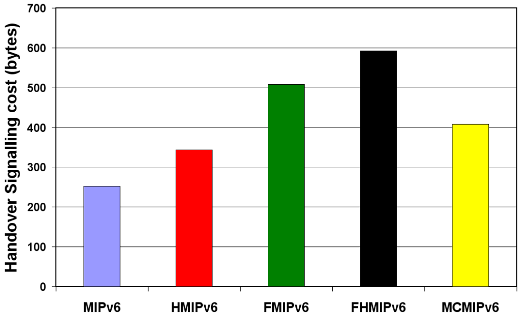

Figure 8. Handover signaling cost

V. CONCLUSION

Mobility management is an interesting issue for mobile networks. There are many challenges related to mobility management such as: (i) minimization of delays and signaling costs and (ii) management of the handover operation locally (without exchanging signaling traffic with the home agent).

In this work we proposed a new IPv6 hard handover management protocol called MCMIPv6 which introduces the use of multicast communication to manage the handover locally in the visited network and improve the handover performances in high mobile networks in general and particularly in vehicular networks. MCMIPv6 also defines a specific stateful configuration module which allows ensuring the addresses uniqueness.

The performance evaluation via simulation study shows that MCMIPv6 improves the results of existing solutions in terms of handover latency and signaling traffic.

Our next researches are: (i) making an analytical study to look into the effects of the RVP-domain size on the MCMIPv6 performances and (ii) implementing MCMIPv6 in our testbed platform to evaluate its performances within the context of vehicular networks.

REFERENCES

[1] RFC 3775: http://www.ietf.org/rfc/rfc3775.txt.
[2] RFC 4140: http://www.ietf.org/rfc/rfc4140.txt.
[3] RFC 4068: http://www.ietf.org/rfc/rfc4068.txt.
[4] RFC 4066: http://www.ietf.org/rfc/rfc4066.txt.
[5] H.Y. Jung, E.A. Kim, J.W. Yi and H.H. Lee, “A scheme for supporting fast handover in hierarchical mobile IPv6 networks”, ETRI Journal, vol. 27, no. 6, pp. 798-801, December 2005.
[6] D-C. Shin and S-G. Min, “Fast Handover Solution using Multi-tunnel in HMIPv6 ”, SENSORCOMM’08, August 08 - Cap Esterel, France.
[7] Qualnet Simulator: http://www.scalable-networks.com.
[8] RFC 3618: http://www.ietf.org/rfc/rfc3618.txt.
[9] RFC 3306: http://www.ietf.org/rfc/rfc3306.txt.
[10] RFC 3307: http://www.ietf.org/rfc/rfc3307.txt.
[11] RFC 3810: http://www.ietf.org/rfc/rfc3810.txt.
[12] RFC 3569: http://www.ietf.org/rfc/rfc3569.txt.
[13] RFC 3513: http://www.ietf.org/rfc/rfc3513.txt.